PRISMA ODS
REVISTA MULTIDISCIPLINARIA
SOBRE DESARROLLO SOSTENIBLE
ISSN: 3072-8452

CONTROL DE TI Y CONFIANZA DIGITAL: MARCO EVOLUTIVO MULTIDIMENSIONAL DEL AUDITOR DE SISTEMAS HACIA EL ASEGURAMIENTO DE CIBERSEGURIDAD

IT CONTROL AND DIGITAL TRUST: A MULTIDIMENSIONAL EVOLUTIONARY FRAMEWORK FOR SYSTEMS AUDITORS TOWARD CYBERSECURITY ASSURANCE

AUTORES/A

JUAN RIGOBERTO CASTILLO SERRACÍN
UNIVERSIDAD DE PANAMÁ
PANAMÁ

JAVIER MIGUEL GÓMEZ
UNIVERSIDAD DE PANAMÁ
PANAMÁ

CARLOS BRUCE
UNIVERSIDAD DE PANAMÁ
PANAMÁ

MARICELLA CORPAS FORD
UNIVERSIDAD DE PANAMÁ
PANAMÁ

MAURICIO RAPÓN
UNIVERSIDAD DE PANAMÁ
PANAMÁ

doi 10.65011

Volumen 5 - Número 5
2026

PRISMA ODS
REVISTA MULTIDISCIPLINARIA SOBRE DESARROLLO SOSTENIBLE
Redilat Red de Investigadores Latinoamericanos
LATINDES INSTITUTO LATINOAMERICANO EN DESARROLLO SOSTENIBLE

Control de TI y Confianza Digital: Marco Evolutivo Multidimensional del Auditor de Sistemas hacia el Aseguramiento de Ciberseguridad

IT Control and Digital Trust: A Multidimensional Evolutionary Framework for Systems Auditors toward Cybersecurity Assurance

Juan Rigoberto Castillo Serracín
juan.castillos@up.ac.pa
https://orcid.org/0009-0006-5821-7028
Universidad de Panamá
Panamá - Panamá

Carlos Bruce
carlos.bruce@up.ac.pa
https://orcid.org/0009-0004-4223-0821
Universidad de Panamá
Panamá - Panamá

Javier Miguel Gómez
javier.gomez@up.ac.pa
https://orcid.org/0009-0000-4583-5157
Universidad de Panamá
Panamá - Panamá

Maricella Corpas Ford
maricella.corpas@up.ac.pa
https://orcid.org/0000-0001-6430-4423
Universidad de Panamá
Panamá - Panamá

Mauricio Rapón
Mauricio.rapon@up.ac.pa
https://orcid.org/0009-0002-1527-6440
Universidad de Panamá
Panamá - Panamá

Artículo recibido: 20/08/2026
Aceptado para publicación: 22/09/2026

RESUMEN

La creciente interdependencia entre tecnologías digitales, ciberseguridad y gobernanza ha ampliado el alcance del auditor de tecnologías de la información y comunicación (TIC), pero la literatura aún presenta de forma fragmentada las dimensiones mediante las cuales evoluciona su capacidad de aseguramiento. Este estudio tuvo como objetivo analizar esa transformación y desarrollar el IT Auditor Evolution Framework (ITAEF). Se realizó una investigación no experimental, documental, descriptiva y analítica mediante una revisión sistematizada de literatura científica y documentación técnica especializada publicada entre 2010 y 2026. Se consideraron artículos revisados por pares en español e inglés, identificados principalmente en Scopus, Web of Science e IEEE Xplore, junto con marcos institucionales relevantes de NIST, ISACA y The Institute of Internal Auditors. Los hallazgos muestran que la evolución del auditor no responde a una trayectoria lineal ni a la sustitución de funciones tradicionales, sino a una reconfiguración multidimensional de capacidades. El ITAEF organiza esta transformación en ocho dimensiones relacionadas con alcance, riesgo, responsabilidades, competencias, técnicas, evidencia, gobernanza y naturaleza del aseguramiento, y propone cuatro orientaciones potencialmente coexistentes: control de TI, riesgo tecnológico, aseguramiento de ciberseguridad y confianza digital. Se concluye que la sofisticación tecnológica no constituye por sí sola evidencia de una transformación sustantiva; esta depende de la capacidad para sustentar conclusiones independientes, oportunas y confiables sobre riesgos digitales complejos.

Palabras clave: auditoría de tecnologías de la información, ciberseguridad, aseguramiento, confianza digital, gobernanza tecnológica

ABSTRACT

The growing interdependence among digital technologies, cybersecurity, and governance has expanded the scope of information and communication technology (ICT) auditing, yet the literature still addresses the dimensions through which assurance capabilities evolve in a fragmented manner. This study aimed to analyze this transformation and develop the IT Auditor Evolution Framework (ITAEF). A non-experimental, documentary, descriptive, and analytical design was adopted through a systematized literature review of scientific publications and specialized technical and professional documents published between 2010 and 2026. Peer-reviewed articles in English and Spanish were identified mainly through Scopus, Web of Science, and IEEE Xplore and were complemented by relevant institutional frameworks from NIST, ISACA, and The Institute of Internal Auditors. The findings indicate that auditor evolution does not follow a linear path or involve the replacement of traditional functions; rather, it reflects a multidimensional reconfiguration of assurance capabilities. The ITAEF organizes this transformation into eight dimensions related to scope, risk, responsibilities, competencies, techniques, evidence, governance, and the nature of assurance, and proposes four potentially coexisting orientations: IT control, technology risk, cybersecurity assurance, and digital trust. The study concludes that technological sophistication alone does not demonstrate substantive transformation; such transformation depends on the auditor's capacity to support independent, timely, and reliable conclusions about increasingly complex digital risks.

Keywords: information technology auditing, cybersecurity, assurance, digital trust, technology governance

INTRODUCCIÓN

La digitalización ha modificado la arquitectura sobre la cual operan las organizaciones y con ella, la naturaleza de los riesgos que deben ser comprendidos, gestionados y sometidos a aseguramiento. Procesos que antes podían depender de aplicaciones e infraestructura ubicadas dentro de límites tecnológicos relativamente definidos se ejecutan hoy mediante combinaciones de servicios en la nube, plataformas Software as a Service (SaaS), interfaces de programación de aplicaciones, identidades federadas, terceros, algoritmos y componentes automatizados. Este entorno de dependencias digitales ha ampliado el objeto de la auditoría y ha desplazado parte de su atención hacia riesgos que ya no se circunscriben a un sistema aislado. Betti y Sarens (2020) documentaron cambios en el alcance, las competencias y las prácticas de auditoría en organizaciones digitalizadas, mientras que Pizzi et al. (2021) identificaron la auditoría continua, la analítica de datos, la detección de fraude y la innovación tecnológica entre las principales líneas de transformación de la disciplina.

Este cambio coincide con una reconceptualización de la ciberseguridad como riesgo organizacional y no exclusivamente técnico. El Cybersecurity Framework 2.0 del National Institute of Standards and Technology (NIST) incorpora Govern como función transversal junto con Identify, Protect, Detect, Respond y Recover, vinculando estrategia, responsabilidades, apetito de riesgo, supervisión y cadena de suministro con la gestión general del riesgo empresarial (Pascoe et al., 2024). En este estudio, gobernanza se entiende como el sistema mediante el cual una organización establece dirección, responsabilidades y mecanismos de supervisión sobre las decisiones relacionadas con TIC, ciberseguridad y riesgo digital. Se diferencia, por tanto, de la gestión del riesgo, que identifica, analiza, trata y monitorea exposiciones, y de los controles, que materializan respuestas preventivas, detectivas o correctivas. Los tres planos se encuentran relacionados, pero constituyen objetos distintos sobre los cuales la auditoría puede proporcionar aseguramiento.

La problemática también se vincula con la Agenda 2030. Su relación más directa se encuentra con el ODS 9 (Industria, Innovación e Infraestructura), por la necesidad de infraestructuras confiables y resilientes, y con el ODS 16 (Paz, Justicia e Instituciones Sólidas), por su énfasis en eficacia, rendición de cuentas y transparencia institucional. En organizaciones dependientes de ecosistemas digitales, un aseguramiento tecnológico confiable puede contribuir a esas condiciones, sin que ello implique atribuir a la auditoría de TIC efectos directos sobre el cumplimiento de los Objetivos de Desarrollo Sostenible (Naciones Unidas, 2015).

