ENTRELÍNEAS
REVISTA CIENTÍFICA INDEXADA DE LA UNIVERSIDAD EUROAMERICANA
ISSN L 2953-3023
Vol. 4. No. 2. Julio-Diciembre 2025
https://ambientevirtualuea.org/ojs/index.php/entrelineas/index

PERCEPCIÓN Y CONTRIBUCIÓN ESTRATÉGICA DE LAS AUDITORÍAS DE SISTEMAS DE INFORMACIÓN EN EL CONTEXTO ORGANIZACIONAL

Perception and strategic contribution of information systems audits in the organizational context

Carlos V. Bruce[1]
https://orcid.org/0009-0004-4223-0821

Juan Rigoberto Castillo Serracín[2]
https://orcid.org/0009-0006-5821-7028

Recibido: 10/06/2025
Aceptado: 18/08/2025
Publicado: 25/08/2025

Cómo citar este artículo: Bruce, C., Castillo Serracín, J. (2025). Percepción y contribución estratégica de las auditorías de sistemas de información en el contexto organizacional. *Entrelineas, 4*(2), e040202. https://doi.org/10.56368/Entrelineas422

RESUMEN

El estudio tuvo como objetivo general analizar la percepción de las auditorías de sistemas de información en el fortalecimiento de los controles internos, la protección de los activos digitales y la generación de valor estratégico en las organizaciones. Se realizó una investigación empírica basada en encuestas dirigidas a profesionales que trabajan en organizaciones del distrito de San Miguelito, Panamá. La muestra incluyó a auditores, personal de TI, gerentes y otros colaboradores relevantes. El instrumento consistió en un cuestionario que evaluó la percepción sobre los diversos aspectos relacionados con las auditorías de sistemas de información y su impacto organizacional. Entre los resultados destacados se conoció que, aunque solo el 47% de los encuestados considera que las auditorías fortalecen los controles internos, el 65% afirma que sus recomendaciones mejoran la protección de los activos digitales. Igualmente, el 72% reconoció que las auditorías generan confianza en el manejo de datos, aunque solo el 50% opina que contribuyen a reducir incidentes cibernéticos, y el 70% consideró insuficientes los procesos actuales para garantizar la eficiencia en la gestión de los sistemas de información. Se evidenció que las auditorías de sistemas de información son vistas como herramientas

[1] Universidad de Panamá, Facultad de Informática Electrónica y Comunicación (FIEC), carlos.bruce@up.ac.pa
[2] Universidad de Panamá, CRUSAM, Facultad de Informática Electrónica y Comunicación (FIEC), juan.castillos@up.ac.pa

estratégicas en muchas organizaciones, aunque persisten desafíos en su implementación y alcance, por lo que se considera necesario mejorar la capacitación técnica de los auditores, fortalecer la adopción de recomendaciones y alinear los procesos de auditoría con los objetivos estratégicos de la organización para aumentar su impacto.
Palabras clave: auditorías de sistemas, seguridad informática, controles internos, eficiencia organizacional, activos digitales.

ABSTRACT

The study's overall objective was to analyze perceptions of information systems audits in strengthening internal controls, protecting digital assets, and generating strategic value in organizations. Empirical research was conducted based on surveys of professionals working in organizations in the San Miguelito district of Panama. The sample included auditors, IT staff, managers, and other relevant collaborators. The instrument consisted of a questionnaire that assessed perceptions of various aspects related to information systems audits and their organizational impact. Among the notable results, it was found that, although only 47% of respondents believe that audits strengthen internal controls, 65% affirm that their recommendations improve the protection of digital assets. Similarly, 72% acknowledged that audits generate confidence in data management, although only 50% believe they contribute to reducing cyber incidents, and 70% considered current processes insufficient to ensure efficient management of information systems. It was evident that information systems audits are viewed as strategic tools in many organizations, although challenges persist in their implementation and scope. Therefore, it is considered necessary to improve auditors' technical training, strengthen the adoption of recommendations, and align audit processes with the organization's strategic objectives to increase their impact.
Keywords: systems audits, information security, internal controls, organizational efficiency, digital assets.

Introducción

Siendo cada vez más dependientes de la tecnología, las organizaciones transitan por situaciones conflictivas en la protección de sus sistemas de información y activos digitales. Estos desafíos comprometen la seguridad de los datos, afectan la seguridad organizacional y el logro de los objetivos estratégicos. En este contexto, las auditorías de sistemas de información se posicionan como medios que garantizan el fortalecimiento de los controles internos, mitigan los riesgos asociados con los activos digitales y aumentan el valor estratégico de las organizaciones. En este entorno, las auditorías de sistemas de información (ASI) han evolucionado considerablemente desde su origen, consolidándose como un medio necesario para apoyar la gestión organizacional moderna. Estas auditorías impactan directamente en la identificación y mitigación de riesgos tecnológicos, desempeñando un papel importante en el mejoramiento de los procesos internos y en la generación de valor estratégico para las organizaciones.

El concepto de auditoría de sistemas de información inició su desarrollo en las décadas de 1960 y 1970, cuando el uso de la computadoras en las empresas se hizo más común. Inicialmente, las auditorías de TI se limitaban a verificar aspectos técnicos como el rendimiento y la seguridad de los sistemas. Con el tiempo, estas prácticas evolucionaron para incluir procesos y controles internos relacionados con la gestión de información. En la década de 1990, con la expansión de la conectividad global a través de internet, las auditorías de sistemas de información comenzaron a afrontar desafíos más complejos, relacionados con al ciberseguridad y la privacidad de los datos. La rápida digitalización y la mayor dependencia de activos tecnológicos incrementaron las amenazas

cibernéticas, obligando a las organizaciones a reforzar sus controles internos mediante auditorías más rigurosas y sofisticadas (van den Heuvel, 2025).

Actualmente, las auditorías de sistemas de información han ampliado su alcance para incluir dentro de la protección de activos digitales su alineación con los objetivos estratégicos de las empresas. Conociendo el entorno empresarial de la ciudad de Panamá, donde convergen grandes corporaciones y pequeñas empresas tecnológicas, las auditorías de sistemas de información se deben convertir en un medio para mantener la seguridad, la eficiencia y la sostenibilidad organizacional, lo que en la actualidad se conoce como un sistema de ciberseguridad.

