Artículo de Investigación Original

# Estrategias de IA aplicada a la auditoria informática
# AI strategies applied to computer auditing

Alejandro Reyes 0009-0003-9399-9166
Universidad de Buenos Aires, Buenos Aires, Argentina
a.reyes@gmx.com

**CITA EN APA:**
Reyes , A. (2023). Estrategias de IA aplicada a la auditoria informática. Technology Rain Journal, 1(1), e18. https://doi.org/10.55204/trj.v1i1.18

**Recibido: 17** de Abril 2023
**Aceptado: 22** de Mayo 2023
**Publicado:** 01 de Julio 2023

Technology Rain Journal
**ISSN:** 2953-464X

Los contenidos de este artículo están bajo una licencia de Creative Commons Attribution 4.0 International (CC BY 4.0 )
Los autores conservan los derechos morales y patrimoniales de sus obras.

**Resumen.** La auditoría se ha visto asociada con conceptos erróneos, como la idea de que su objetivo es buscar errores y atacar a funcionarios. Sin embargo, la auditoría va más allá de estos hallazgos y ha evolucionado con el tiempo. En la actualidad, la auditoría de TI es un tema importante para las organizaciones modernas. En un entorno cambiante, la capacidad de gestionar riesgos y proteger información valiosa se ha vuelto crucial para la sostenibilidad y el valor empresarial. En este contexto, se han realizado esfuerzos para aplicar estrategias de inteligencia artificial en las auditorías de TI, lo que ofrece oportunidades para mejorar el proceso de auditoría. La propuesta es utilizar herramientas y técnicas de IA para analizar grandes volúmenes de datos, identificar patrones y anomalías, automatizar tareas repetitivas y fortalecer los controles internos. Esto permite una mayor eficiencia y efectividad de las auditorías, así como la confianza en un entorno empresarial digital en constante cambio. El objetivo del artículo es explorar el uso de la inteligencia artificial en las auditorías de TI y analizar cómo puede mejorar el proceso, aumentar la seguridad de los activos digitales y proporcionar recomendaciones basadas en hallazgos. La propuesta implica el uso de algoritmos de aprendizaje automático y técnicas de análisis de datos para lograr estos objetivos.
**Palabras Clave:** Inteligencia Artificial, Auditoría informática, Big Data, Aprendizaje Automático, Procesamiento lenguaje natural

**Abstract.** Auditing has been associated with misconceptions, such as the idea that its objective is to find errors and attack officials. However, auditing goes beyond these findings and has evolved over time. Currently, IT auditing is an important topic for modern organizations. In a changing environment, the ability to manage risks and protect valuable information has become crucial for sustainability and business value. In this context, efforts have been made to apply artificial intelligence (AI) strategies in IT audits, offering opportunities to improve the auditing process. The proposal is to use AI tools and techniques to analyze large volumes of data, identify patterns and anomalies, automate repetitive tasks, and strengthen internal controls. This enables greater efficiency and effectiveness in audits, as well as building trust in a constantly changing digital business environment. The objective of the article is to explore the use of artificial intelligence in IT audits and analyze how it can enhance the process, increase the security of digital assets, and provide findings-based recommendations. The proposal involves the use of machine learning algorithms and data analysis techniques to achieve these objectives.

**Keywords:** Artificial Intelligence, IT auditing, Big Data, Machine Learning, Natural Language Processing

## 1. INTRODUCCIÓN

Al hablar de auditoría, a menudo se asocian conceptos erróneos a este proceso, como la idea de que su objetivo es buscar errores en una organización y atacar a funcionarios (Imbaquingo, Díaz, Saltos, Arciniega, & De La Torre, 2020). Si bien esta percepción puede contener algo de verdad, la auditoría va más allá de los hallazgos y de identificar las anormalidades de los auditados. Con el paso del tiempo, el concepto de auditoría ha evolucionado, al igual que las ramas que

derivan de ella ( (Imbaquingo, Díaz, Saltos, Arciniega, & De La Torre, 2020). En la actualidad, la auditoría de TI se ha convertido en uno de los temas principales que se discuten entre los profesionales de la auditoría interna y es de gran importancia para las organizaciones modernas (Adrian Gepp, 2018)

En un entorno en constante cambio, el éxito de una organización está estrechamente relacionado con su capacidad para gestionar los riesgos. A medida que las empresas dependen cada vez más de la información para obtener ventaja competitiva, y la información representa un valor agregado significativo en los productos y servicios de las empresas, proteger la información valiosa y sensible se ha convertido en una capacidad estratégica para asegurar la sostenibilidad empresarial y el valor total de una empresa (Diego A. Arcentales Fernández, 2017).

