Experior
Revista de investigación ADEN

Experior: Revista de Investigación de ADEN University
ISSN L 2953-3090
Vol. 4 (1) enero/junio 2025

# Auditoría de sistemas de información para la seguridad y eficiencia organizacional

*Strategies for the Promotion of Sustainable Tourism in Panama City*

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

**Recibido:** 15/10/2024.
**Aceptado:** 10/12/2024.
**Publicado:** 02/01/2025.

**Cómo citar:** Bruce, C. (2025). Auditoría de sistemas de información para la seguridad y eficiencia organizacional. *Experior, 4*(1), 3-17.https://doi.org/10.56880/experior41.1

## Resumen

Se examina la dependencia de las Tecnologías de Información (TI) y cómo ha impulsado la necesidad de realizar auditorías de sistemas de información, que es un mecanismo para evaluar y garantizar la seguridad, eficiencia y el cumplimiento normativo. El estudio se centra en responder a la pregunta de investigación: ¿cómo contribuye la auditoría de sistemas de información al fortalecimiento de la gobernanza de la información y mitigación de riesgos en las organizaciones? Con este fin, el objetivo se centró en revisar los procesos de la auditoría en la mejora de los controles internos, la protección de los activos digitales y la generación de valor estratégico para las organizaciones. La metodología se basó en un estudio no experimental, descriptivo, documental y transversal, con un enfoque inductivo. Se analizaron 24 fuentes académicas y profesionales entre 2000 y 2024, centrándose en las áreas de auditoría de sistemas, ciberseguridad y gobernanza corporativa, presentando la información mediante tablas y figuras para facilitar la interpretación de los resultados. Se estableció que la auditoría de sistemas fortalece los controles internos al identificar vulnerabilidades y promover medidas correctivas, y que la protección de activos digitales se logra mediante estrategias como la segmentación de redes, los sistemas de detección de intrusos y la autenticación multifactor. Se destaca en las conclusiones que la incorporación de tecnologías avanzadas y la capacitación continua de los auditores son necesarias para aumentar su efectividad, así como mejorar la transparencia, la rendición de cuentas y la gestión de riesgos.

**Palabras clave**: cibercrimen, delito informático, protección de datos, protocolos de redes de computadoras, seguridad de datos computarizados.

## Abstract

The dependence on Information Technology (IT) is examined and how it has driven the need to perform information systems audits, which is a mechanism to assess and ensure security, efficiency and regulatory compliance. The study focuses on answering the research question: how does information systems auditing contribute to strengthening information governance and mitigating risks in organizations? To this end, the objective was to review audit processes in improving internal controls, protecting digital assets and

generating strategic value for organizations. The methodology was based on a non-experimental, descriptive, documentary and cross-sectional study, with an inductive approach. 24 academic and professional sources were analyzed between 2000 and 2024, focusing on the areas of systems auditing, cybersecurity and corporate governance, presenting the information through tables and figures to facilitate the interpretation of the results. It was established that systems auditing strengthens internal controls by identifying vulnerabilities and promoting corrective measures, and that the protection of digital assets is achieved through strategies such as network segmentation, intrusion detection systems and multi-factor authentication. The conclusions highlight that the incorporation of advanced technologies and continuous training of auditors are necessary to increase their effectiveness, as well as improve transparency, accountability and risk management.
**Keywords:** cybercrime, computer crime, data protection, computer network protocols, computer data security.

## Introducción

Actualmente se manifiesta una dependencia creciente de las tecnologías de información (TI) que ha puesto en una posición más activa el área de la auditoría de sistemas de información, de tal manera que la ha consolidado como un instrumento organizacional para evaluar y garantizar la seguridad, eficiencia y cumplimiento normativo de estos procesos empresariales. El fenómeno de la transformación digital, acelerado por los cambios y la forma en que la tecnología se ha ido superando a sí misma, ha incrementado la dependencia de los sistemas informáticos para la toma de decisiones estratégicas y operativas (Galliers & Leidner, 2022). No obstante, este avance también trae consigo sus riesgos inherentes por la proliferación de ciberataques que vulneran la privacidad de terceros y la integridad de los datos, llevando a un incumplimiento normativo y a la exposición a fraudes internos (Guzmán *et al.*, 2023). Esta es una situación que necesita de la evaluación que se pueda realizar acerca de la eficacia de los controles internos y externos que protegen los activos digitales de las organizaciones.

Según Romney *et al.* (2012), la auditoría de sistemas de información es un proceso de recolección y evaluación de evidencias que las organizaciones generan, para determinar si un sistema de información es capaz de salvaguardar los activos, mantener la integridad de los datos, alcanzar las metas organizacionales y utilizar los recursos asignados de manera eficiente. Intelligent Networking (2023) la define también como un proceso que ayuda “a garantizar que los sistemas de información de una organización sean seguros eficientes y efectivos” (párr. 8), pero que también sea capaz de contener problemas que se presenten a futuro y que mejore la calidad que necesitan tener los sistemas de información en las organizaciones.

