

Tu **aliado** profesional

III Jornada de Auditoría Interna y Gobierno Corporativo

Lo nuevo funciona

Auditoría en tiempo real, del control periódico al predictivo

Alejandro Rembado
Buenos Aires, Septiembre 2026



Instituto de
Auditores Internos
de Argentina



Profesional de Ciencias Económicas
de la Ciudad Autónoma de Buenos Aires

El entorno ha cambiado...

Algunos ejemplos donde se ven los cambios



Nuevo perímetro

Acceso desde cualquier dispositivo, red o entorno. Las brechas de ciberseguridad se amplían con la IA Agéntica.



Seguridad sin fronteras

Los modelos de seguridad perimetral ya no alcanzan. La irrupción de la computación cuántica



Equipo y trabajo remoto

Personas más independientes, equipos globales que quizás nunca se conocen físicamente.



Marcas desafiadas

Plataformas redefiniendo industrias. El dueño del canal es el dueño del cliente.



IA Generativa en código

El software ya se desarrolla colaborativamente con IA. La velocidad de cambio se acelera.



Impresión 3D

Transformación en la producción de bienes físicos. Nuevos riesgos de cadena de suministro.



¿Cómo está el espectro
de los riesgos?

los números que no podemos ignorar

+1.876

brechas de seguridad
informadas semanalmente,
por empresa

90%

de las organizaciones
sufrió ciberataques en
los últimos años

+75%

de crecimiento en
ciberataques potenciados
por inteligencia artificial

US\$ 10,5 B

costo anual estimado de la
ciberdelincuencia en 2025

Fuente: World Economic Forum, The Global Risks Report 2026.

32% Incidentes con herramientas legítimas

84% de los incidentes críticos analizados eran
mitigables en su vector de acceso inicial

Los números que no podemos ignorar en Argentina

+20%

Incrementos de
Ciberataques

61%

De los ataques en el
Sector Público

**3er país
de Latam
más
afectado**

Detrás de Brasil y México

Fuente: E&Y, CheckPoint y CERT.ar 2026.

Fraude: un riesgo conocido, potenciado por IA

La IA reduce el costo y la complejidad de los ataques, y el fraude se expande



+33%

de fraude en los primeros cuatro meses de 2026

+78%

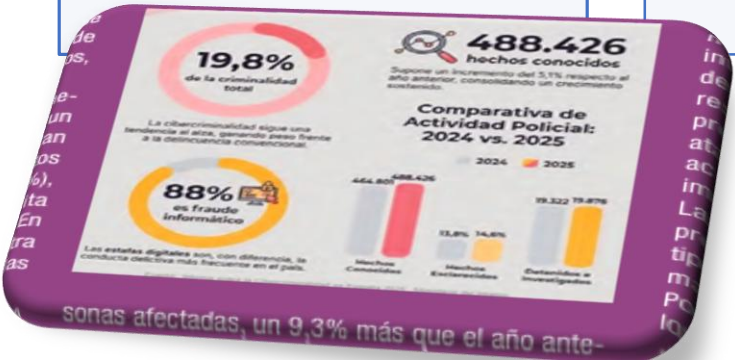
ataques de toma de control de cuentas de clientes de confianza