La implementación de un sistema efectivo de auditoría de TI es fundamental para garantizar la integridad y confidencialidad de la información en una organización. En el entorno empresarial actual, que depende cada vez más de la información, la protección de datos valiosos se convierte en una oportunidad estratégica para asegurar la sostenibilidad y el valor empresarial.

En el ámbito de la auditoría de TI, se han llevado a cabo diversos esfuerzos para abordar los desafíos actuales. Estos esfuerzos incluyen la aplicación de estrategias de inteligencia artificial (IA) en las auditorías de TI, lo que ha surgido como una gran oportunidad para mejorar significativamente el proceso de auditoría. La IA proporciona un conjunto de herramientas y técnicas que pueden analizar grandes cantidades de datos, descubrir patrones y anomalías, y automatizar tareas repetitivas, liberando tiempo y recursos para actividades más analíticas y estratégicas.

En vista de la importancia de la auditoría de TI y los avances en inteligencia artificial, el autor se ha motivado a realizar una propuesta para aprovechar las ventajas de la IA en el proceso de auditoría. La idea es utilizar las herramientas y técnicas de IA para mejorar la eficiencia y efectividad de las auditorías de TI, permitiendo una identificación más precisa de vulnerabilidades, riesgos y deficiencias, así como proporcionando recomendaciones basadas en hallazgos para fortalecer los controles internos y mantener la confianza de los clientes y socios comerciales en un entorno digital en constante evolución.

El objetivo del artículo es explorar el uso de estrategias de inteligencia artificial en las auditorías de TI y analizar cómo pueden mejorar el proceso de auditoría, aumentar la eficiencia y la efectividad, y fortalecer la seguridad de los activos digitales de una organización. La propuesta consiste en aplicar herramientas y técnicas de IA para analizar grandes cantidades de datos, identificar patrones y anomalías, automatizar tareas repetitivas y proporcionar recomendaciones basadas en hallazgos.

La propuesta consiste en utilizar la inteligencia artificial para mejorar el proceso de auditoría de TI. Esto implica el uso de algoritmos de aprendizaje automático y técnicas de análisis de datos para analizar grandes volúmenes de información y descubrir patrones y anomalías. Al automatizar tareas repetitivas y liberar tiempo y recursos, los auditores de TI pueden centrarse en actividades más analíticas y estratégicas, lo que lleva a una mejora en la eficiencia y efectividad de las auditorías. Además, la propuesta busca proporcionar recomendaciones basadas en hallazgos para fortalecer los controles internos y mantener la confianza en un entorno empresarial digital en constante cambio.

## 2. METODOLOGÍA

Se basa en una revisión y análisis exhaustivos de la literatura científica existente sobre la aplicación de estrategias de inteligencia artificial en la auditoría computarizada. Se identifican fuentes recientes relevantes y los resultados se analizan críticamente y se organizan en categorías específicas.

Los resultados se sintetizan en un artículo científico siguiendo una estructura lógica, se revisan para garantizar su coherencia y precisión, y se validan cuando es necesario. El objetivo principal es proporcionar información precisa respaldada por literatura científica y cumplir con los estándares académicos y científicos establecidos.

