Trabajo Fin de Máster

Los marcos COBIT y MAGERIT en el contexto de la auditoría de ciberseguridad

Autora

Gianella Marjorie Romero Anaya

Director

Carlos Serrano Cinca

Área de conocimiento

Economía Financiera y Contabilidad

Facultad de Economía y Empresa. Universidad de Zaragoza

Septiembre de 2024

RESUMEN

En el entorno actual, en el que las tecnologías de la información tienen una relevancia significativa dado a su rápida evolución y utilidad en las distintas organizaciones, es necesario preguntarse si existe un marco idóneo que permita a las empresas realizar una correcta auditoría de ciberseguridad. El objetivo de este trabajo es responder a esta cuestión a través de una revisión bibliográfica exhaustiva basado en la metodología PRISMA centrada en dos metodologías clave: COBIT y MAGERIT. Tras el análisis se encuentra que COBIT es la metodología más estudiada mientras que MAGERIT es la que más se estudia de manera individual. También destaca que ambas son metodologías que se adaptan muy bien a otros marcos logrando ser más eficaces, lo que permite realizar una óptima auditoría de ciberseguridad. Es evidente que se necesita ampliar las líneas de investigación para permitir a las organizaciones tener una base sólida de evidencia que les permita elegir que marco utilizar.

***Palabras clave*:** Ciberseguridad, Auditoría de TI, COBIT y MAGERIT.

ABSTRACT

In the current environment, where information technologies have significant relevance due to their rapid evolution and usefulness in different organizations, it is necessary to ask whether an ideal framework allows companies to conduct a correct cybersecurity audit. This work aims to answer this question through an exhaustive bibliographic review based on the PRISMA methodology focused on two key methods: COBIT and MAGERIT. After the analysis, it is found that COBIT is the most studied methodology while MAGERIT is the one that is most studied individually. It also highlights that both are methodologies that adapt very well to other frameworks, achieving greater efficiency, which allows for an optimal cybersecurity audit to be carried out. The lines of research need to be expanded to allow organizations to have a solid evidence base that allows them to choose which framework to use.

Keywords: Cybersecurity, IT Audit, COBIT and MAGERIT.

ÍNDICE

ÍNDICE DE TABLAS Y FIGURAS

1. INTRODUCCIÓN

1.1. Justificación

En un contexto como el actual se puede observar como las empresas les otorgan cada vez mayor relevancia a las herramientas informáticas para poder agilizar, controlar y revisar sus procesos de producción, entre otras funcionalidades, debido a una cada vez mayor relevancia del entorno virtual en todos los ámbitos. De hecho, una de las causas de las primeras transformaciones empresariales parece haber ido asociada a las relevantes transformaciones tecnológicas de digitalización e información (Rodríguez-Palenzuela, 2001). Así mismo, existe una nueva revolución industrial impulsada por la transformación digital, con los correspondientes beneficios directos e indirectos que conlleva (Barra Novoa, 2021). También, es necesario evaluar las consecuencias menos beneficiosas de la informatización de la industria, en concreto, considerando la exposición de la información generada u obtenida del entorno para la toma de decisiones o procesamiento de sus operaciones, ya que es necesario realizar un análisis costo-beneficio sobre la implementación de controles de esta información (Vaca Benalcázar, 2016).

La protección de la información no es algo reciente y se ha ido desarrollando a lo largo del tiempo, la seguridad informática se centraba principalmente en proteger los datos almacenados en sistemas aislados, con enfoques rudimentarios que incluían contraseñas simples y mecanismos básicos de control de acceso (Anderson, 2020). Durante 1990 y al inicio de los 2000 se empezó a observar la aparición de amenazas más complejas como el malware (programa informático cuya principal característica es que se ejecuta sin el conocimiento o autorización del usuario del equipo infectado y realiza funciones en el sistema que son perjudiciales (IBM, 2022)) y los ataques de denegación de servicio, lo que impulsó el desarrollo de firewalls (herramienta que permite gestionar qué programas pueden establecerlas y qué programas no, y qué tipo de conexiones serán permitidas (INCIBE, s. f.)), sistemas de detección de intrusos y protocolos de encriptación más robustos (Schneier, 2015).

Un claro ejemplo de esta evolución informática es la implementación de nueva tecnología como la inteligencia artificial (IA) cada vez más vigente y transformando

diversos sectores, siendo ámbitos como la auditoría nada ajenos a estos avances (Morán Vilcherrez, 2020). La IA se puede utilizar en la auditoría para automatizar tareas repetitivas, analizar grandes bases de datos y detectar patrones anómalos que podrían indicar riesgos de seguridad (Martínez, 2019). Entre las principales ventajas de la IA, en la auditoría, se encuentran la mejora de la velocidad y la precisión en la recopilación de datos, incluyendo también un nuevo paradigma de análisis predictivo (Adamyk et al., 2023). Sin embargo, la implementación de la IA también presenta inconvenientes, como la necesidad de contar con personal en capacitación continua para gestionar la tecnología emergente y los riesgos asociados a la privacidad y seguridad de los datos utilizados por los algoritmos de IA ya que pueden vulnerar las diversas políticas de protección de datos (Nieto, 2022).

Para poder hacer frente a estas ventajas y desventajas, la ciberseguridad requiere una colaboración público-privada y la adopción de medidas proactivas para afrontar los nuevos desafíos siendo la formación, la concienciación y la inversión en la ciberseguridad necesarias para garantizar la seguridad de la información y los sistemas críticos en un mundo cada vez más digitalizado (Candau, 2021). Concretamente, la ciberseguridad se centra en garantizar la confidencialidad, integridad y disponibilidad de la información siendo necesario para este propósito establecer políticas claras, estrategias de prevención, medidas de seguridad y capacitación del personal (Cuervo Forero, 2023). Como herramienta para este propósito tenemos las metodologías centradas en la gestión de gobierno de TI (COBIT y COSO ERM) y para gestión de riesgos de TI (MAGERIT, OCTAVE, NIST 800-30) (Vaca Benalcázar, 2016).

Actualmente, la ciberseguridad es un aspecto fundamental de la auditoría y se debe integrar en ella para garantizar la fiabilidad de la información y proteger los intereses de las partes involucradas ya que una auditoría bien ejecutada puede ayudar a las organizaciones a entender mejor sus debilidades y a mejorar sus defensas contra posibles amenazas cibernéticas (Ghirardotti & Renna, 2022). Estos procesos de evaluación y verificación son fundamentales para construir una infraestructura de ciberseguridad robusta y con una capacidad de mejora continua, capaz de adaptarse a las nuevas y emergentes amenazas del ciberespacio. Por lo tanto, se hace fundamental realizar un análisis exhaustivo sobre la literatura existente de las metodologías más relevantes para

poder facilitar la realización de una auditoría de ciberseguridad exitosa y con la mayor rigurosidad planteándose la siguiente pregunta de investigación:

¿Una metodología de auditoría de ciberseguridad más amplia como COBIT se ajusta mejor a los requisitos que tiene que cumplir una eficaz auditoría de ciberseguridad o es preferible utilizar una más específica como MAGERIT o una combinación de ambas?

Este trabajo tiene como objetivo realizar una revisión bibliográfica exhaustiva para poder responder a la pregunta de investigación planteada.

1.2. Objetivos

El objetivo general del trabajo es realizar una revisión exhaustiva y metódica sobre la literatura acerca de las metodologías de auditoría de ciberseguridad elegidas para determinar si alguna de las dos predomina sobre la otra en el cumplimiento de una eficaz auditoría de ciberseguridad o si por el contrario sería conveniente utilizar ambas.

Para poder cumplir con este objetivo general se han determinado los siguientes objetivos específicos:

O.E. 1. Identificar los requisitos o criterios necesarios para realizar una auditoría de ciberseguridad apropiada.

O.E. 2. Seleccionar las metodologías a analizar.

O.E. 3. Revisar los criterios y marcos conceptuales utilizados para definir las diferentes metodologías analizadas.

O.E. 4. Organizar la información recabada definiendo un criterio común y único.

O.E. 5. Analizar la información obtenida sobre ambas metodologías.

O.E. 6. Obtener las conclusiones tras el análisis.

El trabajo abordará el análisis de la literatura a través de una revisión sistemática de los trabajos elegidos tras aplicar la metodología elegida para la criba de estos. La estructura del trabajo es la descrita a continuación. En el apartado 2 se iniciará con una

investigación cualitativa incluyendo la revisión sobre la literatura existente, analizando y recopilando la fundamentación teórica existente sobre el tema objeto de estudio. En el apartado 3 se puntualizará sobre sobre la metodología a seguir y el razonamiento tras la elección de los marcos objeto de estudios. Así mismo, en el apartado 4 se mostrarán los resultados obtenidos tras seguir esta metodología elegida. Posteriormente, en el apartado 5 se procederá a comentar la inteligencia artificial y lo que aporta a la ciberseguridad, en el apartado 6 se hablará de las limitaciones encontradas y para finalizar, en el apartado 7, se expondrán las conclusiones.

2. MARCO TEÓRICO

2.1. Auditoría de Ciberseguridad

Las auditorías de TI engloban la ciberseguridad y, a pesar de su relevancia actual, no hay una normativa vigente amplia ni exhaustiva (Sabillón & Cano M., 2019). Debido a esto, al ser la auditoría de ciberseguridad un proceso sistemático y documentado, que tiene como objetivo evaluar la seguridad de un sistema de información, es esencial que las empresas adopten un enfoque proactivo para mejorar su ciberseguridad (Trujillo-Avilés et al., 2024).

2.2. Criterios para una Correcta Auditoría de Ciberseguridad

El establecimiento de un alcance definido y claro es fundamental para una auditoría efectiva, lo que implica identificar los sistemas, redes y aplicaciones a auditar, así como los objetivos específicos de la auditoría (Rios Reyes et al., 2023). También, la planificación detallada, que incluye la asignación de recursos, la definición de roles y responsabilidades, y la elaboración de un cronograma minucioso, asegura que todos los aspectos de la auditoría se aborden de manera eficaz y organizada (Manrique Plácido, 2019).

