AUDITORÍA PREVENTIVA CON INTELIGENCIA ARTIFICIAL

Contraloría del Estado

Juan Daniel Macías Sierra · 30 de octubre de 2026

Mentorías sobre buenas prácticas en la gestión pública municipal

Comité de Participación Social JALISCO

CCME Comisión de Contralores Municipios-Estado

Contraloría del Estado GOBIERNO DE JALISCO

JALISCO GOBIERNO DEL ESTADO

Orden del día | 60 minutos

01	Apertura y cultura de datos	00:00–04:00	4 min
02	¿Qué es la IA? Alcance y límites	04:00–10:00	6 min
03	Herramientas y técnicas de IA	10:00–15:00	5 min
04	Ciclo de auditoría y prevención	15:00–22:00	7 min
05	Auditoría continua y algoritmos	22:00–29:00	7 min
06	Experiencias internacionales	29:00–36:00	7 min
07	Ética, riesgos y datos	36:00–43:00	7 min
08	Gobernanza y controles auditables	43:00–48:00	5 min
09	Perfil del auditor del futuro	48:00–53:00	5 min
10	Demostración práctica	53:00–59:00	6 min
11	Conclusiones y cierre	59:00–60:00	1 min

FUENTE: Guion oral desarrollado y guía de estudio · versión 7 · 60 minutos

Objetivo de la sesión

¿Cómo puede la IA fortalecer una fiscalización más oportuna y preventiva?

Puede ordenar registros, detectar excepciones y priorizar revisiones para reconocer riesgos antes de que se agraven o repitan. Su utilidad exige datos confiables, comprobación documental, atribuciones claras y juicio humano.

FUENTES: Erasmus y Bozkuş Kahyaoğlu (2025)

¿Qué entendemos por inteligencia artificial?

DEFINICIÓN OPERATIVA DE LA OCDE

"Un sistema basado en máquinas que, para objetivos explícitos o implícitos, infiere a partir de los datos de entrada cómo producir resultados como predicciones, contenido, recomendaciones o decisiones que pueden influir en entornos físicos o virtuales. Los sistemas varían en sus niveles de autonomía y de adaptación después de ponerse en funcionamiento."

01 ENTRADAS

Datos e instrucciones

02 INFERENCIA

Procesamiento para generar salidas

03 RESULTADOS

Predicciones, contenidos o decisiones

FUENTE: OCDE (2023; memorando 2024)

Autonomía y adaptabilidad

AUTONOMÍA TÉCNICA

Un sistema puede ejecutar una tarea sin recibir instrucciones humanas a cada paso. La autonomía técnica varía según los permisos y límites definidos.

ADAPTABILIDAD

Algunos sistemas modifican su desempeño ante nuevos datos o condiciones de uso. Esa adaptación requiere seguimiento para identificar cambios y errores.

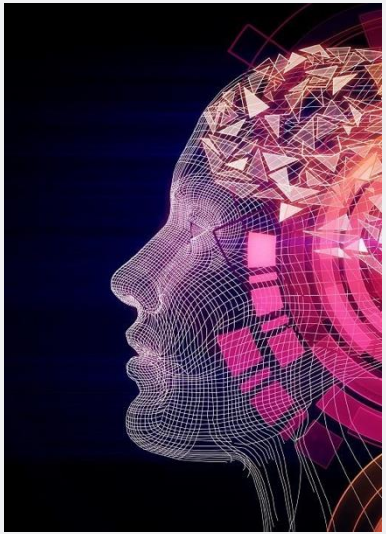
La decisión sobre qué delegar y quién responde por sus efectos corresponde a las personas y autoridades competentes.

FUENTES: OCDE (2024); Cortina (2019); Coeckelbergh (2020)

La IA produce respuestas pero la autoridad decide

Una explicación convincente no acredita sus premisas.

Un modelo puede redactar un texto que parece un dictamen. Corresponde a la autoridad verificar las premisas, aplicar el marco jurídico y asumir la decisión; la fluidez de la respuesta no demuestra su veracidad.



FUENTES: OCDE (2024); Cortina (2019)

Cuatro enfoques tecnológicos aplicables a la auditoría

Automatización

Aplica condiciones definidas por personas; por ejemplo, marcar dos pagos con el mismo folio, contrato e importe.

Analítica

Resume importes, variaciones y concentraciones para identificar operaciones que merecen una revisión.

Machine learning

Un modelo entrenado con registros puede agrupar operaciones o estimar riesgos; debe validarse.

