

Traducción al Español Auspiciada por:



**FLAI**  
Fundación Latinoamericana  
de **Auditores Internos**

# PERSPECTIVAS Y PERCEPCIONES GLOBALES

*La revolución de la Inteligencia Artificial*

**Parte I: Comprender, Adoptar Y Adaptarse A La IA**

**Parte II: Revisión Del Marco De Inteligencia Artificial Del IIA**

**Parte III: El Papel De La Auditoría Interna En La Ética De La IA**



The Institute of  
**Internal Auditors**

# Contenido

---

<b>PARTE I: COMPRENDER, ADOPTAR Y ADAPTARSE A LA IA .....</b>	<b>3</b>
<b>INTRODUCCIÓN .....</b>	<b>5</b>
Una Zona de Crecimiento .....	5
<b>COMPRENDER LA IA.....</b>	<b>7</b>
Más allá de la Simple Automatización .....	7
Poner en práctica la IA.....	8
Oportunidades, retos y riesgos.....	9
<b>EL PAPEL DE LA AUDITORÍA INTERNA.....</b>	<b>12</b>
Técnicas fiables y competencias probadas respaldan la gestión de riesgos de la IA.....	12
Buenas prácticas para poner en práctica la IA .....	12
<b>CONCLUSIÓN .....</b>	<b>14</b>
<b>Parte II: Revisión del marco de inteligencia artificial del IIA .....</b>	<b>15</b>
<b>INTRODUCCIÓN .....</b>	<b>17</b>
<b>COMPONENTES CLAVE.....</b>	<b>18</b>
Estrategias basadas en capacidades, riesgos y oportunidades .....	18
<b>LOS SEIS COMPONENTES.....</b>	<b>19</b>
Gobernanza de la IA .....	19
Arquitectura e infraestructura de datos .....	20
Calidad de los datos.....	21
Medición del rendimiento de la IA .....	21
El factor humano .....	21
El factor de la caja negra .....	22
<b>CONSIDERACIONES ÉTICAS.....</b>	<b>23</b>
La auditoría interna debe permanecer vigilante.....	23
<b>EL PAPEL DE LA AUDITORÍA INTERNA.....</b>	<b>24</b>

---



Asumir el reto del aseguramiento .....	24
<b>CONCLUSIÓN .....</b>	<b>25</b>
<b>PARTE III: EL PAPEL DE LA AUDITORÍA INTERNA EN LA ÉTICA DE LA IA .....</b>	<b>26</b>
<b>INTRODUCCIÓN .....</b>	<b>28</b>
<b>Riesgos y oportunidades .....</b>	<b>29</b>
El entusiasmo por la IA podría eclipsar las consideraciones éticas .....	29
<b>Volver a Conceptos fundamentales de auditoría .....</b>	<b>32</b>
Utilización de enfoques de garantía fundamentales para la nueva tecnología .....	32
<b>Uso de la IA en la auditoría interna .....</b>	<b>34</b>
Entendiendo sobre la privacidad y la responsabilidad de la IA .....	34
<b>Conclusión .....</b>	<b>36</b>



# PARTE I: COMPRENDER, ADOPTAR Y ADAPTARSE A LA IA



## **Sobre el experto**

### **Eric Wilson, CIA, CISA**

Eric Wilson es director de auditoría interna y CAE en Gulfport Energy. Anteriormente dirigió equipos de auditoría interna y consultoría para varias empresas nacionales e internacionales de una amplia gama de sectores, como el energético, el inmobiliario comercial y el cuidado de la salud. Es miembro de la Junta de Asesores de la Steed School of Accounting de la Universidad de Oklahoma, ha dado conferencias sobre auditoría interna en varias universidades y ocupa puestos de liderazgo activo en múltiples organizaciones locales y sin ánimo de lucro. Actualmente forma parte del Comité de Conocimientos Profesionales del Instituto de Auditores Internos (IIA) y del Comité Asesor de Contenidos de Norteamérica. Es miembro de la Junta de Gobernadores de la Sección de Oklahoma del IIA.



# INTRODUCCIÓN

## Una Zona de Crecimiento

Cuando ChatGPT fue introducido en noviembre de 2022, se consideró un importante salto adelante en la inteligencia artificial (IA). Muchos la compararon con Internet por su potencial para cambiar y alterar las prácticas empresariales, las normativas y las normas sociales actuales.

ChatGPT y sus alternativas emergentes son ejemplos de IA generativa. La IA generativa se basa en grandes modelos lingüísticos, sistemas que se entrenan con enormes cantidades de datos procedentes de diversas fuentes y que son procesados por una red neuronal inspirada en el cerebro humano para desarrollar los resultados solicitados. Cuando se le pide, utiliza esta formación y algoritmos para desarrollar contenidos -incluidos texto, imágenes, vídeos, sonidos, voz y código- que se asemejan a lo que podría crear un ser humano.

Aunque este sistema específico ha recibido una enorme atención, es sólo un ejemplo de las muchas herramientas que se engloban bajo el paraguas de la IA. La IA está en el corazón de todos los dispositivos inteligentes que utilizamos y también impulsa aplicaciones mucho más sofisticadas que están transformando los negocios. Se está aplicando en empresas, administraciones públicas, sanidad y muchos otros campos para reproducir el análisis humano e incluso la toma de decisiones.

Se prevé que el mercado mundial de IA compuesta aumente de 900 millones de dólares en 2023 a 4.400 millones de dólares en 2028, con una tasa de crecimiento anual compuesta del 36,5%, a medida que la creciente disponibilidad de datos y recursos de IA estimule el uso y desarrollo de nuevas soluciones de IA.<sup>1</sup> La gran mayoría de los líderes empresariales (94%) cree que la IA será fundamental para el éxito de sus organizaciones en los próximos cinco años, según la [edición más reciente](#) de Deloitte "State of AI in the Enterprise".<sup>2</sup>

"La IA puede convertirse en el desarrollo tecnológico más disruptivo hasta la fecha, creando nuevas oportunidades y riesgos en todos los aspectos de los negocios y la vida", de acuerdo a un [Artículo](#) en la revista *Internal Auditor*<sup>3</sup>. Los auditores internos son expertos en evaluar los riesgos y oportunidades que afectan a la capacidad de una organización para cumplir sus objetivos. Gracias a sus conocimientos y experiencia, "la auditoría interna puede ayudar a una organización a evaluar, comprender y comunicar el grado en que la inteligencia artificial tendrá un efecto (negativo o positivo) en la capacidad de la organización para crear valor a corto, medio o largo plazo", según "[Artificial Intelligence—Considerations for the Profession of Internal Auditing](#)"<sup>4</sup> del Instituto de Auditores Internos (IIA).

Dado el amplio y rápido crecimiento del uso de la IA, es importante que los auditores internos desarrollen rápidamente un profundo conocimiento de su funcionamiento, sus aplicaciones prácticas en empresas y administraciones públicas, y los riesgos y oportunidades

# 94%

de los líderes empresariales creen que la IA será fundamental para el éxito de sus organizaciones en los próximos cinco años.

Fuente: Deloitte - State of AI in the Enterprise, 5<sup>th</sup> Edition

<sup>1</sup> "\$4.4 Billion Composite AI Markets: Growing Intricacy of AI Applications for Better Performance and Accuracy to Drive Growth - Global Forecast to 2028," Research and Markets press release, June 13, 2023.

<sup>2</sup> "State of AI in the Enterprise, Fifth Edition," Deloitte, October 2022.

<sup>3</sup> "Auditing Artificial Intelligence," James Bone, *Internal Auditor*, October 14, 2020.

<sup>4</sup> "Artificial Intelligence—Considerations for the Profession of Internal Auditing", The Institute of Internal Auditors, 2017.



que presenta para las organizaciones. Este informe examinará estas áreas en profundidad y proporcionará las mejores prácticas y puntos de vista para mantener el ritmo.



# COMPRENDER LA IA

## Aprendizaje Automático e Inteligencia Humana Simulada

---

### Más allá de la Simple Automatización

**Los términos IA y automatización suelen utilizarse indistintamente.** Esto refleja una comprensión limitada del potencial de la IA, que es más potente y puede cambiar las reglas del juego. De hecho, aunque la IA puede automatizar tareas rutinarias, sus capacidades y usos son mucho mayores. Por ejemplo, la automatización robótica de procesos (RPA), un nivel básico de automatización, utiliza datos estructurados y lógica para realizar procesos repetitivos basados en reglas, como flujos de trabajo de contabilidad y recopilación de datos. De este modo, permite a las personas asumir tareas de mayor nivel. Puede replicar las *acciones* humanas, pero las herramientas de IA más sofisticadas pueden realizar tareas que simulan la *inteligencia* humana, como comprender las comunicaciones humanas normales, asumir la resolución de problemas y ofrecer un mayor rendimiento y eficiencia operativa. La automatización sigue reglas establecidas, mientras que la IA se basa en la formación que ha recibido para tomar sus propias decisiones.

Las soluciones de IA y aprendizaje automático pueden clasificarse en varias categorías, entre ellas:

- Descriptiva: ¿Qué ha ocurrido?
- Diagnóstico: ¿Por qué ha ocurrido?
- Predictivo: ¿Qué podría ocurrir a continuación?
- Prescriptivo: ¿Qué debe hacerse a continuación?<sup>5</sup>

Sin embargo, en la actualidad la IA no posee el tipo de juicio o contexto que permite a los humanos tomar las mejores decisiones, aunque esas capacidades pueden mejorar a medida que avance la tecnología.

