Actividad formativa

ELECTRICIDAD Y ELECTRÓNICA	
FSE+-PROF-21	Ciberseguridad en Entornos de las Tecnologías de Operación

Características del curso

FSE+-PROF-21 CIBERSEGURIDAD EN ENTORNOS DE LAS TECNOLOGÍAS DE OPERACIÓN

Nivel: Intermedio **Modalidad**: online **Número de horas**: 35 **Plazas**: 12

Fechas de realización y horario: del 03/10/2022 al 26/10/2022 – tardes

MÓDULO	**FECHA/HORARIO - OCTUBRE**
SISTEMAS DE CONTROL INDUSTRIAL SEGUROS	L3 (de 16:00 a 20:00h) + M4 (de 16:00 a 20:00h) OCT
REDES DE COMUNICACIONES INDUSTRIALES SEGURAS	L10 (de 16 a 19:30) + M11 (de 16 a 19:30) OCT
CIBERSEGURIDAD EN PROYECTOS INDUSTRIALES	J13 (de 16:00 a 19:00h) + L17 (de 16:00 a 19:00h) + M18 (de 16:00 a 19:00h) OCT
ANÁLISIS FORENSE EN CIBERSEGURIDAD INDUSTRIAL	X19 (de 16:00 a 19:00h) + J20 (de 16:00 a 19:00h) + L24 (de 16:00 a 19:00h) OCT
TUTORIA	X26 (16:00-17:00h) OCT

Lugar de impartición:

- Sesiones online síncronas y asíncronas a través de una plataforma de comunicación y colaboración.

Destinatarios: Profesorado de especialidades vinculadas a Formación Profesional. Tendrá preferencia el profesorado encargado de la impartición del curso de especialización en Ciberseguridad en Entornos de las Tecnologías de Operación.

Especialidades preferentes:

112 - Organización y Proyectos de Fabricación Mecánica

124 - Sistemas Electrónicos

125 - Sistemas Electrotécnicos y Automáticos

202 - Equipos Electrónicos

206 - Instalaciones Electrotécnicas

Ciclos Formativos Asociados:

ELE01S - Sistemas Electrotécnicos y Automatizados

ELE02S - Sistemas de Telecomunicaciones e Informáticos

ELE03S - Mantenimiento Electrónico

ELE04S - Automatización y Robótica Industrial

IMA03S - Mecatrónica Industrial

Objetivos:

- Analizar buenas prácticas, estándares de aplicación y normativa para definir perfiles de riesgo.
- Definir e incorporar requisitos de ciberseguridad en todas las fases de un proyecto industrial para evitar posibles incidentes.
- Identificar y analizar las tecnologías avanzadas de aplicación en entornos OT para verificar la alineación con los principios de seguridad informática y los riesgos de ciberseguridad.
- Analizar la convergencia de las prácticas profesionales en los entornos OT e IT y las exigencias que supone para aplicar estrategias de ciberseguridad y caracterizar la evolución de los sistemas de control industrial.
- Definir y parametrizar sistemas de control industrial conforme a requisitos establecidos y controles de auditoría para establecer la configuración de los mismos.
- Identificar y caracterizar equipos y configuraciones de redes industriales para realizar listados de posibles vulnerabilidades.
- Evaluar niveles de riesgo asociados a las redes de instalaciones industriales para identificar vulnerabilidades.
- Seleccionar y emplear diferentes herramientas para realizar análisis forenses. i) Definir y aplicar configuraciones en redes industriales minimizando riesgos para integrar los requerimientos de seguridad.
- Aplicar metodologías de análisis forense en sistemas SCADA, DCS, PLC, robótica industrial, dispositivos IoT y redes industriales para integrar procedimientos de seguridad.
- Realizar informes para la presentación de resultados y conclusiones de análisis forense para elaborar documentación técnica y administrativa.
- Determinar la normativa y los procedimientos aplicables a la seguridad física, a la seguridad operacional y a la ciberseguridad para integrar normas y procedimientos de seguridad.
- Definir y aplicar metodologías para la gestión integral de riesgos de seguridad en entornos de la operación.
- Desarrollar manuales de información para los destinatarios, utilizando las herramientas ofimáticas y de diseño asistido por ordenador para elaborar la documentación técnica y administrativa.
- Desarrollar la creatividad y el espíritu de innovación para responder a los retos que se presentan en los procesos y en la organización del trabajo y de la vida personal.
- Analizar y utilizar los recursos y oportunidades de aprendizaje relacionados con la evolución científica, tecnológica y organizativa del sector y las tecnologías de la información y la comunicación, para mantener el espíritu de actualización y adaptarse a nuevas situaciones laborales y personales.
- Evaluar situaciones de prevención de riesgos laborales y de protección ambiental, proponiendo y aplicando medidas de prevención personales y colectivas, de acuerdo con la normativa aplicable en los procesos de trabajo, para garantizar entornos seguros.
- Identificar y proponer las acciones profesionales necesarias, para dar respuesta a la accesibilidad universal y al «diseño para todas las personas».

- Identificar y aplicar parámetros de calidad en los trabajos y actividades realizados en el proceso de aprendizaje, para valorar la cultura de la evaluación y de la calidad y ser capaces de supervisar y mejorar procedimientos de gestión de calidad.

Competencias:

Definir e implementar estrategias de seguridad en las organizaciones e infraestructuras industriales realizando diagnósticos de ciberseguridad, identificando vulnerabilidades e implementando las medidas necesarias para mitigarlas aplicando la normativa vigente y estándares del sector, siguiendo los protocolos de calidad, de prevención de riesgos laborales y respeto ambiental.

Contenidos:

- Ciberseguridad en proyectos industriales
  - Diseño conceptual y preliminar de un proyecto industrial
  - Ingeniería básica y de detalle
  - Presentación de caso de uso
  - Actividades de ciberseguridad en el diseño e ingeniería
  - Provisión del proyecto: gestión de compras
  - Actividades de ciberseguridad para proveedores
  - Ejecución del proyecto
  - Construcción y puesta en marcha
  - Pruebas FAT, iFAT y SAT
  - Actividades de ciberseguridad en la fase de ejecución
  - Operación y mantenimiento
  - Actividades de ciberseguridad en la fase de O&M
  - Desmantelamiento
  - Actividades de ciberseguridad en la fase de desmantelamiento
- Sistemas de control industrial seguros
  - Tecnologías de automatización industrial
  - Presentación de caso de uso y escenarios de riesgo
  - Plataforma ESCIM
  - Diagnóstico de sistemas
  - Diagnóstico de seguridad física
  - Diagnóstico de terceras partes
- Redes de Comunicaciones industriales seguras
  - Tecnologías de redes industriales
  - Diagnóstico de arquitecturas de redes industriales
  - Informe de diagnóstico
  - Presentación de los resultados
  - Redes en la digitalización industrial
  - Capas y componentes de la digitalización industrial
  - Principales protocolos en la digitalización industrial
  - Riesgos en la digitalización industrial
  - Arquitectura segura en la digitalización industrial
- Análisis forense en ciberseguridad industrial
  - Presentación de caso de uso
  - Características del análisis forense

- Análisis forense en sistemas OT
- Análisis forense en redes industriales
- Análisis forense en la integración IT/OT
- Elaboración de un informe de análisis forense
- Presentación del informe