EUROCYBCAR®
CYBERSECURITY TEST

NUEVA NORMATIVA
DE SEGURIDAD UNECE/R155

LOS VEHÍCULOS DEBERÁN TENER UN CERTIFICADO DE CIBERSEGURIDAD

- Entró en vigor el 22 de enero de 2021
- Afecta a coches, autobuses, camiones, autocaravanas y remolques
- Multas económicas por unidad para los modelos que no cumplan la normativa

EUROCYBCAR®
CYBERSECURITY TEST

ÍNDICE

Nota: Este informe está basado en la normativa aprobada el 23 de junio de 2020 por la ONU: ECE/TRANS/WP29/2020/79

Diseño y edición: Grupo CYBENTIA

EUROCYBCAR®
CYBERSECURITY TEST

POR QUÉ ES NECESARIO CREAR UN REGLAMENTO DE CIBERSEGURIDAD PARA VEHÍCULOS

EN VIGOR DESDE EL 22 DE ENERO DE 2021

DURANTE LOS ÚLTIMOS AÑOS los vehículos se han ido haciendo más complejos desde el punto de vista tecnológico. De hecho, se calcula que el software que equipa un coche moderno de gama media se compone de unos 100 millones de líneas de código. Eso significa que los sistemas informáticos que equipa un automóvil actual son más complejos que los de un caza de combate F35 -con 24 millones de líneas de código-, que el sistema operativo Windows Vista -50 millones- o, incluso, que todo el software que emplea Facebook -62 millones- .

Esa 'informatización' de los vehículos ha posibilitado que equipen tecnologías que permiten conectarlos con otros dispositivos. Por ejemplo, con un smartphone -a través del Bluetooth, de un cable USB o de una aplicación móvil-, o a Internet -a través de un punto Wifi instalado en el interior del propio coche-. Todo esto ha dado paso al concepto de 'coche conectado', que la Sociedad de Tecnología Vehicular -VTS, por sus siglas en inglés- define como aquel que equipa aplicaciones, servicios y tecnologías que lo conectan con su entorno.

Pero esa creciente complejidad tecnológica de los automóviles ha hecho que los vehículos empiecen a sufrir ciberataques. Según datos de EUROCYBCAR, desde el año 2012 se han documentado ataques a modelos de más de 50 marcas en todo el mundo, que comprometieron la privacidad de las personas que viajaban a bordo de esos vehículos e, incluso, supusieron un peligro para su vida.

Uno de los casos más divulgados fue la demostración 'en vivo' que le hicieron los hackers Charlie Miller y Chris Valasek a un periodista estadounidense en 2015. En concreto, le invitaron a conducir un Jeep Cherokee y, mientras el reportero circulaba, Miller y Valasek se quedaron en la casa del primero para, desde la distancia, manipular el aire acondicionado, los limpiaparabrisas y el equipo de audio. También lograron interferir en elementos implicados en el movimiento del coche, como los frenos, la transmisión y el motor.

Según EUROCYBCAR, desde 2012 se han documentado más de 450 ciberataques que afectan a modelos de 50 marcas diferentes

■ ALGUNAS DE LAS TECNOLOGÍAS QUE EQUIPAN LOS VEHÍCULOS... -y lo que podrían hacer los ciberdelincuentes con ellas- son:

- **Bluetooth**: chantajearte, suplantar tu identidad o acosarte.
- **Llamada de emergencia E-Call**: impedir que te asistan en un accidente.
- **Airbags**: activarlo o desactivarlo a distancia.
- **Llave inteligente**: robarte el coche o "encerrarte" dentro de él.
- **WiFi**: espiarte, chantajearte o suplantar tu identidad.
- **GPS**: con el objetivo de secuestrarte, espiarte o chantajearte.
- **Radio-RDS**: dar información falsa.

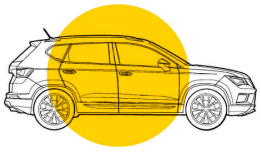
Y, en el futuro, esta tendencia irá a más.

Se prevé que para el año 2023 circulen por el mundo 775 millones de coches conectados . Los vehículos autónomos, que equipan un software más complejo, también van a ir en aumento: se estima que en 2026 **circularán** 50 millones de automóviles sin conductor.
Hasta ahora, los diversos gobiernos y organismos reguladores de todo el mundo habían creado normativas que garantizasen la seguridad física de los vehículos y sus pasajeros, pero la ciberseguridad había quedado fuera de esos marcos reguladores.

Pasado

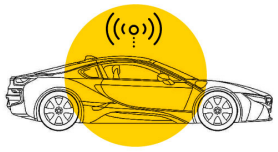
- Conectividad básica
- Unidad principal y telefonía analógica
- 20-30 ECUs
  < 10M LOCs
- Electrónica esencial
- Unidad principal, aire acondicionado, llave con mando a distancia, elevalunas

Presente



- Vehículo conectado con red móvil
- Unidad principal avanzada / Cuadro digital / Wi-fi, Bluetooth, GPS y TPMS
- 50-80 ECUs
  < 100M LOC
- Seguridad activa - amplia variedad de sistemas de seguridad

Futuro



- Vehículo completamente autónomo
- Siempre conectado - 5G
- Gran cantidad de sensores
- > 100 ECUs
  100M - 200M LOCs
- Todos los sistemas del vehículo operados por software

LOC: Lines of Code (Líneas de código) **100M:** Millones **ECU:** Electronic Control Unit (Unidad de control electrónica)

---

https://www.informationisbeautiful.net/visualizations/million-lines-of-code/
https://site.ieee.org/connected-vehicles/ieee-connected-vechicles/connected-vehicles/
Fuente EUROCYBCAR: están registrados, analizados y documentados más de 400 ataques a modelos de 43 marcas diferentes. Se confirma que, desde el año 2012 hasta el primer trimestre de 2020, los ciberataques contra vehículos e infraestructuras relacionadas con los coches han aumentado un 1.600%. Todo parece apuntar que el número real de casos es muy superior; el problema es que, debido al desconocimiento de este tipo de fallos de ciberseguridad entre la población, seguramente hay mucha gente que ha sufrido un ciberataque, pero no lo han considerado un crackeo al no tener evidencias que así lo demostrasen.

QUÉ REQUISITOS DEBE CUMPLIR UN VEHÍCULO PARA VENDERSE EN LA UNIÓN EUROPEA

PARA QUE LOS COCHES SE PUEDAN COMERCIALIZAR en Europa, la Unión Europea exige a los fabricantes que sus modelos cumplan determinados requisitos de homologación, sobre todo, en lo que se refiere a su seguridad. Desde el año 2000 hasta el día de hoy, la Unión Europea ha hecho obligatorios en el equipamiento de los coches los siguientes sistemas de seguridad:

PRINCIPALES NORMATIVAS DE SEGURIDAD EN VEHÍCULOS GENERADAS POR LA UE DESDE EL 2000

MAR 2001	Nuevas condiciones de sistemas de frenado.
ABR 2003	Accionamiento eléctrico en ventanas, techo y mamparas.
JUL 2003	Seguridad en el acristalamiento.
OCT 2003	Medidas de colisión frontal.
OCT 2003	Medidas de colisión lateral.
JUL 2004	ABS obligatorio en los vehículos nuevos.
ENE 2010	Dispositivos de visión indirecta.
MAR 2010	Protección trasera contra empotramiento.
MAR 2010	Protección en depósitos de carburante por peligro de incendio
FEB 2011	Sistema de asistencia a la frenada BAS.
DIC 2012	Protección a peatones.
NOV 2014	Obligatoriedad del ESP en los vehículos nuevos.
MAR 2018	Obligatoriedad del eCall en los vehículos de nueva homologación.
NOV 2019	Obligatoriedad de tecnologías de seguridad vial a partir de 2022.

JUNIO 2020 - OBLIGATORIEDAD DE UN CERTIFICADO DE CIBERSEGURIDAD PARA LOS VEHÍCULOS. ENTRADA EN VIGOR: 22 DE ENERO DE 2021

Fuentes (del gráfico): Noticias coches. http://www.noticias.coches.com - Dirección General de Tráfico. Disponible en: http://revista.dgt.es/es/reportajes/2018/04ABRIL/0404ecall-obligatorio-a-partir-del-31-de-marzo.shtml#.X4ATvmgzbIU

LAS NORMATIVAS QUE LA UNIÓN EUROPEA TOMA DE NACIONES UNIDAS

Y la próxima normativa que la UE implementará es la UNECE/R155

Además de generar normativas propias, la Unión Europea debe adherirse a las normativas que aprueba el Foro Mundial de UNECE para la Armonización de las Regulaciones de Vehículos -conocido como UNECE WP29-.

La Comisión Económica de las Naciones Unidas para Europa, o en inglés United Nations Economic Commission for Europe -UNECE-, fue creada en 1947 como una "comisión regional" de las Naciones Unidas, en la cual están incluidos 56 países miembros de Europa, Norteamérica y Asia .

Con sede en Ginebra, la UNECE tiene como propósito principal promover la integración económica y la cooperación entre los países miembros, así como promover el desarrollo sostenible y la prosperidad económica.

UNECE también establece normas, estándares y convenciones para facilitar la cooperación internacional tanto dentro como fuera de la región y, por ello, numerosos países fuera de la región utilizan los mismos estándares y normativa de la UNECE.