IA generativa

Interpreta descripciones, sintetiza documentos y propone borradores que requieren cotejo.

Cada técnica requiere controles distintos. Una regla sencilla, bien documentada, puede ser más útil que un modelo complejo.

FUENTES: Erasmus y Bozkuş Kahyaoğlu (2025)

Aprendizaje automático e IA generativa

APRENDIZAJE AUTOMÁTICO

Un modelo aprende regularidades a partir de ejemplos o datos. Con ellas puede clasificar registros, estimar riesgos o identificar comportamientos atípicos.

EN AUDITORÍA: priorizar operaciones con patrones inusuales para revisión.

INTELIGENCIA ARTIFICIAL GENERATIVA

Genera contenido nuevo —texto, resúmenes, tablas o propuestas— a partir de instrucciones. Puede interpretar lenguaje y relacionar descripciones distintas.

EN AUDITORÍA: cotejar “luminarias LED” y “equipos de iluminación”.

Ambas pueden apoyar el análisis, pero sus salidas necesitan validación. Un parecido semántico no acredita entrega ni cumplimiento.

FUENTES: Erasmus y Bozkuş Kahyaoğlu (2025)

Técnicas y tecnologías para el análisis de información en auditoría

1	**Reglas**	Documentar la regla exacta, los campos utilizados, el umbral elegido y el archivo de origen. Así cualquier revisor puede repetir el resultado.
2	**Modelo predictivo**	Identificar el modelo y su versión, datos de entrenamiento y prueba, método de validación, precisión y posibles sesgos o cambios de desempeño.
3	**IA generativa**	Conservar el prompt, la versión del sistema, los extractos autorizados y la respuesta. Verificar cada hecho, cifra y referencia jurídica antes de usarla.
4	**OCR**	Verificar importes y folios contra el documento original: el OCR puede confundir caracteres.

FUENTES: OCDE (2026); Erasmus y Bozkuş Kahyaoğlu (2025)

04

La IA en el ciclo metodológico de la auditoría

La inteligencia artificial en las etapas del proceso de auditoría

01

Planeación

La autoridad define objeto, riesgos, universo y criterios.

02

Ejecución

Se ejecutan cruces y se corroboran las excepciones.

03

Informe

El informe distingue hallazgos de simples hipótesis.

04

Seguimiento

Se analizan descargos y se da seguimiento formal.

La IA puede ayudar a reconocer excepciones antes y durante la revisión; para que exista una orientación preventiva, alguien debe corroborarlas y activar medidas dentro de sus facultades. No reemplaza actos formales, evidencia ni supervisión.

FUENTES: Contraloría del Estado; Global Internal Audit Standards (IIA)

La Inteligencia Artificial en la etapa de planeación

Universo

Definir qué contratos, pagos o expedientes serán examinados, sus periodos, sistemas de origen y calidad de registros.

Riesgos

Explorar concentraciones, variaciones y operaciones inusuales para orientar preguntas y seleccionar muestras o pruebas.

Decisiones

El equipo auditor fija materialidad, objetivos, procedimientos, fundamento jurídico y recursos disponibles.

El modelo ayuda a explorar riesgos; las decisiones de programación institucional requieren competencia y justificación.

FUENTES: Erasmus y Bozkuş Kahyaoğlu (2025)

La Inteligencia Artificial en la etapa de ejecución

01

Cruces

Conciliar contratos y pagos mediante identificadores estables.

02

Alertas

Marcar facturas repetidas, diferencias y montos mayores.

03

Contraste

Verificar soportes, cancelaciones, firmas y documentos.

04

Prueba

Registrar origen, cálculo, comprobación y explicación.

Una excepción es el inicio de una prueba, no su resultado. La revisión puede exigir originales, expedientes, bitácoras de obra o verificaciones físicas, según el objeto y las facultades del órgano.

FUENTES: Global Internal Audit Standards (IIA)

La Inteligencia Artificial en el Informe

PUEDE ASISTIR

Un asistente puede organizar antecedentes, proponer un índice, resumir documentación autorizada y revisar la claridad de un borrador. Cada afirmación debe contrastarse con su soporte.

NO DEBE DETERMINAR SOLA

El sistema no puede determinar por sí mismo una falta, acreditar una irregularidad ni resolver sobre derechos. El auditor debe identificar el criterio legal y valorar la evidencia.

Un texto bien redactado carece de fuerza probatoria cuando sus premisas son incorrectas, insuficientes o no verificadas.

FUENTES: Global Internal Audit Standards (IIA)

La Inteligencia Artificial en el seguimiento de auditorías

Registrar

Registrar el archivo fuente, fecha, versión de la regla y datos que activaron la excepción.

