MARCO DE AUDITORÍA DE Inteligencia Artificial

Del IIA

The Institute of Internal Auditors

Tabla de Contenidos

Introducción

Inteligencia Artificial (IA) es un término amplio que ha crecido hasta abarcar una amplia gama de tecnologías existentes y emergentes. Si bien no existe una definición única para el término, IA generalmente se refiere a "sistemas dotados de procesos intelectuales característicos de los humanos, como la capacidad de razonar, interpretar significado, contextualizar o aprender de experiencias pasadas".[1] El auge actual de las aplicaciones de IA demuestra formas aparentemente infinitas en las que las organizaciones pueden aprovechar las tecnologías impulsadas por la IA para mejorar la forma en que trabajamos, al tiempo que plantean riesgos diversos y significativos que son inherentes, dada la naturaleza de la tecnología.

La IA puede ser un tema intimidante para un auditor interno, especialmente a medida que la adopción y el uso de la IA en las organizaciones continúan creciendo. Ahora, más que nunca, las organizaciones buscan en la auditoria interna una mayor orientación sobre la IA. Ya sea asesorando sobre riesgos y controles relacionados con la IA, o asegurando procesos que utilizan o dependen de la IA, por lo que es crucial que los auditores internos desarrollen sus conocimientos sobre esta temática.

Se espera que los auditores internos proporcionen aseguramiento respecto a procesos que pueden variar desde simples transacciones comerciales hasta procedimientos altamente complejos que requieren una comprensión profunda. El alcance y la profundidad de los conocimientos sobre IA necesarios para respaldar las actividades de aseguramiento crean desafíos continuos para los auditores internos, quienes deben desarrollar continuamente sus conocimientos sobre IA para comprender plenamente sus riesgos y desempeñarse de manera efectiva al brindar asesoramiento y aseguramiento.

La IA presenta desafíos únicos para la auditoría interna, y su evolución, significa que los auditores internos deben reevaluar los riegos en los entornos de IA y su mitigación.

Dicho esto, los auditores internos ya poseen conocimientos fundamentales, como pensamiento crítico, capacidad para mapear procesos, evaluar riesgos, evaluar controles de tecnología de la información, comprender estrategias organizacionales y brindar aseguramiento independiente a la función de gobernanza.

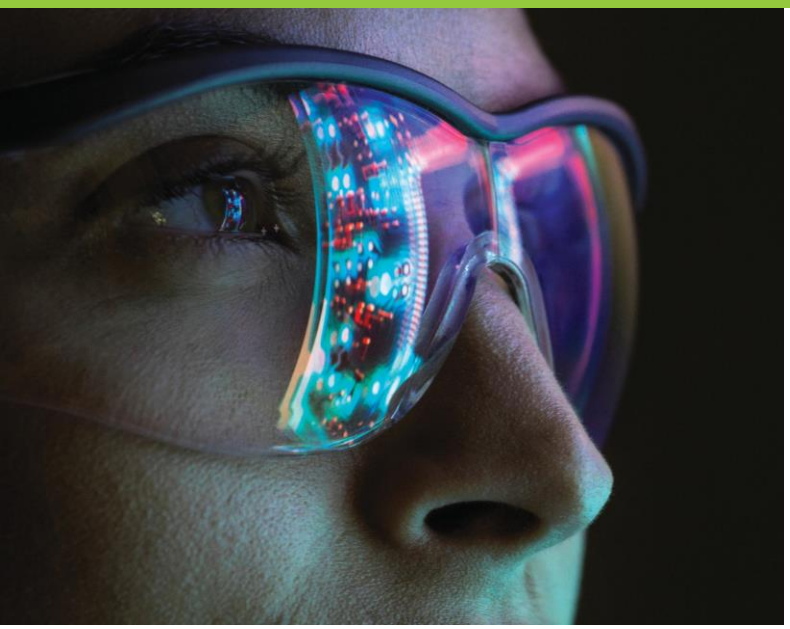
La intención al presentar el Marco de Auditoría de IA del Instituto de Auditores Internos (IIA) es ayudar a los auditores internos a comprender el riesgo e identificar las mejores prácticas y controles internos relacionados al uso de IA, y ayudará a los auditores internos a desarrollar conocimientos básicos sobre la temática. El marco se presenta en cuatro partes:

1. ***Descripción General – Historia y usos de la IA.***
2. ***Primeros Pasos – Comprender cómo se utiliza la IA en las organizaciones.***
3. ***Marco de Auditoría de IA – Gobernanza, Gestión y Auditoría Interna.***
4. ***Guía y glosario para profesionales.***

Este marco, que aprovecha aspectos del Modelo de Tres Líneas del IIA[2], incluirá referencias al Marco Internacional para la Práctica Profesional (IPPF) del IIA, que proporciona una base de requisitos obligatorios y principios rectores para la profesión de auditoría interna. Deben revisarse los estándares aplicables para obtener información adicional. Las guías relacionadas del IIA, como las Guías de Auditoría de Tecnología Global (GTAGs), se mencionan para proporcionar contenido específico sobre el tema. Otros marcos relevantes, como el Marco de Gestión de Riesgos de Inteligencia Artificial (AI RMF 1.0) del NIST, se enumeran como recursos adicionales para los profesionales de auditoría interna.

PARTE 1

Descripción General



Historia y Evolución

Como un abordaje general del tema, es importante que los auditores internos comprendan el desarrollo histórico de la IA, la forma en que la IA se utiliza actualmente en diversas industrias y las tendencias emergentes de IA que los auditores internos deben considerar.

La idea de aplicaciones de la IA se remonta a 1950, cuando el matemático británico Alan Turing planteó la pregunta "¿Las máquinas pueden pensar?" en su artículo "Computing Machines and Intelligence."[3] Se le considera uno de los fundadores de la IA al sugerir que las máquinas eventualmente serían capaces de tener una inteligencia similar a la humana. Dos años más tarde, Arthur Lee Samuel, un informático estadounidense de IBM, desarrolló un programa que podía jugar a las damas utilizando valores programados para identificar el mejor movimiento[4]. El proyecto The Darthmouth Summer Research on Artificial Intelligence en 1956 presentó uno de los primeros usos del término IA, atribuido a John McCarthy, un científico cognitivo e informático estadounidense[5].

La década de 1960 presentó grandes avances en IA, incluido el uso de la robótica, programas de resolución de problemas y el primer programa informático interactivo (también conocido como programa de comprensión del lenguaje natural o PNL) llamado ELIZA, desarrollado por Joseph Weizenbaum, de origen germano-estadounidense, informático y profesor. ELIZA podría considerarse el primer "chatbot", diseñado para simular una conversación con humanos[6].

El Desarrollo de la IA en la década de 1970, incluyó el primer robot inteligente llamado WABOT, desarrollado por la Facultad de Ciencias e Ingeniería de la Universidad de Waseda en Tokio, así como el trabajo en PNL del científico informático indio-estadounidense Raj Reddy[7,8].

Los avances en la década de 1980 incluyeron el desarrollo de una camioneta Mercedes Benz sin conductor en 1986 bajo la supervisión de Ernst Fickmanns, líder alemán en tecnología de conducción autónoma[9].

La década de 1990 tuvo avances en las tecnologías relacionadas con la IA, incluido el software de reconocimiento de voz en Windows, propiedad de Microsoft. Asimismo, IBM desarrolló una IA altamente efectiva como "Deep Blue", que fue noticia en 1997 cuando derrotó al gran maestro de ajedrez Garry Kasparov[10].

En la década de 2000, la IA se había convertido en parte de nuestra vida diaria, incluidas aplicaciones como Alexa de Amazon, Siri de Apple y Google Assistant. El año 2023 marcó un aumento en la adopción de grandes modelos de lenguaje de gran tamaño (LLMs) como ChatGPT, que han elevado aún más las capacidades de la IA, pasando de simplemente predecir resultados a una variedad de creaciones de contenido.

Niveles de adopción

De acuerdo con el Índice global de adopción de IA de IBM en 2022, el 35% de las empresas encuestadas informaron que utilizan IA en sus negocios, y un 42% adicional, informó que están explorando la IA[11]. La continua expansión de la IA refuerza el hecho de que los auditores internos deben asegurarse de incorporar los riesgos relacionados con la IA en la planificación de sus auditorías. Además, los auditores internos deben desarrollar continuamente su conocimiento sobre la IA. La Parte 2, Primeros Pasos, profundizará en las consideraciones que un auditor interno puede tomar en cuenta para identificar el uso de IA dentro de sus organizaciones.

Así como el entorno de la IA continúa evolucionando, también lo hace las formas en que se categoriza la IA. Si bien, existen diferentes perspectivas sobre cómo agrupar las diversas formas de IA, la siguiente sección proporciona un resumen de tipos comunes de IA actualmente en uso (Máquina Reactiva y Memoria Limitada), o que son estrictamente teóricas (Teoría de la Mente y Autoconciencia).

Desde el punto de vista de la funcionalidad, IBM[12] clasifica la IA en cuatro tipos:

1. ***IA de Máquina Reactiva***
2. ***IA de Memoria Limitada***
3. ***IA de Teoría de la Mente***
4. ***IA Autoconsciente***

EJEMPLOS:

- Deep Blue de IBM.
- Algunas aplicaciones de aprendizaje automático se clasifican como IA de máquina reactiva. El aprendizaje automático a menudo se basa en modelos estadísticos que analizan datos y producen resultados predictivos a partir de los datos de entrada. Por ejemplo, una tienda minorista en línea podría utilizar IA en su aplicación móvil o sitio web para sugerir productos basándose en el historial de compras del consumidor. El historial de compras del usuario individual es el conjunto de datos que impulsa el resultado y que se adapta a ese cliente.

Uso de la IA

- **Encuesta de Negocios sobre IA 2022 de PwC (EE.UU.) — El 74% de los encuestados líderes en tecnología utilizan IA en la toma de decisiones, el 62% de los líderes en operaciones y mantenimiento, el 61% de los líderes en experiencia del cliente y el 60% de los líderes en estrategia.**
- **Encuesta Global de Perspectivas de CEO 2023 de EY — El 99% de los CEOs encuestados están realizando o planeando inversiones significativas en IA generativa.**
- **Informe sobre el Estado de la IA 2023 de McKinsey — El 79% de todos los encuestados globales reportan alguna exposición a la IA generativa y el 22% dijo que la está utilizando regularmente.**

1 . IA de Máquina Reactiva

- La IA reactiva es un tipo de IA sin memoria que está diseñada para realizar tareas basadas únicamente en entradas o entrenamiento realizado por humanos. A veces denominada IA Estrecha o Débil, estos sistemas dependen del "Humano en el circuito" ("Human in the loop") para la codificación generada por humanos que indica a la máquina cómo operar por sí sola. Esta programación, que se conoce comúnmente como "algoritmo", consiste en un conjunto de cálculos que incluyen aspectos tanto de informática como de matemáticas o estadística.

2 . IA de Memoria Limitada

- La IA de Memoria Limitada depende menos de la interacción humana para producir resultados, lo que le otorga la capacidad única de aprender y mejorar basándose en el entrenamiento a partir de conjuntos de datos más grandes. Mientras que la IA de Máquina Reactiva sólo puede utilizar datos disponibles actuales, la IA de Memoria Limitada puede incorporar datos pasados y presentes para mejorar el rendimiento.

- Otros ejemplos de aprendizaje automático acceden a conjuntos de datos más grandes y realizan análisis más complejos. Esto se conoce como "Aprendizaje Profundo" ("Deep

Learning"), que es un subconjunto tanto, del aprendizaje automático, como de la IA de Memoria Limitada. Se diferencia por depender menos de la interacción humana para producir resultados. La IA generativa está dentro de esta categoría, y se puede utilizar para crear contenido basado en algoritmos programados.

EJEMPLOS DE IA GENERATIVA INCLUYEN:

- ChatGPT, LLaMA, y Bard son ejemplos de chatbots basados en Modelos de Lenguaje de Gran Tamaño (LLM por sus siglas en inglés), que dependen del aprendizaje profundo y pueden producir contenido de texto, mientras que otras formas de IA generativa pueden producir otro tipo de contenido como música (MusicLM), arte (DALL-E) e incluso códigos informáticos (OpenAI Codex).

- Los Chatbots y los asistentes virtuales son una forma comúnmente utilizada de IA de Memoria Limitada que utiliza el procesamiento del lenguaje natural (PNL) y el aprendizaje por refuerzo para entablar conversaciones similares a las humanas con los usuarios finales. Estas herramientas suelen ser utilizadas por organizaciones como instituciones financieras, que permiten al usuario solucionar diversos problemas, incluso fuera del horario comercial.

Además, el aprendizaje automático, a menudo se subdivide en cuatro categorías:[13]

1. ***Aprendizaje Supervisado*** – El aprendizaje pasado se aplica a datos estructurados con resultados predeterminados.
2. ***Aprendizaje No Supervisado*** – No hay resultados "correctos" predeterminados; en su lugar, busca patrones en datos no estructurados.
3. ***Aprendizaje Semi-Supervisado*** – Contiene elementos tanto del aprendizaje supervisado como del no supervisado.
4. ***Aprendizaje por Refuerzo*** – Programación dinámica donde los algoritmos se entrenan a través de un sistema de recompensas y castigos; aprende sin interacción humana.