Además, la IA es tan buena como su entrenamiento. Al estudiar casos de infracción de normas, investigadores del MIT y de otras organizaciones descubrieron que si los modelos de aprendizaje automático no se entrenan con los datos adecuados, “es probable que emitan juicios diferentes y más severos que los humanos.”<sup>6</sup> Los riesgos relacionados con las limitaciones de la IA se tratarán en otra sección.

---

<sup>5</sup> “AI and Machine Learning: It May Not Be as Difficult as You Think,” RSM, September 7, 2022.

<sup>6</sup> “Study: AI Models Fail to Reproduce Human Judgements About Rule Violations,” Adam Zewe, MIT News, May 10, 2023.





## Poner en práctica la IA

Las aplicaciones prácticas de la IA incluyen herramientas cotidianas que se utilizan desde hace años, como los motores de búsqueda en línea; chatbots que proporcionan información sencilla y respuestas a preguntas; asistentes de voz, como Alexa y Siri, que responden a órdenes y realizan tareas; Google Maps y herramientas similares para seleccionar las mejores rutas de viaje y entrega; coches que se conducen solos; experiencias de compra en línea personalizadas; y publicidad personalizada. Gartner cita ejemplos de cómo puede utilizarse la IA generativa, por ejemplo, en el diseño de fármacos, la ciencia de los materiales, el diseño de chips, los datos sintéticos y el diseño de piezas.<sup>7</sup>

Otros casos de uso de la IA en empresas y administraciones públicas son:

- Resolver la escasez de cualificaciones mediante la automatización de tareas.
- Mejorar el rendimiento informático o de la red
- Diseñar estrategias para retener o atraer a determinados clientes y mejorar su experiencia. Por ejemplo, un reciente [artículo de Harvard Business Review](#) señalaba que Brinks Home, una empresa de tecnología doméstica inteligente, utilizó la IA para ganar reconocimiento de marca en un mercado competitivo.<sup>8</sup>
- Identificar y prevenir fraudes o errores en la información financiera.
- Previsión de la demanda de productos o servicios basándose en el historial y los comentarios de los clientes, así como en la actividad económica y del mercado.
- Abordar los objetivos de sostenibilidad. La IA puede ayudar a alcanzar el 79% de los Objetivos de Desarrollo Sostenible de la Asamblea General de la ONU, según [Nature Communications](#).<sup>9</sup>
- Dar prioridad a las oportunidades o clientes potenciales.
- Seguimiento de las respuestas a las campañas de ventas, estudios de mercado y optimización de motores de búsqueda (SEO).
- Racionalización y mejora de las actividades de atención al cliente.

En la actualidad, las inversiones en IA generativa en las empresas siguen centrándose en gran medida en mejorar las relaciones con los clientes y aumentar los ingresos.

---

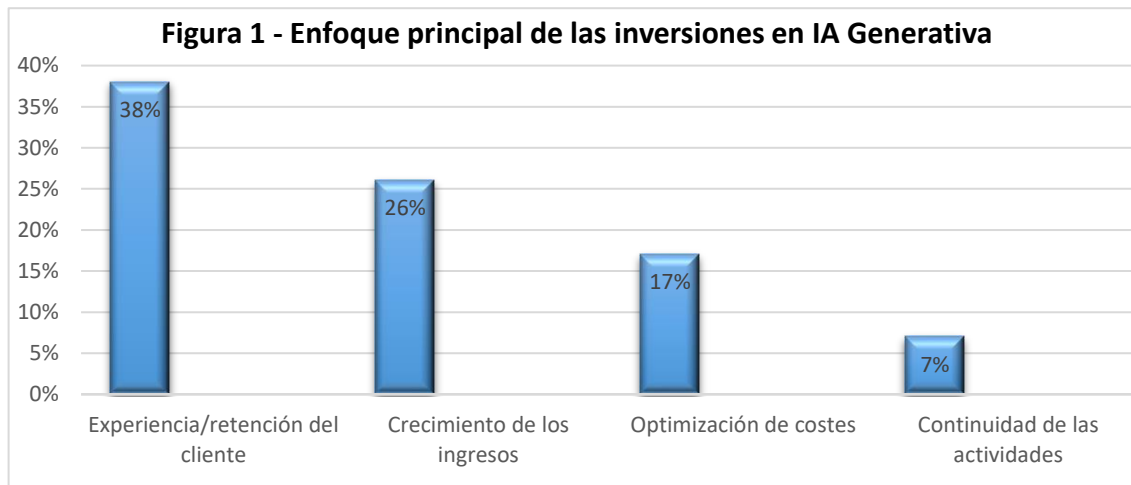
<sup>7</sup> “Beyond ChatGPT: The Future of Generative AI for Enterprises,” Jackie Wiles, Gartner, January 26, 2023.

<sup>8</sup> “Customer Experience in the Age of AI,” David C. Edelman and Mark Abraham, Harvard Business Review, March-April 2022.

<sup>9</sup> “The Role of Artificial Intelligence in Achieving the Sustainable Development Goals,” Ricardo Vinuesa, et al., Nature Communications, January 13, 2020.



Según una encuesta reciente de Gartner, la mayoría de las empresas aún no se han comprometido de forma significativa a impulsar nuevas oportunidades de negocio o nuevos mercados mediante la IA generativa (véase la figura 1).



Fuente: Encuesta de Gartner realizada a más de 2.500 ejecutivos, 2023<sup>10</sup>

## Oportunidades, retos y riesgos

Al desarrollar y aplicar una estrategia de IA, las empresas deben comprender no sólo las posibilidades, sino también las limitaciones y amenazas que puede plantear esta tecnología. Mientras las empresas se apresuran a implantar soluciones de IA, entre los ejemplos de oportunidades de la IA se incluyen la capacidad de:

- Acortar el ciclo de procesamiento de datos.
- Minimizar los posibles errores sustituyendo las acciones humanas por acciones mecánicas perfectamente repetibles.
- Utilice la automatización de procesos para reducir el tiempo y los costes de mano de obra.
- Emplear robots o drones para trabajos potencialmente peligrosos.
- Realizar predicciones más precisas sobre temas que pueden ir desde las ventas potenciales en mercados específicos hasta la predicción de epidemias y catástrofes naturales.
- Utilizar iniciativas y eficiencias de IA para impulsar los ingresos y el crecimiento de la cuota de mercado.<sup>11</sup>

A pesar de todas sus ventajas, aprovechar la IA puede plantear dificultades. Según la *IBM Global AI Adoption Index*, casi una de cada cinco empresas citó dificultades en:

- Garantizar la seguridad de los datos.
- Garantizar la gobernanza de los datos.
- Gestionar fuentes y formatos de datos dispares.

<sup>10</sup> "Gartner Experts Answer the Top Generative AI Questions for Your Enterprise," Gartner, 2023.

<sup>11</sup> *Artificial Intelligence—Considerations for the Profession of Internal Auditing*, Institute of Internal Auditors, 2017.



- Integrar datos en cualquier nube.<sup>12</sup>

Es posible que las organizaciones no sepan cómo aprovechar mejor las oportunidades de la IA. Al mismo tiempo, si no comprenden plenamente el funcionamiento de estos sistemas y los sesgos y errores que pueden infiltrarse en su formación y resultados, las empresas podrían ser vulnerables a una serie de amenazas sin saberlo. Los riesgos que pueden causar daños a la reputación o financieros, entre otras amenazas, incluyen:

- **Falta de transparencia.** Los sesgos o errores no identificados incorporados a la tecnología de IA pueden dar lugar a una serie de decisiones inadecuadas, como la discriminación en la contratación o la concesión de créditos, por ejemplo.
- **Mantener la seguridad y confidencialidad de la información.** "No se pueden exagerar los efectos potencialmente desastrosos de una violación de la ciberseguridad en la que esté implicada la IA", según el informe del IIA [Artificial Intelligence—Considerations for the Profession of Internal Auditing](#). El IIA recomendó que, si las organizaciones no disponen ya de suficiente ciberseguridad, los CAE informen continuamente a las partes interesadas de que debe crearse rápidamente. A medida que las organizaciones pasan a recopilar y almacenar volúmenes de datos cada vez mayores, pueden ser vulnerables a infracciones, violaciones de la privacidad, pérdida de datos o fallos del sistema causados por errores internos y por actos de piratas informáticos u otros ciberdelincuentes. Las tácticas utilizadas por los ciberdelincuentes también pueden incluir el "envenenamiento de modelos", en el que se contaminan deliberadamente los datos de entrenamiento de un modelo de aprendizaje automático. Esto puede corromper los sistemas, producir datos incorrectos, desencadenar una denegación de servicio o iniciar ataques de malware que pueden paralizar las organizaciones.<sup>13</sup>
- **Desafíos Jurídicos.** El plagio, la infracción de los derechos de autor o las violaciones de la propiedad intelectual son peligros potenciales si el contenido que genera la IA no es original. Además, unas pruebas y una supervisión inadecuadas de la IA pueden dar lugar a resultados éticamente cuestionables.
- **Dependencia de vendedores o proveedores.** Esto puede constituir una amenaza particular a medida que la IA se convierte en clave para una amplia gama de sistemas y funciones organizativas.<sup>14</sup> Entre otras preocupaciones, las organizaciones deben asegurarse de que los indicadores de evaluación de riesgos abordan adecuadamente los peligros que entraña el uso o la integración de herramientas de terceros, dadas las preocupaciones asociadas sobre las acciones y comportamientos de vendedores o proveedores.
- **Pérdidas de empleo.** Las organizaciones podrían enfrentarse a decisiones difíciles si la IA sustituye a trabajadores que no pueden ser reasignados o que no pueden encontrar trabajos similares. Además de las consecuencias para las personas, el desempleo en una zona o industria puede provocar trastornos económicos y sociales.