Dentro de UNECE existe el citado Foro Mundial para la Armonización de las Regulaciones de Vehículos -WP29-. UNECE WP29 tiene el objetivo de crear, actualizar y mantener las regulaciones de los vehículos relacionadas con su tecnología, su seguridad y su protección del medio ambiente. Este es el sistema internacional de regulación de vehículos más grande del mundo, porque 54 de sus países miembros -todos, salvo Estados Unidos y Canadá- tienen firmado un acuerdo desde 1958 por el cual se comprometen a reconocer y a aplicar dentro de sus fronteras las normativas aprobadas por UNECE WP29.

ALGUNAS DE LAS NORMATIVAS QUE LA UNIÓN EUROPEA HA ADOPTADO DE UNECE WP29 SON:

- **Reglamento nº 151.** - Disposiciones uniformes relativas a la homologación de vehículos de motor con respecto al sistema de información de puntos ciegos para la detección de bicicletas .
- **Reglamento nº 44.** - Disposiciones uniformes relativas a la homologación de dispositivos de retención para niños ocupantes de vehículos de motor -Sistemas de retención infantil- .

A ESTOS REGLAMENTOS HAY QUE SUMAR, PRÓXIMAMENTE, UNO MÁS: EL WP29/2020/79

Esta nueva normativa obligará a que los coches que se comercialicen en el espacio de la UE tengan un certificado de ciberseguridad.

Consciente de los riesgos de ciberseguridad de los vehículos, UNECE WP29 aprobó, el 23 de junio de 2020, el reglamento ECE/TRANS/WP29/2020/79. Esta normativa exigirá que los vehículos cuenten con un certificado que acredite que están protegidos frente a ciberataques. Y la Unión Europea, entre otras regiones, hará obligatorio este reglamento en todo su territorio para los vehículos -coches, autobuses, camiones, furgonetas y remolques- de nueva homologación a partir de julio de 2022 y para todos los nuevos a partir del 1 de julio del 2024.

Se trata, por tanto, de una normativa muy ambiciosa para la Unión Europea, que cerrará el mercado a vehículos que no sean ciberseguros mucho antes, incluso, que aquellos con motores de combustión. Y es que lo máximo que, por el momento, propone la UE en materia de contaminación es multar a los fabricantes cuya media de emisiones de los vehículos que vendan exceda los 95 gramos de CO2 por kilómetro.

Los países miembros de UNECE son Albania, Alemania, Andorra, Armenia, Austria, Azerbaiyán, Bielorrusia, Bélgica, Bosnia y Herzegovina, Bulgaria, Canadá, Croacia, República Checa, Chipre, Dinamarca, Eslovaquia, Eslovenia, España, Estados Unidos, Estonia, Finlandia, Francia, Georgia, Grecia, Hungría, Islandia, Irlanda, Israel, Italia, Kazajistán, Kirguistán, Letonia, Liechtenstein, Lituania, Luxemburgo, Macedonia del Norte, Malta, Moldavia, Mónaco, Montenegro, Noruega, Países Bajos, Polonia, Portugal, Reino Unido, Rumanía, Rusia, San Marino, Serbia, Suecia, Suiza, Tayikistán, Turquía, Turkmenistán, Ucrania y Uzbekistán.

Texto completo disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:42020X1596&from=EN

La Unión Europea está formada por los siguientes países: Alemania, Austria, Bélgica, Bulgaria, Chipre, Croacia, Dinamarca, Eslovenia, España, Estonia, Finlandia, Francia, Grecia, Hungría, Irlanda, Italia, Letonia, Lituania, Luxemburgo, Malta, Países Bajos, Polonia, Portugal, República Checa, República Eslovaca, Rumanía y Suecia.

INICIATIVAS PREVIAS A LA NORMATIVA UNECE/R155
EN ESPAÑA, EN EUROPA Y EN EL MUNDO

A ESTOS REGLAMENTOS -151 Y 44- SE HA SUMADO UNO MÁS: EL UNECE/R155... PERO, ¿QUÉ ANTECEDENTES HAY PREVIOS A ESTE NUEVA NORMATIVA?

Los documentos previos a la llegada de la normativa UNECE/R155 eran simplemente recomendaciones, no normas vinculantes. Llama la atención que no es hasta el 2016 -aunque un medio de comunicación español alertó en el año 2013 que los vehículos que circulaban por las carreteras podrían no estar suficientemente ciberprotegidos, lo que facilitaría un ciberataque- cuando empiezan a surgir esas primeras recomendaciones de ciberseguridad aplicadas a los automóviles. Es llamativo porque hay registrados ciberataques a vehículos desde el año 2012 -ver introducción-. Una hipótesis podría ser que en 2015 tuvo lugar el ya citado hackeo de Charlie Miller y Chris Valasek a un Jeep Cherokee, el más 'popular' de los que se han producido sobre un vehículo . Lo mediático del suceso pudo haber hecho crecer la preocupación institucional con respecto a las vulnerabilidades de ciberseguridad de los vehículos.

Con esos antecedentes -ver gráfico de siguiente página-, la ONU inició el proceso de desarrollo de una norma que unificase los criterios y los requisitos, y que implante las bases mínimas de ciberseguridad para todos los vehículos. Todo esto se ha traducido en un reglamento en el que han trabajado expertos de todo el mundo y cuyos detalles se explicarán más adelante en este informe.

ISO/SAE 21434, UN VISTAZO A LO QUE VENDRÁ

De forma paralela a la norma aprobada por la ONU/UNECE WP29, la Organización Internacional de Normalización (ISO) y la Sociedad de Ingenieros Automotrices (SAE Internacional) están desarrollando actualmente un texto que busca implementar la ciberseguridad en los vehículos durante todo su ciclo de vida. Se trata del estándar ISO/SAE 21434.

Este documento es similar a la norma de la UNECE/R155 porque especifica unos requisitos para gestionar los riesgos de ciberseguridad durante todo el ciclo de vida de los vehículos, desde sus primeras fases de su diseño hasta su desguace. LA ISO/SAE 21434 también define un lenguaje común para comunicar y gestionar el riesgo de ciberseguridad.

Ambos textos son compatibles, y presentan aspectos comunes, de forma que cumplir con uno hace sencillo cumplir con el otro. La diferencia fundamental entre el texto de la ONU y el de ISO/SAE radica en que mientras que el primero es vinculante para los países miembros de UNECE, el texto de ISO/SAE es un estándar que no es de obligado cumplimiento.

El estándar ISO/SAE 21434 aún está en fase de desarrollo. La última versión es un borrador no aprobado que aún está sujeto a cambios.

La ISO/SAE 21434 también define un lenguaje común para comunicar y gestionar el riesgo de ciberseguridad

El texto completo disponible en https://www.sae.org/standards/content/j3061_201601/
El texto completo disponible en https://www.ic3.gov/Media/Y2016/PSA160317
El texto completo está disponible en https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf
El texto completo está disponible en https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars
El texto completo está disponible en https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles/the-key-principles-of-vehicle-cyber-security-for-connected-and-automated-vehicles y en https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/661135/cyber-security-connected-automated-vehicles-key-principles.pdf
El texto completo está disponible en https://shop.bsigroup.com/ProductDetail/?pid=000000000030365446&_ga=2.267667464.704902458.1545217114-2008390051.1545217114 Caso publicado en Wired. Disponible en https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

EUROCYBCAR®
CYBERSECURITY TEST

INICIATIVAS PREVIAS A LA NORMATIVA UNECE/R155

2013

OCTUBRE

"Una revista española publica un reportaje sobre los riesgos de ciberseguridad en los coches"

"Un hacker podría matarte mientras conduces". Así titula la revista Autofácil - creada y dirigida por Azucena Hernández- el reportaje publicado en el número 156, en el que alerta sobre los riesgos de ciberseguridad que afectan a los sistemas electrónicos de los vehículos. Afirma que algunas vulnerabilidades podrían poner en peligro la vida de los pasajeros si un ciberdelincuente se aprovecha de ellas.

2016

ENERO

"Guía de ciberseguridad para sistemas de vehículos ciberfísicos J3061_201601"[9]

Elaborada por la SAE. En ella se dan unas recomendaciones prácticas que proporcionan orientación sobre cómo establecer un alto nivel de ciberseguridad en los sistemas de los vehículos. Este texto se convertirá en el estándar ISO/SAE 21434, que aún está en fase de desarrollo y cuya última versión es un borrador no aprobado que aún está sujeto a cambios.

MARZO

"Los vehículos motorizados, cada vez más vulnerables a los ciberataques"[10]

El FBI emite un comunicado en el que avisa de que la creciente conectividad de los vehículos conlleva amenazas a la ciberseguridad. El texto pone algunos ejemplos de ciberataques que se podrían llevar a cabo sobre automóviles.

OCTUBRE

"Las mejores prácticas de ciberseguridad para vehículos modernos"

Elaborada por la NHTSA. Es una guía no vinculante para mejorar la ciberseguridad de los vehículos a motor.

2017

ENERO

"Ciberseguridad y resiliencia de automóviles inteligentes"

Elaborado por ENISA. El objetivo de este estudio es identificar buenas prácticas que garanticen la seguridad de los coches inteligentes frente a las ciberamenazas. El estudio enumera los activos sensibles presentes en los automóviles inteligentes, así como las correspondientes amenazas, riesgos, factores de mitigación y posibles medidas de seguridad a implementar.

JULIO

"El equipo fundador de EUROCYBCAR realiza el primer test de ciberseguridad a un vehículo"

Durante tres meses un equipo compuesto por hackers, ingenieros y probadores de coches realizaron las primera prueba de ciberseguridad a un vehículo fabricado en España para comprobar el nivel de ciberseguridad que ofrece un vehículo. El resultado reveló que la ciberseguridad era el gran olvidado de las marcas de coches, a pesar de que afecta a la vida de las personas.