La ciberseguridad "es la práctica de implementar personas, procesos, políticas y tecnologías para proteger a las organizaciones, sus sistemas críticos e información confidencial de los ataques digitales" (Gartner, 2024, párr. 1). Ante esta realidad, el uso y la dependencia de los sistemas de información en las organizaciones modernas presentan riesgos que comprometen su seguridad, eficiencia y competitividad, aunque las auditorías de sistemas de información (ASI) se han posicionado como herramientas para mejorar la gestión ya que, si una implementación es inadecuada o insuficiente, puede exponer a las organizaciones a vulnerabilidades críticas y, si bien es cierto, "los recursos de informática son muy especializados y frecuentemente muy costosos, pero son de suma importancia en las áreas de sistemas" (Razo, 2002, p. 138).

Entre los principales riesgos asociados se encuentra la posibilidad de incluir controles internos deficientes que llevan a exponer fraudes, errores operativos y pérdida de confianza por parte de los stakeholders. Así mismo, la falta de protección de los activos digitales presenta un grave peligro, porque las amenazas cibernéticas como el ransomware, el phishing y los ataques de denegación de servicio (DDoS) tienen la capacidad de paralizar operaciones críticas y generar pérdidas financieras y de reputación (Lozano, 2024). Es por ello que el uso de auditorías de sistemas de información que no estén en línea con los objetivos estratégicos de la organización puede llevar a desaprovechar los recursos y a percibir negativamente la utilidad. Es decir, "que la información en combinación con las nuevas tecnologías que la soportan aparece como un nuevo factor productivo y estratégico que se suma a los ya tradicionalmente conocidos como el trabajo y el capital, diferenciándose […] por su característica de intangibilidad" (Peña Calvo, 2015, p. 16). Hay que añadirle la adopción de mejores prácticas en los entornos empresariales dinámicos, como el que vive ciudad de Panamá, donde la heterogeneidad organizacional y las restricciones presupuestarias dificultan la implementación de auditorías efectivas y sostenibles.

Por esta situación, resulta necesario analizar cómo los procesos de auditoría en este aspecto pueden mejorarse para mejorar las áreas más vulnerables. Identificar los métodos y las prácticas que ayuden a fortalecer los controles internos, proteger los activos digitales generando valor estratégico, son necesidades para las organizaciones que buscan mantenerse seguras.

Ciudad de Panamá, como epicentro regional de actividades económicas y empresariales, alberga una diversidad de empresas que dependen de sistemas digitales robustos para su funcionamiento y competitividad. Sin embargo, muchas de estas organizaciones se enfrentan a la constante amenaza de las vulnerabilidades digitales que ponen de manifiesto la necesidad de realizar procesos de auditoría más efectivos para proteger los activos digitales, generando valor estratégico en la toma de decisiones.

El problema central de esta investigación está en la falta de entendimiento claro sobre el impacto real de las ASI en las organizaciones locales, limitando la capacidad de adaptarse a las situaciones que atraviese, aprovechando su potencial como herramientas estratégicas. Se aborda esta problemática, proporcionando recomendaciones para mejorar los beneficios de las auditorías de sistemas de información en el fortalecimiento de la seguridad y eficiencia organizacional.

El propósito es analizar la percepción del impacto que tienen los procesos de auditoría de sistemas de información en empresas de la ciudad de Panamá, con una visión particular en tres áreas: el fortalecimiento de los controles internos, la protección de los activos digitales y la contribución al logro de los objetivos organizacionales. Los resultados buscan contribuir al conocimiento aplicado en el campo de la auditoría de sistemas de información, ofreciendo a los

investigadores y a los profesionales un sistema de herramientas estratégicas que fortalezcan la seguridad y la eficiencia organizacional. La investigación de delimita al análisis del impacto de las auditorías de sistemas de información en empresas de Ciudad de Panamá, enfocándose en la contribución que constituye esta operación para el fortalecimiento de los controles internos, la protección de los activos digitales y la generación de valor estratégico. Así mismo, geográficamente se ubica en el distrito de San Miguelito en la provincia de Panamá, abarcando empresas que implementan auditorías de sistemas de información en esta zona.

Metodología

Con un enfoque cuantitativo para definir las percepciones y experiencias de la población objeto de estudio, se realizó un cuestionario cerrado. Los datos se recolectaron directamente a través de la encuesta realizada al personal que conformó la muestra del estudio. Si se analiza el período de tiempo para este proyecto, se trata de un estudio transversal, ya que los datos se recolectaron en un solo momento.

La población de este estudio estuvo conformada por 10 empresas, de donde se extrajo una muestra de 50 profesionales y empleados en áreas que interactúan con los sistemas de información y auditorías (5 colaboradores por empresa), aunque no cuentan con una alta especialización en el área, ya que la percepción que tenían fue la que ayudó a obtener una visión realista del entorno de las empresas en San Miguelito.

Se tomaron en cuenta a los colaboradores en departamentos de Tecnología de Información (TI) que gestionan la infraestructura tecnológica en las empresas.

Los auditores internos y externos, porque aunque no sean especialistas en auditoría de sistemas, interactúan con sistemas de información en sus procesos de evaluación.

Los administradores y gerentes que participaron estaban encargados de la supervisión y toma de decisiones relacionadas con la implementación tecnológica.

Se trabajó también con profesionales de pequeñas y medianas empresas (Pymes), porque es el perfil con mayor presencia en este distrito y representan una parte importante del sector económico de Panamá. Esta característica destaca la importancia de conocer cuál es la percepción en los procesos de auditoría y seguridad.

Con las características de la muestra encuestada, se pudo determinar el nivel de madurez tecnológica en Ciudad de Panamá. Utilizando la técnica de la encuesta, en el mes de noviembre de 2024 se aplicó como instrumento un cuestionario diseñado con un total de 10 preguntas dicotómicas para facilitar la respuesta de los encuestados.

Resultados

Las auditorías de sistemas de información (ASI) constituyen un campo relevante dentro de la gestión organizacional, al ser garantes de la eficiencia, seguridad y confiabilidad de los sistemas tecnológicos. De acuerdo con Information Systems Audit and Control Association (Sayana, 2022), la auditoría de sistemas de información es un proceso sistemático que evalúa y valida la integridad, confidencialidad, disponibilidad y cumplimiento normativo de los sistemas informáticos utilizados en una organización. Estas auditorías surgieron como una necesidad ante el auge de las tecnologías de la información en las décadas de 1970 y 1980, cuando las empresas iniciaron su dependencia de los sistemas computacionales para desarrollar mejor sus operaciones.

Con el avance tecnológico, las ASI han evolucionado; anteriormente solo se trataba de la verificación de hardware y software, pero en la actualidad se centran en la gestión de los riesgos tecnológicos, la seguridad cibernética y el cumplimiento de las normativas internacionales, como el caso del estándar ISO/IEC 27001, que establece los requisitos para gestionar la seguridad de la información (ISO/IEC, 2022).

