Gestión de la Ciberseguridad Industrial | ONLINE

-20% socios | -50% desempleados y autónomos con baja actividad

Modalidad	Duración	Precio	Precio socio	Inicio / Fin	Lugar
Online	180 horas	1.395,00€ + I.V.A.	1.115,00€ + I.V.A.	31/10/2025 21/03/2026	AEC

***Contratando cada Módulo (60 h) por separado: 595 € + IVA | socios: 476 € + IVA**

*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: 1350€

Consulta condiciones para la bonificación por módulos.

FINALIDAD

PROTEGE A TU INDUSTRIA FRENTE A CIBERATAQUES Y AMENAZAS DE SEGURIDAD.

El objetivo fundamental del programa es alcanzar **conocimientos integrales en el ámbito de la Ciberseguridad Industrial** que permitan determinar e **identificar amenazas, riesgos** actuales y posibles brechas de seguridad. Los participantes aprenderán a usar **medidas para prevenir o reducir** estos riesgos, protegiendo los activos digitales.

Además, se capacitarán para detectar, encontrar y analizar **posibles ciberataques** o componentes comprometidos, y **tomar las decisiones y acciones** necesarias para responder ante los incidentes detectados. El programa también enseña estrategias para **recuperar los activos y operaciones impactadas** por un incidente, todo ello mediante el establecimiento y monitorización de políticas y estrategias de gestión del riesgo cibernético industrial.

Estructura del Programa (180 h)

El programa está compuesto por **tres módulos** que se pueden cursar de **forma completa o por separado, según el nivel deseado.**

1- Módulo FUNDAMENTALS – Nivel 1 (60 h) : Este módulo ofrece una visión general de la Ciberseguridad Industrial y las Estrategias de Ciberdefensa. Los participantes se familiarizarán con los Sistemas de Automatización y Control Industrial y el modelo organizativo de Gobernanza.

2- Módulo ADVANCED – Nivel 2 (60 h) : Enfocado en la regulación y gestión, este módulo aborda el contexto y la cultura en ciberseguridad, la regulación y estandarización, normativas nacionales e internacionales, y la gestión de la ciberseguridad y del riesgo en entornos industriales.

3- Módulo EXPERT – Nivel 3 (60 h) : Centrado en la operación, este módulo trata los Sistemas de Gestión de la Ciberseguridad Industrial, la Gestión de la Operación y las terceras partes involucradas,

Flexibilidad y Apoyo de Expertos

Cada uno de los niveles tiene una estructura modular y una duración pensada para facilitar a los alumnos **compaginar su formación con sus responsabilidades laborales**. Este enfoque flexible está respaldado por un equipo docente compuesto por profesionales con perfiles multidisciplinarios, de **larga trayectoria y destacada actuación en el sector.** Estos expertos están comprometidos en ofrecer su **máximo apoyo** para que los participantes alcancen sus objetivos.

Gestión de la Ciberseguridad Industrial | ONLINE

-20% socios | -50% desempleados y autónomos con baja actividad

OBJETIVOS

?OBJETIVOS

Los objetivos específicos del programa son:

Obtener conocimiento de la terminología, sistemas y los conceptos en ciberseguridad industrial, de las estrategias de ciberdefensa, de lo que supone la Transformación Digital con la hiperconectividad y sus riesgos. Ser conscientes de la importancia de los datos en unas tecnologías IT y OT en convergencia.

Como proteger las Infraestructuras Críticas y los servicios esenciales, los sistemas ciberfísicos, cómo gestionar los riesgos, amenazas y vulnerabilidades, Políticas, Estrategias y legislación aplicable según cada entorno, país o Unión Europea (LPIC, NIS, NIS2, CER, ENS).

Modelos de gobernanza de la Ciberseguridad, roles que intervienen, niveles de madurez, recomendaciones y controles de seguridad basados en buenas prácticas y estándares internacionales como ISA99/IEC62443, ISO 27001 e ISO 27002, NERC CIP o US CSF NIST. Cómo diseñar e implantar un Plan Director de Ciberseguridad.

Cómo diseñar e implantar un Sistema de Gestión de la Ciberseguridad Industrial(SGCI), realizar su operación y tener presente las Terceras partes y la importancia de la Cadena de Suministros en ciberseguridad.

El programa proporciona a los alumnos un **conocimiento profundo** de todos los **elementos y componentes** físicos y tecnológicos involucrados en los sistemas de automatización industrial (IACS), incluyendo:

- Redes y comunicaciones
- Zonas y conductos de seguridad
- Infraestructuras críticas y servicios esenciales

Se presta especial atención a la **importancia** de estas infraestructuras **para el país y su impacto en el entorno europeo.**

Al finalizar cada nivel, y también al finalizar el programa completo, se otorgará un diploma reconocido por la Asociación Española para la Calidad.