## Primeros pasos hacia la regulación de la IA

El rápido auge y los riesgos potenciales de la IA han provocado llamamientos a una mayor regulación. El Parlamento Europeo ha aprobado un proyecto de [Ley de Inteligencia Artificial](#), que exige mayor transparencia y salvaguardias. La ley establece tres niveles de riesgo de la IA: las aplicaciones y sistemas considerados de riesgo inaceptable, que están prohibidos; las aplicaciones de alto riesgo, que están sujetas a requisitos legales establecidos; y las de riesgo limitado, que podrían cumplir una regulación mínima de transparencia. La IA generativa también tendría que cumplir requisitos de transparencia. Las multas pueden ascender a 33 millones de dólares, es decir, el 6% de los ingresos globales anuales de una empresa.

En Estados Unidos, la Casa Blanca ha publicado [una hoja informativa](#) y un anteproyecto de [Carta de Derechos de la Inteligencia Artificial](#) para garantizar la seguridad y eficacia de los sistemas. China también ha [redactado una normativa](#) que establece posibles límites a la IA generativa. Además, Sam Altman, director general de OpenAI, creadora de ChatGPT, [ha pedido](#) una regulación internacional coordinada de la IA generativa y ha firmado una [declaración sobre el riesgo de la IA](#) junto con cientos de otros expertos en IA y personalidades públicas.

<sup>12</sup> IBM Global AI Adoption Index 2022.

<sup>13</sup> "Do Free AI Tools Pose a Security Risk to Your Business?", Rebecca Neubauer, Business News Daily, May 16, 2023.

<sup>14</sup> "Artificial Intelligence and The Top 6 Business Risks," Chandu Gopalakrishnan, April 28, 2023, The Cyber Express.



- **Riesgos regulatorios.** A medida que los gobiernos intentan comprender y abordar el uso de la IA, las organizaciones pueden tener que adaptar sus estrategias de IA a un panorama normativo en evolución. También puede haber riesgos legales si los problemas con sus sistemas de IA causan pérdidas financieras a terceros o si violan los derechos humanos o las normas éticas.
- **Consideraciones medioambientales.** Los sistemas que alimentan la IA consumen grandes cantidades de electricidad, lo que puede contrarrestar los esfuerzos de sostenibilidad de las organizaciones y obstaculizar la consecución de sus objetivos medioambientales, sociales y de gobernanza (ESG).
- **Toma de decisiones de inversión y resultados.** La organización puede estar en desventaja competitiva debido a una inversión insuficiente en iniciativas de IA o a la resistencia a estas iniciativas por parte de clientes, empleados u otras partes interesadas. El rendimiento de la inversión en IA (infraestructura, investigación y desarrollo, y adquisición de talento) puede no ser el adecuado. Sin una estrategia sólida de IA, estos problemas pueden obstaculizar el esfuerzo de una organización por hacer el mejor uso de las herramientas de IA.



# EL PAPEL DE LA AUDITORÍA INTERNA

## Evaluación de Riesgos y Aporte de Prospectiva

### Técnicas fiables y competencias probadas respaldan la gestión de riesgos de la IA

La auditoría interna está bien equipada para ayudar a las organizaciones a evaluar y comunicar el impacto de la IA en la creación de valor y la consecución de objetivos. Los responsables de auditoría interna pueden incorporar consideraciones de IA en sus evaluaciones de riesgos y determinar cómo debe incluirse la IA en un plan de auditoría basado en riesgos. Los profesionales deben asumir un papel activo en los proyectos de IA desde el principio. Actuando como asesores de confianza, los auditores internos pueden ofrecer asesoramiento y visión sobre la implementación. Esto supone que se ha adquirido o se adquirirá competencia en las áreas pertinentes. Además, la auditoría interna puede ofrecer garantías sobre las áreas de riesgo relacionadas, como el impacto de la IA en la preparación y la respuesta a las ciber amenazas. Es importante señalar que, para mantener la independencia y la objetividad, los auditores internos no deben asumir la propiedad o la responsabilidad de la aplicación de la IA u otras medidas.

Si una organización ya ha implantado la IA en sus operaciones o en un producto o servicio, la auditoría interna puede:

- Ofrecer garantías sobre la gestión de riesgos relacionados con la fiabilidad de los algoritmos subyacentes y los datos en los que se basan.
- Garantizar que se abordan las cuestiones morales y éticas relacionadas.
- Ofrecer garantías sobre las estructuras de gobernanza de la IA.

Los auditores internos están preparados para desempeñar estas funciones por su:

- Comprensión de los objetivos estratégicos de la organización y cómo se logran.
- Capacidad para evaluar si las actividades de IA están cumpliendo sus objetivos.
- Capacidad para ofrecer garantías internas sobre los esfuerzos de gestión de riesgos de IA de la dirección.
- Posición como asesor de confianza que puede ofrecer ideas sobre el uso de la IA para mejorar los procesos empresariales o las ofertas de productos y servicios.

### Buenas prácticas para poner en práctica la IA

Por desalentadora que pueda parecer la IA, lo mejor para los auditores internos es adoptarla lo antes posible y en la mayor medida posible.

#### Marcos y normas de IA

En 2017, el Instituto de Auditores Internos publicó uno de los primeros marcos para auditar la inteligencia artificial. Otras directrices relevantes sobre IA son:

[Marco de gestión de riesgos de la IA](#) del Instituto Nacional de Normas y Tecnología (NIST) de EE.UU., que incluye [investigaciones y normas relacionadas](#).

[El Trustworthy & Responsible Artificial Intelligence Resource Center](#), que forma parte del NIST, es un repositorio de las orientaciones federales estadounidenses actuales sobre IA.

La Oficina del Comisario de Información del Reino Unido ofrece [orientación y recursos](#) sobre la IA.

La Organización de Cooperación y Desarrollo Económicos proporciona un [marco](#), así como información sobre principios y políticas.



"No hay que esconderse de tecnologías avanzadas como la IA", aconseja Eric Wilson, CIA, CISA, director de auditoría interna y CAE de Gulfport Energy Corporation. Para muchas empresas, la IA ya figura en sus perfiles de riesgo desde hace varios años, pero algunas deciden aplazar su abordaje por falta de conocimientos sobre ella y sobre cómo debe auditarse. Sin embargo, Wilson señala que los auditores tendrán que desarrollar su experiencia en herramientas que sus organizaciones ya estén utilizando o que puedan adoptar en breve.

La mejor forma de empezar es probando, algo que es fácil de hacer con IA generativa como ChatGPT o Bard. "Vea cómo funciona, interactúe con el sistema", recomienda Wilson. Como parte del proceso, si el sistema utiliza un modelo de lenguaje interactivo, pídele que te explique la lógica que ha utilizado para producir sus respuestas. Ésta es una opción que sólo está disponible con un sistema de IA generativa, porque se basa en el lenguaje, así que merece la pena intentarlo.

Para comprender mejor los sistemas que no son tan fáciles de interconectar como ChatGPT, Wilson recomienda pedir a las personas de la organización que los utilicen que le sigan de cerca. Esto puede ofrecer una comprensión práctica de cómo se aplica el sistema a diferentes funciones y usos. En un nivel básico, "averigua si las personas que lo utilizan pueden explicarlo o describir cómo está marcando la diferencia en la organización". afirma Wilson. Si no pueden, esta falta de experiencia o laguna en la comprensión de cómo funciona el sistema a un nivel fundamental puede ser una oportunidad para mejorar la utilización que la auditoría interna puede señalar a la organización."



# CONCLUSIÓN

---

**“Este es un momento apasionante para que la auditoría interna desempeñe un papel de liderazgo** en la garantía de la IA,” según el artículo de la revista *Internal Auditor*.<sup>15</sup> Se espera que la expectativa inicial disminuya a medida que las organizaciones se esfuercen por comprenderla y aplicarla, pero su impacto se ampliará a medida que las personas y las empresas encuentren formas más innovadoras de ponerla en práctica.<sup>16</sup> Ahora es el momento de que los auditores internos comprendan las oportunidades y los riesgos para sus organizaciones, de modo que puedan ofrecer garantías y perspectivas valiosas sobre las iniciativas de IA.

---

<sup>15</sup> “Auditing Artificial Intelligence,” James Bone, *Internal Auditor*, October 14, 2020.

<sup>16</sup> “Gartner Experts Answer the Top Generative AI Questions for Your Enterprise,” Gartner, 2023.



## Parte II: Revisión del marco de inteligencia artificial del IIA





## Sobre el experto

### **Eric Wilson, CIA, CISA**

Eric Wilson, CIA, CISA, es director de auditoría interna y CAE de Gulfport Energy. Anteriormente dirigió equipos de auditoría interna y consultoría para varias empresas nacionales e internacionales en una amplia gama de sectores, como el energético, el inmobiliario comercial y el sanitario. Es miembro del Comité de Conocimientos Profesionales y del Comité Asesor de Contenidos para Norteamérica del Instituto de Auditores Internos (IIA). Ha formado parte del Comité de Defensa del IIA y es miembro de la Junta de Gobernadores de la Sección de Oklahoma del IIA. Además de su trabajo con el IIA, Eric es miembro de la Junta de Asesores de la Escuela de Contabilidad Steed de la Universidad de Oklahoma, ha dado conferencias sobre auditoría interna en varias universidades y ocupa puestos de liderazgo activo en varias organizaciones locales y sin ánimo de lucro.