Hace poco más de una década, las auditorías rara vez incluían evaluaciones sobre los riesgos y controles asociados con la seguridad de los datos. No obstante, en el contexto actual de las empresas digitales, los datos se han convertido en activos organizacionales que enfrentan amenazas de seguridad. Las funciones de TI y seguridad -por sí solas- no son suficientes para cubrir estos desafíos y los equipos de auditoría tienen que colaborar con las áreas de TI, la junta directiva, la gerencia y los equipos operativos. Juntos pueden desarrollar una estrategia de ciberseguridad integral y lo suficientemente robusta para

priorizar la identificación de riesgos, la prevención de amenazas y la construcción de resiliencia frente a los desafíos que surgen en materia de seguridad informática (Martin, 2022).

De manera frecuente se estudian los incidentes relacionados con la seguridad de la información, y así lo demuestra el informe de Kaspersky (2024a) cuando registró durante el segundo trimestre de 2024 que el 23.5% de las computadoras ICS (sistemas de control industrial) a nivel mundial estuvieron expuestas a ciberamenazas que, aunque el dato representa una leve disminución frente al 24.4% registrado en el primer trimestre, expone la problemática planteada. África sigue siendo la región más vulnerada con un 30% de las computadoras ICS atacadas, seguida de Oriente Medio, donde el porcentaje alcanzó el 25%.

Estos datos, más el conocimiento de que las organizaciones se enfrentan a normativas como el cumplimiento del Reglamento General de Protección de Datos (GDPR) en Europa (Heim, 2023), o la Ley de Portabilidad y Responsabilidad de Seguros Médicos (*Health Insurance Portability and Accountability Act*, HIPAA) en Estados Unidos, impulsa a que se estén necesitando a nivel mundial procesos constantes de auditoría y monitoreo (Texas Health and Human Services, 2022), porque su ley de privacidad "establece estándares nacionales que protegen los expedientes médicos y demás datos médicos de una persona" (párr. 4).

Como mecanismo preventivo y correctivo, sirve para la identificación temprana de brechas de seguridad (Marques *et al.*, 2019) y para ayudar a mantener la transparencia organizacional, sin embargo, todavía se ha revisado en la literatura una limitación para tratar su implementación específica en las empresas de diversos tipos y escalas organizacionales, reforzando la necesidad de tener una aproximación más adaptativa que contextualice este hecho.

Esta investigación pretende responder a la pregunta ¿cómo contribuye la auditoría de sistemas de información al fortalecimiento de la gobernanza de la información y mitigación de riesgos en las organizaciones? El objetivo que se quiere alcanzar es revisar los procesos de la auditoría en la mejora de los controles internos, la protección de los activos digitales y la generación de valor estratégico para las organizaciones.

## Revisión de la literatura

La auditoría de sistemas de información (ASI) es un campo multidisciplinario que integra las perspectivas de la seguridad informática, más la gestión de riesgos y la gobernanza organizacional, razón por la que la revisión de la literatura presenta las reflexiones teóricas y prácticas que fundamentan su relevancia en la actualidad.

La ASI se entiende como un proceso integral para garantizar la eficiencia, seguridad y cumplimiento de los sistemas informáticos. Su propósito principal es evaluar si los sistemas de información de una organización cumplen con estándares normativos y operan de manera segura y eficiente (Moscove *et al.*, 2000). Este planteamiento está reforzado por Solms & Solms (2008) quienes afirman que la ASI es fundamental en la identificación de las vulnerabilidades y protección de los activos digitales. Hoy en día ese aspecto se tiene que centrar especialmente en entornos que operan con *Big Data* y computación en la nube.

ISSN L 2953-3090
Vol. 4(1) enero-junio 2025

Los componentes fundamentales de la auditoría de sistemas de información se encuentran en la identificación de activos críticos, la evaluación de riesgos, políticas y procedimientos de ciberseguridad, controles técnicos, monitoreo y detección de incidentes, pruebas de seguridad y continuidad, y el cumplimiento normativo (Auditool, 2024).

El impacto de los ciberataques en las organizaciones ha aumentado exponencialmente, tal como lo demuestra el informe de Kaspersky (2023), asegurando que sus soluciones contra ciberamenazas a nivel mundial en el último período pudieron repeler un total de 437.414.681 ataques maliciosos provenientes de recursos de internet en diversos países, detectando 106.357.530 URL maliciosas únicas y bloqueando 112.922.612 objetos maliciosos únicos. Protegieron a 193.622 usuarios únicos contra ataques de cifrado y a 1.140.573 usuarios únicos frente a ataques de criptomineros, además de bloquear los intentos de lanzar programas maliciosos diseñados para robar dinero mediante el acceso a cuentas bancarias en línea, protegiendo a 325.225 usuarios únicos.

