RETECH Redes Territoriales de Especialización Tecnológica

RED ARGOS

Movilidad Inteligente y Cibersegura

Diciembre de 2025

Versión 1.0

Junta de Andalucía

Financiado por la Unión Europea NextGenerationEU

Gobierno de España — Ministerio para la Transformación Digital y de la Función Pública — Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales

Plan de Recuperación, Transformación y Resiliencia

incibe_ Instituto Nacional de Ciberseguridad

Junta de Andalucía

Agencia Digital de Andalucía

Objeto del Expediente:

“ELABORACIÓN DE GUÍAS DE CIBERSEGURIDAD IOT PARA ENTORNOS DE SMART CITIES Y SALUD” (CONTR 2024 829153).

Esta guía forma parte de la colección Guías de Ciberseguridad en IoT para las Smart Cities y el sector Salud creada por la Agencia Digital de Andalucía como parte del Proyecto Red Argos, perteneciente al programa RETECH, de Redes Inteligentes de Especialización Tecnológica, en el marco del Plan de Recuperación, Transformación y Resiliencia, financiado por la Unión Europea-NextGenerationEU, a través de INCIBE.

Autor del documento: Agencia Digital de Andalucía

Tipo de documento: Guía

Fecha de elaboración: 10/12/2025

Fecha de última actualización: 10/12/2025

ÍNDICE DE CONTENIDOS

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
Junta de Andalucía
Agencia Digital de Andalucía

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

1. Introducción

La movilidad urbana está experimentando una transformación acelerada hacia modelos inteligentes, conectados y sostenibles. En este nuevo paradigma, vehículos, infraestructuras y plataformas digitales interactúan de forma continua mediante tecnologías IoT, comunicaciones avanzadas y sistemas de análisis de datos. Gracias a esta interconexión es posible optimizar el tráfico, mejorar la eficiencia energética, integrar modos de transporte heterogéneos y ofrecer servicios orientados al ciudadano de manera más eficiente.

Sin embargo, esta evolución viene acompañada de un incremento notable en la superficie de exposición a ciberamenazas. Los dispositivos IoT desplegados en la vía pública, las redes de comunicaciones que soportan el intercambio de información, los vehículos conectados y las plataformas centrales de gestión pueden convertirse en objetivos de ataques capaces de afectar a la seguridad, comprometer la integridad de los datos o interrumpir servicios esenciales de movilidad.

En este contexto, la ciberseguridad del IoT aplicado a la movilidad inteligente se ha convertido en un elemento esencial para asegurar la fiabilidad de las infraestructuras conectadas, la continuidad de los servicios urbanos y la protección de los usuarios. Garantizar este entorno requiere un enfoque integral que combine soluciones tecnológicas robustas, marcos regulatorios adecuados, prácticas de gestión coordinadas y una estrecha colaboración entre administraciones públicas, operadores de movilidad y proveedores tecnológicos.

2. Objetivo y alcance

2.1. Objetivo

La presente guía tiene como propósito ofrecer un marco de referencia claro y estructurado para comprender, analizar y gestionar la ciberseguridad en los sistemas de movilidad inteligente basados en tecnologías IoT. A través del estudio del ecosistema urbano conectado, de la infraestructura tecnológica de los vehículos inteligentes y de los servicios digitales asociados, el documento aporta una visión integral de los elementos que conforman la movilidad inteligente y de las amenazas que afectan a su seguridad.

Los objetivos específicos de la guía son:

- Describir la arquitectura tecnológica de la infraestructura urbana conectada y de los vehículos inteligentes, incluyendo sus componentes IoT, sistemas OT y mecanismos de comunicación.
- Identificar y clasificar las amenazas asociadas a los sistemas de movilidad urbana inteligente, considerando tanto vulnerabilidades técnicas como operativas.
- Presentar el marco regulatorio, normativo y de buenas prácticas aplicable a soluciones IoT y sistemas inteligentes de transporte dentro del contexto español y europeo.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

- Proponer criterios, medidas de protección y estrategias de mitigación orientadas a garantizar la resiliencia, disponibilidad y confiabilidad de las infraestructuras y servicios de movilidad conectada.

De esta forma, la guía pretende servir como documento de apoyo para responsables de ciberseguridad, administraciones públicas, operadores de servicios urbanos, proveedores tecnológicos y cualquier entidad implicada en el diseño, despliegue o gestión de infraestructuras y servicios de movilidad inteligente.

2.2. Alcance

El presente documento delimita su alcance al análisis de los sistemas y componentes que conforman el ecosistema de movilidad inteligente, con especial atención a aquellos elementos basados en tecnologías IoT y sistemas conectados. En particular, incluye:

- Vehículos conectados y autónomos, independientemente de su motorización (eléctricos, híbridos o de combustión).
- Infraestructuras urbanas sensorizadas, como semáforos inteligentes, señalización dinámica, estaciones de carga eléctrica, sensores de tráfico y cámaras digitales.
- Redes de comunicación y plataformas de gestión, incluyendo soluciones V2X, sistemas de smart parking, smart grid vinculada a movilidad y plataformas de operación de flotas o servicios municipales.
- Procesos y consideraciones de ciberseguridad aplicables a dispositivos IoT, sistemas OT y plataformas asociadas al funcionamiento de la movilidad urbana conectada.

Quedan excluidos del alcance los aspectos estrictamente técnicos de diseño mecánico o industrial de los vehículos y de la infraestructura física que no tengan relación directa con IoT o ciberseguridad.

3. Referencias normativas

El presente documento se apoya en un marco regulatorio y técnico amplio que integra normativa legal, estándares internacionales y guías de buenas prácticas específicamente aplicables a la movilidad inteligente en entornos urbanos conectados.

Dicho marco constituye la base metodológica y conceptual sobre la que se estructura esta guía, asegurando la coherencia con las políticas europeas, nacionales e internacionales en materia de ciberseguridad, movilidad conectada, tratamiento de datos personales e infraestructuras críticas.

- **Normativas**:
  - Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales (en adelante, CRA).
  - Reglamento (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativo a las medidas para asegurar un alto nivel común de ciberseguridad en la UE (en adelante, NIS2).

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

- Reglamento (UE) 2019/2144 del Parlamento Europeo y del Consejo de 27 de noviembre de 2019 relativo a los requisitos de homologación de tipo de los vehículos de motor.
- Reglamento (UE) 2018/858, del Parlamento Europeo y del Consejo de 30 de mayo de 2018 regula la homologación de vehículos, sus remolques y componentes.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales (en adelante, RGPD).
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (en adelante, LOPDGDD).
- UNECE/R155, Reglamento N°155 de la Comisión Económica para Europa de la ONU, que establece disposiciones de seguridad para la homologación de vehículos.

- **Estándares**:
  - IEC 62443, Seguridad para sistemas de automatización y control industrial.
  - ISO/IEC 27400, Seguridad y privacidad en IoT.
  - ISO/IEC TR 23188:2020, Ecosistemas de Edge Computing.
  - ISO/IEC 27001, Gestión de la seguridad de la información.
  - ISO/IEC 27017 y 27018, Seguridad y privacidad en servicios cloud.
  - ISO/IEC 22301, Gestión de la continuidad de negocio.
  - ISO/IEC 50001, Gestión del suministro eléctrico.
  - ISO/SAE 21434, Ciberseguridad en vehículos.
  - UNE 178107, Estándares para la gestión de infraestructuras en Ciudades Inteligentes.

- **Guías**:
  - Cloud Security Alliance (CSA), Matriz de controles Cloud (CCM).
  - ENISA, Guía para la securización de IoT.
  - Guías CCN-STIC del Esquema Nacional de Seguridad (811, 823, 824, 881, 891).
  - Guía NIST SP 800-53 y SP 800-115 (controles y pruebas técnicas de seguridad).
  - OWASP IoT y OWASP, Guías de auditorías técnicas.

4. Definiciones

Acrónimos	Definición
ACC	Control de crucero adaptativo que ajusta velocidad según el tráfico (del inglés, Adaptive Cruise Control).
ADAS	Sistemas avanzados de asistencia al conductor (del inglés, Advanced Driver Assistance Systems).
AEB	Frenado automático de emergencia (del inglés, Automatic Emergency Braking).
ANPR	Reconocimiento automático de matrículas mediante cámaras y software (del inglés, Automatic Number Plate Recognition).

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

Acrónimos	Definición
CCTV	Circuito cerrado de televisión para vigilancia y monitoreo en tiempo real (del inglés, Closed Circuit Television).
C-ITS	Sistemas de transporte inteligente que permiten comunicación entre vehículos e infraestructura (del inglés, Cooperative Intelligent Transport Systems).
DRM	Gestión de derechos digitales para controlar acceso y uso de contenido protegido (del inglés, Digital Rights Management).
EDR	Registrador de datos de eventos (del inglés, Endpoint Detection and Response).
Geofencing	Creación de límites virtuales que activan acciones cuando un dispositivo entra o sale de una zona.
LIDAR	Tecnología láser que mide distancias creando mapas 3D (del inglés, Light Detection and Ranging).
LKA	Asistente de mantenimiento de carril (del inglés, Lane Keeping Assist).
LPWAN	Red de baja potencia y largo alcance para IoT (del inglés, Low Power Wide Area Network).
MaaS	Integración de transporte público y privado en una sola plataforma digital (del inglés, Mobility as a Service).
Microhubs	Pequeños centros logísticos urbanos para distribución de última milla.
RSU	Unidad de carretera que comunica infraestructura con vehículos en V2X (del inglés, Road Side Unit).
SCOOT	Sistema adaptativo de control de tráfico que ajusta semáforos en tiempo real según el flujo vehicular (del inglés, Split Cycle Offset Optimisation Technique).
OBU	Unidad a bordo instalada en vehículos para comunicación V2X (del inglés, On Board Unit).
OTA	Actualización remota de software sin intervención física (del inglés, Over The Air).
V2X	Comunicación que conecta vehículos con infraestructura, peatones y redes para mejorar seguridad y tráfico (del inglés, Vehicle to Everything).

TABLA 1: DEFINICIONES EMPLEADAS.

5. Ecosistema de movilidad inteligente en Smart Cities

El ecosistema de movilidad inteligente en las Smart Cities integra un conjunto de infraestructuras, tecnologías y servicios diseñados para optimizar la circulación urbana, reducir el impacto ambiental, mejorar la seguridad vial y ofrecer nuevas soluciones de transporte basadas en datos. Este ecosistema se sustenta en la interconexión entre vehículos inteligentes, infraestructuras viales, plataformas digitales de gestión y servicios urbanos, generando un flujo continuo de información que permite tomar decisiones en tiempo real.

Concretamente, este ecosistema se basa en cuatro pilares fundamentales:

- Infraestructura urbana conectada, que actúa como la capa sensorial de la ciudad, recogiendo datos y gestionando elementos físicos del tráfico.
- Sistemas de transporte y movilidad urbana, que incluyen transporte público, servicios compartidos, micromovilidad y logística.
- Plataformas digitales avanzadas, encargadas del análisis de datos, operación del tráfico y optimización de recursos.
- Infraestructura de soporte, como las redes de carga eléctrica, comunicaciones V2X o sistemas energéticos inteligentes que garantizan la continuidad operativa de la movilidad conectada.

Este entramado permite que la ciudad funcione como un sistema dinámico, capaz de adaptarse a la demanda, anticipar incidencias y ofrecer servicios de movilidad más seguros, sostenibles y eficientes.

5.1. Infraestructura urbana conectada

La infraestructura urbana conectada constituye la base tecnológica que permite a los vehículos inteligentes y a los sistemas de movilidad operar de manera coordinada en la ciudad. Está compuesta por dispositivos IoT, sistemas de monitorización, equipamiento vial inteligente y elementos de control que permiten la gestión dinámica del tráfico.

Su función principal es dotar al entorno urbano de percepción, comunicación y capacidad de respuesta, proporcionando datos en tiempo real y actuando sobre elementos físicos de la vía. Esta infraestructura permite habilitar servicios V2I/V2X, optimizar flujos de tráfico, mejorar la seguridad y ofrecer información contextualizada a vehículos, peatones y operadores de movilidad.

A continuación, se describen los principales componentes.

5.1.1. Semáforos inteligentes

Los semáforos inteligentes integran sensores y algoritmos de control adaptativo que permiten regular la circulación de forma dinámica en función de las condiciones reales del tráfico. Su objetivo es reducir la congestión, optimizar los flujos de movilidad y aumentar la seguridad de peatones, ciclistas y vehículos.

❖ **Funcionalidades principales**

- Control adaptativo: ajustan automáticamente los tiempos de verde, ámbar y rojo según densidad de tráfico, flujos peatonales o congestión.
- Conectividad V2I: pueden enviar información a vehículos conectados, como estado del semáforo, tiempo restante, recomendaciones de velocidad.
- Priorización automática de transporte público: reducen tiempos de espera para autobuses, tranvías o vehículos prioritarios, como ambulancias y policías.
- Detección inteligente: incorporan cámaras, LIDAR o inductores magnéticos para identificar vehículos, peatones o ciclistas.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

- Integración con centros de control: se conectan con la plataforma municipal para coordinar redes de semáforos en toda la ciudad.

❖ **Caso de uso real**

Córdoba ha iniciado la implantación de semáforos inteligentes que integran cámaras, sensores y algoritmos de análisis en tiempo real para mejorar la seguridad vial y optimizar la movilidad urbana. Estos dispositivos permiten priorizar el paso de peatones con movilidad reducida y facilitar la convivencia entre vehículos, ciclistas y usuarios vulnerables, adaptando dinámicamente las fases semafóricas según el comportamiento detectado en la vía.

Uno de los casos más representativos es el semáforo instalado en la avenida del Aeropuerto, una de las arterias principales de la ciudad. Este dispositivo es capaz de ampliar hasta un 15 % el tiempo de cruce cuando detecta personas en silla de ruedas, con andador o con carritos de bebé, reduciendo el riesgo en pasos de gran afluencia.

5.1.2. Sensores IoT de tráfico

Los sensores IoT instalados en la vía pública proporcionan datos continuos sobre el comportamiento del tráfico urbano. Estos sensores pueden ser fijos, como postes y pavimentos, o móviles, instalados en vehículos municipales.

❖ **Funcionalidades principales**

- Conteo de vehículos, detección de velocidad y clasificación.
- Monitorización ambiental (ruido, calidad del aire, climatología).
- Análisis del uso de carriles y congestión de puntos críticos.
- Activación automática de respuestas en infraestructuras.

❖ **Caso de uso real**

Madrid ha desplegado una extensa red de sensores IoT urbanos destinada a monitorizar el estado del tráfico y apoyar la toma de decisiones en tiempo real dentro del Centro de Gestión de la Movilidad. Esta red combina sensores fijos instalados en pavimento, farolas, pórticos y postes, junto con sensores móviles integrados en vehículos municipales como autobuses, camiones de limpieza y patrullas policiales.

Los sensores recogen datos de volumen de tráfico, velocidad media, ocupación de carriles, ruido ambiental y calidad del aire, enviándolos de forma continua mediante redes 4G/5G y LPWAN a la plataforma municipal de datos. A partir de esta información, el sistema detecta automáticamente congestiones, retenciones inesperadas o patrones anómalos, activando respuestas como ajustes de los ciclos de los semáforos o avisos en paneles de mensajería.