## 3. RESULTADOS

**Big Data**: El término "Big Data" se refiere a conjuntos de datos estructurados o no estructurados que a menudo se caracterizan en términos de las cuatro características V: volumen, variedad, velocidad y veracidad (Chun-Wei Tsai, 2015). El Big Data también se refiere a las técnicas y tecnologías utilizadas para inferir conclusiones a partir de la variedad de tipos de datos. Estas técnicas a menudo buscan inferir relaciones no lineales y efectos causales a partir de datos que a menudo son muy escasos en información. Dada la naturaleza de los datos, estas técnicas a menudo no tienen o tienen supuestos de distribución muy limitados. Los científicos informáticos abordan el Big Data desde el punto de vista de descubrir patrones en el registro completo, lo que a menudo se llama enfoque algorítmico. Los patrones se consideran aproximaciones a la complejidad del conjunto de datos. En comparación, los estadísticos tienden a tratar los datos como observaciones de un proceso subyacente y extraer información y realizar inferencias sobre ese proceso subyacente (Adrian Gepp, 2018).

Big data se refiere a conjuntos de datos que son demasiado grandes para ser procesados por herramientas tradicionales. Esta diversidad refleja diferentes formatos de datos, como datos cuantitativos, textuales e híbridos, así como imágenes, videos y otros formatos. La velocidad mide

la frecuencia con la que hay nuevos datos disponibles y se vuelve más rápido. Finalmente, la calidad y la relevancia de los datos pueden cambiar drásticamente con el tiempo, lo que se denomina precisión. La industria de la auditoría tiene acceso a más y más datos, que son cada vez más diversos y precisos.

Las técnicas estadísticas utilizadas en el Big Data requieren modelos más flexibles, ya que los modelos de regresión tradicionales altamente estructurados son muy poco probables de ajustarse bien al Big data. Además, el volumen (así como la variedad y la velocidad) del Big data es tal que no es factible descubrir la estructura adecuada para los modelos en muchos casos (Chun-Wei Tsai, 2015). El uso de Big data puede traer varios beneficios a la auditoría de TI. Primero, la capacidad de Big data para analizar grandes cantidades de datos significa que los auditores pueden examinar grandes cantidades de información de manera más eficiente y precisa. Esto les permite identificar patrones, tendencias y anomalías que pueden indicar posibles riesgos o problemas en los sistemas informáticos.

Además, Big Data facilita el análisis de diferentes tipos de datos, incluidos datos estructurados y no estructurados, como registros de transacciones, registros de servidores, correos electrónicos, archivos de texto y contenido de redes sociales. Al integrar y analizar esta amplia gama de datos, los auditores obtienen una imagen más completa y detallada de las operaciones y los procesos de la organización, lo que permite una evaluación más precisa del riesgo y la eficacia de los controles internos.

Otro aspecto importante de los grandes datos en la auditoría de TI es su capacidad para proporcionar información en tiempo real. Con análisis en tiempo real, los auditores pueden monitorear y detectar de manera proactiva eventos o actividades sospechosas, como intentos de intrusión o comportamiento inusual en los sistemas informáticos. Esto permite una respuesta rápida y oportuna a amenazas potenciales, mejorando la seguridad y las capacidades de detección de riesgos.

**Machine Learning**: El aprendizaje automático (Machine Learning) es el estudio científico de algoritmos y modelos estadísticos que los sistemas informáticos utilizan para realizar una tarea específica sin ser programados explícitamente. Los algoritmos de aprendizaje se utilizan en muchas aplicaciones que utilizamos a diario. Cada vez que se utiliza un motor de búsqueda web como Google para buscar en Internet, una de las razones por las que funciona tan bien es porque utiliza un algoritmo de aprendizaje que ha aprendido a clasificar las páginas web (Mahesh, 2018).

El Machine Learning ofrece diversas formas de apoyar la auditoría informática, mejorando la eficiencia y precisión de los procesos de revisión. En primer lugar, el ML puede ayudar en la detección de anomalías y la identificación de patrones sospechosos en grandes volúmenes de datos.

Al aplicar algoritmos de ML, se pueden analizar de manera rápida y automatizada registros de transacciones, registros de servidores y otros datos relevantes, identificando posibles riesgos y comportamientos inusuales.

Por tanto, en cuanto a la implementación del Big Data en la auditoría, uno de los beneficios más destacables es la posibilidad de realizar análisis en tiempo real con el objetivo de subsanar las limitaciones existentes y realizar comparaciones de grandes cantidades de datos, de manera que pueden tomar decisiones a través del estudio de casos anteriores referentes al incumplimiento y al fraude (Gómez Palanques, 2021).

