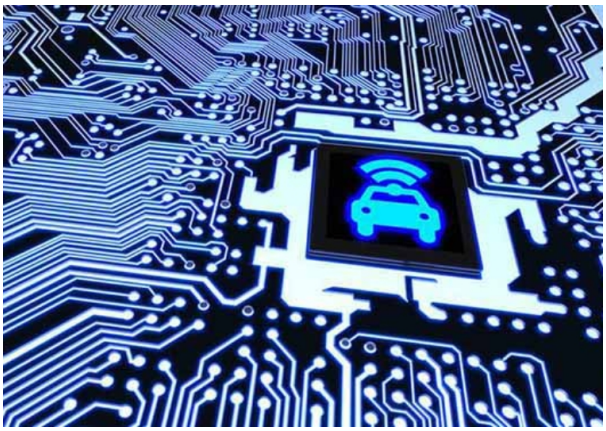
# Ciberseguridad para automoción

Como laboratorio experto en evaluaciones de seguridad de sistemas embebidos, damos soporte a la industra de la automoción evaluando la resiliencia de componentes y sistemas ante ciberataques avanzados, ya sean a nivel hardware, software, de comunicaciones o de criptografía.



Los nuevos vehículos dependen cada vez más de una red de chips y componentes TIC que se comunican internamente entre ellos por cable o de forma inalámbrica (CAN, LIN, Auto Ethernet), y externamente con servicios telemáticos, sistemas de carga de baterías, u otros vehículos e infraestructuras – para las funcionalidades de conducción autónoma.

Los **proveedores (Tier 1)** de la industria de la automoción son responsables del desarrollo de la mayoría de componentes del vehículo que son críticos a nivel de seguridad. Por ello, los **fabricantes (OEM)** les piden garantías de que sus componentes tienen las protecciones y contramedidas necesarias para garantizar la resiliencia del sistema contra potenciales atacantes.

Los **estándares y regulaciones sobre ciberseguridad en vehículos y sus componentes** están aún en desarrollo. La UNECE WP.29 es la única regulación obligatoria en vigor, aunque los OEMs tienen disponibles un gran número de estándares sectoriales y buenas prácticas para definir los requisitos de ciberseguridad que van a pedir a los Tier 1.

A la hora de ensayar y demostrar la resiliencia de los componentes ante ciberataques de última generación, fabricantes y proveedores pueden acudir a **laboratorios independientes** especializados en evaluaciones de seguridad.

# Evaluaciones de ciberseguridad para componentes de automoción

Los laboratorios IT de Applus+ disponen de una gran experiencia evaluando la seguridad de componentes embebidos, a nivel de hardware, software, comunicaciones y criptografía. Nuestro expertise abarca el stack completo OSI, desde el boot del sistema a las comunicaciones dentro del propio sistema. Esta visión general nos permite evaluar sistemas complejos con un alto nivel de garantía.

## Análisis de Amenazas y Evaluación de Riesgos (TARA)

- Revisión – global, por proyecto o continua - de las actividades y la gestión de la ciberseguridad, durante las fases de concepto, desarrollo y post desarrollo del producto, para poder alcanzar el nivel de garantías de seguridad objetivo.
- Los proyectos TARA se pueden realizar siguiendo estándares específicos del sector de la automoción, como la ISO/SAE DIS 21434, o bajo marcos menos sectoriales como la ISO/IEC 62443, incluso se pueden realizar sistema TARA a medida, siguiendo los requisitos del cliente.

## Evaluaciones de seguridad a medida de las necesidades del cliente

Adaptamos el esfuerzo de la evaluación a los niveles de garantía deseados por el cliente (garantía básica, moderada o completa). El objeto de la evaluación también puede ajustarse, evaluando un solo componente (SoC, HSM, PCB), un dispositivo (ECU, TCU, OBC) o un sistema o red completa (3GPP, Bluetooth, CAN, 100-BaseT1).

- Revisión del diseño, revisión del código fuente y análisis de vulnerabilidades.
- Full-stack de ensayos de penetración para evaluar la resistencia y resiliencia a los ataques del dispositivo.
- Evacuaciones a medida para requisitos de conformidad propios entre el OEM y el proveedor.

## Formaciones sobre ciberseguridad y buenas practicas (diseño y código)

Cursos y formaciones en abierto sobre ciberseguridad orientados a roles como ingenieros de sistemas, managers de ciberseguridad o arquitectos de software. Algunos ejemplos de nuestras formaciones:

- Estado del arte de los principios de programación segura y como aplicarlos en las operaciones del día a día.
- Componentes y sistemas de automoción vistos desde la perspectiva de un atacante y maneras atacar dispositivos y componentes de un vehículo. Maneras de aplicar este conocimiento al producto para hacerlo más robusto.

## ¿Por qué escoger a Applus+ Laboratories como partner de ciberseguridad?

- Un laboratorio especialista en evaluaciones de seguridad de alta garantía y con experiencia en diversos sectores: automoción, pagos, telecomunicaciones, industria, mobile…
- Técnicas de ataque avanzadas y equipos para evaluar componentes y dispositivos integrados en el vehículo, cubriendo ataques físicos, de software, ataques de red y wireless.
- Soporte en fase de desarrollo para la validación de la seguridad del producto a lo largo del ciclo de vida.
- Presencia en Europa (2 laboratorios en España) y en Asia (laboratorio funcional en Shanghái).
- Capacidad para cubrir diferentes estándares y regulaciones relacionadas con la ciberseguridad para el sector de la automoción.

Nota: Dado que Applus+ Laboratories está acreditado como laboratorio independiente por varios esquemas de certificación, los ingenieros de Applus+ nunca participan en el desarrollo de producto o la implementación de soluciones, garantizando así su imparcialidad.