Otros Tipos de IA:

Sistemas Expertos simulan el juicio o comportamiento humano. Incorporan el conocimiento de múltiples personas en la resolución de problemas y, en teoría, proporcionan soluciones más efectivas. Los Sistemas Expertos se utilizan en la investigación química para analizar y predecir la estructura molecular y en medicina para identificar bacterias dañinas.

La **tecnología de visión por computadora, combinada con el Aprendizaje Profundo**, permite a las máquinas analizar imágenes. Actualmente se utiliza en el cuidado de la salud para detectar y diagnosticar anomalías en los pacientes basándose en radiografías, resonancias magnéticas o tomografías computarizadas. El reconocimiento facial es otra forma de visión por computadora, con una alta variedad de usos, incluyendo la autenticación al intentar acceder a una cuenta bancaria o restringir el acceso físico a edificios que albergan datos sensibles.

Aunque la **robótica y la IA** son campos distintos, a menudo se combinan para crear herramientas emergentes que pueden usarse en el mundo real. Por ejemplo, los robots que utilizan sensores visuales y procesamiento de imágenes emplean IA para aprender a navegar por su entorno. La manufactura, la agricultura y los bienes de consumo empaquetados son industrias que también dependen de la robótica combinada con IA de Memoria Limitada para aumentar la eficiencia y la productividad en sus operaciones. El uso de cirugías asistidas por robots e IA en la industria de la salud promueve una mayor precisión, lo que puede resultar en una recuperación más rápida para los pacientes.

3 . IA de Teoría de la Mente

Aunque la IA de Teoría de la Mente no está desarrollada hoy en día, la investigación actual busca desarrollar sistemas de IA que comprendan e interactúen con factores como emociones y motivaciones de manera similar a los humanos. El trabajo en esta área incluye esfuerzos para desarrollar sistemas que puedan analizar y

relacionarse con los humanos basándose en la entrada de sus voces, expresiones faciales y sentimientos en tiempo real y responder de manera similar a los humanos.

4 . IA Autoconsciente

La IA Autoconsciente, al igual que la IA de Teoría de la Mente, es actualmente teórica y no existe en la práctica. Relacionada con las recientes conversaciones sobre la posibilidad de la "IA General Artificial" (AGI por sus siglas en inglés), esta versión hipotética de la IA sería única y autoconsciente con lo que muchos imaginan como una profunda conciencia interna que iguala o supera lo que los humanos son capaces de tener. Aunque es un punto de conversación popular en los últimos meses, sigue habiendo debate sobre la viabilidad de este nivel de funcionalidad de la IA.

PARTE 2

Primeros Pasos

A medida que las organizaciones continúan implementando la IA de diversas formas, los auditores internos deben ser proactivos y colaborar estrechamente con la administración para comprender la estrategia de la organización respecto a la IA, su uso actual y que planes a futuro existen al respecto. Especialmente, durante el proceso de planificación los auditores internos deben investigar y recopilar información relevante sobre el uso potencial de IA mediante la revisión de múltiples fuentes internas y externas.

Información interna relevante puede incluir:

- Las políticas y procedimientos que hacen referencia a la IA permiten comprender los procesos de la organización.
- Las iniciativas estratégicas documentadas de una organización o el plan estratégico que incluya los aspectos relacionados a IA.
- Los informes más recientes de la junta, que contienen la visión e información sobre cómo los líderes de la organización y el órgano de gobierno están discutiendo temas como el uso de la IA y las preocupaciones respecto a riesgos asociados a estas tecnologías.
- Información obtenida durante las reuniones de evaluación de riesgos con las partes interesadas.

Fuentes externas pueden proporcionar un marco de referencia adicional a medida que los auditores internos comienzan a revisar la estrategia de IA de su organización. Recursos externos valiosos pueden incluir:

- La trilogía “Global Perspectives & Insights” del IIA: La Revolución de la Inteligencia Artificial[14].
- “Artificial Intelligence 101 Series” del IIA.
- La Conferencia virtual “Analitycs, Automatización e IA” del IIA.
- Los recursos “Foundational IT” y “Cybersecurity Audit”, así como los certificados del IIA: “Programa de Auditoría en Ciberseguridad” y “Controles Generales de TI”.
- Guías de Práctica y Guías de Auditoría de Tecnología Global (GTAGs) del IIA.
- Marco de Gestión de Riesgos de IA (AI RMF 1.0) del NIST.
- Guías del National Cybersecurity Centre para el Desarrollo Seguro de Sistemas de IA[15].
- Executive Order sobre IA de la Casa Blanca de octubre de 2023[16].
- EBook sobre Gobernanza de IA de IBM[17].

Ambiente de Control a Nivel de Entidad: Ejecución y Estrategia

Al recopilar Información, y una vez que los auditores se hayan provisto de estos recursos, hacer la pregunta, **"¿Cómo se está utilizando la IA?"** es un punto de partida simple y efectivo. La respuesta a esta pregunta probablemente implicará preguntar a múltiples personas o departamentos porque muchas organizaciones no tienen una gestión centralizada de la IA, ni políticas establecidas (incluyendo la definición de qué es IA), procedimientos o una estrategia sobre el uso aceptable de la IA.

Para las organizaciones donde la IA ha sido desarrollada y desplegada, un auditor interno debería tener una conversación con el equipo de IA/ciencia de datos. Esta conversación debería incluir pedirles explicación sobre qué IA/algoritmos se han desplegado, incluyendo su función, fuentes de datos utilizadas, uso, limitaciones, riesgos e implicaciones éticas. Los auditores internos también deberían comenzar a entender qué controles existentes están en vigor para ayudar a gestionar los riesgos que plantea la IA, o si la Dirección ha implementado nuevos controles relacionados con el uso y despliegue de sistemas de IA. Obtener una comprensión preliminar del diseño de los controles utilizados para gestionar el riesgo relacionado con la IA es un paso importante que puede realizarse en conjunto con estas discusiones iniciales.

Para las organizaciones donde no está claro cómo se está utilizando la IA (formal o informalmente) o, si efectivamente se está utilizando tecnología de IA; la función de TI de la organización es un buen punto de partida porque, como se indicó en la sección de Niveles de Adopción en la Parte 1, los líderes tecnológicos parecen tener una mayor tendencia a experimentar y utilizar la IA en su departamento. Si TI confirma que se está utilizando IA, o si las consultas iniciales determinan que la IA está siendo utilizada en la organización, la siguiente pregunta lógica es determinar en qué medida se utiliza la IA.

Aunque una conversación inicial con el equipo de IA/ciencia de datos o la gestión de TI es un buen primer paso, la discusión no debe limitarse a esos grupos. De esas conversaciones iniciales, los auditores internos pueden descubrir que otros departamentos o usuarios individuales están utilizando la IA para sus funciones específicas, lo que requeriría conversaciones adicionales. Se recomienda trabajar con la Dirección para revisar o colaborar en la creación de un inventario de las tecnologías utilizadas actualmente y en qué áreas están desplegadas dichas tecnologías de IA. El inventario debe incluir otros aspectos clave como el objetivo de la IA, quién la utiliza, quién la gestiona, las herramientas específicas de IA en uso, las consideraciones de riesgo y quién ejerce supervisión sobre estas herramientas. El proceso de revisar o colaborar con la Dirección para desarrollar un inventario de IA también podría llevarse a cabo durante el proceso de evaluación de riesgos anual.

La mayoría de los auditores internos trabajan estrechamente con su Director Financiero (CFO) en relación con la prueba de controles internos sobre la información financiera, u otros ejecutivos como el Director de Seguridad de la Información (CISO), el Director de Tecnología de la Información (CIO), etc., por lo que tener esa relación profesional con miembros del equipo ejecutivo debería proporcionar otra oportunidad para conversaciones iniciales sobre IA. Los auditores internos pueden plantear las siguientes preguntas a sus ejecutivos de forma de obtener Información relevante:

- "¿Se ha establecido una estrategia de IA, y si es así, ¿Cuáles son los detalles de esa estrategia (incluyendo aspectos como el uso de IA para maximizar la eficiencia de las operaciones o para reducir costos)?"
- "¿La Alta Dirección ha designado quién es responsable de gestionar los riesgos relacionados con la IA?"
- "¿Qué rol tiene la Alta Dirección en la interacción con el Consejo (o equivalente) para consideraciones de gobernanza de IA?"

En este punto, los auditores internos habrán:

- Investigado la IA dentro de su organización y revisados recursos externos.
- Llevado a cabo conversaciones iniciales sobre IA con la Dirección, incluyendo a su equipo de IA/ciencia de datos o la gestión de TI (o ambos) y el equipo ejecutivo (CFO, CISO, CIO, etc.).

- Colaborado con la Dirección en la revisión o desarrollo de un inventario para capturar cómo se está utilizando la IA (o los planes existentes para su uso futuro).
- Iniciado el proceso de comprender el nivel de gobernanza de IA efectivamente implementado.

Cumplir con estas cuatro tareas indicaría que la auditoría interna ha dado los primeros pasos para establecer un conocimiento base sobre la IA en la organización. También proporcionaría una oportunidad para que la auditoría interna alerte sobre cualquier observación inmediata que deba ser comunicada a la Dirección de manera oportuna.

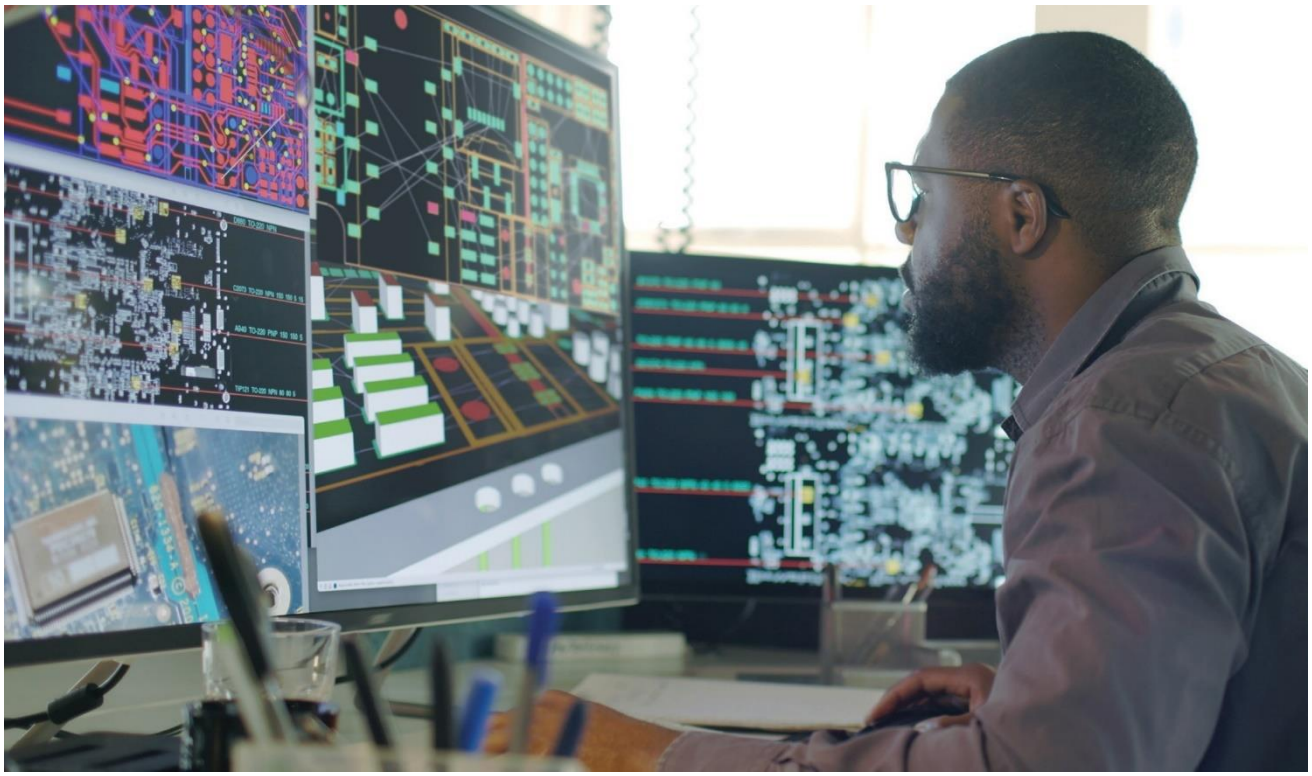
Datos

Después de que los auditores internos hayan comprendido fundamentalmente cómo se está utilizando la IA, deberían desarrollar un conocimiento más robusto sobre el uso de la IA dentro de la organización. Dado que los algoritmos utilizados para potenciar la IA dependen de grandes volúmenes de datos (también llamados “big data”), determinar qué datos organizacionales se están utilizando dentro de cualquier aplicación de IA y cómo se gestionan esos datos es crítico.

Un algoritmo es un conjunto de reglas que la IA sigue y es lo que permite a una máquina procesar rápidamente grandes cantidades de datos que un humano no puede procesar con la misma facilidad o velocidad. Dada la capacidad de la IA para ingerir y responder rápidamente a grandes conjuntos de datos diversos, la arquitectura, el rendimiento y la precisión de los algoritmos involucrados son muy importantes.

Los algoritmos son inicialmente desarrollados por humanos, por lo que el error humano y los sesgos (tanto intencionales como no intencionales) podrían afectar el rendimiento del algoritmo. La Parte 3 de este marco proporcionará más detalles sobre los riesgos relacionados con errores y sesgos en los algoritmos.

