NOTA DE PRENSA

Los vehículos deberán contar con un certificado de ciberseguridad, según una nueva normativa de la ONU/UNECE

**La nueva normativa ONU / UNECE WP.29, que ha entrado en vigor el 1 de enero de 2021, obliga a que los vehículos cuenten con un certificado que garantice que es ciberseguro durante todo su ciclo de vida.**

**Afecta a coches, autobuses, camiones, furgonetas, autocaravanas y remolques.**

**La Unión Europea ya ha anunciado que hará cumplir la norma a partir de julio de 2022 y afectará a todos los vehículos nuevos a partir de julio de 2024.**

**EUROCYBCAR, con sede en Vitoria-Gasteiz, es la única empresa en todo el mundo que, en la actualidad, emite el certificado de ‘Vehículo Ciberseguro’ según la normativa ONU / UNECE WP.29.**

Febrero de 2021

La normativa ONU / UNECE WP.29, que obliga a los vehículos a contar con un certificado de ciberseguridad, ha entrado en vigor el 1 de enero de 2021. Será de obligada aplicación en todos los países de la Unión Europea y afectará a coches, furgonetas, autocaravanas, camiones y autobuses. También a los vehículos ligeros de cuatro ruedas si están equipados con funciones de conducción automatizada a partir del nivel 3 y a los remolques si están dotados con, al menos, una unidad de control electrónico.

En la UE, deberán cumplirla los vehículos que se homologuen a partir de julio de 2022, obligación que se extenderá a todos los vehículos nuevos que se vendan en este territorio a partir del 1 de julio de 2024.

Para lograr el certificado de ciberseguridad, los fabricantes deberán demostrar que sus modelos están protegidos frente a 70 vulnerabilidades. Ese listado de riesgos a evitar incluye posibles ciberataques durante el desarrollo, producción y posproducción del vehículo, por lo que aquellos modelos que logren el certificado estarán protegidos a lo largo de todo su ciclo de vida. Además, se especifica que debe ser una entidad autorizada e independiente del fabricante la que acredite si el vehículo analizado cumple esos requisitos.

En el caso de que algún fabricante ponga a la venta en la UE un vehículo que no cumpla con la normativa ONU / UNECE WP.29 o se demuestre que engañaron a la entidad autorizada para obtener el certificado de manera irregular, se enfrentaría a sanciones de hasta 30.000€ por vehículo y se podría retirar o suspender la homologación de los modelos afectados -lo cual impediría que se pudiesen vender-.

La normativa no detalla qué medidas deben tomar los fabricantes para hacer frente a esas 70 amenazas. Tampoco indica qué tipo de pruebas se deben realizar para saber si un vehículo puede obtener el certificado APTO de ciberseguridad.

Por suerte, ya existe una empresa que dispone de un test que evalúa si un vehículo cumple con los requisitos de esa normativa: [EUROCYBCAR](https://eurocybcar.com/). Las pruebas se realizan en un laboratorio ubicado en Vitoria-Gasteiz, donde hackers, ingenieros IT, probadores de coches y QTester llevan realizando, desde hace años, la evaluación técnica de ciberseguridad -el Test [EUROCYBCAR-](https://eurocybcar.com/) a vehículos de organismos públicos y OEMs.

Una vez que el vehículo se ha sometido al protocolo de pruebas del Test [EUROCYBCAR](https://eurocybcar.com/) y lo ha superado -es APTO- se le concede un certificado de ciberseguridad y se le otorga un “sello” con una nota que va del tres al cinco. Cuanto más alta resulte, significará que el coche analizado dispone de un mayor nivel de protección; es decir, que “será una garantía de que protege los datos y privacidad del usuario así como la vida de quienes viajan a bordo”.

Para [Azucena Hernández](https://www.linkedin.com/in/azucena-hern%C3%A1ndez-palmero-028207a6/), CEO de [EUROCYBCAR](https://eurocybcar.com/), esta regulación es drástica, pero muy necesaria: “los vehículos son grandes ordenadores con ruedas y deben protegerse, como mínimo, igual que se protege un móvil o un portátil”. La CEO explica que “las consecuencias de que no estén bien ciberprotegidos pueden ser trágicas, no sólo a causa de un ciberataque premeditado, sino por un mal uso del propio usuario: puede producirse por algo tan sencillo como descargar música de una web de Internet en un pendrive, conectar ese pendrive al puerto USB de nuestro coche y que al hacerlo estemos introduciendo en realidad, y de forma inadvertida, un virus o un ‘malware’ que bloquee el sistema operativo del vehículo, provocando que el coche se pare por completo mientras circula, con el riesgo que eso podría conllevar”.

**Puedes descargar el informe que ha elaborado EUROCYBCAR con todos los detalles de la normativa ONU / UNECE WP.29 en este enlace:** <https://eurocybcar.com/informes/unece-certificado-ciberseguridad/>