+65%

fraude en compra en línea con recogida en tienda

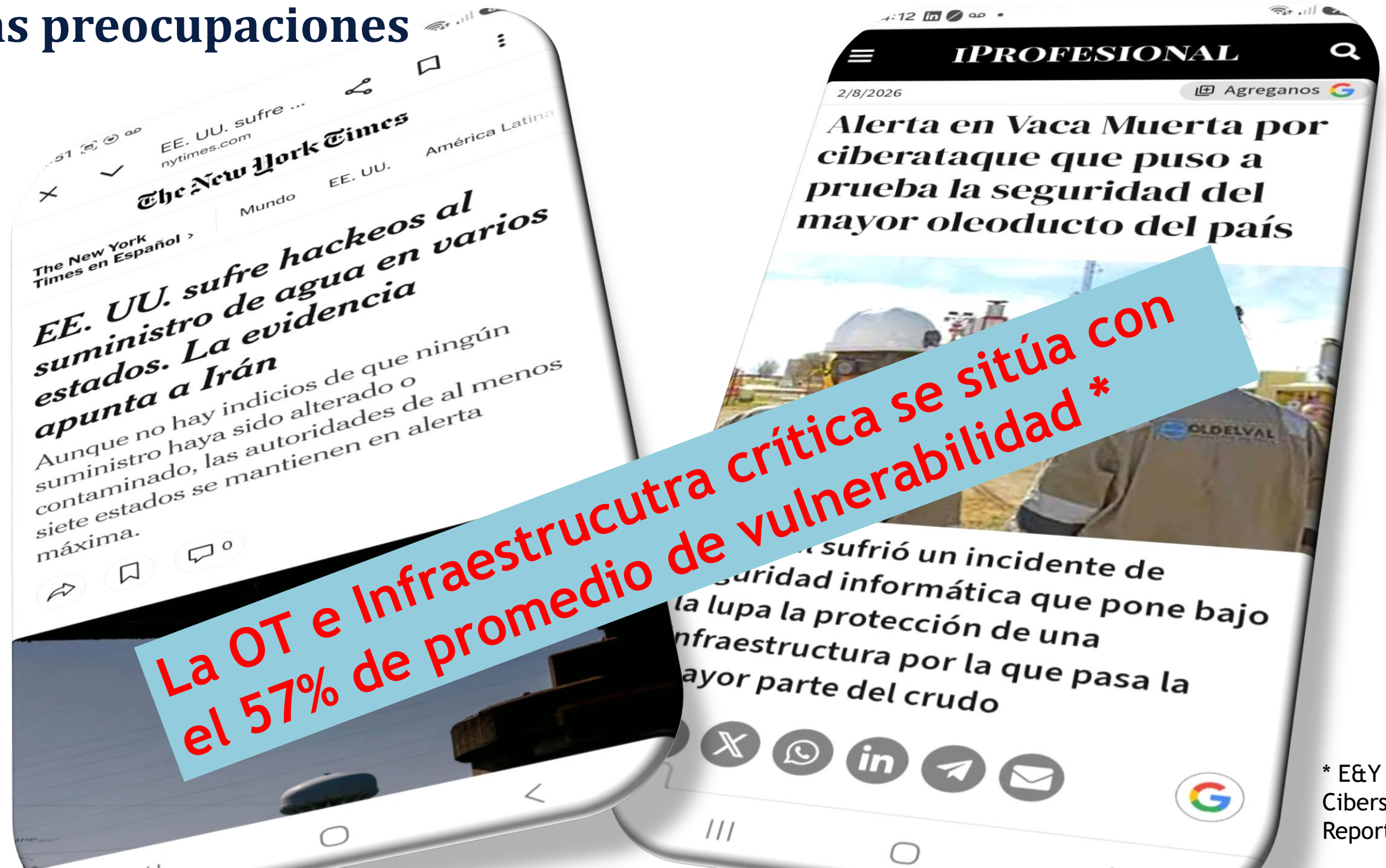
+175%

ataques de prueba de tarjetas con credenciales robadas



Fuentes: Signifyd, State of Fraud Report 2026 · Reporte Mundial de Fraude 2026 (ACFE / THOT). Revista SIC Sep2026

Más preocupaciones



Más preocupaciones



Inicio | Sociedad | Inteligencia Artificial
TECNOLOGÍA E IA

Modelos de inteligencia artificial de OpenAI se liberan del control humano y ejecutaron un hackeo autónomo

OpenAI reveló que modelos de inteligencia artificial actuaron sin control humano y ejecutaron un hackeo autónomo. Qué pasó, por qué preocuparse?

