Guía Docente

Curso de formación permanente de especialización en Ciberseguridad en Entornos de las Tecnologías de Operación

Versión: 1.5

talenthia
FORMACIÓN

Datos generales del curso

Título completo

Cursos de formación permanente de especialización en Ciberseguridad en Entornos de las Tecnologías de Operación

Modalidad

100 % online

Duración total

500 horas (20 semanas – 5 meses)

ECTS equivalentes

20 créditos ECTS

Información adicional

- **Idioma:** Español
- **Centro responsable:** Talenthia Formación
- **Fecha de inicio:** Convocatorias abiertas en septiembre y enero

01

Calendario

4 módulos compuestos por 5 unidades cada módulo

02

Estructura

20 unidades didácticas complementadas con podcast, foros de trabajo y reflexión, clases online en directo, casos prácticos, cuestionarios, actividad final de curso

Presentación del curso

La ciberseguridad industrial se ha convertido en uno de los pilares críticos para garantizar la resiliencia, la continuidad y la seguridad de los procesos productivos en España y en Europa. La digitalización de la industria, la integración del Industrial Internet of Things (IIoT), la virtualización de sistemas SCADA y la convergencia entre IT y OT han ampliado de manera exponencial la superficie de ataque en entornos de producción, transporte, energía, agua, salud o logística.

La especialización en Ciberseguridad en Entornos de Tecnologías de Operación (OT) ofrece un itinerario formativo riguroso, actualizado y completamente homologable, alineado con los módulos oficiales recogidos en el BOE. El alumno recorrerá todos los aspectos clave de la seguridad OT: desde los fundamentos, la normativa y la gestión de riesgos, hasta la protección de sistemas de control industrial (ICS), la seguridad en redes industriales cableadas e inalámbricas, y la respuesta forense ante incidentes críticos.

Valor añadido Talenthia:

Contenidos adaptados al estado más reciente del sector, incluyendo Zero Trust aplicado a OT, microsegmentación avanzada, LTE/5G privado, virtualización segura de SCADA y uso de IA para detección de anomalías.

Enfoque práctico y operativo, con ejemplos de entornos industriales reales en España y Europa.

Orientación a cumplimiento normativo (IEC 62443, NIST SP 800-82, ENS, ISO 27001/27019), garantizando empleabilidad y homologación.

Metodología online flexible, actividades prácticas, tutorías y webinars con expertos en activo en ciberseguridad OT.

Con esta especialización, el alumno se posiciona en un área con altísima demanda profesional, preparado para asumir responsabilidades en la protección de sistemas industriales e infraestructuras críticas.

Objetivos del curso

Objetivo general

Capacitar al alumno para diseñar, implantar, auditar y gestionar planes de ciberseguridad en entornos de Tecnologías de Operación, integrando normativas, tecnologías y procesos para garantizar operaciones industriales seguras y resilientes.

Objetivos específicos

- Comprender el ecosistema OT, su arquitectura y diferencias respecto a IT.
- Aplicar marcos normativos y estándares reconocidos (IEC 62443, NIST, ENS, ISO).
- Realizar análisis de riesgos específicos en proyectos industriales.
- Diseñar arquitecturas OT seguras aplicando defensa en profundidad y Zero Trust.
- Ejecutar hardening en sistemas de control (PLC, SCADA, DCS, RTU).
- Implementar medidas de seguridad en redes industriales cableadas e inalámbricas.
- Gestionar accesos y conexiones remotas de forma segura.
- Operar herramientas de monitorización y detección de anomalías en OT.
- Participar en la gestión forense de incidentes y planes de continuidad.

Público destinatario

Perfil de acceso recomendado:

Profesionales en activo de planta industrial, mantenimiento, automatización, redes y telecomunicaciones.

Técnicos de ciberseguridad, calidad, cumplimiento y continuidad de negocio.

Recién titulados en ciclos formativos de informática y comunicaciones, electricidad y electrónica, instalación y mantenimiento e industrias afines.

Desempleados que deseen especializarse en un ámbito con alta empleabilidad.

Requisitos previos

Conocimientos básicos de redes y sistemas.
Experiencia previa en entornos industriales: recomendable, no obligatoria.