La selección de una metodología reconocida y estandarizada, como COBIT o ISO/IEC 27001, proporciona un marco estructurado y fiable para la auditoría (Calder & Watkins, 2015). Complementariamente, la implementación de herramientas de auditoría adecuadas es importante para realizar evaluaciones precisas y eficientes, ayudando a automatizar la recopilación y el análisis de datos, y reduciendo la posibilidad de errores humanos (Macias et al., 2023). La evaluación de riesgos es otro criterio clave, que implica

la identificación y evaluación de amenazas y vulnerabilidades específicas que pueden afectar a la organización, realizando análisis de riesgos detallados y continuamente actualizados (Rozas Flores, 2014). Evaluar el impacto potencial y la probabilidad de ocurrencia de las amenazas identificadas permite priorizar las acciones correctivas y asignar recursos de manera efectiva (Ochoa Diez et al., 2022).

El cumplimiento normativo es un aspecto fundamental de la auditoría de ciberseguridad y esto incluye una revisión exhaustiva de las políticas y procedimientos de seguridad de la información para asegurar su alineación con las normativas y estándares relevantes (Rios Reyes et al., 2023). La documentación adecuada de los hallazgos y la elaboración de informes claros y detallados son importantes para una auditoría exitosa siendo necesario que estos informes deban incluir recomendaciones prácticas para mitigar los riesgos identificados y mejorar la postura de seguridad (Coha Escalante & Barraza Mármol, 2024). Finalmente, es esencial implementar un plan de seguimiento para asegurar que las recomendaciones se implementen adecuadamente y revisar periódicamente la efectividad de las medidas adoptadas (Calder & Watkins, 2015).

2.3. Metodología COBIT 5 en Auditoría de Ciberseguridad

COBIT (Control Objectives for Information and related Technology) es un marco de referencia desarrollado por ISACA (Information Systems Audit and Control Association) para el gobierno y gestión de las tecnologías de la información (TI). El objetivo de COBIT es proporcionar un marco integral que ayude a las organizaciones a alcanzar sus metas de gobernanza y gestión de TI (ISACA, 2012). Esto incluye asegurar que la tecnología de la información esté alineada con los objetivos empresariales, optimizando el uso de recursos, gestionando riesgos y garantizando el cumplimiento de regulaciones y políticas (Macias et al., 2023). Además, COBIT es una metodología basada en procesos que permiten crear valor dentro de las empresas, garantizando la optimización de solución de riesgos, transparencia de todos los recursos, cumplimiento de normativa reguladora, reglamentos y políticas (López, 2017).

2.3.1. Principios de COBIT

COBIT se basa en cinco principios fundamentales que garantizan un enfoque holístico en la gestión de TI y está diseñado para satisfacer las necesidades de todas las

partes interesadas al alinear los objetivos de TI con los empresariales, ofreciendo también los procesos y catalizadores necesarios para que las organizaciones logren este alineamiento, lo que permite la creación de valor empresarial y al ser perzonalizabe permite adaptarse al contexto de cada organización mediante la cascada de metas (proceso que traduce los objetivos empresariales en metas más concretas y alcanzables, facilitando su seguimiento y cumplimiento) (ISACA, 2012).

Los catalizadores (factores que influyen en el funcionamiento) utilizados en COBIT, que son relevantes para el gobierno y la gestión de la información y de TI, se aplican a nivel de toda la organización, garantizando así una cobertura completa y unificada que destaca por la aplicación de un marco único e integrado que incorpora otros estándares y marcos de referencia existentes, ofreciendo una visión coherente y completa de la gestión de TI (ISACA, 2012). Este enfoque holístico asegura que todas las áreas relevantes, como personas, procesos, tecnología, marcos de trabajo e información, sean consideradas de manera conjunta para alcanzar los objetivos de la empresa (ISACA, 2012).

Un principio clave es la distinción entre las responsabilidades de gobierno y de gestión de TI. El gobierno, que es responsabilidad del consejo de administración, se enfoca en evaluar las necesidades, condiciones y opciones de las partes interesadas para asegurar que se cumplan las metas corporativas a través de la priorización y la toma de decisiones estratégicas, además de medir el rendimiento y el cumplimiento. Por otro lado, la gestión, que recae en la dirección, se encarga de planificar, construir, ejecutar y controlar las tareas de acuerdo con las directrices establecidas por la alta dirección, asegurando así la operatividad alineada con los objetivos organizacionales (ISACA, 2012).

2.3.2. Componentes de COBIT 5

Cascada de Objetivos

Al enfrentarse cada organización a factores externos e internos diferentes, la cascada de objetivos de COBIT traduce las necesidades de las partes interesadas en objetivos específicos y personalizados de TI, asegurando que las iniciativas de TI estén alineadas con las metas empresariales. Este componente facilita la identificación y

priorización de los objetivos estratégicos de TI, así como una alineación entre sus necesidades y las soluciones obtenida (ISACA, 2012).

- Paso 1. Los motivos de las partes interesadas influyen en sus necesidades
- Paso 2. Las necesidades de las partes interesadas desencadenan metas empresariales
- Paso 3. Cascada de metas de empresa a metas relacionadas con las TI
- Paso 4. Cascada de metas relacionadas con las TI hacia metas catalizadoras

Modelo de Referencia de Procesos

COBIT proporciona un modelo de referencia que incluye 37 procesos de gobierno y gestión, organizados en cinco dominios: Evaluar, Dirigir y Monitorizar (EDM); Alinear, Planificar y Organizar (APO); Construir, Adquirir e Implementar (BAI); Entregar, Servir y Soportar (DSS); y Monitorizar, Evaluar y Valorar (MEA) e incluye una serie de guías y herramientas que facilitan su implementación, adaptándola a las necesidades específicas de cada organización (ISACA, 2012).

2.3.3. Aplicación de COBIT en la ciberseguridad

La aplicación de COBIT con un enfoque en la ciberseguridad es un paso relevante para las instituciones, ya que permite adaptar la gestión de la información a las necesidades específicas del sector y garantizar la seguridad de la información en un entorno cada vez más complejo (Orellana-Cabrera & Álvarez-Galarza, 2022). Entre sus ventajas se encuentra su estandarización, flexibilidad y mejora continua mientras que sus desventajas principales serían la complejidad, los costos de implementación y dependencia de personal especializado (Almanza Gómez, 2012).

2.4. Metodología MAGERIT en Auditoría de Ciberseguridad

MAGERIT (Metodología de Análisis y Gestión Riesgos de los Sistemas de Información) es una metodología desarrollada por el Consejo Superior de Administración Electrónica de España para la gestión de riesgos en tecnologías de la información y su objetivo es proporcionar un marco sistemático para identificar, analizar y gestionar los riesgos relacionados con la seguridad de la información, garantizando así la minimización de riesgos a la hora de la implementación y uso de los activos de información así como su confidencialidad, integridad y disponibilidad (CSAE, 2012).

2.4.1. Principios de MAGERIT

La metodología MAGERIT se basa en la norma ISO 31000, que establece directrices para la gestión de riesgos, y se centra en proporcionar un enfoque sistemático para la toma de decisiones informadas en relación con la seguridad de la información (CSAE, 2012).

Los objetivos directos son, primero, el concienciar a los responsables de la información de la existencia de riesgos y de la necesidad de gestionarlos; segundo, ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC), tercero, acompañar a la empresa en su proceso de descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control mientras que el objetivo indirecto derivado es el preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación (CSAE, 2012).

2.4.2. Componentes de MAGERIT

Esta metodología se centra en dos tareas a realizar con respecto a la gestión del riesgo, estas son el análisis y tratamiento, basándose en una serie de pasos claves para el análisis y gestión de riesgos en sistemas de información. En primer lugar, se realiza una contextualización, donde se comprenden los objetivos de la organización y el entorno en el que opera, identificando los sistemas de información y los activos involucrados (CSAE, 2012). A continuación, se procede a la identificación de activos, determinando y caracterizando los elementos relevantes, como información, servicios, aplicaciones, hardware y recursos humanos (Crespo-Martínez & Cordero-Torres, 2018).

El siguiente paso es la identificación de amenazas, donde se consideran tanto las amenazas naturales como las humanas que pueden afectar a los activos (Fernandez & Garcia, 2016). Posteriormente, se lleva a cabo un análisis de vulnerabilidades, evaluando las debilidades en el sistema que podrían ser explotadas por las amenazas identificadas (Vega et al., 2017). Con esta información, se realiza una evaluación de riesgos, estimando la probabilidad de ocurrencia de las amenazas y el impacto que tendrían sobre los activos, lo que permite calcular el nivel de riesgo y, se procede al tratamiento de estos, seleccionando e implementando medidas adecuadas para gestionarlos, ya sea mediante su aceptación, mitigación, transferencia o eliminación (CSAE, 2012).

Es fundamental la documentación y comunicación del proceso, asegurando que los resultados sean compartidos con las partes interesadas para finalmente, establecer un

sistema de monitoreo y revisión, que permite realizar un seguimiento continuo de los riesgos y adaptar el análisis a cambios en el entorno o en los activos (CSAE, 2012).

2.4.3. Aplicación de MAGERIT en la ciberseguridad

Esta metodología ofrece beneficios para las empresas ya que su adaptabilidad la hace especialmente relevante permitiendo una identificación exhaustiva de activos, amenazas y vulnerabilidades (Fernandez & Garcia, 2016). Entre sus ventajas se encuentran la fundamentación sencilla de decisiones, permitir la valoración de información o servicios para su protección y el conocer los riesgos para su posterior gestión (Ferruzola Gómez et al., 2019). Además, el uso de herramientas como PILAR (desarrollado por el Centro Criptológico Nacional) que realizan el papel de fuente fiable basada en marcos internacionales facilita su aplicación en las organizaciones (Vega et al., 2017). Mientras que su principal desventaja es el costo de la traducción de las valoraciones a valores económicos y no tiene un inventario completo de Políticas (Mogollón, 2016).

3. METODOLOGÍA

3.1. Justificación de las metodologías objeto de estudio

La elección de estas metodologías se debe a la relevancia de ambas en un análisis comparativo. En el contexto hispanohablante MAGERIT tiene una relevancia directa por el idioma (Crespo-Martínez & Cordero-Torres, 2018). Por otro lado, COBIT es un estándar internacional ampliamente reconocido y utilizado tanto en países hispanohablantes como anglosajones (Ridley et al., 2004). La comparación de ambas metodologías ofrece una perspectiva tanto local como global. También debemos tener en cuenta la complementariedad de los enfoques de las metodologías, ya que, aunque tienen diferentes alcances, son complementarios en muchos aspectos. COBIT proporciona un marco integral para el gobierno y la gestión de TI (ISACA, 2012), mientras que MAGERIT se especializa en el análisis y gestión de riesgos de seguridad de la información (CSAE, 2012).