AGOSTO

"Los principios clave de la ciberseguridad del vehículo para vehículos conectados y automatizados"

Elaborada por el Gobierno Británico. Es una guía que resume los 8 principios para la obtención de una buena ciberseguridad en el sector de la automoción.

2018

JULIO

"El Centro Vasco de Ciberseguridad crea el primer grupo de trabajo sobre ciberseguridad y automoción"

Tras la inauguración del Centro Vasco de Ciberseguridad –BCSC-, que dirige Javier Diéguez, se promueve la creación de un grupo de trabajo compuesto por los Centros de Investigación Tecnalia, Vicomtech e Ikerland, el BCSC y los fundadores de EUROCYBCAR.

2018

OCTUBRE

"En el evento internacional 12ENISE se descubre la importancia de la ciberseguridad para la movilidad"

Durante el 12ENISE -Encuentro Internacional de Seguridad de la Información que organiza el Instituto de Ciberseguridad de España (INCIBE)-, por primera vez, se habla de las amenazas y vulnerabilidades de ciberseguridad que deben considerarse en el automóvil. La ponencia la imparte Azucena Hernández, actual CEO de EUROCYBCAR.

DICIEMBRE

"PAS 1885:2018" [14]

Elaborada por el Grupo BSI (que está designado por el Gobierno del Reino Unido como el organismo nacional de normalización): Establece principios fundamentales sobre cómo proporcionar y mantener ciberseguridad en relación con la reducción de amenazas y daños a productos, servicios y sistemas dentro de ecosistemas de transporte inteligente cada vez más conectados y colaborativos.

2019

MARZO

"Nace el primer medio de investigación y concienciación de motor y ciberseguridad del mundo"

El medio de comunicación HackerCar, dirigido por Javier García, consigue que periodistas, probadores de coches y hackers trabajen en equipo para testar los coches de una forma nunca vista.

JULIO

"EUROCYBCAR realiza la segunda evaluación técnica de ciberseguridad a un vehículo"

En su laboratorio de Vitoria-Gasteiz, EUROCYBCAR somete a un vehículo fabricado en España al Test EUROCYBCAR: el único test en el mundo que mide el nivel de ciberseguridad de un coche basándose en dos parámetros: de qué forma protege la vida y la privacidad de las personas que viajan a bordo.

2019

NOVIEMBRE

"La ciberseguridad aplicada a la automoción"

El Real Instituto de Elcano publica un artículo de investigación, firmado por Ana Ayerbe –Tecnalia-, en el que se analizan los riesgos de ciberseguridad en los automóviles, las formas de enfrentarse a ellos y qué iniciativas existen en el mundo, citando a EUROCYBCAR, como la única empresa en España que mide la ciberseguridad de los vehículos.

DICIEMBRE

"Por primera vez en el mundo, una institución somete a un vehículo de su flota a un test de ciberseguridad"

El Gobierno Vasco somete a uno de los vehículos de su Parque Móvil al Test EUROCYBCAR para conocer las cibervulnerabilidades a las que se exponen las autoridades que viajan a bordo de dichos vehículos.

2020

Reglamento ECE/TRANS/WP29 /2020/79

Normativa desarrollada por la UNECE WP29 que exigirá que los vehículos cuenten con un certificado de ciberseguridad que acredite que están protegidos frente a ciberataques para poder homologarse.

El texto completo disponible en https://www.autofacil.es/usuario/2013/11/17/hacker-matarte-conduces/16435.html
Grabación de la conferencia disponible en https://www.youtube.com/watch?v=oFi8QxdK_AQ&t=3s
https://hackercar.com/
Los vídeos de sus conferencias se pueden visionar en https://www.youtube.com/watch?v=nu3mHMuXlOw
El texto completo disponible en http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ciberseguridad/ari105-2019-ayerbe-ciberseguridad-aplicada-a-la-automocion

EUROCYBCAR®
CYBERSECURITY TEST

TODO SOBRE LA NORMATIVA UNECE/R155

LA NORMA QUE REGULA LA CIBERSEGURIDAD DE LOS VEHÍCULOS

QUÉ DICE EL REGLAMENTO UNECE/R155

El 23 de junio de 2020, se aprobó esta norma que regula la ciberseguridad de los vehículos. La norma en cuestión es la ECE/TRANS/WP29/2020/79 y se titula "Reglamento de las Naciones Unidas sobre disposiciones uniformes relativas a la homologación de vehículos a motor en lo que respecta a la ciberseguridad y el sistema de gestión de cíber-seguridad".

FASES DE DESARROLLO DE LA NORMA

2018

Septiembre

Comienza la discusión sobre los riesgos de la ciberseguridad que presentan los vehículos.

2019

Junio-agosto

Fase de pruebas con autoridades y fabricantes voluntarios para comprobar la solidez y preparar el borrador.

Septiembre

Decisión de GRVA (Grupo de trabajo sobre vehículos automatizados / autónomos y conectados) sobre el contenido de regulación.

2020

Marzo

Publicación del borrador final.

23 de junio

Aprobación del reglamento final.

2021

Enero 2021

Entrada en vigor. El reglamento estará disponible para su aplicación en los Estados miembros de UNECE. La Unión Europea, Corea del Sur y Japón ya han confirmado que lo aplicarán en sus territorios, como se detallará más adelante.

En inglés, UN Regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system. Texto íntegro está disponible a través del siguiente enlace: http://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf

TRATA SOBRE MEDIDAS UNIFORMES NECESARIAS para crear un sistema de gestión de ciberseguridad en los vehículos. Es decir, un sistema que trate el riesgo asociado con las amenazas y que protege los vehículos de ataques cibernéticos.

EL ÍNDICE DEL DOCUMENTO DEL REGLAMENTO UNECE/R155

1. Ámbito de aplicación: a qué vehículos afecta la norma.
2. Definiciones de algunos términos empleados a lo largo del reglamento.
3. Solicitud de homologación: documentación a presentar para lograr la aprobación.
4. Marca de homologación: símbolo que deberán incluir los vehículos que cumplan el reglamento en su placa de identificación.
5. Homologación: papel de la entidad verificadora del cumplimiento del reglamento.
6. Certificado de conformidad del CSMS.
7. Especificaciones: detalle de las exigencias que el reglamento hará cumplir.
8. Modificación del tipo de vehículo y extensión de la homologación de tipo: cómo efectuar modificaciones en los vehículos
9. Conformidad de la producción.
10. Sanciones por falta de conformidad de la producción.
11. Cese definitivo de la producción:
cómo comunicar que un vehículo cesa su producción.
12. Nombres y direcciones de los servicios técnicos responsables de realizar los ensayos de homologación.

ANEXOS
1 Ficha técnica.
2 Comunicación.
3 Disposición de la marca de homologación.
4 Modelo del certificado de conformidad.
Lista de amenazas y sus medidas de mitigación.
5 Lista de amenazas a evitar y sus correspondientes modificaciones.

ESTE REGLAMENTO PROPORCIONA UN MARCO PARA QUE EL SECTOR AUTOMOTRIZ ESTABLEZCA LOS PROCESOS NECESARIOS PARA:

- Identificar y gestionar los riesgos de ciberseguridad en el diseño de vehículos.
- Verificar que se gestionen los riesgos, incluidas las pruebas.
- Asegurar que las evaluaciones de riesgos se mantengan actualizadas.
- Monitorizar los ciberataques y que se responda efectivamente a ellos.
- Analizar los ataques exitosos o intentados.
- Evaluar si las medidas de ciberseguridad siguen siendo efectivas a la luz de las nuevas amenazas y vulnerabilidades

EL CSMS DEBERÁ PROTEGER A LOS VEHÍCULOS CONTRA 70 AMENAZAS DE CIBERSEGURIDAD ESPECÍFICAS, SEGÚN LA NORMATIVA UNECE/R155

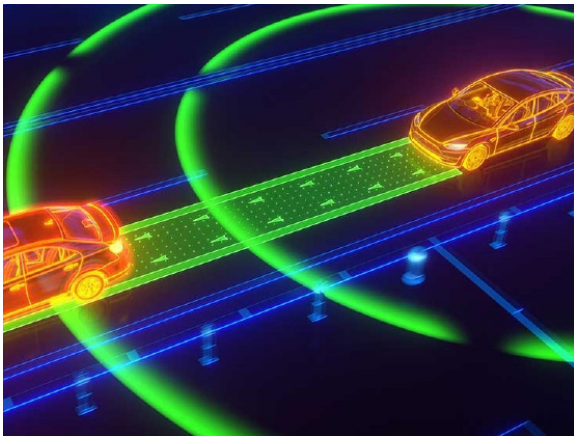
PARA CUMPLIR CON LA NORMATIVA, LOS FABRICANTES TENDRÁN QUE CREAR PARA SUS VEHÍCULOS UN SISTEMA DE GESTIÓN DE CIBERSEGURIDAD -CSMS, POR SUS SIGLAS EN INGLÉS-.

El CSMS es un sistema de procesos que, en conjunto, deben garantizar la ciberseguridad del vehículo de forma adecuada frente a diferentes ciberataques.

Un CSMS que cumpla con los requisitos marcados por la ONU significará que ese fabricante gestiona la ciberseguridad de sus modelos a lo largo de todo su ciclo de vida: desarrollo, producción y posproducción. Además, cada una de esas fases incluirá protecciones contra sus amenazas de ciberseguridad específicas.

