Vol.8 No.2 (2024): Journal Scientific MQRInvestigar ISSN: 2588–0659
https://doi.org/10.56048/MQR20225.8.2.2024.3889-3913

Audit strategies in cybersecurity and their importance in companies: a literature review

Estrategias de Auditoría en ciberseguridad y su importancia en las empresas una revisión bibliográfica

Autores:

Trujillo-Avilés, Moisés Nikolay
UNIVERSIDAD CENTRAL DEL ECUADOR, ECUADOR
Mba. Master in Business Administration
Docente Tutor del área de Contabilidad y Auditoría
Quito - Ecuador
mntrujillo@uce.edu.ec
https://orcid.org/0009-0009-7438-2746

Morales-López,David Alexander
UNIVERSIDAD CENTRAL DEL ECUADOR, ECUADOR
Mtr. Master en Mercadotecnia Mención Marketing Digital
Investigador Marketing e Innovación Empresarial
Quito - Ecuador
damorales@uce.edu.ec
https://orcid.org/0000-0002-0843-2372

Taipe-Yanez, José Francisco
UNIVERSIDAD CENTRAL DEL ECUADOR, ECUADOR
Mgs. Magister en Administración y Marketing
Docente Tutor del área de Marketing y Administración
Quito - Ecuador
jtaipe@uce.edu.ec
https://orcid.org/0000-0002-0268-3007

Pallo-Tulmo, Patricia Alexandra
INSTITUTO SUPERIOR TECNOLÓGICO CONSULTING GROUP ECUADOR - ESCULAPIO, ECUADOR
Ing. Administración de Empresas
Docente Tutor del área Empresarial y Gestión Comercial
Quito - Ecuador
p.pallo@istcge.edu.ec
https://orcid.org/0000-0002-2137-6969

Fechas de recepción: 02-JUN-2024 aceptación: 12-JUN-2024 publicación: 15-JUN-2024

https://orcid.org/0000-0002-8695-5005
http://mqrinvestigar.com/

Resumen

La ciberseguridad se ha convertido en un componente de gran importancia para las organizaciones, ya que garantiza la protección de datos contra amenazas digitales y asegura a los clientes el uso adecuado y acceso a su información personal. El objetivo de esta investigación es determinar la importancia de la auditoría en la ciberseguridad en las empresas. A través de un estudio cuantitativo de carácter bibliométrico, se recopiló información relevante que facilito identificar enlaces, redes, citaciones, vínculos bibliográficos y resultados principales en esta área de estudio. Uno de los resultados más significativos de la investigación es la relación entre "auditoría" y "ciberseguridad" en áreas esenciales como la protección de datos, redes, IoT y registros de auditoría. Esto resalta la importancia de abordar la seguridad desde múltiples perspectivas y fomentar la colaboración en equipo capacitados. La investigación subraya la necesidad de invertir en medidas de seguridad preventivas y desarrollar estrategias de auditoría sólidas aplicadas a la realidad empresarial. La colaboración entre profesionales de auditoría y ciberseguridad es crucial para enfrentar los desafíos del entorno empresarial digital, ya que la combinación de estos conocimientos permite una protección más integral y efectiva de los activos digitales. En conclusión, la integración de la auditoría y la ciberseguridad es fundamental para garantizar la protección de datos en un mundo cada vez más conectado y digitalizado, y es esencial para el éxito y la confianza en las operaciones empresariales modernas.

Palabras clave: Auditoría; ciberseguridad; digitalización; empresa; riesgos digitales,;transformación digital

Abstract

Cybersecurity has become a component of great importance for organizations, as it guarantees the protection of data against digital threats and ensures customers the proper use and access to their personal information. The objective of this research is to determine the importance of cybersecurity auditing in companies. Through a quantitative bibliometric study, relevant information was collected to identify links, networks, citations, bibliographic links and main results in this area of study. One of the most significant findings of the research is the relationship between "auditing" and "cybersecurity" in key areas such as data protection, networks, IoT and audit trails. This highlights the importance of approaching security from multiple perspectives and fostering collaboration in skilled teams. The research underscores the need to invest in preventative security measures and develop robust audit strategies applied to business realities. Collaboration between audit and cybersecurity professionals is crucial to meet the challenges of the digital business environment, as the combination of these skills enables more comprehensive and effective protection of digital assets. In conclusion, the integration of audit and cybersecurity is critical to ensure data protection in an increasingly connected and digitized world, and is essential for success and trust in modern business operations.

Keywords: Audit; cybersecurity; digitalization; digital transformation; enterprise; digital risks; digital transformation

Introducción

Actualmente el desarrollo tecnológico y digitalización empresarial han cambiado las estructuras empresariales mismas que mediante sistemas digitales y conectividad proporcionan un servicio eficaz a los clientes. Ante estos cambios se considera de vital importancia la protección no solo de recursos físicos en las empresas sino también de sus recursos digitales. El objetivo de la presente investigación es determinar la importancia de la auditoría en la ciberseguridad en las empresas.

Dentro de los riesgos digitales a los que las empresas están expuestas se pueden encontrar accesos no autorizados, ciberataque, sustracción de información confidencial, alteración de datos, exposición de información entre otros que van ligados a la vulneración de información (Obaid & Alheeti, 2024).

La ciberseguridad es un principio fundamental en las organizaciones debido a que facilita la protección de datos ante amenazas digitales. Las empresas dentro de su estrategia digital deben establecer mecanismos para garantizar a sus clientes el correcto uso, autorización y acceso a sus datos personales (Liu & Li, 2024).

De igual forma es importante establecer estrategias para evitar el uso no autorizado de esta información e interrupciones en las operaciones de la empresa. Es allí donde la ciberseguridad aporta a la defensa digital de los usuarios y organizaciones.

Las empresas que dentro de su estructura digital implementan ciberseguridad minimizan los efectos no deseados ocasionados por ciberataques, mismos que afectan la confianza de sus clientes, reputación empresarial, interrupción en el correcto desenvolvimiento de sus funciones y problemas legales por el mal uso de la información (Vishnevsky, 2024).

Vulneraciones generales a los que se exponen las organizaciones.

Dentro de las principales vulneraciones a las que las empresas se exponen, son aquellas que van de la mano con la infiltración a los sistemas de seguridad, estos se detallan en la tabla 1

Tabla 1

Tipos de ataque en ciberseguridad

TIPO DE ATAQUE	DESCRIPCIÓN
MALWARE	El término malware se refiere a programas informáticos con intenciones maliciosas. Engloba una diversidad de software diseñado para facilitar a terceros el acceso no autorizado a información confidencial o para interrumpir el funcionamiento normal de infraestructuras críticas. Algunos ejemplos típicos de malware son los troyanos, el spyware y los virus.

RANSOMWARE	El ransomware se refiere a un modelo de negocio y a diversas tecnologías asociadas que los criminales pueden emplear para extorsionar dinero de organizaciones.
ATAQUE DE INTERMEDIARIO	Un ataque de intermediario ocurre cuando una entidad externa trata de ingresar sin autorización a una red durante la transferencia de datos. Estos ataques incrementan las vulnerabilidades en la seguridad de información sensible, como por ejemplo los datos financieros.
PHISHING	El phishing es una amenaza cibernética que emplea estrategias de ingeniería social con el propósito de engañar a los usuarios para que revelen información personal de identificación. Por ejemplo, los ciberatacantes envían correos electrónicos que persuaden a los usuarios para que hagan clic y proporcionen datos de su tarjeta de crédito en un sitio web de pagos falso. Asimismo, los ataques de phishing pueden inducir a la descarga de archivos adjuntos maliciosos que instalan malware en los dispositivos de la empresa.
DDOS	Un ataque de denegación de servicio distribuido (DDoS) consiste en una acción concertada para saturar un servidor mediante el envío masivo de solicitudes falsas. Estos incidentes bloquean el acceso de los usuarios legítimos al servidor de destino.
AMENAZA INTERNA	Una amenaza interna se refiere a un peligro para la seguridad que surge de individuos dentro de una organización que tienen intenciones maliciosas. Estos individuos cuentan con privilegios de acceso elevados a los sistemas informáticos y pueden comprometer la seguridad de la infraestructura desde el interior.

Fuente: Elaboración propia en base a "Exploración integral de la seguridad en redes de proveedores de servicios de internet: Una revisión sistemática de literatura" año 2024

Por lo expresado en la tabla 1 las empresas buscan contar con un personal especialista en ciberseguridad, estos van estrechamente relacionados a mitigar, reducir, prevenir estos riesgos. Otra de las herramientas que las empresas destinan para su ciberseguridad es el uso de softwares y capacitaciones constantes a su personal, permitiendo una defensa solida ante posibles ataques (Viteri Hernández & Ávila, 2024).