3.2. Metodología de revisión

Para la realización de este trabajo se ha elegido la metodología PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) que se ha convertido en un estándar habitual para la realización de revisiones sistemáticas y

metaanálisis en diversos campos (Moher et al., 2009). Se puede considerar esta revisión como una investigación secundaria ya que se basa sobre lo ya investigado a partir de estudios originales primarios sobre la misma temática (Ferreira González et al., 2011). Además utilizaremos el software VOSviewer para obtener las redes empleadas en el análisis (van Eck & Waltman, 2017) y CitNetExplorer para el gráfico de la evolución de autores (van Eck & Waltman, 2014).

3.3. Búsqueda

La búsqueda sistemática tuvo lugar en agosto de 2024 en diferentes bases de datos como Scopus, Dialnet y Web of Science, utilizando los términos “COBIT”, “MAGERIT” Y “CIBERSECUTIRY AUDIT”. Se optó por la base de datos Web of Science con la siguiente combinación de términos: “(TS= ("MAGERIT" OR "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información")) OR TS= (("COBIT" OR "Control Objectives for Information and Related Technology") AND ("cybersecurity" OR "IT audit"))” y se obtuvieron 61 resultados a los cuales se los aplico los siguientes criterios de inclusión y exclusión:

Criterios de Inclusión

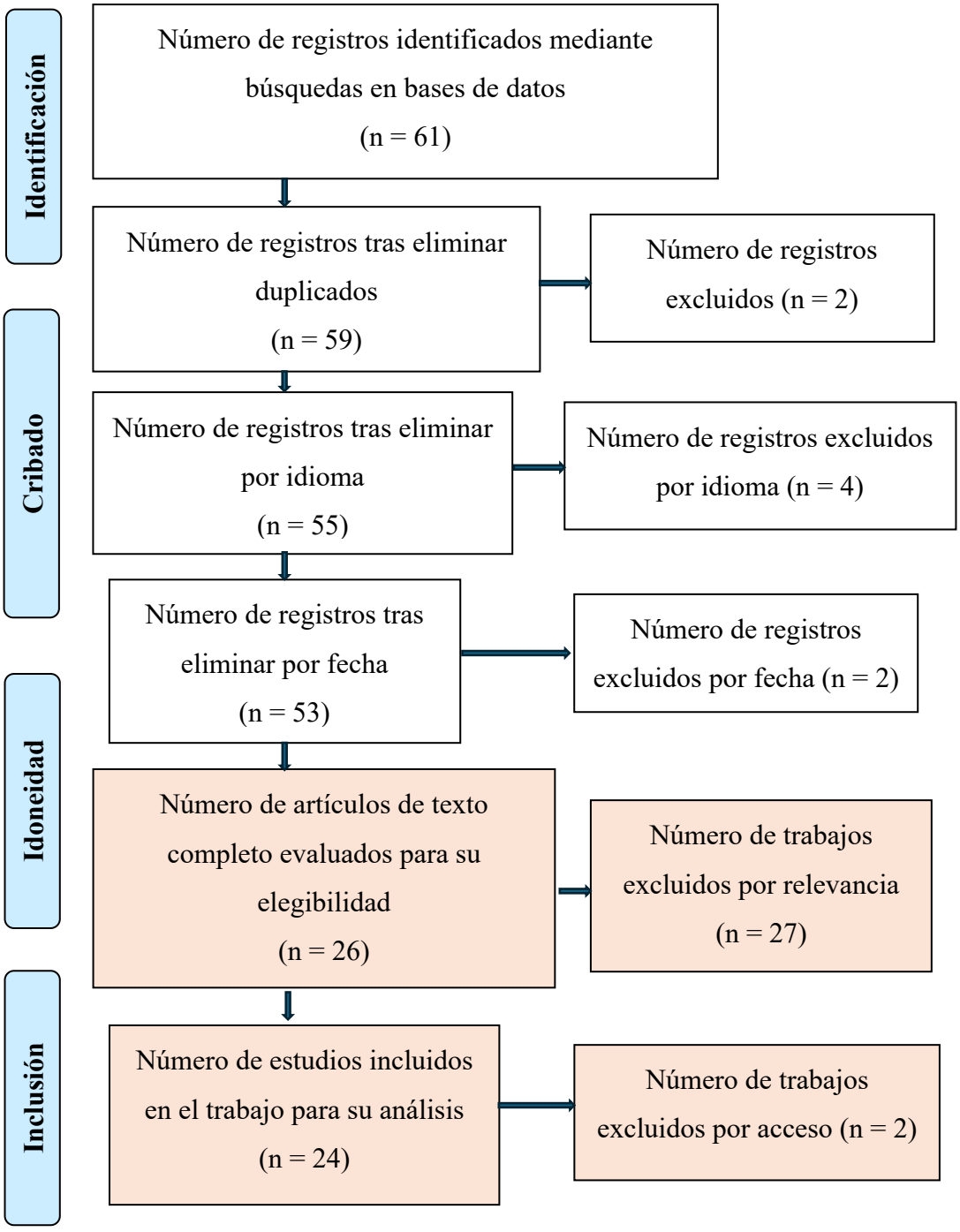
- El artículo debe estar en inglés o español.
- El artículo debe haber sido publicado en los últimos 20 años.
- El artículo debe ser relevante para la comparación entre COBIT y MAGERIT en el contexto de la auditoría de ciberseguridad.
- El artículo debe ser de acceso abierto para poder tener acceso a la información y no estar duplicado.

Criterios de Exclusión

- Excluir artículos duplicados.
- Excluir artículos en idiomas diferentes al inglés y español.
- Excluir artículos de una antigüedad mayor a 20 años.
- Excluir artículos que no sean relevantes para la comparación entre COBIT y MAGERIT en el contexto de la auditoría de ciberseguridad.
- Excluir artículos con acceso no abierto al texto completo o duplicados.

Siguiendo los criterios mencionados y como se explica en el flujograma de la Figura 1 se realizó un cribado sobre la literatura encontrada para poder responder a la pregunta de investigación planteada.

Figura 1. *Flujograma de información a través de las diferentes fases de la revisión sistemática*

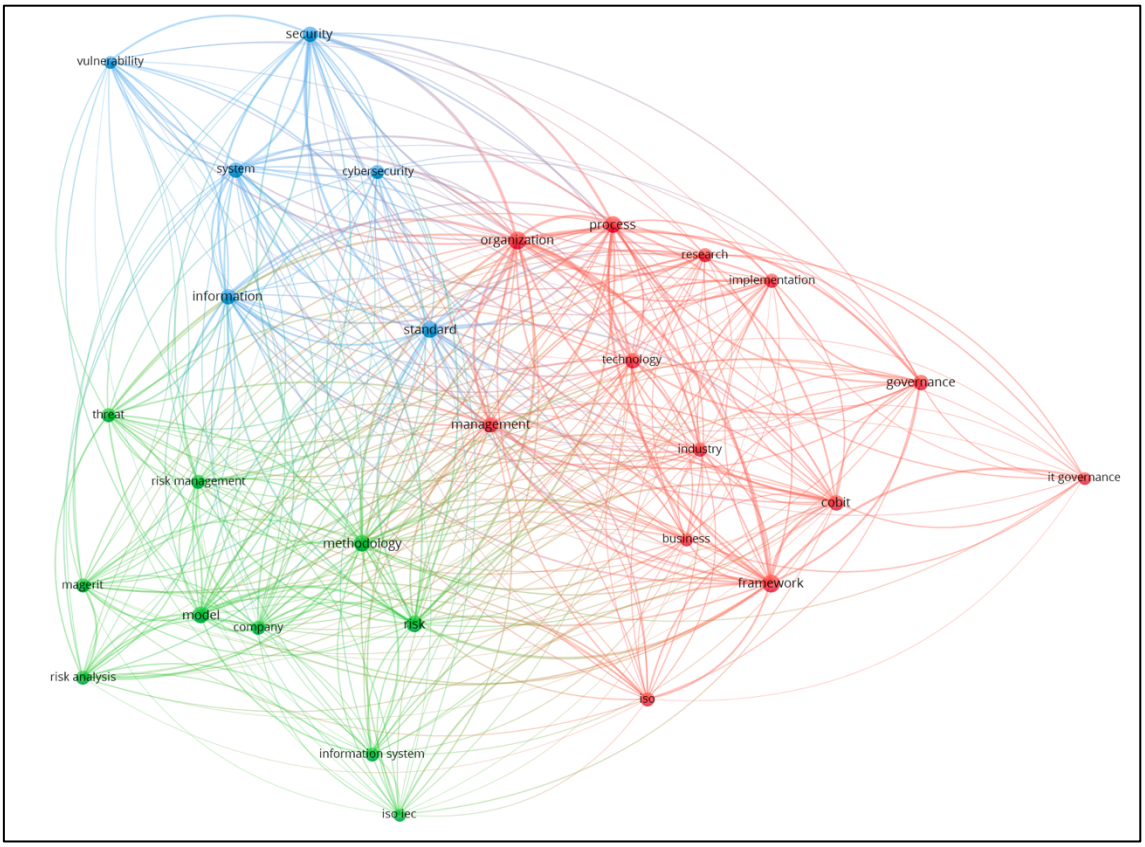


Fuente: elaboración propia.

4. RESULTADOS

4.1.1. Red de palabras claves del primer cribado

Figura 2. *Red de palabras clave del primer cribado*



Fuente: Análisis de Datos Web of Science en VOSviewer.

Para realizar un análisis de la literatura en profundidad se creó una red de palabras claves en VOSviewer (Figura 2) para observar cuales son los términos que destacan después de hacer una criba con la fecha, el idioma y los trabajos duplicados. El primer grupo, que es de color verde, se centra en la gestión y análisis de riesgos, con un enfoque particular en la metodología MAGERIT. Las palabras clave en este grupo sugieren un enfoque en los aspectos prácticos y metodológicos de la identificación, evaluación y gestión de riesgos en sistemas de información. La presencia de "MAGERIT" indica un énfasis específico en esta metodología de análisis de riesgos. Este grupo parece representar el núcleo técnico y metodológico del análisis de riesgos, abarcando desde la identificación de amenazas y vulnerabilidades hasta el diseño de modelos y métodos para gestionarlos reflejando la literatura que se centra en los procesos detallados y las herramientas utilizadas en la gestión de riesgos de TI.