5.1.3. Cámaras digitales

Las cámaras digitales de tráfico forman parte del sistema de supervisión urbano y permiten obtener información visual completa del estado de la circulación mediante el uso de tecnologías como CCTV, ANPR, captación estereoscópica o imagen térmica.

❖ **Funcionalidades principales**

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

- Cámaras CCTV: permiten la monitorización general del tráfico.
- Cámaras ANPR: realizan el reconocimiento automático de matrículas y control de accesos.
- Cámaras estereoscópicas: analizan el flujo de vehículos y su comportamiento en las vías.
- Cámaras térmicas: aseguran la detección continua incluso en túneles o condiciones meteorológicas adversas.

❖ **Caso de uso real**

La M-30 de Madrid integra una de las redes de cámaras de vigilancia y análisis automático más avanzadas de España, gestionada desde el Centro de Control de Madrid Calle 30. Más de un millar de cámaras CCTV, ANPR y térmicas cubren túneles, accesos y tramos exteriores, permitiendo una monitorización continua del tráfico.

El sistema incorpora detección automática de incidentes, capaz de identificar en segundos vehículos detenidos, frenadas bruscas, peatones o circulación en sentido contrario. Cuando ocurre un evento, se envía una alerta al centro de control para activar protocolos como cierre de carriles, mensajes en paneles o avisos a emergencias.

Además, las cámaras ANPR permiten gestionar los accesos a zonas restringidas y monitorizar la velocidad media en determinados tramos, mientras que las cámaras térmicas garantizan la detección incluso en túneles o con en situaciones de climatología adversa.

5.1.4. Señalización dinámica

La señalización dinámica permite adaptar en tiempo real la información mostrada a los conductores mediante paneles de mensaje variable, señales electrónicas de velocidad, señalización LED en túneles o indicadores de ocupación en carriles especiales. Esta flexibilidad convierte a la infraestructura urbana en un sistema capaz de reaccionar de manera inmediata ante cambios en el tráfico, incidentes o condiciones ambientales.

❖ **Funcionalidades principales**

- Difusión de información contextual en tiempo real, como rutas alternativas, incidencias, obras, restricciones temporales o alertas meteorológicas.
- Regulación dinámica de la velocidad máxima, ajustando los límites según congestión, condiciones climáticas o incidentes detectados.
- Gestión adaptable de carriles, incluyendo carriles reversibles, carriles BUS-VAO o carriles de alta ocupación, mostrando ocupación o disponibilidad.
- Coordinación con sensores, cámaras y plataformas urbanas, permitiendo automatizar la activación de mensajes y restricciones en función del estado real del tráfico.

❖ **Caso de uso real**

La autopista A-8, que conecta Irún con Bilbao, dispone de un avanzado sistema de señalización dinámica diseñado para gestionar un corredor especialmente complejo debido a su elevada intensidad de tráfico, la presencia de túneles y viaductos y unas condiciones meteorológicas adversas frecuentes. En este

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

entorno, el Gobierno Vasco ha desplegado paneles de mensaje variable, señales de velocidad variable y sistemas de aviso automático que se actualizan en función del estado real de la vía.

La señalización dinámica de la A-8 se integra con estaciones meteorológicas, sensores de calzada y cámaras de tráfico, lo que permite ajustar de manera automática los límites de velocidad cuando se detecta lluvia intensa, niebla, pavimento deslizante o congestión. En paralelo, los paneles de mensaje variable informan en tiempo real sobre incidencias, retenciones, obras o desvíos recomendados, facilitando decisiones rápidas por parte de los conductores y reduciendo el riesgo de maniobras bruscas.

5.2. Sistemas de transporte y movilidad urbana

Los sistemas de transporte y movilidad urbana agrupan el conjunto de servicios, modos de transporte y soluciones operativas que permiten el desplazamiento de personas y mercancías dentro de la ciudad. Su evolución hacia tipologías conectadas, electrificadas y gestionadas digitalmente es clave para optimizar la eficiencia, reducir emisiones y mejorar la experiencia del usuario.

5.2.1. Transporte público

El transporte público constituye la columna vertebral de la movilidad urbana. La digitalización de autobuses, tranvías, metros y otros sistemas permite mejorar la eficiencia operativa, optimizar las rutas y ofrecer servicios más fiables y sostenibles.

❖ **Funcionalidades principales**

- Seguimiento en tiempo real de flotas y tiempos de llegada.
- Gestión dinámica de rutas, frecuencias y prioridades en intersecciones.
- Integración con sistemas de ticketing digital y pago inteligente.
- Control de eficiencia energética y estado de la flota, especialmente en buses eléctricos.

❖ **Caso de uso real**

Bilbao ha desplegado uno de los sistemas de gestión de flotas de autobuses más avanzados del país, integrando monitorización en tiempo real, analítica avanzada y priorización semafórica en corredores estratégicos. Todos los vehículos de Bilbobus están equipados con sensores de localización y telemetría que envían información continua al Centro de Control de Movilidad, donde se supervisa el cumplimiento de horarios, la ocupación aproximada y las incidencias operativas.

Gracias a esta digitalización, la ciudad ha optimizado las frecuencias en función de la demanda real, especialmente en horas punta, aumentando la regularidad de las líneas. Además, el sistema se integra con los paneles de información al viajero y con la aplicación móvil municipal, ofreciendo tiempos de llegada con alta precisión.

5.2.2. Movilidad compartida

La movilidad compartida incluye servicios como carsharing y motosharing, que permiten utilizar vehículos bajo demanda mediante plataformas digitales. Estos sistemas se apoyan en tecnologías de localización, comunicación y gestión inteligente para optimizar la disponibilidad, la operación y el mantenimiento de las flotas.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

❖ **Funcionalidades principales**

- Gestión inteligente de flotas bajo modelos free-floating o estacionados.
- Optimización del reparto de vehículos mediante algoritmos predictivos.
- Integración con plataformas MaaS y métodos de pago digitales.
- Monitorización del estado del vehículo, batería o mantenimiento.

❖ **Caso de uso real**

El servicio de carsharing Share Now en Madrid constituye uno de los despliegues más relevantes de movilidad compartida en España. Su flota, basada mayoritariamente en vehículos 100% eléctricos, incorpora sistemas telemáticos que reportan en tiempo real información sobre ubicación, disponibilidad, nivel de batería y estado técnico.

La plataforma utiliza modelos de predicción de demanda para anticipar las zonas y franjas horarias con mayor uso, coordinando la redistribución de vehículos y las operaciones de recarga mediante equipos móviles. Además, el servicio está plenamente integrado con el ecosistema digital de la ciudad, lo que permite alinearse con la ordenanza de movilidad, las zonas de bajas emisiones y la regulación local de estacionamiento.

5.2.3. Micromovilidad

La micromovilidad comprende vehículos ligeros y de baja velocidad como bicicletas eléctricas, patinetes eléctricos o ciclomotores ligeros. Se caracteriza por su flexibilidad, bajo coste y facilidad para cubrir distancias cortas.

❖ **Funcionalidades principales**

- Geolocalización en tiempo real y limitación dinámica de velocidad.
- Geofencing para control de zonas de circulación, aparcamiento y áreas restringidas.
- Gestión remota del estado del vehículo (batería, diagnósticos y mantenimiento).
- Integración con plataformas de movilidad urbana.

❖ **Caso de uso real**

El servicio de bicicletas compartidas Bicing en Barcelona combina bicicletas mecánicas y eléctricas con una red extensa de estaciones inteligentes. Cada bicicleta está equipada con sensores de uso y localización que envían información en tiempo real a la plataforma de gestión central, permitiendo controlar su disponibilidad, estado técnico y patrones de demanda.

Las estaciones ofrecen datos instantáneos sobre el número de bicicletas libres y anclajes disponibles, información que se sincroniza con la aplicación móvil y con los paneles urbanos de movilidad. Gracias al análisis predictivo, el operador puede planificar la redistribución de bicicletas para evitar saturaciones o desabastecimientos en horas punta, mejorando la accesibilidad al servicio.

5.2.4. Logística urbana

La logística urbana comprende las actividades de transporte, distribución y entrega de mercancías dentro de la ciudad. La digitalización de flotas, rutas y puntos de entrega permite optimizar la cadena

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

logística en entornos urbanos, reduciendo impactos ambientales, minimizando la congestión y mejorando la fiabilidad del reparto.

❖ **Funcionalidades principales**

- Rutas optimizadas y asignación dinámica de entregas.
- Seguimiento en tiempo real de mercancías y vehículos.
- Gestión de microhubs urbanos y puntos de entrega inteligentes.
- Integración con vehículos eléctricos y de carga ligera.

❖ **Caso de uso real**

Barcelona ha impulsado un modelo pionero de logística urbana basado en microhubs y vehículos de última milla, especialmente desplegados en distritos densos como el Eixample. En este sistema, las empresas logísticas utilizan pequeños centros de consolidación situados en aparcamientos municipales o locales urbanos, donde se agrupan los paquetes destinados a zonas cercanas. Desde estos puntos, las entregas se realizan con bicicletas de carga eléctricas o vehículos ligeros cero emisiones.

El uso de plataformas digitales permite monitorizar en tiempo real el volumen de mercancías, la ocupación del microhub, el estado de las rutas y los tiempos de entrega. Los algoritmos de optimización analizan la demanda diaria y asignan las rutas más eficientes, reduciendo desplazamientos redundantes y evitando la entrada de furgonetas convencionales en áreas congestionadas.

5.2.5. Vehículos de servicios municipales

Incluye vehículos destinados a limpieza, recogida de residuos, mantenimiento urbano, seguridad municipal o emergencias. La digitalización de estas flotas mejora la eficiencia, seguridad y trazabilidad de las operaciones.

❖ **Funcionalidades principales**

- Monitorización en tiempo real de rutas, tareas y rendimiento.
- Optimización de recorridos y planificación de operaciones.
- Control del estado operativo del vehículo y mantenimiento predictivo.
- Integración con sensores de entorno (residuos, calidad del aire, aforo).

❖ **Caso de uso real**

La ciudad de Málaga ha implementado un sistema avanzado de gestión digital para su flota de vehículos de recogida de residuos, combinando sensores IoT, planificación inteligente y vehículos de bajas emisiones. Los camiones están equipados con sistemas telemáticos que registran en tiempo real su ubicación, consumo energético, incidencias y progreso de las rutas asignadas. Esto permite al centro de control municipal visualizar la operación de toda la flota y realizar ajustes inmediatos ante imprevistos.

Asimismo, los contenedores de residuos cuentan con sensores de llenado que envían datos de forma continua, permitiendo generar rutas de recogida optimizadas según la demanda real, evitando desplazamientos innecesarios y reduciendo costes operativos.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

5.3. Infraestructura de soporte

La infraestructura de soporte constituye el conjunto de elementos físicos y digitales que permiten el funcionamiento continuo de la movilidad inteligente. Incluye sistemas energéticos, redes de comunicaciones urbanas y equipamientos especializados que garantizan la recarga, conectividad, localización y gestión operativa de vehículos y servicios de movilidad. Su despliegue es esencial para sostener modelos de transporte electrificados, conectados y digitalizados.

5.3.1. Estaciones de carga eléctrica

Las estaciones de carga eléctrica son infraestructuras clave para la electrificación del transporte urbano. Pueden instalarse en la vía pública, aparcamientos municipales, garajes privados o centros logísticos, y deben integrarse con la red eléctrica y los sistemas de gestión energética de la ciudad.

❖ **Funcionalidades principales**

- Recarga normal, semirrápida, rápida o ultrarrápida según potencia instalada.
- Gestión inteligente de la carga (smart charging) ajustando potencia y horarios.
- Reserva de puntos, monitorización de estado y pago mediante aplicaciones digitales.
- Integración con la red eléctrica y gestión de picos de demanda.

❖ **Caso de uso real**

Barcelona ha desarrollado una de las redes públicas de recarga más amplias de España a través del servicio Barcelona Endolla, gestionado por BSM (Barcelona de Serveis Municipals). La red integra cientos de puntos de recarga distribuidos en la vía pública y en aparcamientos municipales, combinando cargadores semirrápidos para usuarios cotidianos y cargadores rápidos destinados a flotas profesionales y servicios urbanos.

Cada estación está conectada a una plataforma digital que permite a los usuarios localizar puntos disponibles, reservarlos, iniciar y finalizar la recarga y gestionar el pago desde una única aplicación. A nivel técnico, los puntos de carga forman parte del sistema energético municipal, que aplica estrategias de smart charging para equilibrar la demanda y reducir picos en horas de mayor consumo.

5.3.2. Redes V2X urbanas

Las redes V2X (Vehicle-to-Everything) permiten la comunicación entre vehículos y elementos urbanos conectados, como semáforos, señales, centros de control o infraestructuras de carretera. Estas redes son la base de una movilidad cooperativa donde los vehículos reciben información contextual en tiempo real.

❖ **Funcionalidades principales**

- Comunicación V2I (Vehicle-to-Infrastructure) para avisos de señales, semáforos o incidencias.
- Comunicación V2V (Vehicle-to-Vehicle) para alertas de colisión, frenado o maniobras.
- Comunicación V2P (Vehicle-to-Pedestrian) para señales de presencia o riesgo inminente.
- Comunicación V2N (Vehicle-to-Network) para servicios y datos en tiempo real.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

- Avisos cooperativos de seguridad (C-ITS).
- Gestión de prioridades para transporte público o servicios de emergencia.

❖ **Caso de uso real**

La ciudad de Vigo ha desarrollado uno de los proyectos más avanzados de comunicaciones cooperativas V2X en España dentro del marco del programa de movilidad inteligente de la DGT. El piloto incluye la instalación de unidades de carretera (RSU) en intersecciones estratégicas y tramos urbanos, capaces de emitir mensajes C-ITS a vehículos equipados con unidades embarcadas (OBU).

Los vehículos participantes reciben avisos en tiempo real sobre el estado de los semáforos, límites de velocidad dinámicos, presencia de obras, congestiones o incidentes detectados por los sensores municipales. Asimismo, el sistema permite la priorización automática de vehículos de transporte público, mejorando sus tiempos de recorrido sin afectar negativamente a la movilidad general.

5.3.3. Smart parking

Los sistemas de smart parking permiten detectar, monitorizar y gestionar en tiempo real la disponibilidad de plazas de aparcamiento, tanto en superficie como en aparcamientos subterráneos. Reducen la congestión y el tiempo de búsqueda de estacionamiento.

Funcionalidades principales

- Detección de ocupación en plazas mediante sensores.
- Guiado dinámico al usuario hacia plazas libres.
- Predicción de disponibilidad a partir de modelos de datos.
- Integración con sistemas de pago, reservas y movilidad urbana.

❖ **Caso de uso real**

La ciudad de Santander ha implementado uno de los sistemas de smart parking más reconocidos a nivel nacional, como parte del proyecto europeo SmartSantander. La red está compuesta por miles de sensores instalados en plazas de aparcamiento, capaces de detectar la presencia o ausencia de vehículos en tiempo real. Estos datos se transmiten a la plataforma municipal, donde son procesados y distribuidos a aplicaciones de movilidad y paneles informativos.

