

Marco conceptual de adaptación tecnológica de las normas internacionales de auditoría (MCAT)

Conceptual framework for technological adaptation of international standards on auditing (MCAT)

González Celdrán, Debora

Departamento de Finanzas, Facultad de Economía y Empresa, Universidad de Barcelona, Av. Diagonal, 690. 08034 Barcelona, España, deboragonzalez@ub.edu, <https://orcid.org/0009-0007-1110-412X>

Debora González Celdrán, email: deboragonzalez@ub.edu

RESUMEN

La adopción acelerada de tecnologías emergentes —inteligencia artificial y machine learning, blockchain, automatización robótica de procesos (RPA) y ciberseguridad— plantea desafíos estructurales que las Normas Internacionales de Auditoría (NIAs) vigentes no abordan de forma explícita. La mayor parte de la literatura examina estas tecnologías de forma aislada, sin ofrecer un marco que articule conjuntamente las dimensiones tecnológica, normativa y ética. Este trabajo propone el Marco Conceptual de Adaptación Tecnológica (MCAT), un modelo integrador operativizado mediante una matriz aplicada a las NIAs 315, 330 y 500/520, núcleo del ciclo de riesgo en cualquier encargo de auditoría. De ella se derivan 60 ítems de control consolidados en tres tablas —una por NIA— agrupados por tecnología, que constituyen una herramienta práctica para entornos digitalmente avanzados. El artículo concluye con una hoja de ruta de adaptación normativa en cuatro fases. La principal limitación es la ausencia de validación empírica, lo que abre una agenda de investigación futura mediante estudios de caso y encuestas a profesionales del sector.

Palabras clave: NIAs; tecnologías emergentes; auditoría digital; inteligencia artificial; blockchain

Códigos JEL: M42; O33; C88

ABSTRACT

The accelerated adoption of emerging technologies —artificial intelligence and machine learning, blockchain, robotic process automation (RPA), and cybersecurity— poses structural challenges that current International Standards on Auditing (ISAs) do not explicitly address.



Most of the literature examines these technologies in isolation, without offering a framework that jointly articulates the technological, regulatory, and ethical dimensions. This paper proposes the Conceptual Framework for Technological Adaptation (MCAT), an integrative model operationalized through a matrix applied to ISAs 315, 330, and 500/520, the core of the risk cycle in any audit engagement. From it, 60 control items are derived, consolidated in three tables—one per ISA—grouped by technology, constituting a practical tool for digitally advanced environments. The paper concludes with a four-phase regulatory adaptation roadmap. The main limitation is the absence of empirical validation, which opens a future research agenda through case studies and surveys of practitioners.

Keywords: ISAs; emerging technologies; digital audit; artificial intelligence; blockchain

JEL Codes: M42; O33; C88

Recibido: 13 de octubre de 2025

Aceptado: 14 de febrero de 2026

Publicado: 1 de junio de 2026

1. Introducción

La auditoría externa atraviesa una transformación tecnológica sin precedentes. En apenas tres años, la inteligencia artificial ha pasado a analizar series completas de asientos contables en cuestión de horas, los criptoactivos han entrado en los balances de empresas cotizadas y los cierres financieros se ejecutan de forma automatizada. La proliferación de ransomware ha convertido la ciberseguridad en un componente ineludible del riesgo de auditoría. Este escenario no es una tendencia futura: es el entorno actual en el que trabaja el auditor.

Las Normas Internacionales de Auditoría (NIAs) han evolucionado a un ritmo más lento. La revisión de la NIA 315 en 2019 fue un avance necesario, pero insuficiente. Sus conceptos centrales—riesgo inherente, evidencia suficiente y apropiada, controles relevantes—fueron diseñados para entornos donde la información era documental y los procesos, humanos. Ninguno de ellos contempla explícitamente la inteligencia artificial, el blockchain, la RPA o la ciberseguridad. Esta desconexión tiene consecuencias prácticas concretas: el auditor no dispone de orientación normativa para evaluar sesgos en algoritmos de crédito, validar registros en libros mayores distribuidos bajo la NIA 500 o distinguir entre controles RPA y manuales en el marco de la NIA 330.

La literatura ha identificado estas brechas, pero analiza tecnologías y normas de forma aislada, sin marcos integradores que articulen las dimensiones tecnológica, normativa y ética (Appelbaum et al., 2017; Brown-Liburd et al., 2015; Cooper et al., 2019; Dai & Vasarhelyi,

2017). Para cubrir este vacío, el presente artículo propone el Marco Conceptual de Adaptación Tecnológica (MCAT), estructurado sobre tres ejes interdependientes y ejecutado mediante una matriz aplicada a las NIAs 315, 330 y 500/520, de la que se derivan 60 ítems de control para la práctica profesional.