Tipos de ciberseguridad.

La ciberseguridad se aplica en distintas áreas de la organización, dentro de las cuales podemos encontrar en la tabla 2

Tabla 2

Tipos de ciberseguridad

DEFENSA	DESCRIPCIÓN
Ciberseguridad de la infraestructura crítica	La infraestructura crítica se refiere a los sistemas digitales que desempeñan un papel fundamental en aspectos vitales de la sociedad, tales como el suministro de energía, las comunicaciones y el transporte. Dada la importancia de estas áreas, las organizaciones necesitan implementar un enfoque riguroso de ciberseguridad, ya que cualquier interrupción o pérdida de datos podría tener repercusiones significativas en la estabilidad de la sociedad.
Seguridad de la red	La seguridad de red se refiere a las medidas de ciberseguridad destinadas a proteger los dispositivos y equipos conectados a una red. Los equipos de tecnología de la información

	(TI) implementan tecnologías de seguridad de red, tales como cortafuegos y sistemas de control de acceso, con el fin de gestionar el acceso de usuarios y administrar los permisos para recursos digitales particulares.
Seguridad en la nube	La seguridad en la nube se refiere a las acciones que una entidad lleva a cabo para salvaguardar los datos y aplicaciones alojados en entornos de nube. Su importancia radica en fortalecer la confianza del cliente, garantizar la continuidad de las operaciones y cumplir con los requisitos normativos de privacidad de datos en un contexto de escalabilidad.
Seguridad de IoT	El concepto de Internet de las cosas (IoT) se refiere a la conectividad de dispositivos electrónicos a través de Internet para operar de forma remota. Por ejemplo, un sistema de alarma inteligente que envía notificaciones periódicas a un teléfono inteligente puede ser clasificado como un dispositivo IoT. Estos dispositivos IoT introducen un nivel adicional de riesgo en términos de seguridad debido a su continua conectividad y a la posibilidad de errores de software no detectados.
Seguridad de los datos	La protección de datos implica asegurar la integridad y confidencialidad de la información tanto mientras se encuentra en movimiento como mientras está almacenada. Los desarrolladores implementan estrategias defensivas, como la encriptación y la creación de copias de seguridad segregadas, para garantizar la continuidad operativa y prevenir posibles fugas de datos.
Seguridad de las aplicaciones	La seguridad de las aplicaciones implica un esfuerzo conjunto destinado a reforzar la protección de una aplicación contra la manipulación no autorizada durante todas las fases de su ciclo de vida, incluyendo el diseño, desarrollo y pruebas. Los desarrolladores de software se encargan de escribir código seguro con el fin de prevenir la aparición de errores que puedan incrementar los riesgos de seguridad.
Seguridad de los puntos de conexión	La seguridad de los puntos de conexión se ocupa de los riesgos de seguridad que surgen cuando los usuarios acceden de forma remota a la red de una organización. Esta protección examina los archivos de los dispositivos individuales y contrarresta las amenazas al detectarlas.
Planificación de la recuperación de desastres y continuidad del negocio	Los planes de contingencia son estrategias que habilitan a una organización para reaccionar de manera inmediata ante incidentes de ciberseguridad, manteniendo sus operaciones con mínimas o nulas interrupciones. Estos planes incluyen políticas de recuperación de datos diseñadas para hacer frente de manera efectiva a la pérdida de información.
Educación del usuario final	Los individuos dentro de una organización desempeñan un papel fundamental en el aseguramiento del cumplimiento efectivo de las estrategias de ciberseguridad. La capacitación resulta esencial para asegurar que los empleados adquieran conocimientos sobre las mejores prácticas de seguridad, como la identificación y eliminación de correos electrónicos sospechosos, así como la precaución al conectar dispositivos USB desconocidos.

Fuente: Elaboración propia con base en: "The Role of Internal Auditors Characteristics in Cybersecurity Risk Assessment in Financial-Based Business Organisations: a Conceptual Review" (Usman & Ayoib, 2024)

La implementación adecuada de la ciberseguridad dependerá de la estrategia de digitalización empresarial, recursos financieros, tecnológicos y el talento humano especializado que esté disponible en la organización (Usman & Ayoib, 2024).

Estrategia de Ciberseguridad

Al contemplar una estrategia de ciberseguridad para una organización, es indispensable entender los diversos procesos, recursos y tecnología con la cuenta la organización. Dentro de estos podemos encontrar:

- **Personas:** Integral personal altamente calificado para desenvolverse en el área de ciberseguridad es indispensable para prevenir amenazas y optimizar las prácticas de seguridad, protegiendo los dispositivos, información y minimizando los riesgos (Rosales Troya & Ordóñez Parra, 2023).

- **Procesamiento:** El correcto procesamiento de información es indispensable para desarrollar un marco de seguridad solido ante las amenazas actuales, es por ello que una infraestructura informática clara aporta a detectar posibles vulneraciones, esto llevado de la mano con un plan táctico aporta a la respuesta inmediata de la organización (Rosales Troya & Ordóñez Parra, 2023).

- **Tecnología:** Las empresas utilizan los recursos tecnológicos para proteger sus servidores, información y datos frente a posibles amenazas. Esto aporta a dar seguridad y confianza en sus clientes (Rosales Troya & Ordóñez Parra, 2023).

Auditoría

La auditoría consiste en el proceso de verificar, corroborar y validar el cumplimiento de actividades según la planificación establecida y directrices estipuladas. Según la Organización Internacional de Normalización (ISO) la auditoría es un proceso sistemático, documentado e independiente que facilita obtener evidencias para determinar en qué medida se cumplen los criterios de auditoría, estos suelen ser las políticas, procedimientos y recursos a revisar (Minaya Macias & Minaya Macias, 2023).

La auditoría permite establecer que actividades se desarrollaran según lo planificado, cuales no podrán ser cumplidas y aquellas actividades susceptibles a mejora. Promoviendo mejoras e información objetiva para la toma de decisiones (Ávila-Gutiérrez, 2023).

Características de la auditoría

El proceso de realizar una auditoría permite a las organizaciones ser:

- ✓ **Objetivas:** El proceso de auditar aporta a las empresas hechos reales, solidos, sustentables y con evidencias que garanticen su correcto desenvolvimiento (Guevara Vega & Delgado Deza, 2023).

- ✓ **Sistemáticas:** la auditoría al establecer con claridad los pasos y recursos que se ejecutaran según la estrategia empresarial facilita establecer un orden lógico para alcanzar los objetivos planteados, optimizando recursos y tiempo (Guevara Vega & Delgado Deza, 2023).

- ✓ **Profesionales y transparentes:** Los procesos mediados por auditores aportan información sin juicios de valor permitiendo la toma de decisiones estratégicas y planes necesarios para garantizar el buen funcionamiento empresarial (Guevara Vega & Delgado Deza, 2023).

Tipos de Auditoría

En la actualizad existen varios tipos de auditorías, mismos que de aplican dentro de las organizaciones según su necesidad, estos de detallan a continuación en la tabla 3.

Tabla 3

Tipos de Auditorías

AUDITORÍA	DESCRIPCIÓN
Auditoría interna	Se trata de una evaluación realizada internamente por un individuo o equipo dentro de la empresa misma. El propósito es que la organización se someta a un autoanálisis en busca de áreas que puedan ser mejoradas.
Auditoría externa	Esta auditoría es llevada a cabo por un ente que no forma parte de la empresa bajo evaluación. Por lo general, una firma auditora externa examina los procesos de otra compañía que ha contratado sus servicios. El objetivo de este tipo de auditoría es obtener una perspectiva externa, proveniente de un tercero independiente a la entidad mercantil analizada.
Auditoría contable	Este tipo de auditoría implica la revisión de los estados financieros de la empresa con el fin de verificar que estos representen adecuadamente la situación económica de la entidad. Se examinan diversos documentos, incluyendo el balance general, el estado de resultados, el estado de flujos de efectivo y el estado de cambios en el patrimonio neto.
Auditoría operativa	Se trata de una auditoría que tiene como objetivo evaluar si una empresa está utilizando de manera eficaz sus recursos. Es decir, se busca garantizar que sus procesos sean eficientes y no estén ocasionando pérdidas a la organización.