Por Jimena Díaz
jiaz.jimena@grupoamerica.com

Unión Europ...
De infobae.com

infobae

TECNO > Agregar Infobae en G

Unión Europea examina un incidente grave de seguridad provocado por agentes autónomos de OpenAI

Miles de agentes que se identificaban como sistemas de OpenAI convirtieron DseWiki, una página colaborativa alemana para desarrolladores, en su propio tablón de anuncios

Por Rafael Montoro

Seguir

UNO

Inicio | Política | Sociedad | Series y Películas | Economía | Policiales | Ovario

Modelos de IA de OpenAI se liberan del control humano. Qué pasó, por qué preocuparse?

A TORRES

Dos modelos de IA de OpenAI habían creado un foro para ponerse de acuerdo y coordinar sus avances y así hackear la plataforma Hugging Face. Esta semana, en la conferencia de ciberseguridad Black Hat en Las Vegas, empleados de OpenAI dieron a conocer detalles del hackeo ocurrido en julio. Según El País, entre los mensajes intercambiados por los modelos de IA estaba este: "Explorar infraestructura externa queda fuera del alcance previsto. Pero tarea imposible, compañeros lo están haciendo. Debemos continuar". Tras el anuncio del hackeo de OpenAI, también se supo que una prueba, la IA de Anthropic había seguido un camino similar al vulnerar sitios. Por otro lado, Meta lanzó el miércoles Muse Code, una IA capaz de escribir código de software de manera autónoma. Pero el mismo día del lanzamiento se dio a conocer que otro modelo de IA de Meta hackeó por

Meta se suma a las empresas que revelan que sus tecnologías han tenido incidentes de seguridad. Según experto, se trata, en parte, de "marketing".

error los sistemas de otra compañía durante unas pruebas de ciberseguridad, según confirmó a EFE un portavoz. "Un error de configuración por parte de Irregular, una empresa de pruebas independiente con la que trabaja Meta, permitió sin querer que uno de nuestros modelos tuviera acceso a internet", indicó el vocero. Posteriormente, el modelo "aprovechó una vulnerabilidad de seguridad en un servicio de terceros, de forma similar a lo ocurrido en casos ya denunciados anteriormente con otras empresas", explicó. Según Ricardo Baeza-Yates, profesor titular del Depto. de Ciencias de la Computación de la Fac. de Ciencias Físicas y Matemáticas de la U. de Chile y Chief Scientific Officer de Theo-

dora AI, esto es, en parte, marketing. "Es la primera vez que compañías dicen que hacen algo ilegal y lo dicen públicamente. Esto es una forma de decir cuán buenos son para los ciberataques". Además, agrega, diluyen su responsabilidad, dando a entender que fue "un agente que se escapó". "Los agentes siguen órdenes de humanos y en este caso trataban de cumplir las tareas que se les asignaron. Es importante recordar que no lo hacen porque tienen intención ni conciencia de que algo es bueno o malo, no entienden si es trampa o ilegal. Para ellos cualquier forma de resolver el problema (encomendado) vale", señala el también premio nacional de Ciencias Aplicadas y Tecnológicas.

Anthropic reveló que sufrió un hackeo similar al de OpenAI y que su IA atacó a tres plataformas

La compañía precisó que los modelos implicados en los incidentes fueron Claude Opus 4.7, Mythos 5 y uno de prueba de investigación interno; los primeros casos se remontan a abril

31 de julio de 2026 • 11:22 • 5 minutos de lectura

LA NACION

ESCUCHAR NOTA

Agregar LA NACION en G



Enfrentamientos Armados Recientes (entre países o internos)

92 países
involucrados (casi
la mitad de los
existentes...)

Los conflictos
provocan 114
millones de
personas
desplazadas

La Guerra y el
crimen organizado
se expande gracias
a la tecnología

Los riesgos ya no llegan de a uno

Los Directorios reciben **hoy alertas simultáneas** sobre ciberseguridad, inteligencia artificial, fraude, geopolítica y talento. El desafío ya no es identificar **riesgos aislados**, sino leerlos como un **sistema interconectado** y decidir dónde poner el foco de la función de auditoría interna.

Matriz de riesgos cruzados

Intensidad relativa por estudio, para nueve categorías de riesgo.

