ISBN: 978-628-96613-0-9. ISSN: 2414-6390. Digital Object Identifier: https://dx.doi.org/10.18687/LEIRD2024.1.1.584

ISO 27001 for Information Security Management: A Systematic Review in Latin America

Lourdes Alisson Sulca Hinostroza, Bachiller en Ingeniería Industrial[1], Ishel Harumi Idme Medina, Bachiller en Ingeniería Industrial[1] y Guillermo Segundo Miñan Olivos, Magister en Gestión Pública[1]
[1]Universidad Privada del Norte, Perú, N00244877@upn.pe, N00242310@upn.pe, guillermo.minan@upn.pe

Abstract*– The main objetive of the research was to carry out a systematic review of the literature from 2013-2024, with the purpose of evaluating the effectiveness of the implementation of ISO 27001 in Latin American corporations to mitigate exposures to hazards in the protection of the information. The PRISMA methodology was used to search and select sources such as: Dialnet, Google Scholar, IEEE Xplore, Redalyc, Scielo and Scopus. Initially, 19,000 results were generated, which were reduced to 886 studies after the implementation of search strategies. Then, by applying selection and discard criteria, 23 articles were chosen for evaluation. Consequently, the bibliometric results showed that the studies were published in a greater number in 2022, English language and 46% refer to Scopus. Among the main tools identified we can mention: ISO 27001, PDCA, software, among others. The main effect identified was the reduction of data protection incidents, regulatory compliance, as well as the cost of implementation. Finally, it can be concluded that there are results between 2013-2024 that demonstrate the implementation of the regulations.

Keywords*-- ISO 27001, information security, cybersecurity, risk mitigation, data protection.

Digital Object Identifier: (only for full papers, inserted by LEIRD).
ISSN, ISBN: (to be inserted by LEIRD).
DO NOT REMOVE

ISO 27001 para la gestión de la seguridad de la información. Una revisión sistemática en Latinoamérica

Lourdes Alisson Sulca Hinostroza, Bachiller en Ingeniería Industrial[1], Ishel Harumi Idme Medina, Bachiller en Ingeniería Industrial[1] y Guillermo Segundo Miñan Olivos, Magister en Gestión Pública[1]
[1]Universidad Privada del Norte, Perú, N00244877@upn.pe, N00242310@upn.pe, guillermo.minan@upn.pe

Resumen– El objetivo principal de la investigación fue llevar a cabo una revisión sistemática de la literatura desde 2013-2024, con el propósito de evaluar la eficacia de la implementación de la ISO 27001 en corporaciones latinoamericanas para mitigar las exposiciones a los peligros en la protección de la información. Se utilizó la metodología PRISMA para la búsqueda y selección de fuentes como: Dialnet, Google Académico, IEEE Xplore, Redalyc, Scielo y Scopus. Inicialmente, se generaron 19,000 resultados, los cuales se redujeron a 886 estudios tras la implementación de estrategias de búsqueda. Luego, mediante la aplicación de criterios de selección y descarte, se escogieron 23 artículos para su evaluación. Por consiguiente, los resultados bibliométricos demostraron que los estudios se publicaron en una mayor cantidad en 2022, idioma inglés y el 46% se refiere a Scopus. Entre las principales herramientas identificados se puede mencionar: ISO 27001, PDCA, software, entre otros. El principal efecto identificado fue la reducción de incidentes de protección de datos, la conformidad de la normativa, además del costo de la implementación. Finalmente, se puede concluir que existe resultados entre el 2013-2024 que demuestra la implementación de la normativa.

Palabras clave-- ISO 27001, seguridad de la información, ciberseguridad, mitigación de riesgos, protección de datos.

I. Introducción

Actualmente, las empresas enfrentan constantes riesgos operativos que pueden afectar su estabilidad y reputación. También, se subrayan que un proceso continuo alineado con ISO 27001 es crucial para gestionar la protección de datos, implicando etapas de Planificación, Ejecución, Verificación y Acción. Según [1] refuerzan la importancia del ciclo PDCA para establecer un marco de control interno que mitigue amenazas y proteja los datos, permitiendo una gestión proactiva y adaptable ante los desafíos de seguridad. Por otro lado, se añaden que la participación de todos los niveles organizacionales es vital para la implementación efectiva de estas medidas.

De igual modo, enfatizan que una adecuada administración de riesgos permite manejar puntos débiles y peligros, dotando a la empresa de medios para proteger sus recursos informativos. Empleando las palabras de los autores, implementar medidas preventivas y correctivas asegura la defensa de estos recursos contra incidentes y ataques cibernéticos, lo que no solo garantiza la continuidad operativa y la fidelidad de los clientes, sino también el cumplimiento de leyes y estándares actuales. Por lo cual, realizar un análisis exhaustivo del riesgo cibernético antes de implementar medidas de mitigación es fundamental para evaluar la seguridad de la organización [2].

En el entorno empresarial actual, la decisión estratégica de establecer un sistema de administración de protección de datos es esencial para cualquier compañía, ya que no solo se basa en las metas y exigencias de la organización. Asimismo, en el ámbito del SGSI, la implementación de un sistema de gestión de la seguridad de la información es una decisión estratégica crucial para cualquier entidad; su planificación y ejecución dependen de los objetivos y necesidades específicos, los protocolos de seguridad requeridos, los procedimientos internos, y la estructura de la entidad [3].

Respondiendo a la evidencia internacional, el informe semestral sobre la perspectiva mundial de riesgos, preparado por FortiGuard Labs, revela que en América Latina y el Caribe se documentaron más de 360 mil millones de intentos de ciberataques en 2022, siendo México el país más afectado con 187 mil millones, seguido por Brasil con 103 mil millones, Colombia con 20 mil millones y Perú con 15 mil millones. Este notable aumento en los intentos de ataques cibernéticos en los últimos años evidencia la magnitud del problema generando preocupación por la seguridad informática en la región, ya que afecta significativamente la protección de nuestra información personal y empresarial [4].

A nivel nacional, los Chief Information Security Officers (CISO) juegan un papel crucial en la protección de datos y la gestión de riesgos de seguridad informática en EY Perú. Según una encuesta realizada por [5], los CISO en el país enfrentan obstáculos como presupuestos limitados, una regulación fragmentada y falta de alineación con otros líderes empresariales. La encuesta reveló que el 51% de los CISO peruanos reportaron un aumento en los ataques cibernéticos disruptivos desde 2020, y el 63% expresó gran preocupación por la capacidad de sus empresas para gestionar estas amenazas. Por lo tanto, se subraya la importancia de invertir en ciberseguridad y fomentar una mayor colaboración empresarial para abordar estos desafíos, destacando la urgencia de mejorar las prácticas de ciberseguridad y adoptar medidas decisivas para proteger nuestros datos.

