Madurez digital y su correlación en la planificación de la auditoría interna de empresas de Paraguay en el año 2025

Jorge Rojas Barra
Universidad Autónoma de Encarnación - UNAE, Paraguay

En un contexto de creciente transformación digital, la adaptación de la función de auditoría interna es fundamental. Sin embargo, su estado en economías emergentes como la paraguaya ha sido escasamente estudiado. Esta investigación tuvo como objetivo analizar la correlación entre el nivel de madurez digital percibido por las organizaciones de Paraguay y el grado de enfoque en riesgos tecnológicos observado en el plan anual del área en empresas de dicho país. Para ello, se empleó un enfoque cuantitativo con un diseño explicativo-correlacional, aplicando un cuestionario a una muestra no probabilística de dieciocho profesionales de la disciplina. Los principales hallazgos revelan un nivel de madurez digital intermedio, pero "desequilibrado", con mayor adopción de herramientas tecnológicas que de capacidades de gobernanza. Así, se encontró una correlación positiva y no estadísticamente significativa. Se concluye que la adaptación de la función de la tercera línea de defensa en Paraguay a la era digital es un proceso incipiente, pues existe una brecha crítica frente a los cambios más recientes en los estándares internacionales. Esta desconexión se explica por la tensión institucional y el sesgo de comodidad profesional, factores que llevan a la priorización de áreas de control tradicional en desmedro de los riesgos tecnológicos.

Palabras clave: auditoría interna, madurez digital, riesgos tecnológicos, plan de auditoría

Digital maturity and its correlation in internal audit planning of Paraguay companies in 2025

In a context of growing digital transformation, adaptation of internal audit function is crucial despite its poorly studied status in emerging economies such as Paraguay. This study aimed at analyzing the correlation between the digital maturity level perceived by Paraguay organizations and the extent of the approach of

https://doi.org/10.18800/contabilidad.202601.002
Contabilidad y Negocios 21 (41) 2026 / e-ISSN 2221-724X

technology risks observed in the annual plan of the area in Paraguay companies. To such purpose, a quantitative approach with an explanatory correlational design was used, applying a questionnaire to a non-probability sample of eighteen professionals of this field. The main findings reveal an intermediate, yet unbalanced, level of digital maturity, with greater use of technology tools than governance capacities, resulting in a positive correlation and not statistically significant. Therefore, it is concluded that adaptation to the digital era of the third defense line function in Paraguay is emerging, evidencing a critical breach as to the most recent changes in international standard. This disconnection is a consequence of the institutional tension and professional comfort bias, which prioritize traditional control areas to the detriment of technology risks.

Keywords: internal audit, digital maturity, technology risks (IT risks), audit plan

Maturidade digital e sua correlação no planejamento da auditoria interna em empresas do Paraguai no ano de 2025

Em um contexto de crescente transformação digital, a adaptação da função de auditoria interna é fundamental, mas seu status em economias emergentes como o Paraguai tem sido pouco estudado. Este estudo teve como objetivo analisar a correlação entre o nível de maturidade digital percebido pelas organizações do Paraguai e o grau de foco em riscos tecnológicos observado no planejamento anual da área de auditoria interna em empresas paraguaias. Para tanto, se utilizou uma abordagem quantitativa com esquema explicativo-correlacional, aplicando um questionário a uma amostra não probabilística de dezoito profissionais da área. Os principais resultados revelam um nível intermediário de maturidade digital, porém "desequilibrado", com maior adoção de ferramentas tecnológicas do que de capacidades de governança, onde foi encontrada uma correlação positiva e não estatisticamente significativa. Conclui-se que a adaptação da função da terceira linha de defesa no Paraguai à era digital é um processo incipiente, com uma lacuna crítica existente em relação às mudanças mais recentes nas normas internacionais. Essa desconexão se explica pela tensão institucional e pelo viés de conforto profissional, fatores que levam à priorização de áreas de controle tradicional em detrimento dos riscos tecnológicos.

Palavras-chave: auditoria interna, maturidade digital, riscos tecnológicos, plano de auditoria

1. Introducción

En el marco de la cuarta revolución industrial, las compañías necesitarán desarrollar nuevos modelos de negocio, y, principalmente, repensar su modelo de operaciones, considerar cómo atraerán e impulsarán el talento digital, y redefinir cómo medirán el éxito de sus organizaciones. Por ello, las compañías deben fortalecer su paquete de herramientas estratégicas, asegurarse de que el ciclo de aprobaciones de nuevas iniciativas es suficientemente ágil e incluir explícitamente elementos digitales en los planes estratégicos de las organizaciones (World Economic Forum, 2016).

Datos recientes del sector tecnológico refieren que solamente el 3 % de compañías se perciben “maduras” en lo que respecta a ciberseguridad, mientras que un 71 % indica tenerun nivel considerado como “en formación” y un 11 % refiere considerarse en nivel principiante . En ese sentido, es significativamente importante generar un proceso de actualización de competencias (*upskilling*) del talento para asegurar que las brechas existentes identificadas puedan cerrarse (Cisco, 2024)[1].

Reportes especializados de la industria listan, dentro de los temas cruciales, la capacidad de dicha área de construir capacidades digitales[2]. Se destaca también que muchas funciones de aseguramiento han comenzado la implementación de competencias digitales, pero que la adopción aún es limitada, y se encuentra enfocada única y principalmente en temas de muestreo y entrevistas

A nivel regional, organismos multilaterales describen a las tecnologías digitales como instrumentos esenciales para impulsar la productividad y el crecimiento (Comisión Económica para América Latina y el Caribe [CEPAL], 2022). En ese mismo contexto, los principales obstáculos que impiden una mayor adopción digital en el mundo empresarial son la falta de capacidades al interior de las compañías al igual que el limitado acceso al financiamiento por parte de estas, tal como se señala en diagnósticos sobre digitalización en América Latina (Álvarez & Toledo, 2022).

Informes de seguridad informática reportan que al menos el 30 % de las empresas de la región sufrieron por lo menos un incidente de ciberseguridad recientemente (ESET, 2024). En esa misma línea, el reporte subraya que una de cada cinco empresas que no sufrieron ataques de esa naturaleza manifiesta no disponer de mecanismos que pudieran prevenir un potencial ataque. El reporte concluye también que el 23 % de las empresas encuestadas registró al menos un intento de *ransomware* en los últimos dos años.

En el contexto actual de transformación digital, se observa la existencia de una necesidad crítica de evolución por parte de la tercera línea de defensa, motivada por avances tecnológicos, a efectos de que el área mantenga su relevancia y cumpla con su rol de agregar valor (Abdullah & Almaqtari, 2024). En este sentido, los principales obstáculos identificados están asociados por una creciente presión regulatoria y una

---

1 El reporte de Cisco (2024) evalúa la preparación de las empresas ante las amenazas actuales. Además, resalta la correlación existente entre los incidentes de seguridad y la falta de talento.

2 Véase, por ejemplo, el reporte de la consultora Deloitte (2024), que sitúa a la digitalización y la ciberseguridad como aspectos de destacada relevancia.

brecha en las habilidades tecnológicas emergentes, por parte de los colaboradores del área (Eulerich & Bonrath, 2025).

Según datos de observatorios digitales de la región, Paraguay se encuentra en una posición intermedia en comparación con otros países de Latinoamérica, con indicadores mixtos. Los indicadores de conexiones a banda ancha móvil como porcentaje de la población y personas usuarias de internet se encuentran por encima del promedio regional, en niveles del 111 % y 76.3 %, respectivamente, frente a niveles de 103 % y 72.8 % (CEPAL, 2023). Por otro lado, la misma fuente también señala que los indicadores de infraestructura fija y velocidad de descarga se encuentran por debajo del promedio regional. Así, se pone de manifiesto un problema de conectividad asociado a la calidad[3].

Los indicadores mencionados reflejan que el acceso principal de las personas a internet se da a través de la vía móvil (celulares), mientras que el acceso a través de computadoras se encuentra todavía rezagado frente al promedio regional. Esta disparidad sugiere que la digitalización en el país está dada, principalmente, por el acceso móvil individual, mientras que la infraestructura necesaria para una digitalización empresarial profunda aún presenta desafíos.

El gobierno del Paraguay ha lanzado, en conjunto con el Banco Interamericano de Desarrollo (BID), el programa denominado Plan Nacional TIC 2022-2030. En este, el país establece una hoja de ruta para el desarrollo digital nacional, con el objetivo de construir un país más conectado, digitalizado y seguro (Ministerio de Tecnologías de la Información y Comunicación [Mitic], 2022). El Plan Nacional TIC 2022-2030 reconoce las tecnologías de información (TIC) como un elemento transversal y fundamental para alcanzar la competitividad económica, la transparencia en la gestión pública y la reducción de las brechas sociales (Mitic, 2022).

A nivel local, la ausencia de datos sobre la función de control de la tercera línea de defensa es palpable. No existen registros unificados que permitan conocer qué cantidad de empresas cuenta con una estructura de aseguramiento ni cómo dicha función está compuesta. Asimismo, no hay datos relativos a los planes y programas del área, ni desde el punto de vista administrativo-financiero, ni tecnológico, ni de ciberseguridad.

Un aspecto crítico derivado de lo anterior es la inexistencia de investigaciones empíricas locales que midan la correlación entre el nivel de madurez digital de las organizaciones empresariales y el grado de cobertura de riesgos tecnológicos en los planes de aseguramiento de la tercera línea de defensa. Este vacío en la literatura no

[3] Valores de 12.89 % en banda ancha fija frente al 17.9 % del promedio regional (CEPAL, 2023).

permite comprender la realidad local, ni la toma de decisiones respaldada en evidencia, ni el diseño de soluciones encaminadas a soportar a los auditores paraguayos.