Los usuarios pueden consultar desde su móvil la disponibilidad de plazas en distintas zonas de la ciudad, recibir indicaciones de guiado y acceder a información contextual como horarios, tarifas o restricciones. El sistema, además, integra modelos predictivos que estiman la disponibilidad en función de patrones temporales, eventos urbanos y condiciones del tráfico.

5.3.4. Smart grid asociada a la movilidad

La smart grid es la red eléctrica inteligente que soporta el sistema energético urbano, integrando puntos de carga, generación renovable, almacenamiento y gestión dinámica de la demanda. Es decisiva para absorber el impacto del vehículo eléctrico y equilibrar la red.

❖ **Funcionalidades principales**

- Gestión dinámica y flexible de la demanda eléctrica (DRM).

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

- Integración de energías renovables y almacenamiento local.
- Comunicación bidireccional entre usuarios, operadores y red.

❖ **Caso de uso real**

La ciudad de Málaga es uno de los referentes españoles en la implantación de redes inteligentes vinculadas a la movilidad, gracias al proyecto ALDIA y a iniciativas previas dentro del Living Lab Málaga Smart City. En este despliegue se integraron puntos de recarga, generación fotovoltaica, almacenamiento energético con baterías y un sistema avanzado de gestión que coordina la demanda en tiempo real.

Los puntos de recarga permiten la modulación dinámica de potencia, ajustando la energía suministrada a cada vehículo en función del estado de la red, la disponibilidad renovable y las necesidades globales del sistema urbano. Además, se han realizado pruebas piloto de tecnologías V2G, donde los vehículos eléctricos pueden devolver energía a la red en momentos de alta demanda, contribuyendo a la estabilidad del sistema.

5.4. Plataformas de gestión y análisis

Las plataformas de gestión y análisis constituyen el núcleo digital del ecosistema de movilidad inteligente en ciudades conectadas. Permiten recopilar, procesar, almacenar y analizar datos provenientes de vehículos, infraestructura urbana, sensores IoT, sistemas de transporte y redes energéticas, habilitando la toma de decisiones en tiempo real, la planificación estratégica y la optimización de los recursos de movilidad.

5.4.1. Plataformas municipales de movilidad

Son sistemas centralizados que integran información de todos los modos de transporte urbano y elementos de la infraestructura conectada, proporcionando visibilidad completa del tráfico, transporte público y recursos compartidos.

❖ **Funcionalidades principales**

- Monitorización en tiempo real del tráfico y de la ocupación de transporte público.
- Gestión de incidencias, planificación de rutas y optimización de semaforización.
- Integración de datos de micromovilidad, vehículos eléctricos y flotas públicas.
- Predicción de demanda mediante análisis de patrones históricos.

❖ **Caso de uso real**

La ciudad de Valencia cuenta con una plataforma de movilidad urbana operada desde el Centro Integral de Gestión de Movilidad (CIMU). Este sistema integra información procedente de sensores de tráfico, cámaras, autobuses, carriles bici, aparcamientos públicos y sistemas de micromovilidad. La plataforma consolida todos estos datos para ofrecer una visión completa del estado de la movilidad urbana en tiempo real.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

5.4.2. Sistemas de gestión de flotas

Estas plataformas gestionan flotas de vehículos públicos, privados o compartidos, optimizando su operativa, mantenimiento, consumo energético y rutas.

❖ **Funcionalidades principales**

- Localización en tiempo real y seguimiento de vehículos.
- Gestión de rutas y asignación dinámica de recursos.
- Monitorización de estado técnico y eficiencia energética.
- Alertas de seguridad y eventos críticos.

❖ **Caso de uso real**

El Ayuntamiento de Madrid ha implementado un sistema avanzado de gestión de flotas para coordinar vehículos municipales destinados a limpieza, mantenimiento urbano, inspecciones, servicios técnicos y transporte interno. La plataforma integra datos de geolocalización en tiempo real, consumo energético y el estado técnico de cada vehículo.

Gracias a este sistema, el consistorio puede optimizar rutas en función del tráfico, reasignar vehículos ante incidencias y recibir alertas automáticas sobre fallos o mantenimiento predictivo.

5.4.3. Plataformas de datos urbanos

Son sistemas de recopilación y análisis de datos de múltiples fuentes urbanas, incluyendo tráfico, movilidad, climatología, energía y seguridad, proporcionando información estructurada para la toma de decisiones.

❖ **Funcionalidades principales**

- Integración y normalización de datos heterogéneos.
- Análisis predictivo y modelado de escenarios urbanos.
- Generación de informes y alertas para operadores y ciudadanos.
- Soporte a investigación y planificación de políticas públicas.

❖ **Caso de uso real**

Barcelona ha sido pionera en el desarrollo de plataformas de datos urbanos mediante el uso combinado de Sentilo, un sistema abierto de sensores, y CityOS, la plataforma integrada de datos municipales. Esta infraestructura recoge información de miles de sensores distribuidos por la ciudad, como tráfico, ocupación de aparcamientos, contaminación atmosférica, ruido, consumo energético, calidad del agua o estado del alumbrado público.

CityOS normaliza y procesa estos datos, permitiendo a los operadores municipales anticipar patrones de movilidad, detectar incidencias y generar escenarios predictivos para la gestión urbana.

5.4.4. Centros de control de movilidad

Los centros de control de movilidad actúan como hub operativo, coordinando todos los elementos del ecosistema de transporte urbano y supervisando la infraestructura conectada y las flotas de vehículos.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

❖ **Funcionalidades principales**

- Monitorización en tiempo real de vehículos, tráfico y eventos urbanos.
- Coordinación de semáforos, señalización dinámica y rutas de transporte público.
- Gestión de incidentes, emergencias y desvíos de tráfico.

❖ **Caso de uso real**

El Centro de Control de Movilidad de Málaga supervisa la red viaria mediante cámaras, sensores de aforo, paneles de mensaje variable y sistemas de detección de incidencias que permiten conocer el estado del tráfico en tiempo real.

El centro gestiona más de 400 intersecciones semaforizadas que pueden adaptarse dinámicamente a los flujos de tráfico, facilitando la priorización del transporte público o ajustando los ciclos durante eventos especiales, obras o episodios de congestión. La señalización dinámica, los sistemas de información a viajeros y los corredores preferentes para autobuses se coordinan desde la misma plataforma tecnológica.

6. Vehículos inteligentes

Los vehículos inteligentes constituyen uno de los elementos centrales de la movilidad conectada, al integrar capacidades avanzadas de sensorización, conectividad y procesamiento de datos que permiten su interacción con infraestructuras, otros vehículos, servicios urbanos y plataformas de movilidad. Estas capacidades pueden incorporarse en vehículos eléctricos, híbridos o de combustión, el carácter "inteligente" no depende del sistema de propulsión, sino del grado de conexión y de digitalización del vehículo.

En este contexto, se considera vehículo inteligente a cualquier vehículo conectado que disponga de sensores IoT, módulos de comunicación, sistemas de telemetría y plataformas software que habilitan servicios como monitorización remota, actualizaciones OTA, intercambio de datos en tiempo real o comunicación con infraestructuras inteligentes (V2X).

6.1. Vehículos autónomos

Los vehículos autónomos son vehículos inteligentes que incorporan sistemas avanzados de percepción (LIDAR, cámaras, radar, ultrasonidos), redes de sensores, mapas HD e inteligencia artificial para interpretar el entorno y realizar maniobras sin intervención humana.

Su grado de automatización se clasifica según los niveles SAE (0 a 5), que definen de forma estandarizada la progresión desde la asistencia básica hasta la autonomía total.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

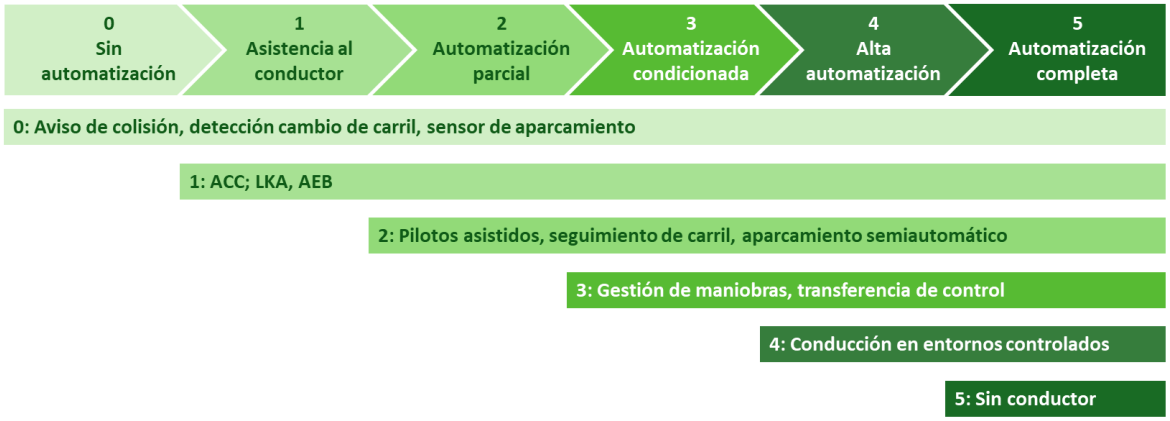

ILUSTRACIÓN 1: NIVELES DE AUTOMATIZACIÓN SAE

❖ Nivel 0: Sin automatización

En el nivel 0 el vehículo no ejecuta ninguna maniobra de conducción por sí mismo, toda la responsabilidad recae en el conductor. El sistema puede ofrecer avisos auditivos o visuales, pero no actúa sobre la dirección, la aceleración o el frenado. Es un nivel centrado en funciones pasivas de asistencia que no influyen en la dinámica del vehículo.

Casos de uso habituales:

- Aviso de colisión frontal o trasera.
- Detección de cambio de carril sin asistencia de dirección.
- Sensores de aparcamiento o alertas de ángulo muerto.

❖ Nivel 1: Asistencia al conductor

En este nivel, el vehículo incorpora sistemas que pueden automatizar una sola función de conducción, ya sea la dirección o el control sobre la aceleración y el frenado. Aunque la asistencia es activa, el conductor debe mantener el control total del vehículo, teniendo en todo momento las manos en el volante y prestando atención constante al entorno.

Casos de uso habituales:

- Control de crucero adaptativo (ACC).
- Asistente de mantenimiento de carril (LKA).
- Frenado automático de emergencia (AEB).

❖ Nivel 2: Automatización parcial

El nivel 2 permite al vehículo controlar simultáneamente la dirección y la aceleración/frenado, logrando una conducción parcialmente automatizada. Sin embargo, el conductor debe supervisar permanentemente el sistema y estar preparado para intervenir en cualquier momento, ya que el coche no tiene una comprensión completa del entorno, solo ejecuta tareas concretas basadas en sensores.

Casos de uso habituales:

- Pilotos asistidos en autopista.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

- Seguimiento automático del carril con control de distancia.
- Sistemas de aparcamiento semiautomático.

❖ **Nivel 3: Automatización condicionada**

En este nivel el vehículo puede gestionar todas las funciones de conducción bajo ciertas condiciones operativas definidas, como tráfico denso o autopistas. El sistema monitoriza activamente el entorno mediante sensores y algoritmos de IA, permitiendo al conductor desatender la conducción. No obstante, puede emitir una solicitud de toma de control cuando detecte una situación fuera del alcance de sus capacidades.

Casos de uso habituales:

- Conducción automatizada en tráfico lento.
- Gestión autónoma de maniobras dentro de escenarios controlados.
- Transferencia dinámica de control entre sistema y conductor.

❖ **Nivel 4: Alta automatización**

Los vehículos de nivel 4 pueden operar sin intervención humana en zonas o condiciones concretas, gracias a capacidades avanzadas de percepción, toma de decisiones y redundancia de sistemas críticos. El conductor puede no ser necesario dentro de estas áreas, como servicios de taxis inteligentes en zonas delimitadas. En caso de fallo, el vehículo es capaz de adoptar un estado seguro por sí mismo.

Casos de uso habituales:

- Servicios de taxi inteligente en zonas urbanas delimitadas.
- Conducción autónoma en campus corporativos, puertos o polígonos industriales.
- Operaciones sin conductor dentro de entornos de alta estructura y control.

❖ **Nivel 5: Automatización completa**

El nivel 5 representa la autonomía total. El vehículo puede operar en cualquier carretera, condición meteorológica y contexto urbano, sin necesidad de conductor humano. No requiere volante ni pedales, y puede tomar decisiones equivalentes a un conductor experto, por lo que la interacción humana en el control desaparece por completo.

Casos de uso habituales:

- Vehículos sin conductor capaces de circular en cualquier entorno urbano o interurbano.
- Sistemas de movilidad totalmente autónoma sin cabina de conducción.

6.1.1. Marco regulatorio en España

En el contexto regulatorio español, la circulación de vehículos autónomos se encuentra actualmente limitada a los niveles SAE 0, 1 y 2, es decir, sistemas de asistencia o automatización parcial en los que el conductor debe mantener en todo momento la supervisión activa y la responsabilidad plena sobre la conducción. Aunque la tecnología de automatización avanzada ya está disponible en el mercado

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

internacional, los niveles SAE 3, 4 y 5 no están todavía autorizados para circular de forma generalizada en vías públicas.

Para permitir el progreso tecnológico, en junio de 2025, la Dirección General de Tráfico (DGT) ha establecido un marco regulador específico para pruebas y ensayos, conocido como Programa Marco de Evaluación de la Seguridad y Tecnología de Vehículos Automatizados (Programa ES-AV). Este programa habilita la realización de pilotos con vehículos equipados con automatización avanzada en entornos reales, siempre bajo condiciones estrictas de seguridad, supervisión humana y autorización previa. Estas pruebas están coordinadas a través de la Oficina para la Facilitación de Pruebas de Vehículos Automatizados (OFVA), organismo encargado de evaluar las solicitudes, analizar los riesgos operativos y monitorizar el despliegue de tecnologías de conducción automatizada.

Paralelamente, España avanza en la elaboración de un Real Decreto destinado a regular la circulación de vehículos con niveles de autonomía superiores (SAE 3, 4 y 5). Este futuro marco normativo establecerá los requisitos técnicos, de responsabilidad, ciberseguridad, conectividad y gestión de datos para permitir la introducción progresiva de vehículos altamente automatizados y autónomos en el tráfico urbano e interurbano. El objetivo de esta regulación es habilitar un despliegue seguro y controlado, alineado con la normativa europea y con las directrices internacionales sobre automatización de la movilidad.

Según lo mencionado, España se sitúa en un proceso de transición regulatoria:

- Circulación permitida actualmente: niveles SAE 0–2.
- Circulación limitada bajo autorización especial: niveles SAE 3–4 en pruebas controladas.
- Regulación en desarrollo: apertura normativa para vehículos autónomos de nivel 4 y nivel 5.

6.2. Arquitectura interna

La hiperconectividad constituye un elemento clave en la arquitectura tecnológica de los vehículos inteligentes, proporcionando una base sólida para su funcionamiento integral y eficiente. Esta interconexión no se limita a la comunicación entre componentes internos del vehículo, sino que se extiende hacia una red más amplia, que incluye la interacción con infraestructuras externas, otros vehículos y plataformas de gestión urbana mediante tecnologías IoT y OT.

En este contexto, la arquitectura de los vehículos inteligentes se puede dividir en dos grandes tipos de conectividad, estrechamente interrelacionadas.

