Curso de Auditoría en Machine Learning y Confianza Digital

Presentado por:

José Lagos, PhD, CISA, CISM, CDPSE

Introducción al Curso

La auditoría de modelos de Machine Learning se ha vuelto fundamental en las organizaciones modernas que buscan implementar inteligencia artificial de manera responsable y confiable.

Objetivo general: Entregar herramientas prácticas para auditar ML y garantizar implementaciones éticas y confiables.

Problemas actuales que enfrentan las organizaciones:

Sesgos y opacidad en los modelos

Los algoritmos pueden perpetuar discriminación y tomar decisiones sin transparencia

Incumplimiento normativo

Falta de adherencia a regulaciones emergentes sobre inteligencia artificial

Riesgos reputacionales y financieros

Pérdidas económicas y daño a la imagen corporativa por fallas en IA

Desplazamiento Laboral

Auditores sin conocimiento necesario para Auditar algoritmos o para desarrollar modelos de machine learning

Objetivos de Aprendizaje

01

Conocer metodologías de auditoría aplicadas a ML

Dominar frameworks y técnicas especializadas para evaluar modelos de inteligencia artificial

02

Identificar riesgos éticos, regulatorios y técnicos

Desarrollar capacidades para detectar vulnerabilidades y amenazas en sistemas de ML

03

Aplicar herramientas prácticas en casos reales

Utilizar tecnologías y metodologías en escenarios empresariales auténticos

04

Preparar a profesionales para marcos regulatorios emergentes

Anticiparse a nuevas normativas y estándares internacionales sobre IA

Metodología de Aprendizaje (Learning by Doing)

01

Exposiciones Teóricas (30%)

- Clases magistrales cortas, enfocadas en conceptos clave.
- Material de apoyo: presentaciones, papers seleccionados y normativa vigente (ISO, NIST, EU AI Act, Ley 21.719).
- Uso de ejemplos reales de fallos y riesgos en ML.

02

Talleres Prácticos (40%)

- Ejercicios en Python aplicando diferentes librerías
- Auditoría de un modelo preentrenado (ej. fraude financiero, scoring de clientes, detección de phishing).
- Aplicación de checklists y matrices de auditoría (riesgos, controles, cumplimiento).

03

Estudios de Casos (20%)

- Análisis de casos:
- Problemas de opacidad en algoritmos de scoring.
- Incumplimientos regulatorios en bancos/seguros.
- Discusión grupal y debate crítico.

04

Evaluación y Retroalimentación (10%)

- Mini-quizzes al final de cada módulo (Kahoot / Mentimeter).
- Trabajo final: auditoría de un modelo ML completo (end-to-end).
- Feedback inmediato del instructor.

Contenidos del Programa

Módulo 1: Fundamentos de Python para Auditoría en ML

- Introducción a Jupyter Notebook y Google Colab Tipos de datos y estructuras básicas en Python (list, dict, Data Frame)
- Librerías clave: pandas, numpy, scikit-learn, matplotlib
- Lectura y validación de datos (read_csv, info, describe)
- Ejecución de scripts y buenas prácticas de trazabilidad

Módulo 2: Introducción a Machine Learning y Confianza Digital

- Riesgos y Definiciones clave: IA, ML, Deep Learning
- Tipos de aprendizaje: supervisado, no supervisado, reforzamiento
- Concepto y pilares de la confianza digital
- Casos de uso y riesgos asociados en auditoría interna

Contenidos del Programa

Módulo 3: Ciclo de Vida del Modelo y Puntos de Auditoría

- Etapas: diseño, desarrollo, validación, implementación, monitoreo
- Controles clave y checklist de auditoría en cada fase
- Riesgos técnicos, operativos y regulatorios
- Herramientas de seguimiento y control

Módulo 4: Riesgos y Controles de ML

- Sesgos y equidad algorítmica
- Riesgos de data drift y concept drift
- Seguridad y protección de datos en modelos ML
- Cumplimiento normativo: Ley 21.719, GDPR, AI Act, NIST AI RMF
- Controles técnicos y organizativos recomendados

Contenidos del Programa

Módulo 5: Auditoría Técnica de Modelos de ML

- Validación de datos de entrenamiento y prueba
- Métricas clave: precisión, recall, Fl-score, AUC, fairness
- Técnicas de explicabilidad: SHAP, LIME
- Herramientas y flujos de trabajo para auditoría (MLflow, Evidently AI)
- Ejercicios prácticos de análisis de métricas

Módulo 6: Confianza Digital y Gobernanza IA

- Principios de confianza digital aplicados a ÍA
- Integración de auditoría de ML en frameworks de riesgo
- Trazabilidad y accountability
- Comunicación de hallazgos y transparencia hacia stakeholders

Contenidos del Programa

Módulo 7: Análisis de Casos

- Caso 1: Sistema Clinico Andino – Enfermedades Respiratorias
- Caso 2: TecnoFIX, Reparaciones de Celulares
- Discusión guiada sobre riesgos, oportunidades y hallazgos de auditoría