El término 'usuarios únicos' es la cantidad de usuarios individuales que fueron afectados, sin contar con las múltiples instancias de un mismo usuario afectado, aclaratoria que es necesaria para conocer que esta delimitación permite ofrecer una cifra que refleja el número de personas o dispositivos que experimentaron un ataque o amenaza, independientemente de cuántos ataques diferentes o intentos de ataques hayan sufrido estos usuarios.

Por otra parte, los objetos maliciosos únicos hace referencia a la cantidad de diferentes archivos o recursos maliciosos detectados por el sistema, sin contar repeticiones, que pueden ser archivos, *script* o códigos que se han identificado como maliciosos, y la cifra indica cuántos tipos distintos de *malware* fueron bloqueados, sin duplicar aquellos que fueron detectados múltiples veces en distintos lugares o dispositivos.

Estos términos son usados para evitar que los datos sean inflados por repeticiones, para dar una visión más precisa de la cantidad real de amenazas y su alcance, pues solo así cobra interés el dato proporcionado por Kaspersky (2024b). El impacto que han cobrado los ciberataques a las organizaciones ha ido en aumento exponencial. Este panorama es el que refuerza la necesidad de realizar auditorías regulares para prevenir y mitigar daños. La Figura 1 presenta los datos de esta empresa de ciberseguridad con la data en vivo durante un día cualquiera del mes de noviembre de 2024, para mostrar las detecciones por segundo, donde los totales de detección de datos se restablecen todos los días a las 0:00:00 GMT.

La gobernanza organizacional proporciona métricas para la toma de decisiones y se beneficia con la ASÍ. Galliers & Leidner (2014) argumentan que la integración de las prácticas de auditoría robustas son las que mejoran la transparencia y fortalecen la confianza entre las partes interesadas, argumento que complementan Josa Arbonés *et al.* (2023) quienes señalan que la auditoría contribuye al restablecimiento de un marco de control interno que mitiga los riesgos financieros y reputacionales.

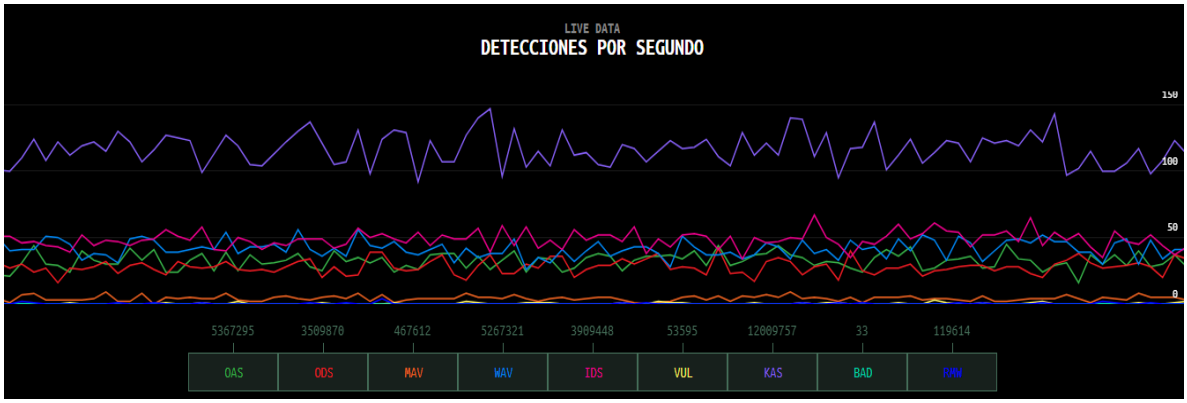


**Figura 1.**
*Detecciones mundiales de ciberataques por segundo*
*Nota*. Kaspersky (2024b).
*Nota 2.* OAS (On-Access Scan); ODS (On Demand Scanner); MAV (Mail Anti-Virus); WAV (Web Anti-Virus); IDS (Intrusion Detection Scan); VUS (Vulnerability Scan); KAS (Laspersky Anti-Spam); BAD (Botnet Activity Detection); RMW (Ransomware).

La Administración de la Seguridad de la Información (ASI) se sustenta en varios modelos teóricos que orientan su implementación en los entornos organizacionales, proporcionando una estructura conceptual para identificar, gestionar y mitigar los riesgos relacionados con esta práctica. Uno de los principales marcos aplicados es el *Committee of Sponsoring Organizations* 2017 (COSO-ERM), un modelo diseñado para abordar la gestión de riesgos empresariales desde el enfoque integral.