La presente investigación es particularmente pertinente, sobre todo, por la reciente actualización emitida por parte del Instituto de Auditores Internos (2024) en lo que respecta al Marco Conceptual para la Práctica Profesional, en el que se ha emitido el Requisito Temático de Ciberseguridad en febrero 2025, que se hará efectivo en febrero de 2026. El requisito demanda que los encargados de aseguramiento de la tercera línea de defensa evalúen los procesos de control de ciberseguridad de las organizaciones (Instituto de Auditores Internos, 2025).

Adicionalmente, la relevancia social de este estudio radica en el interés público que representa esta función (Instituto de Auditores Internos, 2024). Un control interno robusto en las empresas, que son agentes clave para el desarrollo económico, fortalece la confianza en el mercado y beneficia a un amplio número de partes interesadas, que van desde el gobierno hasta los proveedores y empleados, tal como lo confirman los estudios sobre gobernanza corporativa (Ernst & Young [EY] & The Institute of Internal Auditors [IIA], 2021; Financial Crime Academy, 2026).

Este estudio, de tipo transversal, pretende proporcionar herramientas prácticas y evidencia empírica de utilidad para los profesionales del sector, tanto financieros como tecnológicos. Para ello, sobre la base de consideraciones estadísticas, se pone de manifiesto cuál es el grado de correlación existente entre el nivel de madurez digital de las organizaciones en Paraguay y el foco que los planes anuales de trabajo dan a este riesgo, con un corte temporal del periodo de junio a julio de 2025.

El valor teórico de la presente investigación radica, principalmente, en la contribución del presente estudio al cuerpo de investigaciones académicas existentes, al ser la primera de su clase en cuantificar la relación específica entre las variables analizadas en Paraguay. Adicionalmente, la presente pesquisa permitirá contrastar los modelos teóricos globales existentes con la realidad local y fomentará el debate sobre la cobertura de riesgos tecnológicos por parte de la función de aseguramiento de la tercera línea de defensa.

Metodológicamente, el estudio es de naturaleza cuantitativa, con un alcance explicativo-correlacional y un diseño no experimental de tipo transversal, lo cual permite una robusta y pertinente aplicación para futuras investigaciones en áreas asociadas. Lo anterior se fundamenta en la consideración de que el enfoque cuantitativo ofrece un método escalable y objetivo para establecer una línea de base en contextos donde los datos empíricos son escasos, como el caso de Paraguay.

La pregunta general de investigación es la siguiente: ¿cuál es la correlación entre el nivel de madurez digital y el grado de enfoque en riesgos tecnológicos en el plan anual de auditoría interna de las empresas en Paraguay en el periodo de junio a julio de 2025? A continuación, se presentan las preguntas específicas:

1) ¿Cuál es el nivel de madurez digital percibido en las empresas de Paraguay en el período de julio a agosto de 2025?

2) ¿Cuál es el grado de enfoque en riesgos tecnológicos en los planes de auditoría de las empresas del Paraguay en el período de julio a agosto de 2025?

3) ¿Cuál es el nivel de correlación entre el nivel de madurez digital percibido y el grado de enfoque en riesgos tecnológicos en los planes de auditoría interna de la muestra estudiada?

El objetivo general de esta investigación es analizar la correlación entre el nivel de madurez digital y el grado de enfoque en riesgos tecnológicos en el plan anual de auditoría interna de las empresas en Paraguay para el período de 2025. Además, los objetivos específicos son los siguientes:

1) Determinar el nivel de madurez digital percibido en las empresas de la muestra

2) Describir el grado de enfoque en riesgos tecnológicos en los planes de auditoría de dichas empresas

3) Cuantificar la correlación existente entre el nivel de madurez digital percibido y el grado de enfoque en riesgos tecnológicos en los planes de auditoría

Finalmente, la hipótesis general de la investigación consiste en que existe una correlación positiva y significativa entre el nivel de madurez digital de las empresas en Paraguay y el grado de enfoque en riesgos tecnológicos de sus planes anuales de auditoría interna para el período de 2025. La variable independiente es el nivel de madurez digital y la variable dependiente es el grado de enfoque en riesgos tecnológicos.

2. Marco teórico

El análisis de la literatura existente indica que el proceso de transformación digital de la propia área de aseguramiento presenta barreras de tipo cultural, técnico y organizacional. Estas barreras se originan por una desconfianza hacia la fiabilidad de los sistemas informáticos utilizados. Se destaca que la utilización, por parte de

la función de auditoría interna, de herramientas asociadas a la inteligencia artificial o *big data* (solo por nombrar algunas) incrementa de forma importante las capacidades del área (Herrera-Sánchez, 2024).

En relación con los estudios académicos existentes en materia de la tercera línea de defensa, se observa que el conocimiento existente se encuentra fragmentado y principalmente asociado a tres grandes ejes: la calidad de la auditoría, la calidad de la información financiera y la adopción de la tecnología. La referida dispersión temática vuelve a la presente investigación particularmente relevante, ya que, dentro de esta, se busca estudiar las referidas dimensiones de forma integrada (Firza et al., 2025).

De forma complementaria, Lenz et al. (2018) presentan el concepto de "tensión institucional". De acuerdo con este este criterio, la función de aseguramiento enfrenta en su día a día un conjunto de intereses contrapuestos entre lo que dictan las normas que reglamentan la profesión y las diversas expectativas de los grupos de interés. La magnitud de esta tensión será clave para entender la dimensión en la cual el área de aseguramiento de la tercera línea de defensa pueda influir en áreas estratégicas y tecnológicas.

Al profundizar en la auditoría interna informática, los estudios reflejan la relevancia del enfoque de las nuevas tecnologías en el plan anual del área de la tercera línea de defensa. Esta tendencia pone de manifiesto la necesidad de actualización (*upskilling*), en lo relativo a reclutamiento y entrenamiento por parte de las funciones de auditoría interna, a efectos de hacer frente a los desafíos próximos y cerrar las brechas de competencias identificadas (Usul & Alpay, 2025).

Por otro lado, estudios científicos sugieren que existe una relación positiva entre la calidad del proceso organizacional y corporativo de gobierno de tecnología de la información (IT), y la calidad en el ejercicio del rol de la tercera línea de defensa en el ámbito informático. Esta relación positiva se extiende también a las competencias exhibidas por la función de la auditoría interna informática, cuando el gobierno de IT es robusto. Finalmente, los dos factores previamente mencionados repercuten positivamente en el ambiente de controles generales de tecnología (ITGC) (Wu et al., 2024).

A nivel académico, Al-Mohammedi (2020) investigó el rol de la digitalización en el desarrollo de las prácticas de auditoría interna de IT, que refleja la conexión existente entre la madurez digital y la tercera línea de defensa. Dicho estudio, que contó con una muestra de 57 profesionales, concluye que la digitalización contribuye de forma significativa al desarrollo de las prácticas del área.

En relación con la situación de Paraguay, en el transcurso de la presente investigación se realizó la Consulta Pública 93590, dirigida al Ministerio de Industria y Comercio, por medio de la cual se inquirió sobre el nivel de digitalización de las empresas paraguayas medido a través de la herramienta de Chequeo Digital. La respuesta recibida por parte de las autoridades, específicamente, del Viceministerio de Micro, Pequeñas y Medianas Empresas, advierte que se cuenta con 528 empresas registradas en la plataforma de monitoreo establecida por el Gobierno del Paraguay en conjunto con el BID.

En el informe final recibido, se observa que el grado de madurez en términos consolidados es calificado como "novato", con lo que se manifiesta un nivel de madurez digital promedio de 24.23 %. Dada la densidad poblacional del país, se considerarán como representativos los resultados obtenidos para la ciudad de Asunción, en donde, según datos oficiales, el 21.8 % de las empresas refiere que usan la tecnología para mejorar las ventas y la experiencia del cliente (Ministerio de Industria y Comercio de Paraguay, 2025).

Por otro lado, en su gran mayoría (51.22 %), las mismas empresas refieren que no cuentan con un plan definido para un aprovechamiento adecuado de las tecnologías digitales. En ese sentido, se registra que el 56.41 % de las empresas no realizan ventas a través de comercio electrónico. Cuando se consultó cuáles son los programas y aplicativos más utilizados, el 68 % de las empresas responde que usan aquellos que se relacionan con herramientas de ofimática, como hojas de cálculo o programas procesador de texto (Ministerio de Industria y Comercio de Paraguay, 2025).

Las *Normas Globales de Auditoría Interna* (Instituto de Auditores Internos, 2024) requieren que el director ejecutivo de auditoría (DEA) tenga un proceso tanto para la identificación y evaluación de los riesgos significativos existentes, así como para los emergentes. De esa manera, posteriormente, sobre la base de los mismos riesgos, se puede diseñar un plan de auditoría anual que dé una respuesta a las estrategias, los objetivos y los riesgos de la organización (Instituto de Auditores Internos, 2024).

De forma complementaria al marco anteriormente referido, las normas para Auditoría Informática emitidas por la Asociación de Control y Auditoría de Sistemas de Información (ISACA, por sus siglas en inglés) establece que la función de la auditoría de IT debe usar un enfoque basado en riesgos para establecer un plan de sí misma y determinar las prioridades para la asignación eficiente de los recursos de auditoría de tecnología. ISACA (2020) también requiere que dicha evaluación se utilice para justificar la asignación de recursos.

