ACCION FORMATIVA

CIBERSEGURIDAD INDUSTRIAL

DURACION

50 HORAS

OBJETIVO

El objetivo principal de esta acción formativa es proporcionar a los participantes el conocimiento, habilidades prácticas y competencias necesarias para poder gobernar y gestionar los riesgos asociados a la ciberseguridad industrial e integrar las diferentes técnicas y herramientas que permitan hacer frente a los retos y amenazas asociados.

FECHAS Y HORARIO DE IMPARTICIÓN

MES	DIAS	HORARIO	LUGAR
MAYO	15/16	16:00- 20:00	Clases presenciales en la SEDE DE FEMETALiNDUSTRY/FEMETAL C/Marqués de San Esteban 1-6º. Gijón. *(El Aula se determinará con carácter previo al inicio del curso)*
	17	9:30- 14:00	
	22/23	16:00-20:00	
	24	9:30- 14:00	
	29/30	16:00-20:00	
	31	9:30- 14:00	
JUNIO	5/6	16:00-20:00	
	7	9:30-14:00	

**Impartición sujeta a número mínimo de inscritos.*

REQUISITOS

Estar asociado a FEMETAL o a FEMETALiNDUSTRY.

Principado de Asturias
SERVICIO PÚBLICO DE EMPLEO
Financiado por la Unión Europea NextGenerationEU
MINISTERIO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL
Plan de Recuperación, Transformación y Resiliencia

MODALIDAD DE IMPARTICIÓN

Presencial/Aula virtual

CONTENIDOS

1. Fundamentos de ciberseguridad industrial Introducción a los conceptos clave, diferencias entre entornos IT y OT, y el impacto de la Industria 4.0 en la seguridad.

2. Arquitectura de redes y sistemas de control Componentes y funcionamiento de sistemas ICS/SCADA, redes industriales y principales protocolos de comunicación (Modbus, S7, OPC...).

3. Amenazas y riesgos en entornos OT Análisis de vectores de ataque, vulnerabilidades comunes, malware dirigido y casos reales de ciberincidentes en infraestructuras críticas.

4. Gobernanza y normativa aplicable Introducción a estándares como IEC 62443, NIS2, ISO/IEC 27001 y buenas prácticas para la gestión del riesgo y la continuidad operativa.

5. Medidas de protección y defensa en profundidad Estrategias de segmentación, control de accesos, bastionado de dispositivos, seguridad en las comunicaciones y monitorización continua.

6. Gestión de vulnerabilidades y respuesta ante incidentes Procesos de detección, análisis y actuación frente a incidentes de ciberseguridad en OT. Simulacros y planes de resiliencia.

7. Talleres prácticos y simulaciones técnicas Laboratorios virtuales de simulación de redes industriales, captura y análisis de tráfico, pentesting básico, honeypots y herramientas de ciberseguridad OT (SIEM, IDS, EDR, etc.).

8. Conclusiones y recomendaciones finales Revisión de aprendizajes clave, buenas prácticas para la implementación de medidas y madurez en ciberseguridad industrial.