

Programa Executive: Ciberseguridad Industrial | ONLINE

NUEVO Programa AEC Executive -20% 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% 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

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

Identificar los **riesgos y amenazas** que las infraestructuras críticas y el intercambio de datos suponen para una organización es fundamental para proteger sus infraestructuras y servicios esenciales. Este programa te permitirá comprender los términos y conceptos clave 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:

- > Personas en **roles de Alta Dirección y ejecutivos** con capacidad de decisión
- > **Operadores de tecnologías industriales IT** (Tecnologías de la Información y las Comunicaciones) y **OT** (Tecnologías de Operación),

Los participantes saldrán concienciados sobre la importancia de gestionar correctamente los **riesgos y amenazas** de ciberseguridad en el entorno industrial, entendiendo el **impacto directo en sus organizaciones**.

OBJETIVOS

? OBJETIVOS DEL CURSO

El objetivo fundamental del programa es proporcionar **dominio en el ámbito de la Ciberseguridad, con un enfoque especial en el entorno industrial**.

En concreto, los objetivos son:

? **Adquirir un conocimiento sólido** de la terminología, los conceptos clave y las estrategias de ciberdefensa aplicables en la industria.

? **Comprender los objetivos, la importancia y el impacto** de la cuarta revolución industrial (Industria 4.0) y su evolución hacia la Industria 5.0, destacando el papel esencial de la ciberseguridad en este nuevo entorno.

? **Obtener una visión integral** de la Transformación Digital, la digitalización y la conectividad, incluyendo conceptos como la hiperconectividad.

? **Ser conscientes de la relevancia de los datos** y de la convergencia entre las Tecnologías de la Información (IT) y las Tecnologías de la Operación (OT), entendiendo los riesgos asociados a esta evolución.

? **Conocer los nuevos escenarios** en sectores industriales como el eléctrico, impulsados por tecnologías innovadoras como Smart Grid y Smart Meters en el contexto de las Smart Cities.

? **Aprender a proteger Infraestructuras Críticas y servicios esenciales**, incluyendo sistemas ciberfísicos, identificando riesgos, amenazas y vulnerabilidades, y comprendiendo la legislación aplicable en diversos entornos y regiones (Europa, Norteamérica, Latinoamérica, Asia).



Para cualquier duda o consulta llamar al
912 108 120 / 21

Además, puedes consultar en nuestra web
otros programas formativos www.aec.es

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

Programa Executive: Ciberseguridad Industrial | ONLINE

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

?Explorar el estado del arte de la ciberseguridad a nivel internacional, observando buenas prácticas y estrategias transnacionales.

?Entender los Sistemas de Control Industriales como PLC, SCADA, DCS y RTU, y su importancia en el entorno industrial.

?Gestionar riesgos, amenazas y vulnerabilidades, diseñando políticas y estrategias eficaces de ciberseguridad.

?Razonar y estructurar modelos organizativos para la gobernanza de la ciberseguridad, incluyendo roles clave, 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**.

METODOLOGÍA Y PROFESORADO

ONLINE TUTORIZADA: MAXIMIZANDO EL APRENDIZAJE

Nuestra metodología de **formación online tutorizada** combina de manera perfecta la **flexibilidad y practicidad** de la formación online con el **acompañamiento** personalizado de tutores especializados, **maximizando el rendimiento** de tu aprendizaje.

La tutorización del curso actúa como un **apoyo esencial** al autoestudio, favoreciendo el correcto **aprendizaje** de todos los conceptos, junto a la realización de ejercicios prácticos.

Los alumnos contarán con:

- > **Aula virtual:** Un espacio donde los contenidos teóricos se presentan en un **formato amigable** y fácil de interiorizar.
- > **Evaluación continua:** Diseñada para reforzar los conocimientos adquiridos mediante **ejercicios de autoevaluación** que consolidan los conceptos principales y **pruebas de evaluación** necesarias para superar cada módulo.
- > **Casos prácticos:** Ejercicios aplicados a situaciones reales en empresas y organizaciones, para conectar la teoría con la práctica.
- > **Material audiovisual:** Recursos que facilitan la interiorización de los conceptos clave del curso.
- > **Foros interactivos:** Espacios para resolver dudas y compartir experiencias con tutores y compañeros.
- > **Clases virtuales:** Sesiones 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.
- > **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

PROGRAMA EXECUTIVE – 60H

? MÓDULO 1: INTRODUCCIÓN A LA CIBERSEGURIDAD INDUSTRIAL

Objetivo: El programa está diseñado para ofrecer una comprensión profunda de la ciberseguridad en la industria, centrado en la protección de infraestructuras críticas y el impacto de la digitalización en los sistemas de control industrial.

Contenidos:

??¿Qué entendemos por Ciberseguridad?



Para cualquier duda o consulta llamar al
912 108 120 / 21

Además, puedes consultar en nuestra web
otros programas formativos www.aec.es



Programa Executive: Ciberseguridad Industrial | ONLINE

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

Introducción a la Ciberseguridad Industrial. Términos y Conceptos Generales en Ciberseguridad. El ciberespacio. Estrategias de Defensa en Ciberseguridad Industrial.

??¿Qué es 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. IIoT 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 de la Ciberseguridad

? De la Ciberseguridad. Estado del Arte de la Ciberseguridad en Europa.

Clase online: Introducción a la ciberseguridad industrial, Industria 4.0, y digitalización en la industria.

Clase en directo: Introducción a la ciberseguridad Industrial. Infraestructuras Críticas. Estado del Arte Internacional y Europeo de la Ciberseguridad.

? MODULO 2. SISTEMAS DE AUTOMATIZACION Y CONTROL INDUSTRIAL (IACS)

Objetivo: Brindar a los participantes una comprensión profunda sobre los sistemas de automatización y control industrial (IACS), su evolución, las amenazas y vulnerabilidades asociadas, y las mejores prácticas en ciberseguridad necesarias para proteger estos sistemas críticos en entornos industriales.

Contenidos:

?? 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.

??Ciberseguridad en los sistemas de control (OT)

??Amenazas y vulnerabilidades en los 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 CISA 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 en Ciberseguridad 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.

? MÓDULO 3: GOBERNANZA DE LA CIBERSEGURIDAD INDUSTRIAL

Objetivo: Este módulo tiene como objetivo proporcionar a los participantes los conocimientos y las herramientas necesarias para comprender el modelo organizativo y las prácticas de gobernanza en ciberseguridad industrial, con un enfoque en los sistemas industriales críticos (OT/ICS) y la implementación de políticas de seguridad eficaces en estos entornos.

Contenidos:

??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. IIoT Internet de las cosas. Gestión de la Ciberseguridad en SCI (Sistemas Críticos de



Para cualquier duda o consulta llamar al
912 108 120 / 21

Además, puedes consultar en nuestra web
otros programas formativos www.aec.es



Programa Executive: Ciberseguridad Industrial | ONLINE

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

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 en 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: Securalización de un Proceso Industrial en el Sector Eléctrico: Aplicación de las medidas de control de ciberseguridad.

Clase en Directo: Preparación del Caso Práctico (Clase en directo).



Para cualquier duda o consulta llamar al
912 108 120 / 21

Además, puedes consultar en nuestra web
otros programas formativos www.aec.es

