



Curso

Normativa de la ONU en Ciberseguridad para Vehículos



FORMACIÓN
GRUPO CYBENTIA



En colaboración con el Área Técnica de



Normativa de la ONU en Ciberseguridad para Vehículos

Presentación

En junio de 2020 la ONU publicó la normativa de ciberseguridad para vehículos, en los países europeos es la denominada UNECE/R155 y equivalente a **la ISO 21434/2021**, que obliga a los fabricantes a contar con una certificación de ciberseguridad de los vehículos -coches, camiones, autobuses, furgonetas y autocaravanas- que homologuen a partir de julio de 2022 y a todos los que estén a la venta a partir de julio de 2024. Esta normativa ya afecta a múltiples sectores: fabricantes de vehículos, proveedores de componentes, concesionarios, aseguradoras, talleres y usuarios finales.

Grupo CYBENTIA, en colaboración con EUROCYBCAR, te presenta el primer curso de formación basado en la norma de la ONU. Este curso te aportará una visión global del sector, de la ciberseguridad aplicada a la automoción, que engloba desde cómo son los vehículos conectados y qué tecnologías incluyen, hasta a qué riesgos se enfrentan los usuarios, qué tipo de ciberataques se realizan contra los vehículos y flotas de vehículos o quiénes evalúan los vehículos para medir y certificar su nivel de ciberseguridad, según los requisitos que marca la nueva normativa.

¿A quién va dirigido?

Marcas, fabricantes de coches, concesionarios, aseguradoras y peritos.



Foto: megostudio en Envato Elements



Foto: LightFieldStudios en Envato Elements



Foto: photovs en EnvatoElements

Talleres, marcas de componentes y accesorios, empresas con flotas de vehículos o autoescuelas.



Foto: westend61 en Envato Elements



Foto: vanitjan en Envato Elements



Foto: Prostock-studio en Envato Elements

Administración pública, investigadores formadores, consultoras, analistas...



Foto: FabrikaPhoto en Envato Elements

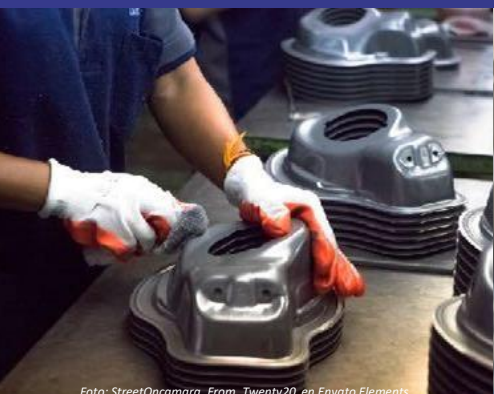


Foto: StreetOncamara_From_Twenty20 en Envato Elements

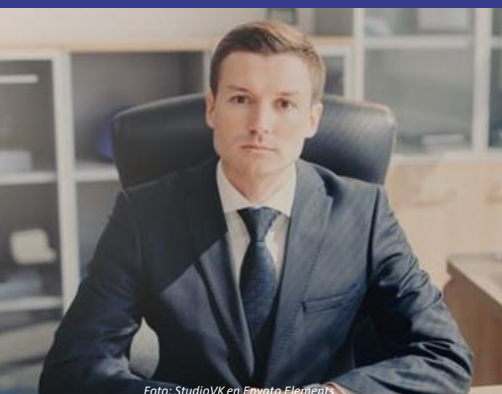


Foto: StudioVK en Envato Elements

- 01
- 02
- 03
- 04
- 05

Las claves del curso



Matriculación
ABIERTA
Cursos mensuales



12
horas



100%
online



En colaboración
con el Área
Técnica

Objetivos

Cibervulnerabilidades de un vehículo.

Conocer cómo es la tecnología que implementan los vehículos conectados y a qué ciber-riesgos se exponen los que viajan a bordo -tanto de privacidad como relacionados con su propia vida si el vehículo no es ciberseguro-.

Normativa de ciberseguridad para vehículos.

Analizar la normativa de la ONU y conocer los requisitos de ciberseguridad que deben cumplir por ley los vehículos que se homologuen a partir de julio de 2021 y todos los que estén a la venta en 2024.

Impacto de la integración de la ciberseguridad en la industria del motor.

Principales efectos de la entrada en vigor de la normativa en los fabricantes, proveedores, concesionarios, talleres, usuarios, aseguradoras, empresas de flotas, transporte y logística.