Auditoría financiera	Este proceso implica examinar la situación financiera y contable de la empresa, y es más exhaustivo que una simple auditoría contable. Para llevar a cabo esta labor de forma integral, se requiere la colaboración de auditorías fiscales, de gestión, informáticas y legales.
Auditoría medioambiental	Se trata de evaluar el efecto que tiene la actividad de una empresa en el medio ambiente, con el fin de verificar el cumplimiento de los estándares legales establecidos. En caso de no cumplir con dichos estándares, se deben considerar medidas o estrategias para mejorar la situación.
Auditoría informática	Esta auditoría consiste en la evaluación de los programas informáticos o sistemas adoptados por la empresa, como por ejemplo aquellos utilizados para los procesos comerciales o fiscales.
Auditoría de calidad	Esta auditoría se realiza para asegurar que el sistema de gestión de calidad implementado por la empresa esté funcionando adecuadamente, de acuerdo con los requisitos establecidos por la norma ISO 9001.
Auditoría de cumplimiento	Esta auditoría consiste en verificar que la empresa cumple con las regulaciones y prácticas recomendadas por la ley para su sector o contexto, asegurando así el cumplimiento normativo y el respeto de las normas establecidas.
Auditoría de gestión	Este tipo de auditoría implica evaluar la eficiencia en el uso de los recursos de la empresa y, a diferencia de la auditoría operativa, también se analiza si se han logrado los objetivos de rentabilidad previstos.

Fuente: Elaboración propia con base a: PEDIMENTOS ADUANALES CON IDENTIFICADORES INEXACTOS: UNA REVISIÓN DE LITERATURA" (Castillo Nevárez , 2023)

Auditoría en la Ciberseguridad

La ciberseguridad, es la protección que brindamos a nuestros sistemas, redes y programas contra los malos actores digitales. Estos malos actores tienen la intención de ingresar, modificar o destruir información importante, causar problemas a los usuarios o interrumpir nuestras actividades comerciales normales (Piminchumo Olivos & García Rodríguez, 2024).

Cuando hablamos de Auditoría en Ciberseguridad, nos referimos a un proceso organizado y minucioso para revisar y evaluar la seguridad de una organización. Esto facilita detectar cualquier debilidad, asegurarnos de que cumplimos con las políticas y regulaciones establecidas, y encontrar maneras de hacer nuestra seguridad aún más sólida. Dentro de los pasos para realizar una auditoría cibernética podemos encontrar (Duchitanga Plasencia, 2024):

- **Planificación:** Facilita delimitar el objetivo de la auditoría, trazando un mapa a seguir dentro de auditoría a realizar.
- **Evaluación de Riesgos**: dentro de esta etapa se busca detectar los posibles riesgos, amenazas y vulneraciones que puedan afectar a la organización.

- **Revisión de Controles:** Delimita las seguridades con las que cuenta la organización y sus posibles vulneraciones.
- **Pruebas y Validación:** Permite establecer el nivel de seguridad que posee la empresa mediante diversas pruebas en diversos escenarios.
- **Informe de Resultados:** En la etapa final se emite un informe en el cual se plasma cada una de las etapas antes mencionadas, vulneraciones y nivel de protección con el que cuenta la organización.

Estrategias para aplicar la Auditoría en la Ciberseguridad

La auditoría en ciberseguridad es una herramienta esencial para evaluar el nivel de seguridad en una empresa y asegurar que las políticas, procedimientos y controles estén en lugar para proteger los activos de información (Lozano Almansa, 2023).
Dentro de las principales estrategias que pueden aplicar en la auditoría en ciberseguridad podemos encontrar:

1. **Planificación y Definición del Alcance**

Para llevar a cabo una auditoría efectiva en ciberseguridad, es importante establecer un enfoque estructurado que enfoque varios aspectos críticos. En primer lugar, es indispensable identificar claramente los objetivos de la auditoría mismos que pueden incluir la evaluación de la efectividad de los controles de seguridad, el cumplimiento de normativas, la identificación de vulnerabilidades y la mejora continua de la seguridad (Ríos Reyes & Vásquez Chiclayo, 2023).

Además, se debe definir cuidadosamente el alcance de la auditoría para evitar la dispersión de esfuerzos, lo que implica determinar qué sistemas, aplicaciones, redes y datos serán auditados, priorizando áreas críticas en función del impacto potencial y la probabilidad de amenazas (Lizárraga Caipo & Mendoza de los Santos, 2022).

Finalmente, es fundamental asignar los recursos necesarios, como auditores con las competencias y herramientas adecuadas, y asegurar el apoyo de la alta dirección para garantizar que la auditoría se realice sin interrupciones y con éxito (Lizárraga Caipo & Mendoza de los Santos, 2022).

2. **Implementación de Metodologías y Técnicas de Auditoría**

Para llevar a cabo una auditoría exhaustiva en ciberseguridad, es importante seguir un proceso que abarque etapas clave. En primer lugar, se debe recopilar información utilizando

una variedad de técnicas, como entrevistas con el personal clave, revisión de documentación y análisis de registros de eventos (Coha Escalante & Barraza Mármol, 2022).

Luego, se procede a evaluar los controles de seguridad que posee la empresa, comparándolos con estándares reconocidos, como ISO/IEC 27001, NIST y COBIT. Conjuntamente se realizan pruebas técnicas, como análisis de vulnerabilidades y pruebas de penetración, llevadas a cabo por personal altamente capacitado para identificar posibles fallas en la seguridad sin interrumpir las operaciones normales (Coha Escalante & Barraza Mármol, 2022).

3. **Análisis y Evaluación de Resultados**

Al realizar una auditoría en ciberseguridad, es esencial establecer un proceso que abarque tres etapas fundamentales. En primer lugar, se realiza un análisis exhaustivo de riesgos, identificando y evaluando las vulnerabilidades encontradas y determinando la probabilidad de las amenazas para priorizar las áreas que requieren atención inmediata (Ochoa Diez & Sepúlveda Arcila, 2022).

Es importante establecer de manera detallada, las vulnerabilidades, los riesgos asociados y el impacto potencial para la empresa, respaldados con evidencia sólida. Finalmente, basado en estos hallazgos, se generan recomendaciones para mitigar las vulnerabilidades y mejorar la postura de seguridad, en función del riesgo y la viabilidad de implementación (Ochoa Diez & Sepúlveda Arcila, 2022).

4. **Comunicación y Reporte de Resultados**

El informe de auditoría debe ser formal e incluir un resumen ejecutivo con los hallazgos detallados, análisis de los riesgos y recomendaciones, presentando información clara y comprensible para todas las partes interesadas, incluidas aquellas sin conocimientos técnicos profundos (Jurado Zambrano & Armijo Perea, 2022).

Finalmente, se debe desarrollar un plan de acción estructurado que especifique responsables, plazos y recursos necesarios para cada acción, y establecer un proceso para monitorear y revisar el progreso de la implementación (Jurado Zambrano & Armijo Perea, 2022).

5. **Monitoreo y Mejora Continua**

Implementar un proceso de monitoreo continuo mediante herramientas de auditoría periódicas permite evaluar la efectividad de los controles de seguridad y detectar nuevas

vulnerabilidades. Es importante que el personal esté altamente capacitado en prácticas de ciberseguridad y en la implementación de los controles recomendados, fomentando una cultura de seguridad dentro de la organización (Moran Olvera & Chávez Cujilán, 2021).

Material y métodos

En la presente investigación, se llevará a cabo un estudio cuantitativo de tipo bibliométrico, con el objetivo de recopilar información estratégica sobre artículos y bibliografía relacionados con la auditoría en ciberseguridad. Mediante este análisis, se pretende determinar los enlaces, redes, citaciones, vínculos bibliográficos y resultados principales dentro de esta temática de estudio (Pole, 2023).

Estrategias de Búsqueda

Dentro del proceso para realizar el análisis bibliográfico, se examinaron dos elementos esenciales tales como: La ciberseguridad; auditoría; modelos de auditoría en ciberseguridad en contextos de motores de búsqueda y bases de datos académicas de Scopus, una plataforma de renombre internacional en el ámbito de la investigación.

Criterios de Selección

Entre los criterios de búsqueda empleados en la investigación se encuentra la cantidad de publicaciones, el análisis de autores, el índice de citación, las palabras clave utilizadas y las referencias contenidas en los artículos seleccionados de Scopus.

Criterios de Inclusión

La investigación contempla una variedad de criterios indispensables, mismos que se detallan en la Tabla 4.

Tabla 3

Criterios *de Inclusión*

INCLUSIÓN
1.- Palabras clave: Auditoría; Ciberseguridad
2.- Región o Nacionalidad
3.- Índice de Publicaciones por revistas
4.- Autores y bibliografía relacionada
5.- Año de Publicación (2014 al 2024)
6.- Afiliación

Fuente: Elaboración propia con base a:"Dideño de Metodologías Mixtas" (Pole, 2023)

Herramienta Empleada

En la presente investigación, se emplearán herramientas de gran relevancia como los análisis y estadísticas bibliométricas proporcionados por la plataforma Scopus y el software VOSVIEWER. Estas herramientas proporcionaran una comprensión de las publicaciones científicas, los autores y los índices de citas relacionados.

