ANÁLISIS DE LAS TECNOLOGÍAS Y NORMATIVAS EN AUDITORÍA INFORMÁTICA: UN ESTUDIO DE IMPLEMENTACIONES BASADAS EN COBIT Y MAGERIT

ANALYSIS OF TECHNOLOGIES AND REGULATIONS IN COMPUTER AUDITING: A STUDY OF IMPLEMENTATIONS BASED ON COBIT AND MAGERIT

Renelmo Wladimir Minaya Macias[1*]

[1] Carrera Tecnologías de la Información y Carrera Ingeniería en Software. Universidad Laica Eloy Alfaro de Manabí, Extensión en El Carmen. ORCID: https://orcid.org/0000-0002-0418-6864. Correo: renelmo.minaya@uleam.edu.ec

Rocío Alexandra Mendoza Villamar[2]

[2] Carrera Tecnologías de la Información y Carrera Ingeniería en Software. Universidad Laica Eloy Alfaro de Manabí, Extensión en El Carmen. ORCID: https://orcid.org/0000-0002-1277-7162. Correo: rocio.mendoza@uleam.edu.ec

Alex Bladimir Mora Marcillo[3]

[3] Carrera Tecnologías de la Información y Carrera Ingeniería en Software. Universidad Laica Eloy Alfaro de Manabí, Extensión en El Carmen. ORCID: https://orcid.org/0000-0002-0883-4603. Correo: alex.mora@uleam.edu.ec

Javier Agustín Intriago Navarrete[4]

[4] Escuela Superior Politécnica Agropecuaria de Manabí - Manuel Félix López. ORCID: https://orcid.org/0009-0002-9883-841X. Correo: j_avitino@hotmail.com

*** Autor para correspondencia: renelmo.minaya@uleam.edu.ec**

Resumen

El presente estudio tuvo como objetivo analizar la implementación e impacto de las metodologías COBIT y MAGERIT en auditorías informáticas, evaluando su efectividad en la gestión de riesgos y la seguridad de sistemas de información. La investigación adoptó un enfoque cualitativo con diseño exploratorio-descriptivo,

siguiendo los lineamientos de la metodología PRISMA. Los criterios de inclusión de artículos científicos publicados entre 2019 y 2024 en español e inglés y relacionados específicamente con auditorías informáticas y la implementación de los marcos normativos mencionados. Se excluyeron revisiones, opiniones, tesis y editoriales. La revisión incluyó 10 artículos seleccionados de una base inicial de 879 registros. Los resultados destacan la capacidad de COBIT y MAGERIT para optimizar la gobernanza y seguridad de los sistemas, mitigando riesgos y fortaleciendo la toma de decisiones estratégicas en entornos tecnológicos. Además, se identificaron interacciones clave entre conceptos y acciones; COBIT se asocia predominantemente con acciones estratégicas y de gobernanza, mientras que MAGERIT se destaca por su impacto significativo en técnicas relacionadas con la gestión de riesgos. En conclusión, el análisis reafirma la relevancia de integrar estas metodologías para responder a los desafíos de la transformación digital y garantizar la sostenibilidad de las infraestructuras informáticas. Estos hallazgos contribuyen al diseño de estrategias más efectivas en auditorías de sistemas de información, alineadas con las necesidades actuales de las organizaciones.

Palabras clave: gestión de riesgos, gobernanza de TI, seguridad informática, transformación digital, Auditoria de sistemas.

Abstract

The objective of this study was to analyze the implementation and impact of COBIT and MAGERIT methodologies in IT audits, evaluating their effectiveness in risk management and information systems security. The research adopted a qualitative approach with an exploratory-descriptive design, following the PRISMA methodology guidelines. The inclusion criteria of scientific articles published between 2019 and 2024 in Spanish and English and specifically related to IT audits and the implementation of the aforementioned regulatory frameworks. Reviews, opinions, theses and editorials were excluded. The review included 10 articles selected from an initial base of 879 records. The results highlight the ability of COBIT and MAGERIT to optimize system governance and security, mitigating risks and strengthening strategic decision making in technological environments. In addition, key interactions between concepts and actions were identified; COBIT is predominantly associated with strategic and governance actions, while MAGERIT stands out for its significant impact on techniques related to risk management. In conclusion, the analysis reaffirms the relevance of integrating these methodologies to respond to the challenges of digital transformation and ensure the sustainability of IT infrastructures. These findings contribute to the design of more effective strategies in information systems audits, aligned with the current needs of organizations.

Keywords: *risk management, IT governance, computer security, digital transformation, systems audit.*

Fecha de recibido: 02/10/2024
Fecha de aceptado: 10/12/2024
Fecha de publicado: 11/12/2024

Introducción

La evolución de las tecnologías de la información ha provocado que las organizaciones dependan cada vez más de sistemas informáticos y redes interconectadas para llevar a cabo sus operaciones diarias. Esta creciente dependencia, sin embargo, viene acompañada de un aumento en los riesgos relacionados con la seguridad de la información y el manejo adecuado de los datos. Para gestionar estos desafíos, han surgido marcos normativos y metodologías como COBIT y MAGERIT, que permiten a las organizaciones establecer controles y realizar auditorías que garanticen la seguridad de sus infraestructuras tecnológicas (Reis, 2015; Solarte & Rosero, 2015).

COBIT (Control Objectives for Information and Related Technologies) es un marco de gobierno de TI desarrollado por ISACA, cuyo objetivo es ofrecer un modelo integral para la gestión y auditoría de sistemas informáticos. COBIT permite a las organizaciones equilibrar los riesgos asociados con la inversión en tecnologías de la información, mediante la definición de dominios clave como planificación, adquisición, implementación y evaluación de sistemas (Marca & Boonen, 2007). La metodología, al estar orientada a la alta dirección y a los auditores, proporciona un marco sólido para la toma de decisiones estratégicas que aseguran el cumplimiento normativo y la eficiencia en los procesos de TI (ISO 27001, 2020).