Módulo 8: Taller Práctico Integrado

- Auditoría completa de un modelo ML (caso real o sintético)
- Identificación de riesgos y brechas
- Elaboración de informe de auditoría con hallazgos y recomendaciones
- Presentación de resultados y debate grupal

Público Objetivo

Auditores internos y externos

Profesionales que buscan especialización en auditoría de sistemas inteligentes y evaluación de riesgos algorítmicos

CISOs y DPOs

Chief Information Security Officers y Data Protection Officers responsables de la seguridad y privacidad de datos

Gerentes de Riesgo y Cumplimiento

Ejecutivos encargados de gestionar riesgos corporativos y asegurar el cumplimiento normativo

Profesionales de Data Science

Científicos de datos y analistas que desarrollan e implementan modelos de machine learning

Beneficios Claves al perfil auditor

cybertrust

Evaluar transparencia y explicabilidad de modelos

Desarrollar capacidades para analizar la interpretabilidad de algoritmos y comunicar resultados de manera clara

Detectar sesgos y validar calidad de datos

Identificar discriminación algorítmica y asegurar la integridad de los conjuntos de datos utilizados

Cumplir con nuevas normativas sobre IA

Mantenerse actualizado con regulaciones emergentes y implementar marcos de cumplimiento efectivos

Obtener ventaja competitiva basada en confianza y responsabilidad

Diferenciarse en el mercado mediante prácticas éticas y transparentes en inteligencia artificial

Información Práctica – Curso Abierto

Duración:

32 horas distribuídas en 8 sesiones de 4 horas cada una

Modalidad:

100% Online

Fechas y horario:

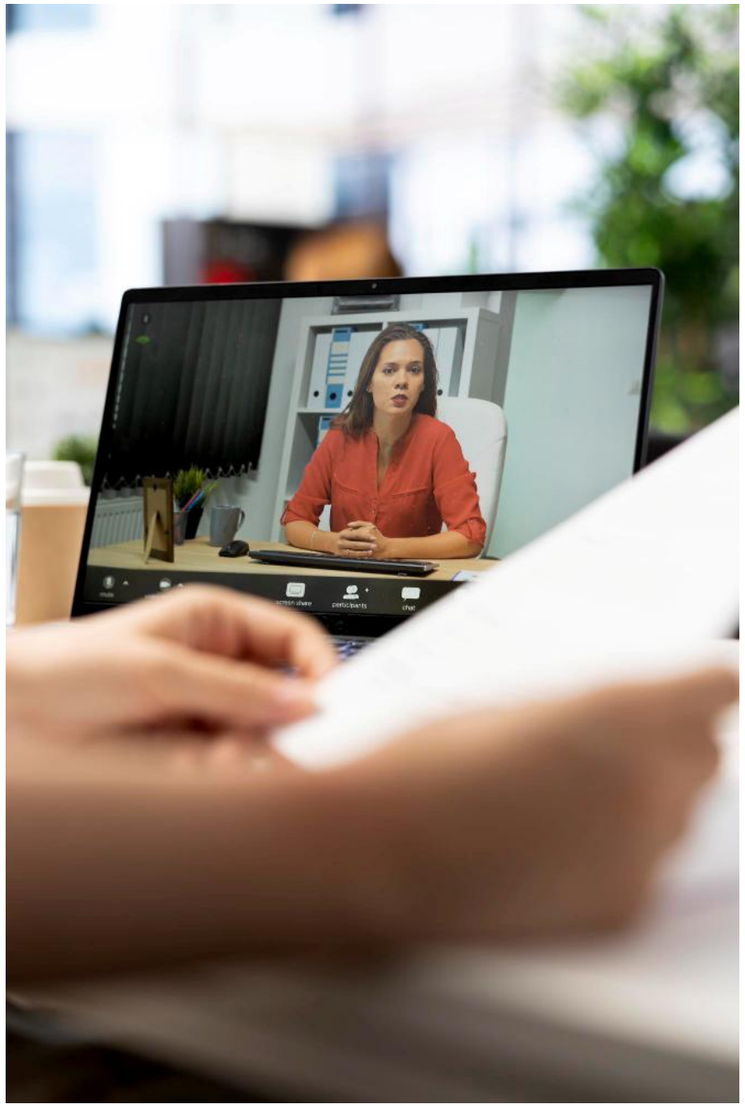
27 de Abril al 15 de Mayo
Lunes –Miércoles-Viernes
de 09:00 a 13:00 hrs

Valor:

18 UF por alumno

Requisitos Previos:

- Cuenta activa en ChatGPT (se recomienda suscripción Plus para acceso a modelos avanzados).
- Cuenta en Google Colab asociada a cuenta Goople personal o corporativa
- Manejo básico de Excel o Goople Sheets
- Conocimiento General en auditoría interna, TI o compliance
- Computador con conexión estable a internet, navegador actualizado, auriculares y micrófono



Información Práctica – Curso Cerrado

Duración:

32 horas distribuídas en 8 sesiones de 4 horas cada una

Fechas y horario:

Fechas y horarios a coordinar según disponibilidad del cliente.