Por fuera de la IA, muchas organizaciones ya han desarrollado una estrategia para recolectar, almacenar, usar, gestionar y proteger datos. La IA es como otras aplicaciones basadas en datos en el sentido de que los mismos aspectos importantes a considerar sobre los datos son relevantes y deben ser considerados en relación a la IA, incluyendo integridad, privacidad, confidencialidad, validez, precisión y completitud.



Big data significa más que sólo grandes cantidades de datos: el big data se refiere a datos que alcanzan un volumen, variedad, velocidad y variabilidad tan altos que las organizaciones invierten en arquitecturas de sistemas, herramientas y prácticas diseñadas específicamente para gestionar los datos. Gran parte de estos datos pueden ser generados por la propia organización, mientras que otros datos pueden estar disponibles públicamente o comprados a fuentes externas. Para una guía completa sobre cómo entender y auditar el big data, incluyendo una discusión sobre oportunidades y riesgos relacionados, y un programa de trabajo de muestra, consulte **"GTAG: Entendiendo y Auditando el Big Data"** del IIA.

Otro aspecto crítico tanto del uso de datos como de las aplicaciones de IA relacionadas es si los datos están alojados en o procesados por una parte externa a la organización. Los auditores internos deben considerar siempre los riesgos relacionados con las transacciones con terceros (y cuartos) porque el ambiente y el control interno de los proveedores pueden no estar alineados a los de la organización. La Guía de Práctica del IIA "Auditoría de la Gestión del Riesgo de Terceros" ofrece a los auditores internos un enfoque detallado sobre los riesgos relacionados con la utilización de proveedores externos.

Otro aspecto importante de los datos es el acceso de los usuarios. Comprender quién puede editar o hacer cambios en los datos es crítico, ya que la manipulación de un conjuntos de datos desde el punto de vista de la entrada puede impactar significativamente en la salida de la IA. Entender y documentar el acceso de los administradores a los datos de los que dependen las aplicaciones que utilizan IA también es imprescindible. La Guía del IIA: "GTAG: Auditoría de la Gestión de Identidad y Acceso", ofrece una visión más cercana de las consideraciones de auditoría interna relacionadas con cómo las organizaciones pueden asegurar que los usuarios tengan el acceso adecuado a los recursos de TI.

Ciberseguridad

La ciberseguridad también debe ser considerada en relación con la restricción de usuarios no autorizados para acceder a datos y garantizar la privacidad, confidencialidad y protección de la información. La adopción y evolución de la IA está obligando a las organizaciones a reforzar sus capacidades de resiliencia informática. A medida que la IA se vuelve más poderosa y más decisiones se delegan en algoritmos nuevos, complejos y poco claros, que utilizan enormes volúmenes de datos, proteger estos sistemas de actos externas maliciosas es crucial para el éxito organizacional. La resiliencia cibernética es vital para cualquier organización que utilice IA.

Los auditores internos suelen estar involucrados en la prueba de la efectividad de los controles internos de TI. Este conocimiento sobre cómo la organización ha implementado controles relacionados con la ciberseguridad puede ayudarlos a validar que esos mismos controles se utilizan para proteger los datos relacionados con la IA. Ejemplos de controles de ciberseguridad incluyen:

- Uso de encriptación.
- Presencia de software antivirus.
- Utilización de sistemas de prevención/detección de intrusiones.
- Registro de eventos de seguridad, tanto de solicitudes como de respuestas.
- Realización periódica de tests de penetración como forma proactiva de búsqueda de vulnerabilidades.
- Capacitación de empleados en mejores prácticas para detectar y evitar esquemas de phishing, smishing y otras técnicas de ingeniería social.

Para más detalles, consulte la Guía del IIA: "GTAG: Auditoría de las Operaciones de Ciberseguridad: Prevención y Detección".

Los auditores internos deben determinar dónde se almacenan los datos de los que dependen las aplicaciones que utilizan IA (internamente, externamente o ambos) y considerar qué controles de ciberseguridad están en funcionamiento. Para los datos almacenados externamente, se debe obtener un informe del Proveedor de Servicios (SOC por su sigla en inglés) para conocer el ambiente de control del proveedor. La Dirección debe estar al tanto de cualquier deficiencia de control encontrada en el informe SOC y asegurar que esas deficiencias no pongan en riesgo los datos utilizados por la IA. Los acuerdos de nivel de servicio (SLA) con los proveedores deben incluir una cláusula de "derecho a auditar".

PARTE 3

Marco de Auditoría de IA

La primera versión del Marco de Auditoría de IA del IIA se emitió en 2017. Proporcionó a los profesionales de auditoría interna un enfoque para realizar servicios de aseguramiento y asesoramiento sobre IA de manera sistemática y disciplinada. Esta versión actualizada del marco moderniza el contenido con ejemplos del entorno actual de IA, al tiempo que proporciona detalles adicionales para ayudar a los auditores internos en su rol tanto de asesores como de proveedores de aseguramiento. El marco se compone de tres dominios:

Marco de Auditoría de IA del IIA

- *Gobernanza*
- *Gestión*
- *Auditoría Interna*

El marco se vincula con el Modelo de Tres Líneas del IIA: El órgano de Gobierno supervisa la Gestión (primer y segunda línea), mientras que el rol de la auditoría interna cubre el tercer dominio, que incluye tanto aseguramiento independiente (tercera línea), como actividades de asesoramiento.

El Marco de Auditoría de IA del IIA tiene como destinatarios a los profesionales de auditoría interna. Sin embargo, los dominios del marco de Gobernanza y Gestión, describen actividades y funciones fuera de auditoría interna, necesarias para gestionar la IA dentro de la organización.

La madurez de una organización respecto al uso de la IA contribuye al rol que desempeñará la función de auditoría interna. Por ejemplo, las organizaciones menos maduras en el uso de IA pueden necesitar una auditoría interna que asuma un papel de asesor en la exploración inicial de la IA, mientras que una organización más madura, probablemente requiera una auditoría interna que proporcione aseguramiento mediante actividades como la evaluación de los procesos definidos y los controles internos establecidos para alcanzar la eficacia operativa. Para desempeñar ambos roles con éxito, la auditoría interna necesita una comprensión sólida de cómo debe gestionarse la IA y de cómo lo está haciendo actualmente la organización.

Gobernanza — El primer dominio del marco se basa en el enfoque de una organización para la planificación estratégica de la IA y en proporcionar supervisión y monitoreo sobre cómo el despliegue de herramientas de IA es planificado, gestionado y ejecutado por la Administración. El órgano de gobierno se apoya en la información que le proporciona la función de auditoría interna. Los auditores internos deben esforzarse por desarrollar una relación de confianza

con los órganos de gobierno, como el comité de auditoría, la junta directiva o el órgano de gobierno equivalente. Esta relación debe incluir temas emergentes, como el uso de IA, que presentan nuevos desafíos para las actividades de supervisión.

El dominio de **Gestión** del marco describe el enfoque que la organización debe seguir al planificar y ejecutar el uso de IA dentro de la organización. El entorno de control interno que rodea a la IA lo establece la Dirección en la "Primera Línea". También incluye aspectos estratégicos como la definición de metas y objetivos relacionados con el plan estratégico general de IA. La auditoría interna debe asegurarse de entender la dirección estratégica de la IA para la organización y el enfoque de la gestión aplicado en el despliegue de la IA.

El dominio de Gestión del marco también alcanza aspectos de monitoreo de la IA en la "Segunda Línea", incluyendo la consideración de cómo la gestión de riesgos empresariales debe supervisar la "Primera Línea". La auditoría interna, a menudo debe participar en el proceso de evaluación de riesgos de la organización. Por lo tanto, los aspectos incluidos en este dominio son esenciales para mantener un conocimiento actualizado sobre los riesgos asociados con la IA.

El tercer dominio del marco, Auditoría Interna, incluye tanto actividades de asesoramiento a la Dirección, como los servicios de aseguramiento ("Tercera Línea"). La auditoría interna puede utilizar el marco como punto de partida en ambos roles cuando se le asigne participar en asignaciones relacionadas con la IA.

Dado que la IA está evolucionando rápidamente, el marco requerirá actualizaciones periódicas. Esta evolución, combinada con la naturaleza compleja de todo lo concerniente a la IA, implica que la auditoría interna probablemente podrá proporcionar solamente un nivel de aseguramiento limitado. El marco por sí solo puede no cubrir todos los aspectos de la IA, pero proporciona una base sólida para que los auditores internos desarrollen un conocimiento fundamental de la IA para el desarrollo de sus actividades.

Gobernanza

El Gobierno de IA se refiere a las estructuras, procesos y procedimientos implementados para dirigir, gestionar y supervisar las actividades de IA en la organización. La gobernanza incluye ayudar a asegurar que las actividades, decisiones y acciones relacionadas con la IA sean consistentes con los valores de la organización, así como con sus responsabilidades éticas, sociales y legales. También incluye proporcionar supervisión para asegurar que aquellos empleados con responsabilidades respecto al despliegue de IA cuenten con las habilidades y la experiencia necesarias.

Como se refleja en el Modelo de las Tres Líneas, la función de auditoría interna actúa como la "Tercera Línea", proporcionando aseguramiento independiente y objetivo sobre funcionamiento adecuado de los controles internos definidos por la organización para gestionar riesgos, incluyendo todos los aspectos de la IA. La auditoría interna puede proporcionar a la organización servicios de asesoramiento relacionados con la IA, pero desde el punto de vista de la Gobernanza, el órgano de gobierno depende en gran medida de las actividades de aseguramiento proporcionados por la auditoría interna para entender mejor la eficacia operativa de la organización.

El Gobierno de IA es crucial. Dos de los roles más importantes que desempeña la gobernanza son evaluar qué tan bien está gestionando la organización las operaciones de IA y si los objetivos estratégicos de IA se están logrando de manera consistente con los valores definidos por la organización. Como se presentó en secciones anteriores, existen una serie de riesgos específicos de IA; sin embargo, una de las principales consideraciones es proporcionar supervisión para garantizar un uso seguro de la IA.

Estrategia

Un plan estratégico permite a las organizaciones aclarar y comunicar el rumbo y visión necesarios para alcanzar sus metas; lo mismo ocurre con una estrategia de IA.

La estrategia de IA de cada organización debe ser única, basada en su enfoque para capitalizar las oportunidades que ofrece la IA, mientras se considera las circunstancias específicas de la organización, como la estructura actual de tecnología o las iniciativas en curso respecto al gobierno de datos. Un enfoque estratégico de IA reflexivo y metódico apoyará la capacidad de la organización para enfocar sus recursos y promover la alineación entre todos los empleados, al tiempo que mitiga los riesgos potenciales.

Dos aspectos importantes a tener en cuenta:

1. Planificar una estrategia de IA no es un evento único; es un proceso iterativo que debe realizarse periódicamente. La auditoría interna debe trabajar con la Dirección para determinar un cronograma para las revisiones de la estrategia de IA.

2. Una estrategia de IA no debe ser definida en forma aislada; dado el rango de posibles fuentes de datos y aplicación, las estrategias organizacionales de IA deben ser transversales. Dada la importancia crítica de la IA, es probable que se requiera la participación y supervisión a nivel del máximo órgano de gobierno, ya que la IA tiene el potencial de modificar o alterar drásticamente la estrategia empresarial.

Abordar estos puntos ayudará a garantizar que las iniciativas de IA respalden los objetivos, y que estos se alineen con los valores organizacionales. Definir metas para el despliegue de IA permite a las organizaciones enmarcar aspectos estratégicos importantes, incluida la respuesta a preguntas básicas como, "¿Por qué estamos utilizando IA?" y "¿Qué estamos intentando lograr?" Las metas de IA deben desarrollarse como otras metas organizacionales utilizando "SMART" — específicas, medibles, alcanzables, relevantes y basadas en el tiempo — para evitar la adopción de herramientas y servicios de IA sin una definición clara de los motivos de la organización para hacerlo[18].

Los atributos deseados de la IA deben incluirse al establecer las metas, objetivos y expectativas. Las expectativas u objetivos organizacionales pueden incluir los siguientes atributos:

Atributos deseables para la implementación de IA

- Eficaz
- Válida
- Confiable
- Segura
- Imparcial
- Transparente
- Ética
- Explicable
- Privada
- Acorde a las leyes y normas
- Justa
- Confidencial
- Responsable
- Precisa
- Eficiente

La actitud y el enfoque general de la organización hacia el riesgo y la gestión del riesgo deben ser una consideración principal al desarrollar o actualizar el plan estratégico de IA y sus objetivos. Tener una mayor tolerancia al riesgo en la búsqueda de objetivos de IA puede no ser apropiado para una organización que sea aversa al riesgo en otros aspectos, mientras que las organizaciones con una tolerancia al riesgo históricamente alta pueden estar más dispuestas a aceptar riesgos relacionados con la IA. Independientemente de la tolerancia al riesgo de la organización, es esencial reconocer y mapear los riesgos durante la planificación estratégica de la IA[19].

Gestión – Primer y Segunda Línea

Al desarrollar la estrategia de IA, la administración es responsable de asegurar que los controles internos estén bien diseñados y funcionen eficazmente para mitigar riesgos. Como se describió en secciones anteriores, los controles internos efectivos son un requisito crítico para la IA. Muchas organizaciones prueban y reportan los resultados de los controles de TI de manera trimestral y/o anual. La gestión debe estar al tanto de cualquier problema en los controles internos que pueda afectar el uso de la IA, especialmente en lo que respecta a las áreas del entorno de control interno que ya están bajo evaluación, como:

- Integridad y gobierno de datos.
- Acceso de Usuarios.
- Ciberseguridad.
- Ciclo de vida del Desarrollo de sistemas.
- Gestión del Cambio.
- Controles de Respaldo/Recuperación.

