Capacita
e-Learning

Executive Internal Audit
Program

Auditoría de Inteligencia Artificial (IA) basada en riesgos: Implementación de ISO 42001 y la métrica del NIST AI RMF

17, 18, 19 y 20 de noviembre, 2026
15:00 Centroamérica
Programa online en vivo

Wilson Andia Cuiza

MSc, CISA, CRISC, CSX, CDPSE, ISO 27001 LA

Descripción del Curso

Introducción

La Inteligencia Artificial está transformando la manera en que las organizaciones toman decisiones, automatizan procesos y generan valor. Sin embargo, su adopción también introduce nuevos riesgos relacionados con la privacidad, la ciberseguridad, los sesgos algorítmicos, la falta de transparencia, el incumplimiento regulatorio y la toma de decisiones automatizadas.

Los enfoques tradicionales de auditoría ya no son suficientes para evaluar estos nuevos riesgos. Los auditores requieren metodologías especializadas que les permitan analizar no solo la tecnología, sino también la gobernanza, el ciclo de vida de los modelos, la calidad de los datos, la supervisión humana y la gestión integral del riesgo.

La publicación de la **ISO/IEC 42001**, primer estándar internacional certificable para Sistemas de Gestión de Inteligencia Artificial (AIMS), junto con el **NIST Artificial Intelligence Risk Management Framework (AI RMF)**, proporciona un marco sólido para evaluar la implementación responsable de la IA desde una perspectiva de gobierno, riesgos y controles.

Al finalizar el curso, los participantes estarán preparados para evaluar la madurez de los Sistemas y procesos de IA, identificar riesgos emergentes, valorar la efectividad de los controles implementados y emitir recomendaciones que fortalezcan la confianza, seguridad y uso responsable de los sistemas de Inteligencia Artificial.

Objetivo

Desarrollar en los participantes las competencias necesarias para planificar, ejecutar y documentar auditorías de sistemas de Inteligencia Artificial (IA) con un enfoque basado en riesgos, utilizando la ISO/IEC 42001 como marco de referencia para evaluar el Sistema de Gestión de IA (AIMS) y el NIST AI Risk Management Framework (AI RMF) como metodología para identificar, analizar, evaluar y gestionar los riesgos asociados a los sistemas de IA, generando hallazgos y recomendaciones alineados con las mejores prácticas internacionales.

Objetivo específico

- Comprender los fundamentos de la Inteligencia Artificial y sus riesgos tecnológicos, éticos y regulatorios.
- Interpretar los requisitos de la ISO/IEC 42001 y su aplicación durante una auditoría.
- Aplicar el NIST AI RMF para identificar y evaluar riesgos de IA.
- Elaborar un programa y planificación de auditoría basado en riesgos para sistemas de IA.
- Evaluar controles de gobernanza, calidad de datos, modelos de IA y ciclo de vida del sistema.
- Identificar riesgos relacionados con sesgos, privacidad, seguridad, explicabilidad y uso responsable de la IA.
- Documentar evidencias, hallazgos y recomendaciones y elaborar informe conforme a las mejores prácticas de auditoría.

¿Porque Asistir?

- Aprenderá una metodología práctica para auditar sistemas de Inteligencia Artificial basada en riesgos.
- Conocerás la ISO/IEC 42001 y el NIST AI RMF y su aplicación.
- Desarrollará competencias para evaluar los principales riesgos de la IA.
- Fortalecerá su perfil profesional en una de las áreas con mayor crecimiento y demanda.
- Obtendrá herramientas y documentos listos para aplicar en su organización.
- Estará preparado para auditar el uso responsable y confiable de la Inteligencia Artificial.

Metodología

Este Curso de 8 horas se desarrollará en formato online en vivo, dividido en 4 sesiones de 2 horas cada una, permitiendo una interacción directa entre los participantes y el facilitador. La metodología combina la exposición conceptual con ejercicios prácticos, aplicando los lineamientos establecidos en la ISO 42001 y la NIST AI RMF.

Las principales características metodológicas incluyen:

- Clases en tiempo real mediante plataforma virtual, con espacios para consultas, análisis conjunto de textos y discusión de observaciones reales.
- Aplicación de ISO 42001 y la NIST AI RMF, enfocados a la Auditoría de IA.
- Talleres prácticos de Auditoría de IA aplicando MAPEO entre ISO 42001 y NIST AI RMF.
- Dinámicas de revisión cruzada entre participantes, fomentando el pensamiento crítico y el aprendizaje colaborativo entre profesionales de distintas industrias.
- Acceso a recursos complementarios digitales, como ISO 42001(resumen) y NIST AI RMF.