Además, el ML puede mejorar la capacidad predictiva en la auditoría informática. Al entrenar modelos de ML con datos históricos, se pueden desarrollar algoritmos que identifiquen patrones de comportamiento que indiquen posibles irregularidades o fraudes. Esto permite a los auditores enfocar sus esfuerzos en áreas de mayor riesgo y tomar decisiones basadas en datos más sólidos.

Otra área en la que el ML puede ser útil es en la automatización de tareas rutinarias. Los algoritmos de ML pueden ayudar a procesar grandes volúmenes de datos, realizar verificaciones y reconciliaciones automáticas, y generar informes de manera eficiente. Esto libera tiempo y recursos para que los auditores se centren en tareas más analíticas y estratégicas, aumentando la productividad y eficacia de la auditoría.

Sin embargo, es importante destacar que el uso del ML en la auditoría informática también plantea desafíos y consideraciones éticas. La interpretación de los resultados de los modelos de ML y la toma de decisiones basadas en ellos requiere una comprensión profunda de los algoritmos utilizados y una validación continua de su precisión y confiabilidad. Además, es fundamental garantizar la privacidad y seguridad de los datos utilizados en el proceso de ML, así como abordar posibles sesgos y discriminaciones inherentes en los datos y algoritmos.

**Natural Language Processing**: El procesamiento de lenguaje natural (NPL) usa el aprendizaje automático para revelar la estructura y el significado del texto. Mediante aplicaciones de procesamiento de lenguaje natural, las organizaciones pueden analizar textos y extraer información sobre personas, lugares y eventos para comprender mejor las opiniones de las redes sociales y las conversaciones de los clientes (Google, 2021).

NLP puede beneficiar a la auditoría informática al procesar y analizar grandes volúmenes de texto, como informes, correos electrónicos, documentos legales y contenido en redes sociales. El NLP permite extraer información relevante, identificar patrones, detectar anomalías y realizar clasificaciones automáticas en estos datos textuales. Además, el NLP puede facilitar la detección de riesgos y fraudes en la auditoría informática. Al analizar el lenguaje utilizado en los documentos

y comunicaciones, se pueden identificar indicios de comportamientos sospechosos o fraudulentos. Esto ayuda a los auditores a enfocar sus esfuerzos en áreas de mayor riesgo y tomar decisiones basadas en datos textuales más sólidos.

El sistema aprende a resumir automáticamente documentos de patentes con textos en lenguaje natural para cualquier dominio técnico dado. La solución de aprendizaje automático identifica terminologías clave técnicas (palabras, frases y oraciones) en el contexto de las relaciones semánticas entre las patentes de entrenamiento y los resúmenes correspondientes como el núcleo del sistema de resumen. (Amy J.C. Trappey, 2020)

Sin embargo, es fundamental abordar desafíos específicos del NLP en la auditoría informática, como la interpretación correcta de la intención y el contexto de los textos, la detección de errores y sesgos lingüísticos, y la privacidad y seguridad de los datos textuales utilizados, para lo cual necesitan ser utilizados bajo la supervisión de personal calificado.

El Procesamiento del Lenguaje Natural ofrece valiosas aplicaciones en la auditoría informática al mejorar el análisis de datos textuales, la detección de riesgos y la automatización de tareas.

**Automatización de tareas repetitivas**: La automatización de tareas repetitivas implica la implementación de técnicas de inteligencia artificial y aprendizaje automático para realizar de manera automática y eficiente actividades que antes requerían intervención manual. Esto incluye la recolección y análisis de datos, la verificación de controles y procesos, la generación de informes y otros procesos rutinarios. Debido a su intensidad laboral y la variedad de estructuras de decisiones, la auditoría ha utilizado tecnología de automatización durante más de tres décadas (Feiqi Huang, 2019).