# INTRODUCCIÓN

---

En 2017, el Instituto de Auditores Internos (IIA) publicó un estudio histórico sobre un tema que ha cobrado mayor importancia desde entonces, [“Inteligencia Artificial - Consideraciones para la Profesión de Auditor Interno.”](#) Este trabajo en tres partes describe el papel del auditor interno en la inteligencia artificial (IA), establece un marco de cuestiones que deben tenerse en cuenta al abordar la IA en el contexto de la auditoría interna, y discute la aplicación práctica de esta tecnología multifacética.

A pesar de los enormes avances en IA durante los seis años siguientes, el marco sigue siendo en gran medida relevante y útil en la mayoría de las áreas de auditoría interna. Este informe comienza revisando algunos de los elementos clave del marco y su continua aplicabilidad. También revisa otras cuestiones a tener en cuenta y concluye examinando el papel del auditor interno en la IA en el futuro.



# COMPONENTES CLAVE

## El marco aborda los factores críticos

---

### Estrategias basadas en capacidades, riesgos y oportunidades

**El marco aborda seis componentes**, todo ello incorporado a la estrategia de la organización. El marco señala que cada organización necesitará una estrategia de IA única basada en sus propias capacidades existentes, así como en su enfoque para gestionar los riesgos y capitalizar las oportunidades. Al evaluar en qué punto se encuentran las organizaciones en su estrategia de IA, la auditoría interna debe considerar cuestiones como las siguientes:

- ¿Tiene la organización una estrategia de IA definida?
- ¿Está invirtiendo en investigación y desarrollo de IA?
- ¿Tiene planes para identificar y abordar las amenazas y oportunidades de la IA?

El marco señala que la IA puede proporcionar una ventaja competitiva a las organizaciones, y que la auditoría interna debe ayudar a la dirección y al consejo a darse cuenta de la importancia de desarrollar una estrategia de IA meditada y coherente con los objetivos de la organización. Estas observaciones siguen siendo válidas hoy en día. La planificación estratégica para la IA también es única debido a la rápida y constante evolución de la tecnología y la amplitud y profundidad de su impacto potencial. Como punto de partida, los auditores internos deben asegurarse de que comprenden plenamente la magnitud de los sistemas de IA. “Algunos componentes críticos son tan diferentes de los sistemas que hemos utilizado y auditado anteriormente, que tanto los usuarios finales como los auditores pueden no entender qué hace el sistema y cómo lo hace,” dijo Eric Wilson, CIA, CISA, director de auditoría interna y CAE de Gulfport Energy.

Una diferencia clave en lo que respecta a la IA es la creación de significado, que se refiere a cómo las personas se entienden o dan sentido a sí mismas, a los acontecimientos que experimentan y al mundo que les rodea. Es un concepto que también se aplica a las tecnologías avanzadas. “La creación de sentido en la era de la IA comienza con una apreciación de lo que las máquinas pueden y no pueden hacer. Es posible, por ejemplo, que una máquina realice determinados tipos de diagnósticos [médicos] con más precisión que una persona. Pero corresponderá a enfermeras, médicos y terapeutas ayudar a los pacientes a comprender las implicaciones y gestionar las consecuencias. Es la diferencia entre conocimiento y significado.”<sup>17</sup>

Con la IA, la tecnología ha pasado de ser capaz simplemente de recopilar y clasificar datos a ser más capaz de tomar información y contextualizarla. Es un paso adelante que ofrece a las organizaciones capacidades, riesgos y oportunidades completamente nuevos. Wilson recomienda que los auditores internos entablen una conversación continua, tanto internamente como con sus compañeros, sobre la auditoría de la estrategia de IA para supervisar adecuadamente su eficacia.

---

<sup>17</sup> “Putting Lifelong Learning on the CEO Agenda,” A. Edmonson and B. Saxberg, *McKinsey Quarterly* 2017 Number 4.



# LOS SEIS COMPONENTES

## Gobernanza, rendimiento y más

### Gobernanza de la IA

Este componente abarca las estructuras, los procesos, y procedimientos que se utilizan para dirigir, gestionar y supervisar las actividades de IA de la organización emprendidas para alcanzar sus objetivos. Una vez más, la formalidad y estructura adecuadas del gobierno de la IA variarán en función de las circunstancias y características de cada empresa. En todos los casos, señala el marco, la gobernanza de la IA aborda la rendición de cuentas y la supervisión, y considera si los responsables de la IA tienen las habilidades y la experiencia necesarias para supervisar su uso y si sus actividades de IA reflejan sus valores. Dados los avances en el impacto de la IA, es fundamental que las acciones y decisiones relacionadas se ajusten a las responsabilidades éticas, sociales y legales de la organización.

La gobernanza de los datos siempre es importante, pero una vez más, el enfoque es un poco diferente cuando se trata de IA. Por ejemplo, dado que los sistemas de IA generativa se entrenan con información específica, es mucho más fácil introducir no solo errores, sino también sesgos en las primeras fases de su desarrollo si no se entrenan con datos fiables. Si a los sistemas tradicionales se les enseña que un determinado tono de rojo es azul, siempre pensarán que ese tono es azul. En cambio, la IA en esa situación pensará que cualquier tono de rojo es azul.

Una vez que un pequeño sesgo o inexactitud se introduce en la tecnología, el sistema seguirá entrenándose en ese error, ampliando su impacto potencialmente de manera exponencial, por lo que el sesgo debe ser detectado y eliminado por adelantado antes de que se utilice en la toma de decisiones, en una comunicación de cara al cliente, o de cualquier otra manera que pueda dañar las finanzas o la reputación de la organización. "Un dato erróneo podría cambiar por completo la forma en que el sistema ve y contextualiza los datos con los que intenta trabajar", afirma Wilson.

### ENFOQUE DE AUDITORÍA

#### Principales normas del IIA

Las Normas Internacionales para la Práctica Profesional de la Auditoría Interna del IIA incluyen varias normas que son particularmente relevantes para la IA, incluyendo:

- Norma 1100 del IIA: Independencia y objetividad
- Norma 1210 del IIA: Competencia
- Norma 2010 del IIA: Planificación
- Norma 2030 del IIA: Gestión de recursos
- Norma 2100 del IIA: Naturaleza del trabajo
- Norma 2110 del IIA: Gobernanza
- Norma 2120 del IIA: Gestión de riesgos
- Norma 2130 del IIA: Control
- Norma 2200 del IIA: Planificación del compromiso
- Norma 2201 del IIA: Consideraciones sobre la planificación
- Norma 2210 del IIA: Objetivos del compromiso
- Norma 2220 del IIA: Alcance del encargo
- Norma 2230 del IIA: Asignación de recursos para el encargo
- Norma 2240 del IIA: Programa de trabajo del encargo
- Norma 2310 del IIA: Identificación de la información
- Norma 2400 del IIA: Comunicación de resultados
- Norma 2410 del IIA: Criterios de comunicación
- Norma 2420 del IIA: Calidad de las comunicaciones
- Norma 2440 del IIA: Difusión de resultados

El texto completo de las Normas está disponible en [theiia.org](http://theiia.org). Cada norma se complementa con una guía de aplicación.



## Arquitectura e infraestructura de datos

El marco establece que la arquitectura y la infraestructura de los datos de IA se parecerán probablemente a las utilizadas para los macrodatos. Las cuestiones que entran dentro de estas áreas abarcan cómo se accede a los datos, junto con la privacidad de la información y los problemas de seguridad a lo largo del ciclo de vida de los datos, desde su recogida y uso hasta su almacenamiento y destrucción. Otras consideraciones son la propiedad y el uso de los datos a lo largo de su ciclo de vida.

Cuando se trata de IA, la ciberseguridad debe ser una de las principales consideraciones de los jefes de auditoría de sus equipos. A medida que el volumen y la complejidad de los datos aumentan con el uso creciente de la IA, hay que tener en cuenta también que la información que utilizan la IA y la IA generativa es tan buena como la que se les proporciona o con la que se les entrena. "Las organizaciones tendrán que saber, hasta el nivel de los puntos de datos, que la información que se introduce en el sistema es exacta y que refleja las actividades reales", afirma Wilson. "Una buena arquitectura de datos es la base de cómo los sistemas de IA interpretarán el mundo que les rodea y en el que les pedimos que actúen", afirmó.

Los controles también serán diferentes para los sistemas de IA. Cuando trabajaba para una antigua empresa, Wilson ayudó a desarrollar un sistema que unía la ciencia de datos, la automatización robótica de procesos (RPA) y la IA para desarrollar una automatización inteligente. La empresa creó un conjunto de controles para cada parte del sistema, muy similar a los controles generales de TI que siempre había utilizado. Sin embargo, al considerar que el sistema de IA objetivo sería uno que mejorara su propio rendimiento con el tiempo, el equipo de Wilson se dio cuenta rápidamente de que era necesario que hubiera controles globalizados sobre todo el sistema. Estos controles son esenciales para regular cómo interactúan los distintos componentes del sistema y qué límites se impondrían al sistema de IA en cuanto a su capacidad para modificar los algoritmos y procesos de ciencia de datos o RPA. "Necesitábamos ver de forma holística cómo el sistema, compuesto por múltiples tecnologías e integraciones, interactuaban y respondían a nuestras preguntas", afirma Wilson. No se trataba sólo de un nuevo concepto, sino de un nuevo problema que resolver. "Le dedicamos mucho tiempo porque afecta a todos los sistemas y tiene que encajar con los controles generales de TI", explicó.