Solicitar

Contrastar el señalamiento con documentación y aclaraciones que aporte el ente revisado.

Resolver

Dejar constancia de por qué una señal se confirma, se descarta o requiere nuevas pruebas.

El seguimiento debe reconocer aclaraciones suficientes y registrar falsos positivos, evitando convertir toda alerta en una observación.

FUENTES: Contraloría del Estado; Global Internal Audit Standards (IIA)

De la auditoría retrospectiva al enfoque preventivo

EXAMEN RETROSPECTIVO

Revisa operaciones y hechos ya realizados. Reconstruye qué ocurrió, aplica criterios y sustenta resultados mediante evidencia y procedimientos documentados.

ORIENTACIÓN PREVENTIVA

Identifica oportunamente riesgos y debilidades de control para orientar verificaciones y, cuando proceda, medidas que eviten daños, su agravamiento o repetición.

APORTE DE LA IA **Cruces frecuentes, clasificación documental y alertas. La persona auditora corrobora fuentes y actúa conforme a sus atribuciones.**

FUENTES: Morgan (2025), cap. 3; Naoufal (2025), cap. 9; IIA (2025)

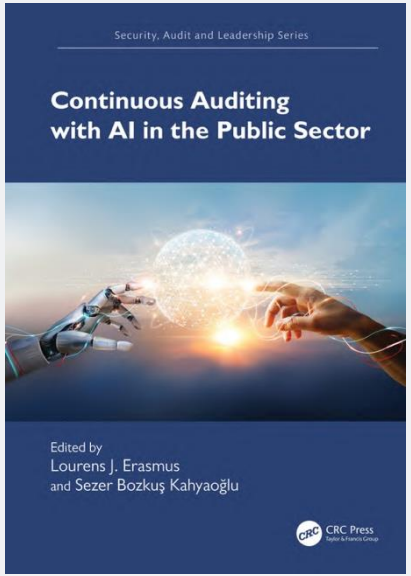
05

Auditoría continua, monitoreo y algoritmos

¿Qué es la auditoría continua?

Pruebas repetibles y frecuentes

La auditoría continua usa pruebas automatizadas y repetibles sobre fuentes estables, con mayor frecuencia que una revisión tradicional. Requiere supervisión, control de datos, responsables y seguimiento de excepciones.



FUENTES: Naoufal (2025), cap. 9, CRC Press

Monitoreo continuo: control de la gestión

MONITOREO CONTINUO

La propia administración examina sus operaciones y controles de forma periódica para detectar fallas, corregir procesos y gestionar riesgos mientras ocurren.

AUDITORÍA CONTINUA

La función de auditoría diseña pruebas independientes, valida alertas y documenta conclusiones conforme a su mandato y metodología.

Un tablero automático necesita responsables, criterios de escalamiento y seguimiento; la frecuencia de análisis no garantiza por sí sola la calidad.

FUENTES: Naoufal (2025), cap. 9, CRC Press

Auditar la inteligencia artificial del gobierno

1	**Datos**	Examinar procedencia, integridad, actualización y si los datos representan correctamente a las personas o procesos afectados.
2	**Criterios**	Identificar variables, supuestos, finalidad autorizada, umbrales y criterios de selección o clasificación.
3	**Resultados**	Evaluar tasas de error, disparidades, consecuencias administrativas y posibles impactos en derechos.
4	**Control**	Verificar registros de decisiones, posibilidad de impugnación, revisión humana, responsables y controles de cambio.

FUENTES: Morgan (2025), cap. 5, CRC Press

Auditar CON IA y auditar LA IA

AUDITAR CON IA

La institución utiliza modelos como apoyo para examinar contratos, pagos o expedientes. Debe validar la técnica y corroborar las señales con evidencia.

AUDITAR LA IA

El órgano de control revisa un sistema utilizado por la administración: sus datos, criterios, resultados, seguridad, supervisión y posibilidad de revisión.

En ambos casos persisten las competencias, el deber de motivar y la independencia profesional.

FUENTES: Morgan (2025); Naoufal (2025)

06

Experiencias internacionales

Brasil | ALICE y el análisis de contrataciones



El Tribunal de Contas da União (Brasilia, BR) aplica ALICE al análisis de procedimientos de contratación para identificar señales tempranas de inconsistencias y priorizar su revisión.

La misma compra puede registrarse con nombres diferentes. La integración y estandarización de datos son parte esencial del sistema.

