Visión Antataura
Vol. 9, No.
Diciembre 2024 – Mayo 2025
pp.30-43
ISSN L 2520-9892

Ciberseguridad y auditoría: una alianza para la protección de los activos digitales

Cybersecurity and audit: an alliance for the protection of digital assets

Eva Patricia Hau Huang[1], Abel Arturo Pérez Moreno[2], Caren Yaneth Bernal Canto[3], Dora Rosaura Batista Peralta[4]

[1]Universidad de Panamá, Centro Regional Universitario de Azuero, Facultad de Administración de Empresas y Contabilidad, Panamá; eva.hau-h@up.ac.pa; https://orcid.org/0009-0004-4529-3449
[2]Universidad de Panamá, Centro Regional Universitario de Azuero, Facultad de Administración de Empresas y Contabilidad, Panamá; abel.perez-m@up.ac.pa; https://orcid.org/0009-0009-5185-8545
[3]Universidad de Panamá, Centro Regional Universitario de Azuero, Facultad de Administración de Empresas y Contabilidad, Panamá; caren.bernal@up.ac.pa; https://orcid.org/0009-0003-3090-668X
[4]Universidad de Panamá, Centro Regional Universitario de Azuero, Facultad de Administración de Empresas y Contabilidad, Panamá; dora.batista-p@up.ac.pa; https://orcid.org/0000-0001-5203-8973

Fecha de recepción: 15-07-2025 *Fecha de aceptación: 26-09-2025*

DOI: https://doi.org/10.48204/j.vian.v9n2.a8877

Resumen: Este ensayo tiene por objetivo explorar la interconexión entre ciberseguridad y auditoría en el contexto actual, para fortalecer la protección de activos digitales. La ciberseguridad se integra en la auditoría para fortalecer la protección de activos digitales. Para su desarrollo se adoptó un enfoque cualitativo documental y reflexivo, sustentado en la investigación de fuentes secundarias para analizar las amenazas digitales, las estrategias de prevención de riesgos cibernéticos y el impacto de la ciberseguridad en la práctica de la auditoría; la metodología se estructuró siguiendo tres etapas: revisión bibliográfica, análisis crítico y argumentativo, y reflexión argumentativa y síntesis de los aportes. Los hallazgos conceptuales indican que la ciberseguridad se integra en la auditoría para fortalecer los controles, evaluar los sistemas de seguridad y asegurar la integridad de los datos; por ello, los auditores deben analizar la efectividad de los controles tecnológicos y utilizar herramientas especializadas para identificar vulnerabilidades cibernéticas, aunque no necesariamente deben ser expertos en tecnología. La creciente importancia de la ciberseguridad ofrece al auditor la oportunidad de participar en la toma de decisiones, integrar medidas de seguridad tecnológicas y especializarse en el área, por lo que la protección de los activos digitales es necesaria, requiriendo del compromiso constante con la seguridad y la adquisición de conocimientos actualizados sobre infraestructura.

Palabras clave: ciberseguridad, auditoría, activos digitales, riesgos cibernéticos, protección de datos.

Abstract: This essay explores the interconnection between cybersecurity and auditing in the contemporary context, with the aim of strengthening the protection of digital assets. A qualitative, documentary, and reflective approachbased on secondary sources was used to analyze digital threats, cyber-risk prevention strategies, and the influence of cybersecurity on auditing practices. The methodology was carried out in three stages: a bibliographic review, critical and argumentative analysis, and a reflective synthesis of contributions. The findings indicate that cybersecurity is being incorporated into auditing to reinforce controls, evaluate security systems, and ensure data integrity. Consequently, auditors must assess the effectiveness of technological controls and employ specialized tools to identify cyber vulnerabilities, although they are not required to be technology specialists. The growing importance of cybersecurity creates opportunities for

auditors to participate in decision-making, integrate technical security measures, and develop specialized expertise. Protecting digital assets therefore demands a sustained commitment to security and the continuous updating of knowledge about infrastructures and controls.

Keywords: cybersecurity, auditing, digital assets, cyber risks, data protection.