EL CSMS DEBERÁ PROTEGER A LOS VEHÍCULOS CONTRA 70 AMENAZAS DE CIBERSEGURIDAD ESPECÍFICAS QUE LA ONU DETALLA EN SU REGLAMENTO. ESTAS VULNERABILIDADES SE DIVIDEN EN 7 APARTADOS Y SON:

• **AMENAZAS RELACIONADAS CON LOS SERVIDORES BACK-END.** Estos servidores son los hacen que todo el sistema informático de los vehículos o las redes informáticas internas del fabricante funcionen. Se deberán evitar, entre otras amenazas, pérdidas de información en la nube, filtraciones de información por compartir datos de forma involuntaria y que un trabajador haga un uso ilícito de los datos a los que tiene acceso.



• **AMENAZAS RELACIONADAS CON LOS CANALES DE COMUNICACIÓN QUE USA EL VEHÍCULO PARA CONECTARSE CON SU ENTORNO** -por ejemplo, otros vehículos o la infraestructura-. Se deberán evitar, entre otras amenazas, que se pueda suplantar la identidad de otros vehículos, inyectar malware -programas que dañan los sistemas informáticos- por los canales de comunicación y manipular o eliminar los datos y códigos del software del vehículo.

• **AMENAZAS A LAS CONEXIONES Y CONECTIVIDAD EXTERNA.** Se deberán evitar, entre otras amenazas, la manipulación de funciones remotas, como la llave, el inmovilizador y la batería; manipular las conexiones telemáticas del vehículo, como la medición de la temperatura de la mercancía en vehículos industriales o desbloquear las puertas de forma remota; y causar interferencias en los sistemas inalámbricos de corto alcance o sensores.

• **AMENAZAS A LOS DATOS/CÓDIGO DEL VEHÍCULO.** Se deberán evitar, entre otras amenazas, que se pueda acceder sin deber a la información privada del propietario -quién es, su cuenta bancaria, ubicación, identificación electrónica del vehículo- y falsificar la identidad o manipular datos del vehículo -kilometraje, velocidad de conducción, enviar mensajes falsos e indicaciones al conductor, etc.-.

• **AMENAZAS RELACIONADAS CON LOS PROCEDIMIENTOS DE ACTUALIZACIÓN DE LOS VEHÍCULOS.** Se deberá de evitar cualquier tipo de amenaza que afecte a los procesos de actualización de los sistemas informáticos de los vehículos, ya sea que se lleven a cabo de forma inalámbrica -Over The Air- o mediante una descarga.

• **AMENAZAS RELACIONADAS CON ACCIONES HUMANAS NO INTENCIONADAS.** Se deberán de evitar, entre otras amenazas, que alguien con acceso al vehículo -como el propietario o un mecánico- pueda introducirle un virus de forma involuntaria si lo engaña un ciberdelincuente.

• **POSIBLES AMENAZAS QUE PODRÍAN EXPLOTARSE SI NO SE PROTEGEN O REFUERZAN LO SUFICIENTE.** Se deberán de evitar, entre otras amenazas, fallos de software, que la información del primer propietario del vehículo pase al segundo dueño -en caso de venderse en el mercado de ocasión-, o que se reemplacen elementos del vehículo que cumplan con la norma por otros que la incumplan.

LA RESPONSABILIDAD DE CUMPLIR CON EL CSMS SERÁ DE LOS OEM -FABRICANTES-. Además, también deberán comprobar que todos los proveedores de su cadena de suministro identifican y gestionan los riesgos de ciberseguridad del componente que proporcionan. Por tanto, los proveedores no están directamente obligados a cumplir con los requisitos de la UNECE/R155 pero no hacerlo les perjudicará a la hora de ser competitivos y no serán rentables.

Si bien la normativa de ONU/UNECE WP29 establece un marco regulatorio y unos requisitos mínimos para los fabricantes a lo largo de la cadena de valor, el texto no incluye una guía de implementación detallada para traducir los requisitos en métodos concretos que eviten los ciberataques. Es decir, a los fabricantes se les proporciona un listado con los riesgos que deben evitar en sus modelos a lo largo de todo el ciclo de vida del vehículo, pero, por el momento, deben de ser ellos quienes piensen cómo darles solución, aunque el certificado deberá emitirlo una entidad externa.

CÓMO OBTENER EL CERTIFICADO DE CIBERSEGURIDAD

UNA ENTIDAD TÉCNICA EXTERNA AL FABRICANTE SERÁ LA QUE ACREDITE QUE EL VEHÍCULO CUMPLE CON LOS REQUISITOS MARCADOS POR LA ONU/UNECE

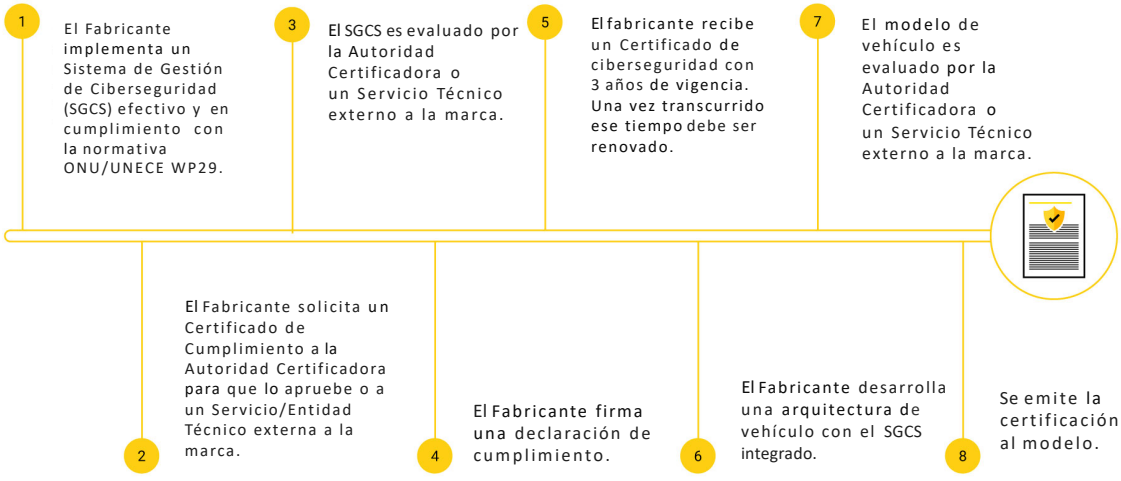
Para que un modelo de vehículo obtenga el certificado de ciberseguridad que acredite que cumple con los requisitos establecidos por la ONU, los fabricantes deberán someterlo a unas evaluaciones. Hasta ahora, los OEMs contrataban a empresas de consultoras de ciberseguridad para auditar de forma puntual algunos de los sistemas de sus vehículos, pero, con la entrada en vigor de la nueva normativa **tendrán la obligación de contratar un servicio técnico externo que certifique que su vehículo es ciberseguro.**

Deberán presentar documentación suficiente para poder evaluar el funcionamiento del CSMS. Entonces, una Entidad Autorizada analizará esos documentos y realizará pruebas al vehículo. Todo este proceso tiene el objetivo de poder certificar que el fabricante ha tomado las medidas mínimas necesarias para garantizar que el tipo de vehículo y su CSMS son ciberseguros, mediante la evaluación de la documentación presentada y la realización de pruebas al tipo de vehículo.

LA ENTIDAD AUTORIZADA O SERVICIOS TÉCNICO que lleve a cabo la evaluación del fabricante, debe asegurar que cumple con los requisitos expuestos en Apéndice 2 del "Acuerdo con respecto a la adopción de reglamentos técnicos armonizados de las Naciones Unidas para vehículos con ruedas, equipos y piezas que pueden montarse y/o utilizarse en vehículos con ruedas y las condiciones para el reconocimiento recíproco de las aprobaciones concedidas sobre la base de este reglamento de las Naciones Unidas" . Algunos de los requisitos que establece el citado acuerdo son que la entidad escogida deberá demostrar que disponen de habilidades apropiadas, conocimientos técnicos específicos y experiencia probada en el campo que cubra cada normativa de la ONU (en el caso del reglamento de ONU/UNECE WP29, ciberseguridad para vehículos), debe de estar libre de cualquier control e influencia de las partes interesadas y debe tener acceso a las instalaciones de prueba y dispositivos de medición necesarios para realizar las pruebas.

Las Entidades Autorizadas deberán ser previamente designadas por los fabricantes para realizar las pruebas de evaluación e inspecciones. Hasta la fecha se desconoce si antes de la entrada en vigor del reglamento, se elaborará algún documento más específico, donde se acuerde una interpretación común de los métodos y criterios de evaluación.

ASÍ ES EL PROCESO DE CERTIFICACIÓN



En inglés: Agreement Concerning the Adoption of Harmonized Technical United Nations Regulations for Wheeled Vehicles, Equipment and Parts which can be Fitted and/or be Used on Wheeled Vehicles and the Conditions for Reciprocal Recognition of Approvals Granted on the Basis of these United Nations Regulations. Disponible en https://www.unece.org/fileadmin/DAM/trans/main/wp29/wp29regs/2017/E-ECE-TRANS-505-Rev.3e.pdf

a= 8 mm min

ESTA ES LA ETIQUETA DE VEHÍCULO CIBERSEGURO

¿EL VEHÍCULO ES APTO O NO APTO?

El servicio técnico o entidad autorizada rechazará la concesión del certificado de cumplimiento con el CSMS del vehículo cuando:

1. No se cumpla con uno o más de los 70 requisitos de ciberseguridad exigidos por el reglamento de ONU/UNECE WP29.

2. En caso de que el fabricante **no proporcione a la Entidad Autorizada la suficiente información** para evaluar la ciberseguridad del tipo de vehículo.