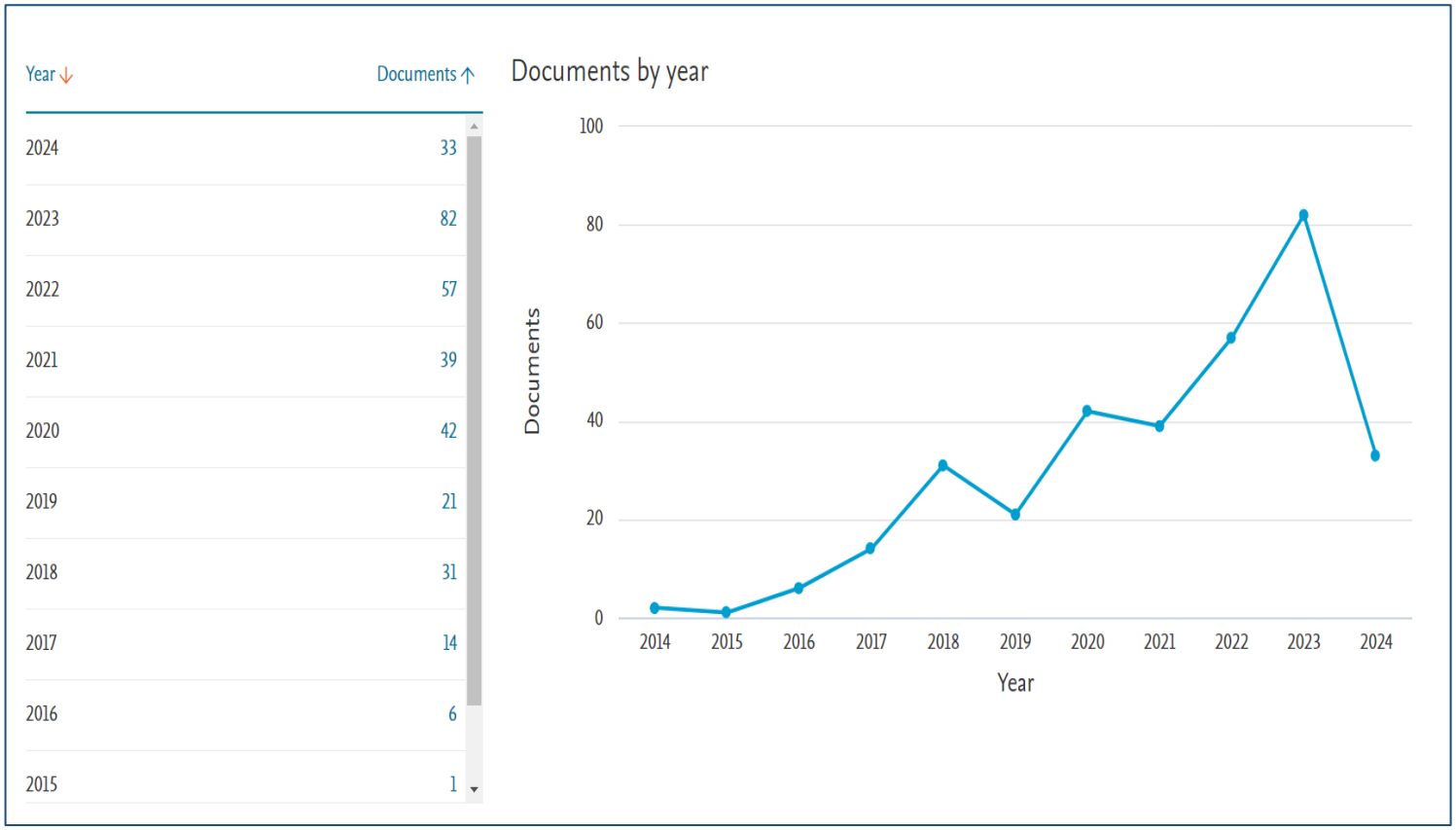
Resultados

Los resultados obtenidos por la base de datos Scopus se muestra a continuación:

Auditoría en Ciberseguridad.

Tras analizar la bibliografía según el año de publicación existente en la base de datos de Scopus se visualiza en la Figura 1, es importante resaltar que las palabras claves utilizadas son: Auditoría y Ciberseguridad.

Figura 1
Bibliografía publicada



Fuente: Análisis de Datos Scopus

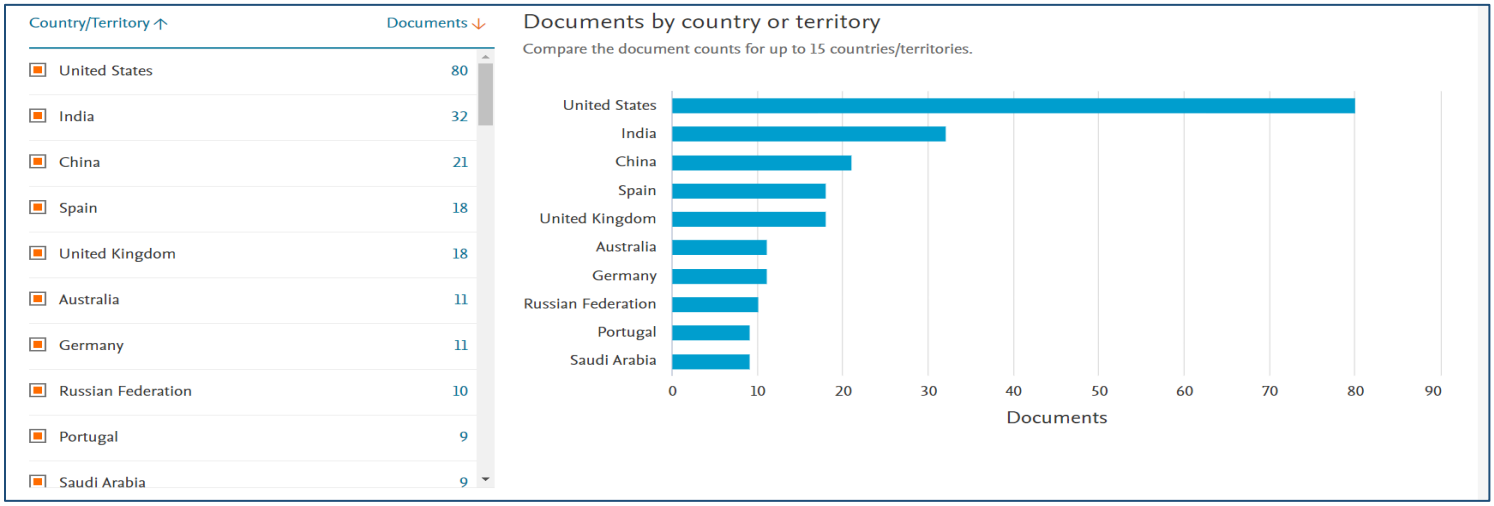
El crecimiento constante de la bibliografía en la auditoría y ciberseguridad en el contexto empresarial y tecnológico sugiere un aumento en la conciencia sobre los riesgos y desafíos asociados con la seguridad digital, así como un alto interés en desarrollar estrategias y soluciones efectivas para abordar estos problemas.

Los años con el mayor número de aportes científicos, como el 2023, el 2022 y el 2020, establecen momentos claves en los cuales la comunidad académica y profesional ha dedicado un mayor esfuerzo y discusión en esta área. El total de 328 recursos y aportes bibliográficos de alto impacto proporciona una base sólida para la exploración y comprensión de la ciberseguridad, lo que demuestra la vitalidad y la urgencia de este tema en la era digital actual.

Publicaciones por territorio de Publicación

La distribución geográfica de los recursos bibliográficos de alto impacto refleja la importancia y el alcance global de la auditoría en ciberseguridad en un contexto cada vez más interconectado y digitalizado.
Los países mencionados, como Estados Unidos, China, y el Reino Unido, son reconocidos por su liderazgo en innovación y tecnología, lo que los convierte en centros especializados para la investigación y desarrollo en auditoría en ciberseguridad. La presencia de India y España en esta lista también indica un interés y compromiso por parte de economías emergentes en abordar los desafíos de seguridad digital. Además, la inclusión de países como Rusia, Portugal y Arabia Saudita sugiere una diversidad geográfica en la producción científica este campo.