En lo relativo a la transformación digital, estimaciones globales revelan que un aproximadamente el 90 % de las organizaciones atraviesa actualmente un proceso de transformación digital. También se considera que la claridad con respecto a este concepto no es solo clave para competir a futuro, sino también para la supervivencia de las organizaciones. Así, se concluye que los procesos de transformación tienen más posibilidades de ser exitosos cuando se enfocan en procesos completos y no únicamente en casos de uso puntuales (McKinsey & Company, 2024).

Para medir el nivel de transformación digital, la consultora Deloitte (2018) ha elaborado un modelo denominado "modelo de madurez digital", el cual incorpora elementos del consumidor, la cultura organizacional, los operativos, la estrategia y aspectos tecnológicos. El indicador permite medir en qué lugar se encuentra una organización determinada en su proceso de transformación, y ayuda a que se puedan establecer planes y objetivos de corto a mediano plazo para realizar transformaciones de impacto.

El marco de control interno tecnológico Control Objectives for Information Related Technology (COBIT, por sus siglas en inglés) 2019, elaborado por ISACA (2018), indica en su dominio AP12.02, denominado "Analizar riesgos", que las organizaciones deben ser capaces de definir el alcance apropiado de esfuerzos de análisis de riesgos, al igual que estimar la frecuencia y la magnitud de una potencial pérdida (o ganancia) asociada a los escenarios de riesgos de tecnología. De igual forma, dicho marco propone establecer una respuesta a los riesgos que excedan el apetito y la tolerancia al riesgo de la organización.

Las normas profesionales exigen un enfoque basado en riesgos para el ejercicio de la auditoría interna (Instituto de Auditores Interno, 2024; ISACA, 2020). Según los estudios previamente referidos de Deloitte (2018), y McKinsey y Company (2024), la transformación digital no solamente trae grandes oportunidades, sino también riesgos adicionales a los cuales la función debe dar respuesta. Un mayor nivel de madurez digital de las organizaciones debería traducirse en un plan de trabajo anual que refleje tales prioridades.

En relación con los términos utilizados, según las normas del Instituto de Auditores Internos (2024), el área de auditoría interna tiene por objetivo fortalecer la capacidad de la organización para crear, proteger y sostener su valor al proporcionar al directorio y a la alta gerencia aseguramiento, asesoramiento, prospectivas y previsiones de manera independiente, objetiva y basada en riesgos. En cuanto al plan de trabajo anual, las normas del Instituto de Auditores Internos aluden a que debe ser un documento creado por el DEA que identifique los trabajos y otros servicios que se prevén

proporcionar en un determinado período. El plan debería estar basado en riesgos y tendría que ser dinámico. Además, debería reflejar los ajustes oportunos en respuesta a los cambios que afecten a la organización.

Según las normas de ISACA (2020), en relación a la planificación de un encargo de auditoría tecnológico, la función en su rama tecnológica debe basarse en un enfoque de riesgo, para generar un plan que permita determinar las prioridades para una designación efectiva de los recursos. De igual forma, se requiere que los auditores identifiquen y evalúen riesgos relevantes dentro de las áreas a ser revisadas.

Con respecto a la gobernanza de IT, el marco COBIT 2019 lo sindica como aquel proceso de gobernanza que permite satisfacer las necesidades de los diferentes grupos de interés, y generar valor a través del uso de la tecnología y la información. Agrega que el sistema de gobierno incluye numerosos componentes que actúan de forma holística; además, es dinámico, y debe estar específicamente diseñado para cada tipo de entidad y para abarcar no únicamente lo tecnológico (ISACA, 2018).

Por su parte, la transformación digital se entiende como un proceso de innovación que permite a las organizaciones desarrollar competencias organizacionales y tecnológicas que confieran una mejora continua en la experiencia del cliente o en una disminución de costos. Así, a lo largo del tiempo, se desarrolla una ventaja competitiva, según reportan consultoras internacionales.

Finalmente, según la consultora Deloitte (2018), la madurez digital es concebida como la capacidad de una organización para adaptarse rápidamente a los avances tecnológicos y las tendencias cambiantes. También sostiene que el enfoque se centra en la capacidad organizacional de aprovechar rápidamente nuevas capacidades y responder a los intereses de los consumidores para obtener ventajas competitivas.

En relación con la base legal aplicable a la presente investigación, es importante destacar que el Código Civil, en su artículo 1111, impone a los directores una responsabilidad ilimitada y solidaria ante la sociedad, los accionistas y terceros por el “mal desempeño del mandato” o por la violación de la ley (Ley 1183/1985, 1985). Por su parte, la Ley del Comerciante (Ley 1034/1983, 1983), resalta, en su artículo 74, que todo comerciante debe registrar una contabilidad ordenada y regular. De esa forma, establece las bases legales para la existencia de sistemas de control fiables.

De forma complementaria, la estructura de gobierno de las sociedades anónimas en Paraguay, regulada de igual forma por el Código Civil, contempla órganos de supervisión interna. El artículo 1102 asigna la administración de las sociedades a uno o más

directores, y el artículo 1117 establece la figura de la sindicatura como el órgano de fiscalización privada (Ley 1183/1985, 1985). Si bien esta normativa no establece la creación de un departamento de aseguramiento para la tercera línea de defensa de forma obligatoria para todas las sociedades, las funciones del síndico presuponen la existencia de un sistema de control interno.

En el sector financiero bancario, la exigencia de una función de auditoría interna se vuelve clara. El Reglamento General sobre Sistemas de Control Interno, aprobado por la Resolución SB. SG. 00032/2008 (2008), establece, en su artículo 1, la obligación de contar con una unidad de Control Interno / Auditoría Interna. De igual forma, el artículo 4 define como función básica del auditor la de evaluación de riesgos operativos, "incluyendo la auditoría informática", al establecer así la base para una supervisión tecnológica formal.

La transición hacia operaciones digitales en Paraguay impone nuevas obligaciones legales a través de la Ley de Protección de Datos Personales Crediticios (Ley 6534/2020, 2020). Esta norma establece un marco de responsabilidad estricto en la gestión de la información personal, al exigir, según el artículo 6, el consentimiento informado del titular de los datos para que el tratamiento de estos sea lícito. El incumplimiento de la Ley 6534/2020 constituye un riesgo latente para las organizaciones, con lo que se genera la responsabilidad de verificar los controles que aseguren la protección de dichos datos, asociada principalmente a la función de auditoría interna.

El marco regulatorio para el sector financiero va más allá por su significativa importancia para la estabilidad macroeconómica. Por ello, prescribe un modelo detallado para la gestión tecnológica a través de la Resolución SB. SG. 00124/2017 (2017), por medio de la cual se aprueba el Manual de Gobierno y Control de Tecnologías de Información (MGCTI). Este se constituye como un marco de referencia obligatorio basado en estándares internacionales, como COBIT. El manual exige a las entidades financieras implementar procesos específicos para la gestión de riesgos tecnológicos.

En conclusión, el marco legal paraguayo crea una obligación tanto implícita como explícita de alinear la planificación de la auditoría con los riesgos digitales. Mientras que el deber general de control se inicia en el Código Civil, en el que se establece una base amplia, las normativas específicas, como la Ley de Protección de Datos y, de manera contundente, el Manual de Gobierno Corporativo de Tecnologías de la Información de la Superintendencia de Bancos, traducen ese deber en mandatos concretos, tanto para la gerencia de las empresas como para las áreas de auditoría (Resolución SB. SG. 124/2017, 2017).

3. Materiales y métodos

A nivel metodológico, se adoptó un enfoque cuantitativo, ya que se busca generar conocimiento mediante datos numéricos y análisis estadísticos. Para ello, se recolectaron datos a través de un instrumento estandarizado del tipo cuestionario, a través de un conjunto estructurado de preguntas sobre las variables a ser estudiadas, para su posterior análisis estadístico.

El alcance de la presente investigación es de índole explicativo-correlacional, al tener por objetivo inicial la descripción y caracterización de las variables principales: el nivel de madurez digital percibido y el grado de enfoque en riesgos tecnológicos en los planes anuales de auditoría. Posteriormente, se procedió a examinar la correlación, es decir, el análisis que incluyó la dirección y la fuerza de la asociación estadística existente entre las mismas.

Al realizar la investigación, se adoptó un diseño de investigación no experimental, ya que las variables no fueron alteradas ni modificadas en forma alguna, sino que se observaron tal como se presentan en su contexto natural. Adicionalmente, dado que la recopilación de datos se realizó en un punto temporal específico (de junio a julio de 2025), el estudio fue de tipo transversal.

La población objetivo de estudio está compuesta por profesionales que ejercen roles de liderazgo o participan como miembros de equipo en las funciones de auditoría interna de empresas de Paraguay. Dada la ausencia de datos, como un censo exhaustivo con la finalidad de determinar el tamaño exacto de esa población, se empleó un muestreo del tipo no probabilístico por conveniencia y de bola de nieve. La muestra final estuvo compuesta por dieciocho profesionales que cumplieron con los criterios de inclusión y respondieron al cuestionario electrónico de evaluación (Google Forms).

La técnica de recolección de datos fue la encuesta, que se realizó a través de un conjunto de preguntas formuladas de manera sistemática y ordenada. El instrumento utilizado fue un cuestionario estructurado de naturaleza digital, el cual fue diseñado ad hoc para esta investigación. El cuestionario anónimo se compuso de catorce preguntas cerradas, organizadas en tres secciones: (1) perfil demográfico, (2) una escala de tipo Likert de nueve ítems para medir la madurez digital y (3) cuantificación del enfoque del plan anual de auditoría.