En los últimos años, el software comercial de análisis de auditoría y las hojas de cálculo electrónicas como Microsoft Excel se han utilizado ampliamente para automatizar pruebas y análisis en la auditoría. Aunque la tecnología ha mejorado significativamente la eficiencia de la auditoría, la integración entre múltiples sistemas o aplicaciones aún es realizada principalmente por los auditores, lo que significa que la auditoría externa real sigue siendo muy laboriosa y artesanal (Feiqi Huang, 2019).

La aplicación de la automatización en la auditoría informática ofrece varios beneficios. En primer lugar, mejora la eficiencia al reducir el tiempo y los recursos requeridos para realizar tareas repetitivas. Esto permite a los auditores enfocarse en actividades más analíticas y estratégicas, como el análisis de riesgos y la evaluación de controles internos.

Además, la automatización mejora la precisión y consistencia de los procesos de revisión al minimizar el error humano y las inconsistencias en la ejecución de tareas. Los algoritmos de

aprendizaje automático pueden analizar grandes volúmenes de datos de manera rápida y precisa, identificando patrones, anomalías y tendencias que podrían pasar desapercibidos en una revisión manual.

La automatización también ayuda a mitigar el riesgo de omisiones y errores al proporcionar una monitorización continua y sistemática de los sistemas y datos. Mediante la implementación de herramientas y algoritmos automatizados, se pueden detectar de manera proactiva eventos y comportamientos anómalos, lo que permite una respuesta rápida y oportuna a posibles amenazas y vulnerabilidades.

**Detección de anomalías**: Se están generando enormes cantidades de datos todos los días mediante submedidores y sensores inteligentes instalados en edificios residenciales. Si se aprovecha adecuadamente, esos datos podrían ayudar a los usuarios finales, los productores de energía y las empresas de servicios públicos a detectar el consumo anómalo de energía y comprender las causas de cada anomalía. Por lo tanto, la detección de anomalías podría evitar que un problema menor se convierta en algo abrumador (Yassine Himeur, 2021).

Las anomalías representan desviaciones del funcionamiento previsto del sistema y pueden llevar a una disminución de la eficiencia, así como a fallas parciales o completas del sistema. Dado que las causas de las anomalías a menudo son desconocidas debido a la dinámica compleja del sistema, es necesario contar con una detección eficiente de anomalías. Los enfoques de detección convencionales se basan en métodos estadísticos y invariantes en el tiempo que no logran abordar la naturaleza compleja y dinámica de las anomalías. (Benjamin Lindemann, 2021)

La detección de comportamientos anómalos se ha convertido en una herramienta innovadora en la auditoría informática para mejorar la seguridad y detección de riesgos de los sistemas informáticos. La estrategia se basa en analizar y monitorear patrones de comportamiento de usuarios y sistemas, identificando actividades inusuales o sospechosas que puedan indicar una posible amenaza o brecha de seguridad.

En el entorno empresarial actual, donde la tecnología de la información desempeña un papel crítico en las operaciones diarias, la auditoría informática se ha convertido en una función esencial para garantizar la integridad y seguridad de los sistemas y datos de una organización. La detección de comportamiento anómalo se ha destacado como una estrategia efectiva para mejorar la seguridad cibernética y la gestión de riesgos en el ámbito de la auditoría informática. Al analizar y monitorizar los patrones de comportamiento de los usuarios y sistemas, esta estrategia permite identificar actividades inusuales o sospechosas que podrían ser indicativas de amenazas o brechas de seguridad.

Con los avances en inteligencia artificial y la creciente importancia de la detección y prevención de anomalías en varios ámbitos, los enfoques de redes neuronales artificiales permiten la detección de tipos de anomalías más complejos al considerar características temporales y contextuales (Benjamin Lindemann, 2021).

La detección de comportamiento anómalo ofrece numerosos beneficios para la auditoría informática. En primer lugar, permite una identificación temprana de actividades sospechosas, lo que facilita una respuesta rápida y proactiva ante posibles amenazas. Al analizar los patrones de comportamiento normales de los usuarios y sistemas, cualquier desviación significativa puede ser detectada y evaluada, lo que ayuda a reducir el tiempo de respuesta ante incidentes de seguridad y minimiza el impacto potencial en la organización.