Figura 2
Publicaciones por Región



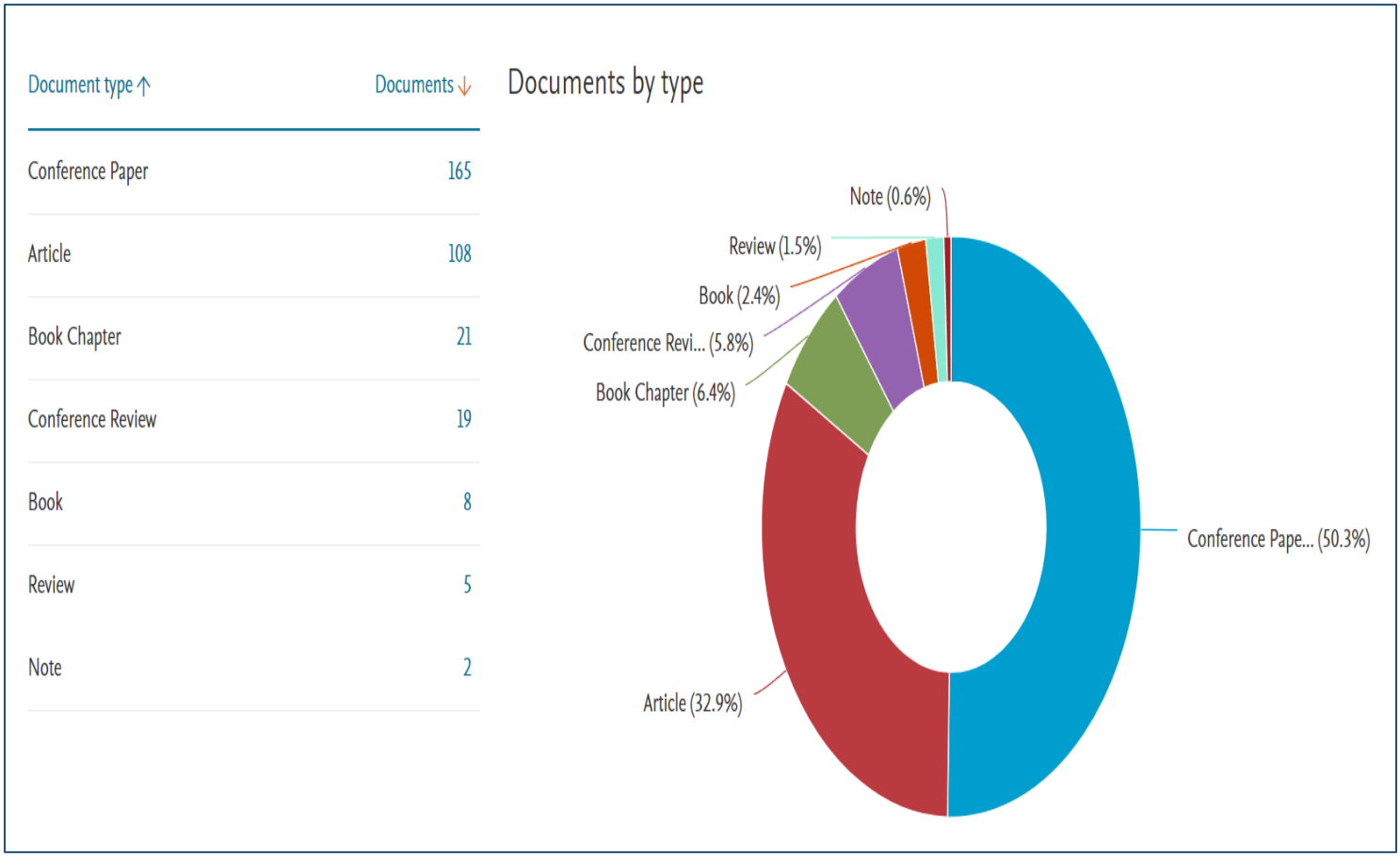
Fuente: Análisis de Datos Scopus

La conexión entre la innovación empresarial y la ciberseguridad marca la importancia de abordar estos temas no solo desde una perspectiva focalizada en la tecnológica, sino también desde una perspectiva empresarial. En conjunto, los países antes mencionados revelan la naturaleza de los desafíos y oportunidades en el campo de la auditoría en ciberseguridad y destaca la necesidad de cooperación internacional para abordarlos de manera efectiva.

Tipos de Publicaciones

Según la información detallada en la Figura 3, las principales fuentes bibliográficas corresponden a: conferencias de artículos en un 50.3%; artículos en un 32.9%; capítulos de libros 6.4%; conferencias 5.8%; libros 2.4%; revisiones 1.5% y notas 0.6%. Esto determina un amplio reto para los investigadores científicos mismos que al aportar libros o artículos científicos a favor del desarrollo de la auditoría en ciberseguridad.

Figura 3
Tipos de documentos

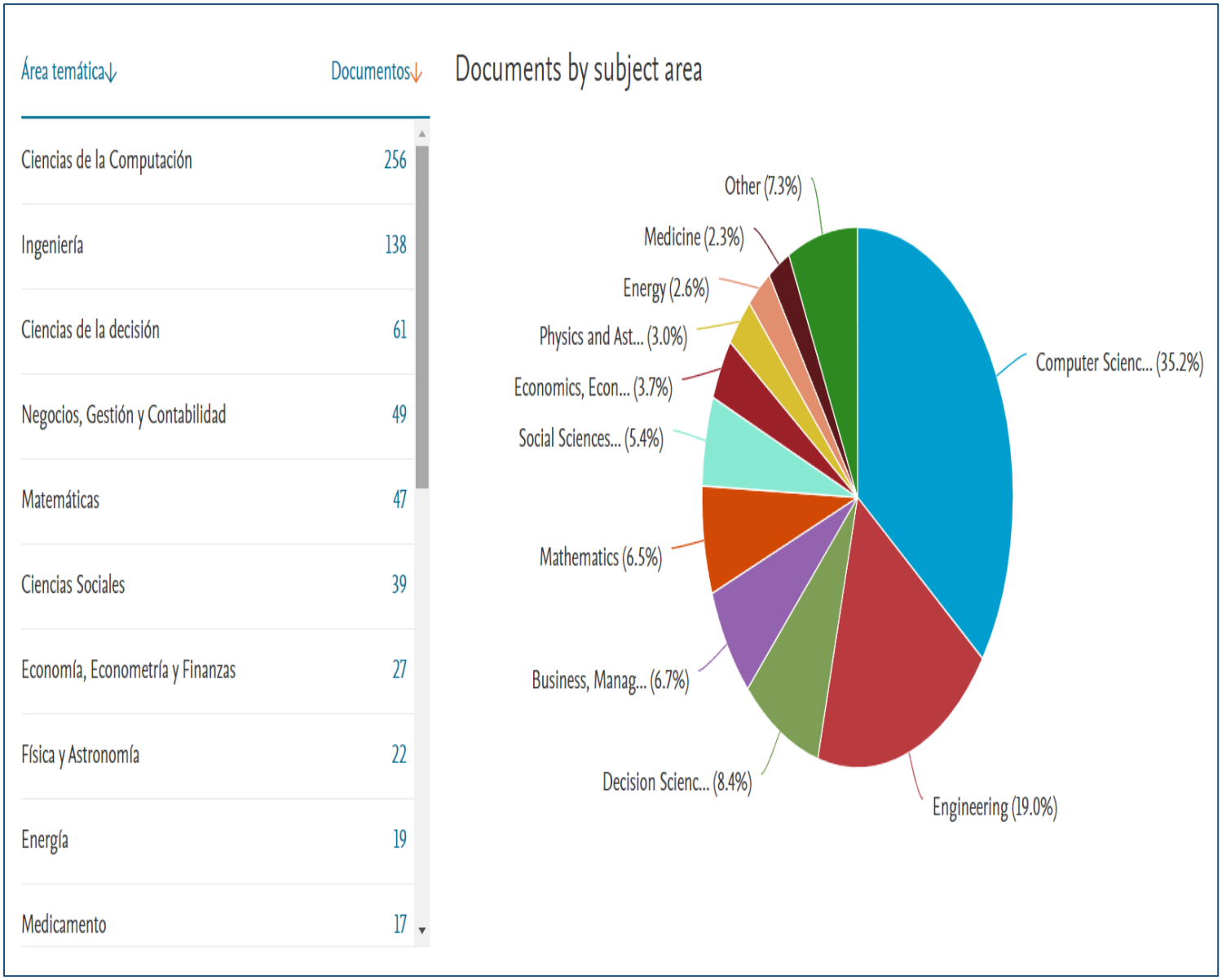


Fuente: Análisis de Datos Scopus

Documentos por áreas de investigación.

Con base a la información proporcionada por la Figura 4, las principales ares de investigación sobre la auditoría en ciberseguridad corresponde a ciencias de la computación; ingeniería; ciencias de la decisión; negocios; matemática y ciencias sociales. Esto corrobora que el uso de varias áreas de estudio aporta a los procesos de auditoría en ciberseguridad.

Figura 4
Áreas de estudio ligados a la auditoría en ciberseguridad.