FUENTES: Tribunal de Contas da União (2024, 2025)

Estados Unidos | GAO 2021

Gobernanza

Identificar liderazgo, funciones asignadas y políticas para desarrollar, adquirir y utilizar IA.

Datos

Comprobar procedencia, calidad y posibles sesgos en los conjuntos de datos.

Desempeño

Evaluar resultados frente al propósito, pruebas de fiabilidad y errores.

Monitoreo

Vigilar cambios, incidentes y desempeño después de poner el sistema en uso.

El marco de GAO (2021) organiza la fiscalización de sistemas de IA en gobernanza, datos, desempeño y monitoreo.

FUENTES: GAO-21-519SP (2021)

China | modelos de lenguaje en auditoría

National Audit Office of the People's Republic of China

ESCENARIOS ESTUDIADOS

El estudio de noviembre de 2025 explora el apoyo de modelos de lenguaje para planear revisiones, analizar expedientes, elaborar informes y dar seguimiento.

RIESGOS IDENTIFICADOS

Se advierten filtraciones, datos deficientes, alucinaciones y dificultades para verificar resultados de modelos poco transparentes.

El interés para una Contraloría está en examinar tanto las oportunidades técnicas como los controles necesarios.

FUENTES: National Audit Office of China, Audit Research Institute (2025), https://www.audit.gov.cn/n6/n39/c10747675/content.html

OCDE 2026 | Estado de la IA en la auditoría pública



Publicación del 7 de mayo de 2026. El estudio examina el uso de IA en auditoría pública, incluyendo detección de anomalías, análisis de documentos y modelos de riesgo; distingue entre experimentación y despliegue operativo.

FUENTES: Heyaca y Pallotta (2026), OECD AI Papers núm. 58

OCDE | La adopción de IA requiere lineamientos, capacitación y madurez institucional

80 %

De las instituciones consultadas, cuatro de cada cinco reportaron lineamientos para el uso de IA.

87 %

La capacitación aparece como condición para evaluar, validar y utilizar herramientas adecuadamente.

87 %

Aunque existen sistemas en operación, persisten diferencias importantes en cobertura y madurez.

FUENTES: OCDE (2026), pp. 8–9; 15 instituciones consultadas

OCDE 2026 | lecciones para las Contralorías Municipales

1	**Datos**	Establecer controles sobre fuentes, formatos y consistencia antes de desarrollar modelos o alertas.
2	**Capacidades**	Fortalecer capacidades institucionales para formular preguntas, evaluar resultados y comprender límites.
3	**Gobernanza**	Aprobar políticas de uso, privacidad, trazabilidad, validación, supervisión y responsabilidades.
4	**Escala**	Probar con problemas acotados, evaluar falsos positivos y resultados, y sólo después decidir si conviene ampliar el uso.

FUENTES: Heyaca, M. E. y Pallotta, A. (2026). DOI: 10.1787/f4a6c658-en

07

Ética y riesgos de la IA

Cinco riesgos para la auditoría pública

Calidad

Un modelo no corrige por sí mismo una fuente incompleta o duplicada.

Sesgo

Datos y criterios pueden producir impactos desiguales entre personas.

Opacidad

No siempre es claro cómo se obtuvo una respuesta o clasificación.

Seguridad

Cargar expedientes puede vulnerar deberes de confidencialidad.

Automatización

La fluidez de la IA facilita confiar demasiado en errores.

La automatización puede amplificar errores cuando faltan controles humanos y documentales.

FUENTES: UNESCO (2021); NIST (2023)

Antes de subir un información y datos a un asistente de IA

1	**Identificar**	Identificar la clasificación de los datos: públicos, personales, reservados o confidenciales. Separar campos que no deben compartirse.
2	**Autorizar**	Comprobar fundamento, autorización, necesidad y finalidad antes de tratar información institucional.
3	**Controlar**	Revisar controles de acceso, retención, transmisión, seguridad y condiciones del servicio.
4	**Preferir**	En ejercicios iniciales utilizar datos sintéticos o información que esté expresamente habilitada para ese uso.

FUENTES: UNESCO (2021); normativa de datos aplicable

UNESCO | Recomendación sobre la Ética de la IA

Proporcionalidad

Utilizar sistemas sólo cuando exista una finalidad legítima y adecuada.

Privacidad

Aplicar privacidad, seguridad y límites al tratamiento de datos.

Equidad

Identificar efectos discriminatorios, errores y consecuencias desiguales.