Importancia de las auditorías de sistemas de información

Las ASI son necesarias para identificar las vulnerabilidades de los sistemas y proteger a las empresas para que operen bajo los estándares más rigurosos. Las amenazas actuales son de índole cibernética y con el paso del tiempo se vuelven más sofisticadas; con la ayuda de las auditorías se puede alcanzar una evaluación crítica de los controles internos y fortalecer la protección de los activos digitales. La Encuesta Global sobre el Futuro de la Ciberseguridad de Deloitte (2023), el 91% de las organizaciones informó haber enfrentado al menos un incidente o brecha cibernética durante el último año. Además, un tercio (38%) reportó haber lidiado con entre seis y diez eventos. El informe destaca que la frecuencia de estos incidentes varía según el grado de madurez cibernética enfrenten más de diez eventos (21%), en contraste con las de alta madurez, donde este porcentaje se reduce al 13%.

Las auditorías funcionan para evaluar la protección de los datos, generando valor estratégico, algo que logran al proporcionar información específica sobre la eficiencia de los sistemas y las áreas de mejora, con lo que ofrecen resultados a las organizaciones para que alineen los recursos tecnológicos con los objetivos estratégicos, mejorando su competitividad en el mercado y protegiendo a los clientes.

Metodologías utilizadas en las auditorías de los sistemas de información

Existen diversas metodologías para realizar las ASI, siendo las más destacadas estas tres:

1. COBIT (Control Objectives for Information and Related Technologies). Es un marco desarrollado por ISACA que se centra en la gobernanza y gestión de las TI, ofreciendo una visión completa de la evaluación y mejora de los procesos tecnológicos en las organizaciones (COBIT, 2019).
2. ITIL (Information Technology Infrastructure Library). Se trata de una metodología que guía la gestión de los servicios de TI y se utiliza frecuentemente para garantizar la calidad y eficiencia en los procesos auditados.
3. NIST Cybersecurity Framework. Proporciona un conjunto de directrices para evaluar y mejorar la resiliencia cibernética en las empresas (Barrett, 2018).

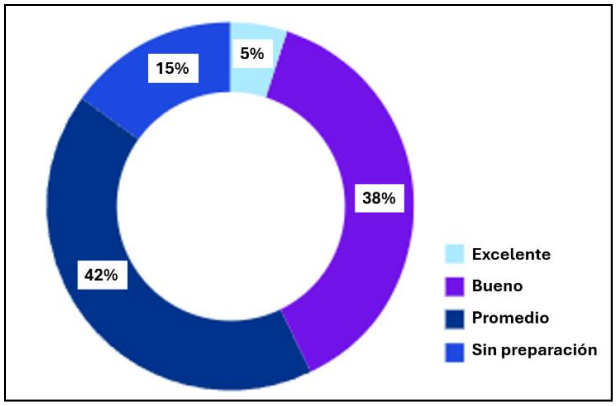
Impacto de las auditorías en la seguridad organizacional

La seguridad de la información es uno de los componentes básicos de las ASI. Según una de las últimas encuestas de KPMG (2024), solo el 42% de los encuestados afirmó tener una preparación excelente o buena para los riesgos de auditoría asociados con tecnologías emergentes como la seguridad en la nube, la inteligencia artificial, el aprendizaje automático y la cadena de bloques. Una preocupación es la presencia de incógnitas desconocidas, donde los equipos de auditoría no son conscientes de los riesgos y, en consecuencia, no los incluyen en las auditorías.

KPMG señala que, como especialistas en riesgo y control, los profesionales de auditoría interna están en una posición única para asesorar a la empresa sobre cómo enfrentar de manera más eficaz el impacto de estas nuevas tecnologías que se encuentran presentes en todos los aspectos de gestión de la empresa. Ante la pregunta sobre qué tan bien preparados estaba su equipo para enfrentar posibles emergencias tecnológicas, las respuestas ofrecidas demuestran que todavía hace falta crear conciencia en este aspecto, tal como se presenta en la Figura 1.

Figura 1

Qué tan bien preparado está su equipo para enfrentar posibles emergencias tecnológicas



Nota. KPMG (2024, p. 8).

Estas auditorías permiten implementar controles como los firewalls, sistemas de detección de intrusos (IDS) y herramientas de monitoreo continuo para prevenir accesos no autorizados y pérdida de datos.

A pesar de sus beneficios, las ASI deben atravesar por situaciones importantes que tienen que ver con la evolución acelerada de las amenazas cibernéticas y la falta de personal especializado. Según Gartner (2024), la escasez de talento en ciberseguridad es una de las principales barreras para poder cumplir con los niveles de calidad en las auditorías en muchas organizaciones.

Relación entre auditorías de sistemas de información y el cumplimiento normativo

En Panamá, la adopción de marcos normativos internacionales debe impulsar la realización de ASI como un mecanismo más para garantizar el cumplimiento de leyes relacionadas con la privacidad de los datos y la seguridad digital, y porque "la información que es tratada en una organización es un recurso crítico que debería ser protegido, ya que la misma es la base de la mayoría de las decisiones que son adoptadas a lo largo del tiempo" (Sánchez Valriberas, 2008, p. 3). Un ejemplo es la Ley 81 26 de marzo de 2019 sobre protección de datos personales, que establece directrices claras para la gestión de la información en las organizaciones panameñas.

Generación de valor estratégico

La auditoría de sistemas trasciende el ámbito técnico al contribuir con la estrategia organizacional para que ajusten sus objetivos tecnológicos con los estratégicos, alcanzando un impacto positivo en su competitividad. Slapničar et al. (2022) se centran en la eficacia de la auditoría de ciberseguridad (CSA) como parte de la función de auditoría interna: al evaluar la eficacia de las políticas de seguridad cibernética y los controles internos, la CSA contribuye a la protección de los activos digitales que se necesitan para el funcionamiento y la eficiencia de la organización, porque si es eficaz, llega a considerarse como un componente estratégico para mitigar los riesgos cibernéticos y garantizar la continuidad del negocio.

El Cybersecurity Audit Index propuesto, con sus tres dimensiones (planificación, ejecución e informe) proporciona un marco para evaluar la madurez y eficacia de la CSA. Las organizaciones pueden utilizar este índice para identificar áreas de mejora y fortalecer su postura de seguridad, traduciendo el proceso en un valor estratégico a largo plazo.

Ali et al. (2024) analizan el impacto de la calidad de la auditoría remota (RAQ) en la calidad del trabajo de auditoría (QAW), destacando la importancia de la preparación tecnológica del cliente y el auditor. Se puede argumentar que la adopción de tecnologías avanzadas para la auditoría remota (como describen los autores en el documento) puede aportar valor estratégico al mejorar la eficiencia y eficacia de sus auditorías; una mayor eficiencia en los procesos puede liberar recursos para que los auditores se centren en áreas de mayor riesgo y valor estratégico para la organización.