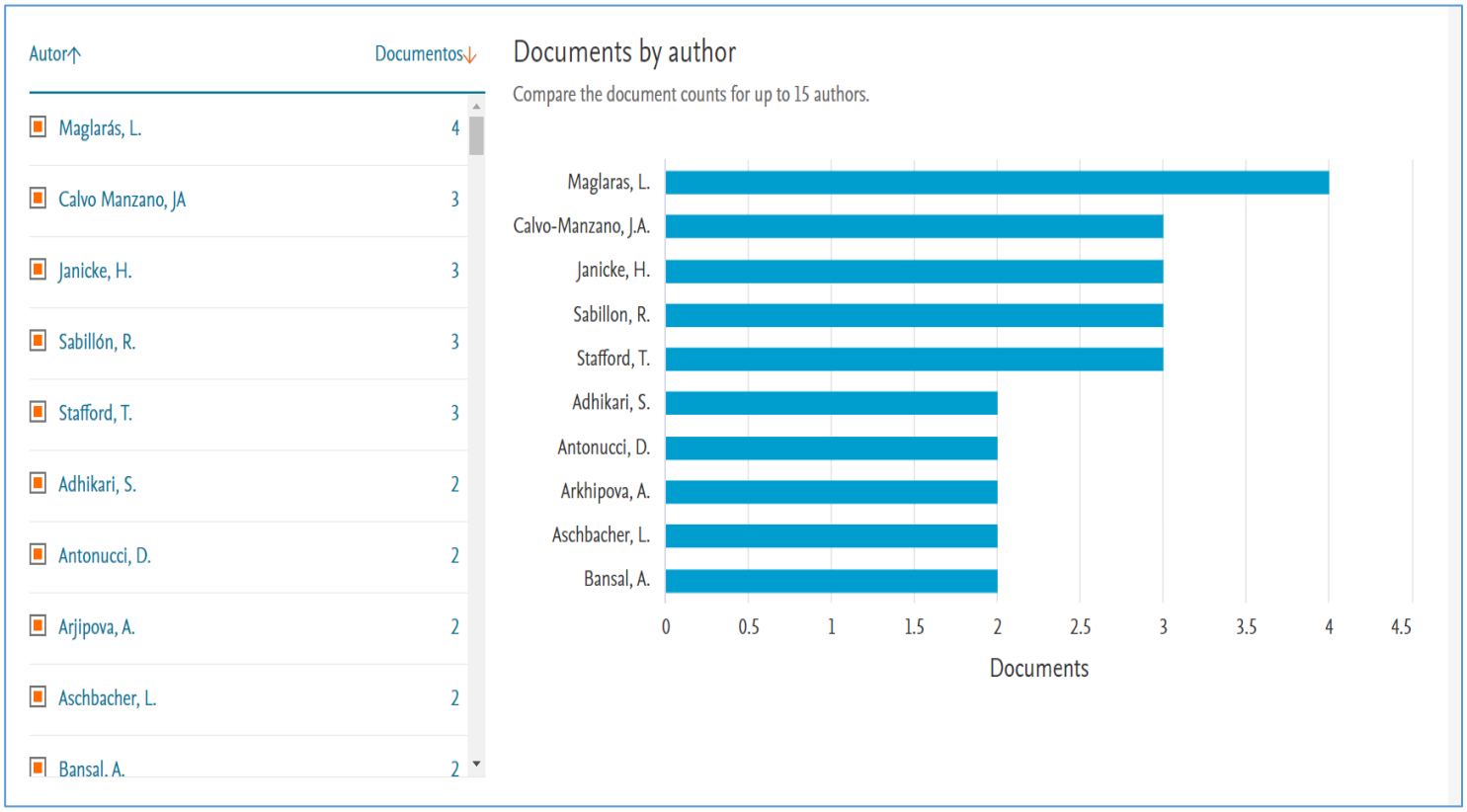


Fuente: Análisis de Datos Scopus

Principales autores de la auditoría en la ciberseguridad

Determinar los principales autores de la auditoría y la ciberseguridad es indispensable para el analisis bibliometrico, dento de la Figura 5 se visualiza los principales autores y numero de publicaciones de alto impacto siendo un promedio de 4 citas por investigador.

Figura 5
Autores del área de auditoría en ciberseguridad.



Fuente: Análisis de Datos Scopus

Estos investigadores, como Maglaras, Calvo Manzano, Janicke, Sabillón, Standford, Adhikari, Antonucci, Arjipova, Aschbacher y Bansal, han dejado un impacto significativo en la auditoría en ciberseguridad. Sus contribuciones van desde la evaluación de riesgos y la gestión de incidentes hasta la integración de estándares internacionales de seguridad. Han explorado aspectos legales y éticos, desarrollado técnicas para la detección y prevención de ataques cibernéticos avanzados, y han sido pioneros en la aplicación de inteligencia artificial para mejorar la seguridad digital.

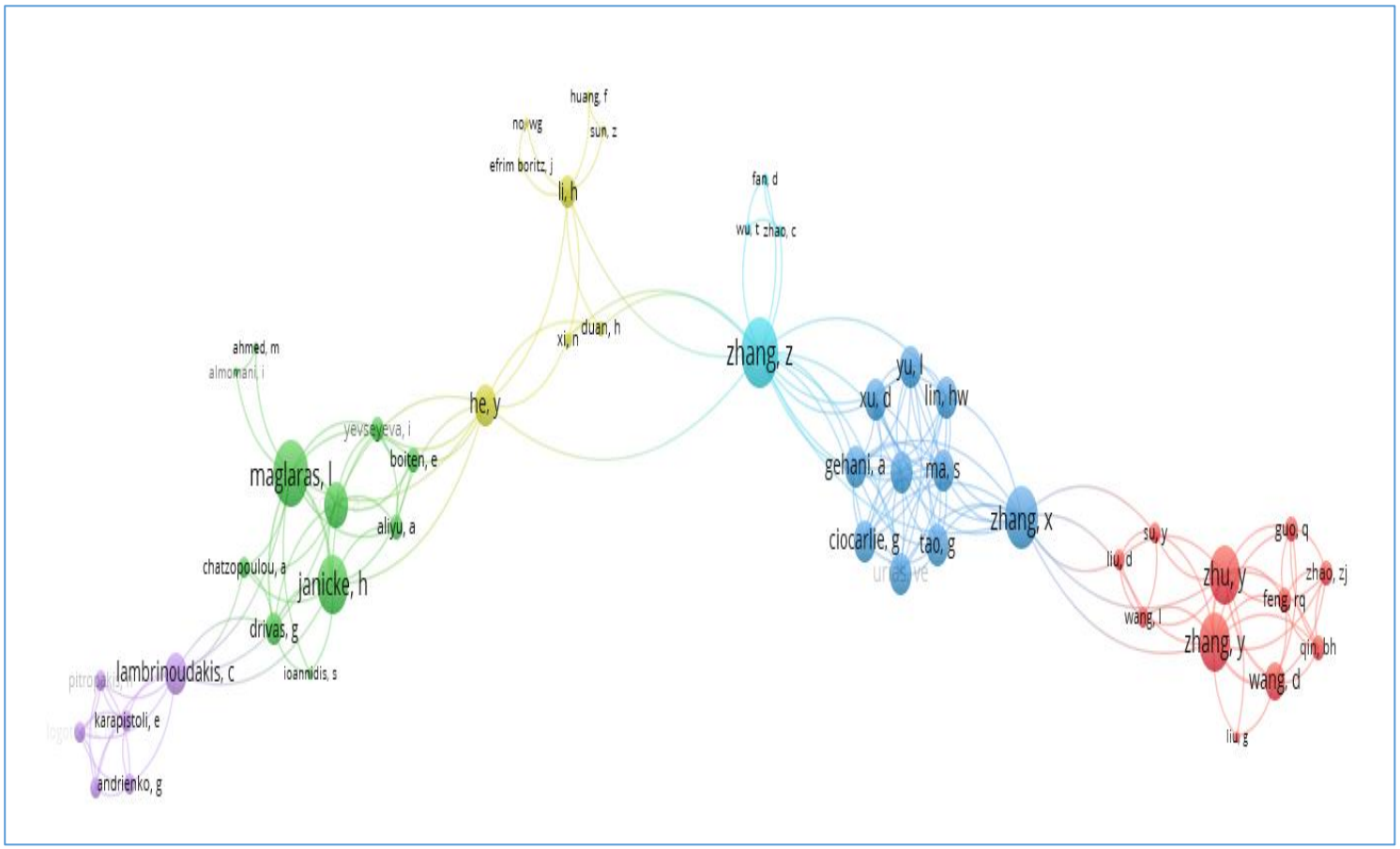
Además, su investigación ha analizado las implicaciones económicas y financieras de la ciberseguridad, y ha desarrollado metodologías para evaluar la seguridad de infraestructuras

tecnológicas complejas. En conjunto, su trabajo ha enriquecido nuestra comprensión de la ciberseguridad y ha proporcionado valiosas perspectivas para enfrentar los desafíos emergentes en un mundo digitalmente conectado.