Metodología

El curso combina diferentes recursos didácticos de formación online, principalmente:



Contacto directo con el profesor durante las sesiones online.



Vídeos formativos de estudio y textos formativos de refuerzo.



Test de progreso auto-evaluable para la superación del curso al final de los módulos que componen la formación.



Sala de chat y foros para el refuerzo de contenidos clave y la resolución de dudas.

Evaluación

El curso concluye con un test final a realizar tras el estudio de los módulos de formación del curso, compuesto por 18 preguntas tipo test, con 3 posibles respuestas de las cuales solo una de ellas es válida.

Dicho test se centrará en los principales conceptos abordados durante el curso, y se dispondrá de dos intentos para superarlo.

El resultado del test supondrá la nota del alumno en el curso.

Además, el curso se complementará con el siguiente material:

- Documento de preguntas y respuestas.
- Informes relacionados.
- Documentación.
- Material adicional.

La estructura y contenidos de la formación será supervisada por personal con formación en calidad de la enseñanza cualificada por la escuela competente donde se realice el curso.

Programa académico

1

POR QUÉ UN
REGLAMENTO DE
CIBERSEGURIDA
D PARA
VEHÍCULOS

2

QUÉ REQUISITOS
DE
CIBERSEGURIDAD
DEBE CUMPLIR
UN VEHÍCULO
PARA VENDERSE

3

LA NORMATIVA
DE LA ONU:
TODO LO QUE
DEBES SABER

4

LA SOLUCIÓN:
EL TEST
EUROCYBCAR
PARA FLOTAS

5

CÓMO MEDIR
Y CERTIFICAR
LA
CIBERSEGURID
AD DE LOS
VEHÍCULOS: EL
TEST
EUROCYBCAR

6

IMPACTO DE
LA
NORMATIVA
DE LA ONU EN
EL SECTOR DE
LA
AUTOMOCIÓN

● INTRODUCCIÓN: ¿TU COCHE ES CIBERSEGURO?

1. **Precedentes y situación actual** del mundo del motor, la movilidad y la ciberseguridad:
2. **Cómo son** los vehículos conectados actuales.
3. **Qué tecnologías** incluyen.
4. **Los riesgos** a los que se enfrenta el usuario si el vehículo no es ciberseguro.
5. **Ataques registrados** contra vehículos, flotas de vehículos, concesionarios...
6. **Qué dicen los hackers.**
7. **Explicar la entrada en vigor** de la normativa de la ONU, por qué Naciones Unidas y la Unión Europea la han desarrollado y aplicado tan rápido y quién está ya realizando el test a los vehículos, según los requisitos de la normativa.



Foto: AlinStock en Envato Elements

06

07

08

09

10

1 POR QUÉ UN REGLAMENTO DE CIBERSEGURIDAD PARA VEHÍCULOS

- 1. El coche conectado:** El equipamiento de los vehículos.
- 2. Dispositivos y tecnologías** que van a llevar los vehículos, por ley, en los próximos años.
- 3. Los vehículos eléctricos:** A qué ciberamenazas están expuestos.
- 4. Ataques registrados a vehículos desde el año 2012:** En 2020 se batieron todos los récords.
- 5. Ataques** registrados a flotas de vehículos.
- 6. Consecuencias de un ataque:** a una flota de coches, camiones, furgonetas, autobuses, autocaravanas...- a concesionarios, a vehículos eléctricos...
- 7. Conclusiones.**



2 QUÉ REQUISITOS DE CIBERSEGURIDAD DEBE CUMPLIR UN VEHÍCULO PARA VENDERSE

- 1. Normativas de seguridad desde el año 2000:** Análisis de las principales normativas de seguridad de vehículos desde el año 2000 hasta hoy.
- 2. Las normativas que la Unión Europea** toma de las Naciones Unidas.
- 3. Iniciativas previas a la normativa de la ONU en España,** en Europa y en todo el mundo.
- 4. Cómo y quién ha participado en la normativa** y cuáles han sido las fases.
- 5. Conclusiones.**

3 LA NORMATIVA DE LA ONU: TODO LO QUE DEBES SABER

1. **A qué hace referencia el reglamento.**
2. **Las fases** de desarrollo de la normativa.
3. **Iniciativas** previas a la normativa.
4. **Regulaciones** previas de ciberseguridad en vehículos.
5. **Países que lo aplicarán.**
6. **Qué debe saber de la etiqueta 'vehículo ciberseguro'**.¿y dónde debe ir?
7. **Qué es el CSMS** y de qué forma afectará a talleres, fábricas, concesionarios...
8. **Conclusiones.**



