INESEM

BUSINESS SCHOOL

Curso Superior en Ciberseguridad Industrial

+ Información Gratis

titulación de formación continua bonificada expedida por el instituto europeo de estudios empresariales

Curso Superior en Ciberseguridad Industrial

duración total: 250 horas ***horas teleformación:*** 125 horas

precio: 0 € *

modalidad: Online

* hasta 100 % bonificable para trabajadores.

descripción

La globalización de procesos industriales bajo control de sistemas automatizados e informatizados requiere de técnicos cualificados capaces de gestionar la ciberseguridad de estas instalaciones, ya que el sector industria tiene a contar todos con este tipo de controles. Este curso se preparara para poder hacer frente a las necesidades de seguridad de los sistemas de control industrial SCADA presentes en prácticamente todas las industrias o hacer frente a la implantación de nuevos sistemas bajo criterios de seguridad adecuados. A través del estudio con Inesem serás capaz de alcanzar los conocimientos requeridos para gestionar la seguridad de un sistema informático en entornos de automatización industrial.

a quién va dirigido

Todos aquellos trabajadores y profesionales en activo que deseen adquirir o perfeccionar sus conocimientos técnicos en este área.

objetivos

- Saber qué características, componentes y tipologías de SCADA integran el mercado actual
- Profundizar en la monitorización mediante sistemas HMI y SCADA tanto en implementación como en diseño de procesos (GEMMA).
- Obtener una visión global de la ciberseguridad y la ciberinteligencia
- Diseñar e Implementar sistemas seguros de acceso y transmisión de datos
- Detectar y responder ante incidentes de seguridad informática

para qué te prepara

Con este Curso en Ciberseguridad Industrial adquirirás las competencias técnicas necesarias para desarrollar desde el punto inicial hasta la puesta en marcha los sistemas de seguridad sobre los procesos automatizados existentes en la industria, realizando auditorías de seguridad informática, analizando los riesgos e información recopilada para llevar a cabo un correcto análisis forense.

salidas laborales

Los titulados en este Curso podrán ejercer su capacidad profesional en empresas de producción industrial, ingenierías o empresas tecnológicas, donde existe una demanda real de profesionales con este perfil a nivel de analista de Seguridad Informática, Consultor de Ciberseguridad en Entorno Industrial, Gestor de seguridad en diferentes entornos industriales y de producción.

titulación

Una vez finalizado el curso, el alumno recibirá por parte de INESEM vía correo postal, la Titulación Oficial que acredita el haber superado con éxito todas las pruebas de conocimientos propuestas en el mismo.

Esta titulación incluirá el nombre del curso/máster, la duración del mismo, el nombre y DNI del alumno, el nivel de aprovechamiento que acredita que el alumno superó las pruebas propuestas, las firmas del profesor y Director del centro, y los sellos de la instituciones que avalan la formación recibida (Instituto Europeo de Estudios Empresariales).

INSTITUTO EUROPEO DE ESTUDIOS EMPRESARIALES

como centro de Formación acreditado para la impartición a nivel nacional de formación
EXPIDE LA SIGUIENTE TITULACIÓN

NOMBRE DEL ALUMNO/A

con D.N.I. XXXXXXXX ha superado los estudios correspondientes de

Nombre de la Acción Formativa

de XXX horas, perteneciente al Plan de Formación INESEM en la convocatoria de XXXX
Y para que surta los efectos pertinentes queda registrado con número de expediente XXXX- XXXX-XXXX-XXXXXX

Con una calificación de SOBRESALIENTE

Y para que conste expido la presente TITULACIÓN en
Granada, a (día) de (mes) de (año)

La direccion General

MARIA MORENO HIDALGO

Sello

Firma del alumno/a

NOMBRE DEL ALUMNO/A

forma de bonificación

- Mediante descuento directo en el TC1, a cargo de los seguros sociales que la empresa paga cada mes a la Seguridad Social.

metodología

El alumno comienza su andadura en INESEM a través del Campus Virtual. Con nuestra metodología de aprendizaje online, el alumno debe avanzar a lo largo de las unidades didácticas del itinerario formativo, así como realizar las actividades y autoevaluaciones correspondientes. Al final del itinerario, el alumno se encontrará con el examen final, debiendo contestar correctamente un mínimo del 75% de las cuestiones planteadas para poder obtener el título.