2. Revisión de la Literatura

2.1. Evolución Tecnológica en la Auditoría: De los Sistemas Tradicionales a las Tecnologías Emergentes

La relación entre tecnología y auditoría llevan décadas en diálogo, aunque su intensidad se ha incrementado desde 2015. Appelbaum et al. (2017) y Cao et al. (2015) argumentan que el big data cuestiona conceptos fundacionales como el muestreo estadístico y la materialidad. Krahel y Titera (2015) añaden que procesar poblaciones completas obliga a redefinir el estándar de evidencia suficiente y apropiada de la NIA 500: la suficiencia deja de depender de la cantidad muestral para centrarse en la calidad de los datos y la fiabilidad de las herramientas analíticas. En el ámbito del blockchain, Dai y Vasarhelyi (2017) proponen auditoría continua sobre libros mayores distribuidos, argumentando que la inmutabilidad podría reducir confirmaciones con terceros. Sin embargo, Bonsón y Bednárová (2019) advierten sobre errores irreversibles en contratos inteligentes y volatilidad en criptoactivos — limitaciones que el colapso de FTX demostró con precisión: la inmutabilidad no sustituye la necesidad de control interno robusto ni de normativa específica para activos digitales (Teeter & Vasarhelyi, 2023).

Respecto a la RPA, Cooper et al. (2019) identifican el sesgo de automatización como riesgo principal, extendido por Teeter y Vasarhelyi (2023) a la IA generativa mediante el riesgo de alucinaciones en análisis financiero.

2.2. Normativa Internacional: Las NIAs ante el Desafío Digital

La revisión de la NIA 315 (2019) representa el avance más significativo del IAASB en materia tecnológica durante la última década. No obstante, la norma mantiene categorías como

"controles TI generales" y "controles de aplicación", diseñadas para sistemas ERP tradicionales, sin contemplar modelos de machine learning, contratos inteligentes ni bots RPA (Griffin & Wright, 2015; IAASB, 2020). La NIA 500 regula la evidencia sin contemplar registros blockchain, rastros de ejecución automatizada ni resultados generados por algoritmos, lo que genera incertidumbre real sobre qué constituye evidencia suficiente en estos entornos. El IAASB reconoce estas limitaciones en documentos de 2020 y 2023, aunque sin revisiones normativas concretas.

Mientras tanto, el marco regulatorio externo ha avanzado con notable rapidez. El AI Act (Reglamento UE 2024/1689), el Reglamento MiCA (2023/1114) y la Directiva NIS2 (2022/2555) imponen obligaciones de documentación, custodia y reporte de incidentes que el auditor deberá verificar, sin que las NIAs ofrezcan orientación sobre cómo incorporar estos requerimientos al programa de trabajo. Esta asimetría es ya operativa: las directrices EBA/GL/2023/01 exigen documentación exhaustiva de los modelos de IA en la gestión del riesgo crediticio, pero ninguna NIA instruye al auditor sobre cómo verificar dicho cumplimiento ni cómo evaluar si la documentación aportada es evidencia suficiente.

2.3. Ética Profesional y Riesgos Tecnológicos

Junto a las dimensiones tecnológica y normativa, la ética es un pilar estructural del MCAT, no un añadido accesorio. Floridi et al. (2018) identifican cinco principios clave —no maleficencia, beneficencia, autonomía, justicia y explicabilidad— cuya integración en el trabajo del auditor sigue siendo incipiente pese al consenso global sobre su importancia (Jobin et al., 2019)

Para el auditor, este desafío tiene tres vertientes concretas. La primera es la equidad algorítmica: determinar si las decisiones financieras automatizadas incorporan sesgos discriminatorios. La segunda es la privacidad: gestionar responsablemente el acceso masivo a datos personales en el marco del RGPD. La tercera es la explicabilidad: validar los resultados de modelos de caja negra cuya lógica interna no es observable mediante procedimientos tradicionales. El IESBA (2021) aborda estas cuestiones, aunque su integración con las NIAs sigue siendo incipiente. El riesgo de sesgo tiene un ejemplo documentado en el algoritmo de reclutamiento de Amazon (2019), cuya discriminación por género tiene un correlato exacto de los modelos de crédito hipotecario que penalizan variables proxy como el código postal.

2.4. Vacíos Identificados y Posicionamiento del Artículo

La Tabla 1 sintetiza los hallazgos por dimensión. El análisis confirma que el problema reside en la falta de integración entre dimensiones: ningún trabajo previo ha propuesto un marco que las articule simultáneamente con enfoque operativo.