4 LA NORMATIVA UNECE/R155: LOS 70 REQUISITOS QUE DEBE CUMPLIR UN VEHÍCULO PARA OBTENER EL CERTIFICADO DE CIBERSEGURIDAD

1. **Los procesos para conseguir el certificado** de "vehículo ciberseguro".
2. **Los 70 requisitos** que debe cumplir un vehículo ciberseguro.
3. **Índice del documento original.**
4. **El análisis de cibervulnerabilidades.**
5. **Las mitigaciones** que deben implementarse en un vehículo ciberseguro.
6. **Las posibles sanciones** si no se cumple la normativa UNECE/R155.
7. **Conclusiones.**

5 CÓMO MEDIR Y CERTIFICAR LA CIBERSEGURIDAD DE LOS VEHÍCULOS: EL TEST EUROCYBCAR

1. ¿Cómo se analiza la ciberseguridad?
2. **Metodologías** para analizar la ciberseguridad de los dispositivos IoT.
3. **Por qué las metodologías 'Common Criteria' y 'Lince'** no sirven para analizar la ciberseguridad de los vehículos y es necesaria una metodología propia.
4. **Cómo son las pruebas** que deben superarse y quién las está realizando ya: El Test EUROCYBCAR.
5. **Conclusiones.**



6 IMPACTO DE LA NORMATIVA DE LA ONU EN EL SECTOR DE LA AUTOMOCIÓN

1. **Principales actores** que forman parte del sector de la automoción.
2. **Fabricantes:** Qué rol tienen en el sector de la automoción, cómo les afecta la normativa de la ONU, la implantación de nuevas políticas y sus consecuencias a corto y largo plazo
3. **Concesionarios:** El papel que interpretan y de qué manera les afecta la normativa de la ONU, sumado al nuevo concepto de concesionario y su relación con el cliente.
4. **Aseguradoras:** Cómo afrontan la normativa y el nuevo marco de negocio que se les abre tras la entrada en vigor de la normativa.
5. **Talleres:** La influencia de la normativa, el nuevo concepto de taller, la creación de nuevos perfiles profesionales y relaciones con los demás actores.
6. **Formación:** Objetivos que tiene en el sector, la nueva estrategia formativa y su importancia.
7. **Clientes/Usuarios:** ¿Cambia la normativa la relación con los otros actores? ¿Y en el criterio a la hora de adquirir un vehículo por parte del consumidor?
8. **Conclusiones.**



FORMACIÓN

GRUPO CYBENTIA



Matriculación
ABIERTA
Cursos mensuales



12
horas



100%
online



En colaboración
con el Área
Técnica

Información e inscripciones CEA Chile

56 2 2232 2654

info@ceadechile.cl



Sede Madrid
C/ Faraday,
7
28049 Madrid



Sede Vitoria-Gasteiz
C/ Hermanos Lumiere, 11
01510 Vitoria-Gasteiz
(Álava)



Curso

Ciberseguridad en las flotas de vehículos



FORMACIÓN
GRUPO CYBENTIA



Club Europeo de Automovilistas de Chile

En colaboración con el Área Técnica de



Ciberseguridad en las flotas de vehículos

Para conocer la situación actual en el sector, con los nuevos retos a los que debe hacer frente

Se ha desarrollado el curso **“Ciberseguridad en las flotas de Vehículos”**. Una formación completamente virtual y que, de la mano de los expertos de EUROCYBCAR, abarca temas que van desde las actuales flotas de vehículos, los sistemas y tecnologías que se emplean en su gestión hasta la importancia del CSMS –sistema de gestión de la ciberseguridad- y las razones por las que es necesario y fundamental garantizar su ciberseguridad.

Grupo CYBENTIA, en colaboración con la empresa tecnológica EUROCYBCAR, lanza **la primera formación** enfocada a la **ciberseguridad** de las empresas que utilizan flotas de vehículos, Sistemas de Gestión de Flotas –SGF- y a los diferentes actores que involucra.

Este curso te aportará una visión global del sector y **responde cuestiones esenciales**: cómo funcionan las flotas de vehículos conectados, cómo se pueden controlar de forma telemática los vehículos que la componen y, sobre todo, a qué riesgos de ciberseguridad están expuestas.

