UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE GUAYAQUIL

CARRERA DE INGENIERÍA DE SISTEMAS

Gestión y técnicas en la manipulación de datos para el área de seguridad de la información: una revisión sistemática

Trabajo de titulación previo a la obtención del
Título de Ingeniero de Sistemas

AUTOR: Bryan Nicolás Molina Estupiñán

TUTOR: Joe Frand Llerena Izquierdo Ing., Msc.

Guayaquil – Ecuador

2024

CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

Yo, Bryan Nicolás Molina Estupiñán con documento de identificación N° 0804277226 manifiesto que:

Soy el autor y responsable del presente trabajo; y, autorizo a que sin fines de lucro la Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de manera total o parcial el presente trabajo de titulación.

Guayaquil, 23 de julio del año 2024

Atentamente,

_____

Bryan Nicolás Molina Estupiñán
0804277226

CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACIÓN A LA UNIVERSIDAD POLITÉCNICA SALESIANA

Yo, **Bryan Nicolás Molina Estupiñán** con documento de identificación No. 0804277226, expreso mi voluntad y por medio del presente documento cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autor(a) del Artículo Académico: "**Gestión y técnicas en la manipulación de datos para el área de seguridad de la información: una revisión sistemática**", el cual ha sido desarrollado para optar por el título de: Ingeniero de Sistemas, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En concordancia con lo manifestado, suscribo este documento en el momento que hago la entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.

Guayaquil, 23 de julio del año 2024

Atentamente,

_____

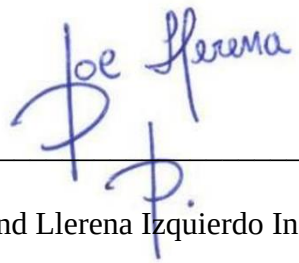
Bryan Nicolás Molina Estupiñán
0804277226

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Joe Frand Llerena Izquierdo con documento de identificación N° 0914884879, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: **Gestión y técnicas en la manipulación de datos para el área de seguridad de la información: una revisión sistemática**, realizado por **Bryan Nicolás Molina Estupiñán** con documento de identificación N° 0804277226, obteniendo como resultado final el trabajo de titulación bajo la opción **Artículo Académico** que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Guayaquil, 23 de julio del año 2024

Atentamente,



Joe Frand Llerena Izquierdo Ing., Msc.

0914884879

DEDICATORIA

A Dios, fuente de sabiduría y fortaleza, quien me ha guiado y fortalecido en cada paso de este camino académico. A mi familia, cuyo amor incondicional y apoyo constante han sido mi mayor inspiración y motivo de perseverancia. Gracias por ser mi sostén en los momentos de dificultad y por celebrar conmigo cada logro. A través de sus enseñanzas y ejemplo, he aprendido el valor del esfuerzo y la dedicación. Este trabajo es un testimonio de su amor y confianza en mí. Que este logro sea también una muestra de gratitud hacia ustedes, quienes han sido mis pilares fundamentales. Con profundo cariño y agradecimiento, dedico este trabajo a Dios y a mi familia, quienes han hecho posible que hoy alcance este importante hito en mi vida académica.

Bryan Nicolás Molina Estupiñán

AGRADECIMIENTO

Quiero expresar mi sincero agradecimiento a Dios, cuya guía y bendiciones han iluminado cada paso de este desarrollo académico. A mi familia, por su amor paciencia, apoyo y sacrificios que han hecho posible mi educación y este logro. Agradezco profundamente a la universidad por brindarme no solo conocimientos y herramientas, sino también oportunidades de crecimiento personal y profesional. Los profesores quienes han sido pilar fundamental en mi formación, ofreciéndome su sabiduría, orientación y aliento constante. Este trabajo no solo representa el fruto de mi esfuerzo, sino también el resultado del respaldo invaluable de quienes creyeron en mí. Con gratitud infinita, dedico este logro a Dios, mi familia y a la comunidad universitaria que me han acompañado y apoyado en este viaje.