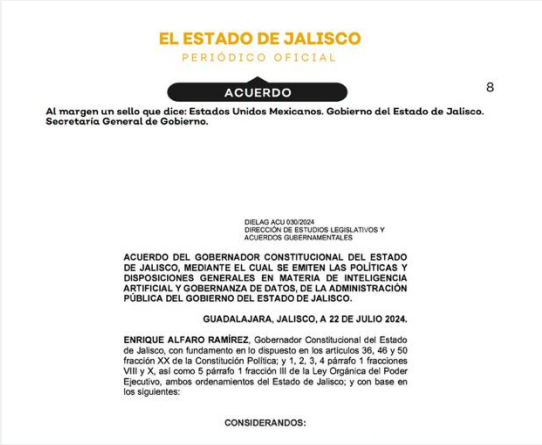
Supervisión humana

Asegurar revisión humana significativa y vías de corrección.

La recomendación UNESCO de 2021 orienta políticas y controles institucionales.

FUENTES: UNESCO (2021). Recomendación sobre la Ética de la IA

Jalisco: política estatal de IA y gobernanza de datos



EL ESTADO DE JALISCO
PERIÓDICO OFICIAL

ACUERDO

8

Al margen un sello que dice: Estados Unidos Mexicanos. Gobierno del Estado de Jalisco. Secretaría General de Gobierno.

DIELAG ACU 030/2024
DIRECCIÓN DE ESTUDIOS LEGISLATIVOS Y ACUERDOS GUBERNAMENTALES

ACUERDO DEL GOBERNADOR CONSTITUCIONAL DEL ESTADO DE JALISCO, MEDIANTE EL CUAL SE EMITEN LAS POLÍTICAS Y DISPOSICIONES GENERALES EN MATERIA DE INTELIGENCIA ARTIFICIAL Y GOBERNANZA DE DATOS, DE LA ADMINISTRACIÓN PÚBLICA DEL GOBIERNO DEL ESTADO DE JALISCO.

GUADALAJARA, JALISCO, A 22 DE JULIO 2024.

ENRIQUE ALFARO RAMÍREZ, Gobernador Constitucional del Estado de Jalisco, con fundamento en lo dispuesto en los artículos 36, 46 y 50 fracción XX de la Constitución Política; y 1, 2, 3, 4 párrafo 1 fracciones VIII y X, así como 5 párrafo 1 fracción III de la Ley Orgánica del Poder Ejecutivo, ambos ordenamientos del Estado de Jalisco; y con base en los siguientes:

CONSIDERANDOS:

Transparencia y explicabilidad

Explicar las capacidades y limitaciones de los sistemas.

Protección de la información

Considerar privacidad, seguridad y uso responsable de datos.

Políticas y Disposiciones Generales en materia de Inteligencia Artificial y Gobernanza de Datos de la Administración Pública del Gobierno del Estado de Jalisco.

Alcance: instrumento expedido para la Administración Pública estatal.

FUENTE: Periódico Oficial de Jalisco · Acuerdo DIELAG ACU 030/2024 (25 julio 2024)

En una Contraloría Municipal, la referencia estatal sirve para plantear preguntas de control antes de adoptar una herramienta:

01	**Finalidad y competencia**	¿Qué tarea realiza, con qué objetivo y quién autoriza su uso?
02	**Datos y privacidad**	¿Qué información se carga, dónde se procesa y quién tiene acceso?
03	**Explicabilidad**	¿Podemos describir sus límites y reconstruir sus resultados?
04	**Supervisión y evidencia**	¿Quién valida las respuestas y conserva la trazabilidad?

Criterios de referencia, sujetos a revisión jurídica e institucional de cada caso.

FUENTES: DIELAG ACU 030/2024 · propuesta didáctica de controles para contralorías

La dimensión ética de la auditoría digital

PRUDENCIA EPISTÉMICA

El auditor debe someter la información a examen crítico: pedir fuentes, buscar explicaciones alternativas y reconocer que un resultado automático puede equivocarse.

DILIGENCIA INSTITUCIONAL

La responsabilidad ética incluye proteger información, evitar imputaciones apresuradas, corregir errores y documentar por qué se acepta o descarta una señal.

La confianza institucional requiere precisión, imparcialidad y posibilidad de revisión.

FUENTES: Steenkamp y Smidt (2025), cap. 10

08

Gobernanza de la IA

NIST | Gestión de Riesgos de IA

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

01

GOVERN

Establecer políticas, roles, supervisión y responsabilidad.

02

MAP

Definir contexto, finalidad, actores y riesgos del uso.

03

MEASURE

Evaluar desempeño, error, sesgos y seguridad del sistema.