6.2.1. Conectividad interna

La conectividad interna está compuesta por una red de dispositivos de campo como son los sensores, actuadores y sistemas de control que colaboran de manera sincronizada para optimizar la eficiencia operativa, mejorar la seguridad y proporcionar una experiencia de conducción mejorada. Esta interconexión permite la recopilación, procesamiento e intercambio de datos en tiempo real, facilitando la toma de decisiones instantánea sobre aspectos críticos como la gestión de energía, la seguridad del vehículo, la respuesta ante situaciones de tráfico, la monitorización del entorno, entre otros.

Algunos de los sensores y dispositivos de conectividad interna son los siguientes:

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

- Sensores LIDAR y cámaras: permiten la percepción avanzada del entorno, generando mapas tridimensionales y detectando obstáculos, peatones, vehículos y objetos en movimiento. Se utilizan en sistemas de asistencia a la conducción (ADAS) para la planificación de rutas, prevención de colisiones y control adaptativo de velocidad.
- Sensores de proximidad y radar: miden distancias con alta precisión mediante ondas electromagnéticas. Se emplean en sistemas de frenado automático, control de carril, mantenimiento de distancia con otros vehículos y detección de obstáculos en entornos con baja visibilidad
- Sensores de telemetría: recogen información interna sobre el vehículo, como el estado del motor, batería, temperatura, presión, climatización, desgaste de componentes y consumo energético. Esta información permite optimizar la eficiencia operativa, detectar fallos y planificar mantenimientos preventivos.
- Sensores GPS y GNSS: proporcionan geoposicionamiento y seguimiento de rutas en tiempo real. Son esenciales para la navegación, planificación de rutas, geocercas, seguimiento de flotas y servicios basados en la ubicación.
- Sensores de comunicaciones DSRC / C-V2X: habilitan la interacción del vehículo con otros vehículos, la infraestructura y la red, transmitiendo datos críticos sobre tráfico, semáforos, señalización y riesgos en carretera, aumentando la seguridad y la eficiencia de la movilidad urbana.
- Cajas negras o Event Data Recorder (EDR): registran datos relevantes de conducción y eventos críticos, incluyendo velocidad, frenado, ángulo de dirección, uso de sistemas de seguridad y posibles colisiones. Son útiles para análisis de accidentes, seguros y estudios de seguridad vial.
- Actuadores y sistemas de control: controlan de manera precisa frenos, dirección, aceleración, suspensión, la gestión de carga y el consumo de batería. Permiten ejecutar decisiones automáticas derivadas de sensores y sistemas ADAS.
- Sistemas de infoentretenimiento: plataformas integradas que ofrecen navegación, conectividad a internet, comunicación con dispositivos móviles, reproducción multimedia y servicios basados en la nube. También permiten la integración con aplicaciones de movilidad urbana y asistentes inteligentes para mejorar la experiencia de conducción y la seguridad.

6.2.2. Conectividad externa

La conectividad externa permite que los vehículos inteligentes se comuniquen de manera bidireccional con sistemas fuera de su perímetro físico, integrándose en un ecosistema de movilidad urbano amplio, que incluye infraestructuras, otros vehículos, estaciones de carga, redes de gestión de tráfico y servicios en la nube. Esta conectividad es clave para habilitar funcionalidades avanzadas, mejorar la seguridad vial, optimizar la eficiencia operativa y garantizar la interoperabilidad entre distintos tipos de vehículos.

Los principales componentes de la conectividad externa son:

- V2X (Vehicle-to-Everything): permite la interacción con vehículos (V2V), peatones (V2P), infraestructura (V2I) y redes (V2N), transmitiendo información sobre tráfico, obstáculos,

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

semáforos, señalización y condiciones de la carretera. Esta comunicación aumenta la seguridad activa y permite coordinación entre vehículos autónomos y sistemas de transporte urbano.

- Redes móviles (4G/5G/6G): facilitan la comunicación en tiempo real con servicios en la nube, actualizaciones de software remotas (OTA) y transmisión de datos críticos para telemetría, geolocalización y diagnóstico remoto.
- Estaciones de carga inteligente: los vehículos eléctricos o híbridos pueden gestionar la carga de la batería de manera eficiente mediante comunicación con estaciones de carga conectadas a la red, permitiendo programación, priorización de carga y pago automatizado.
- Plataformas de gestión de flotas y movilidad urbana: integran datos de múltiples vehículos para optimizar rutas, supervisar el estado de la flota y mejorar la eficiencia del transporte público y privado.
- Servicios en la nube y análisis de datos: permiten almacenar y procesar grandes volúmenes de datos para análisis predictivo, mantenimiento proactivo, mejora de algoritmos de conducción autónoma y servicios personalizados para los usuarios.
- Integración con la infraestructura urbana: el vehículo puede interactuar con semáforos inteligentes, cámaras de tráfico, señalización dinámica y sensores urbanos, mejorando la fluidez del tránsito y reduciendo riesgos de accidentes.
- Ciberseguridad y gestión de identidad: la conectividad externa incorpora protocolos de autenticación, cifrado de datos y sistemas de detección de intrusiones para proteger la información y la integridad del vehículo frente a amenazas externas.

6.2.3. Arquitectura OT

La tecnología OT (Operational Technology) se refiere a sistemas y dispositivos especializados diseñados para gestionar, supervisar y controlar procesos físicos y operativos dentro del vehículo, optimizando la eficiencia, la seguridad y la operatividad. En el contexto de vehículos inteligentes, la arquitectura OT se combina con sensores y actuadores IoT y con la conectividad externa, creando un ecosistema interconectado capaz de recopilar, procesar y reaccionar ante datos en tiempo real.

La arquitectura OT se basa en principios de SCADA (Supervisory Control and Data Acquisition) adaptados a la movilidad inteligente, permitiendo la supervisión centralizada y la actuación automática sobre los sistemas críticos del vehículo.

Los componentes principales de la arquitectura OT son:

- Sensores IoT: dispositivos que actúan como inputs, recopilando información física y operativa del vehículo. Ejemplos incluyen LIDAR, cámaras, radares, sensores de proximidad, telemetría del motor y batería, sensores GPS/GNSS y cajas negras (EDR). Los datos recopilados permiten supervisar y controlar de manera continua el estado del vehículo y su entorno.
- Unidades de Terminal Remota (RTU): módulos intermedios que procesan los datos de los sensores y los transmiten al sistema central de supervisión. Pueden realizar un procesamiento local para filtrar, agregar o validar información antes de enviarla, reduciendo la latencia y mejorando la eficiencia operativa. Por ejemplo, una RTU puede consolidar datos del LIDAR,

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

cámaras y sensores de frenado para generar un evento único de “obstáculo cercano” antes de enviarlo al sistema de control central.

- Elementos de telecomunicación: facilitan la transmisión de datos entre los sensores, RTU y el sistema central. Incluyen comunicaciones cableadas, inalámbricas y protocolos automotrices como Bus CAN, así como enlaces con la conectividad externa para V2X, OTA y servicios en la nube.
- Sistema de control central y terminal de operador: permite supervisar el estado del vehículo, ajustar parámetros críticos (frenado, aceleración, dirección, gestión de batería) y monitorizar alertas generadas por los sensores. Este sistema central funciona como el “cerebro” de la arquitectura OT, integrando información interna y externa.
- Ajuste automático de sistemas de control: mediante algoritmos de control y lógica de seguridad, la arquitectura OT puede actuar de forma autónoma sobre frenos, dirección, aceleración, suspensión o carga de batería, basándose en los datos de telemetría, sensores y comunicaciones V2X.
- Monitorización de alarmas y eventos críticos: el sistema detecta condiciones anómalas o de riesgo (colisiones, fallos de batería, intrusión en el vehículo) y genera alertas, registrando información en cajas negras y, si es necesario, notificando a sistemas externos de gestión de flotas o autoridades de tráfico.

6.2.3.1. Bus CAN

Dentro de la arquitectura OT de los vehículos inteligentes, el Bus CAN (Controller Area Network) es un bus de comunicaciones en serie diseñado para que las distintas unidades electrónicas intercambien mensajes de forma rápida y fiable sin necesidad de una consola central. Por ello, se trata de uno de los componentes fundamentales del vehículo, ya que actúa como columna vertebral de la comunicación interna entre módulos y sistemas críticos. Asimismo, desde 2005, el Bus CAN se ha consolidado como estándar en la industria automotriz, garantizando eficiencia, robustez y seguridad en la transmisión de datos.

Las funciones principales del Bus CAN son:

- Comunicación distribuida: todos los dispositivos y módulos del vehículo (sensores, actuadores, sistemas de infoentretenimiento, unidades de control de motor y batería) se conectan mediante un cable de comunicación común, lo que simplifica el cableado, reduce el peso y disminuye la complejidad del sistema eléctrico.
- Prioridad de mensajes: el Bus CAN permite transmitir mensajes con diferentes niveles de prioridad. Los mensajes críticos, relacionados con la seguridad y la operación del vehículo (como frenos, control de estabilidad o alertas de colisión), se transmiten con prioridad sobre los mensajes menos críticos, asegurando que las decisiones vitales se ejecuten de forma inmediata.
- Integridad y fiabilidad de los datos: incorpora mecanismos de detección y corrección de errores, basados en CRC (Cyclic Redundancy Check), garantizando que los datos transmitidos se reciban correctamente. Además, la red puede tolerar fallos en nodos individuales sin afectar la comunicación del resto de los sistemas, aumentando la robustez y disponibilidad del vehículo.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

- Compatibilidad y escalabilidad: el Bus CAN permite integrar nuevos módulos y sistemas de manera sencilla, facilitando la evolución tecnológica de los vehículos inteligentes, desde funciones ADAS hasta sistemas de conducción autónoma.

6.2.4. Inteligencia artificial y machine learning

Dentro de la arquitectura interna de los vehículos inteligentes, la Inteligencia Artificial (IA) y el Aprendizaje Automático actúan como una capa transversal de optimización sobre los sistemas IoT y OT. Analizando los grandes volúmenes de datos generados por sensores, actuadores, telemetría y conectividad interna/externa, estas tecnologías permiten:

- Detectar patrones anómalos en el comportamiento del vehículo o en el entorno, mejorando la seguridad activa y la anticipación ante posibles incidentes.
- Optimizar la eficiencia energética y la gestión de la batería, ajustando en tiempo real la operación de motores, climatización y sistemas de propulsión.
- Mejorar los sistemas de asistencia avanzada y conducción autónoma (ADAS) mediante predicciones basadas en datos históricos y en tiempo real.
- Automatizar la respuesta ante ciberamenazas, identificando intentos de intrusión o manipulación de la red interna (Bus CAN) y la conectividad externa (V2X, OTA).

6.3. Interacción con el ecosistema urbano

Los vehículos inteligentes forman parte de un ecosistema urbano conectado, donde la interacción con infraestructuras, otros vehículos y plataformas digitales permite mejorar la seguridad, eficiencia y sostenibilidad del transporte. Esta cooperación se realiza a través de tecnologías V2X, que generan un flujo constante de información y control en tiempo real, facilitando la coordinación entre los distintos actores de la movilidad urbana y la respuesta ante cambios en el tráfico.

6.3.1. V2X

La comunicación V2X permite a los vehículos conectados interactuar con distintos elementos del entorno urbano:

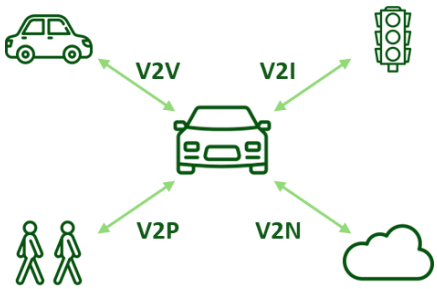

ILUSTRACIÓN 2: COMUNICACIÓN V2X

- V2V (Vehicle-to-Vehicle): intercambio de información sobre velocidad, aceleración, frenado y posición de cada vehículo. Esto permite a los vehículos anticiparse a maniobras de otros, coordinar frenadas y aceleraciones, evitar colisiones, organizarse en grupos autónomos y reducir congestiones mediante decisiones cooperativas en tiempo real.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

- V2I (Vehicle-to-Infrastructure): comunicación con semáforos inteligentes, señales dinámicas, sensores y cámaras de tráfico. Los vehículos reciben datos sobre tiempos de semáforo, incidencias, densidad de tráfico y cambios en la señalización, lo que posibilita optimizar rutas, adaptar la velocidad a las condiciones actuales y priorizar el paso de vehículos de emergencia, minimizando riesgos y retrasos.
- V2P (Vehicle-to-Pedestrian): intercambio de información con dispositivos móviles o wearables de peatones y ciclistas para detectar presencia, distancia, trayectoria y velocidad. Esta comunicación permite alertar al conductor o al sistema de asistencia del vehículo ante situaciones de riesgo, mejorando la seguridad vial en cruces, pasos de peatones y zonas con alta densidad de personas.
- V2N (Vehicle-to-Network): interacción con la nube y sistemas de gestión de tráfico. A través de esta comunicación, los vehículos pueden recibir actualizaciones OTA de software, información sobre incidentes en la red vial, planificación de rutas optimizadas y servicios de análisis de datos en tiempo real, contribuyendo a decisiones más eficientes y a la coordinación de flotas y plataformas de movilidad urbana.

7. Amenazas en la movilidad inteligente

La creciente adopción de arquitecturas IoT en vehículos inteligentes, combinada con la hiperconectividad propia de los entornos urbanos inteligentes, ha ampliado significativamente la superficie de exposición a ciberamenazas. Este contexto hace imprescindible adoptar un enfoque de protección integral, identificando y clasificando los vectores de ataque potenciales para garantizar la seguridad operativa y la protección de los usuarios.

7.1. Contexto en materia de ciberseguridad

Tradicionalmente, la seguridad de los vehículos se centraba en prevenir accesos físicos no autorizados que pudieran comprometer la integridad del sistema o permitir la sustracción del vehículo. Sin embargo, la transformación digital de los vehículos y la integración con la infraestructura urbana han generado nuevos riesgos que van mucho más allá del acceso físico, incluyendo amenazas complejas y persistentes, a nivel digital.

En la actualidad, la ciberseguridad en la movilidad inteligente se caracteriza por un enfoque proactivo, orientado a mitigar riesgos emergentes, como las APT (del inglés, Advanced Persistent Threats), las cuales se definen como ataques sofisticados y prolongados cuyo objetivo puede ser el robo de información sensible, la manipulación de sistemas o el espionaje de infraestructuras críticas.

A nivel internacional y nacional, organismos especializados como NIST, ENISA, CCN-CERT o el UIT-T han desarrollado directrices específicas para proteger estos entornos, promoviendo la incorporación de medidas de ciberseguridad desde las fases iniciales de diseño y desarrollo hasta el ciclo de vida completo de los productos. Estas directrices fomentan prácticas de gestión de riesgos, auditoría continua, monitorización de amenazas y respuesta ante incidentes.

En este contexto, el reglamento UNECE/R155 adquiere un papel clave en el ámbito específico de la movilidad inteligente. Esta normativa introduce un marco estructurado de catalogación de amenazas y

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

requisitos mínimos de ciberseguridad para fabricantes y operadores de vehículos conectados, garantizando un enfoque homogéneo en la identificación, valoración y mitigación de riesgos. El detalle de dicho marco se recoge en el Anexo I, donde se desglosan las tipologías de amenazas contempladas y se describen los potenciales vectores de ataque asociados.