Bryan Nicolás Molina Estupiñán

RESUMEN

Existen riesgos, vulnerabilidades y amenazas potenciales que afectan a la confidencialidad, disponibilidad e integridad de datos sensibles. Para proteger las infraestructuras y datos de TI, las empresas aumentan sus medidas de seguridad basadas en una combinación de personas-procesos-tecnología. La Seguridad de la Información (**SeIn**) es un componente importante en TI, y se refiere a la información que es capturada, almacenada, procesada y compartida a través de una red o personas o dispositivos. Existen regulaciones y estándares para cumplir con las leyes de privacidad y seguridad de la información en diferentes países. Uno de los estándares es ISO 27001 se aplica tanto en empresas privadas como públicas, pequeñas, medianas y grandes. La gestión profesional de los activos de información es esencial para prevenir, prever y reconocer riesgos y amenazas a la SeIn. Para evaluar la gestión y técnicas de manipulación de datos, se realizó una revisión sistemática que utiliza el método PRISMA que consiste en: inicio de la investigación, preguntas de investigación, realización de la búsqueda, selección de artículos, extracción de datos e informe. De esta forma se revisaron 21 artículos sacados de IEEE y ACM. Los resultados mostraron que la manipulación de archivos y de dispositivos físicos son las técnicas más comunes en la manipulación de datos. La práctica de almacenamiento más nombrada es instalar aplicaciones de ciberseguridad. El riesgo más frecuente es la amenaza a la ciberseguridad. PDCA es la metodología más aplicada /referenciada. Los sistemas de análisis de vulnerabilidades son los más utilizados. Se resalta el uso de normativas o estándares como el ISO 27001 en sus diferentes versiones que se adopta en diferentes contextos nacionales y de empresas u organizaciones. Aunque el estándar es una guía internacional, tiene su preferencia en metodología que es la PDCA. Los hallazgos sugieren que las empresas implementan diversas medidas de seguridad y existe una necesidad de enfoques integrales en la gestión de riesgos.

Palabras claves: Seguridad de la información, ISO/IEC 27001, Guía de seguridad cibernética, Gestión de seguridad.

ABSTRACT

There are potential risks, vulnerabilities, and threats that affect the confidentiality, availability, and integrity of sensitive data. To protect IT infrastructures and data, companies increase their security measures based on a combination of people-processes-technology. Information Security (SeIn) is an important component in IT, and refers to information that is captured, stored, processed, and shared across a network or people or devices. There are regulations and standards in place to comply with privacy and information security laws in different countries. One of the standards is ISO 27001 and is applied in both private and public, small, medium and large companies. Professional management of information assets is essential to prevent, foresee, and recognize risks and threats to SeIn. To evaluate the management and techniques of data manipulation, a systematic review was carried out using the PRISMA method consisting of: initiation of the research, research questions, performance of the search, selection of articles, data extraction and report. In this way, 21 articles taken from IEEE and ACM were reviewed. The results showed that manipulation of files and physical devices are the most common techniques in data manipulation. The most commonly mentioned storage practice is installing cybersecurity applications. The most frequent risk is the threat to cybersecurity. PDCA is the most applied/referenced methodology. Vulnerability analysis systems are the most commonly used. The use of regulations or standards such as ISO 27001 in its different versions is highlighted, which is adopted in different national contexts and in companies or organizations. Although the standard is an international guideline, it has its preference in methodology, which is the PDCA. The findings suggest that companies implement various security measures, and there is a need for comprehensive approaches in risk management.

Key words: Information security, ISO/IEC 27001, Cyber Security Guideline, Security management

ÍNDICE DE CONTENIDO

1. INTRODUCCIÓN

La Tecnología de la Información (TI) es uno de los pilares en el desarrollo de áreas críticas como educación, finanzas, salud, transporte, gestión, producción, comercio, entre otros (Llerena-Izquierdo & Ayala-Carabajo, 2022; Zapata-Martínez & Llerena-Izquierdo, 2023). Las empresas privadas y públicas utilizan y adoptan la tecnología, mantienen sus activos claves conectados a Internet para optimizar los productos y servicios, y salvaguardar sus ventajas competitivas (Guaranda Lara, 2021). Para proteger las infraestructuras y datos de TI, las empresas aumentan sus medidas de seguridad basadas en una combinación de personas-procesos-tecnología. Aunque, existen empresas con grandes inversiones en tecnologías de seguridad que informan sobre incidentes continuos de seguridad. Otros autores afirman que el factor humano es el eslabón más débil en la cadena de seguridad, como casos de ciberseguridad por mal cuidado de las personas, desinformado, riesgos de seguridad, fuga de información, manipulación de información, entre otros (Alkhazi et al., 2022; Pérez González, 2021)

La Seguridad de la Información (**SeIn**) es un componente importante en TI, la SeIn implica proteger la información que es capturada, almacenada, procesada y compartida a través de una red o personas o dispositivos. SeIn ofrece confidencialidad y privacidad en la información que esta almacenada o enviada. La protección de la información se inicia desde la generación de los datos hasta llegar al destino final. Existen varios métodos o técnicas para cancelar, cifrar y proteger la información como algoritmos de cifrado, tintas indetectables, esteganografía, entre otros (Shaikh et al., 2024).