En el contexto de la seguridad de los datos empresariales, adoptar la norma ISO 27001 es esencial para proteger los activos informativos frente a amenazas. Por ello, implementar esta norma se convierte en una tarea prioritaria, ya que permite

evaluar fortalezas y vulnerabilidades en diversas organizaciones y proponer estrategias para reducir el riesgo de amenazas que explotan debilidades en la estructura organizacional [6].

Al revisar la literatura existente, se observa que se ha prestado considerable atención a los beneficios generales de adoptar la normativa para el fortalecimiento de la seguridad de los datos y el cumplimiento de las normas. Sin embargo, al profundizar en la relación específica entre la implementación de la ISO 27001 y la mitigación de riesgos en el contexto latinoamericano, se identifica un vacío en la literatura. Pocos estudios han examinado exhaustivamente cómo esta norma influye directamente en la reducción de riesgos. Esta escasez de investigación deja un espacio para explorar cómo las empresas en esta región pueden aprovechar mejor la normativa como un recurso eficaz para gestionar adecuadamente las amenazas relacionadas con la salvaguarda de datos y fortalecer la protección de la información confidencial.

Teniendo en cuenta lo expuesto previamente, el propósito de este análisis fue examinar la siguiente pregunta de investigación en profundidad ¿Qué evidencias empíricas existen sobre la ISO 27001 para mitigar riesgos en la Seguridad de la Información en empresas Latinoamericanas entre el 2013 - 2024?

II. Metodología

Esta investigación se fundamenta en un enfoque cuantitativo con el propósito de llevar a cabo un análisis detallado y exhaustivo de la literatura asociada con la metodología PRISMA. En palabras de [7] las revisiones sistemáticas son análisis de estudios primarios realizados de manera reproducible mediante métodos explícitos, un ejemplo conocido de este enfoque de investigación es el modelo PRISMA.

Asimismo, respecto a la evaluación de criterios (Tabla I) se utilizó los lineamientos establecidos por el método LIA y se procesó la información de la siguiente manera: tabulación de datos en Excel y clasificación de los resultados en ejes bibliométricos y temáticos [32]. Esta metodología permitió generar un análisis de herramientas aplicadas y de los hallazgos más importantes del estudio [33].

En este contexto, la investigación analizó la estrategia de ISO 27001 en empresas desde 2013-2024, desde una perspectiva bibliométrica y examinando los temas abordados en estudios pertinentes. Por lo tanto, [8] mencionan que es una guía destacada para informar sobre el uso de protocolos en investigaciones de revisiones sistemáticas, esto promueve el consenso, garantiza la capacidad de reproducir los resultados y evita distorsiones en la interpretación de las variables durante el análisis.

Como herramienta de gestión bibliográfica, se utilizó Zotero. Zotero es un software de gestión de referencias bibliográficas que facilita la recopilación, organización, citación y compartición de fuentes de información. Permite guardar información de documentos y páginas web, organizar referencias en carpetas, sincronizar la biblioteca en varios dispositivos, insertar citas y crear bibliografías en múltiples estilos, y compartir referencias para colaborar en proyectos. Es una herramienta gratuita y de código abierto, accesible para todos, con una interfaz intuitiva y compatible con otros sistemas de gestión de referencias, lo que la convierte en una opción esencial para investigadores y estudiantes.

Asimismo, se hizo uso de una extensa variedad de fuentes de datos, las cuales abarcaron una serie de bases de datos pertinentes y reconocidas en el ámbito académico y científico, tales como: Dialnet, Google Académico, IEEE Xplore, Redalyc, Scielo y Scopus. Para asegurar la exhaustividad de la búsqueda, se emplearon palabras clave específicas como “ISO 27001”, “mitigación de riesgos”, “seguridad de la información”, “empresas latinoamericanas”, “ciberseguridad”, “amenazas”, “salvaguarda de información”, “identificación de riesgos” y “auditoría”. Es importante destacar que únicamente se consideraron estudios publicados en el período comprendido entre 2013 y 2024, con el fin de garantizar la actualidad y relevancia de los datos recopilados.

Al principio, se identificaron aproximadamente 11,000 estudios relacionados con la variable ISO 27001. Tras aplicar las estrategias de búsqueda adecuadas, se redujo este número a alrededor de 886 investigaciones de las revistas seleccionadas. Todos los artículos seleccionados se exportaron a una hoja de cálculo desde Zotero para proseguir con el proceso de inclusión y exclusión.

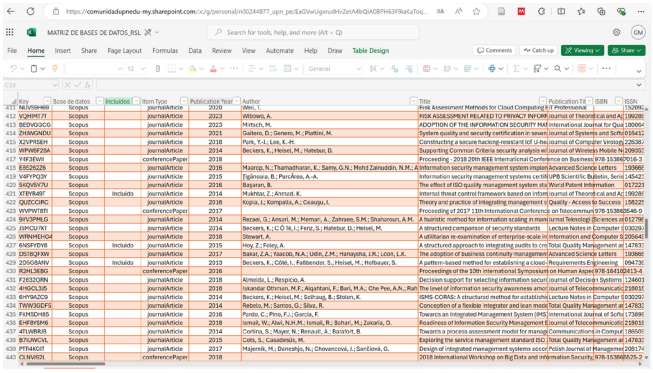

Fig. 1 Información bibliométrica de artículos exportados desde Zotero

Seguidamente, se implementaron criterios más rigurosos para la inclusión o exclusión de estudios. Después de la fase inicial de búsqueda, se centró la atención exclusivamente en la selección de documentos primarios, artículos publicados en revistas científicas, libros académicos y actas de congresos que estuvieran alineados con el título de la RSL. Se tomaron en consideración investigaciones procedentes de plataformas como Dialnet, Google Académico, IEEE Xplore, Redalyc, Scielo y Scopus. Además, se hizo hincapié en que estos documentos abordaran exhaustivamente las variables de interés y sus términos relacionados, analizando ambas ediciones en inglés como en español de los artículos. Se enfatizó la inclusión únicamente de aquellos estudios disponibles en acceso abierto, dentro del ámbito de la ingeniería y con ISSN, provenientes específicamente de países latinoamericanos. En relación con la

pregunta de investigación, se optó exclusivamente por aquellos estudios que ofrecieran evidencia cuantitativa relevante sobre el tema en cuestión. Los criterios para la inclusión y exclusión de los artículos se pueden visualizar en la Tabla I:

TABLA I
CRITERIOS APLICADOS PARA LA SELECCIÓN DE ESTUDIOS

1	El título o el resumen tiene relación con la problemática
2	La fecha de publicación corresponde entre el año 2013 a 2024.
3	El idioma corresponde a: inglés o español
4	El artículo debe estar en acceso abierto.
5	Los artículos incluyen palabras clave asociadas a la pregunta
6	Los artículos deben evidenciar un hallazgo empírico o práctico. No se incluyen estudios teóricos, descriptivos u otras revisiones
7	Los artículos aplican herramientas de ingeniería.

