Informática y Comunicaciones

REQUISITOS DE ACCESO

Para acceder a este curso de especialización es necesario estar en posesión de alguno de los siguientes títulos:

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

Curso de especialización

CIBERSEGURIDAD EN ENTORNOS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

OCUPACIONES Y PUESTOS DE TRABAJO

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

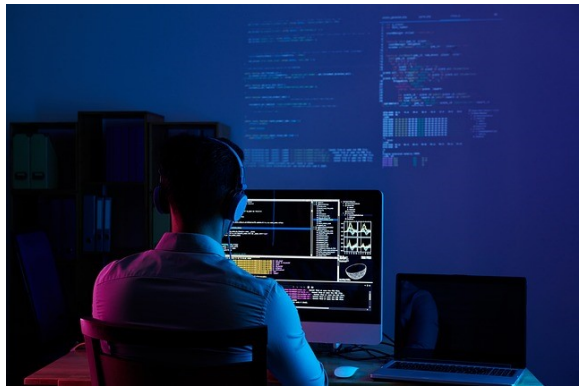
Formación Profesional de La Rioja | Gobierno de La Rioja

IES COMERCIO

NOVEDAD CURSO 2024-2025

CURSO DE ESPECIALIZACIÓN

CIBERSEGURIDAD EN ENTORNOS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN



IES COMERCIO

Paseo del Prior, 97
26004 Logroño
Teléfonos: 941 25 69 57 - 941 23 39 80
e-mail: informatica@iescomercio.com
Web: iescomercio.com/informatica

PERFIL PROFESIONAL

COMPETENCIA GENERAL

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.

IES COMERCIO

Curso de especialización

Ciberseguridad en Entornos de las Tecnologías de la Información

1 CURSO ACADÉMICO

720 HORAS

DE OCTUBRE A MAYO

HORARIO VESPERTINO

Módulos profesionales	Horas	Horas / semana
INCIDENTES DE CIBERSEGURIDAD	140	6
BASTIONADO DE REDES Y SISTEMAS	170	7
PUESTA EN PRODUCCIÓN SEGURA	120	5
ANÁLISIS FORENSE INFORMÁTICO	120	5
HACKING ÉTICO	120	5
NORMATIVA DE CIBERSEGURIDAD	50	2

COMPETENCIAS PROFESIONALES

- Elaborar e implementar planes de prevención y concienciación en ciberseguridad en la organización, aplicando la normativa vigente.
- 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 desplegado de software con la adecuada coordinación entre los desarrolladores y los responsables de la operación del software.
- 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.
- 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.
- 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.