Tabla 1. Síntesis de la revisión de literatura por dimensión de análisis

Dimensión	Estudios representativos	Principales hallazgos	Vacíos identificados
Tecnológica	Appelbaum et al. (2017); Cao et al. (2015); Cooper et al. (2019); Dai & Vasarhelyi (2017)	IA y big data transforman la evidencia; blockchain ofrece registros inmutables; RPA automatiza procesos clave	Falta integración normativa explícita; escasa atención a fallos masivos por automatización
Normativa	IAASB (2019, 2020, 2023); Krahel & Titera (2015); Griffin & Wright (2015)	Las NIAs presentan brechas frente a entornos digitales; la NIA 315 revisada mejora, pero es insuficiente	Sin guías específicas por tecnología; conceptos de evidencia y riesgo no actualizados
Ética	Floridi et al. (2018); Jobin et al. (2019); IESBA (2021)	Sesgo algorítmico, privacidad y transparencia son riesgos éticos emergentes en auditoría digital	Escasa integración de la ética digital en los marcos normativos de auditoría
Intersección	Brown-Liburd et al. (2015); Rezaee & Wang (2019); Bonsón & Bednárová (2019)	La interacción entre dimensiones es mayor que la suma de sus partes	Ningún trabajo previo integra las tres dimensiones con enfoque operativo

Fuente: Elaboración propia a partir de revisión de literatura.

3. Metodología

Este artículo adopta un enfoque conceptual-normativo, modalidad reconocida para marcos analíticos cuando la evidencia empírica es fragmentada (Laughlin, 1995; Humphrey & Moizer, 1990). El MCAT no pretende contrastar hipótesis empíricas, sino sistematizar en un marco coherente las brechas normativas documentadas en la literatura y derivar de ellas herramientas operativas para el auditor. Las limitaciones del enfoque son claras y se retoman en las conclusiones: el MCAT no ha sido validado mediante encuestas a auditores en activo ni mediante estudios de caso, y los ítems de verificación no han sido sometidos a pruebas de

fiabilidad inter-jueces (inter-rater reliability). Ambas limitaciones definen la agenda de investigación futura.

3.1. Selección de normas y tecnologías

La selección de las NIAs 315, 330 y 500/520 responde a un criterio funcional: estas tres normas cubren conjuntamente el ciclo completo del riesgo en cualquier encargo de auditoría:

NIA 315: Identificación de riesgos

NIA 330: Respuesta a riesgos identificados

NIA 500/520: Obtención y evaluación de evidencia

Este enfoque garantiza que las implicaciones de las brechas tecnológicas queden plenamente integradas en el análisis. Las demás normas (informes, partes relacionadas, primeras auditorías) abordan aspectos complementarios, no el núcleo del proceso de riesgo.

La selección de las cuatro tecnologías prioritarias —IA/ML, blockchain, RPA y ciberseguridad— se basa en tres criterios:

Adopción real: presentes en sistemas de entidades auditadas según Deloitte (2024) y PwC (2023); la ciberseguridad se incorpora además como tecnología transversal, dado que los ataques sobre infraestructuras financieras —ransomware, brechas de datos— afectan directamente a la integridad de la información auditada.

Regulación europea: AI Act (2024), MiCA (2023), NIS2 (2022).

Masa crítica académica: representación suficiente en la literatura para identificar riesgos diferenciados por tecnología.

Se excluyen tecnologías en fase incipiente (computación cuántica, Web3 avanzado) cuya presencia en encargos ordinarios es aún marginal.

3.2. Construcción de la MCAT

La construcción de los 60 ítems siguió tres pasos: identificación de las 18 combinaciones dimensión-tecnología como unidades de análisis; revisión sistemática de las guías del IAASB (2020, 2023), COBIT 2019, NIST Cybersecurity Framework y Código del IESBA (2021). Se consolidaron los ítems de cumplimiento por NIA y tecnología, asegurando que cada uno fuera susceptible de verificación y documentación en el informe. El resultado son 60 ítems en 12

bloques (4 tecnologías × 3 NIAs). Con esta base metodológica, la siguiente sección desarrolla la arquitectura del MCAT.

4.Marco Conceptual de Adaptación Tecnológica (MCAT)

4.1. Fundamentos teóricos y estructura matricial

El MCAT se construye sobre tres cuerpos teóricos complementarios: el modelo de riesgo de auditoría —riesgo inherente, de control y de detección—, que articula el núcleo conceptual de las NIAs seleccionadas; los marcos de gobernanza de TI COBIT 2019 y NIST Cybersecurity Framework; y la ética aplicada a la IA según el AI Act europeo y los trabajos del IESBA.