1. Introducción

Este ensayo tiene como propósito explorar la relación entre la ciberseguridad y la auditoría, analizando cómo se interconectan en el contexto actual. Como señalan O'Brien y Marakas (2006), la auditoría debe evolucionar para evaluar los controles que mitiguen las amenazas que se presenten. A través de la investigación de fuentes documentales, se analizan aspectos relacionados con las amenazas digitales, las estrategias para prevenir riesgos cibernéticos en la auditoría y el impacto que la ciberseguridad genera en esta práctica.

El tema se desarrolla porque, en la era digital actual, se deben conocer los beneficios y aplicaciones de las nuevas tecnologías, entendiendo los aspectos relacionados con la ciberseguridad, ya que es un conocimiento necesario para alcanzar la estabilidad y confianza en las actividades que dependen del uso constante de tecnologías y sistemas.

El objetivo es demostrar cómo la integración de la ciberseguridad y la auditoría contribuyen a fortalecer la protección de los activos digitales, al mismo tiempo que se mejora la confianza en las actividades que necesitan del uso de sistemas de información para la investigación y presentación de informes de auditoría. Marcos de gobierno, como COBIT framework de ISACA (2018) contribuyen a fortalecer la protección de los activos digitales, al mismo tiempo que se mejora la confianza en las actividades que necesitan del uso de sistemas de información para la investigación y presentación de informes de auditoría.

Desde una perspectiva académica y práctica, es posible establecer la importancia de comprender los riesgos tecnológicos asociados a la auditoría. No es necesario ser experto en ambas disciplinas, pero sí contar con una visión amplia de al menos una de ellas, lo que permite aplicar adecuadamente las herramientas tecnológicas en el ejercicio profesional. La interacción de ambas áreas incrementa la protección de los activos digitales y ofrece un enfoque más completo a la hora de enfrentar los riesgos tecnológicos.

2. Desarrollo

Este estudio se presenta como un ensayo o artículo de reflexión y, por lo tanto, su enfoque es cualitativo, documental y reflexivo. Para estructurar la argumentación y el análisis, se desarrolló siguiendo tres etapas de: revisión bibliográfica, análisis crítico y argumentativo, reflexión argumentativa y síntesis de los aportes.

La primera etapa se centró en la recopilación y análisis de información secundaria sobre la auditoría, ciberseguridad, riesgos cibernéticos y la protección de los activos digitales, donde se utilizaron las fuentes documentales para establecer el marco teórico sobre la necesidad de que la auditoría evolucione para evaluar los controles que mitigan las amenazas presentadas por la hiperconectividad y la era digital. La segunda etapa consistió en un análisis crítico y argumentativo, para el que se necesitó evaluar y analizar la información documental revisada, para establecer la relación entre la ciberseguridad y la auditoría. Este análisis se enfocó en la identificación del papel del auditor, examinando cómo debe evaluar la efectividad de los controles tecnológicos y utilizar los medios especializados para identificar las vulnerabilidades cibernéticas sin ser un experto en tecnología.

Se argumentó sobre cómo la integración de la ciberseguridad en la auditoría fortalece los controles internos, evalúa los sistemas de seguridad y le da paso a la integridad, confidencialidad y disponibilidad de los datos auditados. También se analizó la necesidad de implementar mecanismos de protección de activos digitales como el cifrado y la autenticación multifactor, e incluir la concientización del personal.

La fase final consistió en la síntesis de los hallazgos conceptuales para proponer una reflexión sobre la necesidad de actualizar el conocimiento del auditor, articulando las oportunidades que la ciberseguridad ofrece a los auditores para participar en la toma de decisiones e integrar medidas tecnológicas de seguridad.

La intención de esta metodología fue establecer que la protección de los activos digitales es una necesidad que necesita sustentarse en el compromiso constante con la seguridad y la adquisición de conocimientos actualizados sobre la infraestructura tecnológica y riesgos cibernéticos. Con este enfoque se pudo alcanzar el objetivo de

demostrar cómo la integración de los dos campos contribuye a la protección de los activos digitales.