El COSO-ERM proporciona metodologías para identificar los riesgos tecnológicos, evaluarlos y definir estrategias para mitigarlos a tiempo, con un enfoque general para que las organizaciones puedan integrar la gestión de riesgos tecnológicos en sus procesos de gobernanza y toma de decisiones (Ramírez Fernández del Castillo, 2017). Más allá de la identificación de riesgos, se centra en cómo pueden impactar los objetivos estratégicos y operativos de una organización, facilitando la alineación entre la seguridad de la información y los objetivos empresariales generales, promoviendo una cultura organizacional para la gestión de riesgos.

Otro modelo teórico aplicado a la ASI es COBIT 2019, desarrollado por ISACA, centrado en la gobernanza y gestión de la tecnología de la información, ajustándose a los objetivos estratégicos y operativos de las organizaciones y su cumplimiento normativo. Proporciona un conjunto de principios, procesos y prácticas que ayudan a las organizaciones a aumentar el valor de sus recursos tecnológicos, para que la infraestructura de TI sea segura, eficiente y funcione de acuerdo con las metas empresariales. Hace que las actividades relacionadas con la TI cumplan con las regulaciones normativas aplicables, reduciendo los riesgos de incumplimiento y mejorando la confianza de los *stakeholders* (ISACA, 2018).

La norma ISO 27001, publicada por la Organización Internacional de Normalización (ISO) en 2018, es uno de los modelos teóricos más reconocidos en la ASI, por ser un estándar internacional que establece los requisitos para implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI) en cualquier organización. Se centra en la protección de la

confidencialidad, integridad y disponibilidad de la información, a través de un enfoque sistemático que incluye la identificación de riesgos, la implementación de controles y la evaluación continua de su efectividad. Con este marco se protege la información sensible, y se respalda su capacidad para cumplir con regulaciones y normativas relacionadas con la seguridad de los datos, promoviendo la cultura de mejora continua a través del ciclo PDCA para planificar, hacer, verificar y actuar (ISO, 2022).

Esta revisión expone la creciente intersección entre la auditoría de sistemas y el análisis predictivo basado en la tecnología. Chowdhury (2021) destaca el uso de herramientas avanzadas para identificar patrones anómalos en grandes volúmenes de datos para mejorar la eficacia de las auditorías. Ikhtiari (2023) se suma a la idea de que la incorporación de tecnologías emergentes (como el *Blockchain*), proporciona mayor transparencia y seguridad en los procesos de auditorías, porque "la tecnología blockchain ha introducido nuevas posibilidades para mejorar la transparencia y la confianza en las auditorías" (p. 137).

## Metodología

Este estudio fue diseñado como una investigación no experimental, descriptiva, documental y transversal, empleando un enfoque inductivo para explorar la relación entre la auditoría de sistemas de información y su impacto en los controles internos, la protección de activos digitales y la generación de valor estratégico para las organizaciones. La metodología adoptada responde a la naturaleza del fenómeno estudiado y al objetivo planteado, considerando que no se manipularon variables, porque el propósito fue analizar los datos disponibles sobre la auditoría de sistemas y su impacto en las organizaciones.

Se buscó caracterizar las relaciones entre los elementos estudiados como la implementación de medidas de auditoría, los controles internos y las estrategias de protección de activos digitales, lo que la convierte en una investigación con diseño descriptivo. Con respecto al enfoque documental, se realizó una revisión de la literatura técnica relevante y se seleccionaron 24 fuentes académicas profesionales publicadas entre 2000 y 2024, dándole una perspectiva longitudinal que incorpora marcos teóricos y avances recientes. Así, el uso de la metodología inductiva permitió construir el conocimiento desde los casos particulares hacia las generalizaciones útiles para interpretar los resultados.

La distribución temática de las fuentes revisadas en auditoría de sistemas fue del 40% de las referencias, centradas en las prácticas de auditoría, la implementación de tecnologías y el análisis de calidad, observado en los estudios de Auditool (2024) e Ikhtiari (2023). El tema de ciberseguridad representa el 35%, con investigaciones sobre detección de intrusiones y normativas internacionales como ISO7IEC 27001:2022 y el análisis de ataques reportados por Kaspersky (2023, 2024a y 2024b). La gobernanza corporativa ocupó el 25% restante para desarrollar la integración de sistemas de gestión y su vínculo con la auditoría y la seguridad, ejemplificado en trabajos como los de Galliers & Leidner (2014) y Heim (2023).

Las áreas de estudio fueron elegidas por su relevancia para entender la auditoría de sistemas, los riesgos tecnológicos y sus ventajas estratégicas, ofrece herramientas específicas para evaluar y fortalecer los controles internos;

se observa cómo los avances en ciberseguridad ofrecen un marco actualizado para la protección de activos digitales y cómo la gobernanza corporativa y el gobierno de TI contextualizan la relación entre la auditoría y el cumplimiento estratégico. La selección de estas áreas permitió contrastar la literatura científica con los estudios de Slapničar *et al.* (2022), Al Lawati *et al.* (2024), y Ramírez-Patajalo (2023), generando una base lo suficientemente sólida para ofrecer la discusión de los resultados.