Finalizar:

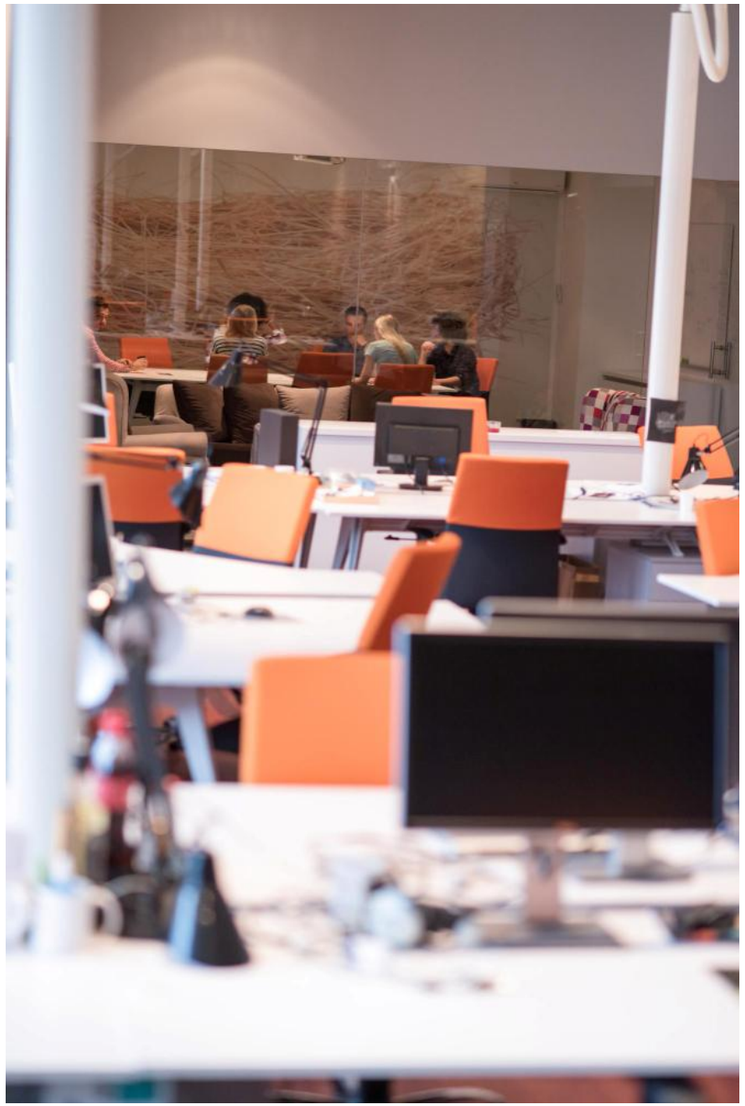
Al finalizar el curso se realiza una prueba, la cual al ser aprobada se entrega un certificado de aprobación.

Modalidad:

Modalidad exclusiva para equipos corporativos.
Online o presencial, en caso de ser presencial debe ser en instalaciones del cliente.

Requisitos Previos:

- Cuenta activa en ChatGPT (se recomienda suscripción Plus para acceso a modelos avanzados).
- Cuenta en Google Colab asociada a cuenta Goople personal o corporativa
- Manejo básico de Excel o Goople Sheets
- Conocimiento General en auditoría interna, TI o compliance
- Computador con conexión estable a internet, navegador actualizado, auriculares y micrófono



Certificaciones

Diploma de Asistencia

La Asistencia superior al 80% del curso otorgará un Diploma de Asistencia

Certificación de Auditoría IA

Las personas que deseen un certificado que acredite los conocimientos aprendidos, deberá rendir una evaluación teórico - práctica y obtendrá un certificado de aprobación, para lo cual es necesario una evaluación superior al 75%

Perfil del Relator, José Lagos

- Doctor en Administración de Negocios - Universidad de Chile
- Major en IA para los Negocios – George Washington University y ADEN Business School
- Major en Big Data y Análisis de Negocio –George Washington University y ADEN Business School.
- Fundamentos de IA y Machine Learning con Python – IEBS Business School (en curso)
- Certificado Profesional en Estrategia y Liderazgo IA – MIT xPRO
- Certificado en Ciberseguridad – MIT xPRO
- Certificado en Trasnformación Digital – MIT xPRO
- Leadership CISO Program – Carnegie Mellon University
- Cybersecurity and Technology – Harvard Kennedy School
- Certificado de Crisis Management en Kellogg School of Management
- Certificado en Gobiernos Corporativos en Kellogg School of Management
- PADE – Programa de Alta Administración – Universidad de los Antes
- Master en Gestión de Negocios – Universidad Adolfo Ibañez
- Master en Marketing y Comercialización – Universidad Adolfo Ibañez
- Master en Tecnología y Gestión, Universidad Católica de Chile

SCAN ME

https://www.linkedin.com/in/joseantoniolagos/

"Auditar IA hoy es proteger el negocio del mañana"

Consultas e inscripciones: academiacybertrust@cybertrust.one

🌐 cybertrustlatam.one

Únete a la revolución de la auditoría inteligente y lidera el futuro de la IA responsable