- **Ciberseguridad y auditoría**

La ciberseguridad es un tema de relevancia creciente en la actualidad, y esto se sustenta en la forma en que ha crecido la hiperconectividad que caracteriza el mundo actual, porque a medida que las organizaciones y los individuos dependen de la tecnología, se enfrentan en esa misma medida a riesgos y amenazas inherentes que pueden comprometer la integridad de sus sistemas de datos (Arreola, 2019). Las amenazas cibernéticas son cada vez más comunes en las infraestructuras tecnológicas, involucrando también el factor humano, porque las decisiones y acciones de las personas influyen directamente en la seguridad. La responsabilidad de mantener seguros los sistemas no recae únicamente en los expertos en tecnología, sino que debe ser compartida por todos los actores involucrados en el manejo y uso de la información digital.

El impacto de la ciberseguridad va más allá de los aspectos tecnológicos porque es, de hecho, un tema transversal que afecta a diversas áreas profesionales, incluyendo la auditoría. El proceso de adaptación en diversas disciplinas integra las metodologías y prácticas que ayudan a gestionar los riesgos digitales de manera efectiva, y siendo la auditoría un proceso indispensable en la evaluación y control de la información dentro de las organizaciones, se encuentra en una posición privilegiada para aplicar principios de ciberseguridad.

La integración de la ciberseguridad en la auditoría incorpora las herramientas tecnológicas de la protección de los datos, como un apoyo al fortalecimiento de los controles internos, la evaluación de los sistemas de seguridad de la información y la implementación de prácticas que aseguren la confidencialidad, integridad y disponibilidad de los datos auditados. En este caso, “una auditoría de riesgos de ciberseguridad realizada con la guía adecuada permite a los auditores ofrecer una garantía razonable sobre la criticidad e impacto potencial de un riesgo” (Sánchez-García *et al*., 2024, p. 72). Por ello, la adopción de estas prácticas en el ámbito de la auditoría permite a los profesionales enfrentar las situaciones que surgen de la interconexión digital, protegiendo activos informáticos y la confianza en los procesos y resultados de las auditorías.

Al integrar estos dos elementos los auditores pueden identificar y mitigar riesgos potenciales, asegurando que los sistemas de información sean utilizados de manera segura y eficiente, porque se trata de un enfoque que contribuye a visionar la gestión de riesgos, considerando aspectos financieros, operativos y tecnológicos para que las amenazas sean evaluadas y gestionadas de manera proactiva. Por lo tanto, la relación que existe entre la ciberseguridad y la auditoría se configura como una forma de garantizar la protección de los datos y sistemas en un mundo cada vez más digitalizado, donde la vulnerabilidad ante los ataques cibernéticos es una realidad que afecta a todos los sectores.

Es importante conocer aspectos clave para lograr que esta relación de tecnologías-auditoría sea efectiva, sin exceder o depender en su totalidad a los sistemas para lograr una integración útil, confiable y adaptable a la realización de cualquier auditoría. Estos aspectos pasan por conocer e identificar riesgos tecnológicos más comunes que pueden ir desde vulnerabilidades en los sistemas redes o datos, hasta el manejo adecuado de la información y la accesibilidad a datos sensibles.

La aplicación de normas y estándares internacionales, como las emitidas por la Organización Internacional de Normalización (ISO) o las Normas de auditoría (NIA's), proporciona un marco de referencia para evaluar la seguridad y eficiencia de los sistemas de información, porque son estándares que facilitan la implementación de buenas prácticas, aseguran la comparabilidad de los procesos y respaldan la conformidad con marcos regulatorios, especialmente en auditorías que abarcan componentes tecnológicos (The Institute of Internal Auditors, 2024).

Hay contextos donde es pertinente diseñar auditorías orientadas solo a evaluar la infraestructura de seguridad digital de una organización, para examinar el grado de protección de los sistemas, redes y dispositivos y la eficacia de las políticas internas de ciberseguridad; esta especialización garantiza tener un mayor control sobre las amenazas emergentes en el mundo digital.