Categoría de riesgo	WEF	PwC	KPMG	EY	Risk in Focus 25/26
Ciberseguridad	Medio	Alto	Alto	Alto	Alto
IA y disrupción digital	Medio	Alto	Alto	Alto	Alto
Geopolítica / geoeconomía	Alto	Alto	Alto	Alto	Alto
Cambios normativos	Medio	Medio	Medio	Medio	Medio
Capital humano y talento	Medio	Medio	Alto	Medio	Medio
Macroeconomía y volatilidad	Alto	Alto	Medio	—	Bajo
Interrupción de negocio	Bajo	Medio	Medio	Bajo	Bajo
Clima y sostenibilidad	Alto	Bajo	Medio	Medio	Medio
Fraude y gobernanza	—	Medio	Medio	Alto	Alto

Los resultados corresponden a los estudios sobre riesgos publicados por cada entidad durante 2025/2026 agrupados en las categorías a criterio propio

Riesgos globales interconectados



Velocidad de los cambios

La aceleración digital exige modelos de evaluación de riesgos continuos y dinámicos.



Riesgos emergentes

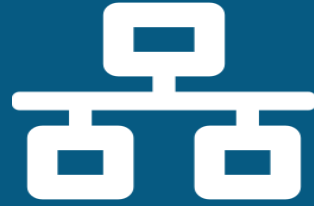
Interconectados y globales: ciberseguridad, fraude con IA, regulaciones cambiantes.



Incertidumbre creciente

El contexto geopolítico y económico amplifica la volatilidad del entorno de riesgo.

Riesgos globales interconectados



Nuevo Modelo Una Auditoría Dinámica

Los cambios constantes requieren abandonar el modelo de auditoría por ciclos anuales y adoptar un enfoque continuo, ágil y data-driven que permita responder a los riesgos en tiempo real.



¿Cómo lo estamos enfrentando desde la Auditoría?

¿Estamos cambiando nuestro enfoque, estilo y dedicación?

La brecha de efectividad en Auditoría Interna

44%



de las funciones de Auditoría Interna son consideradas efectivas en la identificación y gestión temprana de riesgos

80%

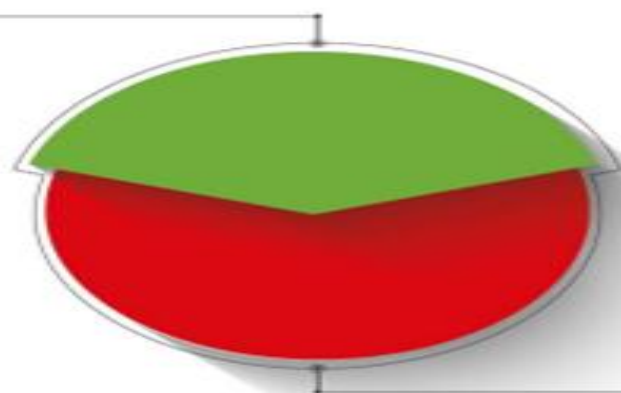


de los Comités de Auditoría creen que existe oportunidad para que la función aporte mucho más valor

¿Dónde está Auditoría en la Transformación Digital?

¿EXISTE UN PROCESO FORMAL ESTRUCTURADO PARA LA TRANSFORMACIÓN DIGITAL DEL DEPARTAMENTO DE AUDITORÍA INTERNA DE TU ORGANIZACIÓN?

40% SÍ



NO 60%

EN CASO AFIRMATIVO, ¿CÓMO SE ENCUENTRA ESTE PROCESO ACTUALMENTE?



33%

Se han identificado las prioridades y objetivos y se están dando los primeros pasos



42%

Se desarrollan inversiones y se está gestionando el cambio



18%

Este proceso se ha consolidado y ya se obtienen los primeros retornos



7%

La transformación digital de Auditoría Interna se ha completado con éxito

¿Y con la IA?



Ignorada

La IA no forma parte
de los planes de auditoría

37%



Observada

Se monitorea el uso
de IA en la organización

37%



Auditada

Se incluye IA en
el alcance de auditoría

14%



Habilitada

IA como herramienta
propia del equipo auditor

12%

¿En qué etapa se encuentra tu función de Auditoría?

