Catálogo de Especialidades Formativas

PROGRAMA FORMATIVO

Ciberseguridad para Vehículos

Septiembre 2021

GOBIERNO DE ESPAÑA
MINISTERIO DE TRABAJO Y ECONOMÍA SOCIAL
SERVICIO PÚBLICO DE EMPLEO ESTATAL SEPE
SISTEMA NACIONAL DE EMPLEO

IDENTIFICACIÓN DE LA ESPECIALIDAD Y PARÁMETROS DEL CONTEXTO FORMATIVO

Denominación de la especialidad:	CIBERSEGURIDAD PARA VEHÍCULOS
Familia Profesional:	INFORMÁTICA Y COMUNICACIONES
Área Profesional:	DESARROLLO
Código:	IFCD101
Nivel de cualificación profesional:	4

Objetivo general

Gestionar la ciberseguridad en diferentes unidades y sistemas de control del vehículo.

Relación de módulos de formación

Módulo 1	Movilidad inteligente (Smart mobility)	20 horas
Módulo 2	Ciberseguridad	100 horas
Módulo 3	Ciberseguridad en el vehículo conectado	100 horas
Módulo 4	Normativas, estándares y homologación en la ciberseguridad del vehículo	20 horas

Modalidades de impartición

Presencial

Duración de la formación

Duración total	240 horas

Requisitos de acceso del alumnado

Acreditaciones/ titulaciones	Cumplir como mínimo alguno de los siguientes requisitos: - Título de Grado o equivalente - Título de Postgrado (Máster) o equivalente - Título de Técnico Superior (FP Grado Superior) o equivalente de la familia profesional: Informática y Comunicaciones - Certificado de profesionalidad de nivel 3 de la familia profesional: Informática y Comunicaciones
Experiencia profesional	En caso de no disponer de las acreditaciones anteriores, se requiere experiencia profesional de 3 años, en los ámbitos de una de las titulaciones anteriores
Otros	Deben poseer conocimientos de programación de ordenadores, sistemas operativos, virtualización y bases de datos

Prescripciones de formadores y tutores

Acreditación requerida	Cumplir como mínimo alguno de los siguientes requisitos: - Licenciado, Ingeniero, Arquitecto o el Título de Grado correspondiente u otros títulos equivalentes. - Diplomado, Ingeniero Técnico, Arquitecto Técnico o el Título deGrado correspondiente u otros títulos equivalentes.
Experiencia profesional mínima requerida	Experiencia profesional mínima de tres años en las temáticas impartidas del curso
Competencia docente	Experiencia docente acreditable de al menos 60 horas en modalidad presencial.

Requisitos mínimos de espacios, instalaciones y equipamientos

Espacios formativos	Superficie m^2 para 15 participantes	Incremento Superficie/ participantes (Máximo 30 participantes)
Aula de informática	45 m^2	2,4 m^2/participante

Espacio Formativo	Equipamiento
Aula de informática	- Mesa y silla para el formador y el alumnado. - Pizarra y material de aula. - PC para el formador de las mismas características que el del alumnado. - Proyector conectado al PC del formador (*). - Pantalla de proyección (*). (*) alternativamente, pizarra digital. - Como mínimo para cada dos estudiantes, un PC instalado en red con la capacidad suficiente para ejecutar sistemas operativos, software de red, software de programación, software de bases de datos herramientas de virtualización que puedan acceder a un entorno de cloud a disposición del estudiantado. - Software licenciado en sistemas operativos, redes, sistemas gestores de bases de datos y entornos de programación. - Servicio de cloud a disposición del estudiantado, con la posibilidad de definir VPN y gateways. - Oferta de cobertura de red inalámbrica WiFi y 5G como Bluetooth. - Sistemas embebidos (software y hardware) para cada dos/tres estudiantes (ECU, BUS CAN, CAN testers y simuladores CAN). - Dispositivos móviles a disposición del alumnado para probar las aplicaciones.

La superficie de los espacios e instalaciones estarán en función de su tipología y del número de participantes. Tendrán como mínimo los metros cuadrados que se indican para 15 participantes y el equipamiento suficiente para los mismos.

En el caso de que aumente el número de participantes, hasta un máximo de 30, la superficie de las aulas se incrementará proporcionalmente (según se indica en la tabla en lo relativo a m^2/ participante) y el equipamiento estará en consonancia con dicho aumento.

No debe interpretarse que los diversos espacios formativos identificados deban diferenciarse necesariamente mediante cerramientos.

Las instalaciones y equipamientos deberán cumplir con la normativa industrial e higiénico-sanitaria correspondiente y responderán a medidas de accesibilidad y seguridad de los participantes.

En el caso de que la formación se dirija a personas con discapacidad se realizarán las adaptaciones y los ajustes razonables para asegurar su participación en condiciones de igualdad.

Ocupaciones y puestos de trabajo relacionados

- 2431 Ingenieros industriales y de producción
- 2441 Ingenieros en electricidad
- 2442 Ingenieros electrónicos
- 2443 Ingenieros en telecomunicaciones
- 3811 Técnicos en operaciones de sistemas informáticos
- 3813 Técnicos en redes
- 3820 Programadores informáticos
- 3833 Técnicos de ingeniería de las telecomunicaciones

Requisitos oficiales de las entidades o centros de formación

Estar inscrito en el Registro de entidades de formación (Servicios Públicos de Empleo)

DESARROLLO MODULAR

MÓDULO DE FORMACIÓN 1: MOVILIDAD INTELIGENTE (SMART MOBILITY)

OBJETIVO

Validar, desde el análisis y evaluación, la ciberseguridad en el vehículo conectado en un contexto de movilidad inteligente

DURACIÓN: 20 horas

RESULTADOS DE APRENDIZAJE

Conocimientos/ Capacidades cognitivas y prácticas

- Identificación de los conceptos clave en la movilidad inteligente *(smart mobility).*
  - Elementos que la movilidad inteligente aporta a la movilidad general.
  - Estrategias de movilidad inteligente en entornos urbanos y en red viaria.
  - Concepto de multi-modalidad en estrategias de movilidad inteligente.
  - Uso de packages y manejo de excepciones.

- Distinción de los conceptos relacionados con el vehículo conectado y la conectividad en el ámbito de la automoción.
  - Concepto del C2C o conectividad vehículo a vehículo.
  - Concepto del C2I o conectividad vehículo a infraestructura.
  - Necesidades y políticas de actualización de los sistemas de control del vehículo.

- Análisis de la operación del vehículo en un entorno de movilidad inteligente
  - El entorno de movilidad inteligente del vehículo conectado y sus necesidades de conectividad con otros vehículos y con la infraestructura viaria.
  - Uso del contexto de movilidad inteligente en la detección y análisis de riesgos y amenazas en los sistemas electrónicos conectados del vehículo.

Habilidades de gestión, personales y sociales

- Asimilación de los factores clave de un reto tecnológico
- Adquisición de actitudes positivas hacía la innovación en materia de las comunicaciones internas de un vehículo
- Capacidad de análisis, síntesis y prospectiva tanto individualmente como de trabajo en grupo utilizando metodologías ágiles.

MÓDULO DE FORMACIÓN 2: CIBERSEGURIDAD

OBJETIVO

Validar, desde el análisis y evaluación, las necesidades de ciberseguridad en el vehículo conectado.

DURACIÓN: 100 horas

RESULTADOS DE APRENDIZAJE

Conocimientos/ Capacidades cognitivas y prácticas

- Definición de los fundamentos de la ciberseguridad.
    - Concepto de ciberseguridad.
    - Necesidades de gestión de la ciberseguridad.
    - Conceptos de confidencialidad, integridad y autenticación.
    - Uso de packages y manejo de excepciones.

- Distinción de los conceptos de redes de ordenadores.
    - Relación de los niveles del modelo de interconexión de sistemas abierto (OSI).
    - Redes públicas y privadas.
    - Tipos de redes: WLAN, 5G, NFC; RFID, Bluetooth, WAN, MAN, LAN, PAN.
    - Características y usos de las VPN, los gateways, los routers y los firewalls.
    - Relación de los niveles de la arquitectura de redes y la conectividad.

- Formulación de criptografía en el ámbito de la movilidad inteligente.
    - Niveles de riesgos, las amenazas y los ataques a redes de dispositivos interconectados.
    - Claves simétricas y asimétricas, PKI y certificados digitales.
    - Comparación y distinción entre VPN, IDS, IPS.

- Identificación de conceptos y herramientas relevantes en ciberseguridad:
    - Formulación de la virtualización. Distinción de las características de la informática en la nube (Cloud computing) y configuración de entornos de virtualización.
    - Necesidades de ciberseguridad en dispositivos electrónicos interconectados.
    - Evaluación y validación de los requisitos de ciberseguridad.
    - Políticas de autenticación y confidencialidad.
    - Necesidades de ciberseguridad en los sistemas (operativos), servicios y aplicaciones.
    - Uso de los conocimientos de redes y de los niveles del modelo de interconexión (OSI) para identificar riesgos, amenazas y ataques que se pueden producir en un sistema interconectado.
    - Soluciones de virtualización en el análisis, evaluación y validación de la ciberseguridad.
    - Aplicación de evaluación heurística en el seguimiento de la HMI.

Habilidades de gestión, personales y sociales

- Demostración de una actitud emprendedora e innovadora en entornos cambiantes con desarrollo de nuevas ideas, proyectos y comunicación eficiente de los mismos.
- Capacidad de análisis, síntesis y prospectiva tanto individualmente como de trabajo en grupo utilizando metodologías ágiles en el ámbito de la ciberseguridad.
- Efectividad en la gestión de los recursos adecuados para llevar a cabo un proyecto de innovación complejo en el ámbito de la ciberseguridad.

MÓDULO DE FORMACIÓN 3: CIBERSEGURIDAD EN EL VEHÍCULO CONECTADO

OBJETIVO

Aplicar los conocimientos, habilidades y criterios sobre la ciberseguridad al análisis, evaluación y validación de la ciberseguridad en el vehículo conectado.

DURACIÓN: 100 horas

RESULTADOS DE APRENDIZAJE

Conocimientos/ Capacidades cognitivas y prácticas

- Relación de los conceptos en el ámbito de los sistemas operativos, las redes, los sistemas distribuidos y el desarrollo de la ciberseguridad con la planificación, el desarrollo y la evaluación de la ciberseguridad del vehículo conectado.
    - Necesidades técnicas en los diferentes tipos de redes inalámbricas (WLAN, Bluetooth, 5G) en el vehículo.
    - Sistemas embebidos (embedded systems -software y hardware-), como ECU, bus CAN, CAN tester y simuladores (CANoe, CP-tool, CANanalyzer, ODIS-tester, CANape, ICSim).
    - Ciclos de vida de las aplicaciones de los sistemas de conectividad del vehículo y su política de actualizaciones usando metodologías ágiles

- Identificación de características de la ciberseguridad en ámbitos específicos del vehículo
    - Criterios en Interacción Persona-Ordenador o Interacción Persona-Máquina (HCi y HMI).
    - Concepto de “infotainment” a los sistemas de conectividad del vehículo.
    - Niveles de ciberseguridad de los sistemas embebidos en el vehículo conectado. Evaluación y validación
    - Necesidades de gestión de la ciberseguridad en movilidad

Habilidades de gestión, personales y sociales

- Capacidad para analizar los factores relevantes de un sistema de ciberseguridad.
- Demostración de una actitud rigurosa en el seguimiento, la evaluación y la validación de los niveles de ciberseguridad
- Efectividad en la coordinación de equipos y proyectos para asegurar la ciberseguridad del conjunto del vehículo conectado

MÓDULO DE FORMACIÓN 4: NORMATIVAS, ESTÁNDARES Y HOMOLOGACIÓN EN LA CIBERSEGURIDAD DEL VEHÍCULO

OBJETIVO

Identificar y aplicar las normativas y los estándares relativos a la ciberseguridad y su homologación al vehículo conectado.

DURACIÓN: 20 horas

RESULTADOS DE APRENDIZAJE

Conocimientos/ Capacidades cognitivas y prácticas

- Identificación de la legislación, normativas y estándares relacionados con la ciberseguridad del vehículo conectado
    - Legislación y normativa sobre ciberseguridad que afecta al desarrollo, evaluación y validación de sistemas embebidos y aplicaciones para el vehículo conectado.
    - Procesos de homologación de los ensayos de ciberseguridad en vehículos conectados
- Aplicación de la normativa y homologación del sistema de ciberseguridad del vehículo conectado.
    - Requerimientos en el software y hardware
    - Posibles problemas para cumplir los requerimientos
    - Soluciones correctivas y de mitigación relacionados con aspectos de homologación
- Elaboración de los informes técnicos y de homologación de los sistemas de ciberseguridad del vehículo conectado.
    - Documentación técnica relativa a los ensayos para la homologación de los sistemas de ciberseguridad del vehículo conectado.
    - Mecanismos y criterios para detectar cambios en las normativas, en los estándares o en la legislación para mantener la información siempre actualizada.

Habilidades de gestión, personales y sociales

- Capacidad de liderazgo para identificar ensayos complejos de ciberseguridad y proponer soluciones.
- Desarrollo de actitudes responsables en la planificación para idear ensayos de ciberseguridad
- Uso de habilidades de comunicación para trabajar en equipos multidisciplinares para elaborar ensayos de homologación de sistemas de ciberseguridad.

EVALUACIÓN DEL APRENDIZAJE EN LA ACCIÓN FORMATIVA

- La evaluación tendrá un carácter teórico-práctico y se realizará de forma sistemática y continua, durante el desarrollo de cada módulo y al final del curso.
- Puede incluir una evaluación inicial de carácter diagnóstico para detectar el nivel de partida del alumnado.
- La evaluación se llevará a cabo mediante los métodos e instrumentos más adecuados para comprobar los distintos resultados de aprendizaje, y que garanticen la fiabilidad y validez de la misma.
- Cada instrumento de evaluación se acompañará de su correspondiente sistema de corrección y puntuación en el que se explicite, de forma clara e inequívoca, los criterios de medida para evaluar los resultados alcanzados por los participantes.
- La puntuación final alcanzada se expresará en términos de Apto/ No Apto.