Red de Relacion de Autores

Dentro de las principales relaciones entre autores tenemos las que se visualizan en la Figura 6

Figura 6
Red de relación de Autores

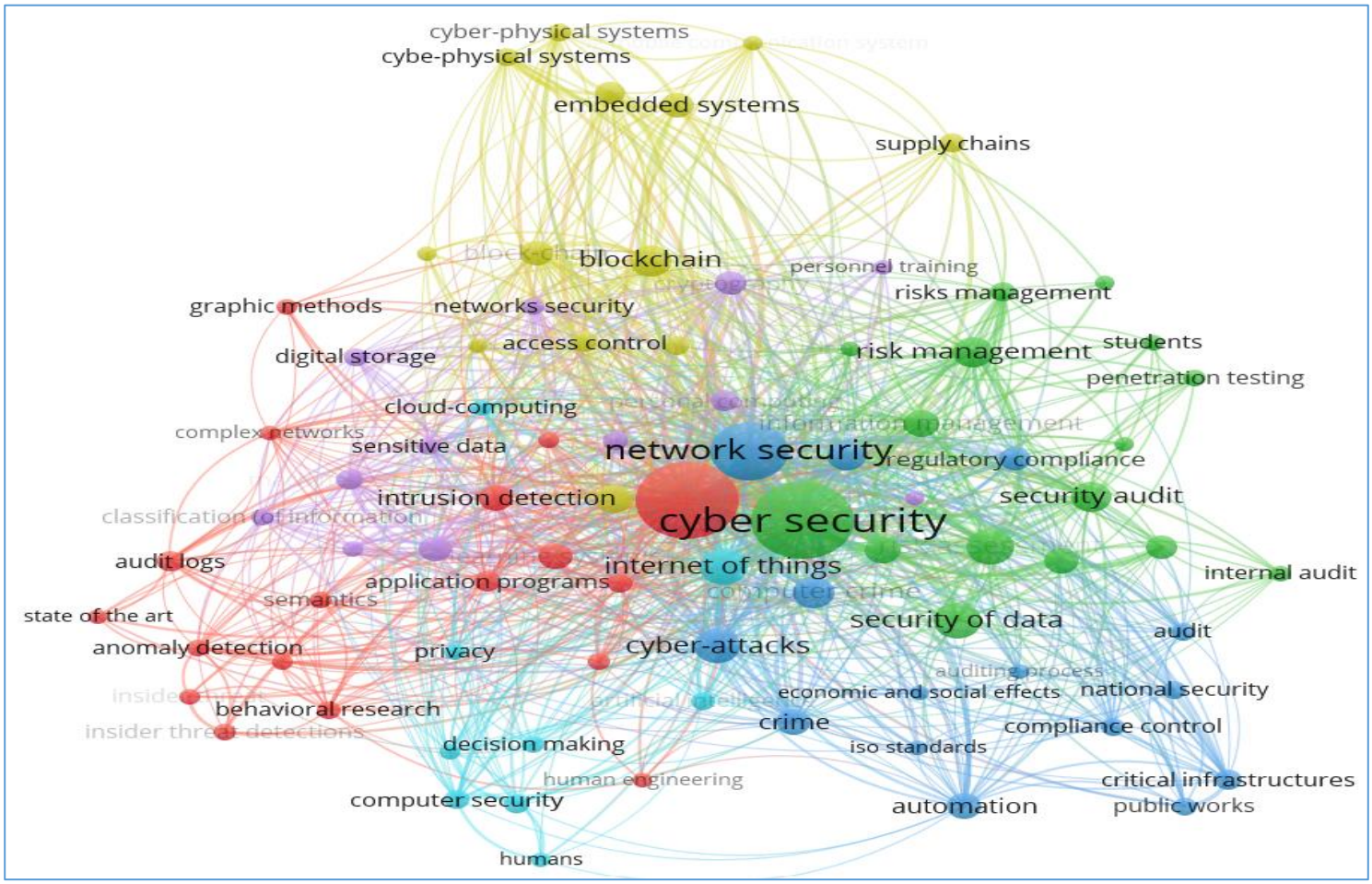


Fuente: Análisis de Datos Scopus en VOSviewer

La red de autores principales recalca su papel fundamental en la construcción y desarrollo del conocimiento en el área de la auditoría en ciberseguridad. Maglaras, Janicke, Zhang, Zhu y Zhang han sido referentes en la producción de investigaciones relevantes y de alta calidad en este ámbito, lo que ha llevado a un gran número de citaciones entre ellos.

Además, la diversidad de nacionalidades representadas por estos autores sugiere una colaboración intelectual internacional robusta, lo que enriquece aún más el panorama de investigación en auditoría en ciberseguridad. Estos aportes establecen un sólido eje de referencia para otros investigadores contribuyendo significativamente a la comprensión y avance de esta área de conocimiento.

Figura 7
Red de palabras claves



Fuente: Análisis de Datos Scopus en VOSviewer

La figura 7 nos muestra cómo las palabras clave "auditoría" y "ciberseguridad" están muy relacionadas con áreas de investigación vitales en el mundo empresarial y tecnológico. Estas áreas incluyen la protección de datos, redes, el Internet de las cosas (IoT) y registros de auditoría, entre otras. Esto nos hace ver la importancia de abordar la seguridad desde diferentes ángulos y trabajar en equipo.

La seguridad de datos y redes nos ayuda a proteger nuestra información, mientras que el IoT nos desafía a mantener la seguridad y privacidad en un mundo cada vez más conectado. Los registros de auditoría son como nuestros detectives digitales, vigilando constantemente cualquier actividad sospechosa en nuestros sistemas.

Esto nos recuerda que es crucial invertir en medidas de seguridad preventivas y desarrollar estrategias sólidas de auditoría. Además, nos enseña que trabajar en colaboración, tanto entre profesionales de la auditoría como de la ciberseguridad, es clave para enfrentar los desafíos que surgen en el mundo empresarial digital.

Discusión

Dentro de los principales resultados obtenidos en la investigación se establece el crecimiento que las publicaciones científicas relacionadas con la auditoría en Ciberseguridad han tenido desde el año 2020 hasta el año 2023, marcando una tendencia creciente en seguridad digital. La auditoría en ciberseguridad se relaciona con varias áreas del conocimiento dentro de las cuales podemos encontrar: ciencias de la computación, ingeniería, ciencias de la decisión, negocios, matemática y ciencias sociales. Esta diversidad temática indica que la auditoría en ciberseguridad es un campo interdisciplinario, abarcando diversos aspectos técnicos, administrativos y estratégicos necesarios para una protección integral de la información.

Dentro de los autores con mayor numero de citaciones se encuentran Maglaras, Janicke, Zhang, Zhu y Zhang cuyos aportes bibliográficos marcan el avance de la auditoría en ciberseguridad. Sus investigaciones han sido referenciadas ampliamente, demostrando la solidez y el impacto de sus contribuciones.

Por lo expresado anteriormente es importante resaltar la relación que existe entre "auditoría" y "ciberseguridad" mismas que al ser analizadas desde múltiples perspectivas aportan un enfoque holístico y colaborativo a favor de las empresas, mismas que al invertir en medidas de seguridad preventivas y desarrollar estrategias de auditoría sólidas garantizan seguridad para sus clientes.

Conclusiones

El desarrollo tecnológico, ha cambiado los riesgos y vulneraciones con las que las empresas se exponen diariamente, ante estos cambios es importante realizar la protección de recursos físicos y digitales mediante estrategias claras de ciberseguridad.

Dentro de los principales riegos que pueden afectar a las empresas se encuentran los accesos no autorizados, ciberataque, sustracción de información confidencial, alteración de datos, exposición de información entre otros que van ligados a la vulneración de información. La ciberseguridad que facilita la protección de datos ante amenazas digitales. Las empresas dentro de su estrategia digital deben establecer mecanismos para garantizar a sus clientes el correcto uso, autorización y acceso a sus datos personales.

La auditoría en ciberseguridad consiste en un proceso organizado para revisar y evaluar la seguridad en las empresas, permitiendo detectar cualquier debilidad y cumplir adecuadamente las políticas establecidas.

Dentro del proceso para realizar una auditoría en ciberseguridad es importante establecer los enfoques a los aspectos críticos que poseen las organizaciones, de este modo se puede medir la efectividad de los controles de seguridad, cumplimientos de procesos y normativas de protección que las organizaciones poseen dentro de su estructura empresarial.