En su función de auditor interno, Wilson también se pregunta a menudo por los límites de eficiencia de los sistemas de IA. "Sólo se puede dejar que el sistema sea eficiente hasta cierto punto, porque tenemos que entender lo que está haciendo y no dejar que se nos escape", dijo. Dado que limitar la eficiencia de la tecnología es un concepto nuevo, puede que sea necesario probar y equivocarse para desarrollar una nueva forma de pensar sobre la IA.

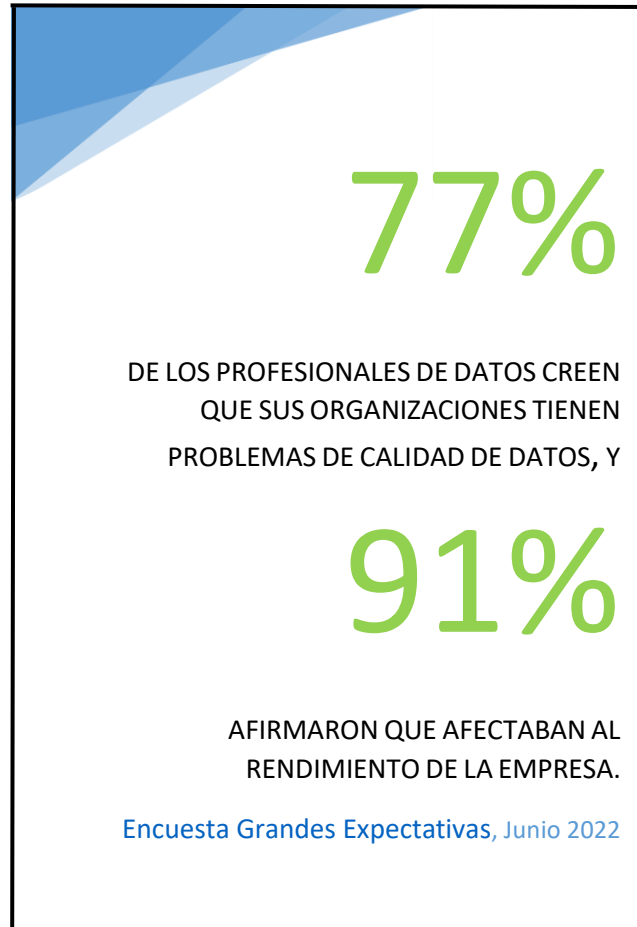


## Calidad de los datos

Teniendo esto en cuenta, está claro que, como establece el marco del IIA, la fiabilidad de los datos sobre los que se construyen los algoritmos de IA es fundamental. Por desgracia, una encuesta realizada el año pasado por la herramienta de código abierto para la calidad de datos Great Expectations reveló que el 77% de los profesionales de datos consideraban que sus organizaciones tenían problemas de calidad de datos, y el 91% afirmaba que estaban afectando al rendimiento de la empresa. Sólo el 11% afirmaba no tener problemas de calidad de datos. La empresa definió las seis dimensiones de la calidad de datos de la siguiente manera:

- Exactitud.
- Integridad.
- Unicidad.
- Coherencia.
- Puntualidad.
- Validez.<sup>18</sup>

La calidad de los datos puede verse dificultada porque los sistemas no se comunican bien entre sí o lo hagan a través de complicados complementos o personalizaciones. "La forma en que se reúnen, sintetizan y validan estos datos es crucial", señala el marco.



## Medición del rendimiento de la IA

¿Cuál es el rendimiento de los sistemas de IA? ¿Cuál es su contribución? El marco establece que, a medida que las organizaciones integran la IA en sus actividades, deben identificar métricas de rendimiento adecuadas que vinculen las actividades a los objetivos empresariales y muestren claramente si la IA está ayudando a alcanzar las metas. Al mismo tiempo, es fundamental que la dirección supervise activamente el rendimiento de sus actividades de IA.

## El factor humano

Según la paradoja de la automatización, cuanto más eficaz es un sistema automatizado, más importante es que los humanos participen en el proceso. En algunos casos, los humanos son necesarios para detectar y corregir errores cometidos por otros humanos. De hecho,

<sup>18</sup> "Data Governance vs. Data Quality: Where Do They Overlap?", Sam Bail, Great Expectations, June 10, 2022.



el 88% de los incidentes de violación de datos se debieron a errores humanos.<sup>19</sup> Los errores y sesgos humanos (tanto intencionados como no intencionados) repercutirán en el rendimiento tanto de los algoritmos como de la formación que son los motores de los sistemas de IA. El marco establece que abordar el factor humano significa:

- Supervisión y gestión del riesgo de error humano o sesgo en el sistema.
- Pruebas para garantizar que los resultados de la IA reflejan el objetivo original.
- Garantizar la suficiente transparencia en las tecnologías de IA dada la complejidad que entrañan.
- Verificar que los resultados de la IA se utilizan de forma legal, ética y responsable.

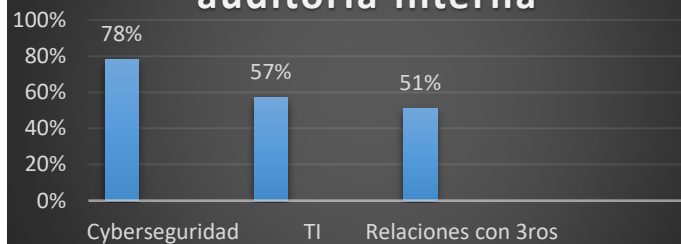
## El factor de la caja negra

El término "caja negra" suele referirse a un complicado dispositivo electrónico cuyo funcionamiento interno no es visible ni comprensible para el usuario. Anticipándose a la IA generativa y a otros sistemas avanzados, el marco señala que, a medida que las organizaciones implantan nuevas tecnologías de IA, utilizando máquinas o plataformas que pueden aprender por sí solas o comunicarse entre sí, el funcionamiento de los algoritmos se hace menos transparente o comprensible. El factor de la caja negra se convertirá en un reto cada vez mayor a medida que las actividades de IA de una organización se vuelvan más sofisticadas. Los avances en IA desde que se publicó por primera vez el marco ciertamente validan y subrayan este punto y todas las observaciones sobre los seis componentes clave.

### La tecnología sigue siendo el principal riesgo

Cuando se les preguntó qué cuestiones suponían un riesgo alto/muy alto para sus organizaciones, los líderes de auditoría interna que respondieron a la encuesta [Pulse of Internal Audit 2023 de Norteamérica](#) otorgaron los tres primeros puestos a los riesgos relacionados con la tecnología. Las elecciones de los encuestados en la encuesta Pulse fueron en gran medida consistentes entre las empresas privadas y las que cotizan en bolsa, los sectores financiero y público, así como las organizaciones sin ánimo de lucro. Es probable que el riesgo tecnológico siga siendo prioritario a medida que las herramientas y los sistemas de IA se vuelvan más complicados y polifacéticos.

### Principales riesgos citados por los responsables de auditoría interna



*Nota:* Encuesta del IIA sobre el pulso norteamericano de la auditoría interna, del 20 de octubre al 2 de diciembre de 2022. P26: ¿Cómo describiría el nivel de riesgo de su organización en las siguientes áreas de riesgo? n = 562.

<sup>19</sup> "Psychology of Human Error' Could Help Businesses Prevent Security Breaches," *CISO Magazine*, Sept. 12, 2020.



# CONSIDERACIONES ÉTICAS

## Garantizar la veracidad de los sistemas de IA

---

### La auditoría interna debe permanecer vigilante

**El marco establece que la auditoría interna debe garantizar** la organización aborda las cuestiones morales y éticas relacionadas con su uso de la IA. Algunos podrían preguntarse cómo se pueden tener en cuenta las consideraciones éticas en un sistema informático, pero la IA y la IA generativa van mucho más allá de los sistemas tecnológicos del pasado en cuanto a su alcance e impacto potencial. De hecho, la dependencia de estos sistemas puede llegar a ser tan grande que todas las operaciones de una organización se basen en las respuestas que proporcionan. Sin la formación y la supervisión adecuadas, los resultados pueden reflejar la respuesta más rápida, pero no necesariamente la más aceptable por muchas razones. Los auditores internos tendrán que preguntarse qué se ha hecho para garantizar que los sistemas de IA sigan las directrices éticas, legales y normativas adecuadas, afirma Wilson.





# EL PAPEL DE LA AUDITORÍA INTERNA

## Impulsar el valor de la IA

---

### Asumir el reto del aseguramiento

**Estas nuevas tecnologías también plantean interrogantes sobre su potencial** de poder quitar trabajo a los humanos. En opinión de Wilson, la IA no va a sustituir a los auditores internos, pero puede tener el potencial de sustituir a los que no la utilizan e impulsar su valor. Con esto en mente, insta a los auditores a conocer las tecnologías de IA existentes y emergentes. La IA ha languidecido en los perfiles de riesgo de muchas organizaciones durante un tiempo, pero muchas han pospuesto la acción por falta de comprensión o de experiencia disponible. Insta a los auditores internos a adelantarse al proceso mojándose los pies. "Demos el salto y aceptémoslo como parte de la cultura", aconseja.