Por otro lado, la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) se centra en la identificación y gestión de riesgos relacionados con el uso de la información en organizaciones. Esta metodología permite analizar los posibles riesgos asociados con los activos tecnológicos, priorizarlos según su impacto y establecer medidas correctivas que ayuden a mitigar dichos riesgos (Ministerio de Hacienda y Administraciones Públicas, 2012). MAGERIT es particularmente relevante en entornos educativos y gubernamentales, donde la seguridad de la información es fundamental para garantizar la continuidad de los servicios (Derrien, 2009).

Las normas de calidad establecen los requisitos necesarios para alcanzar los objetivos de una auditoría, mientras que los estándares de calidad son criterios utilizados para medir la calidad de los sistemas y procesos auditados. Ambos son esenciales en auditorías informáticas, ya que aseguran el cumplimiento de los requisitos y fomentan la mejora continua. Aunque MAGERIT es ampliamente conocida en auditorías informáticas, no es una norma oficial, sino una metodología creada por Luis Joyanes Aguilar y su equipo. Su propósito es gestionar riesgos en proyectos de TI y telecomunicaciones, proporcionando un marco para identificar, analizar y evaluar riesgos (Zapata, 2021, citado por Minaya et al., 2023).

El principal problema que enfrentan muchas organizaciones es la implementación efectiva de estos marcos normativos y metodologías. Aunque COBIT y MAGERIT proporcionan directrices claras para la gestión de riesgos y auditorías, su adopción es limitada en ciertos sectores debido a la falta de recursos, desconocimiento de las normativas o subestimación de los riesgos. Esto deja a las organizaciones vulnerables frente a ciberamenazas que podrían comprometer tanto la integridad de los datos como la operatividad de sus sistemas informáticos (Buendía, 2013). Según Morales (2019), la falta de una adecuada gestión de riesgos en los sistemas informáticos puede provocar pérdidas significativas, tanto económicas como de reputación, para las organizaciones.

Desde una perspectiva normativa, la adopción de marcos como ISO 27001 para la gestión de la seguridad de la información se vuelve crucial. Esta norma internacional establece los requisitos para implementar un

Sistema de Gestión de la Seguridad de la Información (SGSI) que asegure la confidencialidad, integridad y disponibilidad de los activos informáticos de una organización (ISO 27001, 2020). La combinación de COBIT, MAGERIT e ISO 27001 permite a las organizaciones crear un entorno seguro y eficiente para la gestión de la tecnología, mitigando los riesgos y mejorando el control sobre los sistemas de información.

En este orden, es preciso destacar que la auditoría informática es un conjunto de procedimientos llevados a cabo por expertos para recopilar, evaluar y verificar la precisión de los sistemas de información en una organización. Su objetivo es asegurar que la información sea precisa y se gestionen los recursos de manera eficiente, cumpliendo con normas y estándares. Además, la auditoría informática evalúa los procesos organizacionales, identificando fallas y proponiendo mejoras en la verificación y eficiencia operativa, optimizando el uso de los recursos informáticos. Es una herramienta clave para garantizar el buen funcionamiento y control de los sistemas tecnológicos (Lizárraga et al., 2022).

Las auditorías implementadas utilizando el marco COBIT facilitan la verificación del cumplimiento de las políticas y regulaciones aplicables. Además, ofrecen recomendaciones para fortalecer la seguridad y optimizar la gestión de riesgos en el entorno de TI. Al adoptar COBIT, las organizaciones pueden alinear sus procesos de TI con las mejores prácticas y estándares internacionales, lo que mejora la eficiencia y la gobernanza. Estas auditorías no solo aseguran el cumplimiento normativo, sino que también identifican oportunidades para mejorar la infraestructura de seguridad y minimizar vulnerabilidades. En conjunto, contribuye a una gestión más sólida y proactiva de los riesgos tecnológicos (Burgos-Rojas et al.,2024).

La justificación de este estudio se fundamenta en la necesidad imperante de proteger los activos informáticos frente a un panorama de amenazas cibernéticas cada vez más sofisticadas. De acuerdo con Ferruzola (2019), la implementación de auditorías informáticas basadas en COBIT y MAGERIT ofrece una solución efectiva para identificar vulnerabilidades y fortalecer la seguridad de las infraestructuras tecnológicas. Además, la adopción de estos marcos normativos asegura que las organizaciones no solo cumplan con las regulaciones vigentes, sino que también promuevan una cultura de seguridad proactiva dentro de sus estructuras operativas (Falcón & Serpa, 2021).

Por lo tanto, en este artículo se realiza una revisión del estado actual de las tecnologías y normativas que rigen la auditoría informática, con un enfoque en la implementación de COBIT y MAGERIT. El estudio proporciona una revisión exhaustiva de las mejores prácticas en auditoría informática y destacar cómo estas metodologías pueden ayudar a las organizaciones a proteger sus sistemas, reducir riesgos y mejorar su desempeño operativo.

La investigación se realiza con el propósito de analizar la implementación y el impacto de las metodologías COBIT y MAGERIT en auditorías informáticas, evaluando su efectividad en la gestión de riesgos y seguridad en sistemas de información, proporcionando una revisión exhaustiva de las mejores prácticas para optimizar la protección y gobernanza de los activos tecnológicos en organizaciones.

En tal sentido, la pregunta de investigación que se responde con el desarrollo de esta revisión es: ¿Cómo contribuyen las metodologías COBIT y MAGERIT a la mejora de la seguridad informática y la gestión de riesgos en auditorías, y cuáles son las mejores prácticas derivadas de su implementación en diferentes tipos de organizaciones?