El investigador Fernando Pérez en su obra "Análisis bibliométrico de la competitividad en el sector manufacturero del Ecuador" determina que el análisis bibliométrico, facilita la comprensión integrar de un a área de estudio mediante el conocimiento de las fuentes, autores y citaciones que este posee durante un determinado periodo de tiempo (2023, p.10).

Mediante un estudio bibliométrico, se determinó los principales autores, fuentes bibliográficas y áreas de conocimientos vinculados a la auditoría en ciberseguridad, esto brinda un punto de partida para futuras investigaciones sobre esta temática de alto impacto a nivel internacional.

Entre los años con mayores números de publicaciones científicas de alto impacto se encuentran el 2023, 2022 y 2020 mismos que demuestran al auge y relevancia que la auditoría en ciberseguridad posee. Conjuntamente es importante resaltar que el número de fuentes bibliográficas que existen hasta la presente investigación es de 328.

Dentro de la Figura 4 se visualizan las áreas temáticas en las que se han realizado investigaciones sobre la auditoría en ciberseguridad, entre las cuales corresponde a ciencias de la computación; ingeniería; ciencias de la decisión; negocios; matemática y ciencias sociales.

Entre los principales autores que han publicado sobre la auditoría en ciberseguridad se encuentran: Maglaras, Calvo Manzano, Janicke, Sabillón, Standford, Adhikari, Antonucci,

Arjipova, Aschbacher y Bansal quienes han marcado de forma positiva con sus aportes científicos sobre esta área de estudio que es de gran relevancia para el desarrollo empresarial.

La figura 6 establere la red de relación en citaciones de autores siendo los más relevantes Maglaras, Janicke, Zhang, Zhu y Zhang. Los aportes bibliográficos de estos autores han marcado de forma significativa las investigaciones en el área de la auditoría en ciberseguridad mediante las citaciones y referenciaciones de sus obras.

La figura 7 muestra la relación entre "auditoría" y "ciberseguridad" en áreas clave como la protección de datos, redes, IoT y registros de auditoría, resaltando la importancia de abordar la seguridad desde múltiples perspectivas y colaborar en equipo. Subraya la necesidad de invertir en medidas de seguridad preventivas y desarrollar estrategias de auditoría sólidas, destacando la colaboración entre profesionales de auditoría y ciberseguridad como crucial para enfrentar los desafíos del entorno empresarial digital.

Se sugiere continuar realizado investigaciones sobre la auditoría en ciberseguridad, ligadas a su implementación en las empresas, un análisis exhaustivo de los riesgos digitales que afectan a las organizaciones y la importancia de esta área de estudio.

Referencias bibliográficas

Ávila-Gutiérrez, M. J. (2023). Revisión sistemática de Lean 4.0 para el desarrollo de auditorías en las PYMES andaluzas. Universidad de Sevilla, 676-688. https://idus.us.es/handle/11441/153203

Castillo Nevárez , N. (2023). PEDIMENTOS ADUANALES CON IDENTIFICADORES INEXACTOS: UNA REVISIÓN DE LITERATURA. IPSUMTEC, 52-78. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://ipsumtec.itmilpaalta.edu.mx/uploads/2023/03/Castillo-Nevarez.-ART.3.pdf

Coha Escalante, J. M., & Barraza Mármol, R. A. (2022). La auditoría forense ante el fraude por corrupción en el sector público: una revisión teórica. Revista InveCom, 1-9. https://doi.org/https://doi.org/10.5281/zenodo.10975732

Duchitanga Plasencia, Á. E. (2024). La auditoría forense: un análisis integral desde una perspectiva conceptual y metodológica. Revista Metropolitana De Ciencias Aplicadas, 129 - 141. https://doi.org/https://doi.org/10.62452/jpjbrs16

Guevara Vega, E. M., & Delgado Deza, J. R. (2023). Estado actual de la Auditoría de base de datos: Beneficios y Tecnologías emergentes. Scielo. https://doi.org/https://doi.org/10.56469/rcti.v21i27.884

Jurado Zambrano, D. A., & Armijo Perea, J. D. (2022). La efectividad de la auditoría interna en el sector público. Dialnet, 8-20. https://dialnet.unirioja.es/servlet/articulo?codigo=8706462

Liu, Z., & Li, B. (2024). E-healthcare application cyber security analysis using quantum machine learning in malicious user detection. Optical and Quantum Electronics, 56, 476. https://doi.org/10.1007/s11082-023-05854-x

Lizárraga Caipo, Y. G., & Mendoza de los Santos, A. C. (09 de Septiembre de 2022). Impacto de la auditoría informática en las organizaciones: Una revisión bibliográfica. INGENIERÍA INVESTIGA, 4. https://doi.org/https://doi.org/10.47796/ing.v4i0.638

Lozano Almansa, J. M. (2023). Auditoría pública y nuevas tecnologías de la información: una revisión sistemática de la literatura. Segunda parte (tecnologías emergentes). REVISTA AUDITORÍA PÚBLICA, 458 - 510. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://asocex.es/wp-content/uploads/2024/05/04-AUDITORÍA-PUBLICA_.pdf

Minaya Macias, M. M., & Minaya Macias, R. W. (2023). Normas y estándares en auditoría: una revisión de su utilidad en la seguridad informática. Revista Científica Arbitrada Multidisciplinaria PENTACIENCIAS, 588 - 599. https://doi.org/https://doi.org/10.59169/pentaciencias.v5i4.700

Moran Olvera, B. M., & Chávez Cujilán, Y. T. (2021). Auditoría de Sistemas Automatizados. Multidisciplinar, 49-64. https://doi.org/https://doi.org/10.53734/mj.vol3.id168

Obaid, Z., & Alheeti, K. (2024). Comprehensive Study of Side-Channel Analysis (CyberSecurity). International Conference on Developments in eSystems Engineering, 794 - 799. https://doi.org/10.1109/DeSE60595.2023.10469635

Ochoa Diez, M., & Sepúlveda Arcila, E. (2022). La auditoría forense desde una revisión conceptual, metodológica y empírica. Revista Visión Contable, 153–168. https://doi.org/https://doi.org/10.24142/rvc.n25a8

Pérez Sisa, F. G. (10 de Octubre de 2023). Análisis bibliométrico de la competitividad en el sector manufacturero del Ecuador. ERUDITUS, 1-25. https://doi.org/https://doi.org/10.35290/re.v4n3.2023.1060

Piminchumo Olivos, G. E., & García Rodríguez, J. R. (2024). Beneficios del uso de tecnologías en auditorías contables: Una revisión sistemática de la literatura. Revista De Investigación Multidisciplinaria CTSCAFE. https://www.ctscafe.pe/index.php/ctscafe/article/view/209

Pole, K. (2023). Diseño de metodologías mixtas. Una revisión de las estrategias para combinar metodologías cuantitativas y cualitativas. ITESO, 9-10. http://hdl.handle.net/11117/252

Ríos Reyes, J. A., & Vásquez Chiclayo, R. Y. (2023). MÉTODOS EMERGENTES DE AUDITORÍA EN INTEGRIDAD DE DATOS EN LA NUBE: UNA REVISIÓN

SISTEMÁTICA DE LAS ÚLTIMAS TENDENCIAS. Scielo. https://doi.org/https://doi.org/10.23881/idupbo.023.1-8i

Rosales Troya, E. A., & Ordóñez Parra, Y. L. (2023). Desafíos éticos en la integración de tecnologías emergentes en la auditoría financiera. Revista Electrónica De Ciencias Gerenciales, 455 - 472. https://doi.org/https://doi.org/10.35381/gep.v6i1.109

Usman, A., & Ayoib, C.-A. (2024). The Role of Internal Auditors Characteristics in Cybersecurity Risk Assessment in Financial-Based Business Organisations: a Conceptual Review. Revista De Gestão Social E Ambiental. https://doi.org/https://doi.org/10.24857/rgsa.v18n6-008

Vishnevsky, A. (2024). SONIFICATION OF INFORMATION SECURITY EVENTS IN AUDITORY DISPLAY: TEXT VOCALIZATION, NAVIGATION, AND EVENT FLOW REPRESENTATION. Journal of Accessibility and Design for All, 131. https://doi.org/10.17411/jacces.v12i1.359

Viteri Hernández, C., & Ávila, D. (2024). Exploración integral de la seguridad en redes de proveedores de servicios de internet: Una revisión sistemática de literatura. Perspectiva, Febrero. https://doi.org/https://doi.org/10.47187/perspectivas.6.1.215

Conflicto de intereses:

Los autores declaran que no existe conflicto de interés posible.

Financiamiento:

No existió asistencia financiera de partes externas al presente artículo.

Nota:

El artículo no es producto de una publicación anterior.