Los auditores internos están bien equipados para utilizar su experiencia en la evaluación de riesgos y oportunidades que puedan afectar a la capacidad de una organización para cumplir sus objetivos. El marco cita varias actividades críticas para los auditores internos relacionadas con la IA:

- En cualquier organización, la auditoría interna debe incluir la IA en su evaluación de riesgos y considerar su inclusión en su plan de auditoría basado en riesgos. Los numerosos riesgos asociados a la IA incluyen la violación de datos, el plagio o la infracción de derechos de autor en contenidos creados por herramientas generativas de IA, y el envenenamiento de datos de modelos, en el que actores malintencionados manipulan los datos utilizados para entrenar grandes modelos lingüísticos.
- Para las organizaciones que exploran la IA, la auditoría interna debe participar desde el principio en los proyectos de IA, ofreciendo asesoramiento y conocimientos para una implementación exitosa. Tenga en cuenta que, para evitar la pérdida de independencia u objetividad, la auditoría interna no debe ser propietaria ni responsable de la implementación de procesos, políticas o procedimientos de IA.
- En las empresas que han implantado parcialmente la IA, ya sea en sus operaciones o en un producto o servicio, la auditoría interna debe garantizar cómo se gestionan los riesgos relacionados con la fiabilidad de los algoritmos subyacentes y los datos en los que se basan.
- La auditoría interna debe asegurarse de que se toman medidas para abordar las cuestiones morales y éticas que rodean el uso de la IA por parte de la organización.
- La auditoría interna también puede garantizar la existencia de estructuras de gobernanza adecuadas en relación con el uso de la IA.



# CONCLUSIÓN

---

**Al resumir el papel de la auditoría interna, el marco concluía que** "la auditoría interna debe abordar la IA como aborda todo: con métodos sistemáticos y disciplinados para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobernanza relacionados con la IA". El marco de 2017 se adelantó a su tiempo, según Wilson. Todavía se mantiene como un recurso valioso para los auditores internos que avanzan en un entorno de IA rápida y constantemente cambiante.



## PARTE III: EL PAPEL DE LA AUDITORÍA INTERNA EN LA ÉTICA DE LA IA



## Sobre los expertos

### **Andrew Clark, Ph.D., CAP, GSTAT**

Andrew es cofundador y director de tecnología de Monitaur. Es un experto de confianza en el tema de la auditoría y el aseguramiento de ML, y creó e implementó soluciones de auditoría de ML en Capital One. Ha contribuido a las normas de auditoría de LD en organizaciones como ISACA e ICO en el Reino Unido. Antes de Monitaur, Andrew también trabajó como economista y asesor de modelos para varios proyectos criptoeconómicos muy destacados mientras trabajaba en Block Science.

### **Jim Enstrom, CIA, CRISC, CISA**

Jim es vicepresidente senior y director ejecutivo de auditoría interna en Cboe Global Markets, Inc. Líder empresarial consumado, cuenta con una amplia experiencia en auditoría, cumplimiento y gestión de riesgos en áreas como la información financiera, las operaciones comerciales y la tecnología de la información. Antes de incorporarse a Cboe en 2009, Jim trabajó durante 13 años en contabilidad pública en Arthur Andersen y Deloitte.

### **Tim Lipscomb**

Tim es vicepresidente senior y director de tecnología de Cboe Global Markets, Inc. Supervisa la ingeniería de software y el control de calidad de los mercados de renta variable, opciones y futuros de Cboe, así como su negocio de soluciones de datos y acceso. Anteriormente, Tim fue director de operaciones de Cboe Europe, donde supervisó los equipos de ingeniería de software, infraestructura y operaciones de la empresa.

### **Ellen Taylor-Lubrano, Ph.D.**

Ellen es jefa de equipo de aprendizaje automático en la división de regulación de Cboe Global Markets, Inc. Se incorporó a Cboe en 2020 como fundadora del programa de ML de la división reguladora, que aplica ML/AI en la vigilancia de los mercados financieros. Antes de eso, Ellen trabajó en investigación científica fundamental y desarrollo de software de producción.



# INTRODUCCIÓN

---

**En medio de los rápidos avances de la inteligencia artificial (IA), la preocupación por la ética y las cuestiones conexas** han llevado a algunos a recomendar una interrupción o ralentización del desarrollo.<sup>20</sup> Pero a pesar de los llamamientos a una interrupción temporal, muchas organizaciones están incrementando el uso de la IA o tienen previsto hacerlo. Está claro que los auditores internos desempeñarán un importante papel de garantía y asesoramiento a medida que las organizaciones se enfrenten a las opciones de la IA y sus implicaciones.

Los informes anteriores de esta serie se han centrado en lo que los auditores internos deben entender sobre la IA y han vuelto a examinar una publicación de referencia sobre el tema, *Artificial Intelligence - Considerations for the Profession of Internal Auditing*, del Instituto de Auditores Internos (IIA). Aunque se publicó en 2017, este marco en general sigue siendo relevante y útil en la mayoría de las áreas de auditoría interna. "La auditoría interna puede ayudar a una organización a evaluar, comprender y comunicar el grado en que la inteligencia artificial tendrá un efecto (negativo o positivo) en la capacidad de la organización para crear valor a corto, medio o largo plazo", según el marco.<sup>21</sup>

Este tercer y último informe de la serie sobre IA aborda las cuestiones éticas que rodean a esta tecnología polifacética y lo que estas cuestiones significan para las organizaciones y los auditores internos. También incluye recomendaciones y opiniones de directivos y auditores internos que ya trabajan en primera línea en el uso de la IA.

---

<sup>20</sup> <https://futureoflife.org/open-letter/pause-giant-ai-experiments/>

<sup>21</sup> [Artificial Intelligence - Considerations for the Profession of Internal Auditing, Special Edition](#), The Institute of Internal Auditors, 2017.

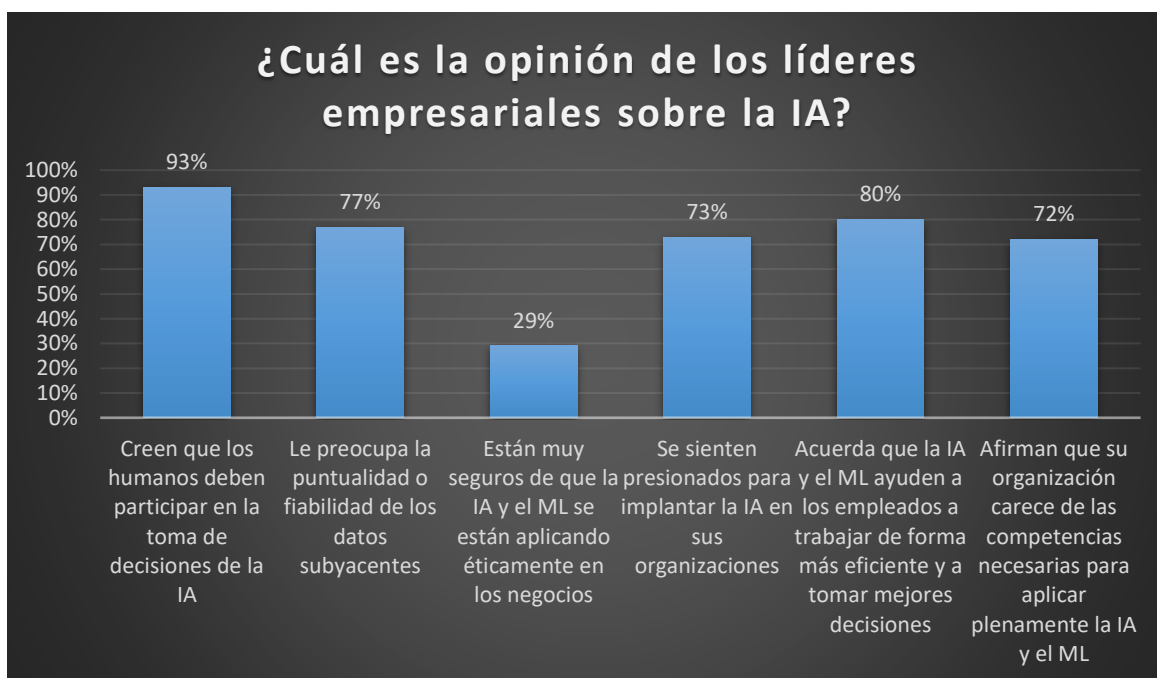


# Riesgos y oportunidades

## La función asesora de la Auditoría Interna

### El entusiasmo por la IA podría eclipsar las consideraciones éticas

El mercado mundial de la IA artificial se valoró en 136.550 millones de dólares el año pasado y se espera que crezca a una tasa anual compuesta del 37% de 2023 a 2030, según Grand View Research, Inc.<sup>22</sup> Esta oleada de interés, así como el entusiasmo y la expectativa que suscitan tecnologías como la IA generativa, han impulsado a muchos desarrolladores de software y organizaciones a precipitarse en sus investigaciones o esfuerzos en materia de IA. Sin embargo, en medio de los rápidos avances, es posible que se pasen por alto muchos riesgos graves e inconfundibles, incluidas cuestiones éticas y de rendimiento. Los auditores internos están bien posicionados para alertar a sus organizaciones sobre estos problemas y ofrecer asesoramiento sobre la eficacia de los controles actuales y la necesidad de mejorar los controles o las barreras de seguridad. De hecho, la Partnership on IA, liderada por ejecutivos de Google, publicó un documento en el que se pide que la auditoría interna desempeñe un papel destacado a la hora de garantizar los procesos de creación y despliegue de la IA y asegurar que cumplen las expectativas y normas éticas.<sup>23</sup>



Fuente: [Encuesta Workday](#), Junio 2023.

<sup>22</sup> [Artificial Intelligence Market Size, Share & Trends Analysis Report By Solution, By Technology \(Deep Learning, Machine Learning\), By End-use, By Region, And Segment Forecasts, 2023 – 2030](#), Grand View Research, Inc., June 2023.