Estos fundamentos se despliegan en tres ejes operativos. El eje tecnológico comprende las características técnicas y perfiles de riesgo de cada tecnología: una misma herramienta puede ser simultáneamente objeto de auditoría e instrumento del auditor, lo que exige competencia técnica además de procedimental. El eje normativo abarca las NIAs y sus brechas, junto al marco regulatorio externo —AI Act, MiCA, NIS2 y RGPD— cuyo cumplimiento el auditor debe verificar con procedimientos que la normativa actual no detalla. El eje ético incorpora principios como transparencia, equidad, privacidad, responsabilidad y escepticismo profesional reforzado.

4.2. Dinámica de las intersecciones: La Matriz Conceptual

La propuesta de valor del MCAT reside en sus intersecciones, formalizadas en la Tabla 2. La convergencia entre tecnología y normativa ($T \leftrightarrow N$) define el ámbito del cumplimiento regulatorio digital. El AI Act clasifica los sistemas de decisión crediticia como de alto riesgo e impone obligaciones de documentación que el auditor debe verificar. El Reglamento MiCA y los estándares del GAFI añaden requisitos de custodia y transparencia sobre criptoactivos, mientras que los marcos COSO y COBIT, junto a las obligaciones sectoriales de la EBA y la CNMV, exigen que todo proceso RPA que intervenga en información financiera esté gobernado y sea reproducible. Ignorar cualquiera de estos análisis puede derivar en una opinión

que valide estados financieros con pasivos contingentes ocultos o automatización no gobernada.

La intersección tecnología-ética (T↔E) cuestiona si el sistema opera de forma justa y transparente. El auditor no solo debe validar la integridad aritmética de los algoritmos, sino también su equidad y explicabilidad, la transparencia de los contratos inteligentes y la existencia de registros auditables que garanticen la supervisión humana sobre decisiones automatizadas.

Finalmente, la relación normativa-ética (N↔E) exige una lectura conjunta del Código del IESBA y las NIAs. El escepticismo profesional evoluciona: ya no es solo una actitud frente a la dirección, sino una barrera crítica frente al sesgo de automatización de sistemas que proyectan una falsa apariencia de infalibilidad.

Tabla 2. Matriz Conceptual de Adaptación Tecnológica (MCAT)

Dimensión / Eje	IA / Machine Learning	Blockchain	RPA / Automatización
TECNOLÓGICA (Características y riesgos propios)	Opacidad algorítmica (black box); sesgo en datos de entrenamiento; dependencia de infraestructura de datos	Irreversibilidad de errores; vulnerabilidad en smart contracts; volatilidad y riesgos de custodia	Fallos masivos por lógica errónea; dependencia de sistemas legacy; ausencia de supervisión humana
NORMATIVA (Impacto en NIAs)	NIA 315: Nuevas categorías de riesgo tecnológico. NIA 330: Revisión de gobernanza. NIA 500: Explicabilidad como evidencia.	NIA 315: Riesgo de anonimato. NIA 330: Auditoría on-chain y nodos. NIA 500: Validez legal de registros distribuidos.	NIA 315: Inventario de procesos robotizados. NIA 330: Auditoría de scripts y logs. NIA 500: Suficiencia de registros de ejecución.
ÉTICA (Principios)	Equidad algorítmica; transparencia en decisiones automatizadas; privacidad de datos	Descentralización vs. responsabilidad legal; transparencia vs. derecho al olvido; ética en protocolos DeFi	Responsabilidad ante errores masivos; supervisión humana adecuada; impacto sociolaboral
INTERSECCIÓN T↔N Cumplimiento regulatorio	AI Act (UE); NIST AI RMF; borradores de guías técnicas del IAASB sobre IA	Reglamento MiCA (UE); estándares FATF/GAFI para criptoactivos; leyes nacionales de valores	Marcos COSO/COBIT; normativas sectoriales sobre control interno y automatización
INTERSECCIÓN T↔E Decisiones responsables	Principios XAI; auditoría de sesgo; revisión ética de outputs de modelos	Auditoría de código abierto; trazabilidad ética de transacciones; transparencia de gobernanza (DAO)	Supervisión humana como salvaguarda ética; logs auditables de decisiones automatizadas
INTERSECCIÓN N↔E Guías profesionales adaptadas	Código IESBA: independencia ante sistemas de IA; escepticismo profesional reforzado	Código IESBA: verificación independiente de activos digitales; conflictos de interés en DeFi	Código IESBA: supervisión del juicio humano en procesos automatizados

Fuente: Elaboración propia a partir de IAASB (2019, 2020, 2023) y revisión de literatura.