04

MANAGE

Mitigar riesgos, responder a incidentes y mejorar controles.

El marco NIST AI RMF 1.0 ofrece una estructura voluntaria y práctica para convertir riesgos de IA en responsabilidades y controles verificables.

FUENTES: NIST AI RMF 1.0 (2023)

Deliberación multidisciplinaria

Auditoría

Define alcance, pruebas y criterios de revisión.

Jurídico

Evalúa facultades, protección de derechos y contratos.

Informática

Valora acceso, infraestructura y controles técnicos.

Datos

Verifica procedencia, completitud y consistencia.

Transparencia

Revisa datos personales, acceso y transparencia.

Un proyecto de mayor impacto necesita contraste jurídico, técnico y profesional antes de aprobarse.

FUENTES: NIST (2023); UNESCO (2021)

Elegir correctamente los casos de uso

1	**Bajo riesgo**	Un piloto para ordenar y resumir documentos públicos presenta riesgos acotados y resultados sencillos de verificar.
2	**Riesgo medio**	Puede requerir autorización, control de acceso, pruebas de exactitud y revisión del tratamiento de información.
3	**Mayor impacto**	Si una clasificación influye en beneficios, sanciones o derechos, las pruebas y garantías humanas deben ser más exigentes.

FUENTES: NIST (2023); GAO (2021)

Cómo comenzar desde una Contraloría Municipal

01

1 · Elegir

Elegir una tarea concreta y evaluable.

02

2 · Preparar

Usar registros autorizados y depurados.

03

3 · Probar

Comparar alertas con casos conocidos.

04

4 · Validar

Revisar privacidad, permisos y controles.

05

5 · Evaluar

Medir fallos y decidir mejoras.

Una Contraloría puede empezar con cruces reproducibles en Excel o Python, usando información autorizada, antes de considerar modelos complejos.

FUENTES: Propuesta prudencial de implementación, guion oral v6

09

Perfil del auditor del futuro

Descripción del perfil del auditor

Pensamiento crítico

Distingue correlación de causalidad, datos de evidencia y una sugerencia de un hecho acreditado.

Alfabetización de datos

Identifica campos, sesgos de captura, faltantes y limitaciones de un conjunto de datos.

Diseño de pruebas

Convierte riesgos del proceso en reglas verificables y conoce cuándo una prueba no basta.

Riesgos digitales

Comprende riesgos de privacidad, acceso, trazabilidad y dependencia tecnológica.

El auditor conserva el conocimiento del proceso y coopera con especialistas para ampliar su capacidad técnica.

FUENTES: Modisane (2025); IIA Competency Framework (2025)

¿Debo aprender a programar en Python?

Puede ser una ventaja; no es una condición universal.

Es útil comprender bases de datos, hojas de cálculo, reglas y lectura de resultados. Python permite automatizar cruces y análisis; el auditor necesita, ante todo, formular buenas preguntas y validar los procedimientos con apoyo técnico cuando corresponda.

FUENTES: Modisane (2025); IIA (2025)

Aprendizaje continuo y colaboración

CONOCIMIENTO DE AUDITORÍA

La experiencia en contratación, obra pública, control interno, competencia y soporte documental sigue siendo esencial para decidir qué revisar y cómo valorar pruebas.

CAPACIDAD DE DATOS

La alfabetización de datos permite identificar errores, interpretar resultados, reconocer incertidumbre y dialogar con especialistas sin delegar ciegamente.

Formación continua, trabajo en equipo y revisión crítica deben acompañar toda adopción de IA.

FUENTES: Modisane (2025); OCDE (2026)

Dimensión ética del perfil profesional

Entender lo suficiente para cuestionar al sistema y a sus proveedores.

La ética profesional exige explicar el uso del sistema, reconocer sus limitaciones y exigir información suficiente para supervisarlo. Si el proveedor no puede justificar resultados ni controles, aumenta el riesgo institucional.

FUENTES: Steenkamp y Smidt (2025)

Cómo evaluar críticamente los resultados de la inteligencia artificial en auditoría

1 **¿De dónde?**

Determinar de qué sistemas provienen los datos, qué periodo abarcan y qué registros faltan.

2 **¿Por qué?**

Explicar las reglas o variables que activaron la señal y revisar su pertinencia.

3 **¿Cómo fallaría?**

Buscar falsos positivos, analizar aclaraciones y reconocer cuándo una prueba no sustenta conclusiones.



