



CIBERSEGURIDAD OT OPERATIVO

Impartido por: **Capacitaciones GoCursos Spa**

Modalidad
Presencial/Elearning

Reunión con Relator
Costo 0

Incluye
Diploma y Certificado





Objetivo general

Proporcionar una comprensión integral de la ciberseguridad en entornos operativos.



Objetivos específicos

- Identificar vulnerabilidades específicas en sistemas de control industrial.
- Implementar estrategias de mitigación de riesgos en entornos OT.
- Desarrollar habilidades para responder a incidentes de seguridad en tiempo real.



Modalidad

Presentamos todas las modalidades que ofrecemos a nuestros alumnos.



ONLINE

Clases asincrónicas, entregándote la libertad de estudiar en el momento y lugar que tú decidas.



ONLINE EN VIVO

Clases remotas en vivo, donde profesor y alumnos se conectan e interactúan en tiempo real, en una fecha y horario establecido



PRESENCIAL

Asiste físicamente a las clases, en nuestras salas o en las propias dependencias del cliente.

Temario del curso:

Módulo 1

Introducción a la Ciberseguridad OT
Aprendizaje Esperado: Comprender la importancia de la ciberseguridad en entornos operativos.

Contenidos:

Definición y contexto de la ciberseguridad OT.
Riesgos y amenazas en sistemas de control industrial.

Comparación entre IT y OT en términos de seguridad.

Impacto de los ciberataques en infraestructuras críticas.

Actividad Práctica: Realizar un análisis de riesgos básico identificando posibles vulnerabilidades en un sistema de control industrial simulado, utilizando herramientas en línea.

Módulo 2

Vulnerabilidades y Amenazas en Sistemas OT
Aprendizaje Esperado: Identificar amenazas comunes y vulnerabilidades en entornos operativos.

Contenidos:

Exploración de vulnerabilidades en dispositivos ICS y SCADA.

Amenazas internas y externas en sistemas OT.

Evaluación de riesgos y su impacto en la producción.

Técnicas de hacking ético en entornos industriales.

Actividad Práctica: Simular un ataque cibernético controlado en un entorno virtual OT para evaluar las respuestas del sistema y desarrollar estrategias de mitigación.

Módulo 3

Estrategias de Mitigación de Riesgos

Aprendizaje Esperado: Desarrollar e implementar estrategias efectivas de mitigación de riesgos.

Contenidos:

Diseño de políticas de seguridad para entornos OT.

Implementación de firewalls y sistemas de detección de intrusos.

Seguridad en la red y segmentación de sistemas OT.

Monitoreo y auditoría de seguridad en tiempo real.

Actividad Práctica: Configurar un sistema de detección de intrusos en un entorno de simulación y analizar los resultados para mejorar la seguridad del sistema.

Módulo 4

Respuesta a Incidentes y Recuperación

Aprendizaje Esperado: Desarrollar habilidades para responder y recuperar de incidentes de seguridad.

Contenidos:

Procedimientos de respuesta a incidentes en sistemas OT.

Recuperación y continuidad del negocio tras un ciberataque.

Coordinación con equipos de IT y OT durante incidentes.

Mejores prácticas para la comunicación de incidentes.

Actividad Práctica: Realizar un ejercicio de simulación de respuesta a un incidente cibernético, coordinando acciones entre equipos y evaluando la efectividad de las medidas implementadas.

Datos del Organismo Capacitador:

Nombre Empresa OTEC:	Capacitaciones GoCursos SPA
Rut:	77919346-2
Giro:	Servicio de Capacitaciones
Dirección	Irrazaval 690 Ñuñoa Santiago de Chile
Cuenta Bancaria	Cuenta Corriente 95466877 Banco Santander
Email:	contacto@gocursos.cl