Las variables fueron operacionalizadas, utilizando marcos de referencia internacionales. La variable independiente, nivel de madurez digital, se operacionalizó tomando como base el modelo de madurez digital de Deloitte (2018). La base de la medición

fue una escala compuesta de nueve ítems, agrupados en cinco dimensiones teóricas. Las dimensiones referidas son las siguientes: 1) cliente (digitalización de procesos comerciales), 2) estrategia (visión directiva clara), 3) tecnología (adopción de arquitectura en la nube), 4) operaciones (eficiencia y gobernanza de datos), y 5) organización / cultura (fomento de la innovación y capacitación del talento).

Por su parte, para la variable dependiente, enfoque del plan de auditoría, se tomó como referencia a los marcos de COBIT 2019 y COSO ERM, a efectos de determinar cinco dominios de aseguramiento: ciberseguridad, continuidad de negocio, gobernanza de IT, privacidad de datos y proyectos de IT. A través de la asignación porcentual de tiempo y recursos en el plan de auditoría interna anual, se cuantificó dicha variable.

Antes de su distribución masiva, el instrumento fue sometido a un proceso de validación a través de una prueba piloto, la cual consistió en la aplicación del mismo a un grupo de testeo conformado por cinco profesionales auditores internos. El propósito de esta validación fue evaluar la claridad de la redacción, la comprensión de las preguntas y la funcionalidad técnica del formulario. La retroalimentación recibida fue utilizada para realizar ajustes finales en el instrumento, a fin de asegurar su adecuación antes del lanzamiento principal.

Los datos fueron procesados mediante el software estadístico R (versión 2025.05.1). Los mismos se analizaron a través de estadística descriptiva, a través de medidas de dispersión y de tendencia central. La correlación de las variables fue medida a través de la correlación de rangos de Spearman (*rho*), la cual es una medida de asociación monótona que utiliza rangos, y mide la fuerza y dirección de dos variables. Además, se consideró el coeficiente de correlación de Pearson como análisis de sensibilidad a fin de evaluar la robustez de los hallazgos.

Asimismo, con el fin de explorar posibles diferencias entre los grupos de la muestra, se utilizó la prueba de Kruskal-Wallis, la cual permite comparar los valores de mediana de una escala de variables, con la finalidad de determinar si las mismas son estadísticamente significativas. La selección de esta prueba consideró la robustez de la misma ante muestras de pequeño tamaño.

Los resultados de la investigación fueron presentados en ocho tablas y un gráfico de dispersión, cada uno acompañado de su respectiva descripción analítica, y con la correspondiente interpretación y contrastación con las teorías vigentes en la materia. Las tablas permitieron una mejor organización de los resultados basados en el perfil demográfico, el análisis de cada variable y, finalmente, el análisis de correlación entre

ambas, lo que facilitó tanto la interpretación como la comprensión de los patrones observados.

Finalmente, se garantizaron los principios del consentimiento informado y la confidencialidad en el estudio realizado. Se obtuvo el consentimiento de todos los participantes al inicio del cuestionario. Asimismo, se aseguró la confidencialidad y el anonimato en el manejo de los datos, los cuales fueron procesados de forma agregada y sin identificación específica de los informantes y sus organizaciones, en cumplimiento de los estándares de integridad científica y transparencia académica.

4. Resultados y discusión

A continuación, se exponen los resultados obtenidos a partir del análisis estadístico de los datos brutos recolectados mediante el cuestionario electrónico vía Google Forms, aplicado a una muestra final de dieciocho profesionales del rubro en Paraguay. La presente sección se estructura en función de los objetivos de la investigación, desde el análisis descriptivo de las variables hasta el análisis correlacional de las mismas. Cada tabla y figura se encuentra acompañada con su respectiva descripción y una discusión que contrasta los hallazgos con las respectivas teorías en la materia.

Tabla 1. *Perfil demográfico de la muestra - industria*

Categoría	Frecuencia	Porcentaje
Industrial / Manufactura	5	27.8 %
Retail / Consumo masivo	5	27.8 %
Financiero (bancos, seguros, financieras)	3	16.7 %
Servicios (salud, educación, consultoría)	3	16.7 %
Energía	1	5.6 %
Gubernamental / Sector público	1	5.6 %
Total	**18**	**100 %**

La tabla 1 detalla el perfil demográfico por industria de las respuestas recibidas en el presente estudio. Se observa una predominancia de los sectores industrial / manufactura (n = 5) y *retail* / consumo masivo (n = 5), que en conjunto representan más de la mitad de la muestra.

Tabla 2. *Perfil demográfico de la muestra – rol del participante*

Categoría	Frecuencia	Porcentaje
Gerente de auditoría	9	50 %
Auditor sénior	5	27.8 %
Director de auditoría	4	22.2 %
Total	**18**	**100 %**

La tabla 2 refleja que la mayoría de las personas que participaron en la encuesta tienen cargos de gerente o DEA. De esta manera, la información obtenida representa a personas que cuentan con cargos de máxima responsabilidad dentro del área en el contexto organizacional.

Tabla 3. *Perfil demográfico de la muestra – área de auditoría interna (por dotación de personal)*

Categoría	Frecuencia	Porcentaje
2 - 5 personas	12	66.7 %
6 - 10 personas	4	22.2 %
1 persona	2	11.1 %
Total	**18**	**100 %**

La tabla 3 refleja que las organizaciones que procedieron a participar del estudio tienen, en su mayoría, funciones de tercera línea de defensa acotadas, de entre 2 a 5 personas.

La composición de la muestra, con una fuerte presencia de los sectores industrial y de consumo, refleja la estructura económica de Paraguay más allá del sector financiero. Esto es relevante, ya que, como señalan diversos estudios de mercado, las presiones competitivas fuerzan a esos sectores a acelerar su transformación digital[4]. La consulta destaca que el 78 % de los ejecutivos sienten que luchan por mantenerse al día con el ritmo del cambio y advierte sobre el riesgo de perder cuota de mercado frente a los competidores por no adaptarse.

Los equipos de auditoría con estructuras pequeñas tienden a limitar la especialización técnica, y ponen de manifiesto el nuevo paradigma dentro de la función, el cual exige colaboradores capaces de adaptarse a las nuevas tecnologías y de desarro-

[4] KPMG International (2024) destaca que el 78 % de los ejecutivos siente dificultad para seguir el ritmo de los cambios tecnológicos.

llar habilidades analíticas de resolución de problemas (Abdullah & Almaqtari, 2024). De igual forma, la evolución de un enfoque tradicional a uno participativo y totalmente digitalizado queda de manifiesto, respondiendo a procesos empresariales en constante evolución (Stepanyan, 2023).

La limitacion en términos estructurales por parte de la función tiene su correlato en los requerimientos de las nuevas normas de auditoría interna y en la capacidad del área de dar cumplimiento cabal a estas últimas. Eulerich y Bonrath (2025) refieren la necesidad de contar con talento especializado a efectos no solamente de agregar valor al interior de la organización, sino también de cumplir con las nuevas Normas Globales de Auditoría Interna.

Esta dinámica de intereses contrapuestos y conflictos es conceptualizada por Lenz et al. (2018) como una tensión institucional. La función de auditoría se ve presionada por la alta gerencia y el comité de auditoría para responder a riesgos emergentes y complejos. Sin embargo, su capacidad para dar respuesta a tal requerimiento está fuertemente condicionada por la estructura y el rol histórico percibido por los grupos de interés. Este desajuste define la brecha de efectividad que enfrentan actualmente muchos profesionales del área.

La muestra de la presente investigación representa un segmento de profesionales experimentados que operan en sectores económicos clave para Paraguay, pero dentro de funciones de auditoría con recursos limitados. Es en este contexto en el que, principalmente, la brecha entre los riesgos crecientes a nivel tecnológico y la capacidad de aseguramiento de la auditoría interna puede ser más pronunciada, lo que es especialmente relevante dada la dificultad para atraer talento especializado para dar el aseguramiento requerido correspondiente, conforme lo señalan asociaciones expertas en la materia (Protiviti & The ERM Initiative at NC State University, 2022).

Tabla 4. *Escala de madurez digital*

Descripción del Ítem	Respuestas (n)	Media	Mediana	Desv. estándar (DE)
Se utilizan herramientas de análisis de datos (*data analytics*) para la toma de decisiones.	18	3.33	3	1.28
Los procesos clave de negocio (por ejemplo, ventas, operaciones) han sido significativamente digitalizados.	18	3.11	3	1.32

Descripción del Ítem	Respuestas (n)	Media	Mediana	Desv. estándar (DE)
Se fomenta una cultura de experimentación e innovación.	18	3.11	3	1.41
La organización invierte en capacitar a los empleados en nuevas habilidades digitales.	18	3.11	3	1.41
Existe un presupuesto asignado específicamente para iniciativas de transformación digital.	18	3.06	3	1.35
La organización utiliza activamente tecnologías en la nube (*cloud computing*).	18	3.06	3	1.30
La alta dirección ha definido y comunicado una visión clara sobre la transformación digital.	18	3.00	3	1.24
Se exploran o utilizan tecnologías emergentes como inteligencia artificial o IoT.	18	3.00	3	1.37
Existen políticas claras sobre la gobernanza, la calidad y la seguridad de los datos.	18	2.72	3	1.27

La tabla 4 presenta las estadísticas de los nueve ítems de la escala de madurez digital, cuyo método de construcción y desarrollo fue enunciado en el apartado de la metodología. El ítem con la media más alta corresponde al uso de herramientas de análisis de datos (*data analytics*) para la toma de decisiones (M = 3.33). En contraste, el ítem con la menor valoración es el relativo a la existencia de políticas claras sobre la gobernanza, calidad y seguridad de los datos (M = 2.72), y es el único ítem que se sitúa por debajo del punto neutral de la escala, el cual es 3.