Así mismo, Ali et al. (2024) señalan que la preparación tecnológica del cliente (CLTR), cuando facilita el acceso a la información y ejecución de los procedimientos de auditoría, ayuda a tener una mejor comprensión de los procesos y controles de la organización, aportando valor estratégico a la auditoría.

Al Lawati et al. (2024), cuando destacan el papel de la gobernanza -en particular, la composición de la junta directiva- en la calidad de la auditoría, explican cómo la auditoría de sistemas proporciona información sobre la eficacia de la estructuras de gobernanza y su impacto en la gestión de riesgos, la transparencia y la rendición de cuentas, que son los aspectos que se necesitan para generar valor estratégico. De estas tres fuentes (Slapničar et al., 2022; Ali et al., 2024; y Al Lawati et al., 2024, respectivamente) se destaca la eficacia de la auditoría de ciberseguridad, la adopción de las tecnologías avanzadas para la auditoría remota, la preparación tecnológica del cliente, el uso de Big Data y la gobernanza, como aspectos que, al ser evaluados y mejorados a través de la auditoría de sistemas, fortalecen la generación de valor estratégico para la organización.

Así mismo, Martin (2022) describe cómo un enfoque integrado para las auditorías de TI y seguridad pueden conducir a eficiencias y una mejor comprensión de la postura de seguridad de una organización, lo que indirectamente puede interpretarse como una forma de valor estratégico. Al respecto, el estudio destaca los siguientes puntos relacionados:

Con respecto a la eficiencia y ahorro de recursos, la integración de las auditorías de seguridad permite que la evidencia recopilada se pruebe una sola vez y se utilice en múltiples marcos, liberando recursos para que los equipos de auditoría y TI se centren en las operaciones diarias en lugar de estar en un modo de auditoría permanente. Esta eficiencia puede considerarse un valor estratégico, porque permite a la organización mejorar el uso de los recursos y enfocarlos en áreas que generan mayor valor. Para contar con una mayor visibilidad de la postura de seguridad, la integración de marcos y el uso de un repositorio de datos centralizado le da una visión más completa de la postura de seguridad de la organización y sus obligaciones de riesgos y asignación de recursos.

En cuanto a la colaboración entre auditoría interna y TI, Martin (2022) enfatiza la importancia de la colaboración entre la función de auditoría interna y el equipo de TI para construir una estrategia de ciberseguridad sólida, que es una colaboración que facilita la detección temprana de las fallas de ciberseguridad y la implementación de controles más efectivos, para reducir los riesgos y generar valor estratégico al proteger los activos de la organización.

Finalmente, para crear una visión proactiva en la gestión de riesgos, se propone crear un modelo de datos integrado que permite a los equipos de auditoría y TI determinar cómo un riesgo de ciberseguridad o un control ineficaz puede llegar a afectar a la empresa. Con este enfoque proactivo, la organización anticipa y mitiga los riesgos de manera más eficaz, ayudando a generar valor estratégico en la medida en que minimiza las interrupciones del negocio y protege la reputación de la organización.

Encuesta realizada

En los datos sociodemográficos se tomó en cuenta el sexo, la edad, el nivel educativo, la función en la organización, y los años de experiencia en la organización. El análisis de los resultados para determinar el sexo del encuestado, con una ponderación de 55% masculino y 45% femenino indicó lo siguiente:

La muestra de la investigación expresa una distribución equilibrada entre los encuestados, aunque ligeramente inclinada hacia los hombres. El 55% de los participantes eran hombres y el 45% mujeres. Este balance es positivo, porque garantiza que ambos sexos estén similarmente representados en el análisis y permite realizar comparaciones equitativas entre las respuestas de hombres y mujeres. Aunque existe una pequeña diferencia, no es una disparidad significativa. La mayor representación masculina está relacionada con la naturaleza del sector y el tipo de organización donde se llevó a cabo el estudio. Aunque el sesgo es mínimo, los resultados pueden estar influenciados por el sexo en ciertos aspectos relacionados con la percepción de la auditoría de sistemas, las seguridad de la información y otros temas tratados.

Los resultados de la pregunta sobre la edad, con una ponderación de 25% menor de 30 año, 50% entre 30 y 50 años y 25% mayor de 50 años, indica que la muestra está predominantemente compuesta por individuos de entre 30 y 50 años, lo que representa el 50% de los participantes. Este rango de edad es comúnmente considerado como el grupo con mayor experiencia laboral y, por lo tanto, pudo ofrecer respuestas más fundamentadas en cuanto a la percepción de los procesos de auditoría de sistemas y la seguridad de la información, ya que tiene una mejor comprensión de lo que sucede organizacionalmente en las áreas estudiadas.

Aunque la mayoría de los participantes están entre 30 y 50 años, la muestra también incluye un 25% de personas menores de 30 año y otro 25% mayores de 50. Esta representación diversificada permitió obtener diversas perspectivas; los participantes más jóvenes estaban más familiarizados con las nuevas tecnologías, mientras que los mayores de 50 aportaron una visión más crítica sobre los procesos y su evolución a lo largo del tiempo. La distribución de los participantes en tres rangos etarios equilibrados (25%-50%-25%) ayudó que el estudio considerara las opiniones de diferentes generaciones dentro de la organización. Esto sirvió para entender cómo los diferentes grupos etarios percibían la eficiencia de los procesos de auditoría y los sistemas de seguridad, que es un dato que puede utilizarse en las empresas para influir en la adopción de tecnologías o en la resistencia al cambio.

Aunque la distribución fue bastante equilibrada, las diferencias de edades influyeron en la percepción de la auditoría de sistemas. Los más jóvenes y los mayores presentaron enfoques distintos en cuanto a la percepción de la seguridad digital y la gestión de riesgos, mientras que el grupo intermedio estuvo en una posición más pragmática y orientada a la implementación de soluciones tecnológicas.

Al preguntar sobre el nivel educativo, la distribución expuso que el 30% tenía nivel secundario el 60% estudios técnicos o universitario y el 10% posgrado. La mayoría de los participantes (60%) tienen formación técnica o universitaria, y ello está relacionado con gran parte de los roles con auditorías y tecnología en las organizaciones, donde se exige un nivel educativo intermedio o superior, y fue un grupo que comprendió con más profundidad los aspectos técnicos y operativos de los sistemas de información y sus auditorías.