Además, la detección de comportamiento anómalo mejora la eficiencia en la detección de fraudes y violaciones de políticas. Al identificar comportamientos inusuales o no autorizados, los auditores pueden enfocar sus esfuerzos en áreas de mayor riesgo y llevar a cabo investigaciones más precisas y dirigidas. Esto permite una asignación más eficiente de recursos y tiempo, evitando la revisión exhaustiva de actividades normales y enfocándose en anomalías que requieren una mayor atención.

La detección de comportamiento anómalo puede aplicarse en diferentes áreas de la auditoría informática. Por ejemplo, en la detección de fraudes, esta estrategia permite identificar patrones de comportamiento inusuales en transacciones financieras o acceso a información confidencial. Además, en la gestión de riesgos, la monitorización del comportamiento de los sistemas puede ayudar a identificar vulnerabilidades o brechas de seguridad que podrían ser aprovechadas por atacantes externos o internos.

La detección de comportamiento anómalo se presenta como una herramienta innovadora y efectiva en la auditoría informática, mejorando la seguridad y la detección de riesgos en los sistemas informáticos. Su capacidad para identificar actividades inusuales o sospechosas permite una respuesta rápida y proactiva ante posibles amenazas, así como una detección eficiente de fraudes y violaciones de políticas. Al implementar esta estrategia de manera adecuada, los auditores pueden fortalecer la seguridad de los sistemas y datos, y garantizar la integridad y confidencialidad en las organizaciones modernas.

## 4. DISCUSIÓN

La implementación de estrategias de inteligencia artificial (IA) en la auditoría informática presenta oportunidades significativas para mejorar la eficiencia y precisión del proceso de revisión. Al automatizar tareas repetitivas y analizar grandes volúmenes de datos, los auditores pueden

enfocarse en actividades analíticas y estratégicas, como la interpretación de resultados y la toma de decisiones fundamentadas.

El análisis de big data y el aprendizaje automático son estrategias de IA destacadas en la auditoría informática. El análisis de big data permite a los auditores examinar eficientemente grandes cantidades de información, identificando patrones y anomalías en los sistemas informáticos. Por otro lado, el aprendizaje automático ayuda a detectar posibles fraudes o anomalías mediante el análisis de datos históricos y la detección de patrones de comportamiento.

Es crucial abordar las preocupaciones éticas asociadas con el uso de IA en la auditoría informática. La transparencia e interpretación de los resultados generados por la IA son elementos fundamentales para asegurar la confianza en los hallazgos y decisiones. Validar adecuadamente los resultados, identificar sesgos y mantener una supervisión y revisión humana en el proceso son aspectos clave para garantizar la responsabilidad y la interpretación adecuada de los resultados generados por la IA.

La aplicación de IA en la auditoría informática brinda oportunidades para mejorar la eficiencia y precisión del proceso de revisión. Sin embargo, es esencial abordar las preocupaciones éticas, garantizar la transparencia e interpretación los resultados y mantener una supervisión humana para obtener resultados confiables y sólidos.

**Estrategias**: Las IA ofrecen un amplio potencial para mejorar la eficacia y eficiencia de la auditoría informática, tras revisar las distintas formas en las que la Inteligencia Artificial puede ayudar con los procesos de auditoría informática, se han planteado distintas estrategias para su uso efectivo:

1. *Automatización de tareas repetitivas*: La IA puede automatizar tareas rutinarias y tediosas en auditorías de TI, como la recopilación y el análisis de datos, la validación de procesos y controles, y la generación de informes. Esto ahorra tiempo y recursos a los contadores, lo que les permite concentrarse en actividades más analíticas y estratégicas.
2. *Big Data Analytics*: AI puede analizar grandes volúmenes de datos de forma rápida y precisa, lo que permite a los auditores identificar patrones, tendencias y anomalías de datos. Ayuda a detectar posibles riesgos o problemas en los sistemas informáticos y mejora la detección de fraudes.
3. *Procesamiento del lenguaje natural (NLP):* NLP permite que la inteligencia artificial comprenda y analice el lenguaje humano en documentos, correos electrónicos y otras fuentes de información textual. Ayuda a obtener información relevante, detectar riesgos y automatizar tareas de procesamiento de textos en auditorías de TI.
4. *Aprendizaje automático y detección de anomalías:* La IA puede utilizar algoritmos de aprendizaje automático para identificar patrones de comportamiento y detectar posibles anomalías o

fraudes en los sistemas informáticos. Estos modelos pueden aprender de los datos históricos y mejorar continuamente sus capacidades de detección.