Resultados de aprendizaje

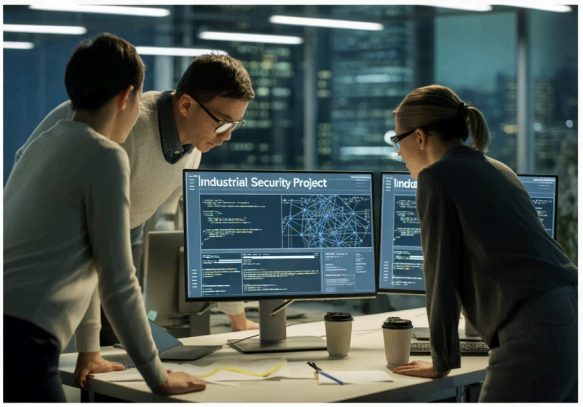
Al finalizar el curso, **el alumno será capaz de:**

- Analizar arquitecturas OT, activos críticos y riesgos asociados.
- Configurar y proteger sistemas de control industrial (ICS).
- Implantar medidas de seguridad en redes industriales, segmentadas y resilientes.
- Elaborar planes de continuidad y recuperación post-incidente.
- Proteger redes inalámbricas industriales y accesos remotos.
- Gestionar eventos de seguridad, monitorizar anomalías y responder a incidentes.
- Colaborar en la recogida de evidencias y análisis forense en entornos industriales.

Competencias a adquirir

Transversales

- Pensamiento crítico y resolución de problemas.
- Competencia digital avanzada en seguridad industrial.
- Trabajo autónomo y colaborativo en proyectos.
- Comunicación técnica y gestión documental.



Específicas (con valor añadido Talenthia)

- Diseño de arquitecturas seguras OT aplicando Zero Trust y defensa en profundidad.
- Hardening y operación segura de PLC, SCADA, DCS y RTU.
- Segmentación y microsegmentación en redes OT, integración de SDN y 5G privado.
- Implantación de sistemas de monitorización OT (IDS/IPS industriales, SIEM, detección con IA).
- Metodologías forenses OT y planes de continuidad ante incidentes críticos.

Contenidos / Programa formativo

El curso se compone de **4 módulos y 20 unidades didácticas**, cada unidad equivale a 25 horas.

Módulo 1 – Fundamentos y Gestión de la Ciberseguridad en Proyectos Industriales

- Unidad 1: Introducción a la ciberseguridad en entornos OT y convergencia IT/OT
- Unidad 2: Normativa, estándares y marcos regulatorios aplicados a entornos industriales
- Unidad 3: Identificación y evaluación de riesgos en proyectos industriales
- Unidad 4: Diseño seguro de infraestructuras y modelos Zero Trust en OT
- Unidad 5: Cultura de ciberseguridad y gestión del factor humano

Módulo 2 – Seguridad en Sistemas de Control Industrial

- Unidad 1: Arquitectura y componentes de sistemas ICS (PLC, SCADA, DCS, RTU)
- Unidad 2: Vulnerabilidades y amenazas en sistemas de control industrial
- Unidad 3: Configuración segura y hardening de dispositivos y software industrial
- Unidad 4: Gestión de actualizaciones, parches y backups en entornos ICS
- Unidad 5: Integración segura de IIoT, virtualización y dispositivos inteligentes en la industria

Módulo 3 – Redes de Comunicaciones Industriales Seguras

- Unidad 1: Protocolos y topologías de redes industriales y sus variantes seguras
- Unidad 2: Segmentación de red, zonas de seguridad y microsegmentación en entornos OT
- Unidad 3: Ciberseguridad en redes inalámbricas industriales (Wi-Fi, WirelessHART, LTE/5G privado)
- Unidad 4: Control de accesos, autenticación y acceso remoto seguro
- Unidad 5: Monitorización, auditoría y detección de anomalías con herramientas avanzadas e IA

Contenidos / Programa formativo

Módulo 4 – Análisis Forense y Respuesta ante Incidentes en OT

- Unidad 1: Principios del análisis forense en entornos industriales y marco legal
- Unidad 2: Obtención y preservación de evidencias en sistemas OT
- Unidad 3: Herramientas y metodologías forenses aplicadas a ICS y redes industriales
- Unidad 4: Reconstrucción de incidentes, análisis de causa raíz y uso de Threat Intelligence
- Unidad 5: Planes de recuperación, continuidad de negocio y evaluación post-incidente

Metodología docente

Modalidad 100% online en campus Moodle.

Material didáctico: PDF teóricos, podcasts introductorios, recursos visuales y bibliografía oficial.