Para facilitar la interpretación de los resultados, se incorporaron figuras y tablas que sintetizan la información relevante para sustentar ciertos aspectos, como en el caso de la categorización de riesgos según probabilidad y factibilidad (Figura 2) y las medidas de protección de activos digitales (Tabla 1), ayudando a integrar visualmente los resultados con las implicaciones prácticas derivadas del análisis teórico.

## Resultados

Las consecuencias de un ciberataque son devastadoras para cualquier organización, al comprometer la información sensible que afecta su estabilidad financiera, los objetivos estratégicos, su reputación y la confianza depositada por clientes, socios y empleados, construida a lo largo de los años (Martin, 2022). El análisis de los resultados obtenidos en este estudio se enfoca en dar a conocer cómo la auditoría de sistemas de información ayuda a mejorar los controles internos, a proteger los activos digitales y a generar valor estratégico para las organizaciones; se presentan y discuten en función de su contraste con los fundamentos teóricos y el objetivo planteado en la investigación.

## Mejora en los controles internos

La auditoría de sistemas fortalece los controles internos, porque identifica y estudia las vulnerabilidades en procesos y sistemas, confirmando que, tras la implementación de auditorías, un alto porcentaje de empresas ha adoptado medidas correctivas de peso. Al Lawati *et al.* (2024), si bien no tratan directamente sobre la mejora de los controles internos con la ayuda de las auditorías de sistemas de información, explican el impacto del *Big Data* en la calidad de la auditoría, cuya relación con los controles internos es directa.

Señalan que la adopción de las tecnologías de *Big Data* ayuda a las empresas a mejorar la eficiencia y eficacia de sus registros financieros, transacciones y estados financieros, facilitando la labor de los auditores y haciendo que las auditorías sean más precisas. Exponen que técnicas como la minería de datos, el análisis de sentimientos, la agrupación en clústeres y la visualización, hacen que sea más sencillo evaluar los riesgos inherentes en los estados financieros y a establecer límites de materialidad.

Con la adquisición de herramientas, experiencia e infraestructura de vanguardia, se puede tener una gestión eficaz de datos, pero a un costo que se refleja en el aumento en las tarifas de auditoría, sin embargo, se justifica por la mejora en la calidad de la auditoría. Las empresas que quieren mantener una buena reputación suelen abogar por la adopción de tecnologías avanzadas para garantizar la precisión y fiabilidad de la información financiera, pero solamente el compromiso a largo plazo con la empresa y su influencia en la reducción de conflictos son los que contribuyen a tener un sistema sólido que mejore más la

calidad de la auditoría (Al Lawati *et al.,* 2024). Aquí se demuestra que el análisis de *Big Data* sí puede ayudar a identificar patrones de fraude o errores en los sistemas de información, para que las empresas fortalezcan sus controles internos y prevengan estos problemas en el futuro.

Ali *et al.* (2024) también analizan cómo la calidad de la auditoría remota (RAQ) influye en la calidad general de la auditoría (QAW) y, de forma indirecta, en los controles internos. Es decir, en la gestión de seguridad de la información y auditoría de sistemas de información, los resultados de estos autores exponen el papel de la tecnología avanzada y la preparación tecnológica en la mejora de los controles internos. La adopción de tecnologías avanzadas en auditorías remotas ayuda a evaluar de manera precisa los sistemas de información, debido a una infraestructura tecnológica robusta, para identificar y mitigar vulnerabilidades antes de que se conviertan en amenazas.

Empresas con sistemas avanzados con las ERP mejoran la gestión de sus datos, transacciones y registros financieros, aumentando la calidad de las auditorías de sistemas, ayudando a los auditores a identificar y recomendar mejoras en los controles internos. Estos autores toman en cuenta que, aunque la preparación tecnológica del profesional es necesaria, tiene que ser complementada con una capacitación especifica para evitar posibles vulnerabilidades en la detección de fallas, ya que un auditor bien capacitado puede ofrecer una auditoría remota de calidad y tiene la capacidad de identificar deficiencias a tiempo.

La auditoría de sistemas mejora los controles internos mediante la evaluación y categorización de los riesgos en función de su probabilidad de materialización, considerando criterios como la frecuencia histórica y la existencia de factores potenciadores para identificar riesgos bajos, medios o altos, ayudando a priorizar las áreas que necesitan mejoras en los controles internos. Así mismo, la frecuencia de ocurrencia de riesgos y su factibilidad permiten a los auditores establecer un marco claro para analizar la vulnerabilidad del sistema y la eficacia de los controles.