Marcos de control interno como COBIT y COSO pueden ser utilizados por las organizaciones para apoyar su enfoque y evaluación del ambiente de control interno [20,21].

Gestión – Primera Línea

Liderazgo

Definir roles y responsabilidades relacionados con las iniciativas basadas en IA apoyará a la organización en la determinación de los recursos necesarios para operar eficazmente. Identificar la responsabilidad ejecutiva, mientras se incorpora la opinión de otros miembros del equipo directivo, ayudará a asegurar la rendición de cuentas.

Un equipo de liderazgo de IA compuesto por miembros de distintas áreas es otra manera en la que las organizaciones pueden monitorear y comunicar iniciativas de IA y promover la rendición de cuentas. Este equipo debería incluir:

- Gerentes de IA y/o Ciencia de Datos.
- Director de Seguridad de la Información (CISO).
- Personal clave de TI.
- Legal (para proporcionar orientación sobre consideraciones regulatorias).
- Finanzas/Contabilidad para identificar costos y ROI de los proyectos de IA.
- Gestión de Riesgos.
- Cumplimiento.

La auditoría interna, con su amplio conocimiento sobre la organización, está en una posición única para servir como asesor y apoyar las iniciativas de IA, y debería considerarse como un miembro del equipo de liderazgo de IA. La participación de auditoría interna debe estructurarse para asegurar que su independencia no se vea comprometida.

Un proceso de planificación adecuado apoyará a la organización en la ejecución de proyectos de IA. Los empleados involucrados en la ejecución de los proyectos deben estar conscientes de los riesgos más críticos, incluyendo resultados no deseados. Es importante resaltar y asegurar que la ejecución de los proyectos tenga en cuenta aspectos sociales, éticos, ambientales y económicos.

Además, fomentar un entorno que anime a los empleados a discutir abiertamente ideas y preocupaciones relacionadas con las iniciativas de IA puede ayudar a crear una cultura de transparencia, conciencia y responsabilidad mutua para apoyar proyectos ambiciosos de IA.

Políticas y Procedimientos – Uso y aplicación en las organizaciones

Definir, adoptar y difundir políticas y procedimientos organizacionales sólidas sobre el uso de la IA dentro de la organización es otro aspecto importante de la estrategia de IA. Políticas y procedimientos claros proporcionan dirección a los empleados directamente involucrados en las iniciativas de IA y a aquellos que pueden usar IA como parte de sus actividades diarias. Desarrollar una política de uso aceptable de IA debe ser una prioridad organizacional. Esta política debería incluir prácticas recomendadas de ciberseguridad, consideraciones legales y de propiedad intelectual, y los riesgos asociados con diversas herramientas de IA. La política debe complementarse con un proceso documentado que los usuarios deben seguir al solicitar el uso de IA. El establecimiento de un proceso formal de aprobación para el uso de IA también apoyará los esfuerzos de la organización para mantener un inventario de usuarios o departamentos que utilicen IA.

Las políticas y procedimientos que establecen pautas y expectativas para desarrollar, implementar y monitorear iniciativas de IA, formalizan el proceso. Proporcionan una base sobre la cual validar si los proyectos se están realizando de manera consistente con las políticas aprobadas, la ética y el apetito de riesgo de la organización. Los auditores internos están en una posición única para proporcionar retroalimentación inmediata sobre este tema, dado su conocimiento y experiencia al proporcionar aseguramiento sobre políticas y procedimientos clave. En muchos casos, como punto de partida, las políticas y procedimientos existentes pueden ofrecer medidas razonablemente efectivas para mitigar los riesgos que plantea el desarrollo de IA. Por ejemplo, los sistemas de IA que se están desarrollando pueden estar sujetos a los procesos de control del Ciclo de Vida del Desarrollo de Sistemas (SDLC por sus siglas en inglés) o de gestión del cambio existentes. Con el tiempo, a medida que las organizaciones evolucionan y aumenta el uso de IA, sin duda será necesario considerar controles más maduros o acordes a las nuevas circunstancias.

En consecuencia, también es importante que las políticas y procedimientos aclaren las expectativas y directivas sobre terceros involucrados en las iniciativas de IA. La coordinación entre los equipos que gestionan la IA y el grupo de la organización que gestiona las relaciones con terceros (Legales, por ejemplo) promoverá relaciones coherentes con los proveedores de IA. Dado que los proveedores de servicios son una extensión de los procesos de la organización, mantener una buena comprensión del entorno de control de los proveedores será crucial. Cuando estén disponibles, la gestión debería obtener informes SOC de los proveedores de IA para entender sus procesos de control y estar al tanto de cualquier preocupación, como hallazgos de auditoría. El uso de terceros en relación con el desarrollo de capacidades de IA o el apoyo continuo a las iniciativas de IA debe estar claramente definido y monitoreado, incluyendo acuerdos de nivel de servicio (SLA) que contengan el derecho a auditar.

Una vez que se hayan delineado las políticas y procedimientos, las organizaciones pueden promover la aceptación generalizada compartiendo los borradores de la documentación, como la política de uso aceptable, con todo el personal, e invitando a realizar comentarios durante un período de consulta abierta.

Las organizaciones también deben planificar los recursos necesarios para capacitar al personal en estas nuevas políticas para asegurarse de que los empleados estén listos para adoptar y adherirse a los roles, controles y responsabilidades definidos en relación con el uso de la IA[22].

Recursos de TI para apoyar la IA

La optimización de los recursos de TI es necesaria para apoyar las iniciativas de IA y en consecuencia, deben asignarse los recursos adecuados. El uso de IA requiere un alto rendimiento de los recursos informáticos para asegurar un procesamiento confiable. Algunos ejemplos de recursos de TI utilizados para apoyar las iniciativas de IA de una organización incluyen:

- ***Unidades de Procesamiento Central (CPU)*** – el "cerebro" del ordenador; procesadores que ejecutan comandos o instrucciones[23].

- ***Unidades de procesamiento gráfico (GPU)*** – procesadores más avanzados que pueden manejar múltiples datos de manera simultánea, incorporando funciones matemáticas adicionales; estos procesadores son aptos para generar gráficos e imágenes, y se utilizan con mayor frecuencia en la producción creativa de IA[24].

- ***Almacenamiento*** – ubicación de los datos que requiere la IA para su procesamiento. El almacenamiento se mide comúnmente en terabytes (1,000 gigabytes) o petabytes (1,000 terabytes); para contextualizar, un video de 5-10 minutos en alta definición mide aproximadamente un gigabyte (1,000,000,000 bytes); los servidores alojados en el sitio o las soluciones basadas en la nube son ejemplos de dónde se pueden almacenar los datos.

- ***Memoria*** – también llamada RAM (memoria de acceso aleatorio, en español); es la ubicación de los datos a corto plazo que están disponibles más rápidamente que los datos de almacenamiento; se mide en gigabytes, donde las estaciones de trabajo de computadoras individuales tienen de 8 a 48 gigabytes de RAM; cuanto más compleja sea la IA que se ejecuta, más RAM se requiere.

- ***Supercomputadoras*** – las computadoras de procesamiento más rápidas que se utilizan para la computación de alto rendimiento y contienen múltiples CPU.

- ***Estaciones de trabajo*** – incluyen escritorios y laptops con especificaciones técnicas que soportan los requisitos de la IA que se está utilizando.

- ***Software*** – plataformas, programas y aplicaciones que se utilizan para desarrollar, implementar y gestionar la IA; software de desarrollo. Algunos ejemplos son Microsoft Azure AI, IBM Watsonx.ai y Google Cloud AI Platform; software de implementación, que se utiliza para integrar la IA en aplicaciones existentes; como por ejemplo Docker y MLflow.

- ***Conectividad de redes*** – esta es una categoría amplia que incluye el hardware, software y servicios que permiten a los usuarios compartir recursos digitales e intercambiar información; como por ejemplo servidores de archivos y enrutadores.

Aunque no se espera que los auditores internos conozcan todas las especificaciones técnicas y detalles de los requisitos de la IA, deben tener un conocimiento básico de los recursos de TI.

Personal y Capacitación

Una dotación adecuada de personal es un elemento importante de la estrategia de IA de una organización. Recursos Humanos debe colaborar con la administración para asegurar que se seleccione personal con la experiencia requerida en IA a lo largo de la organización. La experiencia en IA debe priorizarse no solo para los empleados que están a cargo de gestionar las actividades diarias relacionadas con IA, sino también para la integración de equipos que gestionan los proyectos e iniciativas de IA.

Dada la velocidad en que está desarrollándose la IA, es importante que los empleados de la organización estén al tanto de los avances y los riesgos relacionados. Las organizaciones deben asegurarse de que se brinde capacitación general sobre IA a todos los empleados y que las oportunidades de capacitación más técnicas, como seminarios, formación en línea o cursos educativos, estén disponibles para los empleados que se encargan de las iniciativas de IA.

Como se mencionó anteriormente en la sección de políticas y procedimientos, implementar capacitación sobre la política de uso aceptable de la IA e incluir la IA en el manual del empleado y los procesos de inducción de nuevos empleados son maneras de aumentar la conciencia organizacional sobre la IA junto con los posibles riesgos. Al integrar iniciativas de capacitación centradas en la IA y la alfabetización digital, las políticas y procedimientos organizacionales, y las oportunidades de mejora de habilidades relacionadas, las organizaciones pueden apoyar las iniciativas de IA a través de una inversión directa en los miembros actuales y futuros. La implementación y los resultados de estas iniciativas deben ser monitoreados por la auditoría interna como parte de los controles de IA de una organización.

Ejecución

Gestión de Riesgos por la Primera y Segunda línea

En la Parte 2 se discutió la importancia de identificar riesgos relacionados con la IA, como seguridad, integridad, privacidad y confidencialidad de los datos, y las organizaciones deben abordar estas preocupaciones a medida que ejecutan proyectos de IA. Los algoritmos de IA dependen de datos precisos y confiables, y los equipos de proyecto deben monitorear de cerca los datos de entrada. Existen diversas maneras de validar la integridad de los datos utilizados en proyectos de IA, incluyendo asegurar que los totales de registro sean consistentes, y analizar los informes de errores cuando los datos se transfieren entre sistemas. La Dirección debe diseñar y monitorear controles internos que detecten anomalías en la calidad o integridad de los datos.

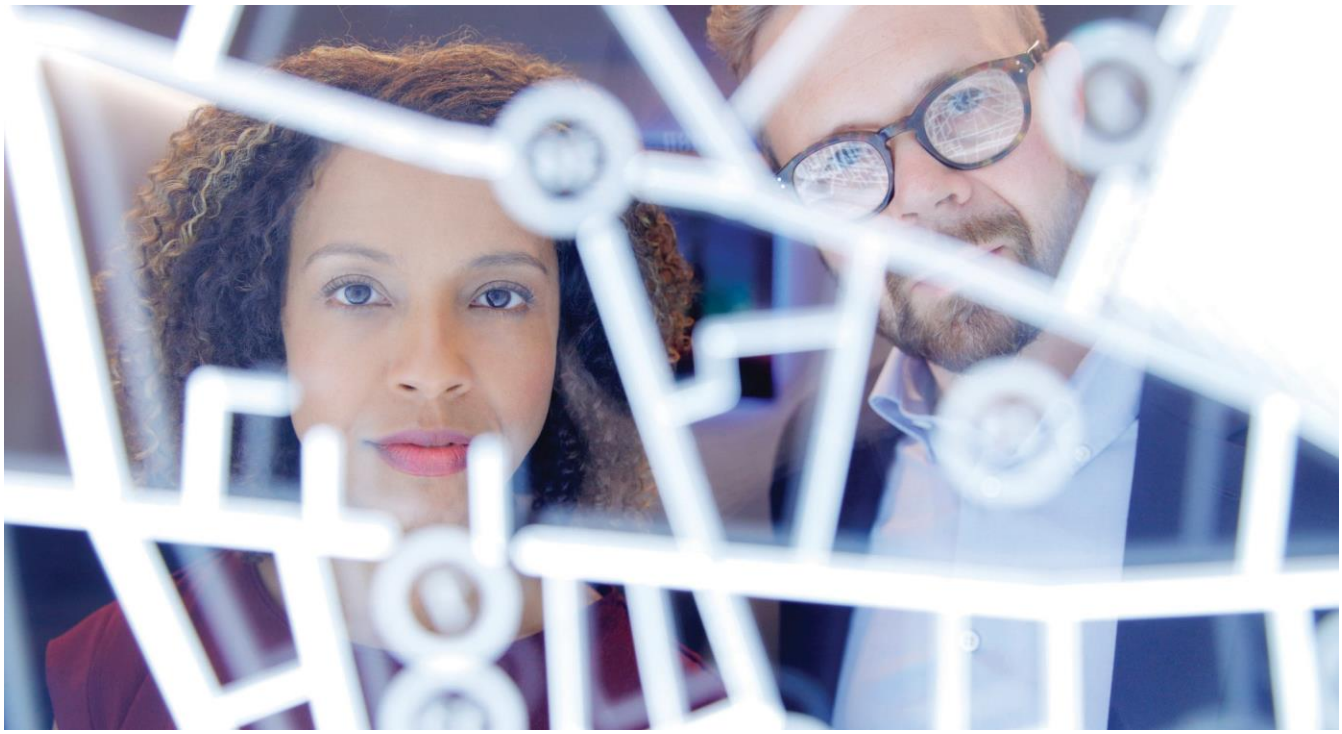
Otras consideraciones importantes sobre los datos incluyen restringir el acceso de los usuarios sólo a aquellos empleados que están trabajando en un proyecto de IA, lo que incluye el acceso de administradores. Determinar roles de usuario y asegurar la segregación adecuada de funciones es igualmente crítico. Por ejemplo, los administradores de bases de datos supervisan los datos de entrada y no deben tener acceso para modificar los algoritmos que procesan esos datos, tarea que tradicionalmente es responsabilidad de un desarrollador.