Materiales y métodos

Este artículo adopta un enfoque cualitativo para analizar la implementación de las metodologías COBIT y MAGERIT en auditoría informática, utilizando un análisis de co-ocurrencia a través del software ATLAS.ti. A continuación, se describen las etapas del proceso metodológico que guiaron esta investigación.

El diseño metodológico de este estudio fue exploratorio-descriptivo, dado que se buscó entender la relación entre los conceptos clave derivados de la literatura sobre auditoría informática. El estudio presenta cómo los marcos normativos y las mejores prácticas de auditoría, específicamente COBIT y MAGERIT, coexisten y se interrelacionan dentro de la seguridad informática y la gestión de riesgos en distintos sectores organizacionales.

Para la revisión de la literatura, se tuvieron en cuenta criterios de inclusión y exclusión siguiendo la metodología PRISMA. Se seleccionaron documentos y estudios relevantes relacionados con la auditoría informática, la gestión de riesgos y la implementación de marcos normativos, específicamente COBIT y MAGERIT en sistemas de información. La selección de los textos se realizó a través de la base de datos Google académico. Se incluyeron en el análisis solo artículos científicos de investigación, publicados entre el año 2019 y 2024, se excluyeron artículos de revisión, informes técnicos, tesis y editoriales. A continuación, se muestra una tabla que refleja los criterios de inclusión y exclusión que se tuvieron en cuenta para la revisión de la literatura.

Tabla 1. Criterios de inclusión y de exclusión.

Criterios	Criterios de inclusión	Criterios de exclusión
Bases de datos	Google Schoolar	Otras bases de datos fuera de las mencionadas
Año de publicación	2019-2024	Estudios publicados antes de 2019
Idioma	Inglés y Español	Otros idiomas diferentes de inglés y español
Tipo de estudio	Artículos de investigación	Artículos de revisión, opiniones, tesis y editoriales.
Temática	Estudios que se centran en auditorías informáticas y el empleo del modelo COBIT y la metodología MARGERIT.	Estudios con otras temáticas no relacionadas.

Para la búsqueda de la literatura se empleó la siguiente cadena de búsqueda: (“auditoría informática” OR “auditoría de TI” OR “auditoría de sistemas de información”) AND (“COBIT” OR “MAGERIT” OR “ISO 27001”) AND (“gestión de riesgos” OR “seguridad informática” OR “gobierno de TI” OR “controles de seguridad”) AND (“mejores prácticas” OR “metodologías de auditoría”).

La aplicación de la estrategia de búsqueda dio como resultado 10 artículos incluidos en la revisión sistemática, tal como se presenta en el siguiente diagrama.

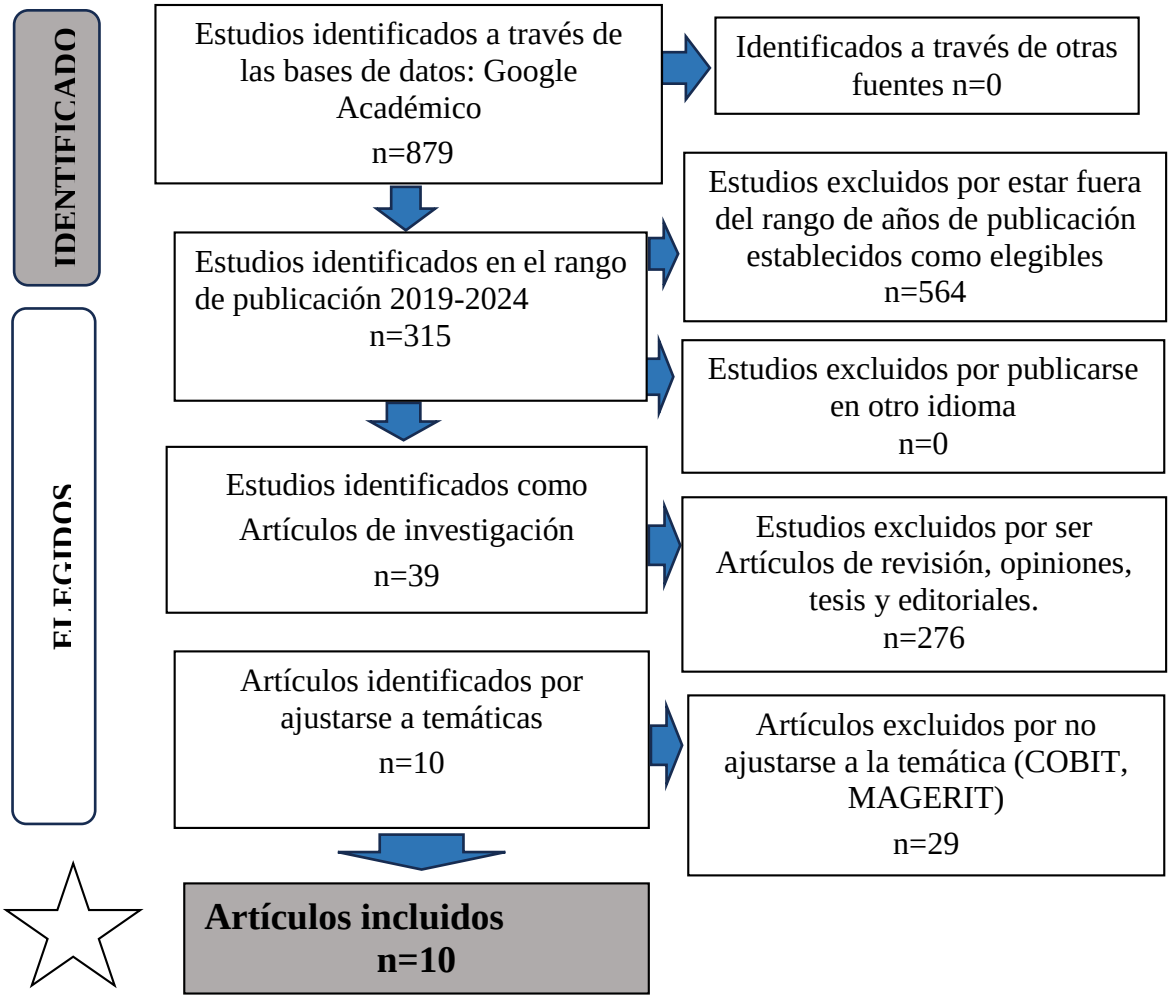

Figura 1. Diagrama PRISMA del proceso de selección de estudio.