Nuestro equipo docente y un tutor especializado harán un seguimiento exhaustivo, evaluando todos los progresos del alumno así como estableciendo una línea abierta para la resolución de consultas.

El alumno dispone de un espacio donde gestionar todos sus trámites administrativos, la Secretaría Virtual, y de un lugar de encuentro, Comunidad INESEM, donde fomentar su proceso de aprendizaje que enriquecerá su desarrollo profesional.

materiales didácticos

- Manual teórico 'Ciberseguridad: Normativa, Política de Seguridad y Ciberinteligencia'

- Manual teórico 'Herramientas, Técnicas de Ciberseguridad y Sistemas SIEM'

- Manual teórico 'Ciberseguridad Aplicada a Inteligencia Artificial (IA), Smartphones, Internet de las Cosas

- Manual teórico 'Sistemas HMI y SCADA en Procesos Industriales'

profesorado y servicio de tutorías

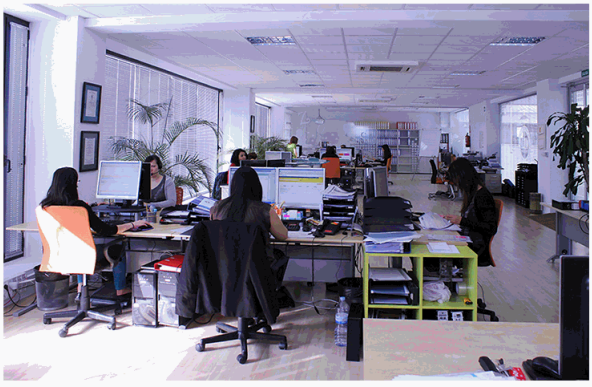
Nuestro equipo docente estará a su disposición para resolver cualquier consulta o ampliación de contenido que pueda necesitar relacionado con el curso. Podrá ponerse en contacto con nosotros a través de la propia plataforma o Chat, Email o Teléfono, en el horario que aparece en un documento denominado “Guía del Alumno” entregado junto al resto de materiales de estudio. Contamos con una extensa plantilla de profesores especializados en las distintas áreas formativas, con una amplia experiencia en el ámbito docente.

El alumno podrá contactar con los profesores y formular todo tipo de dudas y consultas, así como solicitar información complementaria, fuentes bibliográficas y asesoramiento profesional. Podrá hacerlo de las siguientes formas:

- **Por e-mail**: El alumno podrá enviar sus dudas y consultas a cualquier hora y obtendrá respuesta en un plazo máximo de 48 horas.

- **Por teléfono**: Existe un horario para las tutorías telefónicas, dentro del cual el alumno podrá hablar directamente con su tutor.

- **A través del Campus Virtual**: El alumno/a puede contactar y enviar sus consultas a través del mismo, pudiendo tener acceso a Secretaría, agilizando cualquier proceso administrativo así como disponer de toda su documentación



plazo de finalización

El alumno cuenta con un período máximo de tiempo para la finalización del curso, que dependerá de la misma duración del curso. Existe por tanto un calendario formativo con una fecha de inicio y una fecha de fin.

campus virtual online

especialmente dirigido a los alumnos matriculados en cursos de modalidad online, el campus virtual de inesem ofrece contenidos multimedia de alta calidad y ejercicios interactivos.

comunidad

servicio gratuito que permitirá al alumno formar parte de una extensa comunidad virtual que ya disfruta de múltiples ventajas: becas, descuentos y promociones en formación, viajes al extranjero para aprender idiomas...

revista digital

el alumno podrá descargar artículos sobre e-learning, publicaciones sobre formación a distancia, artículos de opinión, noticias sobre convocatorias de oposiciones, concursos públicos de la administración, ferias sobre formación, etc.

secretaría

Este sistema comunica al alumno directamente con nuestros asistentes, agilizando todo el proceso de matriculación, envío de documentación y solución de cualquier incidencia.