5. *Integración de sistemas y datos:* La IA puede ayudar a integrar y analizar datos de diferentes sistemas y fuentes para obtener una comprensión más completa de las operaciones y procesos de una organización. Ayuda a evaluar los riesgos y controles en las auditorías de TI.
6. *Verificación e interpretación de resultados:* Es importante que los resultados que genera la IA en las auditorías informáticas sean debidamente verificados e interpretados. Esto incluye comprender los algoritmos utilizados, evaluar la precisión y confiabilidad de los resultados y asegurarse de que las decisiones basadas en IA sean comprensibles y justificadas.

Al implementar estrategias con Inteligencia Artificial, los auditores pueden optimizar el proceso de revisión, mejorar la detección de riesgos y fraudes y obtener una comprensión más completa de los sistemas informáticos de la organización. Sin embargo, es imperativo abordar las preocupaciones éticas y garantizar la validación e interpretación de los resultados generados por IA.

**Preocupaciones Éticas:** A medida que las tecnologías de inteligencia artificial (IA) se vuelven cada vez más prominentes en nuestra vida diaria, la cobertura mediática de las consideraciones éticas de estas tecnologías ha seguido el mismo camino (Leila Ouchchy, 2020). Con este aumento en la prevalencia y aplicabilidad de la IA han surgido una amplia gama de debates éticos, incluyendo cómo se puede programar a la IA para tomar decisiones morales, cómo se pueden hacer estos procesos de toma de decisiones lo suficientemente transparentes para los humanos y quién debe ser responsable de estas decisiones (Leila Ouchchy, 2020). Existen varias preocupaciones éticas relacionadas con el uso de IA en la auditoría informática. Algunas de estas preocupaciones incluyen:

1. *Privacidad y seguridad de los datos:* La auditoría informática implica el acceso y análisis de datos sensibles. Es crucial asegurar que los datos se manejen de manera segura y se cumplan todas las regulaciones y políticas de privacidad.
2. *Transparencia e Interpretación:* Las decisiones y resultados generados por las IA tienen procesos internos y algoritmos que no son fácilmente comprensibles o explicables para los humanos lo que dificulta la comprensión de cómo se llegó a dichas deducciones. Es importante promover la transparencia y garantizar que los resultados sean explicables y comprensibles para los auditores y las partes interesadas.

3. *Responsabilidad y supervisión humana:* A pesar de la automatización, los auditores deben mantener la supervisión y responsabilidad sobre las decisiones tomadas por las IA. Es necesario establecer un marco de responsabilidad clara y asegurar que los resultados de las IA sean revisados y validados por profesionales humanos.

Para abordar estas preocupaciones éticas y evaluar los resultados generados por las IA en la auditoría informática, se pueden considerar las siguientes validaciones e interpretaciones:

- *Evaluación de la calidad y confiabilidad de los datos:* Los datos utilizados para entrenar algoritmos de IA deben ser de alta calidad e imparciales. Se deben realizar validaciones y pruebas para garantizar que los datos sean representativos y confiables.
- *Interpretación e interpretación de los resultados:* Los resultados generados por la IA deben interpretarse e interpretarse de manera clara y comprensible para los auditores y las partes interesadas. Se deben dar razones y se debe explicar cómo se llegó a conclusiones y decisiones específicas.
- *Revisión y verificación humana:* Los resultados generados por IA deben ser revisados y verificados por profesionales. Los auditores deben monitorear y verificar los resultados para asegurar su precisión y cumplimiento con los objetivos de la auditoría.
- *Monitoreo y Mejora Continua:* La evaluación de los resultados generados por la IA debe ser un proceso continuo. Deben establecerse mecanismos de seguimiento y retroalimentación para identificar posibles mejoras y corregir cualquier desviación o error.

