Prueba Programa Executive: Ciberseguridad Industrial | ONLINE ¡Promo ESPECIAL!

NUEVO Programa AEC Executive -20% todos | -35% socios | -50% desempleados y autónomos con baja actividad

Modalidad	Duración	Precio	Precio socio	Inicio / Fin	Lugar
Online	60 horas	595,00€ + I.V.A.	475,00€ + I.V.A.	31/10/2025 26/12/2025	AEC

-20% TODOS | -35% SOCIOS | -50% DESEMPLEADOS Y AUTÓNOMOS CON BAJA ACTIVIDAD

*Los descuentos correspondientes a esta campaña se aplicarán en factura. Descuentos no acumulables.

Descuentos especiales a partir de la 2ª inscripción corporativa: consulte condiciones.
Bonificación máxima FUNDAE: 450€

FINALIDAD

CONOCE LAS CLAVES PARA DISEÑAR LA ESTRATEGIA DE CIBERSEGURIDAD DE TU INDUSTRIA

Conocer los **riesgos y amenazas** que las infraestructuras críticas y el intercambio de datos suponen para una organización es un elemento clave para aprender a proteger sus infraestructuras y servicios esenciales. Para ello, hemos de aprender los términos y conceptos de la **Industria 4.0** y su impacto en los **Sistemas de Información y las Tecnologías de Automatización Industrial.**

Los participantes aprenderán sobre las últimas **tendencias** en ciberseguridad industrial, mejores **prácticas** y cómo aplicarlas en el diseño de su propia estrategia de Ciberseguridad en el entorno industrial.

Este programa está diseñado para concienciar a aquellas personas que desarrollan roles en la **Alta Dirección, Ejecutivos** con capacidad de decisión, y operadores de tecnologías industriales IT (Tecnologías de la Información y las Comunicaciones)/OT (Tecnologías de Operación u Operativas) sobre el valor para su organización de una correcta gestión de los riesgos y amenazas de Ciberseguridad en el entorno industrial.

OBJETIVOS

OBJETIVOS DEL CURSO

El objetivo fundamental del programa es lograr un dominio en el ámbito de la Ciberseguridad, y con más énfasis en la Industria. En concreto:

Prueba Programa Executive: Ciberseguridad Industrial | ONLINE ¡Promo ESPECIAL!

NUEVO Programa AEC Executive -20% todos | -35% socios | -50% desempleados y autónomos con baja actividad

- Tener un conocimiento de la terminología y los conceptos, de las estrategias de ciberdefensa que podemos implantar.
- Conocer cuáles son los objetivos, importancia e impacto que ha supuesto la cuarta revolución industrial o Industria 4.0, la actualización a la Industria 5.0, y valorar la importancia de la ciberseguridad en este nuevo entorno.
- Tener una visión completa de lo que supone la Transformación Digital, la digitalización y la conectividad (o hiperconectividad, como algunos la denominan).
- Ser conscientes de la importancia de los datos y la realidad de la convergencia entre las Tecnologías de la Información IT y las de la Operación OT. Conocer los riesgos que esta evolución supone.
- Conocer los nuevos escenarios de sectores industriales como el eléctrico, evolucionado gracias a la implementación de nuevas tecnologías: Smart Grid, Smart Meters en las llamadas Smart Cities.
- Como proteger las Infraestructuras Críticas y los servicios esenciales, los sistemas ciberfísicos, los riesgos, amenazas y vulnerabilidades, la legislación aplicable según cada entorno, región y país (Europa, Norteamérica, Latinoamérica, Asia,...). Estrategias transnacionales.
- Observar y aprender del estado del arte de la ciberseguridad a nivel internacional.
- Comprender los Sistemas de Control Industriales, PLC, SCADA, DCS, RTU.
- Como gestionar el riesgo, amenazas, vulnerabilidades, políticas y estrategias.
- Razonar los modelos organizativos, la gobernanza de la Ciberseguridad, los roles que intervienen, los sistemas de gobierno, recomendaciones y controles de seguridad.

Los participantes en el programa recibirán un Diploma con el reconocimiento de la Asociación Española para la Calidad.

DIRIGIDO A:

Orientado a aquellas personas que desarrollan roles en la Alta Dirección, Ejecutivos con capacidad de decisión, mandos intermedios y operadores de tecnologías industriales IT/OT con necesidades de conocimientos de alto nivel y concienciación en Ciberseguridad Industrial.