Una vez que se aplicaron meticulosamente los criterios de selección y exclusión, se detectó un número total de 23 investigaciones apropiadas para su análisis exhaustivo. Para recopilar la información pertinente de manera sistemática, se utilizó una hoja de cálculo especializada, donde se registraron una amplia gama de aspectos bibliométricos de cada estudio, abarcando desde el nombre completo del autor hasta el idioma de publicación, entre otros datos de relevancia. Dicho lo anterior, se llevó a cabo la labor de organizar y tabular minuciosamente el contenido de los estudios mediante el uso de tablas dinámicas, permitiendo así una visualización estructurada y detallada de la información recabada. Por último, se procedió a realizar una evaluación exhaustiva de los resultados obtenidos en los artículos seleccionados, con el objetivo primordial de demostrar de manera inequívoca la eficacia y la relevancia de la implementación de la norma ISO 27001 en el ámbito investigativo y práctico.

III. RESULTADOS

Los resultados se categorizaron en dos ejes: uno bibliométrico y otro de contenido. El análisis bibliométrico facilitó la descripción de los estudios seleccionados, mientras que el análisis de contenido permitió identificar aspectos relacionados con la ingeniería.

A. Resultados Bibliométricos

La enumeración de los autores y títulos de las revisiones sistemáticas que abarcan desde 2013 hasta 2024, enfocadas en las palabras clave "ISO 27001" y "mitigación de riesgo" se presenta en la Tabla II. Dicha tabla permite identificar adecuadamente cada uno de los estudios extraídos en el proceso final de la revisión. Estos estudios fueron seleccionados utilizando la herramienta Zotero.

La herramienta de Zotero no solo funcionó como gestor de referencias, sino que también permitió la revisión eficiente de los estudios para su adecuada clasificación y exportación. De la misma manera, se asegura una trazabilidad de los estudios.

TABLA II
ARTÍCULOS INCLUIDOS EN LA REVISIÓN SOBRE LA ISO 27001 PARA LA MITIGACIÓN DE RIESGOS EN LA SEGURIDAD DE LA INFORMACIÓN

Autores	Título de la investigación
Akinyemi et al. [9]	SWOT analysis of information security management system ISO 27001
Angulo et al. [10]	Propuesta metodológica de seguridad de información para proveedores de servicios de internet en ecuador
Antunes et al. [11]	A Client-Centered Information Security and Cybersecurity Auditing Framework
Arce [12]	Análisis de los riesgos por mitigar a través de la auditoría en operaciones electrónicas en Paraguay al 2022
Ávalos et al. [13]	Trazabilidad de operaciones en base de datos para mitigar riesgos en los procesos de auditoría
Brenner et al. [14]	Better Safe Than Sorry: Risk Management Based on a Safety-Augmented Network Intrusion Detection System
Barafort et al. [15]	Integrating risk management in IT settings from ISO standards and management systems perspectives
Beckers et al. [16]	A pattern-based method for establishing a cloud-specific information security management system: Establishing information security management systems for clouds considering security, privacy, and legal compliance
Chandra et al. [17]	Information Security Risk Assessment Using Situational Awareness Frameworks and Application Tools
Duarte y Monges [18]	Análisis de una metodología de Seguridad de la Información basados en los estándares ISO 27001
Hoy y Foley [19]	A structured approach to integrating audits to create organisational efficiencies: ISO 9001 and ISO 27001 audits
Kamil et al. [20]	Information security objectives and the output legitimacy of ISO/IEC 27001: stakeholders' perspective on expectations in private organizations in Sweden
Llanten et al. [21]	Validation of Cybersecurity Framework for Threat Mitigation
Morales et al. [22]	Sistemas de gestión de seguridad de la información para empresas KPO: una aproximación
Moreno y Coronado [23]	Modelo base de conocimiento para auditorías de seguridad en servicios web con inyección SQL
Mukhtar y Ahmad [24]	Internal threat control framework based on information security management system
Phirke y Ghorpade [25]	Best practices of auditing in an organization using ISO 27001 standard
Podrecca y Sartor [26]	Forecasting the diffusion of ISO/IEC 27001: a Grey model approach
Razikin [27]	Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework
Ruiz et al. [28]	Implementation of Information Security Audit for the Sales System in a Peruvian Company
Țigănoaia [29]	Some aspects regarding the information security management system within organizations - Adopting the ISO/IEC 27001:2013 standard
Yungán y Narváez [30]	Aplicación de la Norma ISO 27001 para la seguridad de los Sistemas de Información
Zaini et al. [31]	A conceptual overview on the relationship between information security practices and organizational agility

Una vez que los estudios han sido descritos, según su información bibliométrica, se organizaron y clasificaron según su año de publicación, el idioma de publicación, el país de publicación y según la base de datos utilizada.

Un gráfico lineal representa la organización de aquellos artículos seleccionados en la revisión sistemática de acuerdo con su año de publicación. En el eje horizontal se encuentran los años del período analizado, y en el eje vertical se presenta la cantidad de artículos seleccionados. Se observa un incremento continuo en el número de artículos publicados anualmente, alcanzando un pico significativo en 2022, lo que podría indicar un mayor interés o avances en el tema estudiado en la Fig. 2.

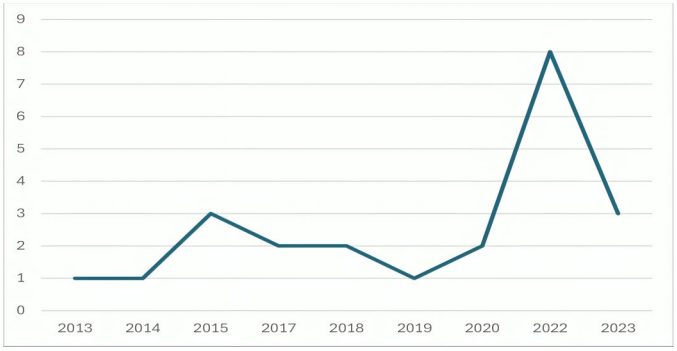

Fig. 2 Año de publicación de los artículos incluidos en la RSL.