La alta valoración en *data analytics* es consistente con la respuesta corporativa a la intensa presión competitiva, la que obliga a las organizaciones a adoptar tecnologías de vanguardia para no perder cuota de mercado (KPMG International, 2024). No obstante, es importante destacar que la mera adopción tecnológica sin una estrategia de gobierno corporativo que la sustente es una trampa común. La transformación digital corresponde a un proceso multidimensional que debe ser concebido a nivel estratégico dentro de las organizaciones, con una hoja de ruta clara sobre su implementación (Aras & Büyüközkan, 2023).

El puntaje relativamente bajo en gobierno de datos (M = 2.72) revela una dinámica llamativa entre las prioridades de la dirección, al no existir estructuras de gobernanza claras, y que aseguren que los procesos de madurez digital se adopten de forma holística y no como iniciativas separadas sin un impacto real a nivel corporativo. Como refiere Tharouma (2025), sin un adecuado apoyo por parte de la alta gerencia, dichos procesos están destinados a encontrar dificultades significativas.

La efectividad del auditor para influir en temas estratégicos se ve fortalecida cuando la función cuenta con el apoyo de la alta dirección, con lo que se refuerza así su credibilidad interna y la alineación estratégica del área (Vaya-Arboledas et al., 2025). Este respaldo se materializa en la priorización de recursos. Al preferir los resultados a corto plazo, las iniciativas como la gobernanza de datos reciben menos respaldo de la gerencia y limitan la capacidad del auditor para impulsar las transformaciones organizacionales (Al Omari et al., 2025).

Estos resultados evidencian un nivel de madurez digital "desequilibrado", con indicadores mixtos. La literatura indica que, para estos casos, la madurez debería evaluarse de forma diferenciada y no limitada a la mera incorporación tecnológica, sino que, además, incorpore los cambios estratégicos necesarios para llevar a cabo el proceso (Tubis, 2023). El desequilibrio observado entre la creación de valor (*analytics*) y la optimización de riesgos (gobernanza) dista de los principios de marcos internacionales como COBIT (ISACA, 2018), y pone de manifiesto un problema de liderazgo más que de tecnología.

Tabla 5. *Estadísticas descriptivas de los ítems de madurez digital*

Riesgo	Respuestas (n)	Media	Mediana	Desviación estándar (DE)
Ciberseguridad	18	3.50	3	1.25
Continuidad de negocio	18	3.33	3	1.37
Gobernanza de IT	18	3.28	3	1.18
Privacidad de datos	18	3.22	3	1.35
Implementación de proyectos	18	3.17	3	0.92

La tabla 5 detalla la percepción de los participantes sobre cinco riesgos tecnológicos clave, conforme a los criterios descritos en la sección de metodología. La ciberseguridad (ciber) es percibida como el riesgo más alto (M = 3.50), seguida de continuidad de negocio (M = 3.33). El riesgo percibido como el más bajo es el de implementación de proyectos (M = 3.17), aunque todos los riesgos se sitúan por encima del punto neutral de la escala, que es de 3.

La primacía de la ciberseguridad como el riesgo principal (M = 3.50) está perfectamente alineada con las encuestas globales sobre riesgos relevantes para la profesión (IIA, 2025; Protiviti, & NC State University's ERM Initiative, 2022). Esto demuestra que los participantes a nivel local comparten las mismas preocupaciones que sus pares a nivel mundial. Esto es natural, debido a los acelerados procesos de digitalización que aumentan las posibilidades de ataques a las organizaciones, según indican reportes especializados en la materia (KPMG International, 2024).

En cuanto a la jerarquía observada, se destaca que existe una priorización de los riesgos de ciberseguridad y continuidad de negocio por sobre los de implementación de proyectos. Este fenómeno se explica por la consolidación de la ciberseguridad como uno de los principales riesgos empresariales en el contexto de los planes de trabajo anuales, como lo revela la literatura (Slapničar et al., 2022). De igual forma, el apoyo de la alta gerencia y el directorio de la entidad a la tercera línea de defensa permite incrementar sustancialmente su efectividad en la mitigación de riesgos (Vuko et al., 2025). Así, los resultados observados resultan coherentes con estudios internacionales.

La percepción relativamente más baja del riesgo del criterio de proyectos *(*M = 3.17) puede reflejar una tensión fundamental en la evolución de la profesión. Lenz y Sarens (2012) ponen de manifiesto la lucha de la actividad auditora por la transición desde su rol histórico de aseguramiento (al proteger el valor existente) hacia un rol más estratégico y consultivo (a modo de asegurar la creación de nuevo valor). Al subestimar el riesgo de proyectos por los auditores, queda de manifiesto la mayor comodidad con su rol tradicional.

Finalmente, este enfoque sugiere una aplicación aún incipiente del marco *COSO Enterprise Risk Management* (Committee of Sponsoring Organizations of the Treadway Commission, 2017), que integra el riesgo con la estrategia. Al priorizar los riesgos operacionales desde el punto de vista de la tercera línea de defensa, sus miembros en Paraguay podrían subestimar la revisión de, por ejemplo, la alineación estratégica de IT, considerada un factor crítico para la creación de valor (Dutta et al., 2022).

Tabla 6. *Descriptivos de las variables principales*

Variable	N	Media	Mediana	DE	Rango
Índice de madurez digital	18	3.06	2.94	1.18	1.0 – 5.0
Porcentaje del Plan a IT (%)	18	10.56	10.00	9.22	0 - 30

La tabla 6 resume las dos variables principales del estudio. El índice de madurez digital, que fue calculado a través de las nueve preguntas detalladas en la tabla 4,

presenta una media de 3.06 y una mediana de 2.94, por lo que se sitúa en el punto neutral de la escala, pero con una considerable desviación estándar (DE = 1.18). El porcentaje del plan a IT, que se midió a través del formulario, muestra una media de 10.56 % y una mediana de 10.00 %, con una desviación estándar aún más pronunciada (DE = 9.22).

La media del índice de madurez digital (M = 3.06) confirma la percepción de un estadio intermedio en el proceso de transformación digital, un hallazgo consistente con los diagnósticos macro de organismos internacionales para la región (Álvarez & Toledo, 2022; Cepal, 2023). De forma contrastante, la alta desviación estándar (1.18) es el dato más revelador, pero consistente con lo manifestado por Haryanti et al. (2023). En su modelo propuesto clasifican a las organizaciones en niveles progresivos en diversas dimensiones de madurez digital, lo que explica la considerable dispersión en los resultados encontrados en este estudio.

El enfoque del plan de trabajo en IT (M = 10.56 %) se encuentra por debajo de los *benchmarks* de funciones calificadas como "maduras" a nivel global por parte de The Internal Audit Foundation. En su estudio *Risk in focus*, se observa que la media de tiempo dedicado por parte del área al plan de IT es por encima del 20 % según los *benchmarks* internacionales (IIA, 2025), lo que pone de manifiesto una marcada dispersión en las respuestas. Por lo tanto, se refleja una falta de consenso sobre la relevancia de los temas tecnológicos que responde a criterios de madurez aislados por parte de cada unidad.

No dejan de llamar la atención casos en los que se observa un 0 % del tiempo de plan anual dedicado a temas de IT. Esto revela que el profesional no cumpliría el rol de asesor estratégico, sino que aún estaría concebido bajo paradigmas tradicionales. En ese sentido, se limita de forma importante la capacidad de la función para mitigar amenazas en entornos de constante transformación y evolución (Lenz & Sarens, 2012).

La pronunciada divergencia identificada se considera consistente con el marco internacional de COBIT 2019, el cual hace énfasis en que el sistema de gobierno de las entidades debe estar adaptado y adecuado a la medida de las necesidades de cada compañía (ISACA, 2018). Considerando dicho marco, la alta dispersión observada pudiera interpretarse como la consecuencia natural del resultado del hecho de que cada función de auditoría pudiera adaptar su plan de IT a su contexto particular, apetito de riesgo y nivel de madurez.

No obstante, pese a la flexibilidad que otorga el marco COBIT 2019, los nuevos requisitos temáticos del Instituto de Auditores Internos (2025), sobre todo, aquel asociado

a ciberseguridad requiere un mínimo aseguramiento dentro del plan de trabajo anual, el cual no puede ser eludido si la función desea cumplir con estándares internacionales, como lo indican McKinsey y Company (2024) en sus perspectivas sobre transformación digital. Consecuentemente, el rezago observado pone en riesgo el cumplimiento del mandato con el que cuenta la tercera línea de defensa según las normas vigentes.

Tabla 7. *Correlación entre madurez digital y enfoque en auditoría de IT*

Método de Correlación	Coeficiente (*r* o *rho*)	Valor *p*
Correlación de Pearson	0.385	0.115
Correlación por rangos de Spearman	0.304	0.220

La tabla 7 presenta los resultados de las pruebas de correlación. El coeficiente de Pearson fue de $r = 0.385$ ($p = 0.115$) y el de Spearman de $rho = 0.304$ ($p = 0.220$). Ambos indican una asociación positiva de débil a moderada, que no es estadísticamente significativa.

Los resultados revelan una correlación positiva, aunque débil y carente de significancia estadística. Esta asociación es consistente con los postulados de la auditoría basada en riesgos, conforme a lo indicado en las *Normas Globales de Auditoría Interna* (Instituto de Auditores Internos, 2024). Esta normativa postula que el proceso de planificación de auditoría debe estar alineado con los riesgos emergentes y, en este caso particular, con los riesgos digitales, lo cual es una tendencia creciente[5].