Cuando se implementa un proyecto de IA, es importante que la organización se asegure de que el proyecto sea transparente, explicable, confiable y auditable:

- ***Transparencia*** – capacidad de entender en términos simples el propósito de la IA o algoritmo.
- ***Explicabilidad*** – capacidad de explicar la configuración, cálculos o resultados procesados por la IA o el algoritmo.
- ***Confiabilidad*** – uso de la IA o algoritmos de manera ética, segura, justa y responsable.
- ***Auditable*** – dado que las aplicaciones de IA pueden comenzar a reemplazar o complementar ciertos procesos clave de cumplimiento u otros procesos empresariales importantes, mantener la trazabilidad a través de registros de auditoría (logs) efectivos o información relacionada, será un componente importante del desarrollo de IA, ya que se necesitarán garantías sobre estos procesos para su utilización.

La gestión de proyectos de IA debe definir los siguientes aspectos para cada iniciativa:

- ***Objetivos, roles y cronograma del proyecto*** – qué pretende lograr la iniciativa, quién participa y cuándo ocurre.
- ***Recursos Necesarios*** – qué recursos tecnológicos y/o de personal son necesarios para lograr el éxito del proyecto.
- ***Datos Requeridos*** – qué datos de entrada requiere la IA o los algoritmos.
- ***Requisitos de privacidad, legales y regulatorios*** – cuáles son los requerimientos de cumplimiento relacionados.
- ***Evaluación de Riesgos*** – cuáles son los riesgos relevantes que amenazan el logro de los objetivos del proyecto o los resultados no deseados, como sesgos, tratamiento no ético o mal uso de la IA.



- ***Indicadores Clave de Rendimiento (KPIs por sus siglas en inglés)*** – cómo se monitorea y mide el éxito del proyecto.

- ***Requerimiento de Pruebas*** – validar que la IA o el algoritmo están funcionando según lo diseñado y qué cambios son necesarios; esto incluirá tanto a los usuarios finales (quienes finalmente utilizarán la IA) como a los profesionales de IA/ciencia de datos; la identificación y comunicación de problemas será crítica en esta etapa. Revisar cómo los desarrolladores externos prueban y confirman la efectividad de sus algoritmos es una consideración importante.

- ***Aseguramiento de la Calidad*** – desde una perspectiva continua, dado que la salida de la IA, por su propia naturaleza, cambia debido a la entrada de datos, se debe considerar la prueba continua o el aseguramiento de la calidad del modelo. Dependiendo del caso, este concepto puede necesitar integrarse en la definición de requerimientos comerciales o en el diseño de la IA.

El monitoreo continuo de los proyectos de IA debe ser realizado por la gerencia para asegurar que la iniciativa esté avanzando según lo planeado y para identificar cualquier problema o preocupación que haya surgido. Como se indica en el Modelo de las Tres Líneas del IIA, la gerencia juega un papel vital en el entorno de control interno al proporcionar el primer nivel de acciones para mitigar el riesgo. El monitoreo a nivel de proyecto es importante porque es donde se detectan inicialmente los problemas. El reporte de la gerencia tanto a la Alta Dirección como al Consejo debe ser parte de este proceso. Es importante no solo monitorear el progreso general del proyecto, sino también identificar y reportar cualquier resultado negativo, como consideraciones éticas o violaciones de información confidencial. También es importante incluir una evaluación de terceros involucrados para asegurarse de que estén cumpliendo con sus responsabilidades en el proyecto de IA.

El monitoreo y el reporte también deben incluir la divulgación de cualquier problema específico del proyecto relacionado con el control interno o el análisis de problemas de control interno provenientes de otras áreas de la organización que puedan afectar el proyecto de IA.

La gestión de riesgos empresariales y/o el cumplimiento también deben ser parte del proceso de monitoreo de problemas de control desde una perspectiva de "Segunda Línea".

Apoyo de la Segunda Línea en la Gestión de Riesgos

Los principales objetivos del proceso de gestión de riesgos empresariales de una organización son comprender cómo los riesgos pueden amenazar el logro de los objetivos organizacionales y luego tomar acciones para mitigar esos riesgos. Las categorías de riesgo incluyen estratégicos, financieros, ambientales, de mercado, sociales, éticos, tecnológicos, económicos, políticos, legales y regulatorios. La IA es un tema que generalmente se considera un riesgo tecnológico; sin embargo, es importante reconocer que el riesgo de IA puede encajar en cualquiera de las categorías mencionadas en la que se clasifican típicamente todos los riesgos; lo que requiere un proceso de gestión de riesgos robusto para los proyectos de IA que considere tanto preocupaciones tecnológicas como no tecnológicas.

El Marco de Auditoría de IA del IIA proporciona consideraciones de gestión de riesgos para apoyar los proyectos de IA, para la implementación de las mejores prácticas en torno a la gestión de riesgos de IA. Cuando sea apropiado, se deben considerar otros marcos existentes, en particular, el Marco de Gestión de Riesgos de Inteligencia Artificial del NIST. Los auditores internos a menudo colaboran con profesionales de gestión de riesgos en actividades como el proceso anual de evaluación de riesgos de la organización; por lo tanto, es necesario que los auditores internos comprendan los riesgos relacionados con la IA y continúen aumentando su base de conocimientos. Además, los auditores internos deben considerar los riesgos relacionados con la IA a nivel de compromiso, es decir, al auditar procesos que incluyan algún aspecto de IA.

Identificación

Identificar los riesgos relacionados con la IA puede ser una actividad nueva para muchas organizaciones. Idealmente, la gestión de riesgos empresariales, (junto con auditoría interna, cumplimiento y legal), participará en las discusiones iniciales de todas las iniciativas de IA para ayudar a enmarcar los riesgos en torno al proyecto de IA.

Como se mencionó en la sección de Estrategia, un equipo de liderazgo de IA multidisciplinario es una manera efectiva de identificar proactivamente los posibles riesgos o amenazas antes de que se materialicen, asegurando que los controles y las técnicas de mitigación de riesgos estén implementados en toda la organización.

Las organizaciones que ya han establecido un proceso efectivo de evaluación de riesgos a nivel empresarial deben considerar realizar una evaluación inicial de riesgos enfocada en IA. Si no es factible una evaluación de riesgos separada para IA, las organizaciones, al menos, deben asegurarse de que la IA esté incluida durante el proceso general de evaluación de riesgos.

Por ejemplo, las organizaciones involucran a los distintos directores ejecutivos de manera periódica para identificar riesgos en varias áreas. En muchos casos, las discusiones o encuestas incluyen preguntas específicas, como: "¿Cuáles son los mayores riesgos estratégicos de la organización?" Para destacar la IA en el proceso de evaluación de riesgos, las organizaciones deben resaltar la IA como un área emergente de riesgo, compartir comentarios continuos del equipo responsable de IA y/o del personal interno, y recopilar las opiniones de los directores ejecutivos en consecuencia. La etapa de identificación de riesgos en el proceso de gestión de riesgos es importante porque puede resaltar riesgos que no se habían identificado previamente.

Las organizaciones que han establecido una estrategia clara de IA, con objetivos y metas definidos, están proporcionando el contexto que la gestión de riesgos empresariales necesita para ayudar en la identificación de riesgos de IA. Este contexto permite que la gestión de riesgos empresariales desarrolle un inventario de riesgos que amenacen el logro de esos objetivos y metas, permitiendo a las organizaciones incorporar en sus planes estratégicos medidas de protección contra posibles daños derivados del uso de la IA. Es importante que las organizaciones sean conscientes de que el panorama de riesgos en torno a la IA continúa evolucionando rápidamente, provocando consecuencias no deseadas y negativas de riesgos no considerados que pueden incluir [25]:

- Resultados sesgados o discriminatorios que pueden afectar injustamente a segmentos específicos de la población.
- Brechas de privacidad o confidencialidad.
- Debilidades en la rendición de cuentas y asignación de responsabilidad.
- Falta de transparencia.
- Falta de claridad.
- Daño Financiero.
- Amenazas Ambientales.
- Manipulación o falta de información.
- Infracciones al derecho de autor (Copyright, en inglés).

La “Caja Nega” (The “Black Box”)

Si bien gran parte de los procesos de identificación, evaluación y mitigación de riesgos para proyectos de IA siguen las mejores prácticas existentes, es importante señalar que la "caja negra" de la IA representa un riesgo único. El término se refiere a la falta de transparencia en los sistemas de IA y la manera en que toman decisiones. Los modelos de aprendizaje profundo, en particular, pueden ser difíciles de entender debido al procesamiento complejo realizado por los algoritmos junto con la visibilidad limitada o nula de cómo se produjo un resultado. Esto puede plantear desafíos específicos a medida que la gestión de riesgos empresariales (y los auditores internos) intentan recopilar la documentación necesaria para respaldar el ciclo de gestión de riesgos definido anteriormente. Los profesionales de gestión de riesgos y los auditores internos pueden abordar directamente la "caja negra" mediante:

Identificar y comunicar claramente dónde puede haber brechas de información o información incompleta dentro de un proyecto de IA.

- ***Ejemplo:*** Si una organización está utilizando un proveedor de servicios que utilizan IA, que no proporciona información detallada sobre los datos de entrenamiento de un algoritmo, esto debe documentarse y divulgarse como un posible riesgo.

Evaluar continuamente e informar al Consejo sobre posibles impactos relacionados con las brechas de información identificadas.

- ***Ejemplo:*** Una vez que se ha documentado la falta de documentación del proveedor sobre el conjunto de entrenamiento, los auditores internos deben informar al Consejo sobre las consecuencias relacionadas con el riesgo identificado (como salida sesgada de IA que sugieren problemas con los datos de entrenamiento, por ejemplo).

Establecer directivas sobre cómo mitigar los riesgos asociados con las brechas de conocimiento de la "caja negra" previamente documentadas y evaluadas.

- ***Ejemplo:*** Basado en las evaluaciones y consecuencias presentadas, la organización toma la decisión de migrar a un nuevo proveedor de IA con documentación de datos más transparente.

Evaluación

La evaluación y el análisis de los riesgos identificados relacionados con la IA deben seguir un proceso similar al que una organización utiliza para revisar otros riesgos: primero se deben considerar el impacto y la probabilidad. El impacto de los riesgos relacionados con la IA puede ser difícil de cuantificar debido a las numerosas consideraciones, como las ramificaciones legales, regulatorias, sociales, financieras, ambientales y éticas. El daño a la reputación de la marca es otra consideración para el impacto.

La combinación de impacto y probabilidad da como resultado el riesgo inherente, que es una medida del riesgo que existe sin la consideración de controles internos implementados. Después de evaluar el riesgo inherente, el siguiente paso es determinar el riesgo residual, que incluye la consideración sobre cómo los controles internos mitigan los riesgos identificados.

Por ejemplo, al evaluar la seguridad de la IA como un objetivo, se pueden identificar las amenazas cibernéticas como un riesgo significativo. Para mitigar estos riesgos, las organizaciones implementan controles de ciberseguridad con el fin de reducir el riesgo inherente a un nivel aceptable de riesgo residual de acuerdo con el apetito de riesgo de la organización. Si, tras esta evaluación, la gestión de riesgos empresariales determina que el riesgo residual aún no ha sido reducido a un nivel aceptable, la organización deberá decidir las acciones a seguir para abordar esta situación.

La priorización de riesgos es el proceso que una organización utiliza para clasificar los riesgos en orden de importancia, es decir, se abordan primero los riesgos de mayor impacto. Las organizaciones tienen recursos limitados, pero enfrentan riesgos ilimitados, por lo que es importante asegurar que los riesgos relacionados con la IA estén priorizados dentro del análisis más amplio a nivel de la entidad. La forma en que los riesgos relacionados con la IA se clasifican dentro de las organizaciones variará según su proceso de evaluación de riesgos, cuánto utilizan la IA y el nivel de madurez del ambiente de control interno. En pocas palabras, no existe un enfoque único para evaluar los riesgos relacionados con la IA.

Mitigación

La mitigación de riesgos es una acción (o acciones) que la gerencia toma para reducir el riesgo a un nivel aceptable. En muchos casos, las organizaciones optan por tratar los riesgos relacionados con la IA mediante acciones de mitigación, como la adición de controles internos; sin embargo, existen otras posibles respuestas a los riesgos, como se describe en la tabla “Posibles Respuestas frente al Riesgo” [26].