Un gráfico de anillo que proporciona una representación visual según el idioma de publicación. Cada segmento del anillo representa un idioma específico, y el tamaño de cada segmento corresponde a la cantidad de artículos publicados en ese idioma en la Fig. 3:

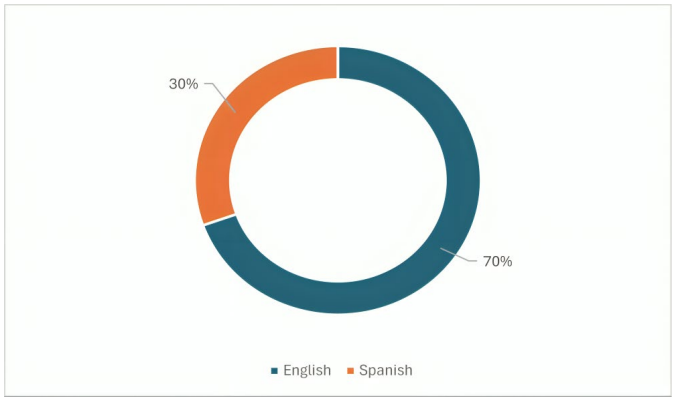

Fig. 3 Idioma de publicación de los artículos incluidos en la RSL.

Un mapa donde cada país está coloreado de manera diferente, indicando la cantidad de artículos seleccionados en la revisión sistemática. Por lo cual, Colombia, Paraguay y Ecuador son los países más oscuros, lo que sugiere que tiene la mayor cantidad de artículos seleccionados según la escala. Asimismo, el país de Perú tiene tonos más claros, lo que indica menos artículos seleccionados en la Fig. 4:

Fig. 4 Países de los artículos incluidos en la RSL.

En la Fig. 5 es un gráfico circular donde esta representación visual muestra la distribución porcentual de las fuentes de información; se visualiza que Scopus representa por el segmento más grande con un 61% del total siendo la base de datos más utilizada en esta revisión sistemática con casi la mitad de los artículos elegidos. Pero, Redalyc e IEEE Xplore tienen el mismo y menor porcentaje del 4% siendo la menos utilizada.

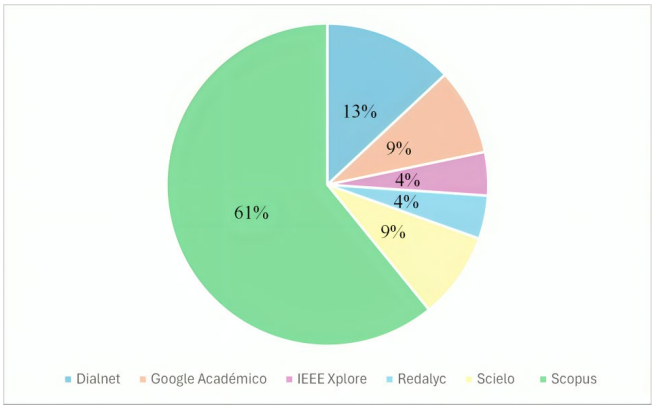

Fig. 5 Base de datos de los artículos incluidos en la RSL.

B. Resultados de Contenido

En la Tabla III, se presentan las herramientas de ingeniería asociadas a la ISO 27001, según los artículos incluidos en la revisión sistemática. Las empresas utilizan ISO 27001 para auditar múltiples sistemas de seguridad de datos, realizando autodiagnósticos y medidas de mitigación, y evaluando transacciones electrónicas con Normas Internacionales de Auditoría; la metodología PDCA facilita la planificación y evaluación de riesgos, alineada con ISO 27001, y la participación de todos los niveles organizacionales es vital; SmartPLS y MAXQDA se usan para el análisis de datos, ProPAn para la administración de seguridad en la nube, Blockchain para garantizar la integridad de los datos, y SQL para prevenir inyecciones; los sistemas de detección de intrusos (IDS) protegen redes al detectar incidentes, y el análisis FODA evalúa puntos fuertes y riesgos del SGSI.

TABLA III
HERRAMIENTAS DE INGENIERÍA O ADMINISTRATIVAS ASOCIADAS A LA ISO 27001 SEGÚN LOS ARTÍCULOS INCLUIDOS EN LA REVISIÓN