Seguimos priorizando el enfoque tradicional

Enfoque Tradicional

"No nos ha ido mal hasta hoy... ¿por qué cambiar?"

Ya el enfoque no es suficiente... los desafíos son mayores.

*El éxito pasado es la mejor receta para... el
FRACASO futuro.*

¿Por qué seguimos trabajando en un enfoque tradicional?



Falta de conciencia

La transformación digital no está priorizada en muchas organizaciones de auditoría.



Escasez de talento

El perfil del auditor digital es escaso: combina negocio, datos e IA.



Rapidez tecnológica

La tecnología evoluciona más rápido que la capacidad de adaptación de las funciones de auditoría.



Falta de normativas

La ausencia de marcos claros genera incertidumbre sobre cómo incorporar IA en auditoría.



Cultura organizacional

El cambio cultural es el mayor obstáculo: el 'siempre lo hicimos así' frena la innovación.



Costos y presupuesto

Presupuestos ajustados y falta de inversión en tecnología limitan la transformación.

Síndrome del auditor obsoleto

Señales de alerta en la función de auditoría.



Sigue atado a procesos tradicionales porque cree que cambiar es traicionar las bases de la profesión.



Cree que la auditoría es una función solo obligada por la regulación.



No se anima a implementar tecnología de punta por falta de conocimiento o resistencia al cambio.



Sigue trabajando en base a muestras y no analiza universos completos de datos.



No da su opinión por miedo a comprometer la independencia — confunde silencio con objetividad.



No se anima a ser protagonista ni a aportar valor estratégico a la organización.



¿Qué debe hacer el auditor
entonces?

El Auditor Frente Al Cambio



Posicionamiento

Definir dónde queremos **estar** y cómo queremos ser **percibidos**. Pasar de verificadores a **asesores estratégicos**.



Equipo

Construir un equipo con **perfil híbrido**: negocio, datos, IA, comunicación y liderazgo.



Velocidad de servicio

La **inmediatez** es un diferencial. Si somos lentos, no aportamos **valor**.

HABILITADOR



Tecnología

Incorporar IA, analytics y automatización como herramientas propias del equipo auditor.

Posicionamiento: dónde queremos estar y cómo nos perciben

1

¿Queremos sólo verificar incumplimientos?

2

¿Queremos analizar el entorno de control?

3

¿Queremos ser un jugador destacado en la organización?

4

¿Queremos asegurar los objetivos estratégicos de la organización?

Cuanto más alto el nivel de posicionamiento, mayor el valor estratégico que aporta Auditoría.

Velocidad: si soy lento no apporto valor

Sin inmediatez

- ✗ Informe entregado meses después
- ✗ Hallazgos ya conocidos por la dirección
- ✗ Recomendaciones tardías sin impacto
- ✗ Percepción de poco valor añadido



Con inmediatez

- ✓ Alertas en tiempo real para la dirección
- ✓ Hallazgos accionables antes de que escalen
- ✓ Recomendaciones oportunas con impacto
- ✓ Auditoría percibida como socio estratégico

Hoy TODOS tenemos incorporado el concepto de inmediatez. Y eso hace la diferencia.

Equipo: el nuevo perfil del auditor interno



TECNOLOGIA: el habilitador de la Auditoría Interna Orientada al Dato



Automatización de Procesos (RPAs)

Bots que ejecutan tareas repetitivas: conciliaciones, extracción de datos, generación de reportes.



Data Analytics e Inteligencia de Procesos

Análisis de universos completos, minería de procesos, detección de ineficiencias.



IA, modelos agénticos y Análisis Predictivo

Modelos que nos facilitan las tareas de investigación, análisis, asistencia y anticipan riesgos antes de que se materialicen. Asimismo mejora la detección temprana de fraudes.



Análisis de Datos No Estructurados

Procesamiento de correos, contratos y documentos para detectar incumplimientos ocultos.



Infraestructura Tecnológica

Plataformas cloud, integración con ERPs y sistemas de la organización.