FUENTES: IIA Global Internal Audit Standards (2024/2025)

10

Demostración corta

Ejercicio práctico | Auditoría de cumplimiento en adquisiciones públicas

Objetivo
Demostrar cómo las herramientas de programación y la inteligencia artificial pueden apoyar la revisión de contrataciones y pagos gubernamentales, y distinguir las tareas automatizables de aquellas que requieren valoración profesional.

Desarrollo
Automatización con Python. Analizaremos archivos CSV para identificar referencias de pago duplicadas y diferencias entre los importes contratados y registrados.
Análisis con inteligencia artificial. Utilizaremos un asistente de IA para interpretar las alertas, identificar posibles explicaciones y proponer procedimientos de revisión.
Verificación del auditor. Determinaremos qué evidencia documental debe obtenerse para confirmar o descartar las inconsistencias detectadas.

Aprendizaje central
La programación automatiza pruebas; la IA amplía las posibilidades de análisis; el auditor verifica los resultados y sustenta sus conclusiones.

Balance crítico: posibilidades y límites

La pregunta es qué puede hacer la IA hoy, con qué riesgos y bajo qué condiciones.

POSIBILIDADES REALES

- Acelera búsquedas, clasificación de documentos y cruces entre bases.
- Ayuda a detectar patrones y riesgos con mayor oportunidad para priorizar verificaciones.
- Apoya borradores y análisis preliminares que el equipo verifica.

LIMITACIONES ACTUALES

- Depende de datos completos, confiables y correctamente interpretados.
- Puede producir sesgos, falsos positivos y respuestas inventadas.
- No acredita hechos ni determina responsabilidades por sí sola.

Una posibilidad preventiva comprobable requiere alertas útiles, responsables definidos y seguimiento documentado.

FUENTES: Naoufal (2025); IIA (2025); OCDE (2026)

Conclusiones

01

Valor acreditable

Una alerta oportuna puede orientar acciones preventivas, pero sólo el examen de fuentes y evidencia permite sustentar conclusiones o recomendaciones.

02

Responsabilidad ética

El uso de IA debe respetar derechos, confidencialidad, legalidad, proporcionalidad, imparcialidad y rendición de cuentas.

03

Juicio independiente

El auditor interpreta, contrasta y responde. La IA ayuda a acelerar tareas y descubrir señales; no reemplaza el criterio ni las atribuciones humanas.

FUENTES: Erasmus et al. (2025); IIA (2025); OCDE (2026); UNESCO (2021)

Bibliografía y fuentes primarias (I)

[B1] Erasmus, L. J. y Bozkuş Kahyaoğlu, S. (eds.). (2025). Continuous Auditing with AI in the Public Sector. CRC Press, cap. 1, pp. 1–12. https://doi.org/10.1201/9781003382706

[B5] Morgan, I. (2025). The emergence of algorithmic auditing in the public sector. En Erasmus y Bozkuş Kahyaoğlu (eds.), cap. 5, pp. 62–79. https://doi.org/10.1201/9781003382706-5

[B8] Modisane, C. (2025). Digital skills of public sector auditors. En Erasmus y Bozkuş Kahyaoğlu (eds.), cap. 8, pp. 115–142. https://doi.org/10.1201/9781003382706-8

[B9] Naoufal, G. (2025). Continuous auditing/continuous monitoring. En Erasmus y Bozkuş Kahyaoğlu (eds.), cap. 9, pp. 143–162. https://doi.org/10.1201/9781003382706-9

[B10] Steenkamp, L. y Smidt, L. A. (2025). The ethical perspective of digital auditing in public sector. En Erasmus y Bozkuş Kahyaoğlu (eds.), cap. 10, pp. 163–184. https://doi.org/10.1201/9781003382706-10

Bibliografía y fuentes primarias (II)

[OCDEdef] OCDE. (2024). Explanatory memorandum on the updated OECD definition of an AI system. https://oecd.ai/en/ai-publications/explanatory-memorandum-on-the-updated-oecd-definition-of-an-ai-system

[OCDE26] Heyaca, M. E. y Pallotta, A. (2026, 7 mayo). The state of artificial intelligence in public audit: Evidence from selected countries and the European Union. OECD Artificial Intelligence Papers, núm. 58. https://doi.org/10.1787/f4a6c658-en

[TCU] Tribunal de Contas da União, Brasil. (2025, 25 septiembre). Tribunal apresenta inovações tecnológicas para delegação da África do Sul [presentación de ALICE]. https://portal.tcu.gov.br/imprensa/noticias/tribunal-apresenta-inovacoes-tecnologicas-para-delegacao-da-africa-do-sul