5. Listas de Verificación Operativas para Auditores

Las listas de verificación traducen las dimensiones del MCAT en interrogantes verificables que el auditor debe resolver y documentar en el expediente, consolidadas en tres tablas —una por NIA— con las cuatro tecnologías agrupadas en filas.

Tabla 3. Lista de verificación: NIA 315 (Identificación de riesgos)

Los ítems siguientes se aplican en la fase de planificación . Una respuesta negativa debe traducirse en un riesgo documentado en la evaluación.

Tecnología	Ítems de verificación
IA / Machine Learning	☐ ¿Se ha identificado el uso de modelos de IA/ML en procesos contables o de control interno relevantes?
	☐ ¿Se ha valorado el riesgo de sesgo en los datos de entrenamiento y su impacto en las decisiones financieras?
	☐ ¿Existe documentación actualizada sobre la gobernanza del modelo (versiones, reentrenamientos, validaciones)?
	☐ ¿Se evaluó la opacidad del modelo y su impacto en la capacidad de cuestionar sus resultados?
	☐ ¿Se identificaron los procesos cuyas decisiones son generadas total o parcialmente por algoritmos de IA?
	☐ ¿Se valoró el riesgo de cambios en el modelo durante el período auditado sin comunicación formal?
Blockchain	☐ ¿Se identificaron operaciones registradas en blockchain con impacto en los estados financieros?
	☐ ¿Se valoró el riesgo de errores en contratos inteligentes (smart contracts) utilizados por la entidad?
	☐ ¿Se evaluó el riesgo de pérdida de claves privadas o acceso no autorizado a wallets corporativas?
	☐ ¿Se identificó la jurisdicción regulatoria aplicable a los activos digitales ?
	☐ ¿Se valoró el riesgo de anonimidad de contrapartes en transacciones con criptoactivos?
	☐ ¿Se evaluó la irreversibilidad de errores en blockchain y su impacto financiero?
RPA / Automatización	☐ ¿Se mapearon todos los procesos contables y de control interno gestionados por bots RPA?
	☐ ¿Se identificaron los riesgos de errores masivos derivados de lógica incorrecta en scripts?
	☐ ¿Se evaluó la dependencia del RPA respecto a sistemas legacy susceptibles de cambios no controlados?
	☐ ¿Se valoró el riesgo de ausencia o insuficiencia de supervisión humana en procesos críticos?
	☐ ¿Existe un inventario actualizado de todos los bots activos, sus permisos y documentación de procesos?
	☐ ¿Se identificaron los procesos en los que el RPA puede alterar datos sin intervención humana?
Ciberseguridad	☐ ¿Se identificaron los activos de información críticos para la información financiera y su exposición a amenazas?
	☐ ¿Se valoró el riesgo de denegación de servicio sobre sistemas contables?
	☐ ¿Se evaluó la gestión de accesos privilegiados en sistemas que afectan a la información financiera?
	☐ ¿Se identificaron vulnerabilidades conocidas y no parcheadas en la infraestructura tecnológica relevante?
	☐ ¿Se valoró el riesgo derivado de proveedores o terceros con acceso a sistemas de información financiera?

Tecnología	Ítems de verificación
	☐ ¿Se evaluó la solidez del plan de continuidad de negocio ante incidentes de ciberseguridad?

Fuente: Elaboración propia a partir de IAASB (2019, 2020, 2023) y revisión de literatura.

Tabla 4. Lista de verificación: NIA 330 (Respuestas al riesgo)

Los ítems siguientes guían la ejecución de procedimientos y de controles. El auditor debe documentar el procedimiento realizado y la conclusión alcanzada.

