Formación

Curso de Ciberseguridad para Vehículos Eléctricos

FORMACIÓN
GRUPO CYBENTIA

En colaboración con el Área Técnica de

EUROCYBCAR®
CYBERSECURITY TEST

Ciberseguridad para vehículos eléctricos

Movilidad eléctrica y ciberseguridad: Dos realidades que definen a los vehículos actuales

El vehículo eléctrico representa el tipo de movilidad más sofisticado que existe en la actualidad. Esta clase de automóviles, además de contar con las avanzadas tecnologías que incluye cualquier modelo de combustión –ayudas a la conducción, digitalización, sistemas de confort y seguridad…- también añade como elemento fundamental, un sistema de propulsión eléctrico que resulta más novedoso y avanzado que el de los modelos 'tradicionales'. Por lo tanto, **a los factores de riesgo y vulnerabilidades relacionadas con la ciberseguridad de cualquier vehículo, se suman** aquí los condicionantes que tienen que ver con la propulsión eléctrica –motor, batería, unidad de control, convertidor…**-** así como con los sistemas de recarga, imprescindibles para el funcionamiento de este tipo de automóviles.

Hablamos de una forma de transporte cuya presencia se extiende a gran velocidad; entre otros motivos, por la obligatoriedad en la Unión Europea de cumplir con los calendarios de electrificación en un sector como el del automóvil que, a partir de 2035, solo podrá vender modelos nuevos 100% eléctricos. A esto hay que sumar que **el número de ciberataques contra este creciente tipo de movilidad se ha incrementado de manera exponencial** en apenas cinco años. La conclusión básica, por lo tanto, es que **la ciberseguridad en los vehículos eléctricos ya se ha convertido en algo fundamental**.

Sin embargo, hasta ahora, no existía una formación específica que tratase ese asunto. Por eso, **Grupo CYBENTIA, en colaboración con los expertos del Área Técnica de EUROCYBCAR,** presenta el curso **"Ciberseguridad para Vehículos Eléctricos".** Una formación centrada en conocer las complejidades y particularidades de este tipo de vehículos –así como las infraestructuras y otro tipo de elementos que le rodean- para, a partir de ahí, conocer los desafíos de ciberseguridad a los que se enfrentan.

Y tú, ¿quieres liderar el futuro de la movilidad?

¿A quién va dirigido?

Fabricantes / Talleres oficiales / Aseguradoras / Gestores de flotas



Profesionales del sector de la automoción, del sector de la energía, instalaciones eléctricas y puntos de recarga / Profesionales de la ciberseguridad



Licenciados en Grado de Automoción / Licenciados en Grado de Ingeniería informática



Las claves del curso

Matriculación **ABIERTA**
Cursos mensuales

25 horas

Modalidad **híbrida**

En colaboración con el **Área Técnica**

Objetivos

CONOCER la tecnología y dispositivos que hacen diferentes a los vehículos eléctricos

Es básico tener un conocimiento de la tecnología específica de los vehículos eléctricos: Desde los motores hasta los sistemas de almacenamiento de energía, protocolos de redes, tipos de enchufes y conexiones, sistemas de recarga...

APRENDER los aspectos normativos relacionados con la ciberseguridad en vehículos

El texto fundamental en este apartado es la UNECE/R155, que también incluye contenido relacionado específicamente con los vehículos eléctricos. Asimismo, la formación trata normativas como la ISO 15118 o la ISO/SAE 21434, al tiempo que se explica la importancia de herramientas como el CSMS.

COMPRENDER los riesgos de ciberseguridad que afectan a los vehículos eléctricos

Todos aquellos componentes específicos del vehículo eléctrico –por ejemplo, la batería, la toma de corriente, el convertidor...- pueden padecer vulnerabilidades de ciberseguridad. Por eso, es básico conocer a qué tipo de ciberataques se enfrentan, sus posibles consecuencias y qué medidas de protección se deben implementar para protegerlos.

PROFUNDIZAR en las mitigaciones para evitar ataques contra las infraestructuras de recarga

Son el principal punto débil de la movilidad eléctrica. De hecho, buena parte de los ataques que se registran tienen como principal objetivo las infraestructuras de carga. Durante la formación se habla de las medidas de seguridad que se pueden aplicar a los puntos de carga para evitar las acciones de los delincuentes.

Metodología

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

Vídeo-tutoriales de estudio individual y textos formativos de refuerzo.

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

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

Además, el curso se complementa con el siguiente material:

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

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

Evaluación

El curso concluye con un test final, a realizar tras el estudio de los módulos de la formación. Una evaluación que se compone de 30 preguntas tipo test, con tres posibles respuestas, de las cuales sólo una es la correcta.

Dicho test está centrado en los principales conceptos abordados durante el curso; se dispone de un único intento para superarlo.

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

Programa académico

1 **EL VEHÍCULO ELÉCTRICO** Y SUS COMPONENTES

2 **NORMATIVAS DE CIBERSEGURIDAD** PARA VEHÍCULOS ELÉCTRICOS

3 **RIESGOS DE CIBERSEGURIDAD COMPARTIDOS** EN VEHÍCULOS ELÉCTRICOS Y TÉRMICOS

4 **RIESGOS DE CIBERSEGURIDAD EXCLUSIVOS** DEL VEHÍCULO ELÉCTRICO

5 **INFRAESTRUCTURAS DE CARGA:** TECNOLOGÍA Y COMPONENTES

6 EL PUNTO DÉBIL DEL VEHÍCULO ELÉCTRICO: **CIBERSEGURIDAD EN PUNTOS DE CARGA**

1 EL VEHÍCULO ELÉCTRICO Y SUS COMPONENTES

1. **Clasificación de los vehículos eléctricos.**
2. **Esquema general de conexiones en un vehículo eléctrico y sus elementos técnicos.**
3. **Los protocolos de redes internas.**
4. **Las ECUs de los vehículos eléctricos.**
5. **Sistemas de almacenamiento de energía.**
6. **Sistemas de carga *on-board*.**

2 NORMATIVAS DE CIBERSEGURIDAD PARA VEHÍCULOS ELÉCTRICOS

1. La UNECE/R155.
2. La norma ISO 15118.
3. La Cyber Resilience Act.

3 RIESGOS DE CIBERSEGURIDAD COMPARTIDOS EN VEHÍCULOS ELÉCTRICOS Y TÉRMICOS

1. Casos reales de ciberataques a todo tipo de vehículos.
2. Cíber-riesgos de la tecnología IoT implementada en vehículos.
3. Cíber-riesgos a través de los protocolos de redes internas.

4 RIESGOS DE CIBERSEGURIDAD EXCLUSIVOS DE LOS VEHÍCULOS ELÉCTRICOS

1. Casos reales de ataques al vehículo eléctrico y/o sus componentes.
2. Vectores de ataque contra el vehículo eléctrico.
3. Tipos de ataques específicos a los vehículos eléctricos.
4. Medidas de mitigación y protección para los vehículos eléctricos.

5 INFRAESTRUCTURAS DE CARGA: TECNOLOGÍA Y COMPONENTES

1. **Conceptos generales de las infraestructuras de carga.**
2. **Elementos que forman las infraestructuras de carga.**
3. **Legislación relevante.**
4. **Particularidades de la carga pública.**
5. **Tendencias de futuro.**
6. **Métodos de acceso: RFID, Apps, QR.**

6 EL PUNTO DÉBIL DEL VEHÍCULO ELÉCTRICO: CIBERSEGURIDAD EN PUNTOS DE CARGA

1. **Casos reales de ciberataques a los puntos de recarga.**
2. **Las *suites* de protocolos y sus riesgos conocidos.**
3. **El peligro del V2G: Los ataques *Man In The Middle*.**
4. **Tipos de crackeos contra los puntos de recarga.**
5. **Medidas de seguridad para las infraestructuras de carga.**

FORMACIÓN
GRUPO CYBENTIA

01
Matriculación
ABIERTA
Cursos mensuales

25
horas

Modalidad
híbrida

EUROCYBCAR
CYBERSECURITY TEST
En colaboración con el **Área Técnica**

Información e inscripciones Grupo CYBENTIA

660 514 710
689 315 507
formacion@cybentia.com