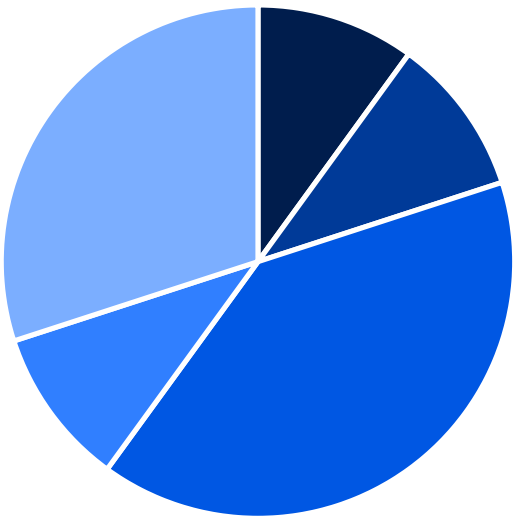
Tutorías semanales personalizadas y programadas online. Webinars con expertos. Soporte docente especializado.

Uso de simuladores, capturas de tráfico OT, plantillas de hardening y guías de respuesta a incidentes.

Actividades por unidad:

- Foros de trabajo y reflexión crítica.
- Casos prácticos entregables.
- Actividades autoevaluables.

Sistema de evaluación



Criterios de superación: obtener al menos un 70 % de la puntuación total de cada Resultado de Aprendizaje.

Profesorado / Equipo docente

Equipo de Talenthia Formación formado por profesionales en activo en ciberseguridad OT, redes industriales y sistemas de control.

Coordinador académico:

Especialista en ciberseguridad industrial y cumplimiento normativo.

Profesorado invitado:

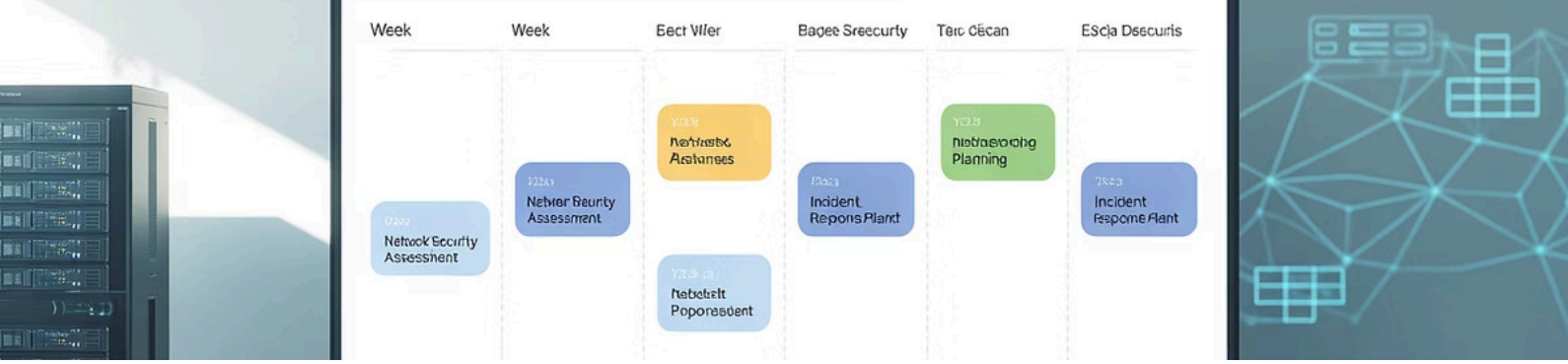
Expertos en ICS/SCADA, microsegmentación, acceso remoto seguro, Threat Intelligence OT y análisis forense.

Salidas profesionales

El egresado podrá **desempeñar funciones** como:

- Técnico/a de ciberseguridad OT
- Especialista en seguridad de sistemas de control industrial (ICS/SCADA)
- Consultor/a en arquitecturas seguras OT
- Analista SOC especializado en redes industriales
- Especialista en respuesta a incidentes y análisis forense OT
- Responsable de auditoría y cumplimiento en ciberseguridad industrial

Sectores con alta demanda: energía, agua, transporte, salud, manufactura, químico-farmacéutico, alimentación y servicios críticos.