Como se muestra en el diagrama, la estrategia de búsqueda aplicada inicialmente identificó 879 resultados de investigación. Al aplicar los criterios de inclusión, las mayores exclusiones (564 estudios) estuvieron dadas por ser estudios publicados fuera del rango de años de publicaciones establecidas como elegibles y estudios excluidos por ser Artículos de revisión, opiniones, tesis y editoriales (276).

Una vez seleccionados los textos relevantes (10 artículos de investigación), se procedió a su importación al software ATLAS.ti para realizar el análisis cualitativo. Los documentos fueron revisados detalladamente para identificar categorías, conceptos clave y relaciones que sirvan como insumos para el análisis de co-ocurrencia.

En el análisis de coocurrencia se analizó la relación entre los conceptos claves y acciones que se presentan a continuación:

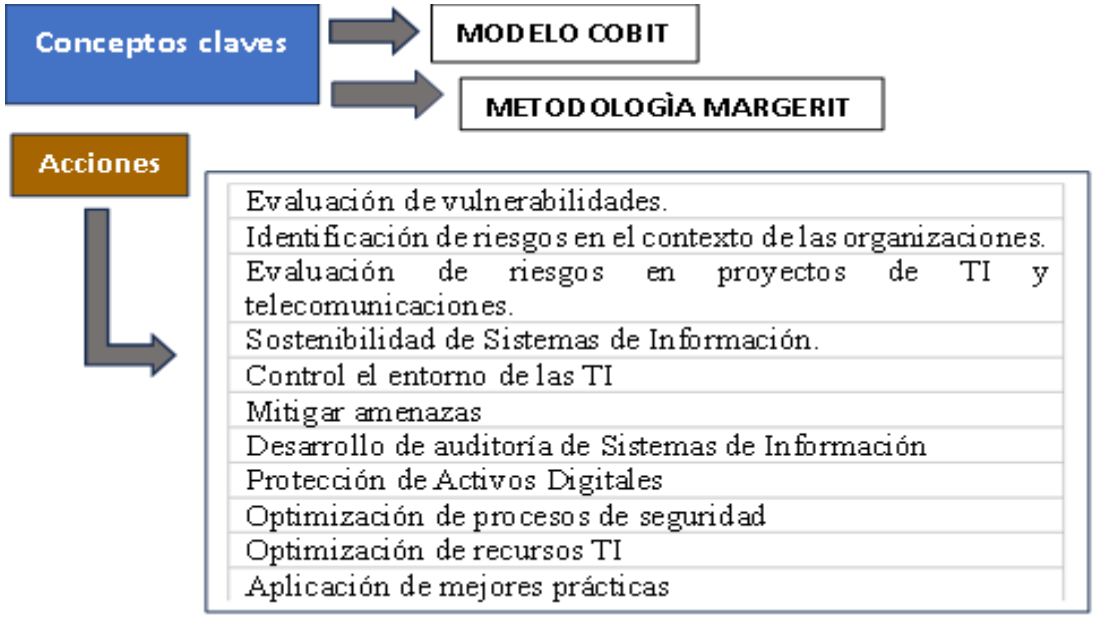

Figura 2. Conceptos claves y acciones de la matriz de doble entrada (ATLAS, ti).

Resultados y discusión

Los resultados de la revisión sistemática incluyeron 10 artículos de investigaciòn, que se presentan en este apartado. En la tabla 2 se muestran los autores, año de publicación, país y título, de cada artículo, en español e inglés. Se ofrece en la tabla 3 una síntesis de los resultados de los artículos incluidos en la revisión sistemática; concretamente, objetivo que persigue cada estudio y aporte màs significativo de sus resultados a la revisión sistemática. Además, se realizó un análisis de co-ocurrencia tomando en cuenta los conceptos claves y acciones de la figura 2.

Tabla 2. Artículos incluidos en la revisión sistemática.

Autores	Año	País	Título en Español	Título en inglés
Anderson Santiago Moran Arellano, Patricia Rosalía Jimbo Santana, Mónica de Jesús Jimbo Santana, Juan Carlos Franco Valverde	2023	Ecuador	Aplicación de COBIT 2019 al gobierno y gestión de las tecnologías de información en instituciones educativas sin fines de lucro	Application of COBIT 2019 to the government and management of information technologies in non-profit educational institutions
Rene Aquino Arcata, Ronald Cuevas Machaca, Gustavo Adolfo Villarroel Laura	2023	Perú	El modelo COBIT 5 para Auditoría Informática de los Sistemas de Información Académica de la Universidad Nacional Jorge Basadre Grohmann	The COBIT 5 model for Computer Audit of the academic information systems of the National University Jorge Basadre Grohmann
Oswaldo Alejandro Zhañay Soliz, Juan Carlos	2019	Ecuador	Modelo de Auditoria de Sistemas de Información para las Cooperativas	Information Systems Audit Model for Savings and Credit Cooperatives