Por otro lado, el análisis de los factores potenciadores del riesgo y la existencia o ausencia de acciones mitigadoras son los que guían el diseño de estrategias específicas. Si no hay acciones mitigadoras en riesgos de alta probabilidad, la auditoría puede proponer controles internos más estrictos como el monitoreo en tiempo real mediante sistemas avanzados; la capacitación del personal en prácticas de seguridad, y la actualización de políticas y procedimientos para fortalecer la respuesta ante los riesgos. Así lo presenta la Figura 2:

| Probabilidad | Descripción | En base a frecuencia | En base a factibilidad |
|---|---|---|---|
| Baja | Es improbable que el riesgo se materialice. | No ha sucedido en los últimos dos años. | No se aprecian factores potenciadores del riesgo, o ocurren algunos factores potenciadores pero hay implementadas acciones orientadas a mitigar el riesgo. |
| Media | Es posible que el riesgo se materialice. | Ha sucedido al menos una vez al año. | Concurren algunos factores potenciadres del riesgo y no hay implementadas acciones mitigadoras o hay dudas sobre su eficacia. |
| Alta | Es altamente probable que el riesgo se materialice. | Ha sucedido al menos una vez al año. | Concurren varios de los factores potenciadores del riesgo.<br>No hay implementadas acciones mitigadoras del riesgo o hay dudas sobre su eficacia. |

**Figura 2**
*Categorización de riesgos según probabilidad, frecuencia y factibilidad*
*Nota.* Josa Arbonés *et al*. (2023, p. 125).

## Protección de activos digitales

Aquí se incluyen datos confidenciales, propiedad intelectual, infraestructuras de TI y sistemas informáticos que mejoran el funcionamiento de las organizaciones, una razón válida para considerar la protección de estos activos para mantener la continuidad operativa, salvaguardar la integridad, confidencialidad y disponibilidad de la información. Slapničar *et al.* (2022) explican la eficacia de la auditoría de ciberseguridad (CSA) como una función de la auditoría interna, tema que se relaciona con la protección de los activos digitales por cuanto su objetivo principal es obtener evidencia independiente del cumplimiento de las políticas de seguridad cibernética, los procesos de gestión de riesgos y los controles internos de una organización. La CSA evalúa la eficacia de las medidas implementadas para proteger la integridad de los activos, la confidencialidad de los datos y su disponibilidad; dentro del contexto de la seguridad y eficiencia organizacional, esto no es más que identificar cómo los activos digitales requieren tener una protección rigurosa.

Este estudio propone un índice de auditoría de ciberseguridad (*Cibersecurity Audit Index*) compuesto por tres dimensiones: planificación, ejecución e informe, donde cada dimensión tiene sus indicadores específicos que reflejan la eficacia de a CSA. Por ejemplo, la dimensión de planificación incluye la proactividad en la comprensión del entorno de ciberseguridad, la realización de riesgos y la utilización de marcos de ciberseguridad. La dimensión de ejecución se centra en la amplitud y profundidad de la recopilación de evidencia, que lleva a evaluar la exhaustividad de los procedimientos de auditoría utilizados para examinar las áreas de ciberseguridad, y la sofisticación de las herramientas técnicas empleadas para garantizar la seguridad cibernética.

En la dimensión de informes se destaca la importancia de proporcionar un informe completo y frecuente al Consejo de Administración y al comité de auditoría, de modo que comunique claramente los hallazgos, las deficiencias de control material detectadas y las recomendaciones para mejorar la gestión de

riesgos de ciberseguridad. Esta transparencia es la que se necesita para que la dirección comprenda el estado de seguridad de los activos digitales y tome medidas correctivas oportunas. Estas tres dimensiones presentadas por Slapničar *et al.* (2022) estudian los aspectos que se necesitan para garantizar la protección de los activos digitales en una auditoría de sistemas de información; al mejorar la eficacia de la CSA, las organizaciones fortalecen sus defensas contra las amenazas cibernéticas y protegen sus activos digitales.

Como estrategias para la protección se ofrecen tres medidas que han demostrado ser efectivas en este aspecto: segmentación de redes internas, sistemas de detección de intrusos (IDS) y autenticación multifactor (MFA).

Con la segmentación de redes internas se divide la infraestructura de TI en subredes aisladas para limitar el alcance de un posible ataque, previniendo la propagación de ciberataques, limitando el acceso a la información sensible y restringiendo el daño a áreas específicas de la red (Villora Divino, 2018). En cuanto a los sistemas de detección de intrusos, se utilizan para identificar intentos de acceso no autorizados en tiempo real, porque los sistemas IDS monitorean el tráfico de la red en busca de comportamientos sospechosos; cuando se detecta un incidente, se activan las alertas para que los equipos de seguridad tomen medidas de manera inmediata. Según Khraisat *et al.* (2019) “la evolución del software malicioso (*malware*) plantea un desafío crítico para el diseño de sistemas de detección de intrusiones” (p. 1) y los IDS son fundamentales para prevenir ataques de ciberseguridad como el *malware*, *ramsonware* y los accesos no autorizados, protegiendo de manera proactiva los activos digitales.