La debilidad de la asociación debe ser considerada como un hallazgo central del presente estudio. Lo referido constituye evidencia empírica tangible del concepto de "tensión institucional" que plantea Lenz et. al. (2018), en la que se observa una dificultad de la función para implementar estándares globales como producto de las expectativas de los grupos de interés, principalmente, en el entorno corporativo de empresas de propiedad local. En ese contexto, estudios realizados en economías emergentes reflejan que la efectividad de la función está condicionada por presiones coercitivas y normativas del entorno (Josh & Karyawati, 2022).

La necesidad de preservar la legitimidad interna ante el directorio conlleva a la posposición de la intención observada de priorizar los riesgos de tecnología (observada en la tabla 4, con el riesgo de ciberseguridad con la ponderación más alta). Al priorizar los riesgos considerados tradicionales, la función de auditoría interna, al igual que

[5] KPMG International (2024) posiciona a la ciberseguridad y la transformación digital como las principales preocupaciones de liderazgo.

otras funciones clave de la empresa, responden a un proceso de adopción digital que se puede calificar como “fragmentado” y no de forma sistemática a nivel institucional.

La disparidad identificada entre los requerimientos teóricos establecidos tanto por las normas internacionales como por las del Instituto de Auditores Internos e ISACA, y la práctica del día a día manifestada por parte de los encuestados puede también ser explicada por la necesidad no solo futura, sino también presente de ampliar sus competencias a efectos de potenciar el reconocimiento institucional y cumplir con su cometido de proteger el valor organizacional (Vitalis et al., 2024).

Un factor diferenciador para la función de auditoría interna está asociado a la calidad del apoyo institucional recibido. Existe una asociación positiva entre el respaldo de la alta gerencia y el efecto sobre el desempeño como resultado de las implementaciones recomendadas por el área (Alzeban, 2021). Lo anterior denota como la capacidad de auditoría se fortalece notablemente mediante el impulso de la implementación de las recomendaciones y mejoras identificadas, que redunda en el fortalecimiento del control interno.

Finalmente, es importante considerar el acoplamiento selectivo al que refiere la literatura en lo relativo a la tercera línea de defensa. De acuerdo al mismo, se incorporan solamente criterios específicos de las normativas globales, pero que no derivan a una implementación plena. Esto redunda a que, en la práctica, la función de auditoría continúe focalizándose en los riesgos y procesos operativos clásicos, con lo que se limita el valor agregado (Contrafatto et al., 2025). Este fenómeno ofrece una explicación relativa a la debilidad en la correlación identificada.

Tabla 8. *Comparación del índice de madurez digital por sector económico (prueba de Kruskal-Wallis)*

Sector Económico	N	Mediana
Retail / Consumo masivo	5	2.89
Industrial / Manufactura	5	2.67
Financiero (bancos, seguros, financieras)	3	3.67
Servicios (salud, educación, consultoría)	3	1.00
Energía	1	2.67
Gubernamental / Sector público	1	3.00
Total consolidado	**18**	**2.94**

Nota. Resultado de la Prueba de Kruskal-Wallis (al comparar los sectores). H = 5.455; Valor p = 0.363. La prueba compara las medianas de los grupos.

La tabla 8 presenta las medianas del índice de madurez digital por sector económico. Descriptivamente, el sector financiero muestra la mediana más alta (3.67), como es de esperarse por la alta dependencia tecnológica, y el nivel de madurez en control interno y gobierno corporativo del mismo. Por otro lado, el sector servicios reporta la mediana más baja (1.00). La prueba de Kruskal-Wallis no encontró una diferencia estadísticamente significativa entre los grupos.

La mediana superior del sector financiero es un hallazgo consistente con el impacto de la regulación emitida por el Banco Central del Paraguay, en donde se exige un marco de control de IT basado en COBIT (Resolución SB. SG. 124/2017, 2017). De esta forma, los principios de ISACA (2018) se convierten en una guía de implementación obligatoria para este sector.

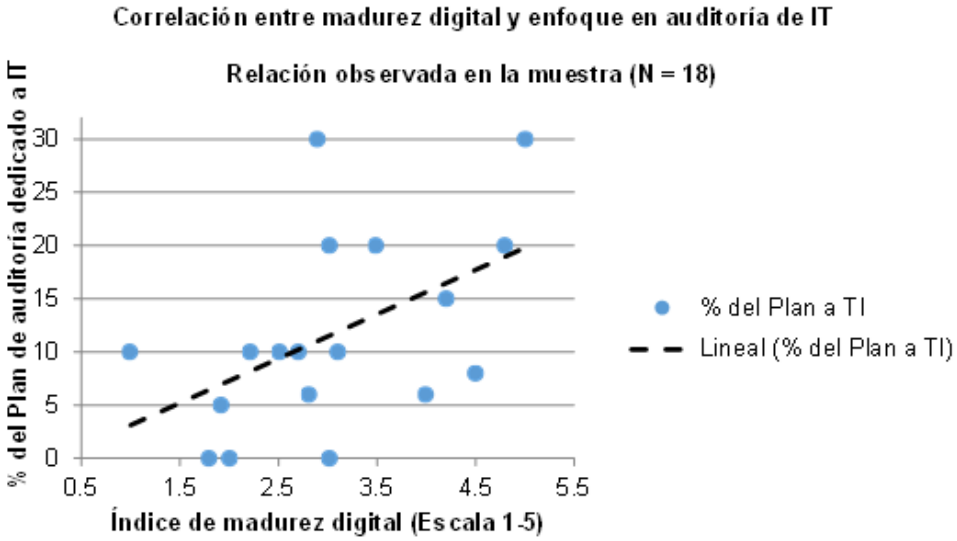
En contraste, en los otros sectores analizados, la adopción digital parece estar más impulsada por la necesidad de obtener una ventaja competitiva[6]. La mediana relativamente baja en el sector de servicios (1.00) evidencia un nivel inicial de incorporación tecnológica en sí mismo. El resultado es consistente con la literatura, que señala que las tecnologías emergentes están aún en fase de consolidación, por lo que se cuenta con limitada evidencia empírica (Agustí & Orta-Pérez, 2023).

Los hallazgos de la literatura reciente reconocen que las diversas organizaciones cuentan con niveles divergentes de avance en los procesos de madurez digital (d'Arcy & Eulerich, 2024). Lo anterior se condiciona adicionalmente de forma específica en lo relativo a la tercera línea de defensa, por una marcada dificultad para atraer y retener talento especializado en dicha materia (Hann et al., 2024).

Finalmente, es importante analizar estos resultados a la luz de lo que plantean Lenz et al. (2018). Los autores ponen de manifiesto la existencia de la denominada "tensión institucional" generada por fuerzas internas dentro de la organización que entran en conflicto, para lo cual el gerente de auditoría debe actuar con la habilidad estratégica dentro de la alta gerencia para conseguir los objetivos propuestos.

[6] KPMG International (2024) destaca que la mejora de la experiencia del cliente y la eficiencia operativa son los motores clave fuera de los sectores regulados.

Figura 1. *Correlación entre madurez digital y enfoque en auditoría de IT*



La figura 1 revela la relación entre el índice de madurez digital y el porcentaje del plan de auditoría dedicado a IT para los dieciocho casos con datos completos. La línea de tendencia de la regresión expone una clara pendiente positiva, en la que se visualiza una correlación entre el mayor nivel de madurez digital, que tiende por consiguiente a corresponder a un mayor enfoque en IT por parte de la auditoría. Sin embargo, es importante observar que los datos exhiben una considerable dispersión alrededor de esa línea.

Esta tendencia positiva es consistente con la teoría del enfoque basado en riesgos conforme con las *Normas Globales de Auditoría Interna* (Instituto de Auditores Internos, 2024). Esta teoría sostiene que la planificación de la auditoría debe ser un reflejo directo de los riesgos estratégicos de la organización. Los riesgos digitales se posicionan con una tendencia creciente, según indican publicaciones especializadas (KPMG International, 2024). La asociación positiva observada sugiere que los auditores de la muestra reaccionan, aunque sea modestamente, a ese nuevo panorama.

A nivel visual, el hallazgo más significativo es la alta dispersión de los puntos, lo que deja en evidencia la debilidad de la correlación entre las variables analizadas. Esta variabilidad refleja la divergencia en el enfoque y profundidad con la que la función de auditoría interna aborda los riesgos tecnológicos en las diferentes empresas. Esto es consistente con la evidencia empírica, que revela la coexistencia de diversos enfoques, inclusive, hasta en un mismo entorno regulado (Ferreira et al., 2025).

Esta divergencia en las observaciones se explica por el hecho de que la mera adopción a efectos formales del modelo de las tres líneas de defensa no es garantía de la gestión efectiva de los riesgos tecnológicos. La literatura advierte que, aun con modelos de gobernanza formalmente establecidos (que incluyen las tres líneas), los desafíos persisten, asociados a temas como definición de responsabilidades, entre otros (Valkenburg & Bongiovanni, 2024).

Otra explicación sobre la heterogeneidad en las respuestas puede atribuirse a la capacidad de acción con la que cuenta cada función de aseguramiento dentro del organigrama organizacional. d'Arcy y Eulerich (2024) refieren que la capacidad con la que cuenta la función de auditoría interna en cada organización no está asociada únicamente a la adopción formal de estándares, sino más bien al grado de integración y evolución de la función dentro del sistema de gobierno corporativo. Puntos con alta madurez digital, pero con un porcentaje bajo de plan de IT, pudiesen significar poca legitimidad para demandar recursos especializados.

En última instancia, es importante destacar que el gráfico no solo muestra una correlación entre las variables, sino también un mapa de cómo diferentes líderes del área ejercen su "influencia positiva" para navegar las presiones conflictivas propias de cada organización (Lenz et al., 2018). La dispersión de los resultados es la evidencia visual de que cada función forja una respuesta única de acuerdo con su contexto, en lugar de seguir un modelo estandarizado.