Además, a través de nuestro gestor documental, el alumno puede disponer de todos sus documentos, controlar las fechas de envío, finalización de sus acciones formativas y todo lo relacionado con la parte administrativa de sus cursos, teniendo la posibilidad de realizar un seguimiento personal de todos sus trámites con INESEM

programa formativo

MÓDULO 1. SISTEMAS HMI Y SCADA EN PROCESOS INDUSTRIALES

UNIDAD DIDÁCTICA 1. FUNDAMENTOS DE SISTEMAS DE CONTROL Y SUPERVISIÓN DE PROCESOS: SCADA Y HMI

1. Contexto evolutivo de los sistemas de visualización
2. Sistemas avanzados de organización industrial: ERP y MES
3. Consideraciones previas de supervisión y control
4. El concepto de “tiempo real” en un SCADA
5. Conceptos relacionados con SCADA
6. Definición y características del sistemas de control distribuido
7. Sistemas SCADA frente a DCS
8. Viabilidad técnico económica de un sistema SCADA
9. Mercado actual de desarrolladores SCADA
10. PC industriales y tarjetas de expansión
11. Pantallas de operador HMI
12. Características de una pantalla HMI
13. Software para programación de pantallas HMI
14. Dispositivos tablet PC

UNIDAD DIDÁCTICA 2. EL HARDWARE DEL SCADA: MTU, RTU Y COMUNICACIONES

1. Principio de funcionamiento general de un sistema SCADA
2. Subsistemas que componen un sistema de supervisión y mando
3. Componentes de una RTU, funcionamiento y características
4. Sistemas de telemetría: genéricos, dedicados y multiplexores
5. Software de control de una RTU y comunicaciones
6. Tipos de capacidades de una RTU
7. Interrogación, informes por excepción y transmisiones iniciadas por RTU´s
8. Detección de fallos de comunicaciones
9. Fases de implantación de un SCADA en una instalación

UNIDAD DIDÁCTICA 3. EL SOFTWARE SCADA Y COMUNICACIÓN OPC UA

1. Fundamentos de programación orientada a objetos
2. Driver, utilidades de desarrollo y Run-time
3. Las utilidades de desarrollo y el programa Run-time
4. Utilización de bases de datos para almacenamiento
5. Métodos de comunicación entre aplicaciones: OPC, ODBC, ASCII, SQL y API
6. La evolución del protocolo OPC a OPC UA (Unified Architecture)
7. Configuración de controles OPC en el SCADA

UNIDAD DIDÁCTICA 4. PLANOS Y CROQUIS DE IMPLANTACIÓN

1. Símbolos y diagramas
2. Identificación de instrumentos y funciones
3. Simbología empleada en el control de procesos
4. Diseño de planos de implantación y distribución
5. Tipología de símbolos
6. Ejemplos de esquemas

UNIDAD DIDÁCTICA 5. DISEÑO DE LA INTERFAZ CON ESTÁNDARES

1. Fundamentos iniciales del diseño de un sistema automatizado
2. Presentación de algunos estándares y guías metodológicas
3. Diseño industrial
4. Diseño de los elementos de mando e indicación
5. Colores en los órganos de servicio

6.Localización y uso de elementos de mando

UNIDAD DIDÁCTICA 6. GEMMA: GUÍA DE LOS MODOS DE MARCHA Y PARADA EN UN AUTOMATISMO

1.Origen de la guía GEMMA
2.Fundamentos de GEMMA
3.Rectángulos-estado: procedimientos de funcionamiento, parada o defecto
4.Metodología de uso de GEMMA
5.Selección de los modos de marcha y de paro
6.Implementación de GEMMA a GRAFCET
7.Método por enriquecimiento del GRAFCET de base
8.Método por descomposición por TAREAS: coordinación vertical o jerarquizada
9.Tratamiento de alarmas con GEMMA