El 30% de los encuestados tienen solamente formación secundaria, indicando la presencia de personal en roles de apoyo y funciones operativas en las organizaciones que participan de alguna manera en los sistemas de información o sus auditorías. Su aporte fue menos técnico, pero el grupo proporcionó una visión práctica desde el ámbito operativo. Solo el 10% de los encuestados han cursado estudios de posgrado, interpretándose como un área de mejora en el contexto organizacional para la zona de San Miguelito. Esta limitada representación de profesionales con formación avanzada influyó en las capacidades estratégicas y de innovación en el uso de las auditorías para la seguridad y eficiencia organizacional. La muestra estuvo compuesta principalmente por individuos con formación técnica o universitaria, haciendo que las conclusiones del estudio mostraran una visión técnica-operativa predominante, aunque complementada por las perspectivas menos técnicas de los encuestados con formación secundaria.

El análisis sobre la función en la organización muestra la siguiente distribución: auditores (20%), personal de TI (40%), gerentes o directivos (25%) y otros roles (15%). Con estos datos se pudo conocer que el 40% de los encuestados pertenece al área de Tecnología de la Información, lo que es coherente con la naturaleza del estudio, porque los procesos de auditoría de sistemas de información involucran directamente a este grupo; esa representación permitió ayudó a obtener la percepción sobre los aspectos técnicos y operativos de las auditorías.

El 25% de los encuestados fueron gerentes o directivos y refleja una participación de la alta dirección. Este grupo señaló perspectivas estratégicas sobre cómo las auditorías contribuyen al fortalecimiento de los controles internos, la protección de activos digitales y la generación de valor para la organización. Con un 20%, los auditores tuvieron una representación equilibrada en la muestra, porque su función está directamente relacionada con la evaluación y control de los sistemas

de información, obteniéndose datos de manera más técnica y crítica sobre las fortalezas y debilidades de los procesos de auditoría.

El 15% corresponde a participantes en distintos roles no categorizados en las opciones anteriores, incluyendo personal que, aunque no está directamente vinculado con las TI, auditoría o el área de gerencia, se pudieron tener interacciones tangenciales con los temas de información, como usuarios o responsables de procesos específicos. La distribución muestra una buena representación de los grupos más relevantes para el estudio, y esto hizo que las opiniones incluyeran aspectos técnicos, estratégicos y operativos, sin embargo, la mayor proporción de personal de TI influyó en que las respuestas reflejaran una perspectiva más técnica que estratégica. La distribución fortaleció el análisis por grupo funcional, lo que es útil a futuro para identificar diferencias en la percepción según la función. Por ejemplo, los auditores se centraron en el cumplimiento y la eficiencia del proceso, mientras que los gerentes enfatizaron el valor estratégico de las auditorías, demostrando que conocen su valor real en la empresa.

Los años de experiencia en la organización mostraron que la distribución segmentó al grupo en 35% con menos de 2 años, 57% que tenían entre 2 a 5 años, y 8% con más de 5 años, lo que incidió en la dinámica de la composición laboral y la experiencia de los participantes. Más de la mitad de los encuestados (57%) tienen entre 2 y 5 años de experiencia en sus organizaciones, siendo un grupo que representa al personal que ya ha adquirido un conocimiento sólido de los procesos internos, incluyendo la implementación de controles y auditorías de sistemas de información, pero que aún se encuentra en etapas de consolidación profesional. El 35% de los participantes son relativamente nuevos en sus organizaciones, reflejando una dinámica de alta rotación laboral o expansión organizacional, donde se contrata a personal joven o con poca antigüedad. Este grupo aportó una visión más clara sobre los procesos de auditoría, pero la experiencia limitada también mostró una visión menos contextualizada de los desafíos organizacionales.

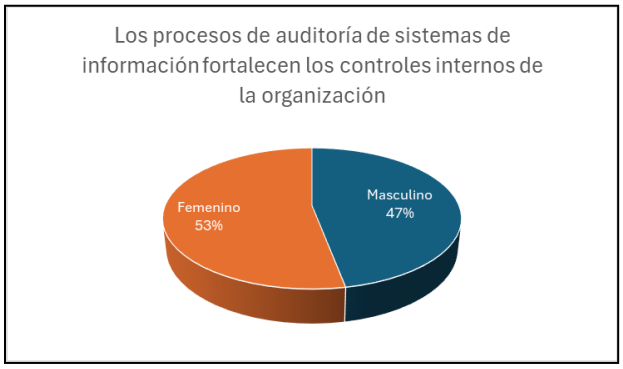
Solamente el 8% cuenta con más de 5 años en sus organizaciones, y este dato también expone la limitación en la acumulación de conocimiento organizacional a largo plazo y la continuidad en las funciones más importantes, afectando la capacidad de las empresas para ejecutar estrategias de mejora en los controles internos y la protección de activos digitales. La predominancia de una experiencia de nivel intermedio y reciente indica que las organizaciones dependen en gran medida de personal que está aún en proceso de consolidación de competencias técnicas y estratégicas, influyendo en la ejecución de las auditorías, ya que faltan perspectivas más experimentadas para evaluar el impacto de los controles implementados

Preguntas sobre auditoría de sistemas

1. ¿Considera que los procesos de auditoría de sistemas de información fortalecen los controles internos de la organización?

Figura 2

Los procesos de auditoría de sistemas de información fortalecen los controles internos de la organización



El análisis de la pregunta 1 (Figura 2) muestra una división casi equitativa en las respuestas, con 47% afirmando que sí y 53% indicando que no. Si bien esta proporción considera que las auditorías fortalecen los controles internos, la mayoría percibió que estos procesos no lograban cumplir completamente con ese objetivo, y la percepción es que podría estar vinculado a la implementación, seguimiento o comunicación de los resultados de las auditorías. La percepción negativa se debió a la falta de comprensión sobre los objetivos de las auditorías, insuficiencia en la capacitación del personal que las realiza y la ausencia de acciones concretas derivadas de los resultados encontrados, así como de una desconexión entre las recomendaciones de las auditorías y su implementación práctica. La percepción de que las auditorías no fortalecen los controles internos limita su efectividad, ya que los colaboradores no las toman en serio, o consideran que es un simple requisito administrativo en lugar de una herramienta estratégica. Los resultados exponen la necesidad de fortalecer los procesos auditores mediante la adopción de enfoques más transparentes y participativos.

2. ¿Cree que las auditorías contribuyen a la identificación oportuna de riesgos en los sistemas de información?

El 69% considera que estas auditorías sí cumplen con la identificación oportuna de riesgos en los sistemas de información y el 31% opinó que no, lo que se interpreta como un reconocimiento del valor preventivo de las auditorías, pero también expone áreas de mejora. La mayoría reconoce que las auditorías son útiles para detectar riesgos en los sistemas de información rápidamente, demostrando que sí están cumpliendo su función como herramienta para la gestión de riesgos que protege los activos digitales y mantiene la operación de las empresas.

