

¿CUÁLES SON LAS SALIDAS PROFESIONALES?

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.

DURACIÓN DEL CURSO

720 HORAS
DESDE OCTUBRE.



SOLICITUD DE PLAZA

MES DE JULIO.

MATRÍCULAS

MES DE SEPTIEMBRE.



IES 50 SAN VICENTE
C/ Lillo Juan, 128 · 03690 San Vicente
☎ 965 93 65 05
www.iessanvicente.com

 **Unió Europea**
Fons Social Europeu
L'FSE inverteix en el teu futur



 **GENERALITAT VALENCIANA**
Conselleria d'Educació,
Cultura i Esport

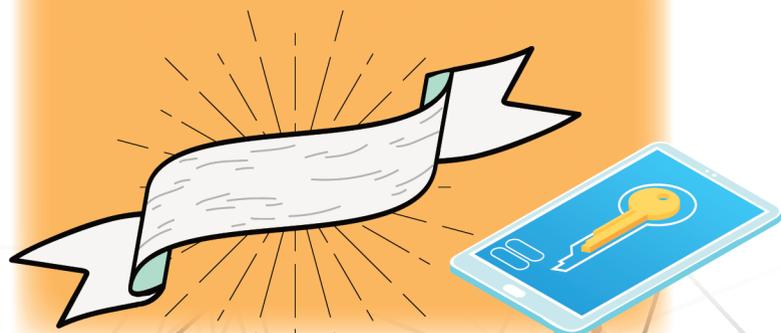


CURSO DE ESPECIALIZACIÓN
en **Ciberseguridad**
en **Entornos de las**
Tecnologías de la
Información

REQUISITOS DE ACCESO

Los títulos que dan acceso a este curso de especialización son los siguientes:

- Título de Técnico Superior en Administración de Sistemas Informáticos en Red.
- Título de Técnico Superior en Desarrollo de Aplicaciones Multiplataforma.
- Título de Técnico Superior en Desarrollo de Aplicaciones Web.
- Título de Técnico Superior en Sistemas de Telecomunicaciones e Informáticos.
- Título de Técnico Superior en Mantenimiento Electrónico.



¿QUÉ VOY A APRENDER Y HACER?

- Elaborar e implementar planes de prevención y concienciación en ciberseguridad en la organización, aplicando la normativa vigente.
- Detectar e investigar incidentes de ciberseguridad, documentándolos e incluyéndolos en los planes de securización de la organización.
- Diseñar planes de securización contemplando las mejores prácticas para el bastionado de sistemas y redes.
- Configurar sistemas de control de acceso y autenticación en sistemas informáticos, cumpliendo los requisitos de seguridad y minimizando las posibilidades de exposición a ataques.
- Diseñar y administrar sistemas informáticos en red y aplicar las políticas de seguridad establecidas, garantizando la funcionalidad requerida con un nivel de riesgo controlado.
- Analizar el nivel de seguridad requerido por las aplicaciones y los vectores de ataque más habituales, evitando incidentes de ciberseguridad.
- Implantar sistemas seguros de despliegado de software con la adecuada coordinación entre los desarrolladores y los responsables de la operación del software.
- Realizar análisis forenses informáticos analizando y registrando la información relevante relacionada.
- Detectar vulnerabilidades en sistemas, redes y aplicaciones, evaluando los riesgos asociados.
- 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.
- Elaborar documentación técnica y administrativa cumpliendo con la legislación vigente, respondiendo a los requisitos establecidos.

PLAN DE FORMACIÓN

Los módulos profesionales de este ciclo formativo son los siguientes:

- Incidentes de ciberseguridad.
- Bastionado de redes y sistemas.
- Puesta en producción segura.
- Análisis forense informático.
- Hacking ético.
- Normativa de ciberseguridad.



AL FINALIZAR MIS ESTUDIOS, ¿QUÉ PUEDO HACER?

Trabajar como:

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