UNIDAD DIDÁCTICA 7. MÓDULOS DE DESARROLLO

1.Paquetes software comunes
2.Módulo de configuraciónHerramientas de interfaz gráfica del operador
3.Utilidades para control de proceso
4.Representación de Trending
5.Herramientas de gestión de alarmas y eventos
6.Registro y archivado de eventos y alarmas
7.Herramientas para creación de informes
8.Herramienta de creación de recetas
9.Configuración de comunicaciones

UNIDAD DIDÁCTICA 8. DISEÑO DE LA INTERFAZ EN HMI Y SCADA

1.Criterios iniciales para el diseño
2.Arquitectura
3.Consideraciones en la distribución de las pantallas
4.Elección de la navegación por pantallas
5.Uso apropiado del color
6.Correcta utilización de la Información textual
7.Adecuada definición de equipos, estados y eventos de proceso
8.Uso de la información y valores de proceso
9.Tablas y gráficos de tendencias
10.Comandos e ingreso de datos
11.Correcta implementación de Alarmas
12.Evaluación de diseños SCADA

MÓDULO 2. CIBERSEGURIDAD: NORMATIVA, POLÍTICA DE SEGURIDAD CIBERINTELIGENCIA

UNIDAD DIDÁCTICA 1. CIBERSEGURIDAD Y SOCIEDAD DE LA INFORMACIÓN

1.¿Qué es la ciberseguridad?
2.La sociedad de la información
3.Diseño, desarrollo e implantación
4.Factores de éxito en la seguridad de la información
5.Soluciones de Ciberseguridad y Ciberinteligencia CCN-CERT

UNIDAD DIDÁCTICA 2. NORMATIVA ESENCIAL SOBRE EL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI)

1.Estándares y Normas Internacionales sobre los SGSI. ISO 2. Legislación: Leyes aplicables a los SGSI

UNIDAD DIDÁCTICA 3. POLÍTICA DE SEGURIDAD: ANÁLISIS Y GESTIÓN DE RIESGOS

1.Plan de implantación del SGSI
2.Análisis de riesgos
3.Gestión de riesgos

UNIDAD DIDÁCTICA 4. INGENIERÍA SOCIAL, ATAQUES WEB Y PHISHING

1.Introducción a la Ingeniería Social
2.Recopilar información
3.Herramientas de ingeniería social
4.Técnicas de ataques
5.Prevención de ataques
6.Introducción a Phising
7.Phising
8.Man In The Middle

UNIDAD DIDÁCTICA 5. CIBERINTELIGENCIA Y CIBERSEGURIDAD

1.Ciberinteligencia
2.Herramientas y técnicas de ciberinteligencia
3.Diferencias entre ciberinteligencia y ciberseguridad
4.Amenazas de ciberseguridad

UNIDAD DIDÁCTICA 6. MÉTODOS DE INTELIGENCIA DE OBTENCIÓN DE INFORMACIÓN

1.Contextualización
2.OSINT
3.HUMINT
4.IMINT
5.Otros métodos de inteligencia para la obtención de información

UNIDAD DIDÁCTICA 7. CIBERINTELIGENCIA Y TECNOLOGÍAS EMERGENTES

1.Tecnologías emergentes
2.Desafíos y oportunidades de la ciberinteligencia en las tecnologías emergentes
3.Análisis de amenazas avanzado
4.Usos de las tecnologías emergentes en la ciberinteligencia

MÓDULO 3. HERRAMIENTAS, TÉCNICAS DE CIBERSEGURIDAD Y SISTEMAS SIEM

UNIDAD DIDÁCTICA 1. COMUNICACIONES SEGURAS: SEGURIDAD POR NIVELES

1.Seguridad a Nivel Físico
2.Seguridad a Nivel de Enlace
3.Seguridad a Nivel de Red
4.Seguridad a Nivel de Transporte
5.Seguridad a Nivel de Aplicación

UNIDAD DIDÁCTICA 2. CRIPTOGRAFÍA

1.Perspectiva histórica y objetivos de la criptografía
2.Teoría de la información
3.Propiedades de la seguridad que se pueden controlar mediante la aplicación de la criptografía
4.Criptografía de clave privada o simétrica
5.Criptografía de clave pública o asimétrica
6.Algoritmos criptográficos más utilizados
7.Funciones hash y los criterios para su utilización
8.Protocolos de intercambio de claves
9.Herramientas de cifrado