Autores	Año	País	Título en Español	Título en inglés
Erazo Álvarez, Cecilia Ivonne Narváez Zurita			de ahorro y crédito del segmento 1, 2, y 3, de la ciudad de Cuenca	of segment 1, 2, and 3, in the city of Cuenca
Kevin Daniel Cusme Zambrano, Yasmina Lizetty Zambrano Loor, Leydi Talía Zambrano Mendoza, Jessica Johanna Morales Carrillo	2022	Ecuador	Procesos de tecnologías de la información en instituciones públicas	Information technology processes in public institutions
Patricia Jimbo-Santana, Karen Cabrera-Pantoja, Mónica Jimbo-Santana	2023	Ecuador	Análisis Comparativo de Metodologías para el desarrollo de Auditorías Informáticas considerando: Análisis de Riesgos, Minería de Datos, Marcos y Normas de Referencia y Normas Internacionales de Normalización	Comparative Analysis of Methodologies for the development of Computer Audits considering: Risk Analysis, Data Mining, Reference Frameworks and Standards and International Standards for Standardization
Julio Pedro Paladines Morán, Grace Liliana Figueroa-Morán, José Nevard Paladines Morán	2021	Ecuador	Plan estratégico de seguridad informática para la protección de recursos en el laboratorio de telecomunicaciones	Strategic plan for computer security for the protection of resources in the telecommunications laboratory
Leidy Angamarca	2022	Argentina	Estrategias de auditoría informática en la era de la transformación digital	IT audit strategies in the era of digital transformation
Juan Carlos Sendón-Varela, Jorge Herrera-Tapia, Lytyet Fernández-Capestany, Marely del Rosario Cruz Felipe, Leonardo Chancay-García, Washington García-Quilachamín	2021	Ecuador	Análisis comparativo entre distintas metodologías para la realización de auditorías de seguridad informática, aplicando el Proceso Analítico Jerárquico (AHP)	Comparative analysis between different methodologies for performing computer security audits, applying the Hierarchical Analytical Process (AHP)
Silvia Edith Albarrán Trujillo, Juan Carlos Pérez Merlos, Mireya Salgado Gallegos, Laura Luz Valero Conzuelo	2020	Mèxico	Las Metodologías de la Auditoría Informática y su relación con Buenas Prácticas y Estándares	The Methodologies of IT Audits and Their Relationship with Good Practices and Standards
Leidy Angamarca	2022	Argentina	Estrategias de auditoría informática en la era de la transformación digital	IT audit strategies in the era of digital transformation

De los artículos incluidos, el 60% son resultados de investigaciones realizadas en Ecuador, con una menor representación de países como: Argentina, Perú y México. El rango de año más frecuente de publicación de los resultados está entre el 2021- 2023, lo que refleja un alto nivel de actualización de los artículos sistematizados.

Tabla 3. Síntesis de los resultados de los artículos incluidos en la revisión sistemática.

No.de Art.	Objetivo	Aporte a la investigación
1	Evaluar la implementación de COBIT en el gobierno y gestión de las tecnologías de la información en instituciones educativas sin fines de lucro.	Proporciona una guía sobre la flexibilidad y facilidad de adaptación de COBIT 2019 en instituciones educativas, lo que optimiza la alineación entre los objetivos tecnológicos y los objetivos organizacionales.
2	Proponer el uso de COBIT 5 para realizar auditorías informáticas de los sistemas académicos en la Universidad Nacional Jorge Basadre Grohmann.	Proporciona un marco práctico para la auditoría de sistemas académicos usando COBIT 5, contribuyendo a mejorar el control y eficiencia de los sistemas de información en entornos académicos.
3	Desarrollar un modelo de auditoría de sistemas de información aplicable a cooperativas de ahorro y crédito, utilizando marcos como COBIT y COSO.	Introduce un modelo específico para cooperativas financieras que carecen de especialización en auditoría informática, lo que mejora su capacidad para realizar auditorías de TI.
4	Identificar y evaluar las áreas clave en los procesos de tecnología de la información de las instituciones públicas, con base en la norma de control interno de la Contraloría General del Estado.	Proporciona un análisis exhaustivo sobre la aplicación de normas de control interno para mejorar los procesos de TI en el sector público.
5	Comparar las metodologías de auditoría informática más utilizadas (MAGERIT, OCTAVE, NIST SP 800-30) para seleccionar la más adecuada según las necesidades organizacionales.	Proporciona un análisis detallado de diferentes metodologías, ayudando a las organizaciones a identificar la mejor herramienta para auditar riesgos de seguridad informática.
6	Desarrollar un plan estratégico de seguridad informática para la protección de los recursos del laboratorio de telecomunicaciones de una universidad	Presenta una solución estratégica para mejorar la seguridad informática en entornos académicos, evaluando los recursos tecnológicos y diseñando políticas de seguridad basadas en estándares internacionales.
7	Proponer estrategias de auditoría informática en la era de la transformación digital, utilizando normas como ISO/IEC 27000, COBIT, y PCI DSS.	Presenta estrategias que se adaptan a la transformación digital, con un enfoque en la gestión de riesgos y auditorías periódicas, permitiendo a las organizaciones mantenerse competitivas en un entorno tecnológico en evolución.
8	Comparar varias metodologías de auditoría de seguridad informática y determinar cuál es la más adecuada para la infraestructura de redes de datos del sector industrial pesquero.	Identifica la metodología OSSTMM como la más efectiva para el sector industrial pesquero, basándose en la facilidad de implementación y complejidad media, lo que permite mejorar los procesos de auditoría de seguridad.

9	Explorar la relación entre las metodologías de auditoría informática y su vinculación con buenas prácticas y estándares internacionales.	Establece un vínculo claro entre las metodologías de auditoría y su alineación con estándares como ISO/IEC 27001, destacando cómo estas prácticas mejoran la seguridad y el cumplimiento normativo.
10	Describir las estrategias necesarias para realizar auditorías informáticas efectivas en el contexto de la transformación digital.	Reitera la importancia de adaptar las auditorías a la transformación digital, evaluando los riesgos y cumpliendo con normas internacionales de seguridad informática.