Por otra parte, existen potenciales riesgos y vulnerabilidades sobre la Confidencialidad, Disponibilidad e Integridad de la información y sistemas de información. Existen diferentes tipos de riesgos como: riesgos sobre infraestructura, vulnerabilidades de software, vulnerabilidades sobre personas y procesos (Melendrez-Caicedo & Llerena-Izquierdo, 2022). Estos riesgos pueden tener varias clasificaciones de consecuencias como: insignificantes, menores, moderados, mayores y catastróficas. Y pueden tener varios niveles como: raro, improbable, posible, probable, cierto (Alwi & Zainol Ariffin, 2020). Además, existen amenazas, riesgos y vulnerabilidades sobre la información que cuestan miles de dólares americanos, varias horas de inactividad e incertidumbre para las empresas. Generan daños serios sobre los activos de información como la pérdida de datos sensibles, pérdidas económicas, quebranto en la reputación empresarial, entre otros (Zerega-Prado & Llerena-

Izquierdo, 2022). La transformación digital de los negocios es una tendencia cada vez más fuerte. Los errores o fallas en la SeIn son una amenaza en el éxito y continuidad de las empresas (Grishaeva & Borzov, 2022).

También, se conoce que los ciberataques son disruptivos, costosos e inquietan a las empresas y gobiernos. El Foro Económico Mundial mantiene perspectivas de ciberseguridad a nivel global que existen tendencias y desafíos sobre cibercrimen. El FEM afirma un aumento en 125% en los ciberataques y continua acentuación, existen riesgos latentes en el sector financiero, salud, amenazas a la estabilidad económica (WEF, 2024). El FEM recomienda utilizar los estándares de información y ciberseguridad, adoptar para asegurar la protección de la información e infraestructura. Existen estándares como NIST, COBIT e ISO 27000, estos se diferencian y tienen diversos propósitos en una empresa (Guo et al., 2021).

En Ecuador y otros países ya existen regulaciones para cumplir con las leyes de privacidad y seguridad de la información; la ley de protección de datos resguarda la privacidad de los ciudadanos ecuatorianos y pretende que las empresas mantengan un control sobre la SeIn (RGLOPD-Ecuador, 2023). De acuerdo a (Putra et al., 2021) el estándar ISO-27001 se utiliza de manera voluntaria en Australia, India, Italia, Luxemburgo, México, Noruega, Polonia, Suiza, Reino Unido, Argentina. Se utiliza de manera mandatorio en Unión Europea, Alemania, Indonesia, Malasia, Nueva Zelanda, Perú. La norma ISO-27001 se puede utilizar en empresas privadas o públicas, además en empresas pequeñas, medias y grandes, además se basa en una metodología de varios pasos: planeación, hacer, la verificación y actuar (Angelo Edu et al., 2023).

Toda empresa necesita invertir tiempo, dinero y personal humano en la planeación y desarrollo de gestión de SeIn, identificar riesgos, utilizar métodos, evaluar riesgos, utilizar tecnologías que agreguen valor a la SI y diseñar planes de control.

La mayoría de las empresas requieren automatizar los procesos de negocio, adoptar tecnologías de información más avanzadas de acuerdo con metodologías de gestión. La gestión profesional sobre los activos de información es importante en todo tipo o tamaño de empresa, para tener capacidad en predecir, prevenir y reconocer los riesgos y amenazas a la SeIn, tener medidas contra los riesgos y optimar los enfoques. En este contexto, es útil una norma ISO para identificación y gestión de riesgos contra la información.