UNIDAD DIDÁCTICA 3. APLICACIÓN DE UNA INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI)

1.Identificación de los componentes de una PKI y sus modelos de relaciones
2.Autoridad de certificación y sus elementos
3.Política de certificado y declaración de prácticas de certificación (CPS)
4.Lista de certificados revocados (CRL)
5.Funcionamiento de las solicitudes de firma de certificados (CSR)
6.Infraestructuras de gestión de privilegios (PMI)
7.Campos de certificados de atributos

8.Aplicaciones que se apoyan en la existencia de una PKI

UNIDAD DIDÁCTICA 4. SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES (IDS/IPS)

1.Conceptos generales de gestión de incidentes, detección de intrusiones y su prevención
2.Identificación y caracterización de los datos de funcionamiento del sistema
3.Arquitecturas más frecuentes de los IDS
4.Relación de los distintos tipos de IDS/IPS por ubicación y funcionalidad
5.Criterios de seguridad para el establecimiento de la ubicación de los IDS/IPS

UNIDAD DIDÁCTICA 5. IMPLANTACIÓN Y PUESTA EN PRODUCCIÓN DE SISTEMAS IDS/IPS

1.Análisis previo
2.Definición de políticas de corte de intentos de intrusión en los IDS/IPS
3.Análisis de los eventos registrados por el IDS/IPS
4.Relación de los registros de auditoría del IDS/IPS
5.Establecimiento de los niveles requeridos de actualización, monitorización y pruebas del IDS/IPS

UNIDAD DIDÁCTICA 6. INTRODUCCIÓN A LOS SISTEMAS SIEM

1.¿Qué es un SIEM?
2.Evolución de los sistemas SIEM: SIM, SEM y SIEM
3.Arquitectura de un sistema SIEM

UNIDAD DIDÁCTICA 7. CAPACIDADES DE LOS SISTEMAS SIEM

1.Problemas a solventar
2.Administración de logs
3.Regulaciones IT
4.Correlación de eventos
5.Soluciones SIEM en el mercado

MÓDULO 4. CIBERSEGURIDAD APLICADA A INTELIGENCIA ARTIFICIAL (IA), SMARTPHONES, INTERNET DE LAS COSAS (IOT) E INDUSTRIA 4.0

UNIDAD DIDÁCTICA 1. CIBERSEGURIDAD EN NUEVAS TECNOLOGÍAS

1.Concepto de seguridad TIC
2.Tipos de seguridad TIC
3.Aplicaciones seguras en Cloud
4.Plataformas de administración de la movilidad empresarial (EMM)
5.Redes WiFi seguras
6.Caso de uso: Seguridad TIC en un sistema de gestión documental

UNIDAD DIDÁCTICA 2. CIBERSEGURIDAD EN SMARTPHONES

1.Buenas prácticas de seguridad móvil
2.Protección de ataques en entornos de red móvil

UNIDAD DIDÁCTICA 3. INTELIGENCIA ARTIFICIAL (IA) Y CIBERSEGURIDAD

1.Inteligencia Artificial
2.Tipos de inteligencia artificial
3.Impacto de la Inteligencia Artificial en la ciberseguridad

UNIDAD DIDÁCTICA 4. CIBERSEGURIDAD E INTERNET DE LAS COSAS (IOT)

1.Contexto Internet de las Cosas (IoT)
2.¿Qué es IoT?
3.Elementos que componen el ecosistema IoT
4.Arquitectura IoT
5.Dispositivos y elementos empleados
6.Ejemplos de uso
7.Retos y líneas de trabajo futuras
8.Vulnerabilidades de IoT
9.Necesidades de seguridad específicas de IoT

UNIDAD DIDÁCTICA 5. SEGURIDAD INFORMÁTICA EN LA INDUSTRIA 4.0

1.Industria 4.0
2.Necesidades en ciberseguridad en la Industria 4.0