



# TÉCNICAS DE CIBERSEGURIDAD SENCE

Impartido por: Capacitaciones GoCursos Spa

Modalidad Presencial/Elearning

Reunión con Relator Costo 0 Incluye
Diplima y Certificado













# Objetivo general

Capacitar a los participantes en la implementación de técnicas de ciberseguridad basadas en el marco NIST, reconociendo la importancia de la protección de datos, la privacidad, y la gestión de ciberataques en contextos organizacionales.



## Objetivos específicos

- Reconocer las dimensiones de protección y privacidad de datos según la normativa y el contexto organizacional.
- Aplicar técnicas de ciberseguridad basadas en marcos de referencia como NIST.
- Identificar y analizar ciberataques, implementando estrategias de defensa según sus características.



## 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:

#### 1Módulo 01: Introducción a la Ciberseguridad

Definición y objetivos de la ciberseguridad. Importancia de la ciberseguridad en entornos organizacionales.

Principales amenazas y vulnerabilidades cibernéticas.

Breve historia y evolución de la ciberseguridad.

#### Módulo 02: Estándar NIST y Marcos de Referencia

Introducción al marco NIST de ciberseguridad. Componentes clave del NIST: Identificar, Proteger, Detectar, Responder, y Recuperar. Comparación del NIST con otros marcos de referencia (ISO 27001, CIS Controls). Ventajas de usar el estándar NIST en organizaciones.

#### Módulo 03: Protección y Privacidad de Datos

Principios básicos de protección de datos. Regulaciones y normativas aplicables (GDPR, Ley de Protección de Datos en Chile). Métodos para garantizar la privacidad de los usuarios.

Herramientas y técnicas para proteger información confidencial.

#### Módulo 04: Técnicas de Ciberseguridad

Aplicación de firewalls y sistemas de detección de intrusos (IDS/IPS). Gestión de contraseñas y autenticación multifactor (MFA). Cifrado de datos en tránsito y en reposo.

Cifrado de datos en transito y en reposo Políticas de seguridad para usuarios y dispositivos.

## Módulo 05: Identificación y Respuesta a Ciberataques

Tipos de ciberataques: phishing, ransomware, DDoS, entre otros.

Reconocimiento de patrones y señales de ataque.

Estrategias para responder a incidentes de seguridad.

Simulaciones prácticas de análisis y mitigación de ciberatagues.

#### Módulo 06: Seguridad en Redes y Sistemas

Principios de seguridad en redes corporativas. Segmentación de redes y control de acceso. Seguridad en la nube y entornos híbridos. Actualización y mantenimiento de sistemas operativos y software.

## Módulo 07: Implementación de un Plan de Ciberseguridad

Pasos para desarrollar un plan de ciberseguridad organizacional. Evaluación de riesgos y auditorías de seguridad.

Capacitación y concienciación de empleados. Pruebas de penetración y análisis de vulnerabilidades.

#### Módulo 08: Recuperación y Mejora Continua

Estrategias de recuperación ante incidentes de ciberseguridad.

Monitoreo y mejora continua del plan de seguridad.

Lecciones aprendidas de incidentes previos. Conclusiones y reflexiones finales.







### Datos del Organismo Capacitador:

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