Es necesario identificar técnicas en la manipulación de datos, clasificar los procesos que perjudican a las empresas, conocer las prácticas en almacenamiento de datos sensibles, identificar posibles situaciones de riesgo, conocer metodologías emergentes que sean confiables, conocer tecnologías confiables en la gestión de datos (Coello Ochoa, 2021; Moncayo Ronquillo, 2021; Muñoz Campuzano, 2021; Zerega-Prado & Llerena-Izquierdo, 2022) Esta información puede servir a futuras investigaciones que apliquen la norma ISO-27001. Los marcos de estandarización internacional son importantes en la gobernanza y aseguramiento de la SeIn en las empresas, ISO-27001 es un estándar muy utilizado en controles de SI.

El objetivo general es: Evaluar la gestión y técnicas en la manipulación de datos para el área de seguridad de la información mediante una revisión sistemática

Los objetivos específicos son:

a) Identificar la gestión y técnicas en la manipulación de datos para la clasificación de procesos perjudiciales y prácticas en almacenamiento de datos sensibles mediante la revisión de literatura.
b) Categorizar la gestión y técnicas en la gestión de manipulación de datos para la determinación de situaciones de riesgo, metodologías emergentes y tecnologías en la adopción de fiabilidad de datos mediante norma ISO-27001 versión 2022.
c) Contrastar los resultados obtenidos para el cumplimiento de estándares y normativas en la gestión de información mediante una tabla comparativa de requisitos de infraestructura, diseño de implementación y metodologías de mejora continua.

2. REVISIÓN DE LITERATURA

2.1. Seguridad de la Información (SeIn)

La SeIn es un mecanismo que certifica la seguridad, integridad y disponibilidad de los Activos de Información, durante la fase de almacén, proceso, envío y transporte de los datos. El mecanismo se aplica en el desarrollo de la educación, capacitación, socialización, adición de política y tecnología. En SeIn se aplican tres conceptos: Confidencialidad, Integridad y Disponibilidad (Anang et al., 2021).

La confidencialidad es la que garantiza que la información sea accesible exclusivamente para personas autorizadas, es decir, que tengan los permisos adecuados (Moncayo Ronquillo, 2021). La integridad asegura que la información sea exacta y completa a través de métodos de procesamiento. La disponibilidad permite que los usuarios autorizados tengan la información y los recursos necesarios (Ponce Larreategui, 2021; Sun et al., 2020).

Entre los ejemplos de aplicación se encuentra el control de acceso mediante políticas y uso de autenticación; la realización de copias de seguridad periódicas y el uso de la nube para prevenir perdida de datos; detección de intrusiones y comportamientos anómalos; educación y capacitación para reducir el riesgo de errores humanos; gestión de incidentes (Angelo Edu et al., 2023; Tintin & Hidalgo, 2023; Wicaksono et al., 2022).

2.2. Manipulación de datos

La manipulación de datos se refiere a cualquier acción que altera, modifica o distorsiona los datos originales con el fin de obtener beneficios ilegítimos (Rosero Tejada, 2021). Abarca una amplia gama de actividades que afectan la integridad, confidencialidad y disponibilidad de los datos. Entre las prácticas comunes esta la alteración de archivos y la manipulación de dispositivos físicos. Los ataques pueden darse por diversas causas como lucro económico, vandalismo por motivos personales o ideológicos, espionaje industrial y actividades delictivas como fraudes, suplantación de identidad, entre otros (Mcafee, 2024).

La manipulación de datos en SeIn, se consideran dos clases de manipulación de datos que son el Engaño y el DoS (Denegación de servicios). Esta clase de ataques actualizan las variables de estado o estimulan una pérdida de información, esta intrusión es más inflexible en comparación con la pérdida de enlaces. Los ataques descoordinados son considerados como un escenario de perturbación persistente o temporal (Jena & Padhy, 2022).

Las empresas privadas y los gobiernos alrededor del mundo implementan medidas como firewalls y aplicaciones de ciberseguridad por el aumento de incidentes de seguridad de la información (Putra et al., 2021; Wicaksono et al., 2022; Yasin et al., 2020). Para asegurar la máxima cobertura de seguridad existen metodologías, métodos y protocolo para determinar riesgos y vulnerabilidades.