El sujeto de esta investigación es el auditor de sistemas, entendido como el profesional de auditoría de tecnologías de la información y comunicación, funcionalmente relacionado con las denominaciones IT auditor e information systems auditor. Su actividad comprende la evaluación independiente de sistemas, infraestructura, procesos, datos, riesgos y controles tecnológicos, así como la obtención y valoración de evidencia para sustentar conclusiones de aseguramiento (Axelsen et al., 2017). Aunque puede formar parte de una función de auditoría interna, el concepto no queda limitado a esa ubicación organizacional ni resulta equivalente a otras funciones relacionadas con seguridad, riesgo o gestión tecnológica.

La ampliación del rol tampoco supone transferir responsabilidades operativas de ciberseguridad hacia auditoría. El auditor de TIC no sustituye al Chief Information Security Officer (CISO), responsable de liderar la gestión de la seguridad de la información y la ciberseguridad, ni a las operaciones de seguridad o a otras funciones encargadas directamente de administrar el riesgo. Los Global Internal Audit Standards y la actualización del Modelo de las Tres Líneas mantienen la independencia, la objetividad y la competencia como fundamentos del aseguramiento y distinguen estas responsabilidades de aquellas propias de la gestión (The Institute of Internal Auditors [IIA], 2024, 2026). La literatura sobre gobernanza de ciberseguridad refuerza esta separación al mostrar la necesidad de interacción entre CISO, auditoría, funciones de control, alta dirección y consejo sin diluir responsabilidades (Slapničar et al., 2023).

La evidencia empírica indica, además, que la transformación del rol no puede explicarse por la simple incorporación de nuevos controles o tecnologías. La efectividad de la auditoría de ciberseguridad se relaciona con factores como la madurez de la gestión del riesgo, las competencias del auditor, la calidad de la supervisión y la cooperación entre funciones responsables del riesgo (Slapničar et al., 2022; Vuko et al., 2025). Slapničar et al. (2022), por ejemplo, encontraron asociación entre mayor efectividad de la auditoría y mayor madurez de la gestión del riesgo cibernético, pero no entre una auditoría más efectiva y una menor probabilidad de sufrir un ataque exitoso. El resultado delimita la contribución de la función: la auditoría puede fortalecer la calidad del aseguramiento sobre gobernanza, riesgo y control, pero no sustituye a quienes gestionan la ciberseguridad ni puede garantizar la ausencia de incidentes.

Esta distinción es relevante porque assurance no equivale simplemente a demostrar conformidad. Spears et al. (2013) diferencian una dimensión simbólica, asociada con legitimidad y evidencia formal de cumplimiento y una dimensión sustantiva, sustentada en

capacidades suficientemente desarrolladas para proporcionar confianza razonable respecto de la gestión efectiva del riesgo. Políticas, matrices de control, certificaciones o herramientas tecnológicas pueden demostrar que determinados mecanismos existen, pero no necesariamente que funcionen con la calidad requerida para sustentar conclusiones amplias de aseguramiento. De allí surge una premisa central de este trabajo: la sofisticación tecnológica de la auditoría no constituye, por sí misma, evidencia de una transformación sustantiva de su capacidad de aseguramiento.

La transformación debe entenderse también dentro del contexto institucional en el que se desarrolla la auditoría. Las presiones regulatorias, profesionales y organizacionales modifican las expectativas respecto de lo que la función debe evaluar, mientras que la creciente interdependencia entre tecnología, ciberseguridad y negocio exige capacidades distintas de aquellas asociadas exclusivamente con el control técnico. Esta perspectiva permite interpretar la evolución del auditor como una respuesta tanto a cambios tecnológicos como a nuevas expectativas de gobernanza, evitando atribuirla automáticamente a la adopción de herramientas digitales (Volodina et al., 2023; Vuko et al., 2025).

Los marcos profesionales recientes reflejan esta ampliación del objeto de auditoría. La quinta edición del IT Audit Framework (ITAF) incorpora con mayor amplitud ecosistemas digitales, computación en la nube, inteligencia artificial y aprendizaje automático, automatización, analítica, gobierno de IA y continuous assurance (ISACA, 2026). A su vez, el Digital Trust Ecosystem Framework (DTEF) vincula la confianza digital con atributos como integridad, seguridad, privacidad, resiliencia, calidad y confiabilidad de las interacciones digitales (ISACA, 2024). Estas aproximaciones muestran que el aseguramiento se extiende más allá de la verificación aislada de controles; no demuestran, sin embargo, que todas las funciones de auditoría evolucionen de la misma forma ni que la confianza digital constituya una etapa final de la profesión.

En este estudio, evolución no se utiliza como sinónimo de madurez ni presupone una progresión lineal, irreversible o universal. Se refiere a la transformación temporal, funcional y profesional del auditor de TIC frente a cambios en la naturaleza del riesgo, las expectativas de gobernanza, las capacidades requeridas y el alcance del aseguramiento. El calificativo multidimensional reconoce, además, que esos cambios pueden producirse a ritmos distintos en el objeto y alcance de auditoría, la orientación frente al riesgo, las competencias, las tecnologías y técnicas utilizadas, la naturaleza y temporalidad de la evidencia, las relaciones con actores

de gobernanza y el tipo de conclusiones que pueden sustentarse. Una función puede exhibir capacidades avanzadas en analítica o ciberseguridad y conservar aproximaciones tradicionales en gobernanza, evaluación del riesgo o calidad de la evidencia. En consecuencia, control de TI, riesgo tecnológico, aseguramiento de ciberseguridad y confianza digital se consideran únicamente orientaciones heurísticas iniciales, potencialmente coexistentes, y no etapas de una escala predefinida.

Revisiones recientes confirman que la transformación del campo ya es visible. Tharwat et al. (2025) cartografiaron la investigación sobre ciberseguridad y auditoría interna entre 2014 y 2024, mientras que Omousha et al. (2026) identificaron un desplazamiento desde aproximaciones predominantemente técnicas y de cumplimiento hacia temas de gobernanza, auditoría interna y tecnologías emergentes. El problema pendiente no es demostrar que el auditor está cambiando, sino explicar la arquitectura de ese cambio. La literatura aborda modificaciones en alcance, competencias, adopción tecnológica, efectividad de la auditoría de ciberseguridad, relaciones entre actores y calidad del aseguramiento, pero estas dimensiones permanecen parcialmente fragmentadas.

Ese vacío resulta especialmente visible al diferenciar modificación de las prácticas y transformación de la capacidad de aseguramiento. Auditar servicios cloud, utilizar analítica avanzada o incorporar ciberseguridad al plan de auditoría constituye evidencia de cambio, pero no permite determinar por sí solo si la función está en condiciones de obtener y evaluar evidencia suficiente, apropiada y confiable sobre la adecuación de la gobernanza, la gestión del riesgo y los controles tecnológicos. La cuestión relevante deja de ser cuántas tecnologías nuevas puede auditar el profesional y pasa a ser qué calidad, oportunidad y alcance de conclusión puede sustentar frente a un entorno de riesgo crecientemente interdependiente.

A partir de este vacío se formula la pregunta rectora del estudio: si el riesgo tecnológico ha cambiado sustancialmente, ¿en qué dimensiones ha cambiado también la capacidad del auditor de TIC para proporcionar aseguramiento independiente y cómo puede representarse esa transformación de manera conceptualmente consistente y empíricamente defendible? De ella se derivan tres preguntas de investigación: RQ1: ¿Qué transformaciones en el rol del auditor de TIC documenta la literatura frente a la evolución del riesgo tecnológico y de ciberseguridad? RQ2: ¿Qué dimensiones permiten caracterizar de manera sistemática esas transformaciones en términos de capacidad de aseguramiento? RQ3: ¿Cómo se articulan las dimensiones identificadas y qué orientaciones, configuraciones o patrones de evolución del rol pueden

derivarse de la evidencia disponible? RQ1 y RQ2 se abordan mediante revisión sistematizada y codificación temática y conceptual, mientras que RQ3 orienta la síntesis integradora y la construcción del marco.