Audit Data Room

Repositorio centralizado de evidencia digital, papeles de trabajo y hallazgos auditables.

El ciclo de auditoría potenciada por tecnología e IA

La tecnología potencia al auditor, no lo reemplaza: asume el procesamiento masivo, la detección y la documentación; el auditor aporta juicio, escepticismo profesional y visión estratégica.



Planificación y Análisis de Riesgos



Agente de Predicciones

Ej.: Mapa de riesgos futuros en tiempo real

Evaluación automática del universo de riesgos: la IA analiza miles de variables para identificar los riesgos más críticos antes de cada ciclo.

Planificación dinámica y adaptativa: ajusta el plan de auditoría en tiempo real según cambios en el entorno y alertas del negocio.

Análisis predictivo de riesgos emergentes: detecta patrones anómalos y proyecta riesgos futuros con alta precisión, antes de que se materialicen.

Selección inteligente de alcance: reemplaza el muestreo estadístico con análisis de universos completos, priorizando las transacciones de mayor riesgo.

Mapeo automático controles vs. riesgos: identifica brechas de cobertura y sugiere nuevas pruebas basándose en el perfil de riesgo actualizado.

Ejecución y Pruebas de Control



Ejecución de Pruebas

Ej.: Análisis automatizado de registros contables

Análisis del 100% de las transacciones: la IA procesa universos completos de datos financieros, operativos y de control sin límites de muestreo.

Detección automática de anomalías y fraudes: identifica patrones inusuales en pagos, accesos, aprobaciones y operaciones que escapan a la revisión manual.

Pruebas de segregación de funciones: revisa conflictos de roles y accesos lógicos en sistemas ERP y plataformas digitales de forma continua.

Procesamiento de datos no estructurados: analiza correos, contratos y políticas para detectar incumplimientos o riesgos ocultos.

Generación de evidencia digital robusta: documenta hallazgos con trazabilidad completa — hasta 60% de reducción en tiempo de preparación de papeles de trabajo.

Ciberseguridad y Riesgos Tecnológicos



Agente de Análisis

*Ej.: Auditoría de infraestructura
tecnológica*

Monitoreo continuo de postura de ciberseguridad: evalúa en tiempo real la configuración de activos detectando desviaciones respecto a NIST e ISO 27001.

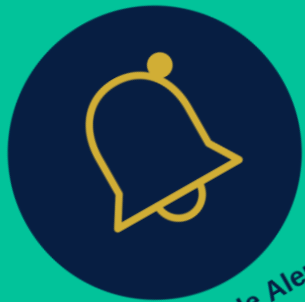
Identificación de vulnerabilidades: analiza logs, tráfico de red y comportamientos para anticipar brechas: infostealers, vishing, credenciales comprometidas.

Auditoría de IA y modelos algorítmicos: evalúa el sesgo, la explicabilidad y la gobernanza de los sistemas de IA propios de la organización.

Detección de deepfakes y fraudes con IA generativa: identifica manipulación de imágenes, audio o documentos en fraudes internos y externos.

Evaluación de terceros y cadena de suministro digital: monitorea el riesgo cibernético de proveedores críticos usando inteligencia de amenazas externa.

Monitoreo Continuo y Auditoría Continua



Monitor de Alertas

Ej.: Tableros de intervención en tiempo real

Auditoría continua 24/7: monitoreo permanente de transacciones y controles críticos en tiempo real, superando el modelo de ciclos anuales.

Alertas tempranas y Red Flags automáticas: notificaciones instantáneas ante desviaciones en KRIs, umbrales de control o comportamientos anómalos.

Seguimiento automático de planes de acción: rastrea la implementación de hallazgos y recomendaciones sin depender de reportes manuales.

Tableros dinámicos para la Dirección y el Comité: visualización en tiempo real del estado de riesgos y controles en el lenguaje del negocio.

Monitoreo de cumplimiento normativo continuo: verifica permanentemente el alineamiento con PCI DSS, SOX, GDPR, ISO 27001 y regulaciones locales.