Herramientas	Aplicación de la herramienta	Indicadores o Mediciones
Auditoría	Las empresas prefieren usar un único SGSI para auditar múltiples sistemas de seguridad de datos. [11] mencionan que la auditoría inicial implica un autodiagnóstico y medidas de mitigación, mientras que las posteriores evalúan su impacto. [12] sugiere auditar transacciones electrónicas en Paraguay con Normas Internacionales de Auditoría para detectar fraude. [13] destacan la auditoría en Oracle, dividiéndola en revisión de componentes y verificación de acciones. [17] señalan que la auditoría incluye recopilación de información, análisis de registros, inspecciones de campo y entrevistas. [19] resaltan la combinación de ISO 9001 e ISO 27001 para evaluar el cumplimiento con estándares. [25] se enfocan en las mejores prácticas del SGSI con referencia a ISO 27001. [28] subrayan la importancia de proteger la información del sistema de comercialización de Domínguez. [29] evalúa el cumplimiento de requisitos tras aplicar la guía SGSI.	Para medir la efectividad de las medidas de seguridad, es crucial considerar varios indicadores. [11] destacan el análisis global obtenido durante la auditoría para evaluar el impacto en la Seguridad de la Información. [12] manifiesta la tasa de detección y mitigación de riesgos como indicador. [13] sugieren la proporción de detección y resolución de anomalías. [17] manifiestan sobre la tasa de resolución de inconformidades. [19] utilizan el indicador de avance constante, comparando áreas de mejora identificadas en auditorías. [25] proponen la proporción del cumplimiento de normativas de protección de datos. [28] sugieren la proporción de problemas detectados y solucionados durante la auditoría del sistema de ventas. Finalmente, [29] refiere la proporción de requisitos cumplidos durante la auditoría de seguridad de la información.
Metodología PDCA	En el contexto de la seguridad de los datos empresariales, la planificación detallada de medidas de seguridad adaptadas a los proveedores es fundamental para proteger los activos informativos frente a amenazas. Así, [10] destacan que la recolección de datos sobre incidentes de seguridad proporciona una visión integral de las amenazas. De acuerdo con [15], la metodología PDCA facilita la integración de la administración de amenazas en TI desde los sistemas de gestión y estándares, promoviendo la interoperabilidad mediante un enfoque sistémico. [27] enfatizan que la evaluación de riesgos es crucial para identificar vulnerabilidades y proponer estrategias de mitigación. Además, [19] subrayan que un proceso continuo alineado con ISO 27001 es crucial para gestionar la protección de datos, implicando etapas de Planificación, Ejecución, Verificación y Acción. [24] refuerzan la importancia del ciclo PDCA para establecer un marco de control interno que mitigue amenazas y proteja los datos, permitiendo una gestión proactiva y adaptable ante los desafíos de seguridad. [31] añaden que la participación de todos los niveles organizacionales es vital para la implementación efectiva de estas medidas. Finalmente, [26] mencionan que este enfoque continuo de PDCA en la protección de datos es esencial para detectar amenazas, implementar medidas de seguridad, evaluar su eficacia y realizar ajustes necesarios, con [22] destacando la importancia de la retroalimentación constante para la mejora continua.	Para medir la efectividad de las medidas de seguridad implementadas, la tasa de incidentes de seguridad es un indicador clave. [10] sugieren que este indicador mide la frecuencia y gravedad de los incidentes, reflejando la eficacia de las medidas implementadas y mejorando la protección de datos y confianza de los usuarios. [15] refieren la proporción de incidentes de seguridad atendidos, que mide cuántos incidentes se gestionan adecuadamente respecto al total detectado, siendo un alto índice de mitigación de riesgos indicativo de una mejor capacidad para responder a amenazas. [18] introducen la proporción de requisitos satisfechos como un indicador que mide la alineación entre las expectativas de los involucrados y las acciones implementadas, donde una alta proporción indica una mejor optimización en la protección de datos. [27] agregan que la proporción de mejoras continuas en la gestión de protección de datos, comparando las mejoras implementadas con el total identificado en un período específico, sugiriendo un abordaje efectivo de amenazas. [24] evalúan la eficacia de las medidas a través de la proporción de incidentes evitados. [31] destacan la importancia de la proporción de cumplimiento normativo como un indicador de la eficacia en la implementación de medidas de seguridad. [26] examinan la proporción de empresas que adoptan medidas de protección de datos como un indicador que refleja la aplicación de prácticas de protección y la conciencia y defensa contra amenazas, y [22] plantean que el uso de encuestas de satisfacción para evaluar la percepción de seguridad entre los usuarios.
Software (SmartPLS)	El análisis exploratorio, confirmatorio y factorial se realizó con SmartPLS 3 y SPSS edición 24. La metodología SEM centrada en la varianza evaluó la relación entre protección de datos y adaptación empresarial, maximizando la varianza explicada de los constructos latentes [31].	La capacidad predictiva de las políticas de protección de datos sobre la flexibilidad organizacional se evalúa con SEM y PLS, mostrando cómo afectan la agilidad empresarial. Una alta capacidad predictiva indica una buena relación entre la protección de datos y la adaptabilidad [31].
Software (MAXQDA)	Es una herramienta esencial para el análisis cualitativo de texto y datos multimedia, que permite evaluar la credibilidad de hallazgos sobre empresas privadas en Suecia. Facilita la gestión y análisis de información textual, ayudando a comprender mejor las expectativas de los interesados y aportando valor a la investigación [20].	La efectividad en el análisis de datos con MAXQDA se basa en la capacidad de interpretar hallazgos para identificar pautas y tendencias relevantes. Esta interpretación de alta calidad permite extraer conclusiones sólidas que enriquecen el conocimiento sobre la protección de datos y la legalidad en empresas privadas [20].
Software (ProPAn)	El software ProPAn establece un sistema integral para la administración de protección de datos en la nube, abordando seguridad, privacidad y cumplimiento legal. Ofrece herramientas para identificar riesgos de privacidad y evaluar peligros en el almacenamiento virtual, facilitando la implementación de tácticas operativas que garantizan seguridad, confidencialidad y conformidad normativa [16].	El software ProPAn es una herramienta completa para la administración de seguridad en la nube. Proporciona soluciones preventivas para asegurar la integridad de los datos y el cumplimiento normativo. Su enfoque ágil permite una implementación eficaz de estrategias de seguridad en entornos de nube dinámicos [16].
Blockchain	Blockchain proporciona una red segura y controlada para usuarios autorizados, garantizando la integridad de los datos mediante algoritmos de consenso y criptografía avanzada, y se destaca como una solución confiable en diversos campos [21].	La proporción de usuarios autorizados en una red Blockchain se calcula comparando el número de usuarios con permisos adecuados con el total de intentos de acceso. Una alta tasa indica una gestión eficaz de permisos y una red segura, mientras que una baja tasa sugiere problemas en la administración de permisos que podrían comprometer la seguridad del sistema [21].

SQL	Para prevenir SQL Injection en APIs como JPA, es esencial evitar la concatenación de entrada de usuario en cadenas SQL y utilizar herramientas y análisis adecuados. Se busca establecer un patrón efectivo para proteger servicios en línea contra infiltraciones SQL [23].	La proporción de vulnerabilidades de inyección SQL en evaluaciones de seguridad refleja la gestión de riesgos. Una tasa alta indica una buena capacidad de respuesta, mientras que una baja señala posibles deficiencias en auditoría o seguridad, requiriendo ajustes para mejorar la protección [23].
Sistema de detección de intrusos (IDS)	La implementación de IDS avanza en la protección de redes al detectar incidentes, analiza riesgos y propone medidas preventivas y correctivas. Al vincular incidentes con amenazas potenciales en sistemas de control industrial (ICS), se fortalece la respuesta y la resiliencia frente a amenazas emergentes [14].	La eficiencia del sistema de detección de intrusos (IDS) se evalúa por la proporción de eventos detectados y solucionados correctamente frente al total de incidentes. Una alta proporción indica una buena gestión de riesgos, mientras que una baja revela debilidades en la detección o en las medidas [14].
FODA	Se evaluaron los puntos fuertes, débiles, oportunidades y riesgos del SGSI en reuniones con expertos en protección de datos. Se identificaron factores internos y externos que podrían afectar su desempeño, y los hallazgos fueron validados mediante encuestas y análisis estadísticos para determinar su importancia y prioridad [9]	La efectividad de los mecanismos de seguridad, el índice de eventos, la complacencia del usuario y la productividad en la administración de incidentes son indicadores clave para evaluar el Sistema de Gestión de Seguridad de la Información (SGSI), alineados con los objetivos y prioridades del análisis FODA [9]

En la Tabla IV, se presentan las herramientas asociadas a la ISO 27001, según los artículos en la revisión sistemática realizada entre los años 2013 y 2024 donde están los siguientes campos: autores, tipo, descripción y medición del efecto.

