



AMEST

ACADEMIA MEXICANA DE ESTUDIOS TECNOLÓGICOS

PLAN DE ESTUDIOS · 2026

Ciberseguridad e IA: Arquitectura Digital

Infraestructura · Inteligencia Artificial · Ciberseguridad

Un programa para comprender, diseñar y proteger la nueva arquitectura digital de las organizaciones.

EN COLABORACIÓN CON

CISO  club

AMEST · CISOCLUB





Cinco módulos. Una sola arquitectura digital.

El programa conecta estrategia, IA, confianza verificable, grandes modelos de lenguaje y una visión aplicada desde la industria.

01 IA, Agentes y Ciberseguridad: Estrategia, Gobernanza y Amenazas Emergentes

Mtro. Juan José Gutierrez



02 IA Estratégica: Tecnología, Aplicaciones y Nuevos Desafíos

Mtro. Cesar Cisneros



03 Confianza verificable en tiempos de la IA

Dra. Erika Mata



04 Grandes Modelos de Lenguaje (como ChatGPT) y Ciberseguridad

Dr. Carlos Moreno





Mtro. Juan José Gutierrez



Juan Gutiérrez cuenta con 32 años de experiencia en el mundo TI. Actualmente es VP del Programa Ejecutivo en Gartner México para Latinoamérica, compañía en la que se encuentra desde el 2005.

Su rol es ser asesor de directores de tecnología, directores generales y financieros a lo largo de Latinoamérica en la toma de decisiones relacionadas a tecnología, así como guía en la formulación de estrategias en temas tales como Inteligencia Artificial, IT Financials, IT Strategy, Analytics, Ciberseguridad y Digital Business entre otros.

MÓDULO 1

IA, Agentes y Ciberseguridad: Estrategia, Gobernanza y Amenazas Emergentes

OBJETIVO GENERAL

Comprender cómo la inteligencia artificial está transformando tanto la estrategia y operación de las organizaciones como el panorama actual de la ciberseguridad, abordando su implementación, impacto financiero, gobernanza y los nuevos riesgos derivados del uso de IA por parte de actores maliciosos.

OBJETIVOS ESPECÍFICOS

01

Comprender los elementos necesarios para desarrollar una estrategia de inteligencia artificial alineada con los objetivos de una organización.

02

Analizar los aspectos financieros asociados con la adopción, implementación y operación de soluciones de IA.

03

Identificar los principales retos de gobernanza, control y seguridad relacionados con agentes de inteligencia artificial.

04

Analizar cómo la IA está modificando las técnicas utilizadas por los ciberdelincuentes y reconocer las principales tendencias emergentes en ciberseguridad.



Mtro. Cesar Cisneros



César Omar Cisneros Melgoza es cofundador y CTO de Birdie, plataforma de gestión de cadena de suministro respaldada por Techstars y 500 Global, donde lidera el desarrollo tecnológico y la incorporación de inteligencia artificial en operaciones logísticas. Cuenta con amplia experiencia en liderazgo tecnológico, ciberseguridad y desarrollo de software, con trayectoria en Kavak, Grupo JA Del Río, URREA y Walmart México. Es también cofundador y COO de CISO Club. Es ingeniero por la UDLAP, MBA por la UVM, maestro en Ciberseguridad por Georgia Tech y en Inteligencia Artificial por UNIR, y actualmente cursa un doctorado en Ingeniería Astronáutica en Capitol Technology University. Fue reconocido con el CIO 100 en 2021.

MÓDULO 2

IA Estratégica: Tecnología, Aplicaciones y Nuevos Desafíos

OBJETIVO GENERAL

Comprender el panorama actual de la inteligencia artificial desde una perspectiva estratégica, analizando su evolución tecnológica, sus principales aplicaciones, el impacto que está generando en las organizaciones y los nuevos desafíos que acompañan su adopción.

OBJETIVOS ESPECÍFICOS

01

Comprender los conceptos, tecnologías y tendencias que están impulsando la evolución actual de la inteligencia artificial.

02

Identificar aplicaciones prácticas de IA en distintos procesos, industrias y contextos organizacionales.

03

Analizar el impacto de la inteligencia artificial en la toma de decisiones, la productividad, la innovación y los modelos de negocio.

04

Reconocer los principales retos asociados con la adopción de IA, incluyendo aspectos de seguridad, ética, gobernanza y uso responsable.

05

Explorar las tendencias emergentes y escenarios futuros que podrían transformar la manera en que personas y organizaciones interactúan con la inteligencia artificial.



Dra. Erika Mata



Directora de CISO BanCoppel y Prevención de Fraudes en Grupo Coppel.

Reconocida por Forbes como "Genio de la transformación digital" y Top Woman in Cybersecurity por WOMCY Latam. Doctora en Seguridad por la EPHE/Sorbona, cuenta con más de 25 años liderando estrategias de ciberseguridad en la banca global (BofA, BBVA, Citi, HSBC). Catedrática, conferencista internacional y referente en la gestión de riesgos de seguridad en entornos financieros.

MÓDULO 3

Confianza verificable en tiempos de la IA

OBJETIVO GENERAL

Comprender cómo diseñar mecanismos de confianza verificable en entornos digitales y de inteligencia artificial, mediante modelos, evidencias, arquitectura y estrategias que permitan evaluar, demostrar y fortalecer la confianza dentro de una organización.

OBJETIVOS ESPECÍFICOS

- 01 Comprender los principios de confianza verificable y su relevancia en entornos digitales impulsados por inteligencia artificial.
- 02 Diseñar un modelo de Trust Score que permita evaluar el nivel de confianza de procesos, sistemas, proveedores o activos.
- 03 Identificar y estructurar las evidencias necesarias para demostrar confianza de manera objetiva y verificable.
- 04 Diseñar una arquitectura de Verifiable Trust que conecte identidad, evidencias, controles y validación.
- 05 Desarrollar una estrategia de confianza verificable aplicable al contexto y necesidades de cada organización.



Dr. Carlos Moreno



El Dr. Carlos Francisco Moreno García es Associate Professor en Robert Gordon University y Co-Director del centro de investigación INSIGHT, en Aberdeen, Escocia. Su trabajo se enfoca en ciberseguridad, inteligencia artificial, aprendizaje de máquina, visión por computadora, biometría y ciencia de datos. Ha participado en proyectos de investigación a nivel internacional, incluyendo iniciativas para la industria, el sector salud y colaboraciones con instituciones como la UNAM.

MÓDULO 4

Grandes Modelos de Lenguaje (como ChatGPT) y Ciberseguridad

OBJETIVO GENERAL

Comprender los fundamentos tecnológicos que dieron origen a los Grandes Modelos de Lenguaje, su evolución hasta las plataformas actuales de inteligencia artificial y los principales retos de ciberseguridad asociados con su implementación y utilización.

OBJETIVOS ESPECÍFICOS

01

Entender las bases del funcionamiento e implementación de las técnicas que dieron origen a los Grandes Modelos de Lenguaje.

02

Analizar la evolución tecnológica que ha permitido a empresas como OpenAI desarrollar productos de inteligencia artificial como los disponibles actualmente.

03

Analizar críticamente los principales problemas y riesgos de ciberseguridad inherentes a los Grandes Modelos de Lenguaje.

04

Aplicar de manera práctica los conceptos estudiados mediante ejemplos y casos de uso.



Ciberseguridad e IA: Arquitectura Digital

Infraestructura · Inteligencia Artificial · Ciberseguridad

EN COLABORACIÓN CON

CISO  club