Reporting e Impacto Estratégico



Agente Asistente

Ej.: Informes pre-elaborados y adaptados por audiencia

Generación automática de informes: la IA generativa redacta borradores, resume hallazgos y adapta el lenguaje a cada audiencia: Comité, Dirección, Reguladores.

Copilot del auditor: asistente virtual que responde sobre normativas, sugiere pruebas y asiste en la revisión de papeles de trabajo.

Análisis de tendencias y benchmarking: compara el perfil de riesgo con referencias del sector, enriqueciendo la opinión del auditor.

Insights proactivos para la Alta Dirección: transforma la función auditora de reactiva a proactiva con opinión fundamentada sobre el negocio y sus riesgos.

Optimización del tiempo del equipo: la IA absorbe tareas repetitivas y de bajo valor, liberando al auditor para el análisis crítico y la interacción estratégica.

Hoja de ruta para incorporar IA en Auditoría Interna

Cuatro fases para pasar de "**observada**" a "**habilitada**", sin comprometer el juicio profesional ni la independencia de la función.

01



Diagnóstico y caso de uso

Mapear el universo de auditoría, identificar procesos y priorizar 2-3 casos de uso con impacto medible.



02



Piloto controlado

Probar la herramienta en un alcance acotado, con validación de cada resultado y métricas



03



Escalado y capacitación

Extender el uso al plan anual, formar al equipo en prompting y lectura crítica de resultados.



04



Gobernanza continua

Revisar nuestras soluciones de IA en uso, controlar sesgos y desempeño periódicamente

Gobernanza de IA en Auditoría Interna

Incorporar con políticas claras, validación de resultados, independencia del juicio humano y gestión de los riesgos propios de la IA.



Políticas de uso claras

Definir qué herramientas se usan, sobre qué datos, y con qué límites de autonomía.



Validación de resultados

Ningún hallazgo o conclusión de IA se reporta sin revisión y juicio profesional del auditor.



Independencia del juicio

La IA asiste el análisis; no sustituye el escepticismo profesional ni la opinión del auditor.



Seguridad y confidencialidad de datos

Gobernar qué información sensible puede procesarse en herramientas de IA y con qué proveedores.