Numerosos factores influyen en cómo una organización determina cómo responder a los riesgos relacionados con la IA. Por lo tanto, es crucial tener un proceso definido y repetible de respuesta a los riesgos. Los riesgos relacionados con la IA pueden cambiar durante el transcurso de un proyecto, por lo que una organización debe revisar continuamente cómo responde y mitiga los riesgos.

Posibles Respuestas frente al Riesgo

RESPUESTA	CARACTERÍSTICAS	DEFINICIONES
Mitigar	Reducir, Tratar, Mejorar, Explotar, Aprovechar, Optimizar	Aplicar controles para reducir el riesgo inherente a un nivel de riesgo residual aceptable, o aplicar otras medidas para maximizar y obtener ventajas potenciales en los resultados.
Aceptar	Aceptar, Continuar	Determinar si los beneficios potenciales justifican asumir el riesgo, habiendo establecido las medidas que se consideren necesarias para mitigar la probabilidad y/o el impacto.
Transferir	Compartir, Distribuir	Compartir el riesgo, ya sea transfiriendo parte o la totalidad de este a un tercero (por ejemplo, mediante seguros o tercerización), o aplicando recursos de varios equipos para protegerse contra posibles pérdidas.
Evitar	Terminar, Eliminar	Terminar o evitar el riesgo abandonando la acción planificada o eliminando el objetivo por completo, priorizando otros objetivos.

Auditoría Interna – Asesoramiento y Aseguramiento

Después de describir cómo una organización debe abordar la IA en los dos dominios del marco anteriores, queda un dominio restante: Auditoría Interna.

Los primeros dos dominios proporcionan una base para que la auditoría interna pueda ofrecer tanto servicios de asesoramiento como de aseguramiento a la organización. Los dominios de Gobernanza y Gestión contienen los detalles que un auditor interno debe utilizar para asesorar a la organización en avanzar hacia las mejores prácticas o para formar una base para evaluar cómo la organización está abordando, utilizando, gestionando y monitoreando la IA.

La "**seguridad razonable**" es un término que se menciona a menudo dentro de la profesión de auditoría interna. Desde el punto de vista del control interno, la seguridad razonable significa que existe una alta probabilidad de que los controles mitiguen el riesgo, pero no es una seguridad absoluta.

El mismo razonamiento debe aplicarse a los auditores internos que están encargados de proporcionar aseguramiento en torno a la IA.

Desafíos

Distintos aspectos de la IA dificultan las actividades de aseguramiento para los auditores internos, incluyendo:

- La IA (o más específicamente, los algoritmos) es inherentemente compleja – un problema de "caja negra" de mayor dificultad.
- Las capacidades y riesgos de la IA se multiplican a un ritmo acelerado.
- La auditoría de la IA es un campo en evolución, con herramientas limitadas y enfoques de auditoría que aún están en desarrollo.
- Existen oportunidades limitadas de formación para mejorar las habilidades de auditoría en IA.

La auditoría de IA puede parecer una temática abrumadora, pero enfocarse en las siguientes consideraciones ayudará a los auditores internos a desarrollar una mentalidad positiva y confiada:

- No se espera que los auditores internos sean expertos en cada área de auditoría; en cambio, su objetivo debe ser mantener un enfoque disciplinado y metódico, centrado en el pensamiento crítico y la identificación de riesgos, aplicable a todas las auditorías, no solo a la de IA. La familiaridad con la temática y un conocimiento práctico de la IA son esenciales; sin embargo, es poco probable conocer todos los aspectos técnicos que involucran a la IA. Puede ser necesario recurrir a expertos externos para asistir en temas más técnicos, como el desciframiento de algoritmos.
- Dado que la IA es altamente compleja y cambiante, es poco probable que los auditores internos lleguen a dominar completamente el tema; considere la auditoría de IA con un enfoque progresivo y no como un destino definitivo – aumente la comprensión de la IA con el tiempo.
- Esté dispuesto a hacer preguntas relevantes sobre la IA dentro de la organización:
  - ¿Cómo ayuda la IA a alcanzar nuestros objetivos estratégicos?
  - ¿Cuáles son los riesgos y cómo los estamos mitigando?
  - ¿Existen controles internos adecuados en torno a los procesos relacionados con la IA?
  - ¿Los datos que se utilizarán para la IA son completos, precisos y confiables?
  - ¿Cómo se prueba la IA antes de su implementación para garantizar que no existan sesgos?
  - ¿Cómo se prueba la IA después de su implementación para garantizar que no existan sesgos?
  - ¿Cómo es la Gobernanza de IA?
  - ¿Cómo se asegura la organización de que exista una capacitación y concienciación adecuadas sobre la IA?

Como se describe en la Parte 2, comprender el uso de la IA en la organización, comienza con la investigación y la discusión. Es fundamental que los auditores internos aprovechen las relaciones profesionales que han desarrollado. La transparencia con la gerencia y con el órgano de gobierno es importante. Deben poder explicar de manera sencilla su enfoque hacia la IA y cómo planean involucrar a la organización para profundizar en el tema.

Las auditorías internas de IA son una responsabilidad relativamente nueva para muchas organizaciones. Si bien, como proveedores de aseguramiento, no se espera que los auditores internos sean expertos en el tema de la IA, deben identificar oportunidades para aumentar su conocimiento y conciencia sobre el tema. Obtener una mejor comprensión de los aspectos más técnicos de la IA, como los algoritmos, será importante para la educación profesional futura.

Aunque la IA ciertamente se compone de elementos complejos, es importante recordar que produce algún tipo de salida a partir de la entrada que recibe. Desde una perspectiva de aseguramiento, es posible que los auditores internos nunca tengan un conocimiento absoluto de todos los aspectos internos de la IA; sin embargo, ayudar a una organización a 1) evaluar lo que están haciendo para asegurar que los datos de entrada sean lo más precisos posible, y luego 2) comprender cómo se examina esa salida, deberían ser los principales objetivos de los auditores. Los auditores internos aplican estos conceptos hoy en día al realizar auditorías de TI. El factor común es la noción de trazabilidad – asegurar que los datos y la salida estén alineados con los objetivos y requisitos comerciales mediante el uso de la IA.

Notas Finales

1 . Britannica, “Artificial Intelligence”.
2. El Modelo de Tres Líneas del IIA.
3. A.M. Turing, “Computing Machinery”.
4. A.L. Samuel, “Checkers”.
5. McCarthy, Dartmouth.
6. Weizenbaum, “ELIZA”.
7. Humanoid Robot, “Waseda University”.
8. Hsu, “Raj Reddy”.
9.“Prometheus Project”.
10. Britannica, “Deep Blue”.
11. Índice de adopción de IA de IBM.
12. IBM “Different types of AI”.
13. Certes, “Types of AI”.
14. IIA Global Perspectives & Insights.
15. National Cybersecurity Centre.
16. White House Fact Sheet.
17. E B o o k Gobernanza de IA de IBM.
18. Doran, “Smart Way”.
19. Moyer, ISACA, “Quantitative Approach”.
20. COBIT, “Framework”.
21 . COSO, “Guidance”.
22 . Deloitte, “3 Lines”.
23 . “Gartner Glossary.”
24. Intel, “GPU”.
25 . Forbes, “15 Biggest Risks”.
26. IIA, CRMA.

PARTE 4

Guía y glosario para profesionales

La guía para profesionales es una lista de verificación (checklist) sencilla que los auditores internos pueden utilizar para comenzar su evaluación de cómo la organización aborda, utiliza, gestiona e informa los aspectos relacionados a la IA. Los auditores internos pueden aprovechar los puntos clave descritos en las secciones Gobernanza, Gestión, Auditoría Interna de la Parte 3 para desarrollar su plan de auditoría, o como consideraciones en un trabajo de aseguramiento. Muchos de los aspectos o consideraciones de la sección de aseguramiento están directamente relacionados con los temas tratados en los otros dominios.

Esta lista de verificación está diseñada para ofrecer una guía rápida, pero debe personalizarse según las consideraciones organizacionales, como el grado de uso actual de la IA y si se han establecido formalmente planes estratégicos, políticas, procedimientos, procesos y reportes de IA.

Actividad	Estado/ Resultado
Crea una visión, estrategia y priorización para la IA, revisándola y actualizándola con frecuencia.	
Vincula las iniciativas de IA con los objetivos estratégicos de la organización (Esto puede incluir usos de la IA que mejoran los ingresos, o aplicaciones internas para reducir costos o mejorar la eficiencia).	
Asegurarse de que la estrategia de IA incluya aspectos éticos, sociales, legales y los relacionados a los sesgos en la IA.	
Determine como medir el éxito de las iniciativas de IA, incluidos los objetivos y ROI.	
Garantizar que el plan estratégico de IA sea consistente con la cultura de riesgo de la organización.	
Asegurarse de que el plan estratégico de IA sea consistente con los valores de la organización.	

Actividad	Estado/ Resultado
Asegurarse de que el plan estratégico de IA se comunique formalmente al Consejo.	
Asegurarse de que el plan estratégico incluya la optimización de recursos de IA.	
Garantizar que el ambiente de control interno sea propicio para respaldar la IA. Considere qué cambios a las políticas son necesarios para impulsar el crecimiento de la IA; por ejemplo, la inclusión en la política de gestión de proveedores externos de aspectos relacionados a la IA.	
Definir los responsables de supervisar las iniciativas de IA.	
Establecer un equipo de liderazgo de IA multidisciplinario para monitorear las iniciativas de IA.	
Asegurarse de que los equipos legales y de cumplimiento supervisen los requerimientos reglamentarios actuales y emergentes.	
Definir el rol de auditoría interna como asesor y/o proveedor de aseguramiento.	
Asegurarse de que el Modelo de Tres Líneas está implementado e incluye aspectos de IA.	
Asegurarse de que el CISO (o equivalente) participe en todas las iniciativas de IA.	
Asegurarse de que los roles de terceros externos a la organización en las iniciativas de IA están claramente definidos y monitoreados.	
Asegurarse de que Finanzas/Contabilidad realice un seguimiento del Retorno de la Inversión (ROI) en las iniciativas de IA.	
Desarrollar una política de uso aceptable de la IA que sea de aplicación obligatoria para todos los empleados.	
Desarrollar políticas y procedimientos para ejecutar y mantener iniciativas de IA.	
Desarrollar políticas y procedimientos para iniciativas de IA que involucren a terceros externos a la organización.	
Asegurarse de que los recursos de TI sean suficientes para respaldar las iniciativas y controles de la IA.	
Garantizar que la estructura de personal sea suficiente para respaldar las iniciativas y controles de IA.	
Asegurarse de que los procesos de contratación de Recursos Humanos se centren en la contratación de profesionales con experiencia en IA.	
Los líderes responsables de las iniciativas de IA cuentan con los conocimientos necesarios sobre la gestión de IA.	
Los empleados que utilizan IA en sus actividades cuentan con conocimiento técnico de IA requerido.	
Todos los empleados son capacitados sobre el uso aceptable y los riesgos relacionados con la IA.	
Se incluye la IA como aspecto en el manual del empleado y en los procesos de inducción para nuevos empleados.	

Actividad	Estado/ Resultado
Garantizar que se consideren aspectos sociales, ambientales y económicos en todas las iniciativas de IA.	
Asegurarse de que los datos relacionados con la IA son seguros, privados y confidenciales.	
Asegurarse de que los datos relacionados con la IA son transparentes, explicables y responsables.	
Definir objetivos, metas, cronograma y requerimientos de recursos para todas las iniciativas de IA.	
Definir responsabilidades operativas para todos los empleados relevantes involucrados en proyectos de IA.	
Garantizar que el acceso de los usuarios a la IA sea proporcional a sus funciones.	
Definir requerimientos de datos y consideraciones sobre privacidad en todas las iniciativas de IA.	
Definir los requerimientos legales y regulatorios aplicables a los proyectos de IA.	
Realice una evaluación de riesgos de cada proyecto de IA para identificar posibles amenazas que puedan afectar el éxito de los proyectos.	
Definir posibles sesgos, incluyendo consideraciones éticas y sociales para proyectos de IA.	
Definir Indicadores Clave de Rendimiento (KPIs) en todas las iniciativas de IA.	
Establezca parámetros para informes requeridos como frecuencia, contenido e hitos en todas las iniciativas de IA.	
Establecer pruebas que validen que la IA está funcionando según lo previsto, antes y después de su implementación.	
Informe a la Alta Dirección y al Consejo sobre los resultados de las métricas definidas/KPIs	
Asegurarse de que los informes incluyan aspectos relacionados a sesgos y consideraciones éticas y sociales.	
Asegurarse de que los informes incluyan el cumplimiento de requerimientos legales y reglamentarios.	
Asegurarse de que los informes incluyan la divulgación de cualquier resultado negativo o no deseado.	
Asegurarse de que los informes incluyan la divulgación de posibles brechas de información, pérdida de datos o violaciones a la privacidad.	
Asegurarse de que los controles internos relacionados sean evaluados y que se informe periódicamente sobre el resultado de estas evaluaciones.	
Incluir la IA como parte del proceso de gestión de riesgos empresariales (ERM, por sus siglas en inglés).	
Identificar riesgos que amenazan la consecución de metas y objetivos estratégicos de IA.	
Identificar riesgos que puedan tener implicaciones éticas, sociales, ambientales o financieras.	

