Global Lynx®

MAKINGITBETTER!

IA SEGURA

Domina los riesgos antes de que te alcancen.

CURSO GRATUITO

WWW.GLOBALLYNX.COM.MX

CURSO GRATUITO

En apoyo a la comunidad de Profesionales de TI
Global Lynx dona el curso:

IA SEGURA

Domina los riesgos antes de que te alcancen.

- Del 8 al 11 de septiembre
- De 10:00 h a 12:00 h (GMT-6)
- En línea con instructor en vivo
- 8 horas (6 módulos)
- 14 fases MITRE ATLAS (Hilo conductor del curso)

¡INSCRÍBETE AHORA!

Global Lynx

IMPULSA TU CARRERA CON LAS SIGUIENTES OPCIONES DISPONIBLES

Sin costo

Basic

$0.00 MXN

- Acceso al curso: Seguridad en la Inteligencia Artificial

Inscribirse ahora

El más recomendado | Opcional

Essentials

$399.00 MXN

- Acceso al curso: "IA segura. Domina los riesgos antes de que te alcancen."
- Constancia de Término de Curso.
- Acceso al Material del Curso durante 1 año.

Disponible pago con TDC

Inscribirse ahora

En caso de solicitar factura, se deberá de realizar lo siguiente:

Al momento de tu registro, selecciona la opción "Sí" en el campo "Requiero factura" para que nuestro equipo de ejecutivos pueda apoyarte en la solicitud y recepción de la información necesaria.

Si tienes alguna pregunta relacionada a facturación, por favor escríbenos un correo a **victor.sanchez@globallynx.com,** con el asunto: "Facturación: IA segura"

Global Lynx

Descripción del Curso

Modalidad

- En línea con instructor en vivo.

Duración

- 8 horas.
- 6 módulos.

Este curso te ofrecerá una guía completa y práctica para identificar los riesgos de seguridad asociados al uso cotidiano de herramientas de Inteligencia Artificial, y tomar acciones de protección.

Inicia con entender cómo el usuario expone su información al usar IA, entender cómo el atacante la usa para preparar y ejecutar el ataque, y qué medidas de protección están al alcance de cualquier usuario.

Provee una guía paso a paso para identificar las medidas de protección **basado en las 14 fases de MITRE ATLAS —** mostrando en cada fase cómo podría actuar un atacante y cómo el usuario puede interrumpirlo y defenderse, mediante un marco ágil de uso seguro de la IA, accionable y con ejemplos de un plan de tareas de 30 días. **Usa referencias como MITRE ATLAS, OWASP Top 10 LLM, NIST AI RMF, ISO 42001.**

Este curso incluye:

- **Ejercicios prácticos** por módulo guiados por instructor.
- **Casos reales** de incidentes con IA.
- **Ejemplo de plan de tareas** de uso seguro de IA.

Incluidos en el paquete Essentials:

- **Constancia digital** de participación.
- **Manual digital** con licencia de 1 año

Global Lynx

Objetivos del Curso

Al final del curso, el participante será capaz de:

- **Identificar los principales riesgos de seguridad** asociados al uso de herramientas de IA, incluyendo exposición de datos, suplantación de identidad y manipulación de información.
- **Aplicar mejores prácticas y controles** para proteger la información personal y laboral al interactuar con sistemas de IA.
- **Reconocer las fases de la cadena de ataque MITRE ATLAS** y las acciones concretas para interrumpir y protegerse en cada fase desde el rol de usuario final.

Especialmente relevante para:

- Gerentes y líderes que supervisan el uso de IA.
- Profesionales en ambientes corporativos que usan IA.
- Responsables de transformación digital, innovación o mejora de procesos.
- Consultores, coordinadores y tomadores de decisión que integran IA en operaciones.
- Organizaciones que buscan adoptar IA minimizando riesgos operativos y reputacionales.

Prerrequisitos del Curso

Interés en usar herramientas de IA de forma segura y responsable. **No se requiere experiencia previa en programación ni conocimientos técnicos de seguridad o inteligencia artificial.**

CONTENIDO

Módulo 1 — IA en el Entorno Profesional Actual
MITRE ATLAS: Reconnaissance · Resource Development

- IA en el entorno profesional: impacto real en organizaciones y roles profesionales.
- Reconnaissance: cómo el atacante investiga al usuario — y cómo reducir la visibilidad como objetivo.
- Resource Development: cómo el atacante construye su arsenal — y cómo evitar ser su recurso.
- Los tres cuadrantes de riesgo: aplicaciones de IA, endpoints y plataformas.
- Marcos de referencia de seguridad en IA: NIST AI RMF, ISO 42001, ISO 23894, OWASP Top 10 LLM, MITRE ATLAS y RAI v2.

Módulo 2 — Riesgos de Seguridad en el Uso Cotidiano de IA
MITRE ATLAS: Initial Access · ML Model Access · Execution

- Initial Access: phishing con IA generativa, credenciales comprometidas y extensiones maliciosas.
- ML Model Access: fugas de información por prompts mal construidos — cómo construir un prompt seguro.
- Execution: prompt injection directa, indirecta y ciega — señales de alerta y acciones de respuesta.
- MITRE ATLAS para el usuario: las amenazas más comunes en las fases 3, 4 y 5.
- OWASP Top 10 para LLMs: los 10 riesgos críticos traducidos en preguntas de autoevaluación.
- Ejercicio: identifica el vector de ataque en tu uso actual de IA.

