SUPLEMENTO EUROPASS AL CERTIFICADO DEL CURSO DE ESPECIALIZACIÓN DE GRADO SUPERIOR

DENOMINACIÓN DEL CURSO DE ESPECIALIZACIÓN

Curso de especialización de Grado Superior de Formación Profesional en Ciberseguridad en entornos de las tecnologías de la información

DESCRIPCIÓN DEL CURSO DE ESPECIALIZACIÓN

El titular tiene adquirida la competencia general relativa a:
Definir e implementar estrategias de seguridad en los sistemas de información realizando diagnósticos de ciberseguridad, identificando vulnerabilidades e implementando las medidas necesarias para mitigarlas aplicando la normativa vigente y estándares del sector, siguiendo los protocolos de calidad, de prevención de riesgos laborales y respeto ambiental.

En este marco, cada MÓDULO PROFESIONAL incluye los siguientes RESULTADOS DE APRENDIZAJE adquiridos por el titular.

"Incidentes de ciberseguridad".
El titular:
- Desarrolla planes de prevención y concienciación en ciberseguridad, estableciendo normas y medidas de protección.
- Analiza incidentes de ciberseguridad utilizando herramientas, mecanismos de detección y alertas de seguridad.
- Investiga incidentes de ciberseguridad analizando los riesgos implicados y definiendo las posibles medidas a adoptar.
- Implementa medidas de ciberseguridad en redes y sistemas respondiendo a los incidentes detectados y aplicando las técnicas de protección adecuadas.
- Detecta y documenta incidentes de ciberseguridad siguiendo procedimientos de actuación establecidos.

"Bastionado de redes y sistemas".
El titular:
- Diseña planes de securización incorporando buenas prácticas para el bastionado de sistemas y redes.
- Configura sistemas de control de acceso y autenticación de personas preservando la confidencialidad y privacidad de los datos.
- Administra credenciales de acceso a sistemas informáticos aplicando los requisitos de funcionamiento y seguridad establecidos.
- Diseña redes de computadores contemplando los requisitos de seguridad.
- Configura dispositivos y sistemas informáticos cumpliendo los requisitos de seguridad.
- Configura dispositivos para la instalación de sistemas informáticos minimizando las probabilidades de exposición a ataques.
- Configura sistemas informáticos minimizando las probabilidades de exposición a ataques.

"Puesta en producción segura".
El titular:
- Prueba aplicaciones web y aplicaciones para dispositivos móviles analizando la estructura del código y su modelo de ejecución.
- Determina el nivel de seguridad requerido por aplicaciones identificando los vectores de ataque habituales y sus riesgos asociados.
- Detecta y corrige vulnerabilidades de aplicaciones web analizando su código fuente y configurando servidores web.
- Detecta problemas de seguridad en las aplicaciones para dispositivos móviles, monitorizando su ejecución y analizando ficheros y datos.
- Implanta sistemas seguros de desplegado de software, utilizando herramientas para la automatización de la construcción de sus elementos.

“Análisis forense informático.”.
El titular:

- Aplica metodologías de análisis forense caracterizando las fases de preservación, adquisición, análisis y documentación.
- Realiza análisis forenses en dispositivos móviles, aplicando metodologías establecidas, actualizadas y reconocidas.
- Realiza análisis forenses en Cloud, aplicando metodologías establecidas, actualizadas y reconocidas.
- Realiza análisis forense en dispositivos del IoT, aplicando metodologías establecidas, actualizadas y reconocidas.
- Documenta análisis forenses elaborando informes que incluyan la normativa aplicable.

“Hacking ético”.
El titular:

- Determina herramientas de monitorización para detectar vulnerabilidades aplicando técnicas de hacking ético.
- Ataca y defiende en entornos de prueba, comunicaciones inalámbricas consiguiendo acceso a redes para demostrar sus vulnerabilidades.
- Ataca y defiende en entornos de prueba, redes y sistemas consiguiendo acceso a información y sistemas de terceros.
- Consolida y utiliza sistemas comprometidos garantizando accesos futuros.
- Ataca y defiende en entornos de prueba, aplicaciones web consiguiendo acceso a datos o funcionalidades no autorizadas.

“Normativa de ciberseguridad”.
El titular:

- Identifica los puntos principales de aplicación para asegurar el cumplimiento normativo reconociendo funciones y responsabilidades.
- Diseña sistemas de cumplimiento normativo seleccionando la legislación y jurisprudencia de aplicación.
- Relaciona la normativa relevante para el cumplimiento de la responsabilidad penal de las organizaciones y personas jurídicas con los procedimientos establecidos, recopilando y aplicando las normas vigentes.
- Aplica la legislación nacional de protección de datos de carácter personal, relacionando los procedimientos establecidos con las leyes vigentes y con la jurisprudencia existente sobre la materia.
- Recopila y aplica la normativa vigente de ciberseguridad de ámbito nacional e internacional, actualizando los procedimientos establecidos de acuerdo con las leyes y con la jurisprudencia existente sobre la materia.

EMPLEOS QUE SE PUEDEN DESEMPEÑAR CON ESTE CURSO DE ESPECIALIZACIÓN

Las ocupaciones y puestos de trabajo más relevantes son los siguientes:

- Experto en ciberseguridad.
- Auditor de ciberseguridad.
- Consultor de ciberseguridad.
- Hacker ético.

EXPEDICIÓN, ACREDITACIÓN Y NIVEL DEL CERTIFICADO

Organismo que expide el certificado del curso de especialización de grado superior en nombre del Rey: Ministerio de Educación y Formación Profesional o las comunidades autónomas en el ámbito de sus competencias propias. El certificado tiene efectos académicos y profesionales con validez en todo el Estado.

Duración oficial del curso: 720 horas.

Nivel del certificado (nacional o internacional).

- NACIONAL: Educación superior no universitaria.
- INTERNACIONAL:
  - Nivel P-5.5.4 de la Clasificación Internacional Normalizada de la Educación (CINE P-5.5.4).
  - Nivel 5C del Marco Europeo de las Cualificaciones (EQF 5C).

Requisitos de acceso: Para acceder al curso de especialización es necesario estar en posesión de alguno de los siguientes títulos de Formación Profesional de Grado Superior:

a) Técnico Superior en Administración de Sistemas Informáticos en Red establecido por el Real Decreto 1629/2009, de 30 de octubre.
b) Técnico Superior en Desarrollo de Aplicaciones Multiplataforma, establecido por el Real Decreto 450/2010, de 16 de abril.
c) Técnico Superior en Desarrollo de Aplicaciones Web, establecido por el Real Decreto 686/2010, de 20 de mayo.
d) Técnico Superior en Sistemas de Telecomunicaciones e Informáticos, establecido por el Real Decreto 883/2011, de 24 de junio.
e) Técnico Superior en Mantenimiento Electrónico, establecido por el Real Decreto 1578/2011, de 4 de noviembre.

Base Legal. Normativa por la que se establece el curso de especialización en Ciberseguridad en entornos de las tecnologías de la información:
Enseñanzas mínimas establecidas por el Estado: Real Decreto 479/2020, de 7 de abril, por el que se establece el Curso de especialización en ciberseguridad en entornos de las tecnologías de la información y se fijan los aspectos básicos del currículo.

Nota explicativa: Este documento está concebido como información adicional al título en cuestión, pero no tiene por sí mismo validez jurídica alguna.

FORMACIÓN DEL CURSO DE ESPECIALIZACIÓN OFICIALMENTE RECONOCIDO

MÓDULOS PROFESIONALES DEL REAL DECRETO DEL CURSO DE ESPECIALIZACIÓN DE GRADO SUPERIOR	**CRÉDITOS ECTS**
Incidentes de ciberseguridad.	9
Bastionado de redes y sistemas.	10
Puesta en producción segura.	7
Análisis forense informático.	7
Hacking ético.	7
Normativa de ciberseguridad	3
	TOTAL CRÉDITOS
	43
DURACIÓN OFICIAL DEL CERTIFICADO DEL CURSO DE ESPECIALIZACIÓN (HORAS)	***720***

* Las enseñanzas mínimas del curso de especialización reflejadas en la tabla anterior, 50%, son de carácter oficial y con validez en todo el territorio nacional. El 50% restante pertenece a cada Comunidad Autónoma y se podrá reflejar en el **Anexo I** de este suplemento.

europass

INFORMACIÓN SOBRE EL SISTEMA EDUCATIVO