Actividad	Estado/ Resultado
Identificar riesgos que estén relacionados con el uso de terceros para IA.	
Asegurarse de que existe un proceso para identificar riesgos nuevos o emergentes.	
Asegurarse de que los empleados con responsabilidades de gestión de riesgos de IA están debidamente capacitados.	
Realizar evaluaciones periódicas de riesgos de IA.	
Priorizar los riesgos relacionados con la IA según su probabilidad e impacto.	
Asegurarse de que existe un proceso para seleccionar las respuestas apropiadas a los riesgos, incluida la evaluación del funcionamiento de las respuestas seleccionadas.	
Asegurarse de que la organización está comprometida con el Consejo y la Alta Dirección respecto a la estrategia, metas y objetivos de IA.	
Asegurarse de que la organización proporcione actualizaciones periódicas al órgano de gobierno sobre la IA de una manera clara y comprensible.	
Asegurarse de que la organización involucre al órgano de gobierno con respecto al enfoque utilizado para la gestión de riesgos de IA.	
Realizar una investigación inicial interna y externa de IA.	
Determinar si se ha desarrollado una estrategia formal de IA.	
Tener conversaciones iniciales con las áreas y personas clave en la organización (como TI y el Director Financiero) para comprender cómo se está utilizando y gestionando la IA en la actualidad.	
Tener conversaciones iniciales con los equipos responsables de AI/ciencia de datos (si aplica) y/o con el equipo de TI.	
Crear un inventario de usos actuales y planificados para la IA.	
Para el uso actual de IA, desarrolle una comprensión de cómo se utiliza, sus metas y objetivos.	
Para los planes e iniciativas de IA a futuro, desarrolle una comprensión del enfoque aplicado, cómo se evalúan los riesgos, y planifique pruebas previas a su implementación.	
Desarrollar una comprensión de los siguientes aspectos relacionados a los datos de entrada en aplicaciones que utilizan IA: • Gobierno. • Arquitectura. • Acceso de Usuarios. • Controles de Ciberseguridad. • Controles de Procesamiento (integridad, precisión, completitud). • Consideraciones de terceros externos (Reportes SOC).	
Verificar como se prueba y revisa la IA para garantizar que alcance sus objetivos y esté libre de sesgos, tanto antes como después de su implementación.	
Verificar que las iniciativas de IA tengan objetivos y metas claros, y que los proyectos de IA sean gestionados por un equipo adecuado con niveles adecuados de responsabilidad.	

Actividad	Estado/ Resultado
Verificar que la gerencia informe periódicamente al órgano de gobierno.	
Verificar que la IA se considere como parte del proceso de gestión de riesgos empresariales (ERM) e incluya riesgos relacionados con: • Ética. • Consideraciones Sociales y Económicas. • Aspectos Ambientales. • Implicaciones Financieras. • Violaciones Legales y/o Reglamentarias.	
Verificar que se hayan desarrollado políticas y procedimientos que describan cómo la organización debe utilizar y gestionar la IA, incluida una política de uso aceptable de la IA.	
Desarrollar una comprensión de cómo la organización apoya el aprendizaje y capacitación en IA para aumentar el conocimiento y concientización de todos los empleados.	

Estándares del IIA relacionados

6 .1 Mandato de Auditoría Interna

6.2 Estatuto de Auditoría Interna

6.3 Apoyo del Consejo y de la Alta Dirección

7.1 Independencia dentro de la Organización

7.2 Cualificaciones del Director Ejecutivo de Auditoría

8 .1 Interacción con el Consejo

8 .2 Recursos

8.3 Calidad

8.4 Evaluación Externa de Calidad

Glosario

Las definiciones de los términos marcados con asterisco se toman del Glosario del Marco Internacional para la Práctica Profesional del IIA®, edición 2017. Otras definiciones se incluyen para los fines de este documento o se derivan de las siguientes fuentes:

IBM. "Explainers." *IBM*. https://www.ibm.com/topics.

Institute of Risk Management. "Risk Culture". *Institute of Risk Management*, 2023. https://www.theirm.org/what-we-say/thought-leadership/risk-culture/.

Anderson, Urton; Michael J. Head; Steve Mar; Sridhar Ramamoorti; Chris Riddle; Mark Salamasick; Paul J. Sobel. Internal Auditing: Assurance & Advisory Services, 5th Edition. (Lake Mary, FL: The Internal Audit Foundation, 2022.) https://www.theiia.org/en/products/bookstore/internal-auditing-assurance-and-advisory-services-5th-edition/.

ISACA. "Glosario", *ISACA*. 2022. https://www.isaca.org/resources/glossary.

NIST Computer Security Resource Center. "Glosario". Gaithersburg, Md.: *NIST*. https://csrc.nist.gov/glossary.

Joint Task Force. *NIST SP 800-53: Security and Privacy Controls for Information Systems and Organizations, Revision 5, Appendix A: Glossary*. Gaithersburg, MD: NIST, September 2020. https://doi.org/10.6028/NIST.SP.800-53r5.

Grassi, Paul; Michael E. Garcia; James L. Fenton. *NIST SP 800-63-3: Digital Identity Guidelines, Appendix A: Definitions and Abbreviations*. Gaithersburg, MD: *NIST*, June 2017. https://doi.org/10.6028/NIST.SP.800-63-3.

Sawyer's Internal Auditing: Enhancing and Protecting Organizational Value, 7th Edition. (Lake Mary, FL: The Internal Audit Foundation, 2019.) https://www.theiia.org/en/products/bookstore/sawyers-internal-auditing-enhancing-and-protecting-organizational-value-7th-edition/.

Techopedia.com. "TechDictionary." https://www.techopedia.com/dictionary.

Algoritmo – Un proceso matemático claramente especificado para el cálculo; conjunto de reglas predeterminadas que, si se siguen, dará un resultado (Glorario NIST).

Apetito de Riesgo* – Los tipos y la cantidad de riesgo que la organización está dispuesta a aceptar al perseguir sus estrategias y objetivos.

Aprendizaje Automático (Machine learning, en inglés) – El aprendizaje automático (ML, por sus siglas en inglés) es una subcategoría de la inteligencia artificial (IA) que desarrolla modelos algorítmicos para identificar patrones y relaciones en los datos. En este contexto, la palabra "máquina" es sinónimo de programa informático, y "aprendizaje" describe cómo los algoritmos de ML se vuelven más precisos a medida que reciben más datos (Technopedia).

Aprendizaje Profundo – El aprendizaje profundo (O Deep Learning en inglés) es un enfoque iterativo de la inteligencia artificial (IA) que apila algoritmos de aprendizaje automático en una jerarquía de creciente complejidad y abstracción. Cada nivel de aprendizaje profundo se crea con el conocimiento obtenido del nivel anterior de la jerarquía (Techopedia).

Big data – Término utilizado para referirse a la gran cantidad de información digital en constante flujo, el aumento masivo en la capacidad para almacenar grandes cantidades de datos, y la cantidad de potencia de procesamiento de datos necesaria para gestionar, interpretar y analizar los grandes volúmenes de información digital (Internal Auditing, 5ª Edición).

Ciencias de la Computación – La Ciencia de la Computación es el estudio del hardware y el software de los computadores. Incluye tanto el estudio de algoritmos teóricos como los problemas prácticos involucrados en su implementación a través del hardware y software informático. El estudio de la informática tiene muchas ramas, incluyendo inteligencia artificial, ingeniería de software, programación y gráficos por computadora (Techopedia).

Chatbot – Un chatbot es un programa de inteligencia artificial que simula una conversación humana interactiva mediante el uso de frases preestablecidas por el usuario y señales auditivas o basadas en texto. Los chatbots son frecuentemente utilizados por organizaciones para proporcionar servicios de gestión de relaciones con clientes (CRM por sus siglas en inglés) las 24 horas. Este tipo de software también puede ser utilizado como un asistente virtual inteligente (Techopedia).

Ciberseguridad – La ciberseguridad se refiere a cualquier tecnología, medida o práctica para prevenir ciberataques o mitigar su impacto. La ciberseguridad tiene como objetivo proteger los sistemas, aplicaciones, dispositivos de computación, datos sensibles y activos financieros de individuos y organizaciones contra virus informáticos simples, ataques de ransomware sofisticados y costosos, y las distintas variedades de ataque existentes entre ambos extremos (IBM).

Comité de Auditoría – Un Comité delegado por el Consejo con la función de recomendar la aprobación de auditores e informes financieros (Sawyer's).

Consejo de Administración* – El órgano de gobierno de nivel más alto (por ejemplo, una junta directiva, un consejo de supervisión, o una junta de gobernadores o patronato) encargado de dirigir y/o supervisar las actividades de la organización y responsabilizar a la alta dirección.

Aunque la definición de gobernanza varía entre jurisdicciones y sectores, normalmente la junta incluye miembros que no forman parte de la gestión. Si no existe una junta, la palabra "junta" en las Normas se refiere a un grupo o persona encargado de la gobernanza de la organización. Además, "junta" en las Normas puede referirse a un comité u otro órgano al que la junta gobernante ha delegado ciertas funciones (por ejemplo, un comité de auditoría).

Control Interno – Mecanismo general que una empresa utiliza para alcanzar y monitorear los objetivos empresariales (Glosario de NIST).

Cultura de Riesgo – La cultura de riesgo es un término que describe los valores, creencias, conocimientos, actitudes y comprensión sobre el riesgo que comparten un grupo de personas con un propósito común. Esto aplica a todas las organizaciones, incluidas empresas privadas, organismos públicos, gobiernos y organizaciones sin fines de lucro (Institute of Risk Management).

Evaluación de Riesgos – El proceso de identificar riesgos para las operaciones organizacionales (incluyendo misión, funciones, imagen, reputación), activos organizacionales, individuos, otras organizaciones y naciones, resultantes de la operación de un sistema de información. Parte de la gestión de riesgos incluye análisis de amenazas y vulnerabilidades, y considera las mitigaciones proporcionadas por controles de seguridad planificados o en funcionamiento. Sinónimo de análisis de riesgos (Glosario de NIST).

Gobierno* – La combinación de procesos y estructuras implementados por el Consejo para informar, dirigir, gestionar y monitorear las actividades de la organización hacia el logro de sus objetivos.

Gobierno de Datos – La gobernanza de datos se refiere al proceso de gestionar la calidad de los datos dentro de una organización para asegurar que en todo momento, durante su ciclo de vida, los datos estén disponibles y sean precisos, consistentes, seguros y utilizables. Los analistas de negocios y los científicos de datos buscan información en toda la empresa para obtener información y comprensión de esa información, apoyando las necesidades empresariales (IBM).

Informe SOC (Service Organization Company o Proveedor de Servicios en español): Informe de auditoría, completado por un evaluador independiente, que evalúa el ambiente de control interno de una organización; puede ser proporcionado por los proveedores a los clientes para fines de aseguramiento de que sus controles internos están operando de manera efectiva.

Inteligencia Artificial – Un Sistema informático avanzado que puede simular capacidades humanas, como el análisis, basado en un conjunto predeterminado de reglas (ISACA).

Integridad de los Datos – La propiedad de que los datos no han sido alterados de manera no autorizada. La integridad de datos cubre datos en almacenamiento, durante el procesamiento y mientras están en tránsito (Glosario de NIST).

Marco de Gestión de Riesgos de la Inteligencia Artificial del NIST(NIST Artificial Intelligence Risk Management Framework (AI RMF), en inglés) – Según lo estipulado por la Ley de Iniciativa Nacional de Inteligencia Artificial de 2020 (P.L. 116-283), el objetivo del AI RMF es ofrecer un recurso a las organizaciones que diseñan, desarrollan, implementan o utilizan sistemas de IA para ayudar a gestionar los múltiples riesgos de la IA y promover el desarrollo y uso responsable y confiable de estos sistemas. El Marco está diseñado para ser voluntario, respetuoso de los derechos, no sectorial y agnóstico en cuanto la aplicación de IA, proporcionando flexibilidad a organizaciones de todos los tamaños y sectores, y en toda la sociedad, para implementar los enfoques del Marco. El Marco está diseñado para equipar a organizaciones e individuos —referidos aquí como actores de la IA— con enfoques que incrementen la confiabilidad de los sistemas de IA y para ayudar a fomentar el diseño, desarrollo, implementación y uso responsable de los sistemas de IA a lo largo del tiempo.

Modelos de Lenguaje de Gran Tamaño (Large language Model en Inglés) – Un modelo de lenguaje de gran tamaño (LLM, por sus siglas en inglés) es un tipo de modelo de aprendizaje automático que puede realizar una variedad de tareas de procesamiento de lenguaje natural (NLP), como generar y clasificar texto, responder preguntas de manera conversacional y traducir texto de un idioma a otro. El término “grande” se refiere a la cantidad de valores (parámetros) que el modelo de lenguaje puede cambiar autónomamente a medida que aprende. Algunos de los LLM más exitosos tienen cientos de miles de millones de parámetros (Techopedia).

NIST – Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology, en inglés).

Procesos de Respaldo/Recuperación – Se refiere al proceso de hacer copias de seguridad de datos en caso de pérdida y configurar sistemas que permitan la recuperación de esos datos debido a la pérdida de información. Realizar copias de seguridad de datos implica copiar y archivar datos informáticos para que sean accesibles en caso de eliminación o corrupción de datos. Los datos de un momento anterior solo pueden ser recuperados si se han respaldado (Techopedia).

Pruebas de Caja Negra – Es un enfoque de pruebas que se centra en la funcionalidad de la aplicación o producto sin requerir conocimiento del código interno. Los evaluadores interactúan con la interfaz de usuario y verifican si el sistema cumple con los requisitos especificados, sin considerar cómo se implementa la lógica interna (ISACA).