TABLA IV
HALLAZGOS O RESULTADOS OBTENIDOS RESPECTO A LA ISO 27001 SEGÚN LOS ARTÍCULOS INCLUIDOS EN LA REVISIÓN

Autores	Hallazgo	Descripción del Hallazgo	Síntesis del Hallazgo
Akinyemi et al. [9]	Falta de conocimiento	La falta de conocimiento en estándares ISO 27000 y técnicas de mejora limita la aplicación de los resultados del estudio, destacando la necesidad de una mejor comprensión.	Permite identificar fortalezas y debilidades del SGSI, y anticipar amenazas y oportunidades externas, mejorando la preparación y respuesta.
Angulo et al. [10]	Falta de implementación de medidas de seguridad de la información	La falta de seguridad en empresas de conectividad en Ecuador expone a riesgos cibernéticos, afectando datos y reputación.	La falta de seguridad en compañías de Internet en Ecuador destaca en el cumplimiento normativo y la satisfacción del cliente, revelando la necesidad de mejorar la protección de datos.
Antunes et al. [11]	Falta de auditoría	La falta de auditoría en las PYME, por recursos limitados, aumenta su vulnerabilidad a amenazas digitales.	Auditorías ineficientes aumentan vulnerabilidades y descontento. Mejorarlas refuerza la protección de datos.
Arce [12]	Por falta de adaptabilidad y respuesta a amenazas	La dependencia de la TI limita la adaptabilidad, y la seguridad de la información es crucial para enfrentar amenazas cibernéticas.	Buenas prácticas en seguridad de datos reducen vulnerabilidades, filtraciones e interrupciones, protegiendo la reputación y mejorando la agilidad.
Ávalos et al. [13]	Exposición a amenazas informáticas	En Paraguay, la deficiente gestión de riesgos cibernéticos destaca la urgencia de auditorías especializadas para proteger las transacciones electrónicas.	El análisis evalúa la reducción de eventos de seguridad, costos de gestión de riesgos y mejoras en eficacia operativa y satisfacción del cliente.
Brenner et al. [14]	Infracción de privacidad y acceso no autorizado	La falta de trazabilidad en bases de datos puede comprometer la seguridad de los datos. Para resolver esto, se propone usar auditoría en bases de datos Oracle para mejorar la privacidad y seguridad.	El impacto se refleja en la reducción de riesgos de privacidad y manejo indebido de datos, junto con mejoras en la detección, respuesta y prevención de amenazas a la información.
Barafort et al. [15]	Vulnerabilidades en sistemas de control	Las vulnerabilidades en sistemas de control industrial exponen redes a ataques remotos. El artículo sugiere usar un sistema de vigilancia de intrusiones para gestionar estos riesgos.	Menos incidentes de seguridad, mejor protección, y rápida detección y respuesta, junto con la capacidad del personal para gestionar estos eventos.
Beckers et al. [16]	Falta de integración de la gestión de riesgos	La falta de integración en la gestión de riesgos de TI lleva a una coordinación deficiente y oportunidades perdidas en seguridad y eficiencia.	La evaluación del impacto mide cómo el sistema de manejo de peligros en TI identifica y gestiona riesgos, mejorando la protección de datos y reduciendo problemas de seguridad.
Chandra et al. [17]	Vulnerabilidades en entornos de nube	Las vulnerabilidades en la nube complican el SGSI. El artículo sugiere usar patrones de ingeniería de requisitos para resolver estos problemas.	Un SGSI para la nube refuerza la seguridad, previene brechas y aumenta la confianza al proteger los datos.
Duarte y Monges [18]	Exposición a amenazas informáticas	El artículo muestra que las organizaciones enfrentan riesgos cibernéticos significativos, revelando la necesidad urgente de mejorar la ciber resiliencia.	La evaluación del impacto protege datos clave, asegura la continuidad operativa y fortalece la credibilidad frente a amenazas de ciberseguridad.
Hoy y Foley [19]	Ineficiencia en la administración de datos.	La mala gestión de datos puede causar filtraciones y pérdidas graves, subrayando la importancia de una administración eficaz de sistemas de información.	Un SGSI reduce riesgos de seguridad, como violaciones, ataques cibernéticos, fugas de datos, incumplimientos regulatorios y pérdida de reputación.

Kamil et al. [20]	Falta de auditoría	La ausencia de auditorías integradas limita la eficiencia. Implementarlas mejora procesos y reduce recursos.	La integración de auditorías reduce la duplicación de esfuerzos, mejora la visibilidad de riesgos y asegura consistencia en los hallazgos, permitiendo decisiones más informadas y una mejor gestión de riesgos.
Llanten et al. [21]	Riesgo de pérdida de confianza y cumplimiento normativo	El riesgo de pérdida de confianza en Suecia depende de la efectividad de las regulaciones de seguridad de información y de cumplir con las expectativas de los involucrados.	Asegurar la legitimidad de los resultados reduce riesgos como pérdida de confianza, clientes e inversores, sanciones, daño reputacional y pérdida de talento.
Morales et al. [22]	Riesgo de ataques cibernéticos y acceso no autorizado	El artículo presenta un esquema de seguridad cibernética que usa IoT, Blockchain y Deep Learning para identificar amenazas y proteger datos.	La medición del efecto evalúa cómo el marco de ciberseguridad reduce riesgos como malware, intrusiones y fugas de datos, protegiendo así los datos y mejorando la seguridad cibernética.
Moreno y Coronado [23]	Infracción de privacidad y manejo indebido de datos	El párrafo se enfoca en cómo las empresas KPO pueden mejorar la seguridad de los datos de clientes mediante métodos y sistemas adecuados.	Un SGSI en compañías KPO reduce riesgos de pérdida de datos, accesos no autorizados, ataques, hurto de propiedad intelectual e incumplimiento normativo.
Mukhtar y Ahmad [24]	Infracción de privacidad y acceso no autorizado	El artículo sugiere un marco para mejorar la seguridad web y proteger datos sensibles de inyecciones SQL, enfocándose en instituciones como la DIAN.	La medición del efecto reduce diversos riesgos asociados con la protección de datos, incluyendo el acceso no autorizado, la pérdida de datos, su alteración y la interrupción del servicio.
Phirke y Ghorpade [25]	Amenazas internas y negligencia en el manejo de datos	El párrafo menciona riesgos internos en datos gubernamentales y propone un marco de Seguridad de la Información para mejorar la protección.	Este efecto reduce riesgos de fuga, sabotaje, robo y errores, mejorando la protección y seguridad de la información.
Podrecca y Sartor [26]	Falta de auditoría y cumplimiento normativo	El artículo indica que, sin auditoría y cumplimiento, se compromete la mala protección de datos, y destaca la importancia de seguir normas y capacitar al personal.	Cumplir con los estándares minimiza riesgos de violaciones de datos, ciberataques y asegura el cumplimiento legal.
Razikin [27]	Riesgo de seguridad de la información, cumplimiento y reputación	El incumplimiento de normas de protección de datos puede causar pérdida de datos, problemas legales y daño a la reputación, afectando la competitividad.	La medición de este efecto evalúa la aceptación del estándar y los riesgos de seguridad, cumplimiento y reputación.
Ruiz et al. [28]	falta de resiliencia frente a amenazas cibernéticas	La falta de resiliencia ante ciberamenazas aumenta la vulnerabilidad del sistema de TI, poniendo en riesgo la seguridad de los datos.	La resiliencia cibernética se mide evaluando la frecuencia y gravedad de incidentes, el tiempo de recuperación y el impacto en los datos.
Țigănoaia [29]	Riesgo de exposición a amenazas cibernéticas y manejo inadecuado de sistemas y datos	El artículo indica que la falta de auditorías de seguridad expone a la empresa peruana a riesgos cibernéticos y que un plan de auditoría es crucial para mejorar la seguridad.	La auditoría en el sistema de ventas minimiza riesgos como acceso no autorizado a datos, fraudes financieros e interrupciones operativas.
Yungán y Narváez [30]	Falta de SGSI formalizado	La falta de un SGSI formalizado expone a las organizaciones a riesgos cibernéticos y compromete la protección de información confidencial, afectando su eficacia operativa.	Este efecto ayuda a mitigar riesgos de seguridad de la información, como ataques cibernéticos, fugas de datos, pérdida de información sensible y daño a la imagen corporativa.
Zaini et al. [31]	Por falta de medidas de seguridad adecuadas	El artículo señala que, sin medidas de seguridad adecuadas, la organización enfrenta riesgos. Un SGSI es clave para proteger los datos y mitigar estos riesgos.	Mitiga riesgos de accesos no autorizados, fugas de datos, vulnerabilidades, malware, ingeniería social, y problemas de integridad y disponibilidad de servicios.

