



ADVANCED IN AI SECURITY MANAGEMENT (AAISM)

Impartido por: **Capacitaciones GoCursos Spa**

Modalidad
Presencial/Elearning

Reunión con Relator
Costo 0

Incluye
Diploma y Certificado





Objetivo general

Desarrollar competencias para diseñar, implementar y gestionar estrategias de seguridad en sistemas de inteligencia artificial, abordando gobierno, riesgos y controles tecnológicos conforme a estándares internacionales.



Objetivos específicos

- Aplicar marcos de gobierno y gestión de programas de seguridad en IA.
- Evaluar y mitigar riesgos asociados al ciclo de vida de sistemas de IA.
- Implementar controles técnicos y organizacionales para asegurar sistemas de IA.



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 Seguridad en Inteligencia Artificial

Contenidos:

Conceptos de inteligencia artificial y machine learning.

Ciclo de vida de sistemas de IA.

Superficie de ataque en sistemas de IA.

Amenazas emergentes: adversarial attacks, data poisoning, model leakage.

Actividad Práctica: Identificación de riesgos en un caso básico de sistema de IA.

Módulo 2

Gobernanza de IA y Gestión de Programas

Contenidos:

Gobierno de IA y frameworks internacionales (ISACA, NIST, ISO).

Políticas, procedimientos y estrategias de seguridad en IA.

Gestión de stakeholders y cumplimiento regulatorio.

Gestión del ciclo de vida de datos y activos de IA.

Actividad Práctica: Diseño de un modelo de gobernanza para un proyecto de IA.

Módulo 3

Gestión de Riesgos en Sistemas de IA

Contenidos:

Identificación y análisis de riesgos en IA.

Evaluación de amenazas y vulnerabilidades.

Gestión de riesgos en proveedores y supply chain de IA.

Tratamiento y mitigación de riesgos en IA.

Actividad Práctica: Elaboración de una matriz de riesgos aplicada a IA.

Módulo 4

Arquitectura y Seguridad de Sistemas de IA

Contenidos:

Arquitecturas seguras para sistemas de IA.

Seguridad en entrenamiento, validación y despliegue de modelos.

Protección de datos y privacidad en IA.

Seguridad en pipelines de machine learning.

Actividad Práctica: Análisis de arquitectura segura en un caso de uso real.

Módulo 5

Controles de Seguridad y Monitoreo en IA

Contenidos:

Controles técnicos y organizacionales en IA.

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