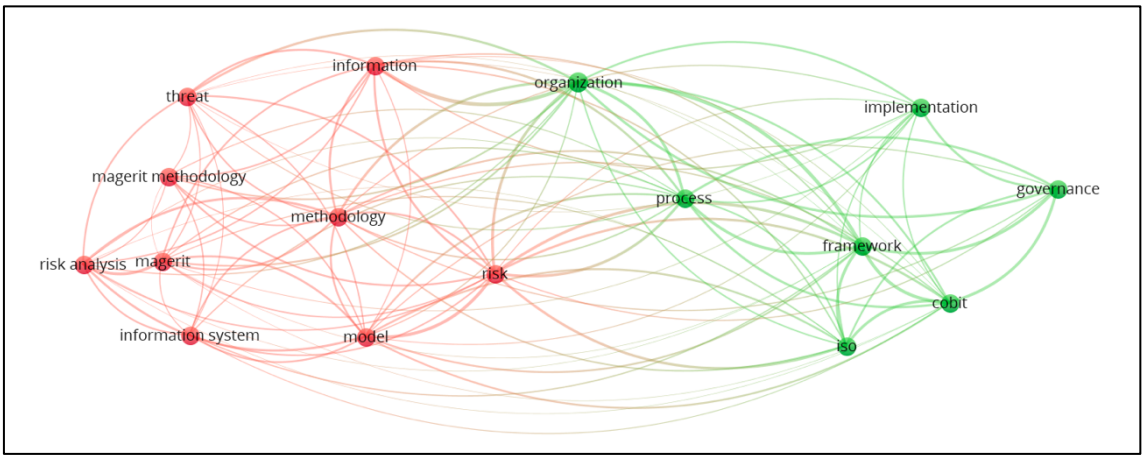
El segundo grupo, de color rojo, se enfoca más en los marcos de gobernanza y los estándares estudiados, con un énfasis particular en COBIT e ISO. Las palabras clave en este grupo sugieren un enfoque en la implementación de marcos de gobierno de TI a nivel organizacional y empresarial. La presencia de "COBIT", "governance" e "ISO" indica un fuerte énfasis en los estándares y mejores prácticas reconocidos internacionalmente. Representa la perspectiva más amplia de la gobernanza de TI y ciberseguridad, abordando cómo estas prácticas se integran en los procesos de negocio y la estrategia organizacional. Este grupo refleja la literatura que discute la implementación de marcos de gobernanza, su impacto en los negocios y los resultados de estos enfoques.

El último grupo es el azul, aunque más pequeño, parece centrarse en aspectos generales de la seguridad de los sistemas de información en un contexto organizacional. La presencia de "security" como término central sugiere que este grupo aborda los principios fundamentales de la seguridad de la información. Este grupo podría representar la intersección entre los aspectos técnicos de la seguridad (grupo verde) y los aspectos de gobernanza (grupo rojo), enfocándose en cómo la seguridad se implementa y gestiona dentro de los sistemas y procesos organizacionales.

La red de palabras clave muestra a priori una división entre los aspectos metodológicos del análisis de riesgos (grupo verde, centrado en MAGERIT) y los aspectos de gobernanza y estándares (grupo rojo, centrado en COBIT e ISO). El grupo azul parece actuar como un puente entre estos dos enfoques, centrándose en la implementación práctica de la seguridad en los sistemas organizacionales. A pesar de que ambas metodologías parecen cubrir aspectos distintos de la ciberseguridad, ambas están presentes en la literatura de manera significativa, siendo la contribución de ambas relevante a la vez que complementaria ya que se abarcan aspectos fundamentales en lo relacionado a la realización de una auditoría de ciberseguridad.

4.1.2. Red de palabras tras el cribado final

Figura 3. *Red de palabras clave del cribado final*



Fuente: Análisis de Datos Web of Science en VOSviewer

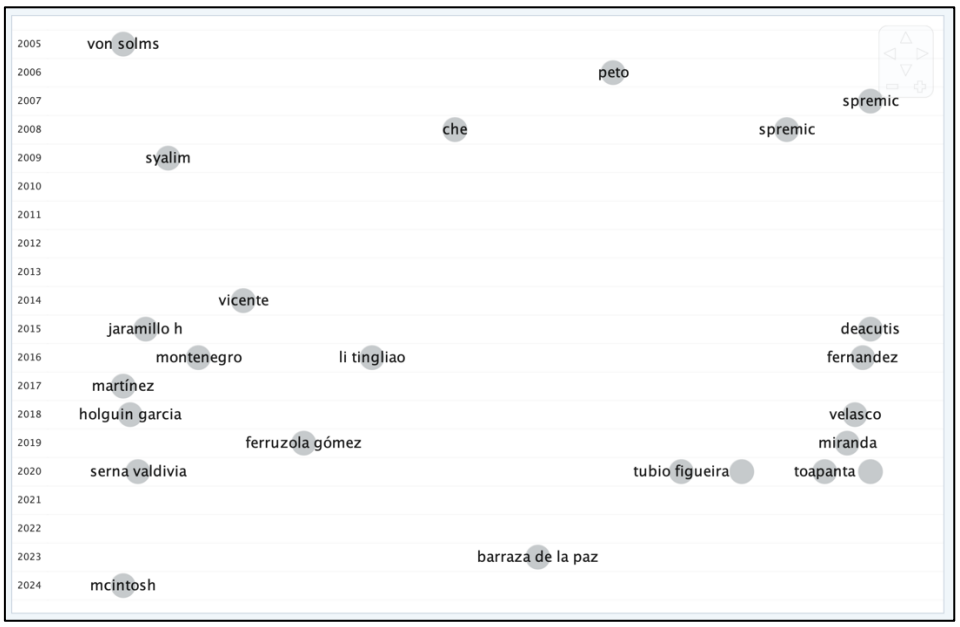
El análisis de la red de palabras clave en los trabajos seleccionados tras la criba final (Figura 3) revela dos ejes principales en la investigación. Por un lado, se observa un fuerte énfasis en los marcos de trabajo y gobernanza de los sistemas de información. Términos como "governance", "framework" y "COBIT", en el grupo verde, indican una preocupación por establecer estructuras y estándares para gestionar la tecnología de la información de manera efectiva. Por otro lado, la red destaca la importancia de la gestión de riesgos en el grupo rojo, con términos como "risk", "methodology" y "MAGERIT" ocupando un lugar central. A pesar de que las metodologías objeto de estudio se encuentran en lado opuestos del gráfico, indicando que tienen claras diferencias y orientaciones en la literatura encontrada, comparten los términos "organization", "process" y "risk" en común siendo esto una clara indicación de que ambas metodologías son utilizadas activamente en las organizaciones para procesar riesgos de ciberseguridad.

La conexión entre estos dos ejes es evidente, ya que los marcos de gobernanza suelen incluir componentes para la gestión de riesgos. En conjunto, los resultados del análisis indican que la literatura encontrada se centra en la intersección entre la gobernanza de TI y la gestión de riesgos, con un enfoque particular en la implementación de marcos y metodologías para garantizar la seguridad y eficacia de los sistemas de información ya que en los trabajos seleccionados además de utilizar los marcos seleccionados (COBIT y MAGERIT) se utilizan otros marcos adicionales para complementar o compararlos entre ellos.

Por lo tanto, podemos afirmar que los trabajos elegidos para analizar nos pueden dar una visión clara sobre como COBIT y MAGERIT son implementados en las organizaciones y cuáles son sus puntos fuertes y débiles.

4.1.3. Red de autores

Figura 4. *Red de autores*



Fuente: Análisis de Datos Web of Science en CitNetExplorer

En la Figura 4 se puede observar como a lo largo de los años han ido aumentando el número de autores presentes en la literatura encontrada, aumentando considerablemente en los últimos años y poniendo en relieve el aumento de la relevancia, evolución y expansión del tema analizado. Además, también se puede observar que algunos autores aparecen en múltiples años (por ejemplo, "spremic" en 2007 y 2008), lo que podría sugerir una producción continua o impacto duradero en el campo. El autor más citado actualmente es Basie von Solms, siendo también el más antiguo, pudiendo implicar esto que las bases de la literatura encontrada son sólidas y se mantienen vigentes. Así mismo, es interesante tener en cuenta la aparición constante de nuevos autores que sugiere una renovación continua de la comunidad investigadora en el área.

4.1.4. Análisis tras el cribado final

Tabla 1. *Resumen de los resultados de las investigaciones seleccionadas*

Autor	Título	Fuente/Revista	Metodología	Resultado
Basie von Solms (2005)	Information Security Governance using ISO 17799 and COBIT	Computers & Security	Enfoque comparativo y analítico	COBIT e ISO 17799 son complementarias y al usarse juntas mejoran la gobernanza de la seguridad de la información, lo que permite gestionar mejor los riesgos y adaptar las prácticas de seguridad a las necesidades de cada organización. Se recomienda evaluar el contexto particular para decidir la implementación de una o ambas metodologías.
David Peto (2006)	Generalized risk assessment index for information systems auditing	ITI 2006: proceedings of the 28th international conference on information technology interfaces	Creación de un índice numérico de medición de riesgos	El estudio concluye que COBIT permite identificar los riesgos primarios y las interacciones críticas entre ellos, lo que facilita una evaluación más completa de los riesgos en las organizaciones. Esto ayuda a mejorar la toma de decisiones en la gestión de la seguridad de la información y a optimizar la asignación de recursos para mitigar riesgos.
Mario Spremic y Matua Popovic (2007)	Towards a corporative IT risk management	Proceedings of the 6th WSEAS international conference on information security and privacy	Desarrollo de un modelo y análisis de casos prácticos	Un enfoque COBIT, estructurado y holístico, para la gestión de riesgos de TI es esencial para alinear los recursos de TI con los objetivos empresariales. El modelo propuesto ayuda a identificar, evaluar y mitigar los riesgos asociados con el uso de TI, mejorando la seguridad y eficiencia operativa. Se destaca la importancia de la gobernanza de TI y la auditoría como componentes clave en la gestión de riesgos.