El objetivo general es analizar la evolución multidimensional del rol del auditor de sistemas frente a la transformación del riesgo tecnológico y desarrollar un marco conceptual que caracterice los cambios en su capacidad para proporcionar formas más amplias de aseguramiento de ciberseguridad y confianza digital. Como resultado de este propósito se propone el IT Auditor Evolution Framework (ITAEF), denominación asignada en este estudio al Marco Evolutivo Multidimensional del Auditor de Sistemas. El ITAEF constituye una propuesta conceptual propia orientada a representar cómo se transforma la capacidad de aseguramiento del auditor de TIC frente a la evolución del riesgo tecnológico y de ciberseguridad. Su estructura no parte de niveles previamente demostrados ni presupone una trayectoria universal; control de TI, riesgo tecnológico, aseguramiento de ciberseguridad y confianza digital operan inicialmente como categorías orientadoras cuya naturaleza y relaciones son contrastadas mediante el análisis documental.

El ITAEF examina la transformación del rol a partir del objeto y alcance de auditoría, orientación frente al riesgo, funciones y responsabilidades, competencias profesionales, tecnologías y técnicas, características de la evidencia, relaciones de gobernanza y naturaleza de las conclusiones de aseguramiento. Su contribución teórica consiste en relacionar estos componentes para distinguir entre una ampliación instrumental de la práctica y una transformación sustantiva de la capacidad de aseguramiento. En el plano metodológico, busca convertir una narrativa profesional ampliamente reconocida en una arquitectura conceptual susceptible de análisis sistemático y posterior operacionalización; en el plano práctico, pretende ofrecer un lenguaje diagnóstico para identificar desalineaciones entre las capacidades de una función de auditoría y la complejidad del entorno tecnológico que pretende asegurar.

Desde esta perspectiva, evolucionar no significa abandonar los fundamentos históricos de control, independencia, objetividad y juicio profesional ni considerar la confianza digital como el destino inevitable de una trayectoria profesional. Significa ampliar la capacidad del auditor para relacionar riesgo, gobernanza, evidencia y control y, sobre esa base, sustentar conclusiones independientes frente a entornos digitales cada vez más interdependientes. Esta es la cuestión que fundamenta la construcción del ITAEF.

METODOLOGÍA

Diseño de la investigación

La investigación se desarrolló mediante un diseño no experimental, documental, descriptivo y analítico, orientado a examinar la evolución del rol del auditor de tecnologías de la información y comunicación (TIC) frente a la transformación del riesgo tecnológico, la ciberseguridad y las nuevas demandas de aseguramiento digital. El estudio se fundamentó en una revisión sistematizada de literatura científica y documentación técnica especializada, cuyos hallazgos fueron integrados mediante análisis temático y conceptual para construir el IT Auditor Evolution Framework (ITAEF).

Participantes y unidad de análisis

Por su naturaleza documental, la investigación no involucró participantes humanos. La unidad de análisis estuvo constituida por artículos científicos y documentos técnicos relacionados con auditoría de TIC, auditoría de sistemas de información, ciberseguridad, riesgo tecnológico, gobernanza, aseguramiento y confianza digital; por tanto, no resultaron aplicables variables demográficas, error estándar ni margen de error propios de estudios con muestras poblacionales.

Procedimiento de selección documental

La selección documental se realizó mediante criterios de elegibilidad previamente definidos. Se consideraron publicaciones comprendidas entre 2010 y 2026, identificadas principalmente en Scopus, Web of Science e IEEE Xplore, mediante combinaciones de términos como IT audit, information systems audit, cybersecurity, cyber risk, technology risk, cybersecurity assurance, digital assurance y digital trust.

Se incluyeron artículos revisados por pares, publicados en español o inglés, relacionados con auditoría de TIC, ciberseguridad, riesgo tecnológico, gobernanza o aseguramiento digital, y que aportaran información sobre cambios en funciones, competencias, alcance, técnicas, evidencia o capacidad de aseguramiento del auditor. Se excluyeron registros duplicados, estudios sin relación directa con las preguntas de investigación, trabajos exclusivamente financieros sin componente tecnológico y publicaciones técnicas de ciberseguridad que no abordaran auditoría, gobernanza, riesgo o aseguramiento. De manera complementaria, se consideraron marcos y documentos profesionales de organismos como ISACA, NIST y The

Institute of Internal Auditors cuando resultaron necesarios para contextualizar conceptos, responsabilidades y estándares profesionales.

La búsqueda y actualización documental se cerró el 7 de agosto de 2026. Tras la aplicación de los criterios de elegibilidad definidos, el corpus científico final analizado estuvo constituido por 23 artículos publicados en revistas científicas revisadas por pares. De manera complementaria, se incorporaron cinco documentos técnico-profesionales de NIST, ISACA y The Institute of Internal Auditors, seleccionados por su pertinencia para contextualizar marcos, responsabilidades y estándares profesionales vinculados con la construcción del ITAEF. Estos documentos se utilizaron como apoyo conceptual y normativo y no como sustitutos de la evidencia científica revisada por pares. Adicionalmente, se utilizó un documento institucional de las Naciones Unidas para contextualizar la relación del estudio con la Agenda 2030 y los Objetivos de Desarrollo Sostenible.

Técnicas de recolección de datos

La técnica utilizada fue el análisis documental. Los registros recuperados fueron revisados inicialmente mediante título y resumen y, posteriormente, mediante lectura del texto completo cuando cumplían los criterios establecidos. La información relevante se organizó en una matriz de extracción que incluyó autor, año, objetivo, contexto, características del rol del auditor, alcance, orientación frente al riesgo, competencias, tecnologías y técnicas utilizadas, características de la evidencia, relaciones con actores de gobernanza y naturaleza del aseguramiento descrito.

Procedimiento de análisis

La información se analizó mediante análisis temático y conceptual de contenido, combinando una lógica deductiva e inductiva. Como categorías sensibilizadoras iniciales se consideraron el objeto y alcance de auditoría, la orientación frente al riesgo, las funciones y responsabilidades, las competencias profesionales, las tecnologías y técnicas, las características de la evidencia, las relaciones con actores de gobernanza y la naturaleza de las conclusiones de aseguramiento. Estas categorías se utilizaron como puntos iniciales de observación derivados de las preguntas de investigación y de la literatura revisada, y no como dimensiones predeterminadas del ITAEF.

Durante el análisis, las categorías sensibilizadoras fueron contrastadas con la evidencia documental y pudieron ser confirmadas, agrupadas, subdivididas, redefinidas o

complementadas de acuerdo con la recurrencia de los conceptos, su diferenciación conceptual y la consistencia observada entre las fuentes. La comparación entre los documentos permitió reconocer transformaciones recurrentes, relaciones entre categorías y patrones conceptuales, así como distinguir entre cambios instrumentales en las prácticas de auditoría y transformaciones sustantivas en la capacidad de aseguramiento. A partir de este proceso se determinaron las categorías con suficiente capacidad explicativa para ser retenidas posteriormente como dimensiones del marco.

Construcción del ITAEF

A partir de la síntesis de los hallazgos se desarrolló el IT Auditor Evolution Framework (ITAEF), organizando las categorías recurrentes en dimensiones conceptuales relacionadas con la transformación del rol del auditor de TIC. Las nociones de control de TI, riesgo tecnológico, aseguramiento de ciberseguridad y confianza digital se utilizaron como categorías orientadoras y no como niveles previamente establecidos.

La estructura del marco se sustentó en la recurrencia de los conceptos identificados, la consistencia entre las fuentes y su capacidad para explicar las preguntas de investigación. En consecuencia, el ITAEF se presenta como un marco conceptual derivado de evidencia documental y no como una escala de madurez validada empíricamente.

Rigor metodológico y consideraciones éticas

Para fortalecer la trazabilidad del estudio se documentaron las etapas de búsqueda, selección, exclusión, extracción y análisis de los documentos, aplicando de manera consistente los criterios de inclusión y exclusión definidos. Asimismo, se diferenció entre evidencia científica revisada por pares y documentación técnico-normativa utilizada como apoyo contextual.

Por tratarse de una investigación documental, no se involucraron participantes humanos ni se trataron datos personales. El estudio utilizó únicamente literatura científica y documentación técnica previamente publicada, respetando los principios de atribución, trazabilidad de las fuentes e integridad académica mediante la adecuada citación y referencia de los documentos analizados.

RESULTADOS Y DISCUSIÓN

Los resultados se presentan a partir de la síntesis e integración de la evidencia documental seleccionada, con el propósito de responder de manera progresiva a las preguntas de

investigación y sustentar la construcción del IT Auditor Evolution Framework (ITAEF). El análisis se organiza desde la identificación de las principales transformaciones observadas en el rol del auditor de TIC, continúa con la delimitación de las dimensiones que permiten caracterizar dicha evolución y culmina con el examen de sus relaciones y posibles configuraciones. La discusión se integra de forma transversal a los resultados, contrastando los hallazgos con la literatura especializada y evitando asumir de manera previa una trayectoria lineal o universal de evolución profesional.

