



CIBERSEGURIDAD DEFENSIVA Y PREVENTIVA: PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE AMENAZAS DIGITALES

Impartido por: **Capacitaciones GoCursos Spa**

Modalidad
Presencial/Elearning

Reunión con Relator
Costo 0

Incluye
Diploma y Certificado





Objetivo general

Desarrollar conocimientos y habilidades para identificar, prevenir y responder ante las principales amenazas de ciberseguridad, aplicando buenas prácticas en el uso seguro de tecnologías, la protección de la información y la gestión inicial de incidentes de seguridad en entornos personales y organizacionales.



Objetivos específicos

- Identificar los principales riesgos, amenazas y vulnerabilidades asociados al uso de tecnologías de la información, aplicando medidas preventivas para fortalecer la seguridad digital.
- Reconocer las principales modalidades de malware, ransomware e ingeniería social, implementando buenas prácticas para prevenir y detectar ataques cibernéticos.
- Aplicar procedimientos básicos para el uso seguro del correo electrónico, la navegación web y la respuesta inicial frente a incidentes de ciberseguridad.



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 la Ciberseguridad Defensiva y Preventiva

Contenidos:

Conceptos fundamentales de ciberseguridad: confidencialidad, integridad y disponibilidad de la información.
Diferencias entre ciberseguridad proactiva y reactiva.
Identificación de amenazas, vulnerabilidades y análisis de riesgos.
Estrategias de prevención, detección temprana, respuesta y recuperación frente a incidentes.
Buenas prácticas para fortalecer la seguridad digital en entornos personales y laborales.

Actividad Práctica: Auditoría personal de seguridad digital mediante la identificación de riesgos y definición de acciones de mejora.

Módulo 2

Identificación y Manejo de Malware y Ransomware

Contenidos:

Concepto y clasificación del malware: virus, troyanos, gusanos, spyware, adware, keyloggers y ransomware.
Ciclo de vida del ransomware y principales vectores de ataque.
Formas de propagación mediante archivos adjuntos, descargas, dispositivos USB y vulnerabilidades del sistema.
Consecuencias operacionales, económicas y reputacionales de un ataque.
Medidas de prevención y mitigación: respaldos, segmentación de redes, listas blancas de aplicaciones y control de accesos.

Actividad Práctica: Simulación de una infección por malware para identificar el origen del ataque, analizar sus causas y proponer medidas preventivas.

Módulo 3

Phishing e Ingeniería Social: Técnicas y Prevención

Contenidos:

Conceptos y fundamentos de la ingeniería social.
Phishing y sus principales variantes: spear phishing, vishing, smishing, pretexting y baiting.
Técnicas de manipulación psicológica utilizadas por los ciberdelincuentes.
Identificación de correos electrónicos, mensajes y sitios web fraudulentos.
Análisis de casos reales y estrategias para prevenir ataques de ingeniería social.

Actividad Práctica: Análisis de correos electrónicos y mensajes sospechosos para identificar indicadores de fraude y definir las medidas de prevención correspondientes.

Módulo 4

Uso Seguro del Correo Electrónico y la Navegación Web

Contenidos:

Buenas prácticas para una navegación web segura.

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