Peirong Che, Zhaokun Bu, Rui Hou y Xinxing Shi (2008)	Auditing revenue assurance information systems for telecom operators	Research and practical issues of enterprise information systems ii, vol 2	Investigación cualitativa basada en el análisis documental y la experiencia práctica	Destaca la importancia de un marco de auditoría robusto que integre COSO y COBIT para las organizaciones (en este caso operadores de telecomunicaciones).
Mario Spremic, Zlatan Zmirak, Krunoslav Kraljevic (2008)	IT Governance and performance measurement: Research study on Croatian companies	Sepads 08: proceedings of the 7th WSEAS international conference on software engineering, parallel and distributed systems	Investigación cuantitativa descriptiva mediante encuesta	Las empresas croatas subestiman la importancia de la planificación y la inversión en TI. Además, se observa que no cuentan con métricas para evaluar la influencia de TI en la productividad. Esto indica una falta de compromiso con la auditoría de TI y la medición del rendimiento, lo que limita la capacidad de las empresas para aprovechar al máximo sus recursos tecnológicos.
Amril Syalim, Yoshiahi Hori, Kouichi Sakurai (2009)	Comparison of Risk Analysis METHODS: MEHARI, MAGERIT, NIST800-30 and Microsoft´s Security Management Guide	2009 International conference on availability, reliability, and security	Investigación comparativa basada en el análisis documental	Tras la comparación de metodologías se observa que los métodos siguen los primeros pasos generales del análisis de riesgos, pero solo NIST800-30 incluye recomendaciones de control dentro de sus pasos de análisis de riesgos. Además, Mehari, MAGERIT y la Guía de Microsoft proporcionan documentos suplementarios que pueden ayudar en el proceso de evaluación de riesgos, mientras que NIST800-30 no. Esto sugiere que la disponibilidad de recursos adicionales puede mejorar la efectividad de los métodos de análisis de riesgos.
E. Vicente, A. Mateos, A. Jiménez-Martín (2014)	Risk analysis in information systems: A fuzzification of the MAGERIT methodology	Knowledge-Based systems	Investigación basada en la fuzzificación	La metodología propuesta (basada en MAGERIT) mejora la evaluación de riesgos al permitir una representación más precisa de la incertidumbre. Se demuestra su aplicación a través de un caso de estudio, donde se optimizan los costos de las salvaguardias y se

				reduce la dependencia de ciertos activos, lo que lleva a una gestión de riesgos más efectiva en sistemas de información.
Marian Deacutis (2015)	The cloud and security governance	Utica college	Investigación basada en el análisis de marcos de gobernanza y estudios de caso	La implementación de marcos de gobernanza adecuados es esencial para gestionar la seguridad en la nube, ayudando a las organizaciones a cumplir con regulaciones y estándares. Además, resalta la importancia de la colaboración entre proveedores de servicios en la nube y clientes para asegurar la protección de datos. La adopción de marcos como ISGcloud y COBIT 5 es clave para mitigar riesgos y mejorar la gestión de la seguridad.
Danilo Jaramillo, Armando Cabrera, Marco Abad, Alfredo Torres y Jose Carrillo Verdum (2015)	Definition of Cybersecurity Businness Framework Based on ADM-TOGAF	2015 10th iberian conference on information systems and technologies	Investigación basada en análisis de marcos de referencia e integración de metodologías existentes	El trabajo propone un marco estructurado para la implementación de ciberseguridad en empresas, destacando la importancia de la integración de metodologías y la evaluación continua de su efectividad. Además, destaca que COBIT complementa las fases del marco, el cual es flexible, y así mejora la postura de seguridad de las organizaciones.
Adrián Fernandez y Daniel F. García (2016)	Complex vs. Simple Asset Modeling Approaches for Information Security Risk Assessment Evaluation with MAGERIT methodology	2016 Sixth international conference on innovative computing technology	Investigación aplicada comparative cualitativa	Los modelos de activos simples son más eficientes que los complejos para la evaluación del riesgo. MAGERIT es flexible y se adapta a ambos sin sacrificar la precisión en la evaluación del riesgo para los activos principales del negocio. Los modelos simples, aunque más rápidos de desarrollar, no afectan la precisión del análisis de riesgo para los activos principales, lo que hace de MAGERIT una herramienta útil para empresas que buscan un equilibrio entre precisión y eficiencia.

Diana Moncayo y Carlos Montenegro (2016)	Information security risk in SMEs: A hybrid model compatible with IFRS evaluation in two Ecuadorian SMEs of automotive sector	Proceedings of the 6th international conference on information communication and management	Investigación de la ciencia del diseño (Design science research)	El estudio implementa MAGERIT entre otros marcos para crear un modelo híbrido de evaluación de riesgos de seguridad en PYMES, demostrando su flexibilidad y eficiencia. El modelo, que combina métodos cualitativos y cuantitativos, es práctico y adaptable a equipos multidisciplinarios. Los resultados muestran que MAGERIT es efectivo para evaluar riesgos en PYMES, incluso al considerar la complejidad del modelo de activos.
Tingliao Li (2016)	The Audit research based on the information system success model and COBIT	Proceedings of the 10th international conference on intelligent systems and control	Investigación basada en el análisis y evaluación de la literatura con una propuesta de diseño	El trabajo propone un enfoque sistemático para la auditoría de sistemas de información que integra el modelo D&M y COBIT, facilitando una evaluación integral y alineada con las necesidades empresariales. Aunque no se centra en un análisis profundo de COBIT, demuestra que este marco es una herramienta útil para el desarrollo de un modelo de auditoría integral y alineado con los objetivos del negocio.
Esteban Crespo Martínez (2017)	ECU@Risk, a methodology for risk management applied to MSMEs	Enfoque UTE	Investigación cualitativa basada en un estudio de caso y análisis comparativo	El estudio evidencia que las PYMES ecuatorianas carecen de sistemas formales para gestionar el riesgo de información, por lo que se propone ECU@Risk, una nueva metodología inspirada en COBIT y MAGERIT, entre otros, que se adapta a la realidad local y considera las mejores prácticas, lo que la convierte en una herramienta útil incorporando aspectos clave como la identificación del contexto organizacional, la evaluación de las actividades de control y el establecimiento de contramedidas

Fresia Yanina Holguin Garcia, Lohana Mariella Lema Moreta (2018)	Maturity Model for the Risk Analysis of Information Assets based on Methodologies MAGERIT, OCTAVE y MEHARI; focused on Shipping Companies	2018 7th International conference on software process improvement	Investigación cualitativa, basada en la revisión de literatura y el desarrollo de un modelo conceptual	Propuesta de un Modelo de Madurez para el Análisis de Riesgos de los Activos de Información en Empresas Navieras, fundamentado en las mejores prácticas de las metodologías MGERIT, Octave y Mehari. MAGERIT juega un papel fundamental, ya que proporciona un enfoque estructurado para la identificación, análisis y gestión de riesgos, priorizando la autenticidad, confidencialidad, integridad y trazabilidad de la información.
Joffre Velasco, Rodrigo Ullauri, Luis Pilicita, Bolivar Jacome, Pablo Saa, Oswaldo Moscoso-Zea (2018)	Benefits of Implementing ISMS according to the ISO 27001 Standard in the Ecuadorian Manufacturing Industry	Proceedings 3rd international conference on information systems and computer science	Investigación cualitativa basada en la revisión de la literatura	La investigación propone implementar un ISMS basado en la norma ISO 27001 en la industria manufacturera ecuatoriana, destacando sus beneficios para la seguridad de la información, gestión de riesgos y optimización de procesos. Utiliza MAGERIT para analizar los riesgos de los activos de información y demuestra que es efectiva en la evaluación y mitigación de riesgos, priorizando la autenticidad, confidencialidad, integridad y trazabilidad de la información. Se concluye que la combinación de ambos mejora la seguridad y el rendimiento de los procesos en las empresas de este sector.
Noreen B. Miranda, Maria Rosario D. Rodavia, Mir-mel I. Miranda (2019)	IT infrastructure auditing using COBIT	2019 6th International conference on technical education and 11th national conference on technical education	Investigación cualitativa basada en la revisión de la literatura	El estudio, realizado en la NLAC, utilizó COBIT 4.1 para evaluar la infraestructura de TI lo que reveló que la institución no cuenta con una política escrita de seguridad, lo que representa un riesgo. COBIT proporciona un marco de trabajo estructural para la evaluación de la infraestructura de TI, lo que permite identificar las deficiencias en la gestión de la información y proponer recomendaciones para mejorar la seguridad de los recursos de la institución.

Enrique Ferruzola Gómez, Johanna Duchimaza S., Johanna Ramos Holguín, María Fernanda Alejandro L. (2019)	Plan de contingencia para los equipos y sistemas informáticos utilizando la metodología MAGERIT	Revista Científica y Tecnológica UPSE	Investigación aplicada	MAGERIT es fundamental en la elaboración de planes de contingencia para sistemas informáticos, garantizando la seguridad de los datos. Esto es útil para empresas que comienzan a gestionar la seguridad de la información, ya que permite analizar el impacto de posibles amenazas y desarrollar medidas preventivas y correctivas. Al aplicarse a través de software, ayuda a identificar procesos críticos en las organizaciones y establecer las acciones necesarias para mejorar y asegurar la seguridad, confidencialidad, integridad y disponibilidad de la información
Einar Jhordany Serna Valdivia y Jezreel Mejia Miranda (2020)	Proposal of an intelligent agent for management and mitigation in cybersecurity risk for IoT environments	2020 9th International conference on software process improvement	Investigación aplicada	Se identificó la necesidad de utilizar normas y estándares, como ISO/IEC 27001 y el framework COBIT, para abordar la seguridad en el creciente entorno del IoT, especialmente en áreas críticas como el IoT industrial y el cuidado médico. Se busca preparar a las organizaciones para futuras amenazas de seguridad. La combinación de COBIT e ISO/IEC 27001 permite identificar errores de seguridad, fugas de información y comportamiento de los usuarios, lo que facilita la creación de políticas de seguridad efectivas.
Segundo Moises Toapanta Toapanta, Yaritza Julieth Teran Terranova, Bertha Alice Naranjo Sanchez, Luis Enrique Mafla Gallegos (2020)	Security and Privacy in Information Management in a Distributed Environment for Public Organizations	Fuzzy systems and data mining vi	Investigación deductiva y exploratoria	El estudio proporciona un marco para mejorar la seguridad y privacidad de la información en el contexto de organizaciones públicas, destacando la importancia de la gestión de riesgos. Se concluye que MAGERIT es una alternativa eficaz para mitigar vulnerabilidades, amenazas y riesgos en los procesos de organizaciones públicas. Además, el prototipo de gestión de riesgos y la fórmula para evaluar la probabilidad de amenazas y

