

CIBERSEGURIDAD INDUSTRIAL

MODALIDAD: HÍBRIDA

CARGA HORARIA: 60 hs

OBJETIVOS DE LA PROPUESTA ACADÉMICA

Este programa proporciona una comprensión sólida de la ciberseguridad industrial, desde los fundamentos hasta la implementación práctica. Los participantes adquirirán habilidades esenciales para proteger las infraestructuras críticas y mantener la continuidad de las operaciones en entornos industriales.

PERFIL DEL/A GRADUADO/A

La/el egresada/o contará con un bagaje teórico y práctico podrá desarrollar su actividad laboral en empresas de cualquier tamaño, públicas y privadas, por cuenta propia o ajena, de distintos sectores de mantenimiento, control de calidad y otros.

En este marco, la/el egresada/o habrá consolidado competencias formativas y actitudinales con capacidades técnicas que la/lo capacitan para desempeñarse en el desarrollo e implementación de proyectos de robótica y ciberseguridad industrial.

CONTENIDOS

CÓDIGO	MÓDULO	CARGA HORARIA	TEMARIO
1	Introducción a la Ciberseguridad Industrial	4 h	<ul style="list-style-type: none">• Conceptos fundamentales de ciberseguridad industrial.• Importancia de la ciberseguridad en entornos industriales.• Amenazas y desafíos específicos.
2	Infraestructura Industrial y Vulnerabilidades	6 h	<ul style="list-style-type: none">• Componentes de la infraestructura industrial.• Identificación de vulnerabilidades.• Evaluación de riesgos y amenazas.

CÓDIGO	MÓDULO	CARGA HORARIA	TEMARIO
3	Normativas y Estándares de Ciberseguridad Industrial	8 h	<ul style="list-style-type: none"> Cumplimiento de regulaciones y estándares industriales. ISO 27001, NIST, IEC 62443, y otros. Desarrollo de políticas de seguridad.
4	Protección de Redes y Sistemas Industriales	10 h	<ul style="list-style-type: none"> Diseño de redes seguras. Firewalls industriales y sistemas de detección de intrusiones. Segmentación de redes y control de acceso.
5	Gestión de Incidentes de Ciberseguridad Industrial	6 h	<ul style="list-style-type: none"> Detección y respuesta a incidentes. Planificación de continuidad de operaciones. Recuperación después de un ataque.
6	Tecnologías de Seguridad Industrial	8 h	<ul style="list-style-type: none"> Criptografía y autenticación. Protección de sistemas de control industrial (ICS). Monitoreo de seguridad en tiempo real.
7	Evaluación de Vulnerabilidades y Pruebas de Penetración	4 h	<ul style="list-style-type: none"> Escaneo de vulnerabilidades. Pruebas de penetración en sistemas industriales. Informes y mitigación de vulnerabilidades.
8	Concienciación y Formación en Ciberseguridad	6 h	<ul style="list-style-type: none"> Capacitación de personal en ciberseguridad. Creación de una cultura de seguridad. Concienciación sobre ingeniería social.
9	Desarrollo de Planes de Ciberseguridad Industrial	6 h	<ul style="list-style-type: none"> Planificación estratégica de ciberseguridad. Implementación de medidas de seguridad. Evaluación y mejora continua.
10	Evaluación Final y Certificación	2 h	<ul style="list-style-type: none"> Examen teórico para evaluar los conocimientos adquiridos en las unidades anteriores.