Además, la evolución tecnológica ha permitido incorporar soluciones avanzadas de ciberseguridad, capaces de detectar patrones anómalos y generar respuestas automáticas frente a ataques. Entre estas tecnologías destacan los sistemas de inteligencia artificial (IA), que analizan grandes volúmenes de datos, aprenden a identificar comportamientos anómalos y ajustan dinámicamente las medidas de protección para adaptarse a amenazas en constante evolución, aumentando la resiliencia de los vehículos y del ecosistema urbano conectado.

7.2. Principales ciberataques

El ecosistema de movilidad inteligente presenta una superficie de exposición amplia y diversa debido a la integración de vehículos conectados, micromovilidad, estaciones de carga, semáforos inteligentes, sensores urbanos y plataformas de gestión de datos. Los actores de amenazas aprovechan esta complejidad para ejecutar ataques que combinan intrusión física, explotación de vulnerabilidades lógicas, manipulación de señales y acceso remoto a sistemas críticos.

Las siguientes tipologías representan los principales vectores de ataque identificados en la actualidad.

7.2.1. Ataques de acceso físico

Los ataques de acceso físico continúan siendo relevantes en la movilidad inteligente, aunque su naturaleza ha evolucionado con la digitalización de los vehículos y la infraestructura. Mientras que históricamente se limitaban a forzar cerraduras, romper ventanillas o acceder al interior del vehículo, hoy los delincuentes emplean técnicas electrónicas y híbridas que permiten el acceso sin contacto físico directo.

Además de los vehículos, ciertos elementos de la infraestructura urbana son susceptibles a ataques físicos, como estaciones de carga, dispositivos de smart parking, semáforos inteligentes o sensores de tráfico. La manipulación física de estos dispositivos puede provocar interrupciones de servicio, robo de datos y riesgos de seguridad para los usuarios.

Los métodos más frecuentes incluyen:

- Ataques a vehículos keyless: dispositivos que interceptan o amplifican señales de llaves electrónicas para desbloquear y arrancar automóviles sin contacto físico (relay attacks o MitM).
- Manipulación de estaciones de carga y smart parking: acceso directo a hardware o puertos de comunicación para alterar su funcionamiento, generar sobrecargas, robar energía o manipular datos de usuarios.
- Acceso a semáforos y sensores urbanos: apertura o desconexión de unidades físicas para alterar la programación, generar congestión o provocar accidentes.

A continuación, se describen algunos dispositivos comúnmente empleados en entornos de investigación o en incidentes reales, cuyo uso facilita la explotación de estas vulnerabilidades.

7.2.1.1. Hack KEY

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

Investigadores de ciberseguridad de Qihoo 360 demostraron en un entorno controlado un ataque basado en la amplificación de señales keyless utilizando dispositivos experimentales de bajo coste conocidos como Hack KEY. Estos prototipos permitían extender artificialmente el rango de comunicación entre el vehículo y la llave legítima, simulando que ambos se encontraban próximos.

El ataque se ejecutaba mediante dos unidades cooperando en modo MitM, una próxima a la llave del propietario y otra cerca del vehículo. El objetivo era retransmitir la señal original sin necesidad de descifrarla, permitiendo desbloquear y arrancar el vehículo. Estos experimentos evidencian la importancia de reforzar la seguridad de los sistemas de acceso inalámbrico mediante protección criptográfica y medidas anti-relay.

7.2.1.2. Dispositivos ocultos en carcasas comerciales

En los últimos años han aparecido dispositivos para el robo de vehículos que se camuflan dentro de carcasas de teléfonos móviles antiguos, especialmente modelos icónicos como el Nokia 3310. Aunque externamente parecen teléfonos convencionales, internamente integran electrónica diseñada para comunicarse ilegalmente con determinadas unidades de control del vehículo a través del puerto diagnóstico.

Estos dispositivos se venden en canales ilícitos y permiten automatizar el proceso de acceso lógico a la centralita, facilitando el arranque del vehículo sin manipulación mecánica visible. Su proliferación subraya la necesidad de reforzar las medidas de autenticación y limitar el acceso al puerto OBD en los vehículos modernos.

7.2.1.3. Flipper Zero

El Flipper Zero es una herramienta multifunción destinada originalmente a profesionales de ciberseguridad y análisis de hardware. Permite interactuar con tecnologías como RFID, NFC, infrarrojos o radiofrecuencia, y está diseñada para realizar pruebas en entornos controlados.

Sin embargo, su popularidad y facilidad de uso han provocado que algunos actores malintencionados intenten modificar el dispositivo añadiendo firmware no oficial o módulos externos capaces de ejecutar funciones no permitidas por el fabricante.

Aunque el dispositivo legítimo no puede vulnerar sistemas modernos que implementan protocolos de rolling code o criptografía robusta, la existencia de versiones alteradas demuestra la importancia de reforzar los mecanismos de autenticación y revisar los sistemas legacy presentes en flotas antiguas.

Concretamente, el módulo NFC del Flipper Zero se ha demostrado efectivo en la explotación de la vulnerabilidad CVE-2022-2754 en los vehículos de la marca Honda Civic del año 2018, permitiendo que la señal enviada por el mando pueda capturarse y retransmitirse, posibilitando así la apertura del vehículo bajo determinadas condiciones técnicas.

7.2.2. Ataques a los sistemas de comunicaciones inalámbricas

Los sistemas de comunicaciones inalámbricas constituyen uno de los vectores más críticos dentro del ecosistema de movilidad inteligente, abarcando vehículos conectados, estaciones de carga, sensores urbanos, semáforos inteligentes y plataformas de smart parking. Al utilizar el medio aéreo como canal de transmisión, presentan características intrínsecas que los hacen vulnerables, como la apertura del canal, la facilidad de interceptación y la variabilidad de la señal.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

Estas vulnerabilidades pueden ser explotadas por actores de amenazas para comprometer la confidencialidad, integridad y disponibilidad de los sistemas, afectando tanto a vehículos como a la infraestructura urbana conectada.

Entre las principales consecuencias derivadas de este tipo de ataques destacan:

- Exposición del canal inalámbrico: la información transmitida puede ser interceptada, alterada o bloqueada por usuarios no autorizados, afectando servicios como la navegación GPS, la gestión de flotas o la comunicación con estaciones de carga.
- Variabilidad del medio: zonas con baja cobertura, interferencias o pérdida de señal pueden impedir la recepción de actualizaciones críticas de software, dejando expuestos dispositivos y vehículos ante vulnerabilidades conocidas.

En términos operativos, los ataques más frecuentes incluyen:

- Ataques tipo Man-in-the-Middle (MitM): interceptación y manipulación de señales entre sistemas legítimos. Por ejemplo, un actor puede redirigir comunicaciones entre un vehículo y la infraestructura V2X para falsificar información de tráfico o controlar funciones del vehículo.
- Denegación de Servicio Distribuida (DDoS): saturación del canal de comunicación mediante un alto volumen de solicitudes, lo que provoca la pérdida de conectividad y afecta a sistemas dependientes como semáforos, estaciones de carga o plataformas de movilidad.
- Explotación de protocolos inalámbricos específicos: vulnerabilidades en Wi-Fi, Bluetooth o comunicaciones OTA que permiten acceso no autorizado, extracción de datos, manipulación de software o control de dispositivos conectados.

A continuación, se analizan los vectores de ataque más comunes asociados a las tecnologías inalámbricas más propensas a potenciales amenazas, detallando su funcionamiento, las vulnerabilidades típicas y el modo habitual de explotación por parte de actores de amenazas.

7.2.2.1. Bluetooth

La tecnología Bluetooth es un protocolo de comunicación inalámbrica ampliamente extendido en los vehículos conectados y los sistemas urbanos para multitud de servicios, por lo que se convierte en un objetivo recurrente para la explotación de vulnerabilidades. Entre los principales tipos de ciberataques asociados a este protocolo se encuentran:

- Sniffers: analizadores de paquetes capaces de interceptar, registrar y examinar los datos transmitidos entre dispositivos Bluetooth, permitiendo vulnerar la confidencialidad e integridad de la comunicación.
- Man-in-the-Middle (MitM): el atacante intercepta y manipula los paquetes transmitidos, posicionándose entre los dispositivos legítimos para alterar o suplantar la comunicación.
- Inyección de paquetes: introducción de código malicioso en la transmisión Bluetooth para alterar el comportamiento del sistema o provocar ejecución no autorizada de acciones.
- Spoofing: suplantación de identidad de un dispositivo legítimo mediante la duplicación de direcciones MAC, con el objetivo de engañar al vehículo o a los sistemas vinculados.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

- Denegación de servicio (DDoS): saturación de solicitudes de conexión que degrada o inhabilita la red Bluetooth, afectando a la funcionalidad de los servicios dependientes.
- Bluesnarfing: explotación de fallos en versiones vulnerables del protocolo para extraer información del dispositivo atacado sin autorización.
- Bluebugging: aprovechamiento de debilidades en los procesos de autenticación para ejecutar comandos AT, posibilitando que el atacante controle remotamente el dispositivo y acceda a información sensible como la intensidad de la señal recibida.

7.2.2.2. Conectividad Wi-Fi

La conectividad Wi-Fi permite la comunicación de vehículos, estaciones de carga, semáforos inteligentes y sensores urbanos con redes locales e Internet. Sin embargo, su uso también expone al sistema a diversos tipos de ciberataques, entre los que destacan:

- Fuerza bruta: intento sistemático de descifrar contraseñas o credenciales mediante combinaciones sucesivas de prueba y error, habitualmente apoyado en diccionarios generados a partir de información obtenida mediante ingeniería social u OSINT (Open Source Intelligence).
- Key Reinstallation Attack (KRACK): ataque MitM dirigido contra el protocolo de cifrado WPA2, que permite forzar la reinstalación de claves criptográficas, comprometiendo la confidencialidad e integridad de los datos transmitidos.
- Pixie Dust: ataque que explota vulnerabilidades del mecanismo WPS (Wi-Fi Protected Setup), empleado para facilitar la conexión rápida a redes Wi-Fi, su explotación permite obtener el PIN del WPS y, con ello, la contraseña de la red Wi-Fi asociada.

7.2.3. Ataques contra servicios digitales

Los servicios digitales en el ecosistema de movilidad inteligente, incluyendo vehículos conectados y el resto de los sistemas relacionados, constituyen uno de los vectores de ataque más relevantes. Estos sistemas combinan componentes IoT/OT y proporcionan funcionalidades críticas: comunicación, navegación, monitorización, gestión de usuarios, actualización de software y conexión con plataformas externas.

Dentro de estos servicios se incluyen los sistemas de infoentretenimiento integrados en los vehículos los los cuales concentran funciones críticas como navegación, comunicaciones, conectividad con el usuario, actualizaciones de software, integración con smartphones y acceso a servicios digitales externos.

Aunque no existen metodologías de seguridad diseñadas específicamente para los servicios digitales de movilidad inteligente, sí pueden aplicarse marcos consolidados que abordan la protección de entornos IoT. En este contexto, el estándar ISO/IEC 27030 proporciona directrices para la seguridad en dispositivos IoT, mientras que la guía NIST SP 800-82r3 adapta el Cybersecurity Framework del NIST a sistemas OT, proporcionando criterios para la protección, monitorización y respuesta en este tipo de arquitecturas.

A continuación, se detallan los principales vectores de ataque asociados a servicios digitales en todo el ecosistema de movilidad:

7.2.3.1. Marketplaces y plataformas de software

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

Los marketplaces y plataformas digitales permiten descargar, actualizar y gestionar aplicaciones destinadas a ampliar las capacidades de los vehículos conectados y sistemas relacionados, así como mejorar la experiencia del usuario. Sin embargo, al actuar como repositorios de software de terceros, introducen un conjunto significativo de riesgos de seguridad.

Las principales ciberamenazas:

- Malware en aplicaciones: incorporación de código malicioso en aplicaciones aparentemente legítimas, que puede comprometer los sistemas tecnológicos de los vehículos y sistemas, manipular procesos internos o abrir puertas traseras para ataques posteriores.
- Brechas de datos sensibles: extracción no autorizada de información almacenada en los distintos sistemas de movilidad inteligente, como historiales de uso, patrones de desplazamiento, credenciales de acceso, datos de usuarios, información de rutas, registros de operación o configuraciones de dispositivos. Estos datos, una vez extraídos, suelen comercializarse en blackmarkets de la Dark Web (como Genesis o 2Easy) y utilizarse para campañas de phishing altamente personalizadas.
- Explotación de vulnerabilidades en aplicaciones o configuraciones: aprovechamiento de errores de diseño, fallos de implementación o configuraciones inseguras en los sistemas, permitiendo desde la manipulación de parámetros internos hasta, en escenarios avanzados, la obtención de capacidades de comando y control sobre determinados componentes del vehículo y los sistemas.

7.2.3.2. Asistentes de voz

Los asistentes de voz y otras interfaces digitales permiten a los usuarios interactuar con vehículos, estaciones de carga, sistemas de parking o plataformas de movilidad mediante comandos verbales o gestuales. Estas interfaces suelen estar integradas en sistemas operativos comerciales como Android Auto, Apple CarPlay o entornos Linux, lo que introduce dependencias tecnológicas externas.

El ciberataque más común a los asistentes de voz es el siguiente:

- Falsificación de respuestas del asistente: mediante la explotación de vulnerabilidades en el sistema operativo o en el software de la plataforma, un actor de amenazas puede manipular la información proporcionada por el asistente. Esta manipulación puede inducir a errores operativos o de navegación, alterar la detección de obstáculos, generar instrucciones incorrectas o producir alertas falsas, comprometiendo la seguridad de los usuarios y del ecosistema de movilidad conectado.

7.2.3.3. Plataformas de gestión

Las plataformas de gestión que centralizan flotas de vehículos, servicios de movilidad compartida, smart parking o la coordinación de sistemas urbanos inteligentes también presentan riesgos de ciberseguridad relevantes. Entre ellos destacan:

- Ataques de inyección y escalada de privilegios: explotación de vulnerabilidades para alterar datos, modificar parámetros de operación o asumir privilegios elevados que comprometan la integridad de la plataforma.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

- Exfiltración de información operativa: obtención no autorizada de datos de rutas, horarios, usuarios, vehículos conectados o recursos urbanos, que puede facilitar fraudes, sabotajes, ataques dirigidos o la planificación de incidentes físicos.
- Denegaciones de servicio (DoS/DDoS): saturación de las plataformas mediante un alto volumen de solicitudes, provocando interrupciones en servicios críticos y afectando la operatividad de la movilidad urbana, la gestión de flotas y la coordinación de infraestructuras inteligentes.

7.3. Histórico de incidentes en el sector

Tras analizar la tipología de ciberataques a vehículos conectados y sistemas urbanos inteligentes, en el siguiente epígrafe se realiza un histórico de los principales ciberataques y vulnerabilidades que ha sufrido el sector durante los últimos años.