<sup>23</sup> ["Closing the AI Accountability Gap: Defining an End-to-End Framework for Internal Algorithmic Auditing,"](#) The Partnership on AI, January 2020.



Teniendo esto en cuenta, es importante que las organizaciones y los auditores internos comprendan los riesgos y las limitaciones de la IA, y el impacto que pueden tener en el uso de la IA por parte de una empresa. “Existe la idea errónea de que la IA es realmente inteligente”, afirma Andrew Clark, cofundador y director técnico de Monitaur, una empresa de software de gobernanza de IA. Por desgracia, la IA generativa, que está recibiendo gran parte de la atención actual de los medios de comunicación y las organizaciones, es tan inteligente como los datos con los que se ha entrenado y, al menos en las primeras etapas de la tecnología, ese entrenamiento puede incluir publicaciones aleatorias en redes sociales, contenido web y otro material que no ha sido autenticado.

El uso de programas públicos de IA generativa puede exponer datos privados o confidenciales de empresas, clientes o socios comerciales. Y como la IA generativa es tan fácil de usar, estas capacidades están al alcance de todos, desde ciberdelincuentes veteranos hasta hackers aficionados. Aunque los esfuerzos de ciberseguridad pueden mitigar algunos de los daños potenciales que pueden causar, la concienciación del elevado riesgo, desde el nivel organizativo hasta el empleado individual, es esencial para una ciberseguridad adecuada.

La IA generativa también puede incorporar sesgos intencionados o inconscientes. Cuando una organización reguladora trabaja para identificar actividades problemáticas, por ejemplo, existen consideraciones éticas y legales sobre si los enfoques de datos que se utilizan podrían estar sesgados en contra de ciertos miembros o tipos de actividad comercial, señaló Ellen Taylor-Lubrano, jefe del equipo de aprendizaje automático--regulatorio, Cboe Global Markets. En otro orden de cosas, los investigadores han detectado elevados porcentajes de error en el uso de sistemas de reconocimiento facial por IA para identificar a personas de color, mujeres y jóvenes, lo que aumenta las probabilidades de que se produzcan identificaciones erróneas y de que las personas sean acusadas injustamente de delitos. La IA también puede estar sujeta a lagunas de conocimiento e imprecisiones. Por ejemplo, aunque los sistemas de IA pueden ser entrenados para detectar enfermedades, es posible que no reconozcan una enfermedad como el melanoma en alguien con características de la piel que no estaban incluidas en su conjunto de datos original.<sup>24</sup>

Los modelos actuales de IA generativa tampoco son transparentes en cuanto a sus fuentes, por lo que, sin conocer los orígenes de la información que generan, los usuarios pueden exponerse a riesgos legales, de derechos de autor y de propiedad intelectual. Y lo que es igualmente alarmante, puede producir "hechos" que el sistema se ha inventado (lo que se conoce como alucinaciones) al intentar responder a una pregunta. La IA generativa "está pensada para imitar a un ser humano, no para ser correcta", afirma Clark. Los auditores internos pueden asesorar a las organizaciones sobre la mejor manera de abordar estos errores u omisiones o sus consecuencias imprevistas.

La facilidad de uso de la IA generativa puede ser otro riesgo para las organizaciones. En el pasado, los modelos solían ser creados por personas con titulaciones superiores o conocimientos de sistemas que tenían experiencia en la automatización de esos modelos, explica Clark. Hoy en día, es posible que personas con poco o ningún conocimiento de los modelos, los sistemas o los datos que están utilizando aprovechen una herramienta como la IA generativa y le pidan que haga una predicción o tome una decisión utilizando información que puede estar incompleta o carecer del contexto adecuado”.

Además de vigilar los posibles problemas derivados del uso interno de la IA, las organizaciones también deben tener en cuenta las amenazas externas. Los mismos modelos que subyacen a tecnologías como ChatGPT pueden utilizarse para crear herramientas capaces de producir software y códigos maliciosos, páginas de estafas y correos electrónicos de phishing. También pueden utilizarse para identificar vulnerabilidades organizativas, así como para entrenar nuevos tipos de herramientas de ciberdelincuencia, entre otras funciones.<sup>25</sup> Además, la IA podría facilitar a los piratas informáticos el desarrollo de programas maliciosos capaces de robar datos o ejercer control sobre ellos.

Aunque estas amenazas puedan parecer desalentadoras, no adoptar la IA también entraña riesgos. Si otros se adelantan en el uso de la IA, una organización puede ser percibida como menos orientada a la tecnología o al futuro por sus clientes o talentos actuales o

---

<sup>24</sup> [“Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification,”](#) Joy Buolamwini and Timnit Gebru, *Conference on Fairness, Accountability and Transparency*, 2018.

<sup>25</sup> [“Surge in Generative AI Tools for Cybercrime Sparks Concerns,”](#) GRC Report, August 10, 2023.



potenciales, lo que daría ventaja a sus competidores. La IA también ofrece beneficios tangibles que pueden permitir a las empresas agilizar y mejorar los procesos, impulsando así la productividad, mejorando el servicio al cliente, minimizando los costes y abriendo potencialmente nuevas oportunidades de servicio, mercado o producto. Además, en muchas situaciones la IA puede ayudar a las organizaciones a identificar riesgos o amenazas o a detectar nuevas oportunidades. La IA puede ofrecer a las organizaciones acceso a una enorme base de conocimientos internos de forma más rápida y eficiente de lo que lo haría una búsqueda directa, según Tim Lipscomb, vicepresidente senior y director de tecnología de Cboe Global Markets. Si una organización utiliza un proceso manual de recopilación de información, es posible que no pueda tomar las mejores decisiones ni responder a las amenazas u oportunidades como lo haría si utilizara la IA.





# Volver a Conceptos fundamentales de auditoría

## Adaptación de tres líneas y otros modelos existentes

---

### Utilización de enfoques de garantía fundamentales para la nueva tecnología

**Aunque una tecnología sea nueva, muchos de los detalles de su aplicación pueden no serlo.** Por ejemplo, los modelos de decisión y el aprendizaje automático se utilizan desde hace tiempo en el sector financiero, señaló Jim Enstrom, vicepresidente senior y director ejecutivo de auditoría de Cboe Global Markets. (Ver el recuadro "Cuidar la gestión del riesgo de modelo" en la página 7.) Los auditores de TI han tenido que abordar una miríada de riesgos, incluidos los usos éticos en el pasado, y la IA no es diferente en este sentido. Por lo tanto, es fundamental garantizar que la auditoría interna tenga un lugar en la mesa para comprender el uso estratégico de la IA dentro de la organización.

Si vemos los sistemas de IA a través de la lente de los procesos de desarrollo de software, los auditores internos pueden volver a conceptos fundamentales, dijo Enstrom. La trazabilidad, por ejemplo, debe tenerse en cuenta si el sistema de IA tomará decisiones o funcionará de forma autónoma, mientras que la auditabilidad también será clave. Al igual que los auditores internos trabajan con los equipos de sus organizaciones para comprender su trabajo, el equipo de auditoría interna también tendrá que trabajar con ingenieros, científicos de datos y programadores para comprender lo que hacen los sistemas, las fuentes de datos utilizadas como entradas, qué requisitos se utilizaron para construir el modelo y qué artefactos pueden utilizarse para defender las decisiones que toma el modelo. "Tenemos que pensar en nuevas ideas para auditar la IA, impulsadas por enfoques ágiles e iterativos, y trabajar en colaboración con la primera y la segunda línea. Sin embargo, también tenemos una clara oportunidad de aprovechar las herramientas, metodologías y enfoques existentes como punto de partida", afirmó.

Taylor-Lubrano señala que, dado que las organizaciones llevan mucho tiempo utilizando modelos estadísticos, pueden considerar el aprendizaje automático y otros ejemplos de IA como una nueva versión de esos modelos. Si los enfoques de las cuestiones éticas u otros riesgos que se utilizaban en el pasado ya no son adecuados, las organizaciones tendrán que replantearse sus enfoques. "Tenemos una buena oportunidad para añadir la ética al debate ahora que la IA ha puesto el foco en ella", añadió Enstrom.

Esto incluye aplicar los criterios de revisión existentes a los sistemas de IA. Dado que su organización utiliza actualmente la IA como tecnología de asistencia, con seres humanos que revisan los resultados, "estamos tratando a la IA básicamente como a un proveedor", afirma Lipscomb. Llevamos a cabo los procesos adecuados de incorporación de proveedores y las estructuras de control correspondientes, y luego esperamos una revisión de tercera línea del proceso."

#### **El modelo de las tres líneas**

Según el modelo de las tres líneas del IIA <sup>26</sup>, la gestión eficaz del riesgo empieza en la cúspide, con la dirección, como primera línea, como propietaria del riesgo y aclara aún más las funciones, incluidas las del consejo de administración. Este marco de gobernanza puede servir como herramienta para ayudar a una empresa a

---

<sup>26</sup> [The IIA's Three Lines Model: An Update of the Three Lines of Defense](#), The Institute of Internal Auditors, 2020.



considerar cómo navegar por las oportunidades y los riesgos que presenta la IA. "Lo utilizamos como parte de nuestro marco de gobernanza", afirma Enstrom. Entre otras cosas, puede ayudar a comprender las funciones y responsabilidades de AI, incluida la supervisión del consejo. Como tercera línea independiente y objetiva, la auditoría interna informa al comité de auditoría, pero también puede ofrecer su punto de vista al consejo en pleno sobre cuestiones éticas y de otro tipo. También puede asesorar sobre cómo los cambios impulsados por la IA pueden alterar el perfil de riesgo de la organización.