Con el acceso al software especializado se vuelve más sencillo procesar grandes volúmenes de datos, porque se detectan las anomalías, se analizan las tendencias y se monitorean en tiempo real los sistemas auditados, y con ello se mejora el trabajo del auditor cuando se automatizan las tareas repetitivas, porque se reducen los errores

humanos y la información visual apoya la toma de decisiones durante la auditoría, haciendo que este uso sea estratégico más que operativo. En los casos en que no es posible eliminar completamente los riesgos detectados durante el proceso auditor se diseñan por estos medios los planes de acción correctivos que contemplan medidas concretas para mitigar las vulnerabilidades y exponen claramente las estrategias para asegurar la continuidad de las operaciones y la protección de los activos digitales, haciendo efectiva la planificación que refuerza el enfoque preventivo y mejora la capacidad de respuesta ante cualquier tipo de incidentes. No obstante, hay que recordar que se trata de un apoyo y o un reemplazo del criterio auditor, pues su eficacia está sujeta a la calidad de los datos ingresados y a la habilidad del profesional para cuestionar los resultados (Huayra y Salazar, 2024).

- **Rol de los auditores en la identificación de vulnerabilidades cibernéticas**

Si bien es cierto algunos de los roles de un auditor en cualquier tipo de auditoría es identificar riesgos, analizar el entorno auditado y elaborar estrategias sobre la marcha, algunas de estas actitudes no se alejan al rol que debe tomar un auditor al momento de enfrentarse a vulnerabilidades cibernética en los sistemas de información de una organización. Su labor no es exclusivamente verificar el cumplimiento de políticas o normas, también debe plasmar un objetivo de evaluar la efectividad de los controles que se implementan en los recursos tecnológicos disponibles del área que se va a auditar, protegiendo los activos digitales que serán utilizados en la auditoría.

Sin embargo, el auditor no debe cumplir el papel de un profesional en tecnologías o redes, pero si debe manejar con destreza las herramientas tecnológicas que él mismo va a utilizar para el desarrollo de la auditoría, ya que “las herramientas de análisis de datos pueden ser vulnerables a la piratería informática, y la información obtenida del análisis de datos puede utilizarse para abordar los ciberataques de forma más eficaz” (Johari *et al.*, 2023, p. 789).

Al referirse a las herramientas que se pueden utilizar al realizar la auditoría, hay que hablar de las prácticas y pruebas que se diseñan para detectar las posibles vulnerabilidades en los sistemas de información organizacionales, porque no se limitan únicamente a los recursos tecnológicos, sino a las metodologías de evaluación para examinar qué tan

robustos son los controles y en qué medida de eficacia cumplen las medidas de seguridad que se ponen en marcha para la identificación de vulnerabilidades.

Una de las principales pruebas es la de accesos que consiste en la simulación controlada de un intento de acceso no autorizado a una sección del sistema que no comprometa la información crítica, pero que resulte funcional para realizar el análisis de seguridad, tal como simular un ciberataque real a un área específica del sistema, que no sea tan sensible, y se realizan pruebas como iniciar una sesión forzada al sistema de asistencia de los colaboradores, para identificar posibles puntos débiles en las redes, sistemas y aplicaciones de la organización, porque esta es un área que comúnmente utilizan los auditores al momento de realizar las revisiones a la entidad.

- **Protección de activos digitales**

Al realizar una auditoría, los activos digitales adquieren un valor incalculable para el desarrollo y objetivo de auditoría, y es de donde se obtendrá la información para realizar la presentación de informe, convirtiéndose en la base de información en la que el auditor basa sus conclusiones y recomendaciones. Estos activos digitales pueden ser desde datos personales, información financiera, propiedades intelectuales de la organización o cualquier tipo de recurso vital para el funcionamiento y actividad de la organización o personal auditado.

La motivación económica convierte a las compañías en objetivos rentables para los cibercriminales, que buscan obtener importantes beneficios económicos en cada ataque (Entel Digital, 2024). Debido al valor e importancia de los activos digitales de cualquier sistema tecnológico, se convierten en un activo susceptible a ser objeto de acciones maliciosas de los usuarios o ciberdelincuentes que generan amenazas digitales con un fin específico de extracción, eliminación o modificación de estos datos en los sistemas. Esta situación lleva a la necesidad de implementar mecanismos de protección de datos eficaces y de alta calidad, dependiendo del valor o cantidad de activos digitales que se desea proteger.