Vulnerabilidades en semáforos inteligentes Países Bajos	
Fecha	Octubre 2024
Víctima	Infraestructura de tráfico en Países Bajos (sistema KAR en semáforos inteligentes)
Activo comprometido	Miles de semáforos conectados que gestionan prioridad para vehículos de emergencia y transporte público
Tipo de Amenaza	Explotación de vulnerabilidad en sistema de radiocomunicación / Manipulación remota de señales de tráfico
Vector del ataque	Uso de radio definida por software (SDR) para replicar señales del sistema KAR Posibilidad de enviar comandos falsos a las cajas de control de semáforos Falta de cifrado y autenticación robusta en el protocolo de comunicación
Origen del ataque	Demostración por hacker ético
Impacto	• Cambio remoto de luces (rojo/verde) en miles de intersecciones • Riesgo de accidentes graves y congestión masiva • Posible bloqueo de rutas críticas para servicios de emergencia • Brecha abierta hasta 2030, cuando se prevé completar la sustitución de semáforos vulnerables

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

Vulnerabilidades en semáforos inteligentes Países Bajos	
Descripción	En 2024, se reveló una grave vulnerabilidad en el sistema KAR, utilizado en Países Bajos para dar prioridad a vehículos de emergencia y transporte público. El investigador Alwin Peppels demostró que, mediante radio definida por software, era posible enviar señales falsas y cambiar semáforos a voluntad desde varios kilómetros de distancia. El hallazgo evidenció la falta de cifrado y autenticación en dispositivos instalados desde 2005, dejando expuesta una infraestructura crítica que afecta a miles de intersecciones. Las autoridades confirmaron que la única solución es reemplazar todos los semáforos vulnerables, un proceso que se prolongará hasta 2030. Este caso subraya cómo la conectividad IoT en entornos urbanos, sin seguridad por diseño, puede derivar en riesgos físicos y caos vial.

TABLA 2: VULNERABILIDADES SEMÁFOROS PAÍSES BAJOS

Vulnerabilidades en vehículos Tesla	
Fecha	Enero 2024
Víctima	Tesla
Activo comprometido	Software de vehículos Tesla e infraestructura IoT asociada (routers internos, cargadores, módulos de telemetría)
Tipo de Amenaza	Explotación de vulnerabilidades críticas en entorno controlado (Bug Bounty / Competencia de hacking ético)
Vector del ataque	• Permisos de root en routers internos, permitiendo control de la red interna del vehículo • Explotación de cargadores específicos de Tesla para manipular disponibilidad y datos • Vulnerabilidades en sistemas IoT (sensores, telemetría, módulos electrónicos) que habilitan ejecución remota de comandos y espionaje de datos
Origen del ataque	Investigadores de Synacktiv durante Pwn2Own Automotive 2024
Impacto potencial	• Riesgo sobre sistemas críticos del vehículo (frenos, dirección, gestión energética) • Exposición de datos sensibles del usuario (patrones de movilidad, ubicaciones, credenciales)

Vulnerabilidades en vehículos Tesla	
	• Posibilidad de ataques en cadena sobre infraestructura urbana conectada
Descripción	En enero de 2024, durante la competencia Pwn2Own Automotive, el equipo Synacktiv descubrió 24 vulnerabilidades críticas en vehículos Tesla y su ecosistema IoT. Las fallas incluían permisos de root en routers internos, explotación de cargadores y vulnerabilidades en módulos de telemetría, lo que podría permitir control remoto del vehículo, fraude energético y espionaje de datos. Aunque el hallazgo ocurrió en un entorno controlado, el caso evidenció la complejidad y riesgos de la conectividad en automóviles inteligentes. Tesla respondió con actualizaciones OTA, endurecimiento de permisos y mejoras en autenticación y cifrado.

TABLA 3: VULNERABILIDADES VEHÍCULOS TESLA

Ciberataque al sistema de transporte en Polonia	
Fecha	Junio 2023
Víctima	Ciudad de Olsztyn (Polonia) – Autoridad de Transportes ZDZ iT
Activo comprometido	Sistema de gestión del tráfico, control de intersecciones, semáforos inteligentes, puntos Wi-Fi en tranvías, sistema de venta de billetes
Tipo de Amenaza	Ciberataque dirigido
Vector del ataque	Acceso remoto no autorizado a servidores de gestión del tráfico
Origen del ataque	No confirmado públicamente, actor externo
Impacto	• Paralización de casi 100 intersecciones en el centro urbano • Interrupción de semáforos y sistemas de transporte público • Grandes atascos en vías principales • Imposibilidad de comprar billetes en taquillas y sistemas digitales • Desconexión física de servidores para contener el ataque

Ciberataque al sistema de transporte en Polonia	
Descripción	En junio de 2023, la ciudad polaca de Olsztyn sufrió un ciberataque que paralizó su sistema de transporte inteligente. El incidente afectó a casi un centenar de intersecciones, interrumpiendo semáforos y otros elementos críticos del tráfico urbano. Además, los ciudadanos no pudieron adquirir billetes de transporte público, lo que agravó el caos en la movilidad. La autoridad de transporte se vio obligada a desconectar físicamente los servidores para frenar la propagación del ataque. Este caso evidenció cómo la dependencia de infraestructuras conectadas sin medidas robustas de ciberseguridad puede derivar en la interrupción total de servicios esenciales en una ciudad inteligente.

TABLA 4: CIBERATAQUE AL SISTEMA DE TRANSPORTE EN POLONIA

Filtración de datos en plataforma de gestión de aparcamientos	
Fecha	2023
Víctima	EasyPark – Plataforma de gestión de estacionamientos inteligentes
Activo comprometido	Base de datos de usuarios con información personal y financiera
Tipo de Amenaza	Acceso no autorizado / Exfiltración de datos
Vector del ataque	Explotación de credenciales débiles o vulnerabilidades en la plataforma web/app, con posible falta de segmentación entre módulos y bases de datos sensibles
Origen del ataque	No confirmado públicamente, actor externo
Impacto	• Fuga de datos personales (nombres, teléfonos, correos electrónicos) • Exposición parcial de información financiera (dígitos de tarjetas) • Riesgo de fraude, phishing y robo de identidad • Pérdida de confianza en la plataforma y afectación reputacional

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

Filtración de datos en plataforma de gestión de aparcamientos	
Descripción	En 2023, EasyPark, una plataforma líder en gestión de estacionamientos inteligentes sufrió un incidente de ciberseguridad que comprometió la privacidad de sus usuarios. El ataque se centró en la base de datos de clientes, exponiendo información sensible como nombres, números de teléfono, correos electrónicos y dígitos de tarjetas bancarias. Aunque la operativa del servicio no se interrumpió, la brecha evidenció deficiencias en la protección de datos y segmentación interna. El incidente puso de relieve cómo la falta de autenticación robusta y controles de acceso adecuados en plataformas digitales puede derivar en riesgos significativos para la confianza del ecosistema de movilidad urbana.

TABLA 5: FILTRACIÓN DE DATOS EN PLATAFORMA DE GESTIÓN DE APARCAMIENTOS

8. Marco normativo actual

La transformación de las ciudades hacia modelos de movilidad inteligente exige un marco normativo sólido que garantice la seguridad, integridad y resiliencia de todos los componentes del ecosistema urbano conectado. Desde los vehículos y sus sistemas electrónicos, hasta la infraestructura sensorizada, los centros de control y las plataformas digitales de gestión, la protección frente a ciberamenazas se ha convertido en un requisito fundamental para asegurar la continuidad de los servicios y la confianza de los ciudadanos.

El presente apartado recopila y describe las normativas, estándares y referencias técnicas más relevantes a nivel internacional, europeo y nacional, para garantizar la ciberseguridad en entornos de movilidad inteligente, abarcando tanto vehículos conectados y autónomos como centros de control de movilidad urbana, infraestructura sensorizada y plataformas de gestión. Su propósito es proporcionar un marco de referencia para asegurar la resiliencia, integridad y disponibilidad de los sistemas urbanos conectados.

8.1. Marco normativo internacional

8.1.1. ISO/SAE 21434:2021 – Road vehicles (Cybersecurity engineering)

El estándar ISO/SAE 21434:2021, desarrollado conjuntamente por ISO y la SAE (del inglés, Society of Automotive Engineers), establece directrices de ciberseguridad a lo largo de todo el ciclo de vida de los vehículos, desde el diseño y desarrollo hasta la operación y mantenimiento.

Aunque su enfoque principal son los sistemas electrónicos y conectividad de los vehículos, sus principios pueden extenderse al ecosistema de movilidad urbano, ya que permiten definir procesos de gestión de riesgos, evaluación de amenazas, seguridad en comunicaciones y actualización de software de manera coherente en sistemas interconectados.

El estándar se organiza en dominios y controles, que especifican prácticas concretas que fabricantes y operadores deben implementar para proteger los sistemas frente a ataques de seguridad y garantizar la seguridad funcional y operativa de los vehículos.

8.1.2. ISO/IEC 27001, 27017, 27018 y 270701 – Gestión de la seguridad de la información

La serie ISO/IEC 27000 establece el marco internacional para los sistemas de gestión de seguridad de la información (SGSI).

- ISO/IEC 27001 define los requisitos para implantar un SGSI basado en análisis de riesgos.
- ISO/IEC 27017 incorpora controles adicionales orientados a servicios cloud.
- ISO/IEC 27018 regula la protección de datos personales en entornos cloud públicos.
- ISO/IEC 27701 regula la protección de datos en los sistemas de información.

En el contexto de movilidad inteligente, estas normas resultan especialmente relevantes para centros de control de tráfico, plataformas de gestión de flotas, aplicaciones de movilidad, sistemas de ticketing, estacionamiento digital y cualquier servicio urbano que procese datos de ciudadanos o de infraestructura crítica. La adopción de estas normas asegura un tratamiento consistente de la confidencialidad, integridad, disponibilidad y privacidad de la información gestionada a escala municipal.

8.1.3. ISO/IEC 62443 – Seguridad en sistemas de automatización y control industrial

La serie ISO/IEC 62443 está orientada a la protección de sistemas de automatización, control industrial y entornos OT/SCADA. Su aplicación es especialmente relevante para infraestructuras urbanas conectadas tales como sistemas de gestión de semáforos, paneles de señalización variable, túneles inteligentes, centros de control de tráfico, redes de sensores de infraestructura crítica, estaciones de carga y sistemas energéticos asociados.

La norma establece modelos de madurez, requisitos para fabricantes y operadores, segmentación de redes, controles criptográficos y procedimientos para la gestión de incidentes. Su adopción es fundamental en las ciudades inteligentes, donde la convergencia IT/OT implica nuevos vectores de ataque y la necesidad de garantizar la continuidad operativa de servicios esenciales.

8.2. Marco normativo europeo

8.2.1. UNECE/R155

La normativa UNECE/R155, adoptada por la Comisión Económica de las Naciones Unidas para Europa (UNECE), define requisitos obligatorios de ciberseguridad para vehículos conectados. Inicialmente basada en recomendaciones técnicas de la UIT-T (Recomendación X.1371), la UNECE/R155 establece tipologías de ciberamenazas y criterios de exposición que los fabricantes deben gestionar para proteger a los usuarios de vehículos conectados y autónomos.

Desde el 1 de julio de 2024, su cumplimiento es obligatorio para fabricantes de vehículos y componentes electrónicos, incluyendo sistemas de control, telemática y conectividad. La normativa obliga a implementar mecanismos preventivos y de mitigación frente a vulnerabilidades y ciberamenazas identificadas.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

Asimismo, el marco de catalogación de UNECE/R155 se presenta en el Anexo I de este documento, y constituye una referencia clave para la evaluación de riesgos y el desarrollo de estrategias de seguridad en la movilidad urbana.

8.2.2. Regulation (EU) 2024/2847 – Cyber Resilience Act (CRA)

El Cyber Resilience Act establece requisitos obligatorios de ciberseguridad para todos los productos con componentes digitales, incluidos dispositivos IoT urbanos, sensores de movilidad, sistemas de tráfico y plataformas digitales asociadas. Obliga a fabricantes y operadores a aplicar prácticas de desarrollo seguro, gestión de vulnerabilidades, actualizaciones y evaluación continua de riesgos.

En el ámbito de movilidad inteligente, el CRA afecta directamente a infraestructuras conectadas (semaforización, centros de control, estaciones de carga, etc.), elevando las exigencias de seguridad y reduciendo la exposición a ciberataques sobre tecnologías críticas en entornos urbanos.

8.2.3. Directive (EU) 2022/2555 – NIS2

La Directiva NIS2 establece un marco europeo de seguridad para operadores de servicios esenciales, ampliando requisitos de gestión de riesgos, controles técnicos, supervisión y notificación de incidentes. Afecta a sectores críticos, incluyendo transporte, administraciones públicas y servicios de movilidad.

En movilidad inteligente, obliga a centros de control, operadores de flotas, sistemas de transporte público y plataformas MaaS a aplicar políticas de seguridad robustas, garantizando continuidad de servicio, protección de datos y resiliencia frente a ciberamenazas.

8.2.4. Regulation (EU) 2019/2144 – General Safety Regulation

El Reglamento (UE) 2019/2144 establece los requisitos de homologación de tipo para vehículos de motor en materia de seguridad, asistencia al conductor y ciberseguridad. Entre sus puntos más relevantes:

- Introduce la obligación de que los vehículos estén equipados con sistemas avanzados de seguridad activa y pasiva, incluyendo frenado automático, detección de peatones y control de estabilidad.
- Define criterios de ciberseguridad y seguridad funcional para componentes electrónicos y sistemas conectados, asegurando que no representen riesgos para los usuarios o el entorno urbano.
- Obliga a fabricantes a garantizar la trazabilidad de fallos y la capacidad de actualización remota segura de los sistemas de vehículos, alineándose con la UNECE R155 y el ISO/SAE 21434.

Este reglamento es fundamental para el despliegue seguro de vehículos conectados y autónomos en la Unión Europea, garantizando que su operación en entornos urbanos cumpla con estándares de seguridad funcional y protección frente a ciberamenazas.

8.2.5. Regulation (EU) 2018/858 - Homologación y supervisión del mercado

El Reglamento (UE) 2018/858 regula la homologación de vehículos, sus remolques y componentes, incluyendo sistemas electrónicos y unidades técnicas independientes. Sus implicaciones para la movilidad inteligente incluyen:

- Establece los criterios para que los fabricantes certifiquen que sus vehículos y sistemas cumplen con requisitos de seguridad, emisiones y funcionamiento correcto de sistemas conectados.
- Introduce obligaciones para la documentación y trazabilidad de fallos en componentes críticos, incluyendo la ciberseguridad de sistemas de conectividad y telemetría.
- Complementa la UNECE R155, ISO/SAE 21434 y el Reglamento 2019/2144, asegurando coherencia entre homologación técnica, seguridad funcional y protección frente a ciberamenazas.

Su aplicación garantiza que los vehículos integrados en las ciudades inteligentes operen de forma segura, interoperable y alineada con estándares europeos, sirviendo de referencia para centros de control de movilidad urbana, flotas corporativas y transporte público conectado.

8.2.6. Regulation (EU) 2016/679 - Reglamento General de Protección de Datos (GDPR)

El Reglamento General de Protección de Datos (GDPR) define los principios y obligaciones para el tratamiento seguro y lícito de datos personales, incluyendo geolocalización, identificadores digitales, matrículas o información de movilidad. Requiere consentimiento, minimización y medidas técnicas que garanticen confidencialidad e integridad.