Caracterización general de los hallazgos

El análisis de la literatura muestra que la transformación del auditor de TIC no puede explicarse adecuadamente como una simple incorporación progresiva de nuevas herramientas. La evidencia examinada describe modificaciones simultáneas en el alcance de auditoría, la naturaleza de los riesgos considerados, las competencias requeridas, las formas de obtener evidencia, la relación con otros actores de gobernanza y el tipo de aseguramiento que puede proporcionarse. Los trabajos iniciales sobre el auditor de sistemas lo situaban principalmente como un especialista encargado de apoyar la evaluación de sistemas y controles tecnológicos; investigaciones posteriores muestran un desplazamiento hacia riesgos digitales que atraviesan procesos, proveedores, arquitecturas distribuidas y estructuras de gobierno organizacional (Axelsen et al., 2017; Betti & Sarens, 2020; Slapničar et al., 2023).

Este desplazamiento tampoco significa la desaparición de las funciones tradicionales. La evaluación de controles generales de TI, accesos, cambios, continuidad, configuración o integridad de datos continúa siendo necesaria; lo que cambia es el contexto dentro del cual esos controles adquieren significado. La digitalización amplía el alcance de las funciones de auditoría y aumenta la relevancia de los riesgos tecnológicos, particularmente los asociados con ciberseguridad, mientras que las técnicas analíticas comienzan a modificar la forma cotidiana de ejecutar los trabajos. Betti y Sarens (2020) identificaron cambios en alcance, conocimientos requeridos y prácticas de trabajo, mientras que Betti et al. (2021) encontraron que mayores niveles de digitalización organizacional se relacionan con un mayor uso de analítica de datos en auditoría. La revisión bibliométrica de Pizzi et al. (2021) converge con estos resultados al identificar auditoría continua, detección de fraude, analítica de datos e innovación tecnológica como núcleos diferenciados de transformación.

Los hallazgos permiten, por tanto, descartar una interpretación estrictamente sustitutiva de la evolución profesional. El control de TI no es reemplazado por el riesgo tecnológico, ni este

desaparece cuando la función incorpora aseguramiento de ciberseguridad. Más bien, se observa una acumulación y recombinación de capacidades, cuya configuración depende de la naturaleza del entorno tecnológico y de las responsabilidades que la organización atribuye a la función de auditoría. En este contexto, Calvin et al. (2025) examinan las características del involucramiento de la actividad de auditoría interna en ciberseguridad y TI, aportando evidencia reciente sobre la ampliación de su participación en estos ámbitos. Esta interpretación es consistente con la evidencia de Slapničar et al. (2023), quienes identifican configuraciones distintas en la distribución de responsabilidades de ciberseguridad, y con Vuko et al. (2025), quienes muestran que la efectividad del aseguramiento de ciberseguridad depende, entre otros factores, de la profesionalización del auditor, las competencias del consejo y la cooperación con las funciones responsables del riesgo.

Transformaciones del rol del auditor de TIC frente al riesgo digital: respuesta a RQ1

La primera transformación identificada afecta al objeto de auditoría. En una orientación predominantemente tradicional, el objeto se encuentra delimitado por aplicaciones, infraestructura, controles generales de TI, procesamiento de información y cumplimiento de procedimientos establecidos. Axelsen et al. (2017) documentan esta especialización al estudiar el papel del auditor de sistemas dentro de auditorías financieras, donde su contribución depende en gran medida de la relevancia de los sistemas para el trabajo principal. Sin embargo, la digitalización reduce la utilidad de concebir el objeto auditado exclusivamente como un sistema delimitado, porque procesos críticos dependen actualmente de combinaciones de servicios cloud, terceros, identidades, datos, automatización y componentes interconectados. Betti y Sarens (2020) observaron precisamente que la digitalización amplía el alcance esperado de la auditoría y aumenta la importancia de los riesgos relacionados con TI y ciberseguridad.

Una segunda transformación se produce en la orientación frente al riesgo. La auditoría de TIC deja de concentrarse exclusivamente en comprobar si determinados controles existen y comienza a evaluar si los mecanismos de gobernanza, gestión y control responden razonablemente a una exposición tecnológica cambiante. Esta diferencia es fundamental para el ITAEF. Slapničar et al. (2022) desarrollaron un índice de efectividad de auditoría de ciberseguridad basado en planificación, ejecución e información y encontraron una asociación positiva entre mayor efectividad de la auditoría y mayor madurez de la gestión del riesgo cibernético. Sin embargo, no encontraron que una auditoría de ciberseguridad más efectiva estuviera asociada con una menor probabilidad de sufrir un ataque exitoso. El resultado

delimita el alcance del aseguramiento: la auditoría puede fortalecer la calidad con la que una organización conoce y gestiona su exposición, pero no puede garantizar la ausencia de incidentes.

Este hallazgo permite distinguir conceptualmente efectividad del aseguramiento de efectividad operacional de la ciberseguridad. Una función de auditoría puede proporcionar evidencia sólida sobre la adecuación del gobierno, la gestión del riesgo y los controles sin convertirse en responsable de prevenir ataques. Esta diferencia preserva la independencia del auditor y evita atribuirle resultados pertenecientes al Chief Information Security Officer (CISO), responsable de liderar la gestión de la seguridad de la información y la ciberseguridad en la organización, a las operaciones de seguridad o a otras funciones responsables directamente de administrar el riesgo tecnológico. La investigación de Steinbart et al. (2012) ya señalaba que auditoría interna y seguridad de la información pueden generar beneficios cuando mantienen una relación constructiva, pero partiendo de responsabilidades diferenciadas. Estudios posteriores han ampliado esta perspectiva hacia configuraciones de gobernanza donde seguridad, CISO, auditoría, dirección ejecutiva y consejo participan en líneas distintas de responsabilidad y rendición de cuentas (Slapničar et al., 2023).

La tercera transformación se refiere a la evidencia. Las aproximaciones tradicionales, construidas alrededor de muestras, revisión documental y comprobaciones efectuadas en momentos determinados, conviven progresivamente con fuentes de mayor volumen, granularidad y continuidad. El process mining, por ejemplo, permite analizar poblaciones completas de eventos almacenados en sistemas empresariales y reconstruir cómo se ejecutan realmente los procesos, en lugar de depender exclusivamente de procedimientos declarados o muestras limitadas (Jans et al., 2013). Werner et al. (2021) muestran que estas técnicas pueden incorporarse a procedimientos contemporáneos de auditoría y fortalecer la robustez de la evidencia, mientras que Yoon et al. (2015) advierten que el volumen de datos no convierte automáticamente esa información en evidencia suficiente, apropiada y confiable.

La transformación de la evidencia introduce una consecuencia menos evidente: el cambio tecnológico no elimina el problema del juicio profesional, sino que lo desplaza. Barr-Pulliam et al. (2024), al revisar la literatura sobre tecnología, evidencia y juicio, muestran que analítica, automatización y aprendizaje automático pueden ampliar las posibilidades de identificación de anomalías y análisis de poblaciones, pero requieren evaluar confiabilidad, relevancia y suficiencia de la información utilizada. Samiolo et al. (2024) llegan a una conclusión

convergente desde otra perspectiva: la automatización de tareas aparentemente rutinarias puede eliminar espacios donde se desarrollan deliberación, interpretación y aprendizaje profesional. De esta manera, un auditor tecnológicamente avanzado no es aquel que sustituye indiscriminadamente el juicio por algoritmos, sino aquel capaz de determinar cuándo y bajo qué condiciones la evidencia generada tecnológicamente puede sostener una conclusión de aseguramiento.

La cuarta transformación corresponde a la temporalidad del aseguramiento. La literatura sobre auditoría continua cuestiona el desfase entre la velocidad con que ocurren los eventos digitales y la periodicidad con que tradicionalmente son examinados. Chan y Vasarhelyi (2011) plantearon tempranamente que la automatización permitía aproximar auditoría y aseguramiento a entornos económicos en tiempo real; posteriormente, Jans y Hosseinpour (2019) combinaron minería de procesos, minería de datos y conocimiento del auditor para abordar verificaciones continuas de transacciones. La evolución reciente del process mining mantiene esa dirección, aunque también evidencia barreras organizacionales y metodológicas que impiden considerar estas técnicas como prácticas universalmente adoptadas (Föhr et al., 2025).