La capacidad de salvaguardar la confidencialidad e integridad de los activos digitales se convierte en una actividad esencial de toda entidad, en la protección de los sistemas de

información. Debido al avance de las amenazas cibernéticas, es más común que las organizaciones opten por contar con fondos económicos específicos para contratar servicios de protección de sistemas o profesionales de la tecnología que les ayuden a prevenir posibles ataques.

El número de incidentes en el ciberespacio responde, en buena medida, el interés económico que motiva a los atacantes. Los activos digitales valiosos se han transformado en el blanco principal de acciones maliciosas, representando un riesgo constante para las organizaciones, independientemente de su tamaño o naturaleza y esta realidad ha sido la que ha llevado a considerar la ciberseguridad como una medida técnica y una estrategia crítica. Además, como señalan Trujillo-Avilés *et al*. (2024), "se debe definir cuidadosamente el alcance de la auditoría para evitar la dispersión de esfuerzos" (p. 3898) y esto tiene que ver con la necesidad de que las organizaciones prioricen sus esfuerzos de protección hacia sus activos más críticos y sus vectores de ataque más probables, destinando recursos de este tipo a las áreas de mayor riesgo.

Entre los riesgos más comunes se encuentran el robo de información, la suplantación de identidad, los ataques a sistemas empresariales o personales y el *pishing*, una técnica que consiste en el secuestro de los datos a cambio de una recompensa económica. Estas son amenazas que afectan por igual a las grandes corporaciones, a las empresas pequeñas y medianas, e incluso a los individuos que tengan acceso a información sensible o que ejercen funciones de alta responsabilidad.

Este es un panorama en el que resulta indispensable conocer e implementar estrategias básicas de protección que puedan integrarse a las prácticas profesionales y a las actividades cotidianas. El uso responsable de las redes sociales, la gestión de contraseñas, el cuidado en el intercambio de información digital y la capacitación continua en seguridad informática son aspectos que ayudan a reducir este tipo de vulnerabilidades. Así como existe el *pishing*, existen otros métodos empleados por ciberdelincuentes cuyo objetivo es vulnerar los sistemas informáticos. Por lo tanto, la prevención y actualización constante en materia de ciberseguridad resulta imprescindible para mantener la protección de los activos digitales en cualquier entorno.

Proteger los activos digitales ha sido una prioridad estratégica por el valor que representan y el número cada vez en aumento de las amenazas que los ponen en riesgo, donde la implementación de medidas preventivas y correctivas aumenta la seguridad de la información para preservar la integridad de los sistemas. Las estrategias se pueden aplicar de forma complementaria y deben ser adaptadas a cada organización, al volumen de los datos y al grado de sensibilidad de la información gestionada. López-Anchala y Ordóñez-Parra (2024) señala que todas las empresas, sin distinción, operan en un medio donde sus activos digitales más importantes también son los más susceptibles a sufrir ataques, debido a la evolución constante de los ciberataques.

El cifrado (contraseñas, mensajes, archivos o firmas digitales) debe ser legible solo para los usuarios autorizados y debe ser complementado con mecanismos de autenticación para verificar la identidad de quienes acceden a estos sistemas, siendo recomendable aplicar la autenticación multifactor para reforzar la seguridad, porque son medidas que reducen la probabilidad de otorgar accesos no autorizados que constituyen una barrera inicial ante posibles ataques.

Otra de las estrategias es aplicar el monitoreo y la detección de amenazas con sistemas de alerta a tiempo de forma continua, ya que esta acción preventiva es propia de la gestión en cualquier organización (Bósquez-Andrade y Torres-Palacios, 2024). Los análisis de comportamiento y la tecnología especializada se están utilizando más para identificar los intentos de acceso indebido y detectar las vulnerabilidades o comportamientos inusuales en tiempo real, ya que es un tipo de vigilancia que, por ser constante, permite actuar de forma proactiva y fortalecer la respuesta ante cualquier incidente, pero también se deben proteger los datos con cifrado o autenticación.