La adopción de la autenticación multifactor es una de las estrategias más efectivas para prevenir accesos no autorizados, porque la MFA añade capas adicionales de seguridad al exigir que los usuarios proporcionen varias credenciales, como contraseñas y un código enviado a un dispositivo móvil antes de acceder a sistemas críticos, siendo una medida que refuerza la seguridad mientras mitiga el riesgo de ataques de *phishing* y otros métodos de suplantación de identidad. Este uso está respaldado en la revisión de la literatura efectuada por Ramírez-Patajalo (2023) cuando señala que “un 65% de los trabajos [revisados] resaltó el crecimiento en la adopción de métodos de autenticación multifactor (MFA) y autenticación de dos factores (MFA) como medidas efectivas para reducir el riesgo de acceso no autorizado” (p. 2225). Ello demuestra que las auditorías de sistemas actúan como un catalizador para mejorar la seguridad organizacional, proporcionando una estructura para la detección temprana y la mitigación de riesgos. La Tabla 1 resume las medidas relacionadas con la protección de los activos digitales:

**Tabla 1**

*Medidas relacionadas con la protección de activos digitales*

| **Medidas relacionadas con la protección de activos digitales** | | | |
|---|---|---|---|
| **Medida** | **Descripción** | **Beneficios** | **Fuente** |
| **Segmentación de redes internas** | División de la infraestructura en subredes aisladas para limitar el | Reduce la propagación de ciberataques y protege datos sensibles | Villora Divino, 2018 |

| | | | |
|---|---|---|---|
| | alcance de posibles ataques | | |
| **Sistemas de Detección de Intrusos (IDS)** | Herramientas que monitorean el tráfico de la red para identificar accesos no autorizados o comportamientos sospechosos en tiempo real | Permite respuestas inmediatas a incidentes y protege contra amenazas del tipo malware y accesos no deseados | Khraisat *et al*., 2019 |
| **Autenticación Multifactor (MFA)** | Requiere múltiples credenciales, como contraseñas y códigos temporales para acceder a sistemas críticos | Refuerza la seguridad de los sistemas, reduciendo riesgos de phishing y accesos no autorizados | Ramírez-Patajalo, 2023 |

*Nota*. Las columnas describen qué es cada medida, cómo funciona y qué beneficios aporta, mientras que las fuentes proporcionan el respaldo académico para cada medida, lo que refuerza su validez en el contexto profesional y científico.

## 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.* 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

ISSN L 2953-3090
Vol. 4(1) enero-junio 2025

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:

**Eficiencia y ahorro de recursos**. La integración de 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.

**Mayor visibilidad de la postura de seguridad**. La integración de marcos y el uso de un repositorio de datos centralizado proporciona una visión más completa de la postura de seguridad de la organización y sus obligaciones de riesgos y asignación de recursos.

**Colaboración entre auditoría interna y TI**. Martin 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.

**Enfoque proactivo en la gestión de riesgos**. El documento propone 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.

## Conclusiones

La auditoría de sistemas de información tiene muchas ventajas que son tomadas en cuenta por las organizaciones. En primer lugar, ayuda a fortalecer

los controles internos en la medida en que identifica y evalúa las vulnerabilidades en los procesos y sistemas organizacionales. La incorporación de tecnologías avanzadas como el *Big Data* sirven para precisar la identificación de los riesgos, patrones de fraude y deficiencias en los registros financieros, sin embargo, estos avances necesitan una inversión considerable y una preparación tecnológica adecuada para aumentar su efectividad, lo que también enfatiza la importancia de la capacitación continua de los auditores.

Con las auditorías de ciberseguridad (CSA), se ha demostrado la fortaleza para salvaguardar los activos digitales de las organizaciones, donde se pueden utilizar estrategias como la segmentación de redes, los sistemas de detección de intrusos y la autenticación multifactor, porque han sido identificadas como medidas efectivas para prevenir y mitigar amenazas cibernéticas. La implementación de *Cyberecurity Audit Index* facilita la planificación, ejecución e informes de auditoría, para que las organizaciones tomen decisiones oportunas para proteger sus infraestructuras críticas.

En la generación de valor estratégico, al ser una herramienta técnica que alinea los objetivos tecnológicos con los estratégicos en la organización, garantiza la integridad de los activos digitales y fortalece la gobernanza corporativa, las auditorías contribuyentes a la transparencia, la rendición de cuentas y la gestión eficaz de riesgos. Se genera valor estratégico con ella, porque se apoya en tecnologías avanzadas en auditorías remotas que incrementan la eficiencia, liberando recursos que pueden enfocarse en áreas de mayor impacto estratégico.