Módulo 3 — Identidad Digital y Privacidad en la Era de IA
MITRE ATLAS: Persistence · Privilege Escalation · Defense Evasion · Credential Access

- Persistence: señales de acceso no autorizado persistente — cómo detectarlo y reportarlo.
- Suplantación con IA: clonación de voz, deepfakes, perfiles sintéticos y cómo verificar identidad.
- Privilege Escalation y Defense Evasion: mínimo privilegio y validación de outputs inusuales.
- Credential Access: gestión de credenciales, MFA y el filtro de 3 preguntas antes del prompt.
- Clasificación de información: 4 niveles prácticos para decidir qué puede ir en un prompt de IA.
- Ejercicio: clasifica tu información y bloquea al atacante en sus fases de persistencia.

Módulo 4 — Políticas y Mejores Prácticas de Uso Seguro
MITRE ATLAS: Discovery · Collection

- Discovery: las políticas de uso de IA bloquean al atacante antes de que mapee tu entorno.
- Collection: límites de acceso, gestión de sesiones y configuraciones de privacidad por plataforma.
- Cómo proteger tu información en ChatGPT, Microsoft Copilot, Google Gemini y Claude.
- IA Responsable (RAI v2 Microsoft): 6 principios de uso ético y criterios de responsabilidad del usuario.
- Ejercicio: auditoría de accesos y configuraciones de privacidad en tus herramientas de IA actuales.

Módulo 5 — Ética, Propiedad Intelectual y Cumplimiento
MITRE ATLAS: ML Attack Staging

- ML Attack Staging: el usuario como última línea de defensa antes del ataque final.
- Responsabilidad del usuario ante el output de IA: cómo validar antes de actuar.
- Propiedad intelectual y IA: riesgos legales y criterios prácticos para el uso de contenido generado.
- Cumplimiento regulatorio: ISO 42001, ISO 23894 y GDPR aplicados al usuario final.

Módulo 6 — Framework Práctico de Uso Seguro de IA
MITRE ATLAS: Exfiltration · Impact

- Exfiltration: señales de que tu información está siendo extraída — cómo detectarlo y detenerlo.
- Modelo de adopción segura: árbol de decisión de 5 preguntas antes de usar IA para cualquier tarea.
- Checklist de uso seguro y protocolo de reporte de incidentes de seguridad en IA.
- Caso aplicado: 3 perfiles ante el mismo incidente de exfiltración — decisiones y aprendizajes.
- Ejercicio integrador: hoja de ruta personal de uso seguro de IA — los próximos 30 días.

Global Lynx

Tu carrera en Inteligencia Artificial comienza aquí:

Curso diseñado para construir el futuro

Global Lynx®
making IT better!

Acerca de Nosotros

Ofrecemos Servicios de Capacitación y Consultoría en Tecnologías de la Información y Negocios; tenemos 30 años apoyando a profesionales y organizaciones en México, USA y LATAM.

Hemos capacitado a más de 5,000 profesionales durante el último año

Principales Áreas de Experiencia:

- Seguridad de la Información
- Ciberseguridad
- Continuidad de Negocio
- Gestión de Riesgos
- Gobierno y Cumplimiento de TI
- Gestión de Servicios de TI
- Metodologías Ágiles
- Gestión de Proyectos
- DevOps
- Gestión de Datos

¿Por qué nos Eligen Nuestros Clientes?

Instructores Acreditados, Certificados y Capacitados

Instructores especialistas en las normas, marcos y estándares más reconocidos por la industria que además implementan éstas a través de nuestros Servicios de Consultoría.

Reconocimiento por Organismos Internacionales

Al estar acreditados por los organismos más importantes de la industria, las certificaciones obtenidas tienen validez oficial a nivel internacional.

Más de 120 Cursos Relacionados con Tecnologías de la Información

Contamos con uno de los portafolios de cursos más grande en Latinoamérica, con opciones específicas para cada necesidad profesional.

Curso desarrollado por Global Lynx®

En Global Lynx®, ofrecemos cursos diseñados internamente para satisfacer las demandas del mercado actual. Con instructores experimentados y contenidos actualizados, garantizamos una experiencia de capacitación de alto nivel.

Global Lynx

Conoce más sobre **nuestros Servicios de Consultoría en Inteligencia Artificial**

Ver más

Consulte más cursos **relacionados con Inteligencia Artificial**

Ver más

Consulte **próximas fechas en nuestro calendario**

Ver más

¡Contáctanos!

Oficina México

Av. Paseo de la Reforma 180
Piso 14, Oficina 1414
Col. Juárez, 06600
Ciudad de México, México

+52 (55) 5511 0193
con terminaciones 95 y 97

+52 56 6049 3865

contact@globallynx.com

Oficina USA

5000 Arlington Centre Blvd.
Building 6, Suite 6133
Columbus, OH 43220
USA

+1 (614) 347-1994

administration@globallynx.com

Sé parte de nuestra comunidad digital
Encuéntranos como Global Lynx México