5. Conclusiones

El análisis relativo al nivel de madurez digital percibido en las empresas de la muestra permitió evidenciar que las organizaciones encuestadas se encuentran en un estadio intermedio, cercano al punto neutral de la escala. Este resultado evidencia la existencia de iniciativas de digitalización. No obstante, se debe considerar que la adopción integral aún se encuentra en fase de desarrollo, con variaciones llamativas entre los diferentes sectores.

Con respecto al aseguramiento de riesgos tecnológicos, se examinó su grado de enfoque en los diferentes planes anuales. Así, se revela que el porcentaje promedio de recursos dedicados a esta área es moderado, nuevamente con una considerable variabilidad entre las diferentes organizaciones. Por lo tanto, la asignación de recursos a la auditoría de IT es aún considerada heterogénea y no necesariamente siempre proporcional a los riesgos digitales que enfrenta el entorno empresarial.

El tercer objetivo específico del estudio buscó cuantificar la dirección y la fuerza de la correlación estadística existente entre ambas variables analizadas: el nivel de madurez digital percibido y el grado de enfoque en riesgos tecnológicos. Este análisis permitió establecer una asociación positiva, aunque de fuerza débil a moderada, entre ambas variables. Dicha asociación no alcanzó la significancia estadística, principalmente, asociada al tamaño de la muestra.

En consecuencia, el objetivo general de la investigación permitió concluir que las organizaciones paraguayas encuestadas están inmersas en procesos de transformación digital y, por consiguiente, sus respectivas funciones de auditoría interna asignan recursos a los riesgos tecnológicos. Se ha de tener presente que la correlación identificada entre ambas variables estudiadas es aún incipiente y requiere una mayor investigación. La adaptación de la función de auditoría a la era digital es un proceso en curso, con desafíos notables asociados a la asignación estratégica de recursos.

Por lo anteriormente planteado, la función de auditoría interna en Paraguay afronta un desafío transformador, al verse enfrentada a la obligatoriedad que establece el nuevo marco normativo global. A efectos de cumplir con dichos requerimientos, la cobertura de ciberseguridad debe integrarse de forma sistémica en los planes anuales de trabajo. En su defecto, se presenta una situación de incumplimiento profesional que pudiera comprometer la calidad del aseguramiento brindado.

Se destaca que la brecha identificada respondería al concepto de tensión institucional. Este condiciona la función del auditor interno en Paraguay, pues se procede a priorizar, dentro del plan anual, a las áreas consideradas tradicionales para preservar legitimidad frente a los grupos de interés. Por otra parte, la literatura destaca que existe evidencia de una percepción comparativamente menor sobre riesgo tecnológico entre los auditores no especializados en IT en relación a los auditores especializados (Nuijten et al., 2023).

Los procesos de transformación digital no modifican únicamente los riesgos organizacionales existentes, sino que, adicionalmente, aumentan las competencias requeridas, debido a la organización, en términos generales, y a la tercera línea de defensa, de manera particular. Al incorporar las tecnologías emergentes, es necesario que los auditores ajusten sus perfiles al volverlos más especializados en analítica y riesgos tecnológicos (Agustí & Orta-Pérez, 2023). Por lo tanto, la brecha observada pudiese estar asociada a la escasa disponibilidad de auditores con competencias técnicas avanzadas.

Desde una perspectiva individual, se recomienda a los profesionales de auditoría interna fortalecer activamente sus capacidades digitales y sus conocimientos en

riesgos tecnológicos emergentes, idealmente, a través de certificaciones de reconocida trayectoria, como las otorgadas por ISACA. De igual forma, la actualización continua en áreas como ciberseguridad, análisis de datos y auditoría de proyectos de transformación se vuelve clave para que sus planes de trabajo reflejen adecuadamente la realidad digital de las organizaciones, lo que garantiza la relevancia de la función.

A nivel institucional, se sugiere a las empresas y sus comités de auditoría promover activamente la integración del plan de aseguramiento de la tercera línea de defensa con la estrategia de transformación digital. Para lograr tal integración, la asignación de recursos adecuados para auditorías tecnológicas es fundamental, junto con la fomentación de la capacitación especializada del equipo de auditoría. Así, puede ser posible establecer una comunicación fluida entre las áreas, que permita alinear los riesgos digitales con el plan anual.

Finalmente, sobre la base de los hallazgos de esta investigación, futuras líneas de estudio a considerar deberían replicar este estudio con una muestra de mayor tamaño, a fin de obtener resultados estadísticamente significativos, con el objeto de generalizar a la población. Se recomienda también explorar la relación entre los niveles de madurez digital y otros aspectos de la auditoría interna, como la adopción de herramientas tecnológicas por la propia función o el impacto de la cultura organizacional.

Contribución de autores:

Rojas, J.: Conceptualización, Metodología, Software, Validación, Análisis formal, Investigación, Recursos, Curación de datos, Escritura -borrador original, Escritura, revisión y edición, Visualización, Supervisión, Administración del proyecto.

Jorge Rojas Barra (Rojas, J.)

Declaración de conflicto de Intereses

El autor declara que, durante el proceso de investigación, no ha existido ningún tipo de interés personal, profesional o económico que haya podido influenciar el juicio y/o accionar de los investigadores al momento de elaborar y publicar el presente artículo.

Referencias bibliográficas

Abdullah, A. A., & Almaqtari, F. A. (2024). The impact of artificial intelligence and Industry 4.0 on transforming accounting and auditing practices. *Journal of Open Innovation: Technology, Market, and Complexity*, 10, 1-20. https://doi.org/10.1016/j.joitmc.2024.100218

Agustí, M. A., & Orta-Pérez, M. (2023). Big data and artificial intelligence in the fields of accounting and auditing: A bibliometric analysis. *Spanish Journal of Finance and Accounting / Revista Española de Financiación y Contabilidad*, *52*(3), 412–438. https://doi.org/10.1080/02102412.2022.2099675

Al-Mohammedi, Y. A. (2020). The role of digitalization in developing internal audit practices in an IT environment. En The Institute of Electrical and Electronics Engineers (Ed.), *2nd Annual International Conference on Information and Sciences (AiCIS)* (pp. 230–236). IEEE Computer Society Conference Publishing Services.

Al Omari, H. M., Abdul Kadir, M. R., Sapingi, R. B., & Al-Dalaien, A. (2025). The dynamics of CAATs adoption in Jordan: Bridging top management support with auditor innovativeness and IT competency. *WSEAS Transactions on Business and Economics*, *22*, 20-31. https://doi.org/10.37394/23207.2025.22.3

Álvarez, F., & Toledo, M. (2022). *Digitalización de las pymes en América Latina*. (Policy Paper N.º 12). CAF; Banco de Desarrollo de América Latina y el Caribe. https://scioteca.caf.com/bitstream/handle/123456789/1970/Policy%20Paper%20%2312%20-%20Digitalizaci%C3%B3n%20de%20las%20PyMEs%20en%20Am%C3%A9rica%20Latina.pdf?sequence=3&isAllowed=y

Alzeban, A. (2021). CEO characteristics, management support for internal audit and corporate performance: An analysis of listed Malaysian companies. *Managerial Auditing Journal*, *37*(1), 102–128. https://doi.org/10.1108/MAJ-02-2021-3012

Aras, A., & Büyüközkan, G. (2023). Digital transformation journey guidance: A holistic digital maturity model based on a systematic literature review. *Systems*, *11*(4), 1-31. https://doi.org/10.3390/systems11040213

Cisco. (2024). *Cisco cybersecurity readiness index 2024*. Cisco. https://newsroom.cisco.com/c/dam/r/newsroom/en/us/interactive/cybersecurity-readiness-index/documents/Cisco_Cybersecurity_Readiness_Index_FINAL.pdf

Comisión Económica para América Latina y el Caribe. (2022). *Agenda digital para América Latina y el Caribe (eLAC2024)*. CEPAL. https://repositorio.cepal.org/server/api/core/bitstreams/1fae5881-feba-42b4-a0b0-53ba8fa1f679/content.

Comisión Económica para América Latina y el Caribe. (2023). *Paraguay: Perfil de política digital*. https://desarrollodigital.cepal.org/es/politica-digital/paises/paraguay

Committee of Sponsoring Organizations of the Treadway Commission. (2017). *COSO Enterprise Risk Management: Integrating with strategy and performance*. https://www.coso.org/_files/ugd/3059fc_61ea5985b03c4293960642fdce408eaa.pdf

Contrafatto, M., Moggi, S., Gervasio, D., & Montani, D. (2025). Audit society, organizational response and (de-)coupling: An Italian story. *Accounting, Auditing & Accountability Journal*, *38*(2), 537–564. https://doi.org/10.1108/AAAJ-08-2022-5974

d'Arcy, A., & Eulerich, M. (2024). Drivers for the maturity of integrated governance in organizations—An empirical investigation. *International Journal of Auditing*, *28*(3), 485–499. https://doi.org/10.1111/ijau.12338

Deloitte. (2018). *Digital Maturity Model: Achieving digital maturity to drive growth*. https://s16705.pcdn.co/wp-content/uploads/2018/08/Deloitte-DMM.pdf

Deloitte. (2024). *Global internal audit hot topics 2024*. https://www.deloitte.com/content/dam/assets-zone2/gr/en/docs/services/risk-advisory/2024/gr_global_internal_audit_hot_topics_noexp.pdf

Dutta, A., Roy, R., & Seetharaman, P. (2022). An assimilation maturity model for IT governance and auditing. *Information & Management*, *59*(1), 103569. https://doi.org/10.1016/j.im.2021.103569