Los artículos revisados destacan la flexibilidad y eficacia de marcos como COBIT, MAGERIT y estándares internacionales como ISO/IEC 27001 en auditorías informáticas. Se resalta su capacidad para optimizar la gestión de TI en sectores educativos, financieros e industriales, además de su alineación con buenas prácticas y normativas internacionales. Los análisis comparativos permiten seleccionar metodologías adecuadas para contextos específicos, mientras que las estrategias enfocadas en la transformación digital refuerzan la seguridad, el cumplimiento normativo y la adaptabilidad tecnológica de las organizaciones. Estos hallazgos consolidan la auditoría informática como herramienta clave en la gestión de riesgos tecnológicos.

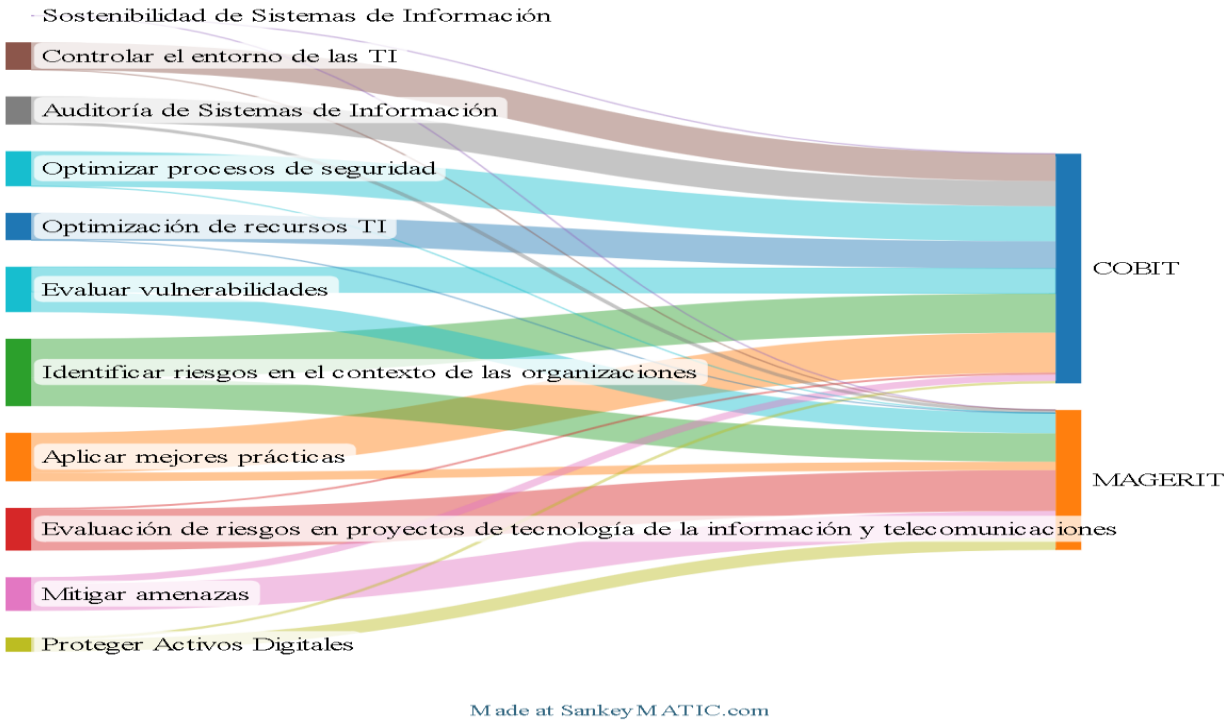

Figura 3: Resultados de la co-ocurrencia entre conceptos claves y acciones.

El gráfico tipo Sankey evidencia la coocurrencia entre las metodologías COBIT y MAGERIT en acciones clave de auditoría y gestión de sistemas de información, destacando las áreas en las que cada una tiene mayor influencia. COBIT se asocia predominantemente con acciones estratégicas y de gobernanza, tales como la sostenibilidad de los sistemas de información, el control del entorno de TI, la auditoría de sistemas, la optimización de recursos tecnológicos y procesos de seguridad y se destaca en la identificación de riesgo en el contexto de organizaciones y en la aplicación de mejores prácticas; lo que refuerza su enfoque en la alineación de los objetivos tecnológicos con los organizacionales. Por otro lado, MAGERIT tiene un impacto significativo en técnicas relacionadas con la gestión de riesgos, como la evaluación de riesgos en proyectos de tecnología de la información y la mitigación de amenazas, destacando su orientación hacia la identificación de riesgos y reducción de vulnerabilidades específicas. En conjunto, estas metodologías complementan sus fortalezas, ofreciendo una visión integral que combina gobernanza estratégica con análisis detallado de riesgos, fortaleciendo así la seguridad y la eficiencia en los sistemas de TI.

Discusión

En la era de la transformación digital, la auditoría informática ha adquirido una relevancia sin precedentes debido a la creciente exposición a riesgos y amenazas cibernéticas. Las metodologías como COBIT, MAGERIT y otras normas internacionales de seguridad informática, como ISO/IEC 27001, se han convertido en herramientas fundamentales para garantizar la protección de los sistemas de información. Diversos estudios han abordado la implementación y comparación de estas metodologías en diferentes contextos, proporcionando enfoques útiles para fortalecer la gestión de riesgos en distintos sectores.

Uno de los principales aportes en la auditoría informática es la flexibilidad que ofrece COBIT 2019 al aplicarse en instituciones educativas sin fines de lucro. Este marco normativo ha demostrado su capacidad para alinear los objetivos tecnológicos con los objetivos organizacionales, mejorando la eficiencia de la gestión de TI en dichas instituciones (Moran et al., 2023). Este hallazgo resalta la adaptabilidad de COBIT 2019 a diferentes sectores, especialmente aquellos que no están orientados al lucro, donde la gestión efectiva de recursos tecnológicos es fundamental.