Al abordar estos problemas éticos y establecer medidas de verificación e interpretación adecuadas, es posible garantizar el uso ético y responsable de la IA en las auditorías de TI. Esto aumentará la confianza en los resultados obtenidos y garantizará que las decisiones tomadas sean justas, transparentes y creíbles.

## 5. CONCLUSIONES

La auditoría de TI ha evolucionado en respuesta a la creciente dependencia de la información en las organizaciones modernas. Su importancia radica en evaluar y garantizar la integridad, confidencialidad y disponibilidad de los sistemas y datos. Además, ayuda a asegurar el cumplimiento de leyes y regulaciones relacionadas con la protección de datos y la seguridad cibernética. La implementación de estrategias de inteligencia artificial (IA) en la auditoría de TI presenta una gran oportunidad para mejorar la eficiencia y precisión del proceso de revisión.

El análisis de Big data permite a los auditores examinar grandes volúmenes de datos, identificar patrones y anomalías, y evaluar los riesgos en los sistemas informáticos. El aprendizaje

automático es otra estrategia de IA que ayuda a detectar posibles anomalías o fraudes mediante el análisis de datos históricos y el reconocimiento de patrones de comportamiento. Estas técnicas liberan tiempo y recursos para que los auditores se enfoquen en actividades más analíticas y estratégicas.

Es importante abordar las preocupaciones éticas asociadas con el uso de IA en la auditoría de TI. La transparencia e interpretación de los resultados generados por la IA son fundamentales para mantener la confianza en los hallazgos y decisiones. Se deben implementar medidas de validación, evaluación de sesgos y discriminación, así como mantener una supervisión y revisión humana en el proceso. Al cumplir con estándares éticos y legales, la auditoría de TI puede aprovechar al máximo el potencial de la IA y obtener resultados confiables y sólidos.

## 6. REFERENCIAS


Aditya, R., & Santosa, P. (2018). Toward Modern IT Audit- Current Issues and Literature Review. *2018 4th International Conference on Science and Technology (ICST)*(doi: 10.1109/ICSTC.2018.8528627.), 1-6.

Adrian Gepp, M. K. (2018). Big data techniques in auditing research and practice:current trends and future opportunities. *Journal of Accounting Literature*, 102-115.

Amy J.C. Trappey, C. V.-L. (2020). Intelligent compilation of patent summaries using machine learning and natural language processing techniques. *Advanced Engineering Informatics*.

Benjamin Lindemann, B. M. (2021). A survey on anomaly detection for technical systems using LSTM networks. *Computers in Industry*.

Chun-Wei Tsai, C.-F. L.-C. (2015). Big data analytics: a survey. *Journal of Big Data*.

Diego A. Arcentales Fernández, X. C. (2017). Auditoría informática un enfoque efectivo. *Dominio de las ciencias*, 157-173.

Feiqi Huang, M. A. (2019). Applying robotic process automation (RPA) in auditing: A framework. *International Journal of Accounting Information Systems*.

Gómez Palanques, N. (2021). Las nuevas tecnologías y su impacto en el sector de auditoría. *Dipòsit Digital de la Universitat de Barcelona* .

Google. (2021). *Google Cloud*. Obtenido de https://cloud.google.com/learn/what-is-natural-language-processing?hl=es-419#:~:text=Natural%20language%20processing%20(NLP)%20uses,media%20sentiment%20and%20customer%20conversations.

Imbaquingo, D., Díaz, J., Saltos, T., Arciniega, S., & De La Torre, J. (2020). Análisis de las principales dificultades en la auditoría informática: una revisión sistemática de literatura. *Revista Ibérica de Sistemas e Tecnologias de Informação*, 427-440.

Leila Ouchchy, A. C. (2020). AI in the headlines: the portrayal of the ethical issues of artificial intelligence in the media. *IA and Society*.

Mahesh, B. (2018). Machine Learning Algorithms - A Review. *International Journal of Science and Research*.

Yassine Himeur, K. G. (2021). Yassine Himeur a, Khalida Ghanem b, Abdullah Alsalemi a, Faycal Bensaali a, Abbes Amira c. *Applied Energy*.