IV. DISCUSIÓN

A. Limitaciones

Tras una exhaustiva revisión sistemática, se identificó una significativa limitación en la cantidad de estudios empíricos sobre temas críticos como el costo de implementación, la reducción de incidentes y el cumplimiento de normativas específicas. Aunque abundan investigaciones sobre la conceptualización de la mitigación de riesgos, estas no ofrecen una explicación funcional del procedimiento necesario para implementar eficazmente la normativa ISO 27001 en empresas latinoamericanas. Según [31], la implementación de la norma ISO 27001 en una empresa tiene un efecto significativo en garantizar la disponibilidad continua de la seguridad de la información, siendo un fundamento principal en la protección de datos.

B. Implicancias y Estudios Futuros

La revisión sistemática se enfoca en identificar herramientas de ingeniería para aplicar directrices sobre seguridad de la información en las empresas, destacando la ISO 27001, el ciclo PDCA y las auditorías. Como una de las herramientas es la auditoría, [28] resaltan que los procedimientos se fundamentan en la detección de riesgos y la evaluación exhaustiva de la organización o sección específica; como afirma [19], la auditoría sigue un proceso que incluye planificación, ejecución,

informes y seguimiento de acciones correctivas. Continuando con la otra herramienta, [31] sostienen que al integrar el ciclo PDCA, las organizaciones pueden mejorar continuamente sus procesos y adaptarse con mayor agilidad a las demandas del entorno cambiante, fortaleciendo su capacidad para mantener altos estándares de seguridad y operatividad. Además, se observa una tendencia creciente hacia el uso de herramientas tecnológicas, como software sencillo o integrado. Según [25] señalan que el software, entendido como aplicaciones que posibilitan la ejecución de funciones específicas en un sistema informático, se vuelve más manejable y eficaz bajo este tipo de gestión.

Para futuras investigaciones, es esencial profundizar en herramientas específicas, como la evaluación personalizada de riesgos de seguridad, la automatización de procedimientos mediante inteligencia artificial y el uso de tecnologías emergentes para la protección de datos, ya que estas áreas prometen avances significativos en ciberseguridad y requieren mayor estudio y desarrollo.

V. Conclusiones

La implementación de la norma ISO 27001 ha demostrado ser esencial para la protección de la información en las corporaciones latinoamericanas, aunque aún no se observa un avance significativo en una implementación más eficaz que permita una mitigación exhaustiva de los riesgos. Las investigaciones sobre la ISO 27001, especialmente entre 2013 y 2024, reflejan un interés creciente en su relevancia para la seguridad de datos en Latinoamérica, destacando su papel crucial en el establecimiento de prácticas robustas de administración de la seguridad de la información.

El impacto de la ISO 27001 se manifiesta en la reducción de incidentes de seguridad de datos y el cumplimiento de regulaciones, aunque persisten desafíos relacionados con los costos de implementación. Este proceso dinámico requiere un compromiso continuo con las mejores prácticas de seguridad, la adopción de tecnologías emergentes y el fomento de una cultura organizacional que priorice la seguridad de la información. La colaboración entre sectores y la capacitación constante son fundamentales para garantizar una implementación efectiva y sostenible de la norma a largo plazo. Finalmente, la atención y adaptación a los nuevos desafíos son esenciales para mantener la eficacia de la ISO 27001 en las empresas latinoamericanas.

Referencias

[1] L. S. Rodriguez Baca, C. F. Cruzado Puente de la Vega, C. Mejía Corredor, and M. A. Alarcón Díaz, "Aplicación de ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana," *Propósitos y representaciones*, vol. 8, no. 3, pp. 1-11, September 2020.

[2] M. Tsiodra, S. Panda, M. Chronopoulos, and E. Panaousis, "Cyber Risk Assessment and Optimization: A Small Business Case Study," *IEEE Access*, vol. 11, pp. 44467-44481, April 2023.

[3] ISO/CEI 27001:2022, "Seguridad de la información, ciberseguridad y protección de la privacidad — Sistemas de gestión de la seguridad de la información — Requisitos," September 2022.

[4] Fortinet, "Fortinet informa que América Latina fue el objetivo de más de 360 mil millones de intentos de ciberataques en 2022," February 2022.

[5] M. Vargas Martín, "Ficha sector. Ciberseguridad en Perú 2023," *Icex*, December 2023.

[6] J. G. Arévalo Ascanio, R. A. Bayona Trillos, and D. W. Rico Bautista, "Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001: análisis del riesgo de la información," *Revista Tecnura*, vol. 19, no. 46, pp. 123-134, November. 2015.

[7] J. Marmo, Msc. C. Zambrano Villalba, and A. Losada, "Propuestas metodológicas en estudios de revisión sistemática, metasíntesis y metaanálisis," *Psicología Unemi*, vol. 6, no. 11, pp. 32-43, July 2022.

[8] K. V. Barrios Serna, D. M. Orozco Núñez, E. C. Pérez Navas, and G. Conde Cardona, "Nuevas recomendaciones de la versión PRISMA 2020 para revisiones sistemáticas y metaanálisis," *Acta Neurológica Colombiana*, vol. 37, no. 2, pp. 105-106, July 2021.