				riesgos presentados son alternativas que mejoran la seguridad y privacidad de la información.
George Morris William Tangka, Andrew Tanny Liem y Joe Yuan Mambu (2020)	Information Technology Governance Audit Using the COBIT 5 Framework at XYZ University	Proceedings of icoris 2020: 2020 the 2nd international conference on cybernetics and intelligent system	Investigación descriptiva	La evaluación de la gobernanza de TI en la Universidad XYZ, realizada bajo el marco COBIT 5.0 sugiere que los procesos de TI no están completamente implementados ni gestionados de manera eficiente. Se recomienda que la universidad implemente evaluaciones continuas para elevar el nivel de capacidad de todos los dominios, con especial atención en aquellos que están más rezagados, utilizando el marco COBIT 5.0 como guía para estas mejoras.
Pedro Tubío Figueira, Cristina López Bravo, José Luis Rivas López (2020)	Improving information security risk analysis by including threat-occurrence predictive models	Computers & security	Investigación aplicada con enfoques cualitativos y cuantitativos	Se propone un modelo predictivo alternativo para el análisis de riesgos basándose en MAGERIT, modificando el cálculo de riesgos, sustituyendo las frecuencias de amenazas históricas por probabilidades de amenazas futuras, considerando las vulnerabilidades actuales del sistema. Se valido a través de un estudio de caso y se observó que los riesgos calculados reflejan mejor el estado de las vulnerabilidades, permitiendo a las organizaciones enfocarse en amenazas más probables.
Masike Malatji, Annlizé Marnewicka, Suné von Solms (2020)	Validation of a socio-technical management process for optimizing cybersecurity practices	Computers & security	Proceso de validación teórica	Se destaca la importancia de un enfoque sociotécnico para la gestión de la ciberseguridad. Los resultados demuestran que COBIT 5, a pesar de ser un marco de seguridad reconocido, puede ser mejorado al incorporar las dimensiones sociales, técnicas y ambientales, así como un modelo de madurez de las capacidades. Esto

				permitiría a las organizaciones medir y mejorar continuamente su desempeño de seguridad.
Juan Vicente Barraza de la Paz, Luis Alberto Rodríguez-Picón, Víctor Morales-Rocha y Soledad Vianey Torres-Argüelles (2023)	A Systematic Review of Risk Management Methodologies for Complex Organizations in Industry 4.0 and 5.0	Systems	Investigación de revisión sistemática	Se realizó una comparación de las características y enfoques de los marcos NIST CSF, ISO/IEC 27001:2022 y MAGERIT debido a la relevancia de la ciberseguridad en el IoT. MAGERIT destaca en la evaluación y gestión de riesgos a nivel organizacional y puede aplicarse a diferentes organizaciones.
Timothy R. McIntosha, Teo Susnjakb, Tong Liub, Paul Watterscc, Raza Nowrozyd, Malka N. Halgamuge (2024)	From COBIT to ISO 42001: Evaluating Cybersecurity Frameworks for Opportunities, Risks, and Regulatory Compliance in Commercializing Large Language Models	Computers & Security	Investigación cualitativa	Se evaluaron cuatro marcos de ciberseguridad: NIST CSF 2.0, COBIT 2019, ISO 27001:2022 y ISO 42001:2023, en relación con su preparación para la adopción de Modelos de Lenguaje Grande (LLMs). Se mostró que el ISO 42001:2023 es el más adecuado para facilitar oportunidades de LLM, mientras que COBIT 2019 se alinea mejor con la próxima Ley de IA de la Unión Europea.

Fuente: Elaboración propia.

En este análisis en detalle de los trabajos (Tabla 1) se observa que de los 24 trabajos analizados 12 hablan de COBIT, 10 de MAGERIT, uno de ambos y otro a pesar de no centrarse directamente en ninguna sí que trata temas relevantes para la ciberseguridad, razón por la cual se ha mantenido el trabajo para el análisis.

En el caso de COBIT se resalta su efectividad para alinear el TI con los objetivos empresariales, subrayando su importancia en la gobernanza de TI y la auditoría, y destacando que su enfoque estructurado y holístico es clave para una gestión eficaz de riesgos (Spremic & Popovic, 2007). Así mismo, se menciona su utilidad para detectar riesgos primarios y las interacciones críticas entre ellos, facilitando una evaluación completa de los riesgos, mejorando la toma de decisiones y optimizando la asignación de recursos (Peto, 2006). También se emplea COBIT para evaluar la infraestructura de TI en una institución educativa, identificando deficiencias en la gestión de la información y señalando la falta de políticas de seguridad escritas, utilizando COBIT para destacar las áreas que necesitan mejoras (Miranda et al., 2019) y se sugiere en otro caso concreto de estudio la implementación de COBIT como marco idóneo para la mejora de ciberseguridad (Tangka et al., 2020). Es destacable la relevancia de este marco comparándolo con otros marcos vigentes y destacando que es el más óptimo en cuanto a alineamiento a la Ley IA de la UE (McIntosh et al., 2024) y también se recalca su flexibilidad (Jaramillo et al., 2015).

Se utiliza COBIT, en combinación con el modelo D&M, para realizar una auditoría integral de sistemas de información, presentando a COBIT como una herramienta útil para asegurar que las auditorías de ciberseguridad estén alineadas con las necesidades empresariales (Tingliao, 2016). Otros autores analizan cómo COBIT, junto a otros marcos como ISO 17799, ISO/IEC 27001, COSO e ISGcloud puede mejorar la gobernanza de la seguridad de la información, destacando que la combinación de estos marcos mejora la gestión de riesgos y adapta las prácticas de seguridad a las necesidades organizacionales (Che et al., 2008; Deacutis, 2015; Serna Valdivia & Mejía Miranda, 2020; Von Solms, 2005). También encontramos autores que resaltan la necesidad de mejora incluyendo aspectos sociales, técnicos y ambientales (Malatji et al., 2020).

Con respecto a MAGERIT, los autores realizaron un estudio comparativo donde destacaron que ofrece documentación complementaria valiosa para el proceso de evaluación de riesgos (Syalim et al., 2009) y también desarrollaron una versión mejorada basada en MAGERIT incorporando técnicas de lógica difusa para una representación más

precisa de la incertidumbre en la evaluación de riesgos (Vicente et al., 2014), recalcando esto el margen de mejora de este marco. Así mismo, destaca la flexibilidad y adaptabilidad de MAGERIT mientras conserva su precisión convirtiéndose en una herramienta útil para empresas que necesitan un equilibrio entre precisión y eficiencia (Fernandez & Garcia, 2016).

Se encuentran trabajos que demostraron la eficacia de MAGERIT en el contexto de las PYMES, integrándola en un modelo híbrido de evaluación de riesgos (Moncayo & Montenegro, 2016) y se profundizó en esta dirección, creando un modelo de madurez para el análisis de riesgos que incorpora elementos clave de MAGERIT, destacando su enfoque estructurado para la gestión de riesgos (García & Moreta, 2018).

La aplicabilidad de MAGERIT en sectores específicos fue explorada y se utilizó para analizar riesgos en la industria manufacturera ecuatoriana, confirmando su efectividad (Velasco et al., 2018). También, extendieron el uso de MAGERIT a la elaboración de planes de contingencia para sistemas informáticos, subrayando su importancia fundamental en la garantía de la seguridad de datos (Ferruzola Gómez et al., 2019). Así mismo, se demuestra que MAGERIT destaca como una alternativa eficaz para mitigar vulnerabilidades, amenazas y riesgos en las organizaciones públicas (Toapanta Toapanta et al., 2020) mientras que otros autores propusieron una innovación significativa al modelo de MAGERIT, introduciendo un enfoque predictivo que sustituye las frecuencias históricas de amenazas por probabilidades futuras, mejorando así la precisión del análisis de riesgos (Tubío Figueira et al., 2020). También un estudio reciente realizó una comparación exhaustiva de marcos de gestión de riesgos, donde MAGERIT destacó por su excelencia en la evaluación y gestión de riesgos a nivel organizacional, así como por su versatilidad para adaptarse a diferentes tipos de organizaciones (Barraza De La Paz et al., 2023).

Finalmente, encontramos un trabajo en el que combina las dos metodologías objeto de estudio, además de otros marcos, de manera exitosa creando un sistema formal de gestión de riesgo para PYMES (Crespo Martínez, 2017) demostrando así su compatibilidad. También se encuentran trabajos que mencionan que existen zonas geográficas en las que para las organizaciones no es relevante la planificación e inversión en TI lo que demuestra su falta de compromiso con la auditoría de TI, limitando así el aprovechamiento de recursos (Spremic et al., 2008). Sin embargo, esto implica también

que existe un margen de mejora e implementación aún no explorado para los marcos objeto de estudio, abriendo puertas a futuras líneas de investigación. Tras analizar en profundidad los trabajos, se puede concluir que COBIT es el marco más utilizado basándonos en la cantidad de trabajos encontrados que lo analizan y lo consideran una metodología optima y adaptable a otros marcos. Sin embargo, MAGERIT es el marco que más estudios tiene en el que se prueba su eficiencia de manera individual lo cual demuestra que es un marco útil, relevante y práctico, sobre todo en los países de habla hispana, ya que la mayoría de los estudios se realizaron en zonas con esta característica.

5. INTELIGENCIA ARTIFICIAL

En el presente trabajo se estudia los avances tecnológicos implementados como un riesgo para la seguridad de las empresas, sin embargo, también se puede ampliar esta visión y plantear como los avances tecnológicos pueden ser una herramienta útil en el campo de la ciberseguridad.