Ninguna de estas medidas para proteger los activos digitales está completa si no se considera la importancia de las capacitaciones y se crea conciencia en el personal, porque el factor humano es uno de los eslabones más vulnerables en la cadena de seguridad digital. Hay que aprender a formar a los colaboradores en buenas prácticas profesionales, fomentar la cultura de ciberseguridad y actualizar cada cierto tiempo su conocimiento sobre las amenazas existentes para que todos protejan conscientemente los sistemas.

- **El auditor en la integración de los sistemas de ciberseguridad**

A pesar de la evolución de los modelos de protección, las amenazas seguirán aumentando y eso necesita de la participación de los auditores en las operaciones de seguridad, porque en la actualidad muchas empresas siguen dependiendo de tecnologías preventivas genéricas y no especializadas que por lo general son gratuitas o de uso global y pueden aplicarse a diferentes tipos de sistemas de información (Campos, 2023). Este argumento es compartido por Bruce (2025), quien señala la necesidad de contar con infraestructura adecuada para identificar a tiempo las vulnerabilidades que pueden tener los sistemas de información antes de que se transformen en amenazas reales. Lo que sucede con esta práctica es que se pueden generar vulnerabilidades importantes, especialmente cuando se trata de sistemas grandes, cuya complejidad necesita de soluciones personalizadas. Cuando se implementan herramientas, el costo para las que se adaptan a las particularidades de cada organización tienen un costo más elevado y no es común que se contemple esto como prioritario en la planificación financiera.

Aquí es donde se recurre a la contratación de un auditor externo que realice una evaluación integral del sistema de información y cuando se detecta una ausencia de barreras de seguridad que cumplan su función, o una baja prioridad para la protección digital, se plantea la necesidad de que el auditor sea inteligente frente a los riesgos existentes. Aunque no sea su competencia directa desarrollar e implementar sistemas tecnológicos para la protección de datos, sí es su responsabilidad emitir recomendaciones claras, específicas y contextualizadas para la mitigación de riesgos.

Los planes de acción en ciberseguridad y la creación de escenarios de riesgo que muestren las consecuencias de no adoptar medidas de protección que sean adecuadas son algunas de las acciones que pueden sugerirse. Con estas recomendaciones se anticipan a las amenazas y se establecen protocolos preventivos, ya que su propósito es evitar que, ante un eventual incidente, se atribuya al informe de auditoría la omisión de advertencias pertinentes. Es la manera de fortalecer las oportunidades que ofrece la auditoría de manera estratégica para promover la incorporación de sistemas de ciberseguridad en el desarrollo de las actividades organizacionales, elevando con ello los niveles de protección, responsabilidad y transparencia en el entorno digital.

- **Oportunidades de la ciberseguridad en la auditoría**

La ciberseguridad se está tomando cada vez más en cuenta en las organizaciones como un método estratégico para la resolución de problemas y detección de riesgos en los sistemas tecnológicos (Acosta, 2024). Esto crea un mundo de oportunidades para los auditores, que les permite involucrarse en la toma de decisiones corporativas y ayudar a las organizaciones a integrar medidas de seguridad tecnológicas, como en la resolución de un problema de seguridad en los sistemas de información antes planteado en los desafíos de la ciberseguridad aplicados a la auditoría.

El uso de tecnologías más recientes, como la inteligencia artificial masificada, los sistemas de información avanzados y las herramientas de ciberseguridad, ha transformado la práctica tradicional de auditoría. Los auditores, que históricamente se apoyaban en métodos convencionales para la revisión documental y elaboración de informes, han comenzado a actualizar sus metodologías, incorporando soluciones que, en muchos casos, han facilitado el proceso, sin embargo, esta transición también ha sido un reto para quienes tienen un conocimiento limitado del manejo de estas tecnologías.