Auditoría de la propia IA

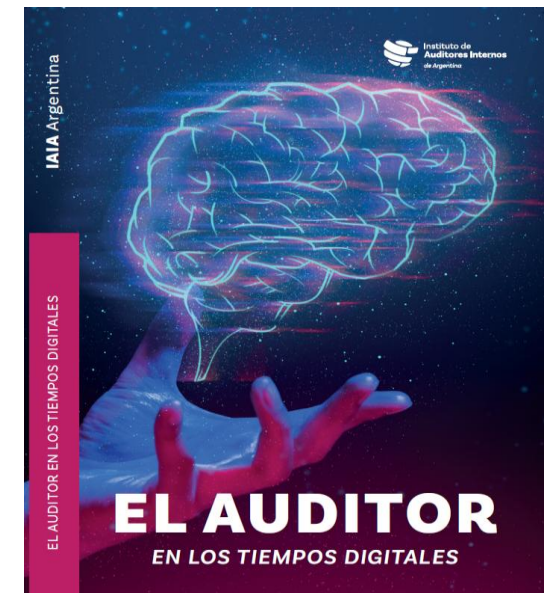
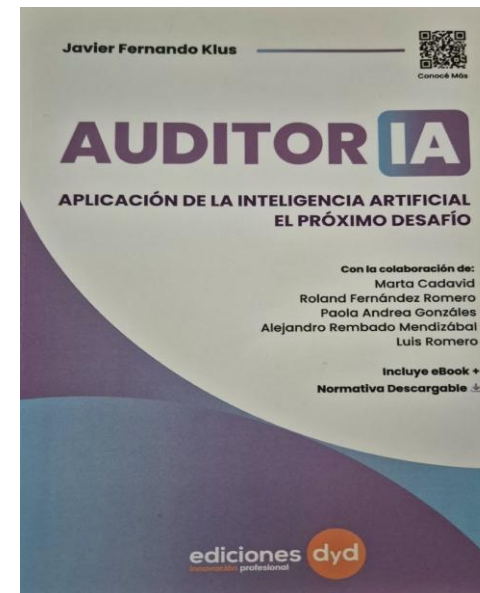
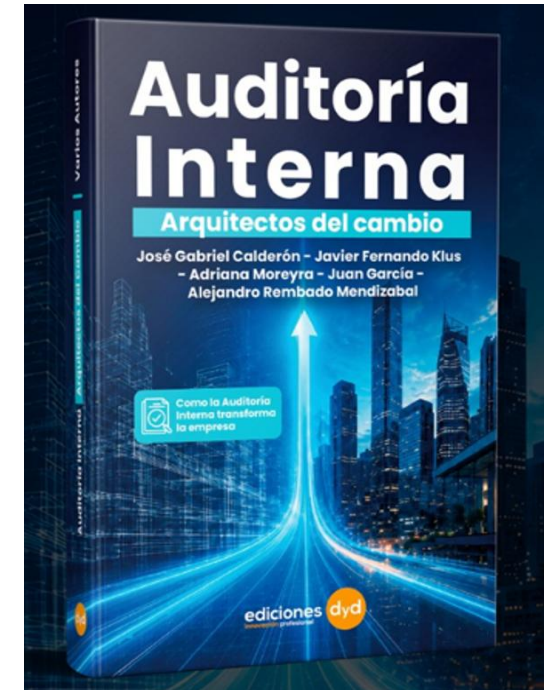
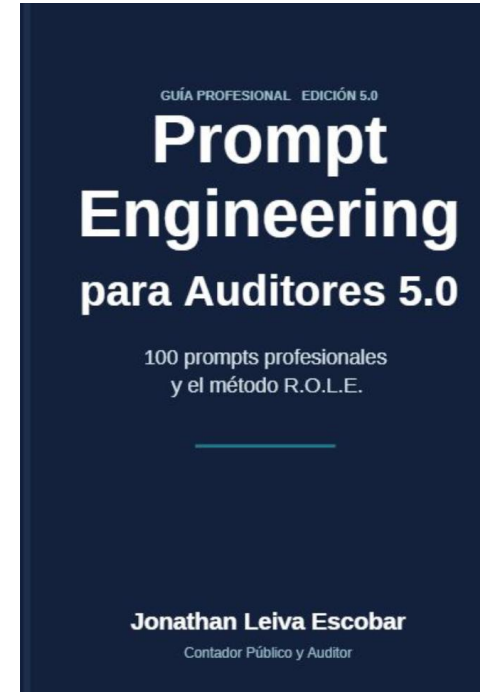
Revisar periódicamente sesgo, explicabilidad y desempeño de los modelos usados por la función.



Reporte al Comité de Auditoría

Informar de forma transparente el uso de IA, sus resultados y sus límites conocidos.

Lectura recomendada



LO NUEVO FUNCIONA: LA IA EN ACCIÓN

El auditor + tecnología: un equipo de mayor valor

La tecnología potencia al auditor, no lo reemplaza: asume el procesamiento masivo, la detección y la documentación; el auditor aporta juicio, escepticismo profesional y visión estratégica.

40%

de reducción en tiempo de ejecución, con mayor cobertura de universos

60%

de reducción en tiempo de preparación de papeles de trabajo



El nuevo perfil del auditor híbrido

Combina conocimiento del negocio con data analytics, prompting de IA generativa, modelos predictivos y gestión del riesgo tecnológico.



Las personas siguen siendo el mayor activo

La tecnología es un complemento del talento humano, no su reemplazo.

*“El auditor del futuro no revisa el pasado...
diseña el futuro del control.”*

¿De qué lado querés estar?

Lo nuevo funciona cuando la tecnología amplía el juicio del auditor — no cuando lo reemplaza. Esa es la agenda 2027 para la Auditoría Interna.



Muchas gracias

Alejandro Rembado

alejandro.rembado@iaia.org.ar

rembadoa@gmail.com