Finalmente, los resultados muestran una transformación de la posición relacional del auditor. En ciberseguridad, la calidad del aseguramiento no depende solamente de las competencias individuales del especialista, sino también de su acceso a información relevante, la interacción con las funciones de gestión del riesgo y el respaldo de los órganos de supervisión. Vuko et al. (2025) encontraron que la profesionalización de los auditores, las competencias del consejo, el apoyo del consejo a la auditoría de ciberseguridad y la cooperación con las primeras líneas explican significativamente su efectividad. En la misma línea, Alzeban et al. (2026) examinan la calidad de las auditorías de ciberseguridad desde la perspectiva de las sinergias entre el chief audit executive, la gobernanza de TI y la función de auditoría interna, reforzando la relevancia de las relaciones institucionales dentro del aseguramiento de ciberseguridad. El resultado es importante porque sitúa la evolución profesional fuera de una lógica exclusivamente individual: una función con personal técnicamente competente puede continuar proporcionando aseguramiento limitado si su posición dentro de la arquitectura de gobernanza restringe acceso, interacción o capacidad de comunicar conclusiones.

En respuesta a RQ1, la evidencia permite concluir que la evolución del auditor de TIC se expresa mediante un desplazamiento desde objetos tecnológicos relativamente delimitados

hacia ecosistemas de riesgo interdependiente; desde la comprobación de controles hacia la evaluación de gobernanza, riesgo y control; desde evidencia principalmente periódica y muestral hacia evidencia digital de mayor cobertura y potencial continuidad; desde competencias fundamentalmente técnico-auditoras hacia combinaciones de auditoría, ciberseguridad, analítica y juicio profesional; y desde una interacción especializada con TI hacia una posición de aseguramiento integrada en estructuras más amplias de gobernanza. Ninguno de estos desplazamientos implica abandono de las capacidades anteriores; representan una ampliación del conjunto de problemas sobre los cuales el auditor debe estar en condiciones de formular conclusiones defendibles.

Dimensiones de la evolución de la capacidad de aseguramiento: respuesta a RQ2

La codificación y comparación conceptual de los hallazgos confirmó y refinó las categorías sensibilizadoras iniciales, permitiendo organizar la transformación observada en ocho dimensiones interrelacionadas. Estas dimensiones no constituyen niveles de madurez ni variables independientes en sentido estadístico. Funcionan como ejes analíticos que permiten describir qué aspecto del rol está cambiando y, especialmente, evitar que la adopción de una tecnología sea utilizada como indicador único de evolución profesional.

Tabla 1

Dimensiones propuestas del ITAEF

DIMENSIÓN	***PREGUNTA ANALÍTICA***	***TRANSFORMACIÓN OBSERVADA***
D1. Objeto y alcance	¿Qué se audita?	De sistemas, aplicaciones y controles delimitados hacia procesos digitales, servicios cloud, terceros y ecosistemas tecnológicos.
D2. Orientación frente al riesgo	¿Desde qué lógica se determina qué evaluar?	De cumplimiento y control hacia riesgo tecnológico, riesgo cibernético y exposición digital integrada al riesgo empresarial.
D3. Funciones y responsabilidades	¿Qué papel cumple el auditor?	De especialista evaluador de TI hacia proveedor independiente de aseguramiento sobre riesgos tecnológicos complejos, sin asumir su gestión.
D4. Competencias profesionales	¿Qué debe saber interpretar?	De conocimiento de controles y sistemas hacia capacidades combinadas de auditoría, ciberseguridad, datos, tecnologías emergentes y juicio profesional.

D5. Tecnologías y técnicas de auditoría	¿Cómo se ejecuta la evaluación?	De procedimientos manuales y herramientas tradicionales hacia analítica, automatización, process mining, IA y técnicas de auditoría continua.
D6. Evidencia	¿Con qué información se sustenta la conclusión?	De evidencia predominantemente documental y muestral hacia poblaciones digitales, registros, telemetría y evidencia potencialmente continua, manteniendo criterios de suficiencia y confiabilidad.
D7. Relaciones de gobernanza	¿Con quién debe interactuar el auditor?	De interacción principalmente con TI hacia relaciones estructuradas con seguridad, riesgo, dirección ejecutiva, comités y consejo.
D8. Naturaleza del aseguramiento	¿Qué puede concluir razonablemente?	De conformidad de controles hacia conclusiones más amplias sobre gobernanza, gestión del riesgo, resiliencia y condiciones que sustentan confianza digital.

Fuente: Elaboración propia a partir de la síntesis temática y conceptual de la literatura revisada.

La primera implicación de esta estructura es que la evolución puede ser asimétrica. Una función puede utilizar analítica avanzada y process mining —D5— y continuar dependiendo de evidencia poco confiable —D6—, poseer escasa interacción con el consejo —D7— o mantener un alcance limitado a verificaciones de cumplimiento —D1 y D8—. Del mismo modo, una función puede tener una sólida orientación al riesgo y una posición institucional adecuada sin haber automatizado significativamente sus procedimientos. La evidencia sobre digitalización respalda precisamente esta heterogeneidad: la adopción de analítica aumenta con la digitalización organizacional, pero no constituye por sí misma evidencia de que haya cambiado la naturaleza del aseguramiento producido (Betti et al., 2021; Pizzi et al., 2021).

Esta distinción permite separar sofisticación instrumental de capacidad sustantiva de aseguramiento, que constituye uno de los resultados centrales del estudio. Spears et al. (2013) diferencian una dimensión simbólica del aseguramiento —capaz de proporcionar legitimidad y señales de conformidad— de una dimensión sustantiva sustentada en capacidades suficientemente desarrolladas para mejorar la gestión del riesgo de seguridad. Aplicado al ITAEF, disponer de dashboards, algoritmos, herramientas automatizadas, certificaciones o matrices extensas no demuestra por sí mismo que una función pueda producir conclusiones más sólidas. Para que exista transformación sustantiva deben cambiar de manera coherente la calidad de la evidencia, la comprensión del riesgo, las competencias, el alcance y la capacidad para comunicar conclusiones relevantes a los responsables de gobernanza.

La dimensión de evidencia adquiere en este punto un papel articulador. Analizar el cien por ciento de una población puede mejorar cobertura respecto de una muestra, pero no corrige automáticamente problemas de procedencia, integridad o interpretación de los datos. Yoon et al. (2015) conceptualizan el big data como evidencia complementaria y no como sustituto automático de otras fuentes; Barr-Pulliam et al. (2024) muestran igualmente que la tecnología modifica la evaluación de evidencia sin eliminar los requisitos de escepticismo y juicio. Por ello, el ITAEF no considera "más datos" como equivalente a "más aseguramiento": el elemento relevante es la capacidad para transformar datos verificables en evidencia suficiente y apropiada para la conclusión que se pretende sostener.

En respuesta a RQ2, las ocho dimensiones identificadas permiten caracterizar de manera más precisa la evolución porque trasladan la unidad de análisis desde las herramientas utilizadas hacia la capacidad de aseguramiento. La pregunta deja de ser si el auditor utiliza inteligencia artificial, analítica o auditoría continua y pasa a ser qué objeto puede evaluar, qué riesgo comprende, qué evidencia obtiene, con quién necesita interactuar y qué conclusión independiente está legítimamente en condiciones de emitir.

Articulación multidimensional y construcción del ITAEF: respuesta a RQ3

El análisis conjunto de las dimensiones no respalda una progresión universal en la que todas las organizaciones deban transitar obligatoriamente por una serie de niveles predeterminados. La literatura muestra configuraciones heterogéneas y dependientes del contexto. Slapničar et al. (2023), por ejemplo, identifican diferentes configuraciones en las líneas de responsabilidad de gobernanza de ciberseguridad; Vuko et al. (2025) demuestran que algunas fuerzas institucionales y organizacionales explican la efectividad de auditoría mientras otras no producen los efectos esperados. La transformación del rol resulta así más consistente con una lógica configuracional que con una escala única de madurez.

A partir de esta evidencia, el ITAEF propone cuatro orientaciones de aseguramiento que funcionan como tipos conceptuales y no como escalones obligatorios: control de TI, riesgo tecnológico, aseguramiento de ciberseguridad y confianza digital. Cada orientación representa una combinación distinta de alcance, riesgo, evidencia, competencias, relaciones y naturaleza de la conclusión. Una misma función puede presentar características de varias orientaciones simultáneamente, especialmente durante procesos de transformación o cuando diferentes trabajos de auditoría requieren capacidades distintas.