Asimismo, el uso de COBIT 5 en la auditoría informática de sistemas académicos ha sido explorado con éxito en la Universidad Nacional Jorge Basadre Grohmann. La investigación demuestra que este marco proporciona una estructura sólida para controlar y mejorar los sistemas de información académica, garantizando la transparencia y eficiencia operativa (Aquino et al., 2023). Estos resultados confirman que COBIT 5 es una metodología versátil, aplicable tanto en el ámbito educativo como en entornos empresariales.

En el contexto financiero, el desarrollo de un modelo de auditoría de sistemas de información para cooperativas de ahorro y crédito en Cuenca, Ecuador, ha sido significativo. Al integrar los marcos de COBIT y COSO, este estudio propone una solución viable para instituciones que carecen de especialistas en auditoría informática, mejorando su capacidad de control interno y gestión de riesgos (Zhañay et al., 2019). Esto resalta la importancia de personalizar los marcos de auditoría para sectores que tienen necesidades específicas y recursos limitados.

El sector público también se ha beneficiado del análisis de los procesos de tecnologías de la información en instituciones gubernamentales. Un estudio que evaluó la auditoría informática en instituciones públicas en Ecuador, utilizando la norma de control interno, muestra que la implementación de procesos estructurados de TI es esencial para mejorar la transparencia y seguridad de los recursos tecnológicos en estas instituciones (Cusme et al., 2022). Este estudio subraya la importancia de la normatividad y la capacitación del personal en la mejora de la gestión pública de los sistemas de información.

Además, la comparación entre metodologías de auditoría informática, como MAGERIT, OCTAVE y NIST SP 800-30, ha permitido identificar las metodologías más apropiadas para distintas organizaciones. En particular, se ha destacado que MAGERIT es ideal para la evaluación de riesgos en infraestructuras críticas debido a su capacidad para abordar amenazas complejas y específicas (Jimbo-Santana et al., 2023). Esto ofrece a las organizaciones una herramienta valiosa para seleccionar la metodología que mejor se ajusta a sus necesidades de seguridad.

Por otro lado, un estudio sobre la implementación de un plan estratégico de seguridad informática en laboratorios de telecomunicaciones demuestra la importancia del diseño de políticas de seguridad basadas en normas internacionales. La investigación sugiere que estas políticas permiten proteger de manera efectiva los recursos tecnológicos, especialmente en entornos académicos donde la investigación y la innovación tecnológica son esenciales (Paladines et al., 2021). Este enfoque refuerza la necesidad de contar con estrategias de seguridad que respondan a las características particulares de los entornos educativos.

En el contexto de la transformación digital, las auditorías informáticas han evolucionado para enfrentar nuevos desafíos tecnológicos. Un estudio sobre las estrategias de auditoría en esta era señala que las normas como ISO/IEC 27000, COBIT y PCI DSS son fundamentales para garantizar la seguridad y protección de la información, mientras se realizan auditorías periódicas para adaptarse a un entorno en constante cambio (Angamarca, 2022). Este aporte es esencial para las organizaciones que desean mantenerse al día con las mejores prácticas de seguridad en la era digital.

De manera complementaria, un análisis comparativo entre distintas metodologías de auditoría de seguridad informática, realizado en el sector industrial pesquero de Ecuador, concluye que OSSTMM es la metodología más adecuada para las empresas de este sector, debido a su complejidad media y facilidad de implementación (Sendón-Varela et al., 2021). Este estudio destaca la importancia de seleccionar metodologías específicas que se ajusten a las características y limitaciones de cada sector industrial.

Por último, la investigación sobre la relación entre las metodologías de auditoría informática y las buenas prácticas y estándares internacionales confirma que una correcta alineación entre estas metodologías y normas como ISO/IEC 27001 mejora significativamente la gestión de riesgos y el cumplimiento normativo (Albarrán et al., 2020). Este hallazgo es crucial para las organizaciones que buscan optimizar su gestión de TI y cumplir con los requisitos regulatorios.

Conclusiones

Con la revisión sistemática se logra identificar la relevancia de los marcos normativos y metodología al destacar cómo las metodologías COBIT y MAGERIT, combinadas con normas internacionales como ISO/IEC 27001 y constituyen herramientas fundamentales para fortalecer la seguridad informática y la gestión de riesgos. Estas metodologías no solo permiten identificar y mitigar vulnerabilidades, sino que también promueven una gobernanza eficiente de los activos tecnológicos en diferentes sectores organizacionales.

Los artículos incluidos en la sistematización evidencian la flexibilidad y la adaptabilidad de las metodologías revisadas El análisis evidencia que COBIT y MAGERIT son ampliamente aplicables en contextos diversos, desde instituciones educativas hasta organizaciones gubernamentales y financieras. Su implementación facilita la alineación de los objetivos tecnológicos con los organizacionales, optimizando los recursos disponibles y promoviendo una cultura de mejora continua en la gestión de TI.

La investigación resalta la contribución a la transformación digital y al cumplimiento normativo, destaca cómo la integración de estas metodologías y normas de seguridad informática responde a los desafíos emergentes de la transformación digital. Estas prácticas no solo fortalecen el cumplimiento regulatorio, sino que también aseguran la resiliencia de las organizaciones frente a las crecientes amenazas cibernéticas, garantizando la sostenibilidad y eficiencia de los sistemas de información.

Referencias

Albarrán Trujillo, S.E., Pérez Merlos, J.C., Salgado Gallegos, M., & Valero Conzuelo, L.L. (2020). Las metodologías de la auditoría informática y su relación con buenas prácticas y estándares. Ideas en Ciencias de la Ingeniería, 1(1). 47-70.