La inteligencia artificial (IA) desempeña un papel fundamental en la ciberseguridad, al mejorar la detección y respuesta a amenazas, permitiendo a los profesionales gestionar la complejidad de los sistemas modernos y analizar grandes volúmenes de datos para identificar comportamientos anómalos (Ayerbe, 2020). Sin embargo, la IA también plantea riesgos, ya que puede ser utilizada por cibercriminales para realizar ataques o generar desinformación y además, su uso puede conllevar decisiones erróneas y falta de transparencia, lo que subraya la importancia de desarrollar sistemas de IA seguros, que protejan la privacidad y sean confiables (Cordova-Alvarado et al., 2024). Para enfrentar estos desafíos, es esencial coordinar las estrategias de ciberseguridad, IA e I+D, integrando la seguridad en el diseño y desarrollo de sistemas basados en IA además de plantear una investigación en inteligencia de ciberamenazas es clave para reducir la intervención manual en los análisis y mejorar la capacidad de respuesta ante ciberataques (Ayerbe, 2020).

6. LIMITACIONES

Una limitación encontrada para este trabajo es la poca literatura disponible comparando ambos marcos, probablemente debido a sus enfoques distintos sobre ciberseguridad, pero esto pone en relieve la relevancia de empezar nuevas líneas de investigación en las que sería interesante el analizar diferentes metodologías aplicadas a

empresas para obtener unos marcos que combinados o de manera individual proporcionen una seguridad informática eficaz a las empresas. Otra limitación fue no encontrar literatura que ahondara más en aspectos específicos de cada metodología, como los procesos, las herramientas y la aplicación en diferentes contextos, esto hubiese permitido un mejor análisis de los aspectos concretos de cada metodología.

7. CONCLUSIONES

En conjunto, los estudios analizados indican que COBIT y MAGERIT ofrecen enfoques complementarios para la gestión de riesgos y la seguridad de la información. Mientras que COBIT se enfoca en la gobernanza y la alineación estratégica, MAGERIT proporciona un análisis detallado y adaptativo de los riesgos, lo que convierte a ambos marcos en herramientas esenciales para mejorar la seguridad y la eficiencia operativa en las organizaciones. Además, podemos observar que ambos marcos ofrecen una gran adaptabilidad a ser compatibles con otros marcos de ciberseguridad existentes, siendo esta característica un hallazgo interesante, ya que permite asegurar que no existe un único marco que aborde todos los problemas de seguridad de información o de TI en todas las empresas, en la literatura se haya una clara tendencia de mejora o unificación de marcos para tener una metodología más completa para cada empresa.

La revisión de la literatura aporta una visión más completa y clara sobre la utilidad y relevancia de seguir investigando sobre los marcos existentes y su adaptabilidad a cada organización para que de esta manera se genere cada vez un entorno más seguro y eficaz en el que las empresas puedan desarrollar su actividad de manera segura. Esto no influye solo en la seguridad de las empresas, influye también en el relevante impacto económico que supone el no tener que lidiar con las consecuencias negativas de ser víctimas de un ciberataque y prevenirlos antes de que sucedan. Este estudio también es importante para las organizaciones que se dedican a diseñar estos marcos ya que se pueden obtener ideas de mejora, ampliación de cada metodología y conocer que zonas geográficas aún no tienen implementadas sus metodologías, siendo para COBIT el hispanohablante y para MAGERIT el anglosajón. Es relevante recalcar que se ha comprobado que MAGERIT tiene ventaja en países hispanohablantes ya que la literatura encontrada pertenecía a esta zona principalmente mientras que COBIT al ser un marco internacional es reconocido de manera más homogénea. Se observa también la diversidad de organizaciones en las que se han empleado como marcos de ciberseguridad tanto COBIT como MAGERIT de

manera eficiente siendo esto una señal de su utilidad en el futuro a medida que se vayan implementando nuevos sectores empresariales.

Con lo comentado se puede concluir que COBIT es un marco que destaca por encima de MAGERIT ya que es un marco más estudiado, basándonos solo en la cantidad de trabajos encontrados de cada uno. Además, se debe tener en cuenta que es una metodología internacional lo que le permite adaptarse mejor a diferentes zonas geográficas, mientras que MAGERIT fue desarrollado originalmente para las organizaciones públicas españolas, lo que podría limitar su inclusión. Sin embargo, no se puede obviar que la diferencia hallada no es tajante debido a la poca diferencia entre los trabajos encontrados. Esto también es significativo porque permite dejar en claro que ambas metodologías son eficaces en su contribución a una auditoría de ciberseguridad óptima ya que los resultados obtenidos en el análisis pormenorizado indica que la combinación de distintos marcos es la manera más efectiva de poder obtener una metodología óptima que cubra todos los requisitos para poder obtener una auditoría de ciberseguridad óptima.

Como futuras líneas de investigación, se sugiere enfocarse en el análisis comparativo, en organizaciones de diversos sectores, de ambos marcos para poder observar si esto influye en como estas metodologías funcionan en empresas que utilizan herramientas de TI variadas o en distintos sectores empresariales. También, el ahondar en cómo se está llevando a cabo la implementación de las nuevas herramientas vigentes, como la inteligencia artificial, es de clara relevancia debido a que presenta una nueva y variada red de posibilidades que pueden permitir realizar auditorías de ciberseguridad más eficaces. Por último, el poder analizar cómo se implementan estos marcos en nuevas zonas, en los que no tenían relevancia, sería de gran importancia para así poner de manifiesto la importancia de la ciberseguridad y evaluar que herramientas son las adecuadas para nuevos entornos.

8. BIBLIOGRAFÍA

Adamyk, O., Benson, V., Adamyk, B., Al-Khateeb-Khateeb, H., & Chinnaswamy, A. (2023). Does Artificial Intelligence Help Reduce Audit Risks? *2023 13th International Conference on Advanced Computer Information Technologies (ACIT)*, 294-298. https://doi.org/10.1109/ACIT58437.2023.10275661

Almanza Gómez, Á. I. (2012). *La aplicación de COBIT en las organizaciones ¿vale la pena el esfuerzo?* http://hdl.handle.net/10654/6537

Anderson, R. (2020). *Security engineering: A guide to building dependable distributed systems* (3.ª ed.). John Wiley & Sons Inc. https://doi.org/10.1002/9781119644682

Ayerbe, A. (2020). La ciberseguridad y su relación con la inteligencia artificial. *Análisis del Real Instituto Elcano (ARI)*, *128*.

Barra Novoa, R. (2021). Nueva Economía en tiempos de crisis: Una aproximación teórica a la transformación tecnológica y social. *Journal Managment & Business Studies*, *3*(1), 1-13. https://doi.org/10.32457/jmabs.v3i1.1554

Barraza De La Paz, J. V., Rodríguez-Picón, L. A., Morales-Rocha, V., & Torres-Argüelles, S. V. (2023). A Systematic Review of Risk Management Methodologies for Complex Organizations in Industry 4.0 and 5.0. *Systems*, *11*(5), 218. https://doi.org/10.3390/systems11050218

Calder, A., & Watkins, S. (2015). *IT governance: An international guide to data security and ISO27001/ISO27002* (6.ª ed.). Kogan Page.

Candau, J. (2021). Ciberseguridad. Evolución y tendencias. *bie3 Boletín IEEE*, *23*, 460-494.

Che, P., Bu, Z., Hou, R., & Shi, X. (2008). Auditing Revenue Assurance Information Systems for Telecom Operators. En L. D. Xu, A. M. Tjoa, & S. S. Chaudhry (Eds.), *Research and Practical Issues of Enterprise Information Systems II* (Vol. 255, pp. 1597-1602). Springer US.

Coha Escalante, J. M., & Barraza Mármol, R. A. (2024). *La auditoría forense ante el fraude por corrupción en el sector público: Una revisión teórica*. Zenodo. https://doi.org/10.5281/ZENODO.10975732

Cordova-Alvarado, R. L., Andrade-López, M. S., & Álvarez-Vera, M. S. (2024). Inteligencia artificial generativa en el ámbito de la ciberseguridad: Una revisión

sistemática de literatura. *MQRInvestigar*, *8*(3), 556-578. https://doi.org/10.56048/MQR20225.8.3.2024.556-578

Crespo Martínez, E. (2017). Ecu@Risk, Una metodología para la gestión de Riesgos aplicada a las MPYMEs. *Enfoque UTE*, *8*(1), 107-121. https://doi.org/10.29019/enfoqueute.v8n1.140

Crespo-Martínez, E., & Cordero-Torres, G. (2018). ESTUDIO COMPARATIVO ENTRE LAS METODOLOGÍAS CRAMM Y MAGERIT PARA LA GESTIÓN DE RIESGO DE TI EN LAS MPYMES. *UDA AKADEM*, *1*, 38-47. https://doi.org/10.33324/udaakadem.vi1.129

CSAE. (2012). *Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro I: Método*.

Cuervo Forero, A. R. (2023). *Importancia del Gobierno TI, Ciberseguridad y Comunidades Digitales*. http://repository.unipiloto.edu.co/handle/20.500.12277/13076

Deacutis, M. (2015). *The cloud and security governance* (1758623669) [M.S., Utica College]. ProQuest Dissertations & Theses A&I; ProQuest Dissertations & Theses Global: The Humanities and Social Sciences Collection; ProQuest Dissertations & Theses Global A&I: The Sciences and Engineering Collection. https://www.proquest.com/dissertations-theses/cloud-security-governance/docview/1758623669/se-2?accountid=14795

Fernandez, A., & Garcia, D. F. (2016). Complex vs. Simple asset modeling approaches for information security risk assessment: Evaluation with MAGERIT methodology. *2016 Sixth International Conference on Innovative Computing Technology (INTECH)*, 542-549. https://doi.org/10.1109/INTECH.2016.7845064

Ferreira González, I., Urrútia, G., & Alonso-Coello, P. (2011). Revisiones sistemáticas y metaanálisis: Bases conceptuales e interpretación. *Revista Española de Cardiología*, *64*(8), 688-696. https://doi.org/10.1016/j.recesp.2011.03.029

Ferruzola Gómez, E., Duchimaza S., J., Ramos Holguín, J., & Alejandro Lindao, M. (2019). Plan de contingencia para los equipos y sistemas informáticos utilizando la metodología MAGERIT. *Revista Científica y Tecnológica UPSE*, *6*(1), 34-41. https://doi.org/10.26423/rctu.v6i1.429

García, F. Y. H., & Moreta, L. M. L. (2018). Maturity Model for the Risk Analysis of Information Assets based on Methodologies MAGERIT, OCTAVE y MEHARI;

focused on Shipping Companies. *2018 7th International Conference On Software Process Improvement (CIMPS)*, 29-39. https://doi.org/10.1109/CIMPS.2018.8625848

Ghirardotti, M. S., & Renna, J. I. (2022). Auditoría y ciberseguridad. *Audit.AR*, *2*(1), 014. https://doi.org/10.24215/27188647e014

IBM. (2022, abril 14). *¿Qué es el malware?* https://www.ibm.com/es-es/topics/malware

INCIBE. (s. f.). *Usar cortafuegos en nuestros equipos ¿si, no, depende?* Recuperado 29 de agosto de 2024, de https://www.incibe.es/ciudadania/blog/usar-cortafuegos-en-nuestros-equipos-si-no-depende

ISACA (Ed.). (2012). *COBIT 5: A business framework for the governance and management of enterprise IT: an ISACA® framework*. ISACA.