Tabla 2

Configuraciones orientadoras del ITAEF

ORIENTACIÓN	***OBJETO PREDOMINANTE***	***LÓGICA PRINCIPAL***	***EVIDENCIA CARACTERÍSTICA***	***RELACIÓN DE GOBERNANZA***	***RESULTADO DE ASEGURAMIENTO***
Control de TI	Sistemas, aplicaciones y controles	Conformidad y funcionamiento de controles	Documentos, configuraciones, muestras y pruebas periódicas	TI y responsables del proceso	Adecuación y funcionamiento de controles determinados
Riesgo tecnológico	Procesos y dependencias tecnológicas críticas	Exposición y priorización basada en riesgo	Evidencia de controles integrada con análisis de riesgo	TI, riesgo, negocio y comités	Razonabilidad de la respuesta frente al riesgo tecnológico
Aseguramiento de ciberseguridad	Superficie de riesgo, capacidades de protección, detección, respuesta y recuperación	Riesgo cibernético y resiliencia	Logs, configuraciones, telemetría, pruebas técnicas, analítica y evidencia de gobernanza	CISO, seguridad, riesgo, alta dirección y consejo	Conclusión independiente sobre gobernanza y gestión del riesgo cibernético
Confianza digital	Ecosistemas, datos, terceros, IA, privacidad, resiliencia e interacciones digitales	Confiabilidad del ecosistema y expectativas de partes interesadas	Evidencia multidominio y potencialmente continua	Gobernanza empresarial y actores internos y externos relevantes	Aseguramiento sobre condiciones que sustentan interacciones digitales confiables

Fuente: Elaboración propia a partir de la integración conceptual de los hallazgos de la revisión.

La primera orientación, control de TI, conserva el núcleo histórico de la disciplina y continúa siendo indispensable. Su limitación aparece cuando el perímetro de evaluación se confunde con el perímetro real del riesgo. Un control puede funcionar conforme a diseño dentro de una aplicación y, al mismo tiempo, formar parte de un proceso cuya exposición depende de identidades externas, servicios cloud o terceros que quedan fuera del alcance. La segunda orientación, riesgo tecnológico, amplía la pregunta desde "¿funciona el control?" hacia "¿es este el riesgo que debería estar cubriendo el aseguramiento y es razonable la respuesta organizacional?". Esta modificación coincide con el cambio de alcance descrito por Betti y

Sarens (2020) y con la creciente integración del riesgo tecnológico en mecanismos organizacionales de supervisión.

La tercera orientación, aseguramiento de ciberseguridad, introduce una diferencia cualitativa. Aquí no basta con auditar controles de seguridad de manera aislada; el auditor debe estar en condiciones de evaluar la coherencia entre gobernanza, exposición, capacidades y evidencia. El trabajo de Slapničar et al. (2022) proporciona apoyo empírico a esta distinción al mostrar que la efectividad de la auditoría de ciberseguridad comprende planificación, ejecución y comunicación y se relaciona con la madurez de la gestión del riesgo. A ello se añade la evidencia de Vuko et al. (2025), que vincula efectividad con competencias, respaldo del consejo y cooperación interfuncional. En consecuencia, el aseguramiento de ciberseguridad no constituye simplemente "auditoría de TI con controles adicionales"; modifica las relaciones organizacionales y la naturaleza de las conclusiones necesarias.

La cuarta orientación, confianza digital, requiere mayor cautela conceptual. La literatura disponible no permite afirmar que la confianza digital sea una etapa final demostrada empíricamente de la profesión. Resulta más defendible interpretarla como una ampliación potencial del objeto de aseguramiento hacia condiciones de seguridad, integridad, privacidad, resiliencia, transparencia y confiabilidad que atraviesan ecosistemas digitales. En este estudio, la confianza digital se aborda como un constructo multidimensional en el que la seguridad constituye uno de sus componentes, pero no su totalidad, interpretación consistente con el enfoque ecosistémico del Digital Trust Ecosystem Framework (DTEF) de ISACA (2024). Por su parte, la quinta edición del IT Audit Framework (ITAF) amplía el alcance de auditoría hacia computación en la nube, inteligencia artificial y aprendizaje automático, automatización, gobernanza de IA, analítica, aseguramiento continuo y consideraciones vinculadas con confianza digital (ISACA, 2026).

Este resultado impide establecer una equivalencia causal entre auditoría y confianza digital. El auditor puede proporcionar aseguramiento sobre condiciones que contribuyen a la confiabilidad, pero no producir confianza por sí mismo ni garantizarla. La confianza depende también de desempeño, comportamiento organizacional, seguridad, privacidad, calidad del servicio y percepciones de distintas partes interesadas. Esta delimitación es consistente con la distinción entre aseguramiento simbólico y sustantivo propuesta por Spears et al. (2013): una certificación, opinión o evidencia formal puede contribuir a legitimidad, pero su existencia no demuestra automáticamente capacidades efectivas de gestión del riesgo.

De esta forma, la respuesta a RQ3 es que las dimensiones del ITAEF se articulan mediante configuraciones parciales y potencialmente coexistentes, no mediante una secuencia rígida. La evolución puede representarse como una reconfiguración del centro de gravedad de la función de auditoría, mediante combinaciones de capacidades que permiten abarcar riesgos más interdependientes, evidencia más dinámica y relaciones de gobernanza más complejas. Una función puede encontrarse avanzada en D5 —tecnología de auditoría— y rezagada en D7 —gobernanza—; otra puede presentar un alcance propio del aseguramiento de ciberseguridad y seguir utilizando evidencia predominantemente periódica. El concepto de evolución multidimensional adquiere precisamente su utilidad al hacer visibles estas desalineaciones.

La integración de estos hallazgos permite representar visualmente el ITAEF como una arquitectura multidimensional de capacidades de aseguramiento. Como se observa en la Figura 1, las ocho dimensiones identificadas funcionan como ejes interrelacionados del marco, mientras que control de TI, riesgo tecnológico, aseguramiento de ciberseguridad y confianza digital se representan como orientaciones conceptuales potencialmente coexistentes. La disposición no secuencial de estas orientaciones busca reflejar que la evolución del auditor no constituye una progresión lineal ni una escala de madurez, sino una reconfiguración diferenciada de capacidades cuyo grado de desarrollo puede variar entre dimensiones y contextos organizacionales.

Figura 1. Marco Evolutivo Multidimensional del Auditor de Sistemas hacia el Aseguramiento de Ciberseguridad (ITAEF)

Fuente: Elaboración propia a partir de la síntesis temática y conceptual de la literatura revisada.

Implicaciones teóricas del ITAEF

La principal contribución teórica derivada de los resultados consiste en desplazar el criterio de evolución desde lo que el auditor utiliza hacia lo que el auditor está en condiciones de asegurar. Esta distinción modifica la interpretación habitual de la transformación digital de la auditoría. Analítica, inteligencia artificial, automatización o process mining pueden aumentar cobertura, velocidad y capacidad analítica, pero su valor para el aseguramiento depende de que produzcan evidencia confiable y sean integradas dentro de un proceso de juicio profesional apropiado. La investigación contemporánea sobre tecnología y auditoría respalda esta cautela: las herramientas pueden ampliar la capacidad de análisis y simultáneamente introducir nuevos problemas de dependencia, interpretación o juicio (Barr-Pulliam et al., 2024; Samiolo et al., 2024).

Esta perspectiva también explica por qué el ITAEF no debe interpretarse como una taxonomía de herramientas. La utilización de inteligencia artificial en una auditoría no implica, por sí sola, que la función de auditoría se encuentre orientada hacia la confianza digital, de la misma forma que analizar logs no demuestra por sí solo una capacidad sustantiva de aseguramiento de ciberseguridad. La revisión de Wassie y Lakatos (2024) reconoce el potencial de la inteligencia artificial para automatizar procedimientos y ampliar servicios de valor, pero también

documenta una adopción todavía desigual y ausencia de marcos suficientemente consolidados para su integración. Estudios recientes sobre juicio del auditor muestran asimismo que la interacción entre profesionales y sistemas automatizados genera problemas específicos de confianza, interpretación y dependencia de la evidencia tecnológica (Barr-Pulliam et al., 2024; Samiolo et al., 2024).