VIGENCIA DE TRES AÑOS. El certificado de conformidad del CSMS **será válido por un máximo de tres años** a partir de la fecha de expedición, a menos que sea retirado. Cuando la validez del certificado esté próxima a finalizar, se deberá solicitar un nuevo certificado de cumplimiento -si ha habido cambios en el reglamento-, o extender la validez del anterior por un período adicional de tres años. Para esto, la Entidad Autorizada designada, deberá evaluar que se los requisitos expuestos en el reglamento se siguen cumpliendo. En el caso de que ya no se cumpla con los requisitos tras la caducidad del certificado, se procederá a la retirada de este.

SERÁ OBLIGATORIO. Además, el fabricante también deberá informar a la Entidad Autorizada de **cualquier cambio que afecte a la relevancia del certificado** de cumplimiento del CSMS, como la aparición de nuevos ciberataques. Tras consultar con el fabricante, la Entidad Autorizada decidirá si es necesario realizar nuevas comprobaciones para saber si se siguen cumpliendo los requisitos exigidos.

LA ETIQUETA DE VEHÍCULO CIBERSEGURO. Aquellos vehículos que reciban el certificado de cumplimiento con el CSMS deberán indicarlo en su ficha de homologación mediante una marca. **Esta marca estará compuesta por:**

• **Una letra "E"** seguida del número distintivo del país que ha concedido la certificación, rodeados ambos por un círculo.

• A la derecha de esa marca se situará **el número del reglamento de la ONU.**

• A ese número lo seguirá **una letra "R", un guion y el número de homologación.**

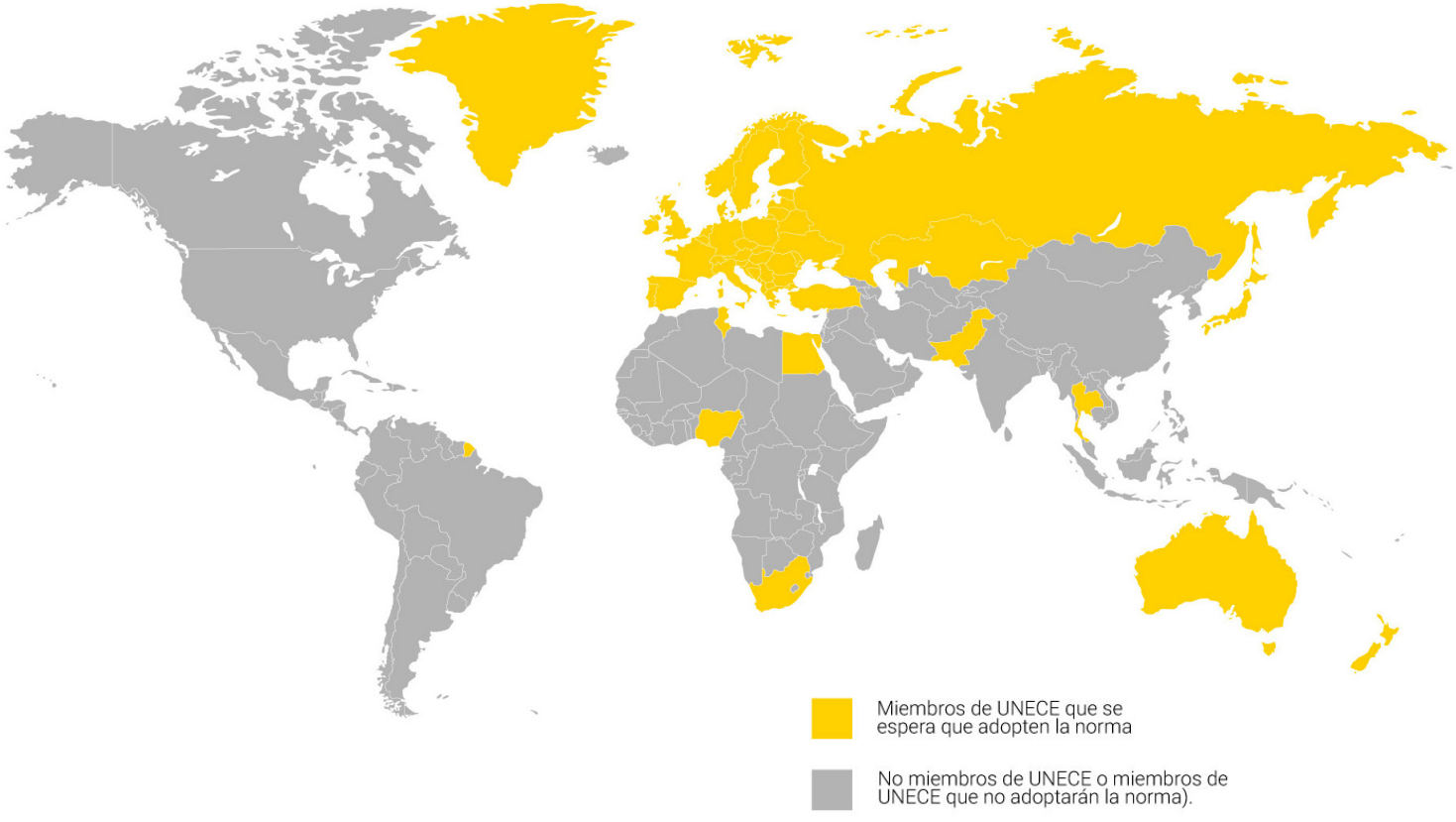
Esta marca deberá situarse de forma visible y fácilmente accesible dentro o cerca de la placa de identificación del vehículo.

La imagen de la parte superior es un ejemplo de marca de homologación para mostrar que un vehículo tiene un CSMS cuyo funcionamiento ha sido certificado según los requisitos de ONU/UNECE WP29. En este ejemplo, **los elementos que componen esta marca de homologación indican lo siguiente:**

• **E4:** Muestra que el CSMS del vehículo ha sido certificado en los Países Bajos -el número varía según el país-.

• **155:** Indica el número del reglamento para el cual el coche ha logrado la certificación.

• **R-001234:** El número de homologación. Los dos primeros dígitos del número de homologación -00- indican que se homologó con los requisitos del reglamento de la ONU en su forma original.



MIEMBROS DE UNECE QUE ADOPTARÁN LA NORMATIVA UNECE/R155 PORQUE FIRMARON ACUERDO DE RECONOCIMIENTO RECÍPROCO DE APROBACIONES

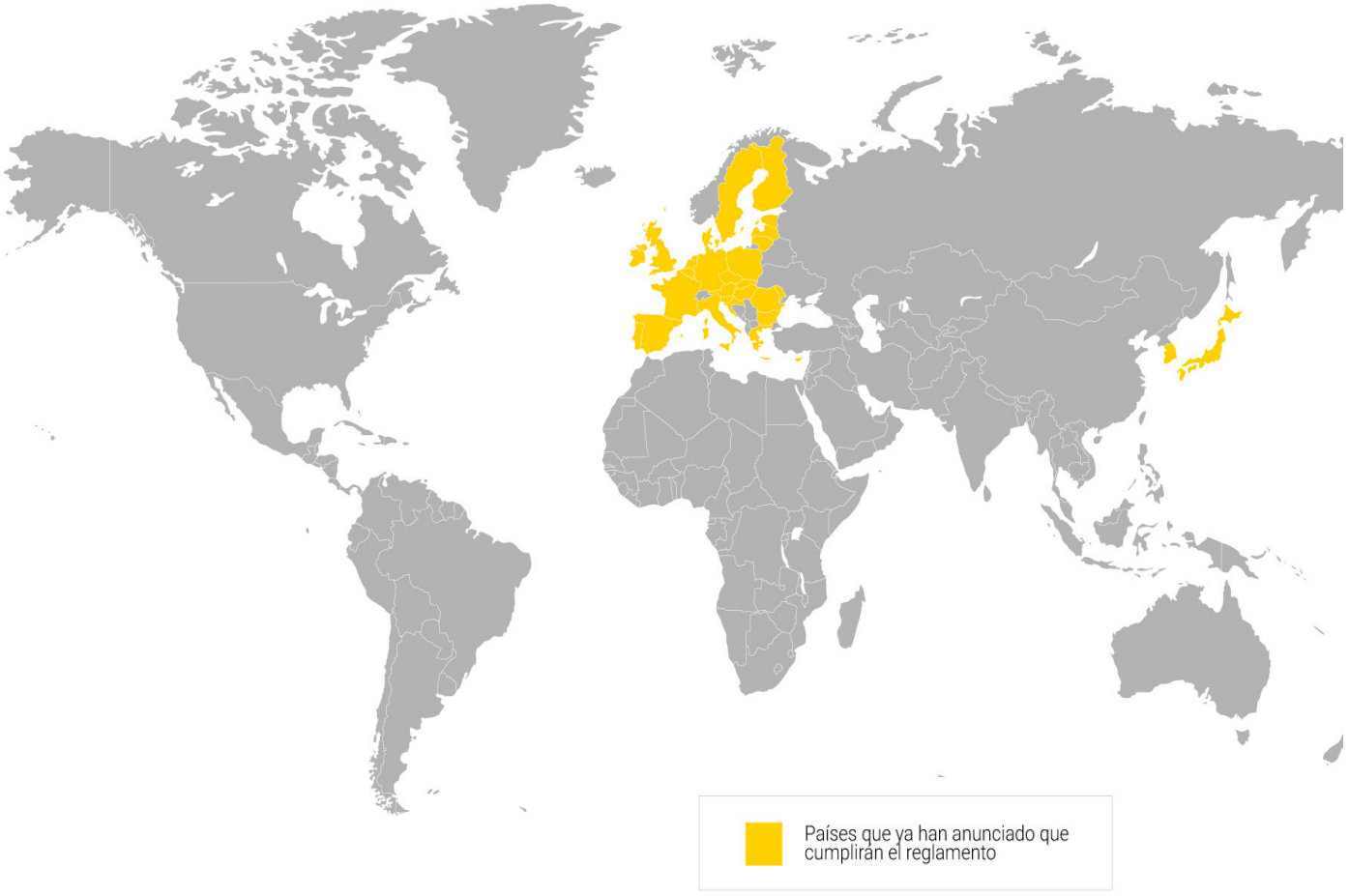
QUÉ PAÍSES APLICARÁN LA NORMA Y EN QUÉ PLAZOS

El texto ya está aprobado y desde el 22 de enero de 2021 entra en vigor. A partir de esa fecha, ya lo han adoptado 54 estados de los 56 estados miembros de UNECE -todos salvo EE.UU. y Canadá-, ya que son ellos los que tienen firmado un acuerdo de reconocimiento recíproco de las regulaciones que este foro apruebe. Esos países son los siguientes:

Los 54 miembros de UNECE que aplicaron la norma desde el 22 de enero 2021

-Albania
-Armenia
-Australia
-Austria
-Azerbayán
-Bielorrusia
-Bélgica
-Bosnia Herzegovina
-Bulgaria
-Croacia
-Rep. Checa
-Dinamarca
-Egipto
-Estonia
-Finlandia
-Francia
-Georgia
-Alemania
-Grecia
-Hungría
-Italia
-Japón
-Kazajistán
-Letonia
-Lituania
-Luxemburgo
-Malasia
-Montenegro
-Países Bajos
-Nueva Zelanda
-Nigeria
-Macedonia
-Noruega
-Pakistán
-Polonia
-Portugal
-Corea del Sur
-República de Moldova
-Rumanía
-Federación Rusa
-San Marino
-Serbia
-Eslovaquia,
-Eslovenia
-Sudáfrica
-España
-Suecia
-Suiza
-Tailandia
-Túnez
-Turquía
-Ucrania
-Reino Unido
-Irlanda del Norte

A la izquierda aparecen los países en los que se va a comenzar a aplicar la norma UNECE/R155 dentro de sus territorios a fecha de 22 de enero de 2021.



PAÍSES QUE YA HAN CONFIRMADO QUE APLICARÁN LA NORMA UNECE/R155 EN SUS TERRITORIOS

Union Europea

Alemania
Austria
Bélgica
Bulgaria
Chipre
Croacia
Dinamarca
Eslovenia
España
Estonia
Finlandia
Francia
Grecia
Hungría
Irlanda
Italia
Letonia
Lituania
Luxemburgo
Malta
Países Bajos
Polonia
Portugal
República Checa
República Eslovaca
Rumanía
Suecia

Asia Pacífico

Japón
Corea del Sur

La Unión Europea ha establecido que todos los vehículos que se homologuen a partir de julio del 2022 deberán cumplirlo. Esa obligación se extenderá a partir del 1 de julio de 2024 a todos los coches nuevos. Por su parte, las autoridades japonesas han trasladado que pretenden exigir a las marcas que vendan vehículos dentro de sus fronteras que cumplan el reglamento desde enero de 2021.
En cuanto a Corea del Sur, ya viene aplicando el reglamento desde el segundo semestre de 2020, aunque, según parece, de forma gradual.

https://www.unece.org/trans/maps/un-transport-agreements-and-conventions-18.html

A QUÉ VEHÍCULOS AFECTARÁ LA NORMATIVA UNECE/R155

EL REGLAMENTO SE APLICARÁ A LAS SIGUIENTES CATEGORÍAS DE VEHÍCULOS

• **CATEGORÍA M.** Vehículos a motor destinados al transporte de personas y que tengan al menos cuatro ruedas, o tres ruedas y un peso máximo superior a 1 tonelada. Por ejemplo, turismos, autobuses y autocaravanas.

• **CATEGORÍA N.** Vehículos a motor destinados al transporte de mercancías y que tengan por lo menos cuatro ruedas, o tres ruedas y un peso máximo superior a 1 tonelada. Por ejemplo, furgonetas y camiones.

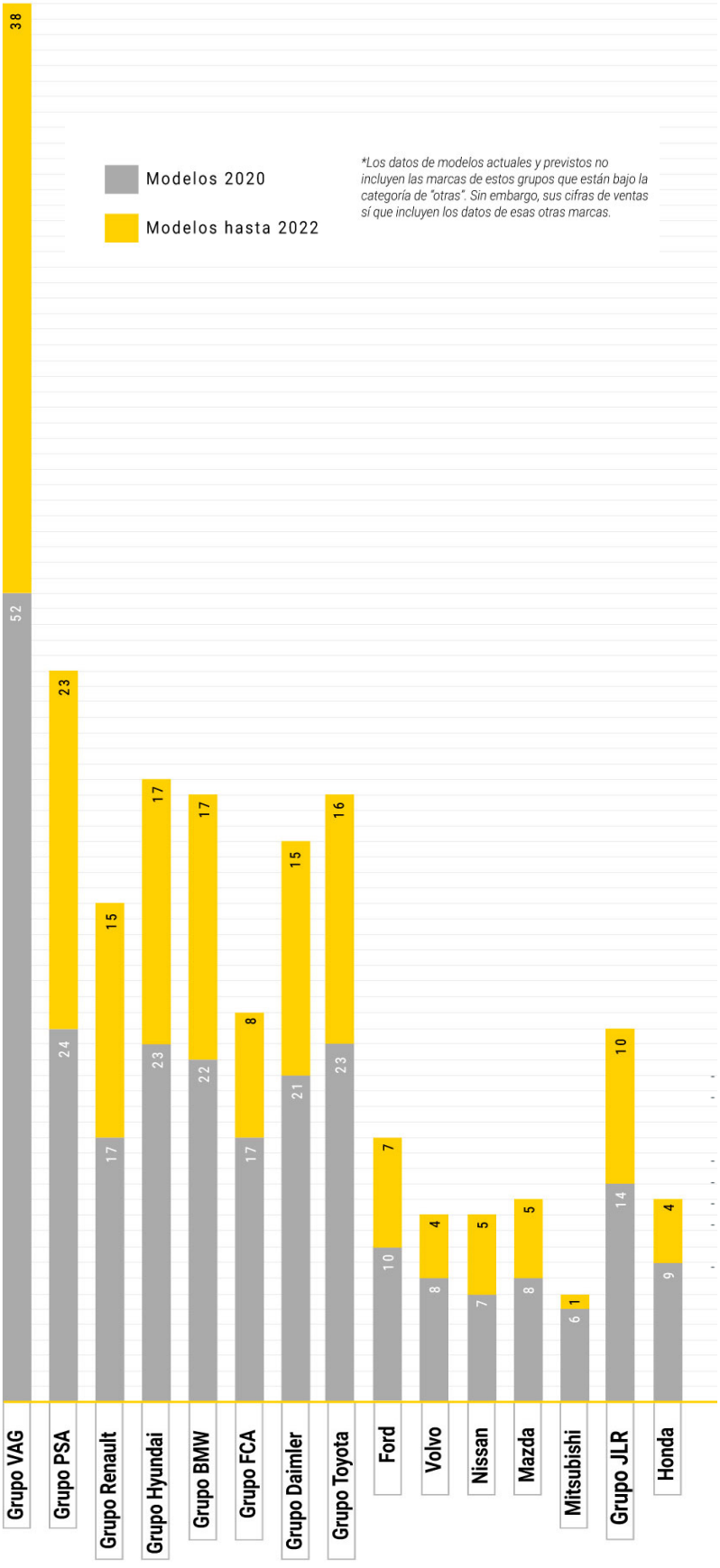
• **CATEGORÍA O.** Remolques y caravanas con una unidad de control electrónico.

• **CATEGORÍAS L6 Y L7.** Cuadriciclos con o sin cabina para el transporte de personas. En este caso, solo les afecta el reglamento si están equipados con funciones de conducción automatizada desde el nivel 3 en adelante.

Por tanto, todos los fabricantes de turismos, furgonetas, camiones y autobuses que quieran homologar nuevos modelos a partir de julio del 2022 o, simplemente, vender vehículos nuevos a partir del 1 de julio del 2024 en los países miembros de la UE deberán cumplir con los requisitos exigidos por la normativa UNECE/R155.

¿A CUÁNTOS VEHÍCULOS AFECTARÁ?

NÚMERO DE MODELOS ACTUALES QUE TIENEN A LA VENTA CADA GRUPO AUTOMOVILÍSTICO Y LOS QUE LANZARÁN HASTA 2022



Para estimar la cantidad de vehículos que se verían afectados cada año por la normativa de ONU/UNECE WP29, se ha tomado como referencia 2019 -el último año completo del que se tienen datos de ventas de vehículos-. Ese año, en todo el mundo se vendieron 91.358.457 vehículos. De esa cifra, 22.126.597 unidades se vendieron en la UE, Japón y Corea del Sur -las regiones que ya han confirmado que aplicarán el reglamento UNECE/R155, distribuidas de la siguiente manera:

- **15.136.247 uds.** vendidas en 2019 en la Unión Europea.
- **5.195.216 uds.** vendidas en 2019 en Japón.
- **1.795.134 uds.** vendidas en 2019 en Corea del Sur.

Eso supone que, de todos los vehículos que se venden cada año en el mundo, aproximadamente el 25% de ellos lo hacen en territorios donde se aplicará el reglamento UNECE/R155.

En cuanto a los nuevos modelos que se comercializarán durante el periodo 2021-2022, los principales grupos automovilísticos pondrán a la venta, en la UE, 100 nuevos modelos, que se sumarán a los 231 que tienen en su catálogo en 2020.

Por otro lado, se abre una oportunidad de negocio para las OEMs que fabrican coches en España, porque serán más competitivos si son los primeros que fabrican coches ciberseguros -que cumplen con los requisitos de ciberseguridad que exige la nueva normativa, sometiendo sus vehículos al Test EUROCYBCAR.

Fábricas Coches / Furgonetas

SEAT	Barcelona: 5 modelos
GRUPO PSA	Zaragoza: 3 modelos
	La Coruña: 11 modelos
	Madrid: 3 modelos
FORD	Valencia: 6 modelos
GRUPO VW	Navarra: 2 modelos
IVECO	Valladolid: 1 modelo
RENAULT	Palencia: 3 modelos
	Valladolid: 2 modelos
MERCEDES	Vitoria: 5 modelos

Fábricas Camiones

- **IVECO** Madrid: 3 modelos

Fábricas Autobuses / Carroceros

- **11 MARCAS** 70 modelos

Esa información ha sido recopilada a fecha de octubre de 2020. Es un calendario no oficial de lanzamientos previstos hasta el año 2022, basado en la información del ciclo de vida de los modelos actuales y en los datos recopilados por el equipo de expertos y análisis de mercado de Grupo Cybentia.

Datos de Expansión disponibles en https://datosmacro.expansion.com/negocios/produccion-vehiculos

A QUÉ SANCIONES SE ENFRENTAN LOS FABRICANTES SI NO CUMPLEN LA NORMATIVA

LOS FABRICANTES QUE INCUMPLAN EL REGLAMENTO UNECE/R155 SE PUEDEN ENFRENTAR A DOS TIPOS DE SANCIONES: UNA DE LA PROPIA UNECE Y OTRA DE LA PROPIA UNIÓN EUROPEA

- **En el caso de la UNECE/R155**, el apartado 10 de su reglamento de ciberseguridad en vehículos afirma que un país podrá retirar la homologación concedida a un tipo de vehículo si descubre que no cumple con los requisitos establecidos por la UNECE/R155. Además, ese país deberá notificar inmediatamente la infracción al resto de estados que apliquen el reglamento.

- De forma paralela, como para poder homologar vehículos **en la UE será necesario cumplir con la normativa UNECE/R155** -según las condiciones explicadas anteriormente-, incumplirlo conllevará también incumplir el reglamento de homologación de la UE, por lo que el fabricante sería sancionado según el Reglamento sobre homologación y vigilancia del mercado de vehículos de motor.

En él se afirma que, si la UE detecta que un fabricante ha infringido la normativa de homologación en sus vehículos, podrá sancionar a la marca por cada unidad que no reúna las condiciones de ciberseguridad exigidas. La UE también podrá retirar o suspender la homologación de tipo de esos vehículos.

EUROCYBCAR®
CYBERSECURITY TEST

¿CÓMO CUMPLIR CON EL REGLAMENTO?

UNA SOLUCIÓN: ESTP (EUROCYBCAR® STANDARD TEST PROTOCOL)

LA ONU/UNECE HA DEJADO LIBERTAD A LOS FABRICANTES a la hora de buscar soluciones para cumplir con los 70 requisitos que refleja en su reglamento, porque no detalla cómo evitar esas amenazas. Eso abre la puerta a que los fabricantes colaboren activamente con las empresas especializadas en soluciones de securización automotriz, como Argus, Upstream, Guardknox o Harman.

Tampoco la normativa aún indica qué tipo de pruebas se deben realizar para saber si un vehículo puede obtener el certificado APTO de ciberseguridad. Pero hay una empresa que dispone de un test que evalúa y certifica si el vehículo cumple con los 70 requisitos de ciberseguridad que exige la norma ONU/UNECE WP29: EUROCYBCAR. Las pruebas se realizan en un laboratorio ubicado en Vitoria-Gasteiz, donde hackers, Ingenieros IT, probadores de coches y CyberQTester desde hace años realizan la evaluación técnica de ciberseguridad -el ESTP- a vehículos de organismos públicos y OEMs.

EL TEST EUROCYBCAR CERTIFICA SI EL VEHÍCULO CUMPLE LOS REQUISITOS QUE EXIGE LA UNECE/R155, REALIZANDO TRES TIPOS DE PRUEBAS

• **DE ACCESO FÍSICO:** El equipo de expertos de EUROCYBCAR comprueba, por ejemplo, si un ciberdelincuente podría manipular -a través del puerto OBD del vehículo- el airbag, sus frenos o su dirección; o si a través del puerto USB se puede introducir un virus que provoque la paralización de los sistemas del vehículo y ponga en riesgo la vida de los pasajeros.

• **DE ACCESO REMOTO:** se analiza sistemas inalámbricos como la conexión Bluetooth -que permite enlazar el dispositivo móvil al vehículo para compartir sus datos-, WiFi -que proporciona conexión a internet a los dispositivos móviles de los pasajeros-, el eCall -llamada automática a Emergencias en caso de accidente- o el sistema keyless -que, por ejemplo, permite abrir o cerrar un coche sin necesidad de utilizar la llave- para comprobar su nivel de ciberseguridad y valorar si la seguridad del vehículo o los datos privados de los usuarios se está poniendo en riesgo.

• **PRUEBAS DE APLICACIONES:** Por último, se evalúan las vulnerabilidades de las aplicaciones que ya están integradas en el vehículo, y también las apps oficiales de la marca que el usuario se descarga en su móvil.

Algunas de estas aplicaciones permiten al usuario controlar desde su smartphone diversos parámetros del vehículo -como encender la calefacción antes de entrar- o acceder a información almacenada en el vehículo -como el kilometraje o las rutas seguidas habitualmente por el conductor-. Esto, obviamente, es un peligro si un ciberdelincuente consigue vulnerar dichas aplicaciones, ya que podría acceder a sistemas del vehículo y llegar incluso a provocar un accidente.

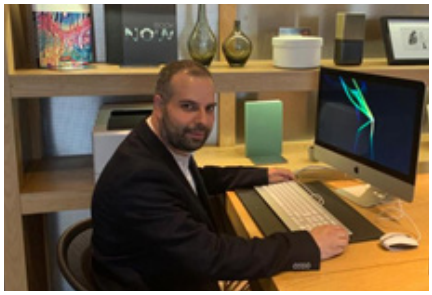
EL ESTP -EUROCYBCAR Standard Protocol Test- es el único TEST integral en todo el mundo -con patente internacional- que identifica vulnerabilidades y mide el nivel de ciberseguridad de un vehículo -coches, autobuses, camiones y furgonetas-, según lo requisitos de la nueva normativaUNECE/R155.

Una vez que el vehículo se ha sometido al protocolo de pruebas de EUROCYBCAR 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 sea, significará que el coche analizado dispone de un mayor nivel de protección; es decir, que "será una garantía de que protege los datos que el vehículo almacena del usuario" cuando, por ejemplo, conecta su smartphone.

Pero, sobre todo, una buena nota en el test también será sinónimo de que el coche en cuestión lleva implementadas las medidas mínimas para evitar que alguien pueda tomar el control a distancia de sistemas como la dirección, los frenos, el motor… y causar accidentes con grave riesgo para la vida del conductor y los pasajeros, o la de otros usuarios de la vía-.

EUROCYBCAR®
CYBERSECURITY TEST

¿QUÉ OPINAN LOS EXPERTOS?



PABLO ESCAPA
CTO DE EUROCYBCAR

Pablo Escapa ha participado en el grupo de trabajo español que ha contribuido al desarrollo de la normativa de UNECE/R155. Escapa afirma que estas normativas pretenden regular los mecanismos que deben equipar los vehículos para ser ciberseguros. Es decir, contar con herramientas tanto para evitar como para mitigar los ataques a los que puedan ser expuestos. La ciberseguridad 100% no existe, pero resultará más difícil ciberatacar a un coche que cumpla con toda la normativa.

Además, la norma se aplicará a todos los futuros automóviles vendidos en Europa -y otros países dentro del marco de la ONU/UNECE-. Se necesitará un certificado de conformidad en materia de ciberseguridad para poder homologar los vehículos destinados al espacio económico europeo. ¿Lo más revolucionario? El sistema de gestión de las actualizaciones online que coexiste con esta normativa.

Para los fabricantes de vehículos la adaptación a nueva norma para implementar la ciberseguridad en todos los procesos va a suponer un gran reto, tanto en costes de tiempo como económicos, porque los niveles que se requieren son muy exhaustivos -más propios de la protección de una infraestructura crítica- ya que la conducción autónoma se considera una actividad crítica.
Por suerte hay fabricantes que ya se están adelantando para adaptarse a la nueva regulación, incluso realizando el ESTP a sus modelos.

AZUCENA HERNÁNDEZ
CEO DE EUROCYBCAR

Llevamos años concienciando a instituciones y empresas en España y en Europa para que la "cybersecurity by design" sea la base de la movilidad cibersegura del futuro y la ONU/UNECE "nos ha dado la razón" con esta normativa que ha entrado en vigor el 22 de enero de 2021 y que obligará a los fabricantes de vehículos a incorporar la ciberseguridad desde la fase de diseño e, incluso, en sus sistemas de gestión.

La UNECE/R155 es una normativa drástica porque exigirá que los vehículos cuenten con un certificado de ciberseguridad que acredite que están mínimamente protegidos contra ciberataques y se llegará, incluso, a cerrar el mercado europeo a los coches, autobuses, camiones y furgonetas que no cumplan con los 70 requisitos que establece dicha normativa.

La regulación es drástica, pero muy necesaria, porque los vehículos son grandes ordenadores sobre cuatro ruedas y deben protegerse, como mínimo, igual que se protege un móvil o un portátil. Las consecuencias de que no estén bien ciberprotegidos pueden ser trágicas: basta con que una persona introduzca en el puerto USB de su coche un pen drive con música que se ha descargado de internet, -sin saber que también lleva un virus o un malware que puede infectar el vehículo- para provocar que el motor del vehículo se pare o desconecte el sistema de frenada de emergencia, por ejemplo.

NURIA ROMÁN
JEFA DE ÁREA DE LA SUBDIRECCIÓN GENERAL DE CALIDAD Y SEGURIDAD INDUSTRIAL (MINISTERIO DE INDUSTRIA, COMERCIO Y TURISMO). ADEMÁS, HA LIDERADO EL GRUPO DE TRABAJO ESPAÑOL DE LA NORMATIVA UNECE/R155

¿QUÉ ASPECTOS DE LA NORMA TE PARECEN LOS MÁS DESTACADOS?

Los vehículos actuales ya se diseñan con arquitecturas electrónicas y de sistemas de información complejos que, por ejemplo, permiten abrir o arrancar el vehículo, manejan la inyección de combustible y, por tanto, los regímenes de funcionamiento del motor, monitorizan los sistemas del vehículo y ofrecen información de diagnóstico para su reparación o intervienen en casos de emergencia. Garantizar un nivel mínimo de seguridad en el acceso a estos sistemas es lo que pretende el nuevo reglamento de ciberseguridad.

Esta reglamentación permitirá evaluar la protección contra accesos no autorizados a la información y los sistemas contenidos en los vehículos, armonizando los mínimos que deben superarse en todos los fabricantes, que ya adoptaban medidas de protección, hasta ahora de forma no evaluada durante el proceso de homologación.

UNA VEZ QUE LA NORMATIVA ENTRE EN VIGOR, ¿CUÁLES SON LOS SIGUIENTES PASOS A SEGUIR?

El marco de homologación de vehículos en la Unión Europea establece una serie de reglamentos de Naciones Unidas o, en su caso, Reglamentos o Directivas UE, que los vehículos deben cumplir para poder ser comercializados en el mercado interior. Una vez se exija el reglamento de ciberseguridad para la homologación de tipo europea, prevista en el año 2022, dicho reglamento deberá evaluarse, junto con el resto de los exigidos durante el proceso de homologación. Hasta entonces, los fabricantes pueden aplicarlo de forma voluntaria, pero a partir de que sea obligatorio, no podrán homologarse nuevos tipos de vehículos que no lo cumplan.

¿CÓMO ES EL PROCESO PARA EVALUAR SI UN TIPO DE VEHÍCULO POSEE UN CSMS ACORDE A ESTA NUEVA NORMATIVA?

Se trata de un reglamento complejo, distinto a los tradicionales de homologación en el que no resulta posible identificar un ensayo a efectuar sobre el peor de los escenarios. El reglamento tiene en cuenta esta dificultad y emplea la metodología del análisis de riesgos y la especificación de amenazas y protecciones mínimas que deben contemplarse en un vehículo. Además, está en elaboración

"Uno de los requisitos más destacados de la normativa es que obliga a considerar los aspectos de ciberseguridad desde el diseño de la arquitectura".

una guía de aplicación que recomienda el uso de diversas metodologías de evaluación de los sistemas de gestión de la ciberseguridad y la seguridad de la información. En primera instancia es el fabricante el que debe evaluar el cumplimiento de los requisitos, documentando el análisis de riesgo, las medidas de protección, su implementación y las pruebas ejecutadas para verificar su efectividad. Posteriormente, el servicio técnico evaluará la conformidad de todas estas evidencias y por muestreo, llevará a cabo otras pruebas. En cualquier caso, deberá seguir las recomendaciones de la guía de aplicación, que aún está en elaboración.

¿POR QUÉ JAPÓN Y COREA QUIEREN ADELANTARSE A LA FECHA DE IMPOSICIÓN DE LA NORMA? ¿TIENEN ESTOS PAÍSES YA DESARROLLADOS PROTOCOLOS DE EVALUACIÓN?

Se trata de dos países muy avanzados en tecnología electrónica y automática. Desconocemos el estado de sus protocolos de evaluación, aunque la guía de aplicación desarrollada en el grupo de Naciones Unidas ya ofrece la posibilidad de aplicar varias metodologías de evaluación estandarizadas. En cualquier caso, la fecha de aplicación en la UE es también muy próxima, en 2022. Dado que el acuerdo de 1958 sobre armonización técnica exige el reconocimiento mutuo de las homologaciones concedidas entre las partes firmantes, lo ideal es recurrir a la guía de aplicación que sea finalmente acordada en ese foro.

¿ESTÁN LOS FABRICANTES PREPARADOS PARA APLICAR LA NORMATIVA? ¿QUÉ ESFUERZOS LES SUPONDRÁ? ¿CUÁL ES EL MAYOR CAMBIO QUE DEBERÁ REALIZAR UN FABRICANTE PARA CUMPLIR CON LOS REQUISITOS?

Evidentemente la entrada en vigor de un nuevo reglamento exige adaptaciones a la industria. No obstante, la tecnología suele ir por delante de la reglamentación, y en este caso, la industria no parte de cero para adaptarse a la normativa. Los fabricantes ya tenían en cuenta la protección de los sistemas de información presentes en el vehículo, lo que cambia ahora es que deben adaptarse a los requisitos del reglamento y evaluarse durante el proceso de homologación del vehículo.

LA NORMATIVA TAMBIÉN INDICA QUE SE VERÁN AFECTADOS TODOS LOS DEPARTAMENTOS INVOLUCRADOS EN LA PRODUCCIÓN DE UN TIPO DE VEHÍCULO, ¿CÓMO AFECTARÁ ESTO A TALLERES Y PROVEEDORES?

El proceso de fabricación de los vehículos incorpora componentes y sistemas de una multiplicidad de proveedores. El reglamento obliga a definir la arquitectura de los vehículos teniendo en cuenta la ciberseguridad, por lo que la integración de los componentes estará prevista desde un punto de vista "ciberseguro". Pero, además, es indudable que el reglamento afecta también a los proveedores de sistemas y componentes, y así el fabricante del vehículo debe evaluar los riesgos asociados al vehículo final, incorporando esos componentes, lo que impone tener en cuenta la ciberseguridad en toda la cadena de suministro.

¿POR QUÉ ESTA NORMATIVA NO AFECTA A MOTOS, BARCOS O TRENES? ¿SALDRÁ PRONTO ALGUNA NORMATIVA AL RESPECTO?

El acuerdo de Ginebra de 1958 sobre armonización técnica que sirve de marco al reglamento de ciberseguridad afecta solo a los vehículos de ruedas. En el caso de las motocicletas, no se han considerado incluidas en esta primera versión del reglamento debido a su menor grado de avance hacia la conducción automatizada, al menos en este momento.

EUROCYBCAR®
CYBERSECURITY TEST

QUÉ SABER SOBRE EUROCYBCAR®

EUROCYBCAR SL, es una empresa de base tecnológica, con sede en Vitoria-Gasteiz, que desarrolla productos y servicios innovadores de ciberseguridad para el sector de la automoción/movilidad que protejan la vida y los datos de las personas y de los vehículos.

EUROCYBCAR es pionera a nivel global al aunar la ciberseguridad, la automoción y la movilidad en su core business, desarrollando en base a ello todo un portfolio de productos y servicios con el objetivo de conseguir una protección integral de la movilidad en el ámbito de la ciberseguridad.

EUROCYBCAR posee un demostrado expertise -más de 30 años de experiencia- en Investigación, Automoción, Movilidad y Ciberseguridad, estando el core del equipo formado por hackers, investigadores, ITs, expertos en Seguridad, probadores de coches y expertos en legislación.

EUROCYBCAR ha creado la primera evaluación técnica de ciberseguridad en el mundo que cumple con los requisitos de la nueva normativa de seguridad de UNECE/ R155, que mide y certifica el nivel de ciberseguridad de un coche, basándose en dos parámetros: de qué forma protege la privacidad del conductor y de los pasajeros -SUS DATOS- y, lo que es más importante, SU VIDA. El protocolo de la evaluación técnica de ciberseguridad -con patente internacional- se realiza en su laboratorio de Vitoria-Gasteiz.

Además, **EUROCYBCAR** dispone de un amplio portfolio de productos y servicios -siempre relacionados con la ciberseguridad y la movilidad-, con el objetivo de conseguir una ciberprotección integral de la movilidad: el Test Integral de Ciberseguridad para Sistemas de Gestión de Flotas, el Test V2D -test a las conexiones entre el coche y los dispositivos que el usuario conecta al vehículo-, el Test para Aplicaciones de Movilidad, el Test para neumáticos inteligentes o el Test para locomotoras/trenes son ejemplos de la preocupación de EUROCYBCAR por una movilidad más cibersegura.

MÁS INFORMACIÓN:

WWW.EUROCYBCAR.COM
PARQUE TECNOLÓGICO DE ÁLAVA EDIFICIO BIC
ALBERT EINSTEIN KALEA, 15 - 01510
VITORIA-GASTEIZ, ÁLAVA
+34 619 291 892
INFO@EUROCYBCAR.COM