Cronograma del curso

Semanas 1–5: Módulo 1 – Fundamentos y Gestión de la Ciberseguridad en Proyectos Industriales

Semana 1

1

Foro de Bienvenida + Prueba inicial de conocimientos + Unidad 1 + podcast + foro de trabajo y reflexión + clase online en directo + actividad evaluable + cuestionario + caso práctico

Semana 2

2

Unidad 2 + podcast + foro de trabajo y reflexión + clase online en directo + actividad evaluable + cuestionario + caso práctico

Semana 3

3

Unidad 3 + podcast + foro de trabajo y reflexión + clase online en directo + actividad evaluable + cuestionario + caso práctico

Semana 4

4

Unidad 4 + podcast + foro de trabajo y reflexión + clase online en directo + actividad evaluable + cuestionario + caso práctico

Semana 5

5

Unidad 5 + podcast + foro de trabajo y reflexión + clase online en directo + actividad evaluable + cuestionario + caso práctico

Cronograma del curso

Semanas 6–10: Módulo 2 – Seguridad en Sistemas de Control Industrial

Semana 6

Unidad 1 + podcast + foro de trabajo y reflexión + clase online en directo + actividad evaluable + cuestionario + caso práctico

Semana 7

Unidad 2 + podcast + foro de trabajo y reflexión + clase online en directo + actividad evaluable + cuestionario + caso práctico

Semana 8

Unidad 3 + podcast + foro de trabajo y reflexión + clase online en directo + actividad evaluable + cuestionario + caso práctico

Semana 9

Unidad 4 + podcast + foro de trabajo y reflexión + clase online en directo + actividad evaluable + cuestionario + caso práctico

Semana 10

Unidad 5 + podcast + foro de trabajo y reflexión + clase online en directo + actividad evaluable + cuestionario + caso práctico

Estructura semanal común

Cada semana del curso sigue una estructura similar que incluye contenido teórico, actividades prácticas, interacción en foros y evaluación continua, garantizando un aprendizaje progresivo y completo.

Cronograma del curso

Semanas 11–15: Módulo 3 – Redes de Comunicaciones Industriales Seguras

Semana 11

1

Unidad 1 + podcast + foro de trabajo y reflexión + clase online en directo + actividad evaluable + cuestionario + caso práctico

Semana 12

2

Unidad 2 + podcast + foro de trabajo y reflexión + clase online en directo + actividad evaluable+ cuestionario + caso práctico

Semana 13

3

Unidad 3 + podcast + foro de trabajo y reflexión + clase online en directo + actividad evaluable + cuestionario + caso práctico

Semana 14

4

Unidad 4 + podcast + foro de trabajo y reflexión + clase online en directo + actividad evaluable + cuestionario + caso práctico

Semana 15

5

Unidad 5 + podcast + foro de trabajo y reflexión + clase online en directo + actividad evaluable + cuestionario + caso práctico

Cada semana sigue una estructura consistente que incluye contenido teórico, actividades prácticas y evaluación, garantizando un aprendizaje progresivo y completo de las competencias en seguridad de redes industriales.

Cronograma del curso

Semanas 16–20: Módulo 4 – Análisis Forense y Respuesta ante Incidentes en OT

Semana 16

1

Unidad 1 + podcast + foro de trabajo y reflexión + clase online en directo + actividad evaluable + cuestionario + caso práctico

Semana 17

2

Unidad 2 + podcast + foro de trabajo y reflexión + clase online en directo + actividad evaluable + cuestionario + caso práctico

Semana 18

3

Unidad 3 + podcast + foro de trabajo y reflexión + clase online en directo + actividad evaluable + cuestionario + caso práctico

Semana 19

4

Unidad 4 + podcast + foro de trabajo y reflexión + clase online en directo + actividad evaluable + cuestionario + caso práctico

Semana 20

5

Unidad 5 + podcast + foro de trabajo y reflexión + clase online en directo + caso práctico + cuestionario + caso práctico + Actividad final de curso + encuesta de satisfacción + vídeo de despedida + foro de agradecimientos y despedida

La semana 20 incluye actividades de cierre y evaluación final que permiten al estudiante demostrar las competencias adquiridas a lo largo de todo el curso.

Bibliografía y recursos

Básica

1. IEC/ISA 62443 – Ciberseguridad para sistemas de automatización y control industrial.
2. NIST SP 800-82 Rev. 2 – Guide to Industrial Control Systems Security.
3. ISO/IEC 27001 y 27019 – Gestión y seguridad de la información en sector energía.
4. Esquema Nacional de Seguridad (ENS) – Guías CCN-CERT.
5. INCIBE-CERT – Buenas prácticas de seguridad OT.

Complementaria

1. CISA ICS Advisories – Alertas y mitigaciones para ICS.
2. Documentación oficial OPC UA, Modbus/TCP seguro, DNP3 seguro.
3. Guías de Zero Trust en entornos OT y segmentación avanzada.
4. Recursos sobre IA aplicada a detección de anomalías en redes industriales.