En movilidad inteligente, su cumplimiento es crítico en plataformas MaaS, centros de control de tráfico, sistemas de ticketing, cámaras urbanas y aplicaciones de movilidad, donde se recopilan y procesan datos de ciudadanos de forma constante.

8.3. Marco normativo nacional

8.3.1. Estrategia de movilidad segura, sostenible y conectada 2030

La Estrategia de Movilidad Segura, Sostenible y Conectada 2030 (EMSSC 2030), impulsada por el Ministerio de Transportes y Movilidad Sostenible, constituye el marco nacional para transformar el sistema de transporte en España. La estrategia prioriza la seguridad vial, la digitalización de infraestructuras, la sostenibilidad ambiental y el impulso a la movilidad conectada, automatizada y basada en datos. Incluye líneas de actuación orientadas a promover vehículos conectados y autónomos, mejorar la interoperabilidad de infraestructuras y desarrollar servicios inteligentes para ciudadanos y operadores urbanos.

Desde una perspectiva de ciberseguridad, la EMSSC 2030 establece la necesidad de integrar requisitos de seguridad digital en infraestructuras críticas, redes de transporte, plataformas de movilidad y sistemas municipales. Impulsa la adopción de estándares internacionales, el refuerzo de la protección de datos y la creación de capacidades para la gestión de riesgos tecnológicos asociados a la movilidad inteligente. La estrategia sitúa la ciberseguridad como un elemento transversal para garantizar la resiliencia, continuidad de servicio y confianza en el ecosistema de movilidad urbana conectada.

8.3.2. Real Decreto 311/2022 - Esquema Nacional de Seguridad (ENS)

El Esquema Nacional de Seguridad (ENS), regulado por el Real Decreto 311/2022, establece los principios, requisitos y medidas que deben cumplir las administraciones públicas españolas, así como las empresas que les prestan servicios, con el fin de garantizar la seguridad de los sistemas que soportan

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

servicios públicos digitales. El ENS define un conjunto de medidas organizativas, operativas y de protección que deben implantarse según el nivel de seguridad (básico, medio o alto).

En entornos de movilidad inteligente, el ENS es clave para los centros de control urbano, las plataformas de gestión de tráfico y los sistemas y aplicaciones municipales asociadas. Su aplicación asegura que los servicios públicos digitales operen de forma segura, con controles adecuados de acceso, monitorización, trazabilidad, cifrado, continuidad de negocio y gestión de incidentes, contribuyendo a la resiliencia global del ecosistema urbano.

8.3.3. Ley Orgánica 3/2018 – LOPDGDD

La LOPDGDD complementa y transpone el Reglamento General de Protección de Datos al marco jurídico español, adaptándolo a las particularidades nacionales y estableciendo garantías adicionales sobre el tratamiento de datos personales, especialmente en ámbitos públicos. La norma refuerza obligaciones como la evaluación de impacto, la protección desde el diseño, el enfoque de responsabilidad proactiva y los derechos digitales aplicables a los ciudadanos.

En el ámbito de la movilidad inteligente, la LOPDGDD resulta especialmente relevante para administraciones locales y operadores urbanos que gestionan datos personales procedentes de sensores, cámaras, aplicaciones móviles, plataformas de movilidad, sistemas de estacionamiento o servicios públicos digitalizados. Su cumplimiento exige aplicar medidas de minimización y asegurar que cualquier tratamiento de datos urbanos se realice con garantías suficientes de seguridad, transparencia y proporcionalidad.

8.3.4. Código de Tráfico y Seguridad Vial

El Código de Tráfico y Seguridad Vial (Real Decreto Legislativo 6/2015, de 30 de octubre) establece las normas de circulación, seguridad vial y requisitos de vehículos que circulan en España. Aunque su enfoque principal es la seguridad de la conducción y la regulación de infraestructuras, también incluye disposiciones relevantes para la movilidad conectada, como:

- Requisitos para la homologación y uso de sistemas electrónicos de asistencia a la conducción (ADAS).
- Normas sobre instalación y uso de dispositivos de comunicación y control en vehículos.
- Responsabilidades legales de fabricantes, operadores y conductores ante fallos de sistemas tecnológicos.

Este marco jurídico español proporciona la base legal para garantizar que la integración de vehículos conectados y autónomos en entornos urbanos cumpla con los estándares de seguridad vial, al tiempo que se coordina con iniciativas de ciberseguridad y gestión de movilidad inteligente.

9. Buenas prácticas

La seguridad de los entornos tecnológicos que soportan la movilidad inteligente, incluyendo vehículos conectados, vehículos autónomos, flotas corporativas, transporte público y servicios municipales, es un elemento crítico para garantizar la operativa diaria, la protección de los usuarios y la resiliencia de los servicios.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

Tras el análisis de arquitecturas, comunicaciones, normativas y ciberamenazas, se establecen las siguientes recomendaciones, orientadas a reforzar de manera proactiva la protección de todos los sistemas vinculados al ecosistema de movilidad.

9.1. Recomendaciones

9.1.1. Comunicaciones

Las comunicaciones constituyen el pilar fundamental de la movilidad inteligente, ya que permiten el intercambio continuo de información entre vehículos, infraestructuras, plataformas de gestión, sensores y servicios externos. Este ecosistema integra comunicaciones V2I, V2V, V2P, V2N, enlaces entre dispositivos IoT y plataformas municipales, así como la conexión de usuarios con servicios urbanos para consultar tiempos de paso, incidencias o rutas. Garantizar su seguridad implica asegurar que los datos transmitidos no puedan ser manipulados, interceptados o utilizados para comprometer el funcionamiento de los sistemas urbanos.

- **Gestión segura de sesiones**

Es necesario asegurar que el establecimiento y mantenimiento de sesiones de comunicación entre los distintos componentes del ecosistema urbano se gestione de forma estricta y controlada. Esto implica que solo los sistemas y usuarios autorizados puedan iniciar o mantener un canal de comunicación, reduciendo la posibilidad de accesos no legítimos, interferencias o manipulaciones durante la interacción entre vehículos, plataformas y dispositivos IoT.

- **Filtrado de paquetes y control de tráfico**

Debe implantarse un modelo de supervisión continua del tráfico que permita detectar comportamientos anómalos, patrones inusuales o intercambios que excedan las funciones previstas dentro del sistema de movilidad. Este control contribuye a prevenir que incidentes aislados se propaguen hacia otros elementos, manteniendo la operatividad y la protección de los servicios esenciales.

- **Segregación de redes y entornos**

Es recomendable dividir los flujos de comunicación en dominios funcionales independientes con el fin de evitar que un incidente en un área no crítica pueda derivar en un impacto sobre componentes esenciales para la seguridad o la operación. Este enfoque ayuda a contener fallos, limitar su alcance y mantener la continuidad del servicio incluso ante un compromiso parcial.

- **Cifrado y protección extremo a extremo**

Es fundamental garantizar que la información intercambiada, ya sea entre vehículos, infraestructura o plataformas urbanas, se transmita de manera íntegra y confidencial. El uso de mecanismos criptográficos robustos y actualizados permite evitar fugas de información, suplantación de entidades o alteraciones no autorizadas del contenido transmitido.

9.1.2. Actualización de software

El software es un componente dinámico dentro de cualquier entorno de movilidad conectada y, por tanto, debe mantenerse actualizado para garantizar su seguridad. Las actualizaciones periódicas permiten corregir fallos, incorporar mejoras funcionales y reforzar la protección ante nuevas amenazas que puedan surgir en un entorno tecnológico cambiante.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

❖ **Aplicación temprana de parches y actualizaciones**

Es indispensable establecer procedimientos que garanticen la actualización continua de todos los elementos tecnológicos implicados: vehículos, sensores, dispositivos IoT, plataformas de gestión y sistemas de comunicación. Una gestión ágil y estructurada de los parches minimiza el riesgo derivado de vulnerabilidades conocidas y contribuye a mantener la resiliencia del sistema en su conjunto.

❖ **Gestión del proceso de actualización**

El proceso de actualización debe diseñarse para evitar errores o manipulaciones que puedan comprometer la integridad operativa. Esto incluye la validación de la procedencia del software, la verificación de su integridad y la existencia de mecanismos que permitan revertir cambios en caso de incidencias, garantizando que el sistema siga funcionando de forma segura.

9.1.3. Criptografía

La protección de la información es una prioridad en los entornos de movilidad, donde se manejan datos de geolocalización, operación, estado de vehículos, itinerarios y posibles datos personales. La criptografía constituye la herramienta principal para asegurar la confidencialidad, integridad y autenticidad de dicha información.

❖ **Gestión segura del ciclo de vida de las claves**

Es necesario contar con un marco de gobernanza que regule la creación, distribución, uso, renovación y retirada de claves y certificados utilizados en el ecosistema. Una gestión sólida evita exposiciones innecesarias, garantiza la trazabilidad y asegura que la protección criptográfica se mantenga efectiva durante todo el ciclo de vida de los servicios.

❖ **Eliminación de configuraciones predeterminadas**

Todo componente tecnológico debe ser integrado en el sistema mediante configuraciones personalizadas y seguras. Mantener credenciales o parámetros por defecto constituye una de las formas más comunes de acceso no autorizado y debe evitarse desde la fase inicial de despliegue.

9.1.4. Protección contra software malicioso

La complejidad del ecosistema urbano conectado implica que pueda ser objeto de intentos de intrusión, manipulación o interrupción de los servicios mediante software malicioso. Una estrategia de protección adecuada evita que este tipo de amenazas afecten a la continuidad operativa o comprometan datos sensibles.

❖ **Solución antimalware centralizada**

Debe establecerse un sistema global de supervisión, capaz de analizar comportamientos sospechosos en los distintos dispositivos que conforman el ecosistema de movilidad. Este enfoque coordinado permite identificar de forma temprana intentos de manipulación o la presencia de software no autorizado.

❖ **Gestión de la ejecución de archivos o procesos**

Es recomendable limitar de forma estricta la capacidad de ejecutar contenido o procesos no verificados en los equipos de soporte, herramientas de mantenimiento o dispositivos asociados al sistema urbano.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

Esta medida reduce significativamente el riesgo de propagación de amenazas entre distintos elementos de la infraestructura.

9.1.5. Control de accesos

El acceso a los sistemas de movilidad debe estar regulado bajo criterios de seguridad que garanticen que únicamente las personas y sistemas adecuados puedan interactuar con los distintos componentes, minimizando así los riesgos derivados de accesos indebidos o uso malintencionado de las plataformas.

- **Principio de mínimo privilegio**

Es esencial que cada usuario, dispositivo o servicio disponga únicamente de los permisos estrictamente necesarios para desempeñar sus funciones. Reducir la exposición de los accesos limita la posibilidad de que un fallo puntual derive en un impacto mayor sobre el sistema.

- **Reglas estrictas para accesos remotos**

Los accesos remotos a vehículos, plataformas urbanas o sistemas de supervisión deben estar sometidos a procedimientos robustos de autenticación y a una supervisión continuada. Esto evita que terceros no autorizados puedan manipular elementos críticos.

- **Autenticación multifactor (MFA)**

La autenticación multifactor y otros sistemas avanzados de verificación de identidad refuerzan la protección de las plataformas, evitando que credenciales comprometidas puedan utilizarse para acceder a entornos críticos.

9.1.6. Monitorización

La movilidad inteligente requiere una monitorización continua que permita identificar comportamientos inusuales, prever incidentes y actuar con rapidez ante cualquier señal de alerta. La capacidad de detectar anomalías de manera temprana es clave para limitar el impacto de potenciales amenazas.

- **Detección de comportamientos anómalos**

La monitorización debe centrarse tanto en la infraestructura como en los vehículos y dispositivos asociados, identificando patrones anómalos, desviaciones no previstas o indicadores tempranos de riesgo que puedan anticipar un incidente.

- **Gestión segura del registro de logs**

Los registros deben almacenarse, gestionarse y revisarse de manera estructurada, asegurando su integridad y la disponibilidad de información suficiente para llevar a cabo análisis posteriores, auditorías o investigaciones forenses. Concretamente, bajo los siguientes principios:

- Formato homogéneo y preparado para análisis forense.
- Aplicación del principio de mínimo privilegio para evitar manipulación.
- Sincronización temporal de todos los dispositivos para asegurar la trazabilidad de incidentes.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

9.1.7. Auditoría técnica

Para garantizar que las medidas implantadas se mantienen eficaces en el tiempo, es imprescindible llevar a cabo revisiones periódicas que evalúen el estado real del sistema y detecten posibles desviaciones u oportunidades de mejora.

- **Revisión periódica de la seguridad**

Debe establecerse un calendario regular de auditorías técnicas que supervise configuraciones, accesos, arquitecturas y mecanismos de protección, permitiendo detectar brechas o prácticas inseguras.

9.1.8. Continuidad de negocio

La continuidad de los servicios de movilidad es esencial para los servicios urbanos y los usuarios. Un fallo prolongado puede generar impactos significativos en la actividad urbana, por lo que es necesario prever escenarios y establecer mecanismos de recuperación.

- **Realización de un Análisis de Impacto en el Negocio (BIA)**

El BIA permite identificar qué elementos de la infraestructura son críticos para el funcionamiento diario, así como los tiempos máximos de recuperación aceptables. Este análisis constituye la base para planificar respuestas eficaces frente a incidentes.

- **Elaboración de un Plan de Continuidad del Negocio (PCN)**

El PCN establece los procedimientos que deben activarse para garantizar el funcionamiento de los servicios de movilidad ante fallos de infraestructura, indisponibilidad de plataformas, ataques de seguridad o interrupciones imprevistas.

- **Gestión de backups**

Las copias de seguridad periódicas de datos críticos permiten recuperar la operativa tras incidentes, evitando pérdidas de información que puedan generar interrupciones prolongadas.

9.1.9. Contingencia

La contingencia se centra en la capacidad de respuesta ante incidentes graves que comprometan de forma significativa la infraestructura de movilidad.

- **Desarrollo de un Plan de Recuperación ante Desastres (DRP)**

El DRP define los procedimientos y recursos necesarios para restablecer la operativa en situaciones extraordinarias, garantizando que los servicios esenciales puedan volver a funcionar de forma segura y ordenada.

9.1.10. Gestión de incidentes

Una gestión eficiente de los incidentes permite minimizar el impacto y restablecer en el menor período de tiempo posibles la normalidad operativa de los servicios.

- **Establecimiento de un proceso formal de notificación de incidentes**

Debe existir un procedimiento claro que determine cómo se identifican, clasifican, registran y comunican los incidentes, tanto internamente como ante organismos competentes.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

9.1.11. Formación y concienciación

La seguridad tecnológica depende también del factor humano. La formación y la concienciación son elementos clave para prevenir errores operativos y anticipar amenazas basadas en ingeniería social.

- **Programas periódicos de capacitación**

Los operadores, personal técnico, responsables municipales y usuarios que intervienen en el ecosistema de movilidad deben recibir formación actualizada que les permita comprender los riesgos y aplicar buenas prácticas en su actividad diaria.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

10. Anexos

Este apartado incluye información complementaría que respalda y amplía el contenido principal del documento.