Dirigido a:

- Miembros de Comités (ej. de Riesgo y Cumplimiento, Auditoría, de Ciberseguridad y de TI)
- Tecnologías de la información
- Seguridad Cibernética y de la información
- Riesgo Operativo (Riesgo Tecnológico)
- Cumplimiento
- Auditores Internos y Auditores Externos

Contenido

Módulo 1

Fundamentos de la Inteligencia Artificial para Auditores

- **Evolución de la IA**
  - IA Tradicional
  - Machine Learning
  - Deep Learning
  - IA Generativa
  - Large Language Models (LLM)
- **Tipos de IA**
  - Supervisada
  - No Supervisada
  - Reforzamiento
  - IA Generativa
- **Componentes de un Sistema de IA**
  - Datos
  - Algoritmos
  - Modelos
  - Entrenamiento
  - Inferencia
  - Prompt Engineering
- **Riesgos asociados a la IA**
  - Riesgo operacional
  - Riesgo tecnológico
  - Riesgo reputacional
  - Riesgo legal
  - Riesgo ético
  - Riesgo de privacidad
  - Riesgo de ciberseguridad

Módulo 2

- **Introducción al Gobierno de IA**
  - Gobierno de IA
  - Roles y responsabilidades
  - Modelo de Tres Líneas
  - Comité de IA
  - Políticas de IA
- **Conociendo la ISO/IEC 42001:2023**
  - Contexto de la Organización
  - Liderazgo
  - Planificación
  - Soporte
  - Operación
  - Evaluación del desempeño
  - Mejora continua
  - Anexo A: objetivos de control
- **Conociendo la NIST Artificial Intelligence Risk Management Framework (AI RMF)**
  - Funciones
  - Govern
  - Map
  - Measure
  - Manage
- **Características de IA Confiable**
  - Validez
  - Seguridad
  - Resiliencia
  - Explicabilidad
  - Equidad
  - Privacidad
  - Transparencia
  - Rendición de cuentas
- **Integración o MAPEO de los dos marcos ISO 42001 NIST AI RMF**
  - Construcción de una matriz de correspondencias: qué subcategoría del RMF (Govern/Map/Measure/Manage) alimenta de evidencia a qué cláusula o control del Anexo A de ISO 42001.

Módulo 3

- **Cómo auditar evidencia de la ISO 42001 y NIST (Govern, Map, Measure y Manage)**
  - ¿Qué debería existir? (el requisito)
  - ¿Qué evidencia lo demuestra? (el artefacto)
  - ¿Qué le pregunto al auditado? (la entrevista)
  - ¿Qué señales de alerta indican que la evidencia es débil o simulada? (el red flag)
- **El Proceso y la documentación de la Auditoría de IA (Metodología práctica)**
  - Iniciando una Auditoría de IA
  - Fase de relevamiento de información
  - Fase de Planificación de la Auditoría de IA
    - Elaboración del Programa de Auditoría de IA
    - Elaboración de los Procedimientos de Auditoría, ChekList, Cuestionarios a utilizar en la Auditoría de IA
  - Fase de Ejecución de la Auditoría de IA (trabajo de campo)
    - Atributos de la evidencia de Auditoría de IA
    - Aspectos claves a considerar para obtener la evidencia
  - Fase de elaboración del Informe borrador de Auditoría de IA
  - Fase de Seguimiento de la Auditoría de IA (Auditoría posterior)

Módulo 4:

- **Aplicación práctica y cierre**
  - Caso integral de auditoría de IA
  - Trabajo en grupos.



Wilson Andia Cuiza

CISA, CRISC, CSX, CDPSE, ISO 27001 LA

Tiene en su "ADN" Tecnología y Auditoría, con más de 22 años de experiencia en Auditorías de TI, Seguridad, Riesgos y Control de TI, reconocido en diferentes Bancos como Auditor Externo y por sus conferencias internacionales, así como por las docencias en Certificaciones mundialmente reconocidas y Maestrías de alto impacto.