2.3. ISO-27001

La norma ISO-27001 es un sistema de gestión establecido en procesos que brindan a las organizaciones la capacidad de optimizar la negociación y aumentar la confianza en los sistemas informáticos e información. Es una norma que mejora u optimiza las actividades de Seguridad de la Información. En las organizaciones, el aplicar y obtener la certificación en SeIn se consiguen varios beneficios internos y externos, aunque no todas las empresas consiguen todos los beneficios. Una ventaja es el plano estratégico para armonizar recursos pensando en los riesgos y obtener mejoría competitiva. Otra ventaja es la credibilidad que comunica estabilidad y confianza por el uso de prácticas disponibles en SI (Alves et al., 2024). Sin embargo, requiere de un alto presupuesto para el análisis y la adaptación (Chaiwut & Rueangsirarak, 2022).

Esta norma se basa en tres categorías: Confidencialidad es la propiedad que la información solo está a disposición del dueño y no entidades no autorizadas. Disponibilidad es la propiedad de ser información accesible a entidades autorizadas. La Integridad es la propiedad de exactitud, sin alteración ni perdida ni destrucción de la información (Suorsa & Helo, 2023).

2.4. Casos de ISO-27001 en empresas

La investigación se enfocó en evaluar los riesgos de seguridad y establecer la mitigación es los riesgos encontrados de acuerdo con la norma ISO. Generaron un valor en la prioridad de riesgo, y obtuvieron 14 clasificaciones de riesgos a ser gestionadas; los riesgos los clasificaron en nivel alto, medio y bajo (Wicaksono et al., 2022).

El artículo propone implementar una evaluación sobre la madurez de la SeIn en empresas que utilizan la norma ISO-27001, utilizan un método similar a COBIT5 para valorar los controles y cláusulas de seguridad. Los autores afirman buenos beneficios de aplicar en diferentes tipos de empresa. Obtienen métricas y recomendaciones para mejorar el entorno de gestión, y su uso para tomar de decisiones estratégicas (Monev, 2020).

El artículo compara estos dos estándares en una empresa de telecomunicaciones y genera otra versión dirigida a SeIn basada en ISO-27001. Los autores implementaron la versión mejorada de ISO-20000 en una empresa real con buenos resultados que la versión anterior (Tanovic & Marjanovic, 2020).

En Tailandia utilizaron ISO-27001 para analizar brechas de la norma y generar una guía preliminar en las empresas que deseen diseñar sus políticas de seguridad. La aplicación web evalúa la empresa basada en la ISO, el análisis alcanza los 14 dominios, entrega un puntaje y el nivel de seguridad. En las evaluaciones, las empresas industriales tienen puntuaciones más altas que las empresas gubernamentales (Chaiwut & Rueangsirarak, 2022).

Este artículo aplica la seguridad de datos públicos, la empresa es el Registro de la Propiedad del Cantón Pedro Moncayo, Provincia de Pichincha-Ecuador que las operaciones en la gestión de datos públicos se respaldó en la ISO, integraron varias normativas nacionales de acuerdo a los organismos de control, la empresa tiene un alto estándar de seguridad aplicado a los datos públicos para asegurar la confianza en los procedimientos y documentación realizados por los propietarios de inmueble (Tintin & Hidalgo, 2023).

3. METODOLOGÍA

Para identificar la gestión y técnicas en la manipulación de datos para la clasificación de procesos perjudiciales y prácticas en almacenamiento de datos sensibles. Se utiliza la revisión sistemática de la literatura que es un método para localizar, analizar y aclarar acerca de investigaciones disponibles sobre gestión y técnicas en la manipulación de datos. La revisión de la literatura se sitúa en tres fases: Planificación, Realización e Informes (Juma et al., 2023).

Figura 1. Revisión sistemática.

Preguntas de investigación: ¿Cuáles son las técnicas en manipulación de datos?, ¿Cuáles son los riesgos en seguridad de información?, ¿Cuáles son las metodologías utilizadas en seguridad de información?, ¿Cuáles son las tecnologías utilizadas en seguridad de información?

Búsqueda de investigaciones: En librerías como IEEE, Scopus y ACM Digital Library. Palabras de búsqueda son “ISO-27001”, “Manipulation data”, “Information security”.

Criterios de inclusión y exclusión: Criterios de inclusión son: artículos escritos en idioma inglés, artículos de acceso libre, acceso completo al texto completo, acerca de ISO-27001. Criterios de exclusión: artículos duplicados, artículos no escritos en inglés, artículos de tipo resumen.

Para categorizar la gestión y técnicas en la gestión de manipulación de datos. Se desarrolla la contestación de las preguntas de investigación sobre las situaciones de riesgo, metodologías emergentes y tecnologías; esto basado en norma ISO-27001. Se presentan gráficos de barras o porcentajes, se presenta el análisis de los riesgos, metodologías y tecnologías.