Una segunda contribución consiste en situar la gobernanza como dimensión constitutiva del aseguramiento y no solamente como contexto externo. El Cybersecurity Framework 2.0 del National Institute of Standards and Technology incorporó Govern como función transversal para relacionar estrategia, responsabilidades y riesgo cibernético con la gestión empresarial, mientras que la evidencia empírica muestra que el apoyo del consejo y la interacción entre auditoría y otras líneas contribuyen a explicar la efectividad del aseguramiento de ciberseguridad. De manera paralela, los estándares profesionales de auditoría mantienen competencia, objetividad, posición independiente, supervisión y calidad de la evidencia como fundamentos de la función. En consecuencia, ampliar el alcance de auditoría no significa transferir al auditor funciones de gestión; significa elevar su capacidad para evaluar de forma independiente cómo esas funciones administran el riesgo.

La tercera contribución corresponde a la diferenciación entre cambio instrumental y transformación sustantiva. Un cambio instrumental modifica herramientas, velocidad o eficiencia de procedimientos; una transformación sustantiva modifica la capacidad para formular una conclusión más amplia, oportuna y defendible sobre un riesgo relevante. Esta distinción ofrece una explicación para situaciones en las que organizaciones tecnológicamente sofisticadas mantienen aproximaciones de aseguramiento relativamente tradicionales. También evita confundir modernización técnica con evolución profesional y proporciona un criterio conceptual susceptible de ser operacionalizado posteriormente.

Síntesis de las preguntas de investigación

Tabla 3

Respuestas derivadas del análisis

PREGUNTA	***SÍNTESIS DE LA RESPUESTA***
RQ1. ¿Qué transformaciones documenta la literatura?	Ampliación del objeto de auditoría, mayor orientación al riesgo, incorporación de ciberseguridad, nuevas competencias, analítica y automatización, evidencia digital de mayor cobertura y temporalidad, mayor interacción con actores de gobernanza y ampliación de las conclusiones de aseguramiento.
RQ2. ¿Qué dimensiones caracterizan esas transformaciones?	Ocho dimensiones: objeto y alcance; orientación frente al riesgo; funciones y responsabilidades; competencias; tecnologías y técnicas; evidencia; relaciones de gobernanza; y naturaleza del aseguramiento.
RQ3. ¿Cómo se articulan y qué patrones pueden derivarse?	Las dimensiones configuran perfiles heterogéneos y no necesariamente lineales. Control de TI, riesgo tecnológico, aseguramiento de ciberseguridad y confianza digital pueden interpretarse como orientaciones coexistentes cuyo grado de expresión varía entre dimensiones y contextos.

Fuente: Elaboración propia a partir de la síntesis de los resultados de la investigación.

En conjunto, los resultados respaldan un Marco Evolutivo Multidimensional del Auditor de Sistemas hacia el Aseguramiento de Ciberseguridad en el que la evolución no se determina por la cantidad de tecnologías adoptadas ni por el abandono de las funciones históricas de control. El cambio sustantivo ocurre cuando la función desarrolla la capacidad de obtener y evaluar evidencia suficientemente sólida para emitir conclusiones independientes sobre riesgos cuya naturaleza supera el perímetro tradicional de los sistemas individuales. Bajo esta interpretación, la confianza digital constituye una orientación de aseguramiento de mayor amplitud conceptual, pero no una etapa final demostrada ni un resultado atribuible exclusivamente a auditoría.

El ITAEF propone, por tanto, comprender la evolución profesional como una reconfiguración de capacidades de aseguramiento. Esta formulación permite explicar por qué dos funciones que utilizan tecnologías semejantes pueden diferir considerablemente en el alcance y calidad de sus conclusiones, así como por qué una función puede presentar simultáneamente características tradicionales y avanzadas. Más que clasificar auditores en una jerarquía, el marco busca identificar dónde se producen las transformaciones, dónde persisten desalineaciones y hasta qué punto la capacidad de aseguramiento responde a la complejidad del riesgo tecnológico que pretende evaluar.

CONCLUSIÓN

El presente estudio examinó la transformación del rol del auditor de tecnologías de la información y comunicación (TIC) frente a la creciente complejidad del riesgo digital y, a partir de la síntesis de la evidencia documental, fundamentó la construcción conceptual del IT Auditor Evolution Framework (ITAEF). Los hallazgos indican que esta evolución no responde a una trayectoria lineal, jerárquica ni basada en la sustitución de funciones históricas, sino a un proceso acumulativo y multidimensional. La evaluación de controles generales y específicos de TI continúa siendo un componente esencial del aseguramiento; sin embargo, su alcance resulta insuficiente cuando se analiza de forma aislada frente a entornos caracterizados por servicios en la nube, terceros, arquitecturas distribuidas, automatización, datos y riesgos de ciberseguridad interdependientes. En este contexto, la función de auditoría requiere articular el análisis de controles con una comprensión más amplia de gobernanza, riesgo tecnológico, resiliencia y dependencias digitales.

La principal aportación conceptual del estudio consiste en diferenciar sofisticación instrumental de capacidad sustantiva de aseguramiento. La incorporación de analítica avanzada, process mining, automatización o inteligencia artificial puede ampliar la cobertura, velocidad y profundidad de los procedimientos de auditoría, pero no constituye por sí misma evidencia de una transformación sustantiva de la función. El cambio adquiere relevancia cuando esas capacidades permiten obtener y evaluar evidencia suficiente, apropiada y confiable, interpretar riesgos tecnológicos complejos y sustentar conclusiones independientes útiles para los órganos de gobernanza. La tecnología modifica, por tanto, los medios disponibles para el auditor, pero no sustituye el juicio profesional, la independencia ni la responsabilidad de evaluar críticamente la evidencia sobre la cual se fundamenta el aseguramiento.

Esta distinción resulta particularmente relevante en ciberseguridad. Una función de auditoría puede contribuir a evaluar la adecuación de la gobernanza, la gestión del riesgo y los controles sin asumir responsabilidades operativas correspondientes al Chief Information Security Officer (CISO), a las operaciones de seguridad o a otras funciones encargadas directamente de gestionar el riesgo. La evolución propuesta por el ITAEF implica ampliar la capacidad de evaluación independiente y no transferir responsabilidades entre líneas organizacionales. De esta manera, el aseguramiento de ciberseguridad se diferencia tanto de la administración directa de los controles como de la simple comprobación de su existencia.

Los resultados permiten asimismo delimitar el papel de la confianza digital dentro del marco. Esta no debe interpretarse como una etapa final garantizada de la evolución del auditor ni como un resultado atribuible exclusivamente a la función de auditoría. Se configura, más bien, como un ámbito más amplio en el que convergen condiciones relacionadas con integridad, privacidad, seguridad, resiliencia y confiabilidad de los ecosistemas digitales. Sobre estas condiciones el auditor puede proporcionar aseguramiento razonable, pero no certeza absoluta. En consecuencia, las cuatro orientaciones propuestas por el ITAEF —control de TI, riesgo tecnológico, aseguramiento de ciberseguridad y confianza digital— representan configuraciones conceptuales potencialmente coexistentes y no niveles obligatorios de una escala de madurez.

Esta interpretación constituye una de las implicaciones centrales del carácter multidimensional del ITAEF. Una función de auditoría puede disponer de tecnologías avanzadas y, simultáneamente, presentar limitaciones en la calidad de la evidencia, la orientación frente al riesgo, la interacción con los órganos de gobernanza o el alcance de sus conclusiones. De forma inversa, una función con una sólida orientación al riesgo y adecuada integración institucional puede mantener procedimientos tecnológicos relativamente tradicionales. El marco permite hacer visibles estas posibles desalineaciones al examinar conjuntamente ocho dimensiones: objeto y alcance de auditoría, orientación frente al riesgo, funciones y responsabilidades, competencias profesionales, tecnologías y técnicas utilizadas, características de la evidencia, relaciones de gobernanza y naturaleza del aseguramiento proporcionado.

Desde la perspectiva del desarrollo sostenible, los resultados presentan una relación principalmente con los ODS 9 y 16 de la Agenda 2030. Una capacidad de aseguramiento tecnológico independiente y adecuadamente alineada con la complejidad del riesgo digital puede contribuir al fortalecimiento de infraestructuras y procesos digitales confiables y resilientes, vinculados con el ODS 9, así como favorecer condiciones de rendición de cuentas, supervisión y transparencia institucional relacionadas con el ODS 16. Esta relación debe entenderse como una contribución potencial a dichas condiciones y no como evidencia de un efecto causal directo del ITAEF sobre el cumplimiento de los Objetivos de Desarrollo Sostenible.