10.1. Anexo I. UNECE/R155 (Marco de catalogación de amenazas)

A continuación, se incorporan las principales vulnerabilidades y ciberamenazas identificadas por la normativa UNECE/R155 junto a la descripción de estas:

Categoría	Amenaza	Método de ataque
Amenazas de los VEC relacionadas con los servidores de soporte.	Uso de servidores de soporte como medio para atacar un vehículo o extraer datos.	Abuso de privilegios por parte de usuarios, es considerado como un ciberataque de tipo interno.
		Acceso no autorizado desde internet al servidor (por medio de puertas traseras, vulnerabilidades del software de sistema sin parches, inyecciones SQL u otros medios).
		Acceso físico no autorizado al servidor (por medio de dispositivos USB u otros medios que puedan conectarse al servidor).
	Alteración de los servicios del servidor de soporte para afectar al funcionamiento de un vehículo	El ataque al servidor de soporte detiene su operativa e impide la interacción con los VEC para proporcionar los servicios de los que éstos dependen.
	Pérdida o exposición de los datos almacenados en los servidores de soporte (brecha de datos).	Abuso de privilegios por parte de usuarios, es considerado como un ciberataque de tipo interno.
		Pérdida de información en la nube, pudiendo perderse datos sensibles debido a ataques o accidentes si los datos son almacenados por servicios en la nube de terceros.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

Categoría	Amenaza	Método de ataque
		Acceso no autorizado desde internet al servidor (por medio de puertas traseras, vulnerabilidades del software de sistema sin parches, inyecciones SQL u otros medios).
		Acceso físico no autorizado al servidor (por medio de llaves USB u otros medios que se conectan al servidor).
		Divulgación involuntaria de información debido al intercambio no intencionado de datos, como por ejemplo, fallos en la administración en el almacenamiento de datos en servidores ubicados en garajes.
Amenazas de los vehículos relacionadas con sus canales de telecomunicaciones.	Manipulación de mensajes o datos recibidos por el vehículo.	Manipulación de mensajes mediante la usurpación de identidad (por ejemplo, 802.11p V2X durante la agrupación, mensajes del GNSS, etc.).
		Ataque Sybil (para simular vehículos en la carretera y provocar accidentes viales).
	Uso de canales de comunicación para realizar manipulación no autorizada, supresión u otras modificaciones en el código y datos almacenados en el vehículo.	Inyección de código en los canales de telecomunicación (por ejemplo, introduciendo código malicioso en la corriente de telecomunicación).
		Manipulación de código o datos del vehículo por medio de canales de telecomunicación.
		Sobreescritura de código o datos del vehículo por medio de canales de telecomunicación.
		Borrado de código o datos del vehículo por medio de canales de telecomunicación.
		Introducción de código o datos del vehículo por medio de canales de telecomunicación.
	Recepción, por medio de canales de telecomunicación que posibilitan mensajes	Admisión información de una fuente sospechosa no fiable.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

Categoría	Amenaza	Método de ataque
	sospechosos y no fiables o vulnerables para la manipulación de la sesión mediante ataques por repetición.	Ataque de intercepción y manipulación de la sesión.
		Ataque por repetición (por ejemplo, un ataque contra una pasarela de comunicación permite al atacante degradar el software de un ECU o el software del fabricante de la pasarela de pagos).
	Posibilidad de acceso directo a la información mediante intercepción de las comunicaciones o por acceso no autorizado a archivos o carpetas sensibles.	Intercepción de información mediante la interferencia de las ondas de radio de las comunicaciones.
		Obtención de acceso no autorizado a archivos o datos.
	Ataques de denegación de servicio (DDoS) a través de los canales de comunicación para perturbar las funciones del vehículo.	Envío de un gran número de peticiones al sistema de información del vehículo, con el objetivo de evitar que pueda prestar servicios de manera normal (DDoS).
		Ataque DDoS con el objetivo de perturbar las comunicaciones entre vehículos.
	Capacidad de un usuario sin privilegios de obtener acceso privilegiado a los sistemas del vehículo.	Obtención de acceso privilegiado por un usuario sin privilegios (acceso al usuario raíz).
	Malware integrado en los medios de comunicación que pueden infectar los sistemas de los vehículos.	Infección de los sistemas de los vehículos por medio de malware integrados en los medios de comunicación.
	Mensajes recibidos por el vehículo (mensajes X2V o de diagnóstico) o transmitidos en él, que incluyen contenido malicioso.	Mensajes internos maliciosos (por ejemplo, Bus CAN).
		Mensajes V2X maliciosos (como mensajes de infraestructura a vehículo o de vehículo a vehículo, por ejemplo, CAM, DENM).

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

Categoría	Amenaza	Método de ataque
		Mensajes de diagnóstico maliciosos.
		Mensajes maliciosos enviados por el OEM o el proveedor de componentes, sistemas y funciones).
Amenazas de los vehículos relacionadas con sus procedimientos de actualización.	Uso indebido o de los procedimientos de actualización.	Procedimientos de actualización del software inalámbricos comprometidos. Esto incluye la fabricación de programas de actualización del sistema y de software del fabricante.
		Procedimientos de actualización del software local y físico comprometido.
		Manipulación del software antes del proceso de actualización, manteniendo el proceso de actualización intacto, pero quedando el software corrompido.
		Claves criptográficas del proveedor de software comprometidas permitiendo actualizaciones no válidas.
	Rechazo de actualizaciones legítimas.	Ataque DDoS contra el servidor o la red de actualización para evitar la distribución de actualizaciones de software esencial o desbloquear características específicas del cliente.
Amenazas de los vehículos relacionadas con acciones humanas no intencionales.	Mala configuración de equipos o sistemas por parte de usuarios legítimos o el equipo de mantenimiento.	Mala configuración del equipo por parte del equipo de mantenimiento o el propietario durante la instalación, reparación, utilización y provocando consecuencias no deseadas.
		Utilización o administración erróneas de los dispositivos y sistemas (incluidas las actualizaciones OtA).
	Acciones realizadas por usuarios legítimos que faciliten involuntariamente ciberataques.	Engaño al usuario o equipo de mantenimiento con el fin de que realice una acción para instalar involuntariamente un software malicioso y permitir un ataque.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

Categoría	Amenaza	Método de ataque
		No se siguen los procedimientos de seguridad definidos.
Amenazas de los vehículos relacionadas con su conectividad y sus conexiones externas.	Manipulación de las funciones de conectividad del vehículo que hagan posible un ciberataque. Por ejemplo: telemática, sistemas que permiten operaciones a distancia y sistemas que utilizan telecomunicaciones inalámbricas de corto alcance.	Manipulación de funciones destinada a explotar sistemas de manera remota, como la clave a distancia, el inmovilizador y la pila de carga.
		Manipulación de la telemática del vehículo (por ejemplo, manipulación de la medición de temperatura de elementos sensibles como la batería o el desbloqueo a distancia de las puertas de carga).
		Interferencia con sistemas o sensores inalámbricos de corto alcance.
	Uso de software de terceros, como aplicaciones de entretenimiento, para atacar los sistemas del vehículo.	Utilización de aplicaciones con poca seguridad para vulnerar los sistemas del vehículo.
	Conexión de dispositivos a interfaces externas, como puertos USB u OBD, para atacar a los sistemas del vehículo.	Introducción de códigos utilizando interfaces externas, como por ejemplo puertos USB, a modo de puntos de ataque.
		Medios infectados por un malware y conectados a un sistema del vehículo.
		Uso del acceso de diagnóstico (adaptadores en el puerto OBD) para facilitar un ataque de manipulación (directa o indirecta) de los parámetros del vehículo.
Posibles objetivos de un ciberataque.	Extracción de datos del vehículo.	Extracción o liberalización mediante jailbreak de las licencias de software del fabricante).

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

Categoría	Amenaza	Método de ataque
		Acceso no autorizado a la información privada de datos del usuario como la identidad personal, la información de la cuenta de pago, la información del libro de direcciones, la información de localización y el identificador electrónico del vehículo, etc.
		Extracción de claves criptográficas.
	Manipulación de datos del vehículo.	Cambios ilegales no autorizados al identificador electrónico de un vehículo.
		Fraude de identidad del usuario del vehículo.
		Medidas para eludir los sistemas de supervisión (por ejemplo, mediante la manipulación o bloqueo de mensajes tales como los datos del administrador).
		Manipulación de datos para falsificar los datos de conducción del vehículo (por ejemplo, kilometraje, dirección de conducción, etc.).
		Cambios no autorizados de los datos de diagnóstico del sistema.
	Borrado de datos	Borrado o manipulación sin autorización del registro de eventos del sistema.
	Implantación de malware.	Introducción y actividad de software malicioso.
	Instalación de nuevo software o sobreescritura del software existente.	Elaboración de software del sistema de control o de información del vehículo.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

Categoría	Amenaza	Método de ataque
	Perturbación de sistemas o u operaciones.	Denegación de servicio (por ejemplo, poniendo en marcha en la red interna inundándola de mensajes en un Bus CAN o provocando fallos en una ECU mediante una alta densidad de envío de mensajes).
	Manipulación de parámetros del vehículo.	Acceso no autorizado para falsificar los parámetros de configuración de las funciones clave de un vehículo (por ejemplo, los datos de frenado o el umbral para el despliegue del airbag, etc.).
		Acceso no autorizado para falsificar los parámetros de carga, (por ejemplo, el voltaje de carga, la potencia de carga, la temperatura de la batería, etc.).
Potenciales vulnerabilidades que pueden ser explotadas si no están suficientemente protegidas o fortalecidas.	Uso insuficiente o incorrecto de tecnologías criptográficas.	No combinación de caracteres en las claves de cifrado junto a longitudes cortas y sin un periodo de validez permiten al atacante romper las claves con facilidad.
		Utilización de algoritmos criptográficos para proteger sistemas sensibles.
		Utilización de algoritmos criptográficos obsoletos.
	Vulnerabilidades existentes en componentes de los vehículos.	Equipos o software, diseñados para permitir un ataque o que no cumplen los criterios para detenerlo.
	Vulnerabilidades existentes en equipos o software.	La presencia de errores de código aumenta el riesgo de vulnerabilidades explotables si el software no se ha probado para corregirlos.
		Explotación de vulnerabilidades en hardware y software (por ejemplo, puertos de depuración de errores, puertos JTAG, microprocesadores, certificados de desarrollo, contraseñas de programador, etc.) también puede dar acceso a las ECU o permitir a los atacantes obtener privilegios más elevados.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

Categoría	Amenaza	Método de ataque
	Vulnerabilidades existentes en el diseño de la red.	El acceso a los sistemas de la red por puertos de comunicación abiertos sin supervisión.
		La no segregación de redes (por ejemplo, el uso de pasarelas o de puntos de acceso, como las pasarelas camión-remolque, desprotegidos para eludir las protecciones y obtener acceso a otros segmentos de la red para realizar actos maliciosos tales como el envío de mensajes de Bus CAN arbitrarios y ofuscar la conducción).
	Pérdida física de los datos	Daños causados por un tercero. Los datos sensibles pueden perderse o quedar comprometidos debido a daños físicos en casos de accidentes viales o robo.
		Pérdida de datos por conflictos de gestión de los derechos digitales DRM (del inglés, Digital Rights Management).
		Pérdida de datos sensibles o menoscabo de la integridad de estos, debido al desgaste habitual de los componentes electrónicos.
	Transferencia de datos involuntaria.	Filtrado de datos privados o sensibles de los usuarios del vehículo (por ejemplo, cuando el vehículo se vende o es utilizado por otras organizaciones como vehículo de alquiler).
	Manipulación física de los sistemas.	Manipulación del equipo del OEM (por ejemplo, añadiendo equipos no autorizados al vehículo, haciendo que sea posible un ataque de MiTM).

TABLA 6: MARCO DE CATALOGACIÓN DE AMENAZAS UNECE/R155

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Junta de Andalucía
Agencia Digital de Andalucía

11. Referencias

1. Asociación Española de Normalización (UNE. (2021). *Normalización en Ciberseguridad para la Movilidad Conectada y Automatizada de vehículos y su entorno*. https://www.une.org/normalizacion_documentos/Informe%20Ciberseguridad%20Movilidad%20Inteligente.pdf

2. European Automobile Manufacturers Association (ACEA). (2023). *Automotive Regulatory Guide*. https://www.acea.auto/publication/automotive-regulatory-guide-2023/

3. European Union Agency for Cybersecurity (ENISA). (2025). *ENISA Threat Landscape 2025.* https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025#contentList

4. European Union Agency for Cybersecurity (ENISA). (2021). *Recommendations for the security of CAM*. https://www.enisa.europa.eu/publications/recommendations-for-the-security-of-cam

5. European Union Agency for Cybersecurity (ENISA). (2019). *ENISA good practices for security of Smart Cars*. https://www.enisa.europa.eu/publications/smart-cars

6. European Union. (2019). *Regulation (EU) 2019/2144 of the European Parliament and of the Council on horizontal cybersecurity requirements for motor vehicles*. https://eur-lex.europa.eu/eli/reg/2019/2144/oj/eng

7. European Union. (2018). *Regulation (EU) 2018/858 of the European Parliament and of the Council on the approval and market surveillance of motor vehicles*. https://eur-lex.europa.eu/eli/reg/2018/858/oj/eng

8. International Organization for Standardization. (2022). *ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. https://www.iso.org/standard/27001

9. Ministerio De Tranportes y Movilidad Sostenible. (2020). *Estrategia de Movilidad Segura, Sostenible y Conectada 2030*. https://www.transportes.gob.es/movilidad-sostenible/estrategia-de-movilidad-segura-sostenible-y-conectada-2030

10. OWASP Foundation. (2023). *OWASP Internet of Things Project.* https://owasp.org/www-project-internet-of-things/

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
Junta de Andalucía
Agencia Digital de Andalucía

11. United Nations Economic Commission for Europe (UNECE). (2021). *UN Regulation No. 155 - Cyber security and cyber security management system.* https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security

12. World Economic Forum (WEF). (2025). *Automotive and New Mobility*. https://www.weforum.org/communities/the-future-of-autonomous-and-urban-mobility/

12. Otras referencias de interés

El presente apartado recoge un resumen de los principales temas abordados en la guía, así como la relación de productos y servicios mencionados en ella. Su finalidad es ofrecer una visión global de los ámbitos tratados y facilitar la identificación de posibles referencias o elementos relevantes para futuras consultas o ampliaciones documentales.

12.1. Lista de materias tratadas en la guía

- Ecosistema de movilidad inteligente en Smart Cities.
- Infraestructura urbana conectada.
- Sistemas de transporte y movilidad urbana.
- Infraestructura de soporte a la movilidad inteligente.
- Plataformas de gestión y análisis de servicios de movilidad urbanos.
- Vehículos inteligentes.
- Vehículos autónomos.
- Amenazas en la movilidad inteligente.
- Marco regulatorio de movilidad inteligente.
- Buenas prácticas de seguridad para la movilidad inteligente.
- UNECE/R155
- ISO/SAE 21434:2021

12.2. Lista de productos mencionados en la guía

No se mencionan productos específicos en la guía.

12.3. Lista de servicios mencionados en la guía

No se mencionan servicios específicos en la guía.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía

Movilidad Inteligente y Cibersegura

Diciembre de 2025

Versión 1.0

Junta de Andalucía

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad
Junta de Andalucía
Agencia Digital de Andalucía