METODOLOGÍA Y PROFESORADO

METODOLOGÍA

Nuestra metodología de formación online tutorizada combina a la perfección la flexibilidad y practicidad de la formación online con el acompañamiento personalizado de tutores especializado, para sacar el máximo rendimiento a tu formación.

La tutorización del curso actúa como apoyo principal al autoestudio para favorecer, junto a la realización de ejercicios, el correcto aprendizaje de todos los conceptos. Los alumnos contarán con:

- Un **aula virtual** en la que se ordenan los contenidos teóricos en un **formato amigable y fácil de interiorizar.**
- Una evaluación continua que ayudará a reforzar los conocimientos adquiridos a través de **ejercicios de autoevaluación** para consolidar los principales conceptos y pruebas de evaluación para superar cada uno de los módulos.
- **Casos prácticos** de aplicación real a empresas y organizaciones.
- **Material audiovisual** de ayuda a la interiorización de los principales conceptos.
- **Foros** de resolución de dudas e **intercambio** de experiencias **con tutores y alumnos.**
- **Clases virtuales** por videoconferencia (en directo o en diferido) para profundizar en los conceptos más relevantes.

Este programa formativo también está **disponible en modalidad In Company**, formación a medida para tu empresa.

PROFESORES

- **José Antonio Sánchez Durán.** Senior Consultant / Advisor GOVERTIS Advisory Services / Telefónica Tech
- **Joan Figueras Tugas.** Security & GRC Advisor en Govertis.

Prueba Programa Executive: Ciberseguridad Industrial | ONLINE ¡Promo ESPECIAL!

NUEVO Programa AEC Executive -20% todos | -35% socios | -50% desempleados y autónomos con baja actividad

- **Mónica de la Huerga.** CISO en cliente final. GRC Senior Consultant en Govertis, parte de Telefónica Tech
- **Vladimir Barrero Castro.** GRC Consulting Business Development Representative HISPAM Telefónica Tech

PROGRAMA

Nivel 1. FUNDAMENTALS – 60h

1.1 Introducción a la Ciberseguridad Industrial

- ¿Qué entendemos por Ciberseguridad? Introducción a la Ciberseguridad Industrial. Términos y Conceptos Generales en Ciberseguridad Industrial. El Ciberespacio. Estrategias de Defensa en Ciberseguridad Industrial.
- ¿Qué es la Industria 4.0? Objetivos. Importancia de la Industria 4.0. Impactos en la Industria. Beneficios que aporta la Industria 4.0. Importancia de la Ciberseguridad en la Industria 4.0.
- Digitalización y Conectividad en la Industria 4.0. Actualización a la Industria 5.0. Impacto en los Sistemas de Información y las Tecnologías de Automatización Industrial. Intercambio de datos y Convergencia IT/OT Tecnologías de la Información / Tecnologías de la Operación. IoT Industrial (IIoT). Transformación digital. Evolución hacia Cloud Computing, Edge Computing e Industria Conectada. Riesgos en la Convergencia IT / OT y en la Digitalización de la Industria. Nuevos escenarios en el sector eléctrico: Smart Grid, Smart Meters en las Smart Cities.
- Infraestructuras Críticas. Definición y sectores. Riesgos y amenazas en las Infraestructuras Críticas. Sistemas Ciberfísicos (CPS) en la Industria 4.0 y 5.0. ¿Qué son? y ¿Cómo se protegen? Relación entre Protección de Servicios Esenciales y Seguridad en Industria 4.0 y 5.0. Legislación sobre Infraestructuras Críticas.
- Estado del Arte Internacional de la Ciberseguridad. Estado del Arte de la Ciberseguridad en Europa.
- **Clase online: Introducción a la Ciberseguridad Industrial: ¿Qué entendemos por Ciberseguridad? ¿Qué es la Industria 4.0? Digitalización y Conectividad en la Industria 4.0**
- **Clase en directo: Introducción a la Ciberseguridad Industrial. Infraestructuras Críticas. Estado del Arte Internacional y Europeo de la Ciberseguridad**