El impacto en la gobernanza y competitividad también es claro, porque aporta información de calidad sobre la efectividad de las estructuras de gobernanza, ayudando a las organizaciones a mejorar la calidad de sus controles internos y su capacidad para gestionar riesgos. Estas son mejoras que refuerzan la reputación organizacional, la confianza de los *stakeholders* y la competitividad en el mercado, justificando las inversiones en herramientas avanzadas y capacitación especializada.

## 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

Auditool. (2024). Auditoría de TI. https://www.auditool.org/blog/auditoria-de-ti/siete-aspectos-basicos-a-tener-en-cuenta-en-una-auditoria-de-ciberseguridad

Chowdhury, E. K. (2021). Prospects and challenges of using artificial intelligence in the audit process. *The Essentials of Machine Learning in Finance and Accounting*, 139-156. https://doi.org/10.4324/9781003037903

Galliers, R. D., & Leidner, D. E. (2014). *Strategic information management: challenges and strategies in managing information systems*. Routledge.

Guzmán, C., Palacios, D., & Palacios, E. (2023). Incidencias de los ciberdelitos y sus regulaciones en la ciudad de Panamá. *Revista Semilla Científica*, (4), 524-539. https://doi.org/10.37594/sc.v1i4.1296

Heim, T. N. (2023). *Global governance and regulation of cybersecurity: Towards coherence or fragmentation?* (Doctoral Dissertation). University of Twente.

Ikhtiari, K. (2023). Best Practices and Innovations in Modern Financial Statement Audits. *Advances in Managerial AuditingResearch*, 1(3),2023.135 -145. https://doi.org/10.60079/amar.v1i3.277

Intelligent Networks. (2023). ¿Qué es una auditoría de sistemas de información y por qué es esencial para tu empresa? https://acortar.link/s9FzeH

ISACA. (2018). *COBIT 2019*. ISACA Buenos Aires Chapter.

ISO. (2022). *ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. ISO*. https://www.iso.org/es/contents/data/standard/08/28/82875.html

Josa Arbonés, N., García, E. R., i Díaz, L. M. C., & Vivas, M. P. (2023). Evaluación de riesgos en los Planes de Integridad versus su utilización en la planificación de las actuaciones de control financiero en las entidades locales. *Auditoría pública: revista de los Órganos Autónomos de Control Externo*, (81), 120-130. https://asocex.es/wp-content/uploads/2023/05/Articulo-9.pdf

Kaspersky. (2023). Nueva epidemia: el phishing se sextuplicó en América Latina con el reinicio de la actividad económica y el apoyo de la IA. https://latam.kaspersky.com/blog/panorama-amenazas-latam-2023/26586/

Kaspersky. (2024a). Kaspersky informa de un aumento de los ataques de ransomware y spyware en sistemas industriales. https://acortar.link/1BSNl0

Kaspersky. (2024b). *Cyberthreat Live Map*. https://cybermap.kaspersky.com/stats

Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity*, *2*(1), 1-22. https://doi.org/10.1186/s42400-019-0038-7

Marques, R. P., Santos, C., & Inacio, H. (Eds.). (2019). *Organizational Auditing and Assurance in the Digital Age*. IGI Global.

Martin, C. (2022). An Integrated Approach to Security Audits. https://www.isaca.org/resources/news-and-trends/industry-news/2022/an-integrated-approach-to-security-audits

Moscove, S. A., Simkin, M. G., & Bagranoff, N. A. (2000). *Core concepts of accounting information systems*. John Wiley & Sons, Inc.

Ramírez Fernández del Castillo, A. (2017). Actualización COSO ERM 2017. Nuevos riesgos, nuevas estrategias. En *PwC, PricewaterhouseCoopers*. https://www.pwc.com/mx/es/coso-erm-framework.html

Ramírez-Patajalo, G. A. (2023). Seguridad en desarrollo web: mejores prácticas para proteger aplicaciones y datos. *Domino de las Ciencias*, *9*(3), 2219-2229. https://doi.org/10.23857/dc.v9i3.3552

Romney, M., Steinbart, P., Mula, J., McNamara, R., & Tonkin, T. (2012). *Accounting Information Systems Australasian Edition*. Pearson Higher Education AU.

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

Solms, S. V., & Solms, R. (2008). *Information security governance*. Springer Science & Business Media.

Texas Health and Human Services. (2022). La HIPAA y las leyes sobre la privacidad. https://acortar.link/jevI3p

Villora Divino, B. (2018). *Evaluación y gestión de vulnerabilidades: Cómo sobrevivir en el mundo de los ciberataques.* [Tesis de Grado]. Universitat Politècnica de València.