El estudio presenta como principal limitación su naturaleza documental y conceptual. El ITAEF se deriva de la integración de literatura científica y documentación técnico-profesional y, por tanto, no constituye todavía un instrumento validado empíricamente para medir

capacidades organizacionales. Esta limitación abre una línea directa de investigación orientada a su operacionalización y contrastación en diferentes contextos organizacionales y sectores económicos. Estudios posteriores podrían examinar el comportamiento de sus dimensiones mediante estudios de caso, investigaciones comparativas y diseños cuantitativos, así como analizar su aplicabilidad frente a entornos caracterizados por servicios en la nube, inteligencia artificial, cadenas de suministro digitales, terceros y mecanismos de aseguramiento continuo.

En síntesis, el ITAEF propone comprender la evolución del auditor de sistemas no por la cantidad de tecnologías que incorpora a su práctica, sino por la transformación de la capacidad de aseguramiento que puede sostener de manera independiente sobre un entorno de riesgo digital cada vez más complejo. Desde esta perspectiva, evolucionar no significa abandonar el control de TI, sino ampliar y reconfigurar la capacidad para relacionar controles, riesgos, evidencia, gobernanza y juicio profesional en conclusiones de aseguramiento relevantes para organizaciones cuya operación depende crecientemente de ecosistemas digitales interconectados.

REFERENCIAS

Alzeban, A., Al-Hajaya, K., Sawan, N., Chammaa, H., & Foster, S. (2026). The quality of cybersecurity audits: Do synergies among the chief audit executive, IT governance and internal audit functions matter? Managerial Auditing Journal, 41(2), 322–349. https://doi.org/10.1108/MAJ-05-2025-4825

Axelsen, M., Green, P., & Ridley, G. (2017). Explaining the information systems auditor role in the public sector financial audit. International Journal of Accounting Information Systems, 24, 15–31. https://doi.org/10.1016/j.accinf.2016.12.003

Barr-Pulliam, D., Calvin, C. G., Eulerich, M., & Maghakyan, A. (2024). Audit evidence, technology, and judgement: A review of the literature in response to ED-500. Journal of International Financial Management & Accounting, 35(1), 36–67. https://doi.org/10.1111/jifm.12192

Betti, N., & Sarens, G. (2020). Understanding the internal audit function in a digitalised business environment. Journal of Accounting & Organizational Change, 17(2), 197–216. https://doi.org/10.1108/JAOC-11-2019-0114

Betti, N., Sarens, G., & Poncin, I. (2021). Effects of digitalisation of organisations on internal audit activities and practices. Managerial Auditing Journal, 36(6), 872–888. https://doi.org/10.1108/MAJ-08-2020-2792

Calvin, C. G., Eulerich, M., & Holt, M. (2025). Characteristics of cybersecurity and IT involvement by the IA activity. International Journal of Accounting Information Systems, 56, 100726. https://doi.org/10.1016/j.accinf.2025.100726

Chan, D. Y., & Vasarhelyi, M. A. (2011). Innovation and practice of continuous auditing. International Journal of Accounting Information Systems, 12(2), 152–160. https://doi.org/10.1016/j.accinf.2011.01.001

Föhr, T. L., Reichelt, V., Marten, K.-U., & Eulerich, M. (2025). A framework for the structured implementation of process mining for audit tasks. International Journal of Accounting Information Systems, 56, 100727. https://doi.org/10.1016/j.accinf.2025.100727

The Institute of Internal Auditors. (2024). Global Internal Audit Standards. https://www.theiia.org/en/standards/2024-standards/global-internal-audit-standards/

The Institute of Internal Auditors. (2026). Three Lines Model: Assurance and advice in support of effective governance. https://www.theiia.org/en/standards/documents/

ISACA. (2024). Digital Trust Ecosystem Framework (DTEF). https://www.isaca.org/digital-trust

ISACA. (2026). IT Audit Framework (ITAF): A professional practices framework for IT audit (5th ed.). https://www.isaca.org/resources/it-audit

Jans, M., Alles, M., & Vasarhelyi, M. (2013). The case for process mining in auditing: Sources of value added and areas of application. International Journal of Accounting Information Systems, 14(1), 1–20. https://doi.org/10.1016/j.accinf.2012.06.015

Jans, M., & Hosseinpour, M. (2019). How active learning and process mining can act as continuous auditing catalyst. International Journal of Accounting Information Systems, 32, 44–58. https://doi.org/10.1016/j.accinf.2018.11.002

Naciones Unidas. (2015). Transformar nuestro mundo: La Agenda 2030 para el Desarrollo Sostenible (A/RES/70/1). https://sdgs.un.org/es/2030agenda

Omousha, M. M., Al-Zoubi, J. H., Bani Yaseen, O. K., AlNsour, S., Al Ebbini, M., & Al Sardi, A. D. A. (2026). The role of IT audit and management in cybersecurity governance: A bibliometric review. EDPACS. Advance online publication. https://doi.org/10.1080/07366981.2026.2631887

Pascoe, C., Quinn, S., & Scarfone, K. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

Pizzi, S., Venturelli, A., Variale, M., & Macario, G. P. (2021). Assessing the impacts of digital transformation on internal auditing: A bibliometric analysis. Technology in Society, 67, 101738. https://doi.org/10.1016/j.techsoc.2021.101738

Samiolo, R., Spence, C., & Toh, D. (2024). Auditor judgment in the fourth industrial revolution. Contemporary Accounting Research, 41(1), 498–528. https://doi.org/10.1111/1911-3846.12901

Slapničar, S., Axelsen, M., Bongiovanni, I., & Stockdale, D. (2023). A pathway model to five lines of accountability in cybersecurity governance. International Journal of Accounting Information Systems, 51, 100642. https://doi.org/10.1016/j.accinf.2023.100642

Slapničar, S., Vuko, T., Čular, M., & Drašček, M. (2022). Effectiveness of cybersecurity audit. International Journal of Accounting Information Systems, 44, 100548. https://doi.org/10.1016/j.accinf.2021.100548

Spears, J. L., Barki, H., & Barton, R. R. (2013). Theorizing the concept and role of assurance in information systems security. Information & Management, 50(7), 598–605. https://doi.org/10.1016/j.im.2013.08.004

Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2012). The relationship between internal audit and information security: An exploratory investigation. International Journal of Accounting Information Systems, 13(3), 228–243. https://doi.org/10.1016/j.accinf.2012.06.007

Tharwat, H., Hafez, S. T., Elgohary, I. E., & Hassanein, A. (2025). A decade of cybersecurity research in internal auditing: Bibliometric mapping and future research agenda. Discover Sustainability, 6, 1066. https://doi.org/10.1007/s43621-025-02031-w

Volodina, T., Grossi, G., & Vakulenko, V. (2023). The changing roles of internal auditors in the Ukrainian central government. Journal of Accounting & Organizational Change, 19(6), 1–23. https://doi.org/10.1108/JAOC-04-2021-0057

Vuko, T., Slapničar, S., Čular, M., & Drašček, M. (2025). Key drivers of cybersecurity audit effectiveness: A neo-institutional perspective. International Journal of Auditing, 29(1), 188–206. https://doi.org/10.1111/ijau.12365

Wassie, F. A., & Lakatos, L. P. (2024). Artificial intelligence and the future of the internal audit function. Humanities and Social Sciences Communications, 11, 386. https://doi.org/10.1057/s41599-024-02905-w

Werner, M., Wiese, M., & Maas, A. (2021). Embedding process mining into financial statement audits. International Journal of Accounting Information Systems, 41, 100514. https://doi.org/10.1016/j.accinf.2021.100514

Yoon, K., Hoogduin, L., & Zhang, L. (2015). Big data as complementary audit evidence. Accounting Horizons, 29(2), 431–438. https://doi.org/10.2308/acch-51076

: https://doi.org/10.65011/prismaods.v5.i5.342

Cómo citar este artículo (APA 7ª edición):
Castillo Serracín, J. R., Bruce, C., Gómez, J. M., Corpas Ford, M., & Rapón, M. (2026). Control de TI y Confianza Digital: Marco Evolutivo Multidimensional del Auditor de Sistemas hacia el Aseguramiento de Ciberseguridad. *Prisma ODS: Revista Multidisciplinaria Sobre Desarrollo Sostenible*, 5(5), 1-30. https://doi.org/10.65011/prismaods.v5.i5.342