Wilson es Ingeniero de Sistemas con Postgrados en Seguridad y Auditoría de TI y Certificaciones Internacionales CISA, CRISC, CSX y CDPSE de ISACA e ISO 27001 y es Instructor acreditado CISA y CRISC por APMG. Inicialmente fue Analista Programador en diferentes Empresas. Posteriormente trabajó como Consultor Internacional en Auditoría de TI y Seguridad en países de Sud, Centro América y el Caribe en Bancos de prestigio y Empresas, así como Entidades Fiscalizadoras como Contralorías, Cámara de Cuentas y Tribunal de Cuentas, Proyectos Financiados por BID, Banco Mundial, PNUD y Unión Europea.

Actualmente es director de Auditorías y Consultorías de TI de una de las Firmas con mayor presencia en República Dominicana en el Sector Bancario, teniendo entre otros clientes a 10 Bancos de prestigio.

El Sr. Andia es experto en:

- Dirección de Auditorías de TI y de Ciberseguridad.
- Auditoría de TI y Seguridad en Bancos Múltiples y de Ahorro y Crédito.
- Auditoría y Seguridad de Core Bancarios: FISERV, FISA, BANCA 2000, SYSDE BANCA, ABANKS.
- Auditoria a Sistemas MONITOR PLUS, SENTINEL CUMPLIMIENTO/PREVENTION, ULTRAFISGON.
- Auditor de TI en Prevención del Lavado de Activos (PLA/FT).
- Auditoría de cumplimiento PCI-DSS.
- Seguridad, Riesgos y Auditoría de TI basado en metodologías y estándares ISO de TI COBIT, COSO, ISO 27001, 27002, 22301, 27031, 12207, 25000, 9126, 15504.
- Desarrollo e Implementación de Planes de Continuidad (BCP) y de Recuperación ante Desastres Informáticos (DRP).
- Desarrollo e Implementación de Políticas de Seguridad de TI.
- Detección de fraudes o delitos informáticos.
- Análisis Forense Informático usando Software (EnCase y Forensic ToolKit, Autopsy)
- Software de Auditoría (IDEA, ACL, TEAM MATE, MEYCOR COBIT, COBIT ADVISOR)
- Ley Sarbanes Oxley (SOX) relacionado con TI.
- Análisis, Programación e Implementación de Sistemas Informáticos.
- Administración de Bases de Datos ORACLE, SQL SERVER, SYSBASE, DB2.
- Lenguajes de programación ORACLE, .NET. C#, Java.
- Conferencias Internacionales de Seguridad, Auditoría y Riesgos de TI
- Docente de Certificaciones CISA y CRISC en capítulos de ISACA.
- Docente de Maestrías en Auditorías y Seguridad de TI.
- Expositor y capacitador en Auditoría, Riesgos y Seguridad de TI.

Inversión y formas de pago

Día: 17, 18, 19 y 20 de noviembre del 2026

Horario:

Zona Pacífico EEUU - **13:00**
Zona Montaña EEUU - **14:00**
Centroamérica, México y Zona Central EEUU - **15:00**
Perú, Panamá, Colombia, Ecuador y Zona Oriental EEUU - **16:00**
Rep. Dominicana, Bolivia y Venezuela - **17:00**
Brasil, Chile , Paraguay, Uruguay y Argentina - **18:00**
Guinea Ecuatorial - **22:00**

Costo:

Socios: USD 195,00 + IMP
No socios: USD 245,00 + IMP

Incluye:

- Asistencia al curso
- Material de apoyo
- Certificado de Participación
- Acceso al aula virtual

Pago del Curso:

Transferencias Bancarias
Banco intermediario Swift: CITIUS33. ABA: 021000089
Nombre: CITIBANK N.A.
Dirección: 111 Wall Street, New York, New York 10043
Transferir a Cuenta: 36026966. Swift: BSNJCRSJ.
Nombre: BAC San José (formerly Banco San José, S.A.)
Dirección: Calle 0 Avenidas 3 y 5, San José Costa Rica
Beneficiario Capacita Int S.A.
Cuenta Cliente: 10200009301147801
Cuenta IBAN: CR47010200009301147801
Cedula jurídica: 3-101-663566
IMPORTANTE: LA TRANSFERENCIA DEBE SER ENVIADA EN FORMATO MT103.
Favor remitir comprobante del deposito bancario escaneado al e-mail: info@capacita.co

Contáctenos

+506 4404 4859 / +506 6292 7902 / info@capacita.co / **www.capacita.co**