Tecnología	Ítems de verificación
IA / Machine Learning	☐ ¿Se realizaron pruebas sobre la calidad, representatividad y actualidad de los datos de entrenamiento?
	☐ ¿Se revisó la documentación de gobernanza del modelo: políticas de reentrenamiento y umbrales de rendimiento?
	☐ ¿Se evaluó la existencia e implementación efectiva de herramientas de explicabilidad del modelo (XAI)?
	☐ ¿Se verificó que los resultados del modelo son revisados periódicamente por personal técnico competente?
	☐ ¿Se comprobó la existencia y funcionamiento de controles compensatorios ante posibles fallos del modelo?
	☐ ¿Se realizaron pruebas del modelo con datos del período auditado para verificar consistencia de resultados?
Blockchain	☐ ¿Se realizó análisis de transacciones en cadena sobre las operaciones seleccionadas?
	☐ ¿Se verificó la coherencia entre los registros blockchain y los estados financieros de la entidad?
	☐ ¿Se revisó el código de contratos inteligentes relevantes o se obtuvo informe de auditoría de código independiente?
	☐ ¿Se comprobó la validación de transacciones por múltiples nodos de la red como prueba de integridad?
	☐ ¿Se obtuvieron confirmaciones de saldos desde exploradores de bloques fiables e independientes?
	☐ ¿Se verificaron los procedimientos de custodia de claves privadas?
RPA / Automatización	☐ ¿Se revisaron los logs de ejecución de los bots RPA para el período auditado completo?
	☐ ¿Se realizaron pruebas sobre los controles que supervisan la ejecución automatizada y gestionan excepciones?
	☐ ¿Se verificó que las excepciones generadas por el RPA son gestionadas por personas competentes?
	☐ ¿Se comprobó la integridad y actualidad de la parametrización de los scripts respecto a la normativa vigente?
	☐ ¿Se realizó reconciliación entre resultados automatizados y registros manuales o fuentes independientes?
	☐ ¿Se evaluó si los cambios en scripts RPA durante el período siguieron un proceso formal de control de cambios?
Ciberseguridad	☐ ¿Se revisó la política de gestión de accesos y su aplicación efectiva en sistemas financieros clave?
	☐ ¿Se evaluó la periodicidad, cobertura y documentación de las actualizaciones y parches de seguridad?
	☐ ¿Se comprobó la existencia y funcionamiento de sistemas de detección y prevención de intrusiones (IDS/IPS)?
	☐ ¿Se revisaron los resultados de las evaluaciones de vulnerabilidades?
	☐ ¿Se verificó la existencia, actualidad y prueba periódica del plan de respuesta a incidentes de seguridad?
	☐ ¿Se evaluó la efectividad de los controles de acceso entre entornos críticos?

Fuente: Elaboración propia a partir de IAASB (2019, 2020, 2023) y revisión de literatura.

Tabla 5. Lista de verificación: NIA 500/520 (Evidencia y analíticas)

Los ítems siguientes orientan la evaluación de si las fuentes de evidencia digital cumplen los estándares de suficiencia y adecuación exigidos por las NIAs.

Tecnología	Ítems de verificación
IA / Machine Learning	☐ ¿Se obtuvo evidencia suficiente sobre la trazabilidad de las decisiones automatizadas con impacto financiero?
	☐ ¿Se documentaron los registros de versiones del modelo utilizados durante el período auditado?
	☐ ¿Se evaluó si los resultados del modelo son suficientemente comprensibles, verificables y confiables como evidencia?
	☐ ¿Se aplicaron procedimientos analíticos para detectar anomalías o patrones inusuales en resultados de IA?
	☐ ¿La evidencia obtenida es reproducible y comprensible para un auditor sin conocimiento técnico especializado?
	☐ ¿Se consideraron las limitaciones intrínsecas de los resultados de IA al evaluar la suficiencia de la evidencia?
Blockchain	☐ ¿Se utilizaron registros blockchain como evidencia y se documentó formalmente su confiabilidad?
	☐ ¿Se confirmó la integridad de los registros consultados en la cadena de bloques?
	☐ ¿Se verificó que las direcciones de billetera (wallet) utilizadas pertenecen efectivamente a la entidad auditada?
	☐ ¿Se obtuvo evidencia adecuada sobre la valoración de criptoactivos a la fecha de los estados financieros?
	☐ ¿Se documentaron las limitaciones de la evidencia blockchain?
	☐ ¿Se evaluó la confiabilidad de fuentes externas como evidencia?
RPA / Automatización	☐ ¿Se evaluó la suficiencia de los registros de RPA como evidencia respecto a la totalidad de transacciones procesadas?
	☐ ¿Se verificó que la evidencia de supervisión humana sobre el RPA está documentada en el período?
	☐ ¿Se realizaron procedimientos analíticos sobre los datos automatizados para detectar inconsistencias?
	☐ ¿Se confirmó que los reportes de excepción del RPA cubren el período completo auditado?
	☐ ¿Se valoró el riesgo de que los logs puedan ser alterados o incompletos como limitación de la evidencia?
	☐ ¿Se obtuvo evidencia independiente que corrobore los resultados de los procesos gestionados por RPA?
Ciberseguridad	☐ ¿Se obtuvo y evaluó evidencia sobre todos los incidentes de seguridad significativos del período?
	☐ ¿Se revisaron los registros de acceso a sistemas financieros como evidencia de la efectividad de controles?
	☐ ¿Se documentó la evidencia sobre pruebas de seguridad realizadas por la entidad o por terceros independientes?
	☐ ¿Se evaluó el impacto de brechas de seguridad sobre la integridad de los datos financieros?
	☐ ¿Se verificó que la evidencia digital cumple con los requisitos de cadena de custodia ?
	☐ ¿Se consideraron las limitaciones de la evidencia de ciberseguridad al formular la opinión del auditor?