El modelo de las tres líneas también puede ayudar a las organizaciones a reconocer la necesidad de que cada línea evalúe y controle el riesgo dentro de su propio ámbito, señaló Enstrom. Si la IA se utiliza de forma autónoma, sin una revisión humana rigurosa de sus resultados o de la toma de decisiones, el riesgo puede ser alto, lo que significa que la dirección debe implantar procedimientos de garantía de calidad mejorados u otros controles en la primera línea. En cuanto a la segunda línea, los directores de riesgos o de cumplimiento pueden tener que determinar la mejor manera de establecer una garantía y un control adecuados, lo que también sería una consideración para la función de garantía de la auditoría interna, como tercera línea. A la luz de cualquier nuevo cambio, la auditoría interna también podría plantear preguntas sobre cómo se está implantando la tecnología autónoma, si es una prioridad en la agenda del consejo y cómo puede gestionarse en el futuro.

La conclusión es que no importa cuántos cambios pueda impulsar la IA, "tenemos la oportunidad de añadir valor posicionando la auditoría interna como un elemento clave del marco de gobernanza de la IA, aprovechando nuestros conocimientos y experiencia en torno a los controles, y lo que sabemos como profesión; todo esto se traslada al futuro", dijo Enstrom.

## Gestión del riesgo de modelo

La gestión del riesgo de modelo aborda los riesgos que pueden derivarse cuando se toman decisiones utilizando modelos incorrectos o mal empleados. El objetivo de la gestión del riesgo de modelo es identificar, medir y mitigar o prevenir el uso de datos, hipótesis, metodologías, procesos o interpretaciones inexactos. El sector bancario tiene paradigmas de gestión del riesgo de modelo bien establecidos que se utilizan para supervisar los modelos de crédito, finanzas y actividades de comercialización, señaló Clark. (Véase [OCC 2011-12, Supervisory Guidance on Model Risk Management](#), de la Oficina del Interventor de la Moneda.) Como se señala en un manual de la Oficina del Contralor sobre el tema, "una buena gobernanza del modelo incluye la supervisión del consejo de administración y de la dirección, políticas y procedimientos, un sistema de controles internos, auditoría interna, un inventario del modelo y documentación."<sup>27</sup> Las organizaciones pueden aprovechar estas recomendaciones dirigidas al sector bancario, aconsejó Clark, y evitar tener que construir desde cero sus propios sistemas de gestión de modelos de riesgo. La gestión eficaz del riesgo de modelo es un factor para acelerar la adopción de la IA y el aprendizaje automático, "creando confianza y responsabilidad entre las partes interesadas mediante una gobernanza y una gestión del riesgo adecuadas", según EY.<sup>28</sup>

---

<sup>27</sup> [Safety and Soundness: Model Risk Management, Version 1.0, Comptroller's Handbook](#), Office of the Comptroller of the Currency, August 2021.

<sup>28</sup> ["Understand Model Risk Management for AI and Machine Learning."](#) Gagan Agarwala, et al., May 13, 2020, EY.



# Uso de la IA en la auditoría interna

## Mejorar la garantía de eficacia con las nuevas tecnologías

### Entendiendo sobre la privacidad y la responsabilidad de la IA

Además de comprender las implicaciones de la IA para sus organizaciones, los auditores internos también tendrán que estudiar la mejor manera de utilizar la IA generativa y otras herramientas en sus propias auditorías, y qué tipo de riesgos para la privacidad deben tener en cuenta. Por ejemplo, al trabajar con IA generativa, "es esencial garantizar que los datos introducidos en ChatGPT sean anónimos y que la información sensible no se comparta ni almacene en la plataforma", según un artículo de [Internal Auditor](#)<sup>29</sup>. "Además, los auditores internos deben asegurarse de que cuentan con el consentimiento y la autorización adecuados para utilizar los datos en ChatGPT." El artículo detalla cómo los auditores internos pueden utilizar la IA en la planificación, las pruebas, la elaboración de informes y la supervisión, y subraya la importancia de aprovechar las capacidades de herramientas como ChatGPT al tiempo que se protege la confidencialidad y la privacidad de los datos sensibles.

#### **Preguntas clave a considerar**

Clark recomienda que las organizaciones desarrollen una comprensión estratégica de lo que la IA significa o puede significar para ellas. La auditoría interna puede recomendar que las organizaciones aborden cuestiones como:

- ¿Dónde y cómo se utiliza la IA?
- ¿Qué intenta modelar la empresa? ¿Cuál es el objetivo de ese modelo?
- ¿Existen soluciones distintas de las herramientas de aprendizaje automático que puedan ayudarnos a alcanzar nuestros objetivos?
- ¿Qué riesgos implica?
- ¿Cómo automatiza o debería automatizar la organización la toma de decisiones con modelos?
- ¿Existen controles adecuados de supervisión y gestión de riesgos en torno a la IA?
- ¿Existe una función de segunda línea dedicada a la gestión del riesgo de modelo? En caso afirmativo, ¿existen sistemas de gestión del riesgo de modelo que puedan utilizarse con herramientas de IA?
- ¿Cómo afecta la IA al alcance y al proceso de auditoría?

Las organizaciones deben asegurarse de abordar las cuestiones éticas si se utiliza un algoritmo en un proceso que toma decisiones importantes sobre las personas. En tal caso, deben preguntarse:

- ¿Existen protecciones o leyes en vigor? En caso afirmativo, ¿cómo puede garantizar la organización que se cumplen los procesos que utilizan IA?
- Si no hay consideraciones de cumplimiento externas, ¿aun así hay pasos que deben seguirse para garantizar que la empresa está haciendo lo correcto, de acuerdo con sus propios valores?

<sup>29</sup> "On the Frontlines: AI in IA," Alex Rusate, *Internal Auditor*, May 17, 2023.



La auditoría interna puede tratar estas consideraciones con el mismo cuidado que los mandatos externos, asegurándose de que existe un proceso para supervisar y validar el cumplimiento e informar sobre los problemas de cumplimiento relacionados.

La auditoría interna puede tratar estas consideraciones con el mismo cuidado que los mandatos externos, asegurándose de que existe un proceso para supervisar y validar el cumplimiento e informar sobre los problemas de cumplimiento relacionados.



# Conclusión

---

**Debido a las importantes cuestiones éticas relacionadas con la IA,** Clark aconseja que las organizaciones que no confíen en los resultados que puedan producir los sistemas den un paso atrás antes de implantarlos. En su lugar, recomienda abordar la IA inicialmente como un proyecto de investigación y desarrollo (I+D), dando a la empresa la oportunidad de explorar cómo la tecnología se adapta a sus necesidades e identificar los riesgos potenciales.

La transformación digital es apasionante, pero los auditores internos deben mantener una visión clara de los riesgos y limitaciones de cualquier tecnología y centrarse en proporcionar asesoramiento y garantías pertinentes. En medio de la exageración que rodea a cualquier nueva tecnología, "tenemos que ser nosotros los que nos preguntemos qué problemas empresariales resolverá realmente y qué problemas de privacidad de datos y otros riesgos puede conllevar", afirma Clark.



## Acerca del IIA

El Instituto de Auditores Internos (IIA) es una asociación profesional internacional sin ánimo de lucro que cuenta con más de 235.000 miembros en todo el mundo y ha concedido más de 190.000 certificaciones de Auditor Interno Certificado (CIA) en todo el mundo. Fundado en 1941, el IIA es reconocido en todo el mundo como el líder de la profesión de auditoría interna en normas, certificaciones, educación, investigación y orientación técnica. Para más información, visite [theiia.org](https://theiia.org).

## Disclaimer

En la Parte III: El papel de la auditoría interna en la ética de la IA, los puntos de vista y opiniones expresados son ofrecidos por los expertos a título personal y no reflejan los puntos de vista y opiniones de Cboe Global Markets, Inc. y sus filiales.

El IIA publica este documento únicamente con fines informativos y educativos. Este material no pretende ofrecer respuestas definitivas a circunstancias individuales específicas y, como tal, sólo está destinado a ser utilizado como liderazgo de pensamiento informado por pares. No constituye una guía formal del IIA. El IIA recomienda buscar asesoramiento experto independiente en relación directa con cualquier situación específica. El IIA no acepta ninguna responsabilidad por cualquier persona que confíe exclusivamente en este material.

Los Resúmenes de Conocimientos Globales pretenden abordar temas que son oportunos y relevantes para una audiencia global de auditoría interna, y cada tema cubierto es revisado por miembros del Comité Asesor de Contenido Norteamericano voluntario del IIA. Los expertos en la materia se identifican y seleccionan principalmente a partir de la lista de colaboradores de Global Guidance del IIA.

Para solicitar su inclusión en la lista de colaboradores de Global Guidance, envíe un correo electrónico a [Standards@theiia.org](mailto:Standards@theiia.org). Para sugerir temas para futuras Síntesis de Conocimiento Global, envíe un correo electrónico a [Content@theiia.org](mailto:Content@theiia.org).

## Copyright

Copyright © 2023 The Institute of Internal Auditors, Inc. Todos los derechos reservados. Para obtener permiso de reproducción, póngase en contacto con [copyright@theiia.org](mailto:copyright@theiia.org).

Noviembre 2023

Traductora: Andrea Correa (servicios contratados), revisor: Roberto Loo, control de calidad

Traducción al Español Auspiciada por:



The Institute of  
Internal Auditors

### Global Headquarters

The Institute of Internal Auditors  
1035 Greenwood Blvd., Suite 401  
Lake Mary, FL 32746, USA  
Phone: +1-407-937-1111  
Fax: +1-407-937-1101