El 31% que no percibe este beneficio está influenciado por factores relacionados con una ejecución deficiente de las auditorías, falta de seguimiento en las recomendaciones y desconocimiento de los resultados obtenidos, reflejando una brecha en la comunicación o implementación de las medidas sugeridas por los auditores. Para atender a las preocupaciones de la minoría, se deben implementar metodologías de auditorías que sean completas y estén adaptadas a las necesidades específicas de cada organización, capacitando a los equipos en la interpretación y aplicación de los resultados, para aumentar su efectividad. Sin embargo, esa percepción positiva mayoritaria demuestra la importancia estratégica de las auditorías en la gestión organizacional, muy particularmente en un medio donde los riesgos cibernéticos evolucionan rápidamente.

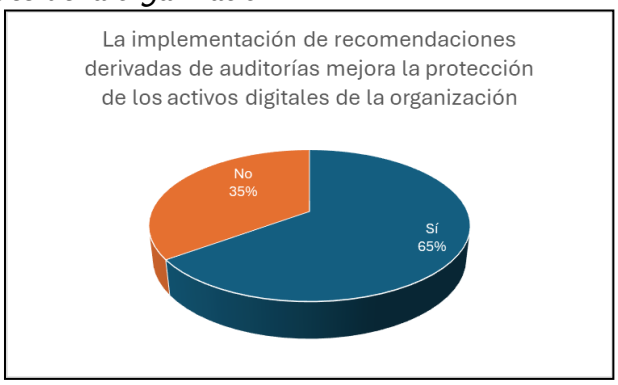
3. ¿Ha observado que la implementación de recomendaciones derivadas de auditorías mejora la protección de los activos digitales de la organización?

En la pregunta 3, un 65% está de acuerdo con esta pregunta y un 35% no lo está, destacando la percepción mayoritaria del impacto positivo de las auditorías, pero también señalando áreas que necesitan atención adicional. El 65% que considera que la implementación de las recomendaciones fortalece la protección de los activos digitales, establece la efectividad de las auditorías como un medio estratégico para las organizaciones que adopten estas sugerencias, porque estarán mejorando sus controles y minimizando los riesgos asociados a la seguridad de la información.

La proporción de los encuestados que no observa esta mejora la asocia con la falta de implementación efectiva de las recomendaciones, dificultades en el seguimiento de las acciones correctivas sugeridas, incompatibilidad entre las recomendaciones y las necesidades reales de la organización, así como las limitaciones en cuanto a recursos técnicos, humanos y financieros para aplicar los cambios. Este es un resultado que destaca que las auditorías deben proporcionar recomendaciones claras, garantizando su implementación correcta si se cuenta con planes de acción específicos, se establecen prioridades y se monitorea el cumplimiento de las medidas propuestas (Figura 3).

Figura 3

La implementación de recomendaciones derivadas de auditorías mejora la protección de los activos digitales de la organización



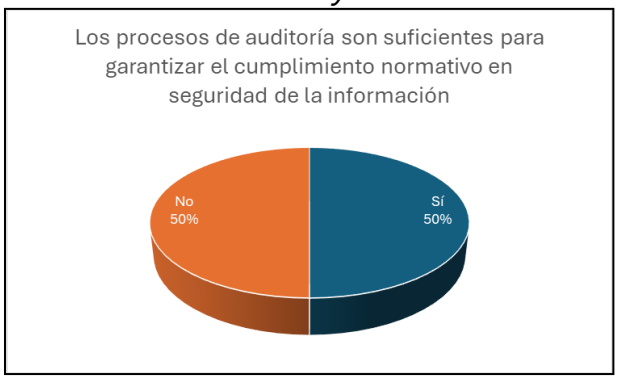
Para cerrar la brecha en esta percepción, se debe mejorar la cultura organizacional para que se valore la protección de los activos digitales como una parte estratégica, integrando las auditorías en la planificación continua de la gestión del riesgo y asegurándose de la participación de todos los niveles jerárquicos que hacen vida en cada empresa.

4. ¿Piensa que los procesos de auditoría han ayudado a reducir incidentes cibernéticos en la organización?

Esta pregunta refleja una división exacta entre las percepciones de los encuestados, con un 50% respondiendo 'sí' y otro 50% respondiendo 'no', mostrando un panorama mixto con respecto al empleo de las auditorías en la mitigación de incidentes cibernéticos. En este sentido, la mitad de los participantes que considera que las auditorías han sido útiles, lo atribuyen a la implementación correcta de los controles derivados de las auditorías, la detección y corrección de vulnerabilidades críticas en los sistemas y una mejora en la concientización sobre los riesgos y ciberseguridad en la organización (Figura 4).

Figura 4

Los procesos de auditoría han ayudado a reducir incidentes cibernéticos en la organización



El otro 50% no lo percibe así, porque observa que los procesos de auditoría no aplican las mejoras necesarias en las áreas críticas de vulnerabilidad, que falta ejecución y/o seguimiento de las recomendaciones por parte de la organización, o que persisten los incidentes a pesar de las auditorías, lo que puede deberse a un desfase entre los hallazgos de una auditoría y las amenazas que se presentan. Con los resultados se desprende la necesidad de evaluar y rediseñar las auditorías para que sean más específicas y efectivas en la identificación y reducción de riesgos cibernéticos, haciendo que incluyan una fase de seguimiento para verificar que las medidas implementadas

cumplen con su objetivo, e incorporar métricas claras para medir el impacto de una auditoría en la reducción de incidentes

5. ¿Cree que los procesos de auditoría son suficientes para garantizar el cumplimiento normativo en seguridad de la información?

La mayoría (73%) percibe que los procesos de auditoría, por sí mismos, no son suficientes para garantizar el cumplimiento normativo, debido a la naturaleza limitada que tienen, donde solamente se hacen evaluaciones puntuales y no procesos continuos. También se comentó acerca de la falta de integración entre los hallazgos y la gestión estratégica de la seguridad de la información; además, opinan que los cambios normativos constantes no son actualizados por las auditorías con la debida frecuencia. Solamente el 27% confía en que sí son una buena herramienta para asegurar el cumplimiento normativo, porque han tenido experiencias positivas y han notado que se generan cambios, así como la confianza que tienen en estas revisiones como estrategia principal para cumplir con las regulaciones.