Fuente: Elaboración propia a partir de IAASB (2019, 2020, 2023) y revisión de literatura.

6. Implicaciones y Hoja de Ruta de Adaptación

6.1. Para la práctica profesional

Las listas de verificación aportan valor en tres puntos: evitan olvidos al planificar, ayudan a crear metodologías propias y señalan los sectores de alto riesgo que requieren expertos

6.2. Implicaciones para el Marco Normativo del IAASB

La implementación del MCAT demuestra que actualizar las NIAs exige redefinir sus pilares conceptuales. La evidencia suficiente y adecuada (NIA 500) debe reconfigurarse para integrar registros blockchain, registros de RPA y resultados de IA. El riesgo inherente (NIA 315) debe tipificar formalmente el sesgo algorítmico como categoría de riesgo material. La última actualización de la NIA 315 requirió casi una década. Se propone que el IAASB desarrolle con carácter urgente Guías de Práctica por tecnología, coordinadas con el IESBA desde su origen.

6.3. Implicaciones para la Formación del Auditor

La estructura matricial del MCAT facilita materiales formativos que conectan principios normativos con desafíos tecnológicos concretos, evitando tanto la formación exclusivamente tecnológica como la exclusivamente normativa. Los organismos profesionales deberían incorporar el análisis de las intersecciones MCAT como competencia nuclear en sus programas de habilitación y formación continua.

6.4. Hoja de Ruta de Adaptación Progresiva

La implementación se sintetiza en una hoja de ruta de cuatro fases (Tabla 6): la Fase 1 puede iniciarse de forma inmediata; las Fases 2 y 3 requieren desarrollo coordinado de capacidades y alineación regulatoria; la Fase 4 retroalimenta el ciclo mediante evidencia empírica.

Tabla 6. Hoja de ruta de adaptación del marco de auditoría a tecnologías emergentes

Fase	Acciones clave	Actores responsables	Horizonte temporal
Fase 1 Concienciación	Formación de auditores en tecnologías emergentes; diagnóstico de brechas NIA-tecnología en firmas; difusión del MCAT como herramienta de diagnóstico	Firmas Big 4, IFAC, organismos profesionales nacionales (ICAC, ICJCE en España)	Corto plazo (1–2 años)
Fase 2 Adaptación normativa	Publicación de guías prácticas IAASB por tecnología; revisión de NIAs 315, 330 y 500 incorporando los ejes MCAT; integración coordinada con el IESBA	IAASB, IESBA, reguladores nacionales (EBA, ESMA, CNMV)	Medio plazo (2–4 años)
Fase 3 Integración operativa	Incorporación de checklists MCAT en metodologías de auditoría; desarrollo de herramientas digitales de soporte; pilotos en sectores con alta exposición tecnológica	Firmas de auditoría, desarrolladores de software de auditoría (IDEA, ACL, TeamMate)	Medio plazo (3–5 años)
Fase 4 Validación empírica	Estudios de campo para validar la eficacia del marco; análisis de encargos con alta presencia tecnológica; ajuste iterativo basado en evidencia	Academia, reguladores, organismos profesionales; grupos de investigación especializados	Largo plazo (5+ años)

Fuente: Elaboración propia.

7. Conclusiones

Este trabajo ha abordado un problema crítico: el desfase entre la normativa profesional y los entornos tecnológicamente avanzados. Las NIAs vigentes no contemplan de forma explícita el sesgo algorítmico, la evidencia basada en cadenas de bloques, los fallos sistémicos por

automatización ni los dilemas éticos derivados del uso de la IA, incrementando el riesgo de auditoría tal como evidencian los casos analizados.

El MCAT surge como propuesta integradora frente a esta carencia. Su valor fundamental reside en sus intersecciones: el cumplimiento regulatorio digital ($T \leftrightarrow N$), la dimensión de las decisiones responsables ($T \leftrightarrow E$) y la adaptación de guías profesionales ($N \leftrightarrow E$), áreas que el análisis individual de cada eje no logra explicar satisfactoriamente.

Como marco teórico, el MCAT requiere validación empírica mediante encuestas a profesionales, estudios de caso y pruebas de fiabilidad inter-jueces.