[TCU24] Tribunal de Contas da União, Brasil. (2024). Uso de inteligência artificial aprimora processos internos no Tribunal de Contas da União. https://portal.tcu.gov.br/imprensa/noticias/uso-de-inteligencia-artificial-aprimora-processos-internos-no-tribunal-de-contas-da-uniao

[GAO] U.S. Government Accountability Office. (2021). Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities (GAO-21-519SP). https://www.gao.gov/products/gao-21-519sp

[CHINA] National Audit Office of China, Audit Research Institute. (2025, 7 noviembre). 生成式大语言模型在审计中的应用：场景、风险及对策 [Aplicaciones de modelos de lenguaje en auditoría: escenarios, riesgos y respuestas].

Bibliografía y fuentes primarias (III)

[ANAO] Australian National Audit Office. (2025). Governance of Artificial Intelligence at the Australian Taxation Office. https://www.anao.gov.au/work/performance-audit/australian-taxation-offices-adoption-of-artificial-intelligence

[IIA] Institute of Internal Auditors. (2025, 10 julio). Global Practice Guide: Internal Auditing Competency Framework. https://www.theiia.org/en/content/guidance/global/competency-framework

[IIAS] Institute of Internal Auditors. (2024; vigencia desde 9 enero 2025). Global Internal Audit Standards. https://www.theiia.org/en/content/standards/complete-global-internal-audit-standards/

[UNESCO] UNESCO. (2021). Recomendación sobre la Ética de la Inteligencia Artificial. https://www.unesco.org/ethics-ai/en/recommendation

[NIST] National Institute of Standards and Technology. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). https://www.nist.gov/itl/ai-risk-management-framework

Bibliografía y fuentes primarias (IV)

[CORTINA] Cortina Orts, A. (2019). Ética de la inteligencia artificial. Anales de la Real Academia de Ciencias Morales y Políticas, pp. 379–394. https://www.boe.es/biblioteca_juridica/anuarios_derecho/articulo.php?id=ANU-M-2019-10037900394

[COECK] Coeckelbergh, M. (2020). AI Ethics. MIT Press. https://mitpress.mit.edu/9780262538190/ai-ethics/

[FLORIDI] Floridi, L. y Sanders, J. W. (2004). On the morality of artificial agents. Minds and Machines, 14, 349–379. https://doi.org/10.1023/B:MIND.0000035461.63578.9d

[RUSSELL] Russell, S. y Norvig, P. (2021). Artificial Intelligence: A Modern Approach (4.ª ed., edición global). Pearson. Referencia bibliográfica de consulta conceptual

[CEJ] Contraloría del Estado de Jalisco. Plataforma de seguimiento de auditorías, consulta institucional. https://contranet.jalisco.gob.mx/auditorias/principal/auditorias

JALISCO · ACUERDO

Gobierno de Jalisco (2024). Acuerdo DIELAG ACU 030/2024, Políticas y Disposiciones Generales en materia de Inteligencia Artificial y Gobernanza de Datos. Periódico Oficial, 25 de julio de 2024, tomo CDXI, núm. 7, sección VI, p. 8 y ss.

https://periodicooficial.jalisco.gob.mx/seccion/periodico/22418

Fuentes del enfoque preventivo

[B3] Morgan, I. (2025). New auditing perspectives for a blockchain-based accounting system in the public sector. En Erasmus y Bozkuş Kahyaoğlu (eds.), Continuous Auditing with AI in the Public Sector, cap. 3, pp. 30–46. CRC Press. DOI: 10.1201/9781003382706.

[B9] Naoufal, G. (2025). Continuous auditing/continuous monitoring. En Erasmus y Bozkuş Kahyaoğlu (eds.), Continuous Auditing with AI in the Public Sector, cap. 9, pp. 143–162. CRC Press. DOI: 10.1201/9781003382706.

[IIACA25] The Institute of Internal Auditors. (2025, 25 de septiembre). Continuous Auditing and Monitoring, 3rd Edition. Global Technology Audit Guide (GTAG). https://www.theiia.org/en/content/guidance/recommended/supplemental/gtags/continuous-auditing-and-monitoring

[OCDE26] Heyaca, M. E., y Pallotta, A. (2026). The state of artificial intelligence in public audit: Evidence from selected countries and the European Union. OECD Artificial Intelligence Papers, núm. 58. https://doi.org/10.1787/f4a6c658-en

Muchas gracias

Juan Daniel Macías Sierra

Auditoría preventiva con inteligencia artificial · 30 de octubre de 2026