La insuficiencia en las auditorías se percibe por la necesidad de complementar los procesos con políticas, controles internos y programas de formación continua que aborden el cumplimiento normativo de manera integral, lo que se puede hacer adoptando sistemas de gestión de seguridad de la información como los que están basados en la ISO/IEC 27001, que promueven una cultura de cumplimiento constante, estableciendo ciclos de auditoría más frecuentes y personalizados según las normativas aplicables a la organización.

6. ¿Considera que las auditorías promueven la eficiencia en la gestión de los sistemas de información?

Al preguntar si se considera que las auditorías promueven la eficiencia en la gestión de los sistemas de información, el alto porcentaje de respuestas negativas (70%) explica la percepción generalizada de que no están logrando impactar positivamente en la eficiencia de la gestión de los sistemas de información, porque los hallazgos y las recomendaciones no se aplican como debe ser ni se integran en los procesos operativos; muchas veces se enfocan en identificar problemas en lugar de mejorar los procesos o fomentar una cultura de mejora continua; así mismo, los encuestados asocian las auditorías con procesos lentos y costosos que no necesariamente le dan valor tangible a la eficiencia.

El porcentaje que sí cree que las auditorías promueven la eficiencia (30%) reflejan experiencias en organizaciones donde han sido bien aprovechadas para ajustar procesos y eliminar redundancias, enfocándose en ciertas instituciones para convertir las recomendaciones en planes de mejora concretos. Estos resultados permiten recomendar la necesidad de mejorar la percepción de las auditorías y demostrar la utilidad en la gestión de los sistemas de información, integrándolas como parte de un ciclo continuo de mejora de procesos, en lugar de verlas como un evento aislado. El diseño de las auditorías no debe verse solo como el cumplimiento de requisitos normativos, sino como la identificación de oportunidades para mejorar procesos y reducir costos, pero son los equipos responsables los que deben entender el valor estratégico que tienen.

7. ¿Piensa que las auditorías han generado confianza en el manejo de los datos por parte de los usuarios internos y externos de la organización?

Un 72% de los encuestados piensa que las auditorías han contribuido a la confianza en el manejo de los datos, mientras que el 28% opina lo contrario; la mayoría reconoce que las auditorías permiten identificar y corregir vulnerabilidades, reforzando los sistemas de información; opinan que estos procesos van de la mano con los estándares y regulaciones, aumentando la credibilidad entre usuarios internos y externos. Adicionalmente, creen que la implementación de recomendaciones de auditoría mejora los controles internos, contrario al 28% que cree que existen áreas de mejora para que las auditorías cumplan con las expectativas de todos los usuarios.

Este grupo que opinó de forma negativa siente que su escepticismo se debe a que, aunque identifican problemas, no se traducen en cambios en el manejo de los datos; señalan que si los resultados de las auditorías no se comunican, el usuario desconoce si hay avances y cree que los riesgos continúan. Para mejorar esa percepción, las empresas deben compartir las mejoras realizadas a partir de la aplicación de las auditorías para aumentar la confianza de los usuarios escépticos, complementarlas con procesos regulares de seguimiento, y permitirle a los usuarios internos y externos que conozcan lo que hace cada empresa al respecto para generar confianza y compromiso.

8. ¿Cree que los procesos de auditoría contribuyen a la toma de decisiones estratégicas relacionadas con la tecnología en la organización?

Solo el 31% reconoce la contribución estratégica, porque considera que con una auditoría se puede destacar las áreas donde la tecnología debe fortalecerse, ayudando a priorizar las inversiones. En este grupo se incluyen quienes consideran que las recomendaciones que surgen de este proceso coinciden con las metas estratégicas que influyen en la planificación tecnológica; así mismo, algunos gerentes perciben que las auditorías ayudan a evitar decisiones riesgosas al identificar las vulnerabilidades tecnológicas.

La mayoría (69%) siente que en muchas organizaciones las auditorías se centran en aspectos operativos y de cumplimiento normativo, sin vincularse a decisiones estratégicas; una de las razones para responder negativamente está en que los resultados de las auditorías no son considerados en los procesos de planificación estratégica y su impacto queda imitado; otros opinaron que son herramientas correctivas y no para guiar las decisiones a largo plazo. Incorporar recomendaciones estratégicas (además de las operativas) que respalden las decisiones relacionadas con la adopción o mejora de tecnologías, incluir a gerentes y directivos en el proceso para garantizar que los hallazgos se consideren en la planificación tecnológica, y seguir educando sobre el valor estratégico que tiene este proceso puede cambiar las percepciones negativas.

9. ¿Considera que los auditores internos o externos tienen el conocimiento técnico suficiente para evaluar los sistemas de información?

El análisis de la pregunta 9 expuso que el 55% cree que sí cuentan con el conocimiento técnico necesario, mientras que un 45% opina lo contrario. Los auditores que tiene certificaciones reconocidas son los que inspiran confianza por sus competencias técnicas, y la exposición práctica que tienen en áreas de tecnología refuerza la confianza de los encuestados. Este grupo que opina de manera positiva, percibe a los auditores como conocedores que tienen la capacidad de realizar hallazgos relevantes para mejorar los sistemas de información.

El 45% que plantea dudas sobre las competencias técnicas del auditor, señalan que no saben lo actualizados que pueden estar sobre las últimas tendencias tecnológicas, o si dominan herramientas específicas de sistemas de información. La calidad en la ejecución de las auditorías también han generado percepciones de falta de conocimiento técnico, así como en otras organizaciones donde piensan que sus auditores necesitan tener niveles de especialización que no cumplen. Para contrarrestar este porcentaje, la organización debe promover certificaciones reconocidas para su personal especializado en auditorías, elegir firmas reconocidas por su experiencia en sistemas de información, y fomentar el trabajo conjunto entre los auditores y los equipos de TI, para que se puedan realizar análisis más completos de los sistemas.

10. ¿Está de acuerdo en que los resultados de las auditorías de sistemas de información aportan valor estratégico a la organización?

El 80% de los encuestados considera que los resultados de las auditorías de sistemas de información contribuyen al valor estratégico de la organización, mientras que un 20% no está de acuerdo con esta afirmación. El porcentaje mayoritario valora las auditorías como una herramienta que aporta beneficios a nivel estratégico, porque considera que permite prever y mitigar los riesgos que impactan en las operaciones, porque los datos y análisis derivados ofrecen información para

definir estrategias tecnológicas y de negocio, señalan ineficiencias en la gestión de sistemas para que se asignen mejor los recursos, y garantizan el cumplimiento de las normas y estándares de seguridad, lo que refuerza la reputación de la organización, contribuyendo con la competitividad.