Referencias Bibliográficas

- Appelbaum, D., Kogan, A., & Vasarhelyi, M. A. (2017). Big data and analytics in the modern audit engagement: Research needs. *Auditing: A Journal of Practice & Theory*, 36(4), 1–27. <https://doi.org/10.2308/ajpt-51684>
- Bonsón, E., & Bednárová, M. (2019). Blockchain and its implications for accounting and auditing. *Meditari Accountancy Research*, 27(5), 725–740. <https://doi.org/10.1108/MEDAR-11-2018-0406>
- Brown-Liburd, H., Issa, H., & Lombardi, D. (2015). Behavioral implications of big data's impact on audit judgment and decision making and future research directions. *Accounting Horizons*, 29(2), 451–468. <https://doi.org/10.2308/acch-51023>
- Cao, M., Chychyla, R., & Stewart, T. (2015). Big data analytics in financial statement audits. *Accounting Horizons*, 29(2), 423–429. <https://doi.org/10.2308/acch-51068>
- Cooper, L. A., Holderness Jr., D. K., Sorensen, T. L., & Wood, D. A. (2019). Robotic process automation in public accounting. *Accounting Horizons*, 33(4), 15–35. <https://doi.org/10.2308/acch-52466>
- Dai, J., & Vasarhelyi, M. A. (2017). Toward blockchain-based accounting and assurance. *Journal of Information Systems*, 31(3), 5–21. <https://doi.org/10.2308/isis-51804>
- Deloitte. (2024). AI in audit: Transforming risk assessment and evidence gathering. Deloitte Insights. <https://www2.deloitte.com/insights>
- European Banking Authority (EBA). (2023). Guidelines on the use of machine learning models for internal ratings-based approaches (EBA/GL/2023/01). <https://www.eba.europa.eu>

- European Union. (2022). Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (NIS2). Diario Oficial de la Unión Europea, L 333, 80–152.
- Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., & Vayena, E. (2018). AI4People — An ethical framework for a good AI society. *Minds and Machines*, 28(4), 689–707. <https://doi.org/10.1007/s11023-018-9482-5>
- Griffin, P. A., & Wright, A. M. (2015). Commentaries on big data's importance for accounting and auditing. *Accounting Horizons*, 29(2), 377–379. <https://doi.org/10.2308/acch-51066>
- Humphrey, C., & Moizer, P. (1990). From techniques to ideologies: An alternative perspective on the audit function. *Critical Perspectives on Accounting*, 1(3), 217–238. [https://doi.org/10.1016/1045-2354\(90\)90031-7](https://doi.org/10.1016/1045-2354(90)90031-7)
- International Auditing and Assurance Standards Board (IAASB). (2019). NIA 315 (Revisada 2019): Identificación y valoración de los riesgos de incorrección material. IFAC.
- International Auditing and Assurance Standards Board (IAASB). (2020). Exploring the growing use of technology in the audit, with a focus on data analytics. IFAC. <https://www.iaasb.org>
- International Auditing and Assurance Standards Board (IAASB). (2023). Technology position paper: The use of automated tools and techniques in an audit. IFAC. <https://www.iaasb.org>
- International Ethics Standards Board for Accountants (IESBA). (2021). Technology and the code: Exploring the ethical implications of technology for professional accountants. IFAC. <https://www.ethicsboard.org>
- Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. *Nature Machine Intelligence*, 1(9), 389–399. <https://doi.org/10.1038/s42256-019-0088-2>
- Krahel, J. P., & Titera, W. R. (2015). Consequences of big data and formalization on accounting and auditing standards. *Accounting Horizons*, 29(2), 409–422. <https://doi.org/10.2308/acch-51065>
- Laughlin, R. C. (1995). Empirical research in accounting: Alternative approaches and a case for 'middle-range' thinking. *Accounting, Auditing & Accountability Journal*, 8(1), 63–87. <https://doi.org/10.1108/09513579510145>
- National Institute of Standards and Technology (NIST). (2023). Artificial intelligence risk management framework (AI RMF 1.0). U.S. Department of Commerce. <https://doi.org/10.6028/NIST.AI.100-1>
- PricewaterhouseCoopers (PwC). (2023). Global digital trust insights survey 2023. <https://www.pwc.com/gx/en/issues/cybersecurity/global-digital-trust-insights.html>

Teeter, R., & Vasarhelyi, M. A. (2023). Auditing in the age of generative AI: Challenges and opportunities. *Journal of Emerging Technologies in Accounting*, 20(1), 1–18.
<https://doi.org/10.2308/JETA-2023>