Y tú, ¿Quieres liderar el sector de la movilidad cibersegura?

¿A quién va dirigido?

Empresas, tanto públicas como privadas, que cuentan con vehículos para poder llevar a cabo su trabajo o para que su personal y miembros puedan realizar sus desplazamientos profesionales.



Foto: megastudio en Envato Elements



Foto: LightFieldStudios en Envato Elements



Foto: photovs en Envato Elements

Marcas, fabricantes de vehículos, empresas de renting/leasing de vehículos, de coche compartido, de logística, aseguradoras y peritos.



Foto: westend61 en Envato Elements



Foto: vanitjan en Envato Elements



Foto: Prostock-studio en Envato Elements

Talleres, fabricantes de componentes y accesorios, preparadores de vehículos de flota, decisores de compra de las empresas, responsables de SGF.



Foto: FabrikaPhoto en Envato Elements

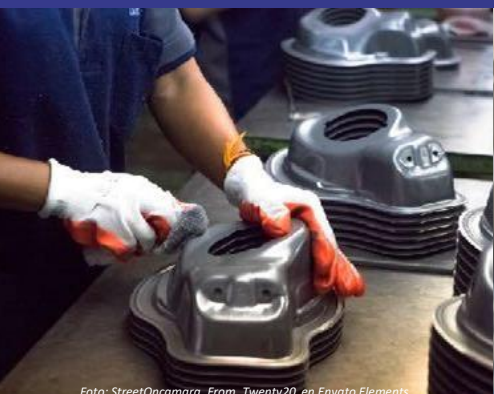


Foto: StreetOncamara_From_Twenty20 en Envato Elements



Foto: StudioVK en Envato Elements

- 01
- 02
- 03
- 04
- 05

Las claves del curso



Matriculación
ABIERTA
Cursos mensuales



12
horas



100%
online



En colaboración
con el Área
Técnica

Objetivos

Cibervulnerabilidades de las flotas de vehículos

Conocer cómo es la tecnología que implementan los vehículos conectados integrados en una flota de vehículos y a qué ciber-riesgos exponen a la empresa y a los que viajan a bordo -tanto de privacidad como relacionados con su propia vida-, como a la empresa de la que forman parte.

Impacto de la integración de la ciberseguridad en las flotas y sus SGF

Cómo se debe realizar la integración, desde qué momento debe llevarse a cabo, que cambios y mejoras obliga a implementar en la organización, en los SGF y en los vehículos con los que cuente una empresa para realizar sus trabajos y funciones.

Conocer el nivel de ciberseguridad de una flota de vehículos y su SGF

Qué legislaciones de ciberseguridad aplicadas a vehículos o al SGF existen en la actualidad, y cómo se aplican; cual es el objetivo del Test EUROCYBCAR y todo lo que aporta a los vehículos conectados de una empresa.

Metodología

El curso combina diferentes recursos didácticos de formación online, principalmente:



Contacto directo con el profesor durante las sesiones online.



Vídeos formativos de estudio y textos formativos de refuerzo.



Test de progreso auto-evaluable para la superación del curso al final de los módulos que componen la formación.



Sala de chat y foros para el refuerzo de contenidos clave y la resolución de dudas.

Evaluación

El curso concluye con un test final a realizar tras el estudio de los módulos de formación del curso, compuesto por 10 preguntas tipo test, con 3 posibles respuestas de las cuales solo una de ellas es válida.

Dicho test se centrará en los principales conceptos abordados durante el curso, y se dispondrá de dos intentos para superarlo.

El resultado del test supondrá la nota del alumno en el curso.

Además, el curso se complementará con el siguiente material:

- Documento de preguntas y respuestas.
- Informes relacionados.
- Documentación.
- Material adicional.

La estructura y contenidos de la formación será supervisada por personal con formación en calidad de la enseñanza cualificada por la escuela competente donde se realice el curso.