[9] I. Akinyemi, D. Schatz, and R. Bashroush, "SWOT analysis of information security management system ISO 27001," *International Journal of Services Operations and Informatics*, vol. 10, no. 4, pp. 269-287, November 2020.

[10] N. G. Angulo Murillo, M. F. Zambrano Vera, G. García Murillo, and F. Bolaños Burgos, "Propuesta metodológica de seguridad de información para proveedores de servicios de internet en ecuador," *MIKARIMIN Revista Multidisciplinaria*, vol. 4, no. 4, pp. 165-176, September 2018.

[11] M. Antunes, M. Maximiano, and R. Gomes, "A Client-Centered Information Security and Cybersecurity Auditing Framework," *Applied Sciences (Switzerland)*, vol. 12, no. 9, May 2022.

[12] N. E. Zárate Arce, "Análisis de los riesgos por mitigar a través de la auditoría en operaciones electrónicas en Paraguay al 2022," *Revista de Ciencias Empresariales, Tributarias, Comerciales y Administrativas*, vol. 1, no. 2, pp. 225-245, March 2023.

[13] C. A. Mayta Avalos, F. Rosales Castilla, and M. Gines Colana, "Trazabilidad de operaciones en base de datos para mitigar riesgos en los procesos de auditoría," *Innovación y Software*, vol. 3, no. 2, pp. 40-51, September 2022.

[14] B. Brenner, S. Hollerer, P. Bhosale, T. Sauter, W. Kastner, J. Fabini, and T. Zseby, "Better Safe Than Sorry: Risk Management Based on a Safety-Augmented Network Intrusion Detection System," *IEEE Open Journal of the Industrial Electronics Society*, vol. 4, pp. 287-303, July 2023.

[15] B. Barafort, A. L. Mesquida, and A. Mas, "Integrating risk management in IT settings from ISO standards and management systems perspectives," *Comput Stand Interfaces*, vol. 54, pp. 176-185, November 2017.

[16] K. Beckers, I. Côté, S. Faßbender, M. Heisel, and S. Hofbauer, "A pattern-based method for establishing a cloud-specific information security management system: Establishing information security management systems for clouds considering security, privacy, and legal compliance," *Requir Eng*, vol. 18, no. 4, pp. 343–395, June 2013.

[17] N. A. Chandra, K. Ramli, A. A. P. Ratna, and T. S. Gunawan, "Information Security Risk Assessment Using Situational Awareness Frameworks and Application Tools," *Risks*, vol. 10, no. 8, August 2022.

[18] O. Duarte Burgos and M. R. Monges Olmedo, "Análisis de una metodología de Seguridad de la Información basados en los estándares ISO 27001," *ScientiAmericana Revista Multidisciplinaria*, vol. 5, no. 2, November 2018.

[19] Z. Hoy and A. Foley, "A structured approach to integrating audits to create organisational efficiencies: ISO 9001 and ISO 27001 audits," *Total Quality Management and Business Excellence*, vol. 26, no. 5, pp. 690-702, June 2015.

[20] Y. Kamil, S. Lund, and M. S. Islam, "Information security objectives and the output legitimacy of ISO/IEC 27001: stakeholders' perspective on expectations in private organizations in Sweden," *Information Systems and e-Business Management*, vol. 21, no. 3, pp- 699-722, August 2023.

[21] Y.-I. Llanten-Lucio, S. Amador-Donado, and K. Marceles-Villalba, "Validation of Cybersecurity Framework for Threat Mitigation," *Revista Facultad de Ingeniería*, vol. 31, no. 62, pp. 4840, October 2022.

[22] E. Morales-Osorio and M. López-Trujillo, "Sistemas de gestión de seguridad de la información para empresas KPO: una aproximación," *Ventana Informatica*, no. 37, September 2018.

[23] J. E. Moreno Marín and P. C. Coronado Sánchez, "Modelo base de conocimiento para auditorías de seguridad en servicios web con inyección SQL," *Ingeniería*, vol. 25, no. 3, pp. 264-283, October 2020.

[24] Z. Mukhtar and K. Ahmad, "Internal threat control framework based on information security management system," *J Theor Appl Inf Technol*, vol. 70, no. 2, pp. 316-323, January 2014.
[25] A. Phirke and J. Ghorpade-Aher, "Best practices of auditing in an organization using ISO 27001 standard," *International Journal of Recent Technology and Engineering*, vol. 8, no. 2, pp. 691-695, July 2019.
[26] M. Podrecca and M. Sartor, "Forecasting the diffusion of ISO/IEC 27001: a Grey model approach," *TQM Journal*, vol. 35, no. 9, pp. 123-151, April 2023.
[27] K. Razikin and B. Soewito, "Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework," *Egyptian Informatics Journal*, vol. 23, no. 3, pp. 383-404, September 2022.
[28] L. C. Ruiz, M. L. Amado, J. R. Carrasco, and L. Andrade-Arenas, "Implementation of Information Security Audit for the Sales System in a Peruvian Company," *Int J Adv Sci Eng Inf Technol*, vol. 12, no. 3, pp. 1189-1195, June 2022.
[29] B. Ţigănoaia, "Some aspects regarding the information security management system within organizations - Adopting the ISO/IEC 27001:2013 standard," *Studies in Informatics and Control*, vol. 24, no. 2, pp. 201–210, June 2015.
[30] J. I. Carlos Yungán-Cazar and C. I. Valeria Narváez-Contero, "Aplicación de la Norma ISO 27001 para la seguridad de los Sistemas de Información," *Dominio de las Ciencias*, vol. 8, no. 3, p. 14, July 2022.
[31] M. K. Zaini, M. N. Masrek, and M. K. J. A. Sani, "A conceptual overview on the relationship between information security practices and organizational agility," *Adv Sci Lett*, vol. 21, no. 5, pp. 1289–1292, May 2015.
[32] G. S. Miñan, J. A. Moreno, y X. D. Fernández, "LIA Method for the Application of Microsoft Excel in Data Tabulation in Systematic Reviews," CEUR Workshop Proceedings, vol. 20342, pp. 1-12, Dec. 2023.
[33] F. A. Chero-Yenque, T. M. Rodriguez-Bazan, G. S. Miñan-Olivos, y M. W. Valderrama-Puscan, "Sigma methodology and its effect on quality: A systematic review of the literature between 2010-2020 in industrial companies," 20th LACCEI International Multi-Conference for Engineering, Education, and Technology: "Education, Research and Leadership in Post-pandemic Engineering: Resilient, Inclusive and Sustainable Actions", Boca Raton, Florida, USA, 2022, pp. 1-7.