Para contrastar los resultados obtenidos para el cumplimiento de estándares y normativas en la gestión de información. Se presenta una tabla comparativa de requisitos de infraestructura

(hardware, software, instalaciones, redes, servidores, infraestructura local, infraestructura nube), diseño de implementación (arquitectura de implementación, especificaciones de implementación, planes de implementación) y metodologías de mejora continua (Planificar, Hacer, Verificar, Actuar).

4. RESULTADOS

Se presenta una revisión sistemática de la literatura por medio de cuatro pasos indicados en el protocolo PRISMA: identificación, revisión, elegibilidad e inclusión, con los que se rescata el estado de la gestión y las técnicas en la manipulación de datos para el área de seguridad de la información. Inicialmente se obtuvieron 170 artículos científicos en la búsqueda realizada en IEEE y ACM en junio de 2024. Solo 21 artículos cumplieron con el alcance de la investigación y 149 fueron descalificados. Se realizó la respectiva lectura y análisis de los artículos seleccionados. En la Figura 2 se muestra el proceso de selección.

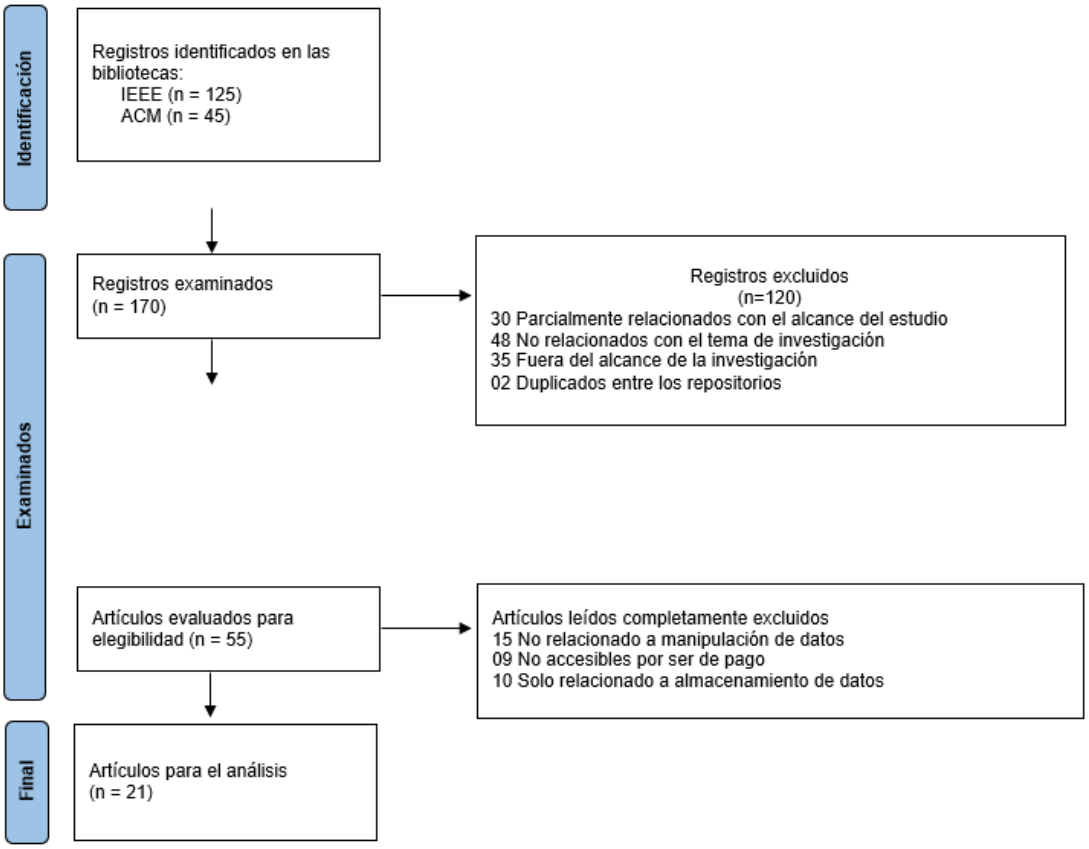


Figura 2. PRISMA.

Se incluyeron 18 artículos de IEEