CURSO ESPECIALIZACIÓN IFCE01

Curso de especialización en ciberseguridad en entornos de las tecnologías y la información

INFORMÁTICA Y COMUNICACIONES

Competencia general:

La competencia general de este curso de especialización consiste en 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.

Duración:

720 horas: 1 curso académico.

Plan de estudios:

Módulos profesionales		*Créditos ECTS*	*Duración (horas)*	*Carga lectiva semanal (horas)*
Código	*Denominación*			
5021	Incidentes en ciberseguridad.	9	80	2
5022	Bastionado de redes y sistemas.	10	210	6
5023	Puesta en producción segura.	7	140	4
5024	Análisis forense informático.	7	110	3
5025	Hacking ético.	7	140	4
5026	Normativa de ciberseguridad.	3	40	1

Requisitos de acceso:

Para acceder al curso de especialización en ciberseguridad en entornos de las tecnologías de la información es necesario estar en posesión de alguno de los siguientes títulos:

a) Técnico Superior en Administración de Sistemas Informáticos en Red.
b) Técnico Superior en Desarrollo de Aplicaciones Multiplataforma.
c) Técnico Superior en Desarrollo de Aplicaciones Web.
d) Técnico Superior en Sistemas de Telecomunicaciones e Informáticos.
e) Técnico Superior en Mantenimiento Electrónico.

Referencia legislativa:

Enseñanzas Mínimas del Título:
Real Decreto 479/2020, de 7 de abril (BOE 13.05.2020), modificado por Real Decreto 261/2021, de 13 de abril- D.F. 4ª (BOE 07.05.2021)

Currículo de la Comunidad de Madrid:
Decreto 201/2021, de 1 de septiembre (BOCM 08.09.2021)

CURSO ESPECIALIZACIÓN IFCE01

Curso de especialización en ciberseguridad en entornos de las tecnologías y la información

INFORMÁTICA Y COMUNICACIONES

Entorno profesional:

Este profesional ejercerá su actividad en entidades de los sectores donde sea necesario establecer mecanismos y medidas para la protección de los sistemas de información y redes de comunicaciones.

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

a) Experto en ciberseguridad.
b) Auditor de ciberseguridad.
c) Consultor de ciberseguridad.
d) Hacker ético.

Competencias profesionales:

a) Elaborar e implementar planes de prevención y concienciación en ciberseguridad en la organización, aplicando la normativa vigente.
b) Detectar e investigar incidentes de ciberseguridad, documentándolos e incluyéndolos en los planes de securización de la organización.
c) Diseñar planes de securización contemplando las mejores prácticas para el bastionado de sistemas y redes.
d) Configurar sistemas de control de acceso y autenticación en sistemas informáticos, cumpliendo los requisitos de seguridad y minimizando las posibilidades de exposición a ataques.
e) Diseñar y administrar sistemas informáticos en red y aplicar las políticas de seguridad establecidas, garantizando la funcionalidad requerida con un nivel de riesgo controlado.
f) Analizar el nivel de seguridad requerido por las aplicaciones y los vectores de ataque más habituales, evitando incidentes de ciberseguridad.
g) Implantar sistemas seguros de desplegado de software con la adecuada coordinación entre los desarrolladores y los responsables de la operación del software.
h) Realizar análisis forenses informáticos analizando y registrando la información relevante relacionada.
i) Detectar vulnerabilidades en sistemas, redes y aplicaciones, evaluando los riesgos asociados.
j) Definir y aplicar procedimientos para el cumplimiento normativo en materia de ciberseguridad y de protección de datos personales, implementándolos tanto internamente como en relación con terceros.
k) Elaborar documentación técnica y administrativa cumpliendo con la legislación vigente, respondiendo a los requisitos establecidos.
l) Adaptarse a las nuevas situaciones laborales, manteniendo actualizados los conocimientos científicos, técnicos y tecnológicos relativos a su entorno profesional, gestionando su formación y los recursos existentes en el aprendizaje a lo largo de la vida.
m) Resolver situaciones, problemas o contingencias con iniciativa y autonomía en el ámbito de su competencia, con creatividad, innovación y espíritu de mejora en el trabajo personal y en el de los miembros del equipo.
n) Generar entornos seguros en el desarrollo de su trabajo y el de su equipo, supervisando y aplicando los procedimientos de prevención de riesgos laborales y ambientales, de acuerdo con lo establecido por la normativa y los objetivos de la organización.
ñ) Supervisar y aplicar procedimientos de gestión de calidad, de accesibilidad universal y de «diseño para todas las personas», en las actividades profesionales incluidas en los procesos de producción o prestación de servicios.