La ampliación hacia la auditoría digitalizada mejora las oportunidades de desarrollo de competencias y servicios especializados y es una forma en la que el auditor se posiciona como un aliado en la gestión de riesgos cibernéticos capaces de ser identificados, evaluados y controlados con procesos adaptados al entorno digital. Este argumento lo refuerza Sánchez (2024), quien señala que, al modificarse las operaciones de las empresas, los datos se vuelven más voluminosos, haciendo necesario el uso de medios digitales para analizarlos, consolidando el papel del auditor moderno como un profesional que se encuentra en el centro de este proceso.

En la actualidad se observa una creciente demanda de auditores especializados en tecnología y cibernética, capaces de aplicar sus conocimientos en cualquier tipo de auditoría. Esto se debe a que, en los procesos, ya no basta con realizar revisiones contables o financieras; ahora se necesita incluir análisis de riesgos, planes de acción ante vulnerabilidades, pruebas de acceso cuando se utilicen sistemas específicos, y la generación de recomendaciones en posibles incidentes. Estas son acciones con las que el auditor emite

un informe más completo y con mayor valor agregado para la entidad auditada, al facilitar la identificación de brechas de seguridad y proponer mejoras de forma proactiva.

Se reconoce que los auditores deben adquirir nuevas habilidades y conocimientos relacionados con la tecnología que está surgiendo, como el aprendizaje automático y la inteligencia artificial. Esto lleva a adoptar posturas estratégicas para utilizarla como una aliada y no como una amenaza a las labores tradicionales de auditoría. La evolución también es un desafío, porque las organizaciones esperan que los auditores les brinden recomendaciones generales y que también actúen como asesores especializados capaces de analizar totalmente los riesgos existentes, identificar oportunidades que puedan utilizar y proponer el uso estratégico de la tecnología en la gestión y protección de los sistemas de información.

3. Conclusiones

Actualmente, la protección de los activos digitales en cualquier organización, no debe ser una opción en la cual se considere o no invertir, sino que se ha convertido en una necesidad del entorno digital de cualquier entidad que desee mantener sus activos digitales de manera confidencial, protegidos y alejados de cualquier amenaza. Esto solo se logrará mediante un compromiso vigente y constante con la seguridad, siendo esta un reflejo de la calidad de los sistemas que adquiera la empresa, y así mismo funcionará frente a una situación de riesgo.

También es importante resaltar la responsabilidad que debe tener en cuenta el auditor si desea utilizar cualquier tipo de sistema de información como apoyo a la labor de auditoría, porque la integración de cualquier práctica es fundamental para gestionar los posibles riesgos y amenazas cibernéticas que puede enfrentar el auditor para presentar información sensible, y para la entidad que posee activos digitales valiosos.

Con la creciente demanda y los avances tecnológicos, se requiere que los auditores obtengan cada vez más conocimientos sobre tecnologías y ciberseguridad, lo cual representa una oportunidad de conocimientos laborales, y una vía para que las organizaciones fortalezcan su seguridad y adopción de tecnologías a medida que van evolucionando dentro de las organizaciones. El auditor no solamente debe nutrirse con

conocimientos financieros y de control, sino que también se debe adoptar un conocimiento sólido y en constante actualización sobre infraestructura tecnológica y riesgos cibernéticos.

La ciberseguridad y la auditoría se entrelazan de manera importante para fortalecer la protección de los activos digitales en la organización. Esta es una necesidad en el entorno actual y la integración de las prácticas se vuelve fundamental a la hora de gestionar riesgos y amenazas para la entidad auditada y para el auditor que maneja información sensible, por lo que se requiere que los auditores adquieran conocimientos sólidos y actualizados sobre infraestructura tecnológica y los riesgos cibernéticos.

