



TÉCNICAS DE CIBERSEGURIDAD EN REDES Y TECNOLOGÍAS DE LA INFORMACIÓN

Impartido por: **Capacitaciones GoCursos Spa**

Modalidad
Presencial/Elearning

Reunión con Relator
Costo 0

Incluye
Diploma y Certificado





Objetivo general

Formar en las principales áreas de conocimiento, habilidades y estándares que necesita el especialista en Seguridad de la Tecnología de la Información para realizar las tareas profesionales relacionadas con el desarrollo de planes y procesos de seguridad para la tecnología de la información y la ciberseguridad.



Objetivos específicos

- Identificar y mitigar vulnerabilidades
- Implementar medidas de protección
- Responder a incidentes de seguridad
- Fortalecer la seguridad en entornos de red



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:

<ul style="list-style-type: none"> • MÓDULO 1: Fundamentos de Seguridad en Redes: Hardware • Firewalls de hardware y software • Firewalls con estado. Deep Packet Inspection (DPI) • Firewall de nivel de aplicación • Uso de servidores, servidores de pasarela, VPN y servidores proxy • Diferencias entre tipos de proxies: <ul style="list-style-type: none"> • Proxies inversos • Proxies transparentes • Proxies anónimos • Proxies altamente anónimos • Socks 4 y proxies 5 • Proxies del Sistema de Nombres de Dominio (DNS) • Redes perimetrales o "Zona desmilitarizada" (DMZ) • Redundancia de datos y RAID (matriz redundante de discos independientes) • Cómo se implementa la redundancia de datos • Lista de tipos de matrices RAID • Configuración de procedimientos de seguridad física para sistemas de TI • Uso de "embedded system security". Acceso al nivel de seguridad • MÓDULO 2: Software de Seguridad de Red • Protocolos de red • Modelo OSI y su relación con la seguridad de la red • Números de puerto básicos respecto a la seguridad de la red • Administración de parches y la seguridad del software 	<ul style="list-style-type: none"> • Antivirus • Anti-malware • Implementación de software de seguridad • Métodos para gestión de control de acceso • Mitigaciones de ataque DNS • Denegación de servicio (DoS) • Denegación de servicio distribuido (DDoS) • Envenenamiento de caché (Cache Poisoning) • Amplificación de DNS • DNS de flujo rápido • Zero Day Attack • Secuestro de TCP / IP • Man-in-the-Middle. Replay Attack • Evil Twin • Procedimiento de seguridad de acceso a SQL • Configuración de Internet Information Services (IIS) para acceder a SQL Server • SQL Injection Attack • MÓDULO 3: Seguridad Inalámbrica • Estándares de seguridad inalámbrica IEEE • Propósito de las claves de cifrado inalámbricas • Temporal Key Integrity Protocol (TKIP) • Advanced Encryption Standard (AES) • 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