1.2 Sistemas de Automatización y Control Industrial (IACS)

- Sistemas de Control Industrial (SCI / ICS / IACS). Procesos Industriales. Historia. Procesos Industriales y elementos de los Sistemas de Control. Tipos de Procesos Industriales. Elementos y Dispositivos de Control
- Pirámide de la Automatización Industrial.
- Ciberseguridad en los sistemas de control (OT).
- Amenazas y vulnerabilidades en Sistemas IACS. Ataques a las Tecnologías de la Operación OT. Catálogo de Escenarios de Riesgos en ICS. Amenazas emergentes en Ciberseguridad ENISA. Catálogo de amenazas ENISA especialmente dirigido a las Smart Grid. Guía NIST de Seguridad para Sistemas de Control Industrial (ICS).
- Sistema de Alertas y Avisos de Ciberseguridad CISA. Sistema de Alertas y Avisos SCI de INCIBE-CERT (ES). CVE (Common Vulnerabilities and Exposures). Principales ataques a Sistemas Industriales. Principales predicciones en ciberseguridad industrial.
- Contramedidas y Buenas Prácticas.
- Responsabilidades de Seguridad del C-Level
- **Clase online: Sistemas de Automatización y Control Industrial (IACS). Sistemas de Control Industrial (SCI / ICS / IACS). Los Procesos Industriales y los elementos de los Sistemas de Control**
- **Clase en directo: Sistemas de Automatización y Control Industrial (IACS). Pirámide de la Automatización Industrial. Ciberseguridad en los sistemas de control. Amenazas y vulnerabilidades en Sistemas IACS. CVE (Common Vulnerabilities and Exposures). Principales ataques a Sistemas Industriales. Contramedidas y Buenas Prácticas. Responsabilidades de Seguridad del C – Level**

1.3 Gobernanza de la Ciberseguridad Industrial

- Modelo organizativo de la Ciberseguridad: funciones y responsabilidades ¿Qué es el modelo organizativo de la ciberseguridad? Importancia del modelo organizativo de la ciberseguridad. El modelo organizativo de la ciberseguridad. Elementos clave del modelo organizativo de ciberseguridad. Implementación del modelo organizativo de ciberseguridad. Mejores prácticas y estándares internacionales para el modelo organizativo de ciberseguridad. Buenas prácticas recomendadas por expertos y organismos internacionales. Perspectivas futuras del modelo organizativo de la ciberseguridad. Rol de CSO (Chief Security Officer). Rol de CISO (Chief Information Security Officer)
- Sistema de Gobierno de la Seguridad en OT. Redes OT e ICS. IoT Internet de las cosas. Gestión de la Ciberseguridad en SCI (Sistemas Críticos de

Información). Medidas básicas recomendadas. Controles de Seguridad en Sistemas OT.

> Introducción al estándar NERC CIP, marco principal de referencia de ciberseguridad en sistemas industriales del sector eléctrico. Requisitos fundamentales del cumplimiento de NERC CIP

> Marcos Normativos de Referencia en Ciberseguridad Industrial. Las políticas nacionales y europeas en ciberseguridad. Protección de Infraestructuras Críticas. ENISA y la directiva NIS2

> Introducción al estándar ISA99 / IEC62443 marco principal de referencia internacional de ciberseguridad en sistemas industriales. General. Políticas y procedimientos. Requisitos del sistema. Requisitos de los componentes.

> Diagnóstico de la Ciberseguridad Industrial. Buenas prácticas en el diagnóstico de la Ciberseguridad Industrial. Estado de la Ciberseguridad en una instalación industrial. Puntos débiles en ciberseguridad industrial. Información actualizada y completa sobre arquitectura de redes y sistemas. Riesgos en ciberseguridad industrial. Recomendaciones de mejora en ciberseguridad industrial. Diseño de Políticas de Seguridad. Desarrollo de Estrategias de Ciberseguridad Industrial. Requisitos de seguridad en ciberseguridad industrial. Responsabilidades en ciberseguridad industrial.

> **Clase online: Gobernanza de la Ciberseguridad Industrial. Funciones y responsabilidades. Sistema de Gobierno de la Seguridad en OT. Estándar NERC CIP, marco principal de referencia de ciberseguridad en sistemas industriales**

> **Clase en directo: Gobernanza de la Ciberseguridad Industrial. Marcos Normativos de referencia en Ciberseguridad Industrial. Estándar ISA99 / IEC62433. Diagnóstico de la Ciberseguridad Industrial**

CASO PRÁCTICO: Autodiagnóstico cumplimiento Directiva (UE) 2022/2555 NIS2. Securización de un Proceso Industrial en el Sector Eléctrico. Aplicación de las medidas de control.

> **Clase en directo: Preparación del Caso Práctico.**