



TECNICAS DE CIBERSEGURIDAD.

Impartido por: **Capacitaciones GoCursos Spa**

Modalidad
Presencial/Elearning

Reunión con Relator
Costo 0

Incluye
Diploma y Certificado





Objetivo general

2 Proveer un conocimiento profundo en técnicas de ciberseguridad para proteger sistemas y datos.



Objetivos específicos

- 3 Entender los conceptos básicos de ciberseguridad.
- Identificar y evaluar amenazas cibernéticas.
- Implementar medidas de seguridad efectivas.



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: Fundamentos De Ciberseguridad

Aprendizaje esperado: Conocer los principios básicos de seguridad informática.

- Conceptos básicos: Introducción a la ciberseguridad, sus objetivos y desafíos.
 - Amenazas y vulnerabilidades: Identificación de riesgos en sistemas informáticos.
 - Tipos de ataques: Análisis de diferentes tipos de ataques cibernéticos.
 - Políticas de seguridad: Implementación de políticas para mitigar riesgos.
- Actividad práctica: Estudio de caso sobre un incidente de seguridad real.

Módulo 2: Criptografía

Aprendizaje esperado: Comprender el uso de la criptografía en la protección de datos.

- Algoritmos criptográficos: Estudio de algoritmos de cifrado más utilizados.
 - Criptografía simétrica: Uso y aplicación de cifrado simétrico.
 - Criptografía asimétrica: Funcionamiento y ventajas del cifrado asimétrico.
 - Firmas digitales: Importancia y aplicación de firmas digitales.
- Actividad práctica: Simulación de un sistema de cifrado.

Módulo 3: Seguridad En Redes

Aprendizaje esperado: Implementar medidas de seguridad en redes de comunicación.

- Configuración de firewalls: Uso de firewalls para proteger redes.
 - Seguridad en redes inalámbricas: Técnicas para asegurar redes wifi.
 - Detección de intrusos: Métodos para identificar intrusiones en redes.
 - VPN y conexiones seguras: Implementación de redes privadas virtuales.
- Actividad práctica: Configuración de un firewall en un entorno simulado.

Módulo 4: Gestión De Incidentes

Aprendizaje esperado: Responder efectivamente a incidentes de seguridad.

- Planificación de respuesta: Creación de planes para manejar incidentes.
 - Análisis forense: Técnicas para investigar incidentes post-mortem.
 - Recuperación de desastres: Estrategias para la recuperación de sistemas.
 - Comunicación en crisis: Manejo de la comunicación durante incidentes.
- Actividad práctica: Juego de rol sobre gestión de una crisis de seguridad.

Módulo 5: Seguridad En Aplicaciones

Aprendizaje esperado: Proteger aplicaciones contra vulnerabilidades comunes.

- Desarrollo seguro: Principios de programación segura.
 - Pruebas de penetración: Evaluación de la seguridad de aplicaciones.
 - Gestión de parches: Implementación de actualizaciones de seguridad.
 - Seguridad en aplicaciones web: Protección contra ataques web.
- Actividad práctica: Pruebas de penetración en una aplicación web simulada.

Módulo 6: Seguridad En La Nube

Aprendizaje esperado: Asegurar datos y aplicaciones en entornos de nube.

- Modelos de servicio en la nube: Comprensión de SaaS, PaaS, IaaS.
- Riesgos en la nube: Identificación de amenazas específicas de la nube.
- Herramientas de seguridad: Uso de herramientas para proteger datos en la nube.

y mucho más...

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