



## CIBERSEGURIDAD EN ENTORNOS DE LAS TECNOLOGÍAS DE OPERACIÓN

Duración: 720 horas

### Competencia general:

La competencia general de este curso de especialización consiste en definir e implementar estrategias de seguridad en las organizaciones e infraestructuras industriales realizando diagnósticos de ciberseguridad, identificando vulnerabilidad 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

### Plan de formación:

La formación se realizará en el **centro educativo**, a través de una formación teórico-práctica.

Los contenidos se agrupan en los siguientes **módulos profesionales**:

- 5027 Ciberseguridad en proyectos industriales (120h)
- 5028 Sistemas de control industrial seguros (120h)
- 5029 Redes de comunicaciones industriales seguras (150h)
- 5030 Análisis forense en ciberseguridad industrial (180h)
- 5031 Seguridad integral (150h)

### Títulos que dan acceso a este Curso:

- ✔ Título de Técnico Superior en Automatización y Robótica Industrial.
- ✔ Título de Técnico Superior en Mecatrónica Industrial.
- ✔ Título de Técnico Superior en Sistemas de Telecomunicaciones e Informáticos.
- ✔ Título de Técnico Superior en Sistemas Electrotécnicos y Automatizados.
- ✔ Título de Técnico Superior en Mantenimiento Electrónico.

### Horario:

Por la tarde de lunes a jueves de 17:20 a 22:00 h.

### Orientación en Formación Profesional y visitas:

[03001911.orientafp@edu.gva.es](mailto:03001911.orientafp@edu.gva.es)

### IES Antonio José Cavanilles

Av. Alcalde Lorenzo Carbonell 32-34

03007 ALICANTE

Teléfono: 965 936 500

<https://cavanilles.edu.es>



### Entorno profesional:

Las personas que hayan obtenido el certificado que acredita la superación de este curso de especialización podrán ejercer su actividad en organizaciones de distintos sectores, donde sea necesario establecer y garantizar la seguridad de los procesos industriales que desarrollan.

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

- ✔ Experto en ciberseguridad en entornos de la operación.
- ✔ Auditor de ciberseguridad en entornos de la operación.
- ✔ Consultor de ciberseguridad en entornos de la operación.
- ✔ Analista de ciberseguridad en entornos de la operación.

### ¿Qué voy a aprender y hacer?

- ✔ Determinar perfiles de riesgo de las organizaciones identificando buenas prácticas, estándares y normativa aplicable.
- ✔ Verificar alineación de los equipos y sistemas de las organizaciones en relación a los principios de la seguridad informática y de los riesgos de ciberseguridad.
- ✔ Elaborar informes de ciberseguridad relativos a sistemas y entornos industriales tanto nivel técnico y organizativo evaluando los elementos de seguridad desplegados.
- ✔ Aplicar estrategias de ciberseguridad en las fases de los proyectos industriales para minimizar el impacto de cualquier posible incidente.
- ✔ Caracterizar la evolución de los sistemas de control industrial valorando su impacto en la organización.
- ✔ Establecer la configuración de sistemas de control industrial minimizando los riesgos de la organización.
- ✔ Aplicar las metodologías reconocidas en el sector valorando los escenarios de riesgo tecnológico en redes industriales.
- ✔ Identificar vulnerabilidades y establecer la configuración de dispositivos de redes minimizando los escenarios de riesgo.
- ✔ Realizar análisis forenses en sistemas y redes industriales detectando vulnerabilidades en la organización.
- ✔ Integrar las normas y procedimientos de seguridad física, operacional y de ciberseguridad.