Jaramillo, D., Cabrera, A., Abad, M., Torres, D., & Verdún, J. C. (2015). *Definition of cybersecurity businness framework based on ADM-TOGAF*. https://doi.org/10.1109/CISTI.2015.7170391

López, D. N. (2017). Modelo de gestión de los servicios de tecnología de información basado en COBIT, ITIL e ISO/IEC 27000. *Revista Tecnológica - ESPOL, 30(1)*. http://orcid.org/0000-0001-7596-0194

Macias, M., Macias, R., Navarrete, M., & Navarrete, J. (2023). Normas y estándares en auditoría: Una revisión de su utilidad en la seguridad informática. *Revista Científica Arbitrada Multidisciplinaria PENTACIENCIAS*, *5*, 584-599. https://doi.org/10.59169/pentaciencias.v5i4.700

Malatji, M., Marnewick, A., & von Solms, S. (2020). Validation of a socio-technical management process for optimising cybersecurity practices. *Computers & Security*, *95*, 101846. https://doi.org/10.1016/j.cose.2020.101846

Manrique Plácido, J. M. (2019). *Introducción a la auditoría*. https://repositorio.uladech.edu.pe/handle/20.500.13032/14790

Martínez, I. (2019). Auditoría e inteligencia artificial: El papel de los contables/auditores en el siglo XXI. *AECA: Revista de la Asociación Española de Contabilidad y Administración de Empresas*, *125*, 26-29.

McIntosh, T. R., Susnjak, T., Liu, T., Watters, P., Xu, D., Liu, D., Nowrozy, R., & Halgamuge, M. N. (2024). From COBIT to ISO 42001: Evaluating cybersecurity frameworks for opportunities, risks, and regulatory compliance in

commercializing large language models. *Computers & Security*, *144*, 103964. https://doi.org/10.1016/j.cose.2024.103964

Miranda, N. B., Rodavia, M. R. D., & Miranda, M. -m. I. (2019). IT Infrastructure Auditing using COBIT Framework. *2019 6th International Conference on Technical Education (ICTechEd6)*, 1-6. https://doi.org/10.1109/ICTechEd6.2019.8790861

Mogollón, A. (2016). Análisis Comparativo: Metodologías de análisis de Riesgos. *Universidad Centroccidental Lisandro Alvarado*.

Moher, D., Liberati, A., Tetzlaff, J., & Altman, D. G. (2009). Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. *BMJ*, *339*, b2535. https://doi.org/10.1136/bmj.b2535

Moncayo, D., & Montenegro, C. (2016). Information security risk in SMEs: A hybrid model compatible with IFRS: Evaluation in two Ecuadorian SMEs of automotive sector. *2016 6th International Conference on Information Communication and Management (ICICM)*, 115-120. https://doi.org/10.1109/INFOCOMAN.2016.7784226

Morán Vilcherrez, M. (2020). El enfoque de la auditoría en el entorno de la era digital y la inteligencia artificial. *Revista la Junta*, *3*, 15-41. https://doi.org/10.53641/junta.v3i2.54

Nieto, Á. P. P. (2022). *Desafios y oportunidades del uso de la inteligencia artificial en la auditoría interna* [Universidad Militar Nueva Granada]. http://hdl.handle.net/10654/42293

Ochoa Diez, M., Sepúlveda Arcila, E., Ramírez Oquendo, J., & Velásquez Pérez, M. (2022). Auditoría forense desde una revisión conceptual, metodológica y empírica. *Revista Visión Contable*, *25*, 153-168. https://doi.org/10.24142/rvc.n25a8

Orellana-Cabrera, X. E., & Álvarez-Galarza, M. D. (2022). Marco de trabajo de gobierno de TI orientado a la ciberseguridad para el sector bancario bajo COBIT 2019. *Polo del Conocimiento*, *7*(3). https://doi.org/10.23857/pc.v7i3.3758

Peto, D. (2006). Generalized risk assessment index for information systems auditing. *28th International Conference on Information Technology Interfaces, 2006.*, 97-102. https://doi.org/10.1109/ITI.2006.1708459

Ridley, G., Young, J., & Carroll, P. (2004). COBIT and its utilization: A framework from the literature. *37th Annual Hawaii International Conference on System Sciences, 2004.*, 8. https://doi.org/10.1109/HICSS.2004.1265566

Rios Reyes, J., Vasquez Chiclayo, R., & Santos, A. (2023). MÉTODOS EMERGENTES DE AUDITORÍA EN INTEGRIDAD DE DATOS EN LA NUBE: UNA REVISIÓN SISTEMÁTICA DE LAS ÚLTIMAS TENDENCIAS. *INVESTIGACION & DESARROLLO*, *23*. https://doi.org/10.23881/idupbo.023.1-8i

Rodríguez-Palenzuela, D. (2001). *Innovación en tecnologías de la información y su interacción con la organización de empresas*. *340*, 73-82.

Rozas Flores, A. E. (2014). AUDITORIA FORENSE. *Quipukamayoc*, *16*(32), 67. https://doi.org/10.15381/quipu.v16i32.4825

Sabillón, R., & Cano M., J. J. (2019). Auditorías en Ciberseguridad: Un modelo de aplicación general para empresas y naciones. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, *32*, 33-48. https://doi.org/10.17013/risti.32.33-48

Schneier, B. (2015). *Secrets and Lies: Digital Security in a Networked World.* https://doi.org/10.1002/9781119183631

Serna Valdivia, E. J., & Mejía Miranda, J. (2020). Proposal of a Intelligent Agent for Management and Mitigation in Cibersecurity Risk for IoT Environments. *2020 9th International Conference On Software Process Improvement (CIMPS)*, 148-154. https://doi.org/10.1109/CIMPS52057.2020.9390114

Spremic, M., & Popovic, M. (2007). Towards a corporate IT risk management model. *Proceedings of the 6th WSEAS International Conference on Information Security and Privacy*, 111-116.

Spremic, M., Žmirak, Z., & Kraljevic, K. (2008). IT governance and performance measurement: Research study on Croatian companies. *Proceedings of the 7th WSEAS International Conference on Software Engineering, Parallel and Distributed Systems*, 187-192.

Syalim, A., Hori, Y., & Sakurai, K. (2009). Comparison of Risk Analysis Methods: Mehari, Magerit, NIST800-30 and Microsoft's Security Management Guide. *2009 International Conference on Availability, Reliability and Security*, 726-731. https://doi.org/10.1109/ARES.2009.75

Tangka, G. M. W., Liem, A. T., & Mambu, J. Y. (2020). Information Technology Governance Audit Using the COBIT 5 Framework at XYZ University. *2020 2nd International Conference on Cybernetics and Intelligent System (ICORIS)*, 1-5. https://doi.org/10.1109/ICORIS50180.2020.9320803

Tingliao, L. (2016). The IT audit research based on the information system success model and COBIT. *2016 10th International Conference on Intelligent Systems and Control (ISCO)*, 1-3. https://doi.org/10.1109/ISCO.2016.7727117

Toapanta Toapanta, S. M., Terán Terranova, Y. J., Naranjo Sánchez, B. A., & Mafla Gallegos, L. E. (2020). Security and Privacy in Information Management in a Distributed Environment for Public Organizations. En A. J. Tallón-Ballesteros (Ed.), *Frontiers in Artificial Intelligence and Applications*. IOS Press. https://doi.org/10.3233/FAIA200716

Trujillo-Avilés, M. N., Morales-López, D. A., Taipe-Yanez, J. F., & 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

Tubío Figueira, P., López Bravo, C., & Rivas López, J. L. (2020). Improving information security risk analysis by including threat-occurrence predictive models. *Computers & Security*, *88*, 101609. https://doi.org/10.1016/j.cose.2019.101609

Vaca Benalcázar, C. P. (2016). CIBERSEGURIDAD Y GESTIÓN DEL RIESGO TECNOLÓGICO EN EL MARCO DE LA NIIF. *Revista Científica UISRAEL*, *3*(2), 35-50. https://doi.org/10.35290/rcui.v3n2.2016.9

van Eck, N. J., & Waltman, L. (2014). CitNetExplorer: A new software tool for analyzing and visualizing citation networks. *Journal of Informetrics*, *8*(4), 802-823. https://doi.org/10.1016/j.joi.2014.07.006

van Eck, N. J., & Waltman, L. (2017). Citation-based clustering of publications using CitNetExplorer and VOSviewer. *Scientometrics*, *111*(2), 1053-1070. https://doi.org/10.1007/s11192-017-2300-7

Vega, R., Arroyo, R., & Yoo, S. G. (2017). Experience in Applying the Analysis and Risk Management Methodology called MAGERIT to Identify Threats and Vulnerabilities in an Agro-industrial Company. *International Journal of Applied Engineering Research*, *12*, 6741-6750.

Velasco, J., Ullauri, R., Pilicita, L., Jacome, B., Saa, P., & Moscoso-Zea, O. (2018). Benefits of Implementing an ISMS According to the ISO 27001 Standard in the Ecuadorian Manufacturing Industry. *2018 International Conference on Information Systems and Computer Science (INCISCOS)*, 294-300. https://doi.org/10.1109/INCISCOS.2018.00049

Vicente, E., Mateos, A., & Jiménez-Martín, A. (2014). Risk analysis in information systems: A fuzzification of the MAGERIT methodology. *Knowledge-Based Systems*, *66*, 1-12. https://doi.org/10.1016/j.knosys.2014.02.018

Von Solms, B. (2005). Information Security governance: COBIT or ISO 17799 or both? *Computers & Security*, *24*(2), 99-104. https://doi.org/10.1016/j.cose.2005.02.002