Ernst & Young & The Institute of Internal Auditors. (2021). *The future of internal audit: (Webinar #2).* https://iia.no/wp-content/uploads/2021/04/IIA_Webinar_EY_2_The_Technology-002.pdf

ESET. (2024). *ESET security report 2024*. https://eset-la.com/images/mailing/2024/ESET-Security-Report_2024_ESPA%C3%91OL.pdf?utm_campaign=latam-es-online-esr_2024&utm_medium=email&utm_source=eloqua&elqTrackId=df1f8ad7176c4e9d9f246cc8b2d1059f&elq=9046d550e98048e4b9362a591df83612&elqaid=2834&elqat=

Eulerich, M., & Bonrath, A. (May de 2025). *Technology and internal auditing: An overview of performance effects* (SSRN paper). SSRN Electronic. https://doi.org/10.2139/ssrn.5255858

Ferreira, L. V. A., Alves, C. A. D. M., Peotta De Melo, L., & Nunes, R. R. (2025). Internal audit strategies for assessing cybersecurity controls in the Brazilian financial institutions. *Applied Sciences*, *15*(10), 1-22. https://doi.org/10.3390/app15105715

Financial Crime Academy LLC. (2026). *Beneficios y costes de los controles internos*. https://financialcrimeacademy.org/es/beneficios-y-costes-de-los-controles-internos/

Firza, S. U., Kesuma, S. A., & Muda, I. (2025). The role of digital transformation in improving audit and accounting information quality. *New Applied Studies in Management, Economics & Accounting*, *103*, 1-14.

Hann, R. N., Yang, J., & Zheng, Y. (2024). *The price of an accountant shortage: Evidence from job vacancy duration and internal control weaknesses* (SSRN Scholarly Paper 4695588). SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4695588

Haryanti, T., Rakhmawati, N. A., & Subriadi, A. P. (2023). The extended digital maturity model. Big Data and Cognitive Computing, *7*(1), 1-24. https://doi.org/10.3390/bdcc7010017

Herrera-Sánchez, M. J. (2024). Transformación digital en la auditoría interna y su efecto en la eficiencia operativa. *Revista Científica de Ciencia y Método*, *2*(3), 13–25. https://doi.org/10.55813/gaea/rcym/v2/n3/45

The Institute of Internal Auditors. (2025). *Latin America risk in focus 2025: Board briefing*. https://www.theiia.org/globalassets/site/foundation/latest-research-and-products/risk-in-focus/2025/latin-america-risk-in-focus-2025-board-briefing-spanish.pdf

Instituto de Auditores Internos. (2024). *Normas Globales de Auditoría Interna*. https://www.theiia.org/en/standards/2024-standards/global-internal-audit-standards/

Instituto de Auditores Internos. (2025). *Ciberseguridad - Requisito temático*. https://www.theiia.org/globalassets/site/standards/topical-requirements/cybersecurity/cybersecurity_topical_requirement_spanish.pdf

ISACA. (2018). *COBIT 2019 - Governance and management objectives*. https://netmarket.oss.aliyuncs.com/df5c71cb-f91a-4bf8-85a6-991e1c2c0a3e.pdf

ISACA. (2020). *IT audit framework - A professional practices framework for IT audit*.

https://www.isaca.org/resources/frameworks-standards-and-models

Josh, P. L., & Karyawati, G. (2022). The institutional theory on the internal audit effectiveness: The case of India. *Iranian Journal of Management Studies*, *15*(1), 35-48. https://www.sid.ir/en/VEWSSID/J_pdf/1101-277491-en-1123179.pdf

KPMG International. (2024). *Global tech report 2024. Beyond the hype: Balancing speed, security and value*. https://assets.kpmg.com/content/dam/kpmgsites/xx/pdf/2024/09/kpmg-global-tech-report-2024.pdf

Lenz, R., & Sarens, G. (2012). Reflections on the internal auditing profession: what might have gone wrong? *Managerial Auditing Journal*, *27*(6), 532–549. https://doi.org/10.1108/02686901211236382

Lenz, R., Sarens, G., & Klarskov Jeppesen, K. (2018). In search of a measure of effectiveness for internal audit functions: An institutional perspective. *EDPACS*, *58*(1), 1-19. https://doi.org/10.1080/07366981.2018.1511324

Ley 1034/1983. (1983). Ley del Comerciante. Congreso Nacional del Paraguay. https://www.bacn.gov.py/leyes-paraguayas/2538/del-comerciante

Ley 1183/1985. (1985). *Código Civil Paraguayo*. Congreso Nacional del Paraguay . https://www.bacn.gov.py/leyes-paraguayas/5293/codigo-civil

Ley 6534/2020. (2020). *Ley de Protección de Datos Personales Crediticios*. Congreso Nacional del Paraguay. https://www.bacn.gov.py/leyes-paraguayas/9417/ley-n-6534-de-proteccion-de-datos-personales-crediticios

McKinsey & Company. (2024). *What is digital transformation?* https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-digital-transformation#/download/%2F~%2Fmedia%2Fmckinsey%2Ffeatured%20insights%2Fmckinsey%20explainers%2Fwhat%20is%20digital%20transformation%2Fwhat-is-digital-transformation-v2.pdf%3F

Ministerio de Industria y Comercio de Paraguay. (2025). *Respuesta a solicitud de acceso a la información pública 93590 (Memorando y anexos)*. https://informacionpublica.paraguay.gov.py/public/2025/1753298792_1_25-07-2169MEMOrespuestasolicitudInformacin93590yanexo.pdf

Ministerio de Tecnologías de la Información y Comunicación. (2022). *Plan nacional TIC - Paraguay 2022-2030*. https://mitic.gov.py/plan-nacional-de-tic-2022-2030/

Ministerio de Tecnologías de la Información y Comunicación. (2025). *Portal unificado de* información pública. https://informacionpublica.paraguay.gov.py/#!/ciudadano/solicitud/93590

Nuijten, A. L. P., Keil, M., & Zwiers, B. (2023). Internal Auditors' Perceptions of Information Technology-Related Risks: A Comparison Between General Auditors and Information Technology Auditors. *Journal of Information Systems*, *37*(1), 67–83. https://doi.org/10.2308/ISYS-2020-040

Protiviti, & NC State University's ERM Initiative. (2022). *Executive perspectives on top risks*. https://www.protiviti.com/sites/default/files/2022-12/nc-state-protiviti-survey-top-risks-executive-summary-2022-2032_global.pdf

Resolución SB. SG. 32/2008. (2008). *Reglamento General sobre Sistemas de Control Interno*. Banco Central del Paraguay. https://www.bcp.gov.py/documents/20117/375860/RESOLUCIONSBSGNro3208.pdf/4201cea6-ec00-2432-3680-c2514050cccf

Resolución SB. SG. 124/2017. (2017). *Manual de Control Interno Informático para las Entidades Supervisadas por la Superintendencia de Bancos*. Banco Central del Paraguay. https://www.bcp.gov.py/documents/20117/0/Manual+de+Gobierno+y+-Control+de+TI.pdf/9b179744-cdcd-c82c-1fcf-416c6a8a512a

Slapničar, S., Vuko, T., Čular, M., & Drašček, M. (2022). Effectiveness of cybersecurity audit. *International Journal of Accounting Information Systems*, 44, 1-21. https://doi.org/10.1016/j.accinf.2021.100548

Stepanyan, S. (2023). The evolution of internal audit in a digital environment. *Alternative*, 151–156. https://doi.org/10.55528/18292828-2023.2-01

Tharouma, S. (2025). *Impact of digital transformation on the performance of management control systems* [Tesis doctoral, Business School- Kolea]. Repositorio Dspace. http://dspace.esc-alger.dz:8080/xmlui/handle/123456789/2167

Tubis, A. (2023). Digital maturity assessment and organizational transformation: A review and conceptual framework. *Sustainability*, *15*, 1-24. https://doi.org/10.3390/su152015122

Usul, H., & Alpay, B. Y. (2025). Digital transformation in internal audit: Paradigm shifts, emerging risks, and strategic resilience. *European Journal of Digital Economy Research*, *6*, 23–36. https://doi.org/10.5281/zenodo.12819118

Valkenburg, B., & Bongiovanni, I. (2024). Unravelling the three lines model in cybersecurity: A systematic literature review. *Computers & Security*, *139*, 1-11. https://doi.org/10.1016/j.cose.2024.103708

Vaya-Arboledas, Á., Ferrer-Oliva, M., & Medina-Merodio, J. A. (2025). Evolution and perspectives in IT governance: A systematic literature review. *Computers*, *14*(12), 1-48. https://doi.org/10.3390/computers14120520

Vitalis, A., Boritz, J. E., & Simeoni, L. (2024). Enhancing CPA competencies for internal audit roles. *International Journal of Auditing*, *28*(3), 458–484. https://doi.org/10.1111/ijau.12337

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

World Economic Forum. (2016). *Digital transformation of industries: Digital enterprise.* World Economic Forum. https://www.netscout.com/digital-transformation-realtime-information-platform/jim/data/pdf/jim/world-economic-forum-digital-transformation-of-industries.pdf

Wu, T.-H., Huang, S. Y., Chiu, A.-A., & Yen, D. (2024). IT governance and IT controls: Analysis from an internal auditing perspective. *International Journal of Accounting Information Systems*, *52*, 100663. https://doi.org/10.1016/j.accinf.2023.100663

Fecha de recepción: 06/09/2025
Fecha de revisión: 18/09/2025
Fecha de aceptación: 25/02/2026
Contacto: jorge.rojas@unae.edu.py