Referencias Bibliográficas

Acosta C., N. N. (2024). *Impacto de la inteligencia artificial en la ciberseguridad empresarial: un análisis crítico de la evolución de amenazas y medidas preventivas*. [Tesis de Grado]. Universidad Técnica de Babahoyo. https://dspace.utb.edu.ec/bitstream/handle/49000/15738/PI-UTB-FAFI-SIST-00011.pdf?sequence=1&isAllowed=y

Arreola G., A. (2019). *Ciberseguridad. ¿Por qué es importante para todos?* Universidad Anáhuac México. https://goo.su/I6f4

Bósquez-Andrade, E. I., y Torres-Palacios, M. M. (2024). Auditoría continua y monitorización en tiempo real: detección, mitigación de riesgos empresariales en industrias hoteleras. *Revista Metropolitana de Ciencias Aplicadas*, *7*(2), 76-86. https://doi.org/10.62452/q62zma54

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

Campos I., C. (2023). *Ciber riesgos, una nueva era de riesgos paralas empresas. Análisis del impacto en los resultados, la marca y la reputación. Modelos de prevención y de gestión*. [Tesis de Grado]. Comillas, Universidad Pontificia. https://repositorio.comillas.edu/rest/bitstreams/599675/retrieve

Entel Digital. (2024). *Guía completa de ciberseguridad para empresas y activos digitales*. https://www.enteldigital.cl

Huayra C., E. D., y Salazar T., M. (2024). *Escepticismo profesional y calidad de auditorías financieras desde la percepción de los auditores independientes de Junín, 2023*. [Tesis de Grado]. Universidad Nacional de Huancavelica. https://apirepositorio.unh.edu.pe/server/api/core/bitstreams/ab8a6531-1be0-4e4e-a1f5-97101a6ad01f/content

ISACA. (2018). COBIT 2019 Framework: introduction & methodology. ISACA. https://community.mis.temple.edu/mis5203sec003spring2020/files/2019/01/COBIT-2019-Framework-Introduction-and-Methodology_res_eng_1118.pdf

Johari, Z. A., Ghazali, A. W., Mat Isa, Y., Shafie, N. A., & Sanusi, S. (2023). Digital Disruption and Cybersecurity Threats: Redefining The Role of Internal Auditing. *Social and Behavioural Sciences, 131*, 788-801. https://doi.org/10.15405/epsbs.2023.11.65

López-Anchala, K. A., y Ordóñez-Parra, Y. L. (2024). Auditoría y ciberseguridad en el sector comercial: evaluación de resiliencia ante amenazas digitales [Audit and cyber security in the commercial sector: assessing resilience to digital threats]. *Revista Multidisciplinaria Perspectivas Investigativas*, *4*(especial), 14-27. https://doi.org/10.62574/rmpi.v4iespecial.154

O'Brien, J. A., y Marakas, G. M. (2006). *Sistemas de información gerencial*. McGraw-Hill/Interamericana Editores, S.A. DE C.V. https://dspace.itsjapon.edu.ec/jspui/bitstream/123456789/1420/1/sistemas-de%20informaci%C3%B3n%20gerencial.pdf#page=9.09

Sánchez S., E. F. (2024). Análisis de las auditorias digitales y su influencia en los mecanismos de simplificación del proceso de auditoría realizados en Ecuador en el año 2022 [Tesis de Grado]. https://www.dspace.uce.edu.ec/server/api/core/bitstreams/bbec6b82-0694-4fad-85fa-8a9379689206/content

Sánchez-García, I. D., Rea-Guaman, A. M., Feliu, T. S., y Calvo-Manzano, J. A. (2024). Auditoría de riesgos de ciberseguridad: Revisión de Literatura, propuesta y aplicación. *RISTI-Revista Ibérica de Sistemas e Tecnologias de Informação*, (53), 69-87. https://doi.org/10.17013/risti.53.69-87

The Institute of Internal Auditors. (2024). *Normas globales de auditoría interna*. The Institute of Internal Auditors. https://www.theiia.org/globalassets/site/standards/editable-versions/global-internal-audit-standards-spanish.pdf

Trujillo-Avilés, M. N., Morales-López, D. A., Taipe-Yanez, J. F., y Pallo-Tulmo, P. A. (2024). Estrategias de Auditoría en ciberseguridad y su importancia en las empresas una revisión bibliográfica. *MQRInvestigar*, *8*(2), 3889-3913. https://doi.org/10.56048/MQR20225.8.2.2024.3889-3913