Angamarca, L. (2022). Estrategias de auditoría informática en la era de la transformación digital. Diario de lluvia tecnológica , 1 (1), e1. https://doi.org/10.55204/trj.v1i1.1

Aquino Arcata, R., Cuevas Machaca, R., & Villarroel Laura, GA (2023). El modelo COBIT 5 para Auditoría Informática de los Sistemas de Información Académica de la Universidad Nacional Jorge Basadre Grohmann. Revista Peruana de Tecnología , 34 (2), 12-30.

Burgos-Rojas, MA, Haro-Polo, CI, & Mendoza-de los Santos, AC (2024). Impacto del uso de diversos marcos de seguridad en las auditorías informáticas dentro de las organizaciones: Revisión sistemática. Revista UCSA , 11(2), 103-115.http://dx.doi.org/10.18004/ucsa ./ 2409-8752 /2024.011.02.0103

Buendía, JF (2013). Seguridad informática . McGraw-Hill.https://www.mheducation.es/seguridad-informatica

Cusme Zambrano, KD, Zambrano Loor, YL, Zambrano Mendoza, LT y Morales Carrillo, JJ (2022). Procesos de tecnologías de la información en instituciones públicas. Revista Pública de Gestión TI ,18 (2), 55-70.

Derrien, Y. (2009). Técnicas de la auditoría informática . Marcombo.https ://www .marcombo .com /auditoria -informati

Falcón, AL y Serpa, GR (2021). Cerca de los métodos teóricos y empíricos de investigación: Significado para la investigación educativa. Conrado. Revista pedagógica de la Universidad de Cienfuegos , 17 (S3https://conrado.ucf.edu.cu/index.php/conrado//artículo /vista /2266

Ferruzola Gómez, JD (2019). Plan de contingencia para los equipos y sistemas informáticos utilizando la metodología MAGERIT. CTU Revista Científica y Tecnología UPSE .https://revistas.upse.edu.ec/index.p/ctu /artículo /vista /250

ISO 27001. (2020). Sistema de Gestión de la Seguridad de la Información .https://normaiso27001.es//a9 -control -de -acceso/

Jimbo-Santana, P., Cabrera-Pantoja, K. y Jimbo-Santana, M. (2023). Análisis Comparativo de Metodologías para el desarrollo de Auditorías Informáticas considerando: Análisis de Riesgos, Minería de Datos, Marcos y Normas de Referencia y Normas Internacionales de Normalización. Revista de Auditoría y Control , 10 (3), 112-135.

Lizárraga Caipo, YG, Panaqué Domínguez, JA, & Mendoza de los Santos, AC (2022). Impacto de la auditoría informática en las organizaciones: una revisión bibliográfica. Ingeniería , 4 (e638), 2708-303https://doi.org/10.47796/ing.v4i0.638

Marca, M. y Boonen, R. (2007). Metas corporativas de negocio COBIT 5 . Instituto de Gobierno.https://www.isaca.org/bookstore/cobit-5

Ministerio de Hacienda y Administraciones Públicas. (2012). MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Madrid: Ministeriohttps://www.ccn-cert.cni.es/index.php/es/magerit

Minaya Macías, MM, Minaya Macías, RW, Intriago Navarrete, ML, & Intriago Navarrete, JA (2023). Normas y estándares en auditoría: una revisión de su utilidad en la seguridad informática. Pentaciencias, 5 (4), 584-599.https://editorialalema.org/index.php/pentaciencias/article/view/700/976.

Morales Gortárez, FJ (2019). Tecnología de la información como herramienta de la auditoría. Contaduría pública .https://doi.org/10.22201/fca.24488410e.2020.2316

Morales, G. (2019). Mantenimiento de equipos informáticos. https ://www. educacionyfp .gob .es /catalogo /formacion -profesional /mantenimiento .html

Morán Arellano, AS, Jimbo Santana, PR, Jimbo Santana, MDJ, & Franco Valverde, JC (2023). Aplicación de COBIT 2019 al gobierno y gestión de las tecnologías de información en instituciones educativas sin fines de lucro. Revista Tecnología y Sociedad, 15 (2), 98-115.

Paladines Morán, JP, Figueroa-Morán, GL y Paladines Morán, JN (2021). Plan estratégico de seguridad informática para la protección de recursos en el laboratorio de telecomunicaciones. Serie Científica de la Universidad de las Ciencias Informáticas ,14 (11), 43-59.

Reis, LC (2015). Fundamentos de COBIT 5. https ://www. fundacioncedia .org /libro -fundamentos -cobit- 5

Sendón-Varela, JC, Herrera-Tapia, J., Fernández-Capestany, L., Cruz Felipe, MR, Chancay-García, L., & García-Quilachamín, W. (2021). Análisis comparativo entre distintas metodologías para la realización de auditorías de seguridad informática, aplicando el Proceso Analítico Jerárquico (AHP). Revista Ibérica de Sistemas e Tecnologias de Informação , (E40), 352-367.

Solarte, NF y Rosero, JS (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. Revista Tecnológica ESPOL ,28 (5). https://doi.org/10.18840 /revtecespol. v28i5.125.

Zapata, J. (2021). Aplicación de metodología Margerit en la Gestión de Riesgos de Tecnologías de la Información en la agencia Metro Santana Elena. Universidad Nacional Pedro Ruiz Gallo. Lambayeque. Perú.

Zhañay Soliz, OA, Erazo Álvarez, JC, & Narváez Zurita, CI (2019). Modelo de Auditoría de Sistemas de Información para las Cooperativas de ahorro y crédito del segmento 1, 2, y 3, de la ciudad de Cuenca. Revista de Auditoría Financiera, 7 (1), 4.