El porcentaje que no percibe el aporte estratégico (20%), lo atribuye a una falta de implementación, porque creen que si las recomendaciones de las auditorías no se aplican, el valor estratégico no se materializa. Otros coinciden en que, en sus organizaciones, las auditorías son vistas como una herramienta operativa y no como una gestión estratégica, limitando su valor en la aplicación; también se lo asignan a una mala presentación, o a una falta de alineación de los resultados con los objetivos estratégicos, y esto reduce la percepción de su relevancia. Para este subgrupo, hace falta reforzar la integración estratégica (que la auditoría no se limite a identificar problemas, sino que se usen como base para diseñar planes estratégicos), la capacitación en valor estratégico (entrenar a los equipos para interpretar los resultados de las auditorías en el contexto de los objetivos organizacionales), y el seguimiento y monitoreo (implementar sistemas para medir el impacto y sus recomendaciones en la estrategia de la organización) (Figura 5).

Figura 5

Los resultados de las auditorías de sistemas de información aportan valor estratégico a la organización

Conclusiones

El estudio realizado en organizaciones de San Miguelito evidenció importantes hallazgos sobre la percepción y el impacto de las auditorías de sistemas de información en el fortalecimiento de la seguridad y la eficiencia organizacional. Uno de los principales resultados es que la frecuencia de estas auditorías es limitada, demostrando que existe una falta de políticas estructuradas que evidencien la evaluación continua de los sistemas informáticos, porque esta situación puede comprometer la capacidad de las organizaciones para identificar y mitigar los riesgos de manera oportuna.

Las auditorías de sistemas de información son percibidas como herramientas que fortalecen los controles internos y protegen los archivos digitales, sin embargo, entre los encuestados existe un porcentaje considerable que no identifica de manera clara estos beneficios, lo que sugiere que existe la necesidad de mejorar la comunicación de los resultados de las auditorías y su vinculación con las prácticas de control organizacional. Uno de los problemas más destacados es la falta de procedimientos claros para gestionar los hallazgos, que es una ausencia que limita la implementación de las recomendaciones y reduce su impacto potencial en la mejora de la eficiencia operativa. Además de ello, se identificó que están siendo subutilizadas en su capacidad para generar soluciones prácticas que aumenten la productividad y mejoren los procesos organizacionales.

Otro aspecto que se destacó en las encuestas fue la insuficiencia en la inversión de tecnologías que respalden las auditorías. Esta falta de recursos tecnológicos impide mejorar los beneficios de estos procesos y dificulta la identificación de brechas de seguridad. A pesar de ello, los encuestados reconocen que son útiles para detectar las vulnerabilidades en los sistemas, y esto refuerza su relevancia como mecanismo preventivo y correctivo. La capacitación y sensibilización del personal

es otro punto débil en las organizaciones estudiadas, porque la formación limitada sobre auditorías de sistemas de información reduce la efectividad de los equipos encargados de implementar y gestionar los procesos, una situación que se puede llegar a traducir en menor calidad de los controles internos.

A pesar de que muchos participantes reconocen el valor estratégico por su aporte a las organizaciones, todavía existe una desconexión entre los hallazgos técnicos y su aplicación en la toma de decisiones estratégicas. Esta situación indica que se debe trabajar más en alinear las auditorías con los objetivos organizacionales para aumentar sus efectos positivos. Los resultados del estudio demuestran la importancia de fortalecer las capacidades organizacionales en torno a las auditorías de sistemas de información, invirtiendo en tecnología, capacitación y estrategias que aseguren su integración en la seguridad y eficiencia organizacional.

Ante la situación, se recomiendan cuatro iniciativas: implementar programas de capacitación continua para fortalecer el conocimiento técnico y estratégico sobre auditorías de sistemas de información; diseñar y estandarizar los procedimientos de manera tal que se puedan gestionar y actuar sobre los hallazgos de las auditorías; incrementar la inversión en tecnologías avanzadas que respalden los procesos de auditoría y reduzcan las brechas de seguridad que se presentan más frecuentemente en las empresas, y; sensibilizar a los gerentes y directivos sobre la importancia estratégica de las auditorías para integrar los resultados en los planes organizacionales.

Referencias

Al Lawati, H., Sanad, Z. & Al Farsi, M. (2024). Unveiling the Influence of Big Data Disclosure on Audit Quality: Evidence from Omani Financial Firms. *Administrative Sciences, 14*, 216. https://doi.org/10.3390/admsci14090216

Ali, M.A.S., Elshaer, I.A., Montash, A.A., Metwally, A.B.M. (2024) The Role of Technological Readiness in Enhancing the Quality of Audit Work: Evidence from an Emerging Market. *Journal of Risk and Financial Management*, *17*, 489. https://doi.org/10.3390/jrfm17110489

Barrett, M.P. (2018). *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.* National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.04162018

COBIT. (2019). *Control Objectives for Information Technologies*. https://www.isaca.org/resources/cobit

Deloitte. (2023). *Deloitte study: nine out of ten organizations reported at least one cyber incident or breach last year*. https://n9.cl/dy27m

Gartner. (2024). *2024 top trends in cybersecurity focus on resilience, performance*. https://www.gartner.com/en/cybersecurity/topics/cybersecurity-trends

ISO/IEC. (2022). *Information security, cybersecurity and privacy protection - Information security management systems - Requirements*. ISO/IEC.

KPMG. (2024). *Trailblazing digital frontiers. Global IT internal audit Outlook*. https://n9.cl/3fdde

Ley 81 de 2019. Sobre protección de datos personales. Gaceta Oficial Digital No. 28743-A, de 26 de marzo.

Lozano, M. (2024). Amenazas cibernéticas afectan la seguridad del sector financiero en el siglo 21. En *ITC Connect, Noticias tecnológicas en Latinoamérica*. https://itconnect.lat/portal/amenazas-ciberneticas-00001/

Martin, C. (2022). An Integrated Approach to Security Audits. https://n9.cl/iyv0y

Peña Calvo de la, N. (2015). *UF1643-Gestión y control de los sistemas de Información*. Editorial Elearning, SL.

Razo, C. M. (2002). *Auditoría en sistemas computacionales*. Pearson Educación.

Sánchez Valriberas, G. (2008). Control interno y auditoría de sistemas de información. En Piattini Velthuis, M. G. (2008). *Auditoría de tecnologías y sistemas de información*. (3-30). Ra-Ma Editorial.

Sayana, A. (2022). The Evolution of Information Systems Audit. *ISACA Journal*, 1, 1-5. https://n9.cl/19hb5

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

van den Heuvel, E. (2025). Evolution of IT auditing in a nutshell – journey towards a dynamic landscape. *Maandblad voor Accountancy en Bedrijfseconomie*, 99(2), 73–83. https://doi.org/10.5117/mab.99.140994