Reconocimiento de Voz – El reconocimiento de voz, también conocido como reconocimiento automático de voz (ASR, por sus siglas en inglés), reconocimiento informático de voz o conversión de voz a texto, es una capacidad que permite a un programa procesar el habla humana en un formato escrito. Aunque a menudo se confunde con la identificación de voz, el reconocimiento de voz se centra en la transcripción del habla de un formato verbal a uno textual, mientras que la identificación de voz se refiere a la capacidad de distinguir o autenticar la identidad de un usuario en particular a partir de su voz (IBM).

Reconocimiento Facial – El reconocimiento facial es un tipo de tecnología biométrica que utiliza datos para verificar la presencia del rostro de un ser humano en una captura digital. Hay dos usos principales para el software de reconocimiento facial: reconocimiento y autenticación (Techopedia).

Respaldo – Archivos, equipos, datos y procedimientos disponibles para su uso en caso de falla o pérdida, si los originales se destruyen o quedan fuera de servicio (ISACA).

Riesgo –Amenaza sobre el logro de un objetivo.

Robótica – La robótica es la ingeniería y operación de máquinas que pueden realizar tareas físicas de manera autónoma o semiautónoma en el lugar de un humano. Típicamente, los robots realizan tareas que son altamente repetitivas o demasiado peligrosas para que un humano las lleve a cabo de manera segura (Technopedia).

Referencias

Ambrozi, Austin. "11 Challenges Of Adopting AI In Business (And How To Address Them Head-On)," *Forbes*, October 24, 2023. https://www.forbes.com/sites/forbesbusinesscouncil/2023/10/24/11-challenges-of-adopting-ai-in-business-and-how-to-address-them-head-on/?sh=6710c8474bfe.

Ankers, Damon. "Types of Artificial Intelligence: A Detailed Guide." *Certes IT Service Solutions*. https://certes.co.uk/types-of-artificial-intelligence-a-detailed-guide.

Appel, Gil; Juliana Neelbauer; David A. Schweidel. "Generative AI Has An Intellectual Property Problem." *Harvard Business Review*, April 7, 2023. https://hbr.org/2023/04/generative-ai-has-an-intellectual-property-problem.

Billington, James. "The Prometheus Project: The Story Behind One of AV's Greatest Developments." *ADAS & Autonomous Vehicle International*, August 22, 2018. https://www.autonomousvehicleinternational.com/features/the-prometheus-project.html.

Britannica . "Artificial Intelligence ." *Encyclopedia Britannica* . 2023 . https://www .britannica .com/technology/artificial-intelligence.

Britannica . "Deep Blue Computer Chess-Playing System." *Encyclopedia Britannica*. 2023. https://www.britannica.com/topic/Deep-Blue.

COSO. "Guidance, Internal Control Integrated Framework." *COSO*. 2023. https://www.coso.org/guidance-on-ic.

Deloitte. "Modernizing the three lines of defense model: An internal audit perspective." Deloitte, 2023. https://www2.deloitte.com/us/en/pages/advisory/articles/modernizing-the-three-lines-of-defense-model.html.

Doran, George T. "There's a SMART Way to Write Management's Goals and Objectives." *Management Review*, 70, November 1981, 35-36. https://community.mis.temple.edu/mis0855002fall2015/files/2015/10/S.M.A.R.T-Way-Management-Review.pdf.

EY. "The CEO Outlook Pulse – October 2023," EY, 2023. https://www.ey.com/en_us/ceo/ceo-outlook-global-report#:~:text=The%20CEO%20Outlook%20Pulse%20

Gartner . "Gartner Glossary ." *Gartner* . 2023 . https://www .gartner .com/en/information-technology/glossary/cpu-central-processing-unit.

Hsu, Hansen. "Meet 2021 CHM Fellow Honoree Raj Reddy." *Computer History Museum*. https://computerhistory.org/blog/meet-2021-chm-fellow-honoree-raj-reddy/.

Humanoid Robotics Institute. "History of Humanoid Robot in Waseda University." Waseda University. https://www.humanoid.waseda.ac.jp/history.html.

IBM. "eBook: Build responsible AI workflows with AI governance." *IBM*. https://www.ibm.com/account/reg/us-en/signup?formid=urx-51898.

IBM. "IBM Global AI Adoption Index." *IBM*, 2023. https://www.ibm.com/watson/resources/ai-adoption.

IBM. "Understanding the Different Types of Artificial Intelligence." *IBM*, October 2023. https://www.ibm.com/blog/understanding-the-different-types-of-artificial-intelligence/.

The Institute of Internal Auditors. *CRMA Study Guide and Practice Questions, 3rd Edition*. The IIA. 2023. https://www.theiia.org/en/products/bookstore/crma-study-guide-and-practice-questions-3rd-edition/.

The Institute of Internal Auditors. *Global Perspectives & Insights: the Artificial Intelligence Revolution*. The IIA. 2023. https://www.theiia.org/en/content/articles/global-perspectives-and-insights/2023/global-perspectives-insights-the-artificial-intelligence-revolution/.

The Institute of Internal Auditors. *The IIA's Three Lines Model: An update of the Three Lines of Defense*. The IIA. 2020. https://www.theiia.org/en/content/position-papers/2020/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense/?msclkid=f2923355c01e11ecb401fe1dc46cbc38.

The Institute of Internal Auditors. International Professional Practices Framework. 2017 ed. (Lake Mary, FL: The Institute of Internal Auditors, 2017). https://www.theiia.org/en/products/bookstore/international-professional -practices-framework---ippf---2017-edition/.

Intel. "What is a GPU?" Intel. https://www.intel.com/content/www/us/en/products/docs/processors/what-is-a-gpu.html.

ISACA. "COBIT, An ISACA Framework." *ISACA*. 2023. https://www.isaca.org/resources/cobit.

ISACA. "Glossary." *ISACA*. 2022. https://www.isaca.org/resources/glossary.

Marr, Bernard. "The 15 Biggest Risks of Artificial Intelligence." *Forbes*. June 2, 2023. https://www.forbes.com/sites/bernardmarr/2023/06/02/the-15-biggest-risks-of-artificial-intelligence/?sh=16756d8b2706.

McCarthy, J; M.L. Minsky; N. Rochester; C.E. Shannon. "A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence." *BibSonomy*. https://www.bibsonomy.org/bibtex/24550126962fd8014daa80db1ffae4df2/mhwombat.

Moyer, Steven; Gunter Brunhart; Richard Dubs, Thomas Erickson, Robert Skalamera, Rob Kepner, Marty Meyer, "A (Kind of) Quantitative Approach to Organizational Risk Tolerance." *ISACA*, July 8, 2021. https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2021/a-kind-of-quantitative-approach-to-organizational-risk-tolerance.

National Cyber Security Center. "Guidelines for secure AI system development." *National Security Centre*. 2023. https://www.ncsc.gov.uk/collection/guidelines-secure-ai-system-development.

NIST. *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, Gaithersburg, Md.: NIST, 2023. https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf.

NIST Computer Security Resource Center. "Glossary." Gaithersburg, Md.: NIST. https://csrc.nist.gov/glossary.

PwC. "PwC 2022 AI Business Survey (U.S.)." *PwC*. https://www.pwc.com/us/en/tech-effect/ai-analytics/ai-business-survey.html.

QuantumBlack AI by McKinsey. "The State of AI in 2023: Generative AI's Breakout Year." *McKinsey*. 2023. https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-in-2023-generative-AIs-breakout-year.

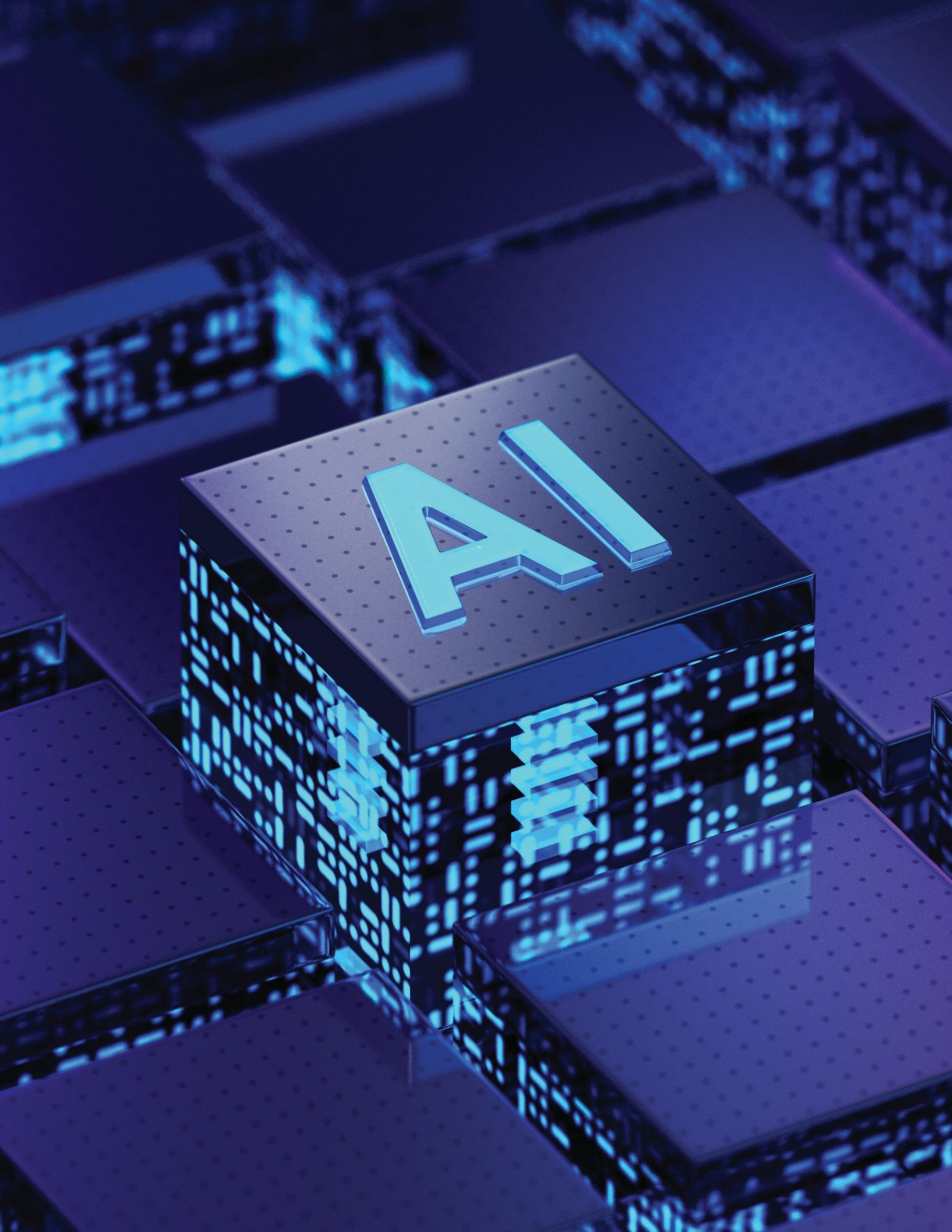
Samuel, A.L. "Some Studies in Machine Learning Using the Game of Checkers." *IBM Journal of Research and Development*. July 1959. https://ieeexplore.ieee.org/document/5392560.

Techopedia.com. "TechDictionary." https://www.techopedia.com/dictionary.

Turing, A.M. "Computing Machinery and Intelligence." *Mind*, Volume LIX, Issue 236, October 1950, Pages 433–460. https://academic.oup.com/mind/article/LIX/236/433/986238.

Weizenbaum, Joseph. "ELIZA—A Computer Program For the Study of Natural Language Communication Between Man and Machine." *Communications of the Association for Computing Machinery*. January 1966. https://dl.acm.org/doi/10.1145/365153.365168.

White House. "Fact Sheet: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence." *The White House*. October 30, 2023. https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/.


AI

Equipo de Desarrollo del Marco
George Barham, Allison Banzon, Anne Mercer, Kat Seeuws, Geoff Nordhoff.

Colaboradores
Andrew Cook, Pam Stroebel Powers, Robert Perez, Jim Enstrom, Scott Moore.

Acerca del Instituto
El Instituto de Auditores Internos (The Institute of Internal Auditors o IIA) es la asociación profesional de auditores internos constituida como la voz global de la profesión, autoridad líder y principal defensor, educador y el proveedor de normas, guías y certificaciones reconocido por la profesión de auditoría interna. Fundado en 1941, el IIA actualmente atiende a más de 230.000 miembros en más de 170 países y territorios. La sede global de la asociación se encuentra en Lake Mary, Florida, EE.UU. Para más información, visita **www.theiia.org**.

Descargo de Responsabilidad
El IIA publica este documento con fines informativos y educativos. Este material no tiene como finalidad ofrecer respuestas definitivas a circunstancias específicas y puntuales y, como tal, solo está pensado para su uso como guía. El IIA recomienda solicitar siempre asesoramiento de expertos independientes para cualquier situación específica relacionada. El IIA no asume responsabilidad por quien tome este material como su única fuente confiable.

FLAI
Fundación Latinoamericana
de **Auditores Internos**

Instituto Uruguayo de
Auditoría Interna

IIA Headquarters
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746 USA

The Institute of
Internal Auditors