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.

Gestión de la Ciberseguridad Industrial | ONLINE

-20% socios | -50% desempleados y autónomos con baja actividad

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

PROGRAMA

? MÓDULO FUNDAMENTALS- NIVEL 1 (60H)

Proporcionar una comprensión básica de la ciberseguridad industrial, incluyendo su importancia en la Industria 4.0 y 5.0, los riesgos asociados con la convergencia IT/OT, y cómo proteger infraestructuras críticas mediante el análisis de amenazas y buenas prácticas de seguridad.

Contenidos:

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 1 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 1 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.

Gestión de la Ciberseguridad Industrial | ONLINE

-20% socios | -50% desempleados y autónomos con baja actividad

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

Clase en directo: Preparación del Caso Práctico.

? MÓDULO ADVANCED – NIVEL 2 (60 H)

Desarrollar las habilidades necesarias para gestionar la ciberseguridad industrial en entornos avanzados, mediante el conocimiento de normativas, marcos de referencia, y la implementación de estrategias de gestión de riesgos, continuidad del negocio y resiliencia en entornos industriales.

Contenidos:

2.1 Contexto de la Ciberseguridad Industrial

Contexto de la Ciberseguridad en entornos industriales. La Automatización Industrial. Importancia y objetivos de la Automatización Industrial. Beneficios de la Automatización Industrial.

Cultura en Ciberseguridad Corporativa. Conocimientos, hábitos y percepciones. Actitudes, normas y valores personales. Retos, obstáculos y prioridades.

Ciberseguridad en la Automatización Industrial. Niveles tecnológicos y obsolescencia admitida. Probabilidad de amenaza. Vulnerabilidades y probabilidad de materialización. Consecuencias de la materialización de las amenazas sobre los Sistemas de Automatización y Control Industrial (IACS). Utilización de Sistemas y Software obsoleto sin soporte.

Medidas de Protección (Controles). NERC CIP. Ciclo de vida de los Sistemas IT/OT.

La Ciberseguridad en la Cadena de Suministro Industrial.

Clase online: Contexto de la Ciberseguridad Industrial

2.2 Regulación y estandarización

Estrategias de Ciberseguridad Nacional en Europa, EEUU y Latinoamérica. Organismos responsables. Normativas nacionales en Europa. Estrategia de Ciberseguridad nacional en España. La ciberseguridad en Infraestructuras Críticas. Directivas UE NIS2 / CER. NIST. Instituto Nacional de Estándares y Tecnología de los EEUU. CISA (Cybersecurity & Infrastructure Security Agency). CISA y los Sistemas de Control Industrial, la Seguridad y Resiliencia de Infraestructuras Críticas y las mejores prácticas en Ciberseguridad. ENISA Agencia de la Unión Europea para la Ciberseguridad. Responsabilidades y funciones clave. Principios que rigen el enfoque internacional de ENISA. Objetivos y disposiciones específicas bajo objetivos estratégicos individuales.

Normativas de protección y mejores prácticas. NERC CIP Cybersecurity Standards. IEC 62433. ISO 27001 e ISO 27002. NIST SP 800-82 Guía de seguridad de los sistemas de control industrial (ICS).

Gestión de la Ciberseguridad Industrial | ONLINE

-20% socios | -50% desempleados y autónomos con baja actividad

Clase online: Regulación y estandarización. Estrategias de Ciberseguridad Nacional en Europa, EEUU y Latinoamérica. Normativas nacionales en Europa. Estrategia de Ciberseguridad nacional en España. La ciberseguridad en Infraestructuras Críticas. Directivas UE NIS2 / CER. NIST. Instituto Nacional de Estándares y Tecnología de los EEUU. CISA ENISA Agencia de la Unión Europea para la Ciberseguridad

Clase en directo: Regulación y estandarización. Normativas de protección y mejores prácticas. NERC CIP Cybersecurity Standards. IEC 62433. ISO 27001 e ISO 27002. NIST SP 800-82 Guía de seguridad de los sistemas de control industrial (ICS)

2.3 Gestión de la Ciberseguridad Industrial

Sistemas de Gestión de Ciberseguridad Industrial (SGCI). Estrategia y Política. Gestión del riesgo. Cultura de la Ciberseguridad. Normativas de protección de instalaciones. Resiliencia y continuidad. Mejora Continua.