Programa académico

1

EL VEHÍCULO
CONECTADO

2

ASPECTOS
ORGANIZATIVOS
Y OPERACIONES
DE UN SGF

3

MEDIOS
TECNOLÓGICOS
EMPLEADOS EN
LAS FLOTAS DE
VEHÍCULOS

4

OBJETIVOS DE LOS
CIBERDELINCUENTES

5

LA SOLUCIÓN:
EL TEST
EUROCYBCAR PARA
FLOTAS

1 Las flotas de vehículos: El vehículo conectado

- 1. El Vehículo Conectado:** Cómo -y por qué- los vehículos actuales actúan como dispositivos conectados en movimiento.
- 2. Las flotas de vehículos y el papel básico que juegan en el mundo:** Las flotas y su relevancia en la actualidad.
- 3. Sistema de Gestión de Flotas (SGF):** Qué es, sus funciones y ejemplos.
- 4. Tipos de flotas de vehículos:** Tipos más comunes de flotas, sus clasificaciones y particularidades.
- 5. El papel de los responsables del Sistema de Gestión de Flotas:** competencias y responsabilidades que tienen los empleados que trabajan directamente con el SGF, así como los datos que manejan en su labor diaria.
- 6. La ciberseguridad en las flotas de vehículos.**
- 7. Conclusiones.**



2 Las flotas de vehículos: Aspectos organizativos y operaciones de un SGF

1. **Adquisición de vehículos:** tipos de adquisición de vehículos para la flota y características de estos con sus ventajas e inconvenientes.
2. **Costes del Sistema de Gestión de Flotas:** Objetivos que se deben tener en cuenta a la hora de realizar los costes, explicación de los tipos que existen.
3. **Operaciones de los vehículos de una flota:** Objetivos que se deben tener en cuenta al realizar las operaciones necesarias y principales actividades que se realizan, explicadas de manera detallada.
4. **La ciberseguridad en los aspectos organizativos y operacionales de un Sistema de Gestión de Flotas.**
5. **Conclusiones.**



3 Las flotas de vehículos: Medios tecnológicos empleados

1. **Sistemas de Información en un SGF:** Objetivos de cara al diseño y a la implementación de un sistema de gestión de flotas, así como aspectos técnicos que se deben tener en cuenta.
2. **Gestión y seguimiento de los vehículos:** Enumeración de los parámetros más destacados a la hora de realizar un control y seguimiento de los vehículos de manera eficiente.
3. **Tecnologías empleadas en un Sistema de Gestión de Flotas:** Desarrollo de los requisitos fundamentales que debe cumplir la tecnología implementada en la gestión de la flota. Tratamiento exhaustivo de la principal tecnología de un SGF: La Telemática.
4. **Tendencias futuras:** Cuatro tendencias que afectan y afectarán a los SGF. Pequeño anticipo de la ciberseguridad, aspecto que es desarrollado mas en profundidad en los siguientes módulos.
5. **La ciberseguridad en los medios tecnológicos empleados en las flotas de vehículos.**
6. **Conclusiones.**

4 Las flotas de vehículos: Objetivos de los ciberdelincuentes

- 1. Vulnerabilidades en los vehículos:** De qué maneras puede un cracker atacar los vehículos que compongan la flota de una determinada organización.
- 2. Vulnerabilidades en el Sistema de Gestión de Flotas:** Qué le puede hacer un cracker al software, hardware y aplicaciones encargadas de la gestión de la flota de vehículos.
- 3. Vulnerabilidades causadas por el factor humano:** Qué consecuencias existen si no se siguen los protocolos adecuados y las buenas prácticas que se deben llevar a cabo.
- 4. Ejemplos Prácticos:** Casos Reales.
- 5. Conclusiones.**



Foto: duallogic en Envato Elements

5 La solución: El test EUROCYBCAR para flotas

- 1. Ciberseguridad: Legislaciones Aplicables:** El marco legislativo que rige sobre los sistemas de gestión de flotas y vehículos, y cómo contemplan la ciberseguridad.
- 2. El Vehículo Ciberseguro: el Test EUROCYBCAR para Vehículos:** Cómo el Test EUROCYBCAR, y su metodología ESTP, puede ayudarnos a elegir vehículos ciberseguros para nuestra flota.
- 3. El SGF Ciberseguro: el Test EUROCYBCAR para Sistemas de Gestión de Flotas:** Cómo este Test mide y evalúa el nivel de ciberseguridad de los diferentes elementos que componen el sistema que gestiona la flota de vehículos.
- 4. Conclusiones.**



FORMACIÓN

GRUPO CYBENTIA



Matriculación
ABIERTA
Cursos mensuales



12
horas



100%
online



En colaboración
con el Área
Técnica

Información e inscripciones CEA Chile

56 2 2232 2654

info@ceadechile.cl



Sede Madrid
C/ Faraday, 7
28049 Madrid



Sede Vitoria-Gasteiz
C/ Hermanos Lumiere, 11
01510 Vitoria-Gasteiz (Álava)