Modelos de madurez en Ciberseguridad. C2M2 (Cybersecurity Capability Maturity Model). NIST SP 800-53, CSF-NIST. ISEM (Information Security Evaluation Maturity Model).

Gestión del Riesgo de Ciberseguridad Industrial.

Recomendaciones y Siguientes Pasos. Estableciendo un Plan Director de Ciberseguridad Industrial. Qué es el Plan Director de Seguridad Industrial (PDSI). Esquema general de un Plan Director de Seguridad Industrial. Medidas organizativas, de gestión y de concienciación. Medidas de Control, Intervención y recuperación. Indicadores de Compromiso. Medición de procesos. Afectación del negocio.

Estrategias de Continuidad de Negocio y Garantía de Resiliencia. Análisis de Impacto del Negocio (BIA). Plan de Continuidad de Negocio (BCP). Evaluación de la Resiliencia. Gestión de Riesgos. Nivel de Madurez. Formación y concienciación.

Clase online: Gestión de la Ciberseguridad Industrial

2.4 Gestión del riesgo en entornos industriales

Activos: Definición de Zonas y Conductos de Seguridad. Zonas de Seguridad. Conductos de Seguridad.

Amenazas: Definición de Fuentes y Agentes de Amenaza. Niveles Objetivo. Fuentes y Agentes de Amenaza. Niveles Objetivo de Seguridad.

Vulnerabilidades. Catálogo de Vulnerabilidades conocidas Explotadas de MITRE. Modelo Zero Trust en entornos OT. Mayor exposición a ataques en la industria. Tecnologías convergentes hiperconectadas. Ransomware en entornos industriales.

Incidentes OT. Reducción de la Probabilidad y Minimización del Impacto. The Oldsmar Cyberattack, Florida US. The Washington DC Cyberattack. Colonial Pipeline Cyberattack US.

Análisis Forense en Sistemas OT. Características. Análisis forense en la integración de IT/OT.

Centro de operaciones de seguridad OT (SOC). Detección de Incidentes y Gestión.

Cooperación y Coordinación sectorial, estatal y europea.

Clase en directo: Gestión del Riesgo en entornos Industriales Activos. Definición de Zonas y Conductos de Seguridad. Amenazas. Vulnerabilidades. Incidentes OT. Análisis Forense en Sistemas OT. Centro de operaciones de seguridad OT (SOC). Cooperación y Coordinación sectorial, estatal y regional

CASO PRÁCTICO: Diseño de Plan Director de Ciberseguridad Industrial, Análisis de Riesgos, Plan de Tratamiento del Riesgo y Estrategias a aplicar. Diseño de Arquitecturas Seguras. Implementación del estándar NERC CIP.

Clase en directo: Preparación del Caso Práctico.

? MÓDULO EXPERT – NIVEL 3 (60 H)

Capacitar para la implementación y operación avanzada de un Sistema de Gestión de Ciberseguridad Industrial (SGCI), con énfasis en auditorías, análisis forenses, y la colaboración con terceras partes para asegurar la protección de las infraestructuras críticas industriales.

Contenidos:

3.1 Sistemas de Gestión de la Ciberseguridad Industrial (SGCI)

Sistema de Gestión de la Ciberseguridad Industrial (SGCI). ¿Qué entendemos por un Sistema de Gestión de la Ciberseguridad Industrial? Marco de Referencia del SGCI. Pasos para su implementación.

Esquema de desarrollo del Sistema de Gestión de Ciberseguridad Industrial. Compromiso de la Gerencia / Alta Dirección. Roles y Responsabilidades Funciones y Cometidos. Alcance del SGCI. Identificación, evaluación y análisis del Riesgo. Implementación de las medidas y controles de seguridad. Medidas Organizativas. Medidas físicas. Medidas técnicas. Desarrollo del Plan de Acción. Monitorización y seguimiento. Mejora continua y lecciones aprendidas.

Soft Skills del Responsable de Ciberseguridad en OT.

Auditorías en Tecnologías Operativas (OT). Auditoría de la Capa de Dirección OT. Auditoría en la Capa Física OT. Auditoría en la Capa de Red OT. Auditoría del Hardware y Software OT. Auditoría del Tráfico de red IT/OT. Auditoría sobre el Personal.

Gestión de la Ciberseguridad Industrial | ONLINE

-20% socios | -50% desempleados y autónomos con baja actividad

Clase online: Sistemas de Gestión de la Ciberseguridad Industrial

3.2 Operación de la Ciberseguridad Industrial

Vigilancia y monitorización en SOC IT-OT / CERT-CSIRT. Centro de Operaciones de Seguridad SOC IT-OT. Funciones del SOC IT-OT. Personal componente del Centro de Operaciones de Seguridad (SOC). Equipo de Respuesta a Emergencias Informáticas CERT. Características de un CERT / CSIRT. Funciones del CERT / CSIRT. Retos a los que se enfrentan los CERT / CSIRT. CERT / CSIRT en Europa.

Pentesting. Tipos de Pentesting. Atendiendo al conocimiento de la infraestructura. Atendiendo al objetivo. Fases en el Pentesting. Herramientas y técnicas de Pentesting. Desafíos éticos y legales asociados con el Pentesting. Beneficios de la realización del Pentesting. Ejemplos de Pentesting exitosos. Perspectivas futuras y tendencias en Pentesting.

Vectores de Ataque. Acción, Defensa y Evaluación. Ingeniería Social. Explotación de Vulnerabilidades de Software. Ataques de Fuerza Bruta. Ataques de Inyección de Código. Phishing y Smishing. Explotación de Vulnerabilidades de Red. Ataques de Ingeniería Inversa. Inyección de SQL. Ataques de DoS/DDoS (Denegación de Servicio Distribuido). Malware y Ransomware.

Tendencias en ciberdelincuencia.

CSIRT Nacionales y Europeos.

Ciberseguridad en España y Europa: Avances, Riesgos y Desafíos Futuros.

El Observatorio de la Ciberseguridad: Fortaleciendo la Resiliencia Digital.

Clase online: Operación de la Ciberseguridad Industrial. Vigilancia y monitorización en SOC IT-OT / CERT-CSIRT. Pentesting. Vectores de ataque. Acción, Defensa y Evaluación. Tendencias en Ciberdelincuencia

Clase en directo: Operación de la Ciberseguridad Industrial. CSIRT Nacionales y Europeos. Ciberseguridad en España y Europa: Avances, Riesgos y Desafíos Futuros. El Observatorio de la Ciberseguridad. Actividad Maliciosa Contra Infraestructuras Críticas

3.3 Terceras Partes

Grupos de interés gremiales en Ciberseguridad Industrial

Programa de Ciberseguridad de la Comunidad Europea

Asegurando la Infraestructura Crítica: El Rol Vital de los Proveedores de Ciberseguridad Industrial. Entendiendo la Amenaza. Soluciones Adaptadas. Colaboración y Concientización. Mirando hacia el Futuro.

Plataforma RECIN del Centro de Ciberseguridad Industrial (CCI)

Plataforma CATÁLOGO ACTIVO

De la teoría a la práctica. Implementación de un Sistema de Gestión de la Ciberseguridad Industrial (SGCI). Por qué se requiere la implantación de un SGCI. Su importancia. Características singulares de IACS/ICS frente a sistemas información IT. Estándares de referencia. IEC 62443. ISO 27001. ISO 27002. ISO 17799. NERC CIP. Ciclo de vida del Sistema de Gestión de Ciberseguridad Industrial (SGCI). Fases en la Gestión de la Ciberseguridad Industrial. Entornos que proporcionan un marco integral para el diseño, implementación y gestión de un SGCI.

Paso a paso al Sistema de Gestión de Ciberseguridad Industrial (SGCI). PASO 1. La Estrategia de Ciberseguridad Industrial. PASO 2. Gestión de Riesgos. PASO 3. Cultura de Ciberseguridad Industrial. PASO 4. Establecer las medidas de protección. PASO 5. Resiliencia y Continuidad. PASO 6. Revisión y mejora continua.

Clase online: Terceras Partes. Grupos de interés gremiales en Ciberseguridad Industrial. Programa de Ciberseguridad de la Comunidad Europea. El Rol Vital de los Proveedores de Ciberseguridad Industrial. Entendiendo la Amenaza. Soluciones Adaptadas. Colaboración y Concientización. Mirando hacia el Futuro. El reto de la ciberseguridad industrial

Clase en directo: Terceras Partes. Plataforma RECIN del Centro de Ciberseguridad Industrial (CCI). Plataforma CATÁLOGO ACTIVO. Implementación de un Sistema de Gestión de la Ciberseguridad Industrial (SGCI).

Clase online: Sesión Especial Auditoría de Campo. Guía de Campo Auditoría NERC CIP como referencia en el entorno Europeo

CASO PRÁCTICO: Implantación de un Sistema de Gestión de la Ciberseguridad Industrial (SGCI): Planificación, definición del modelo organizativo, requisitos mínimos sobre sistemas (arquitecturas de seguridad) evaluación y control periódicos, mejora continua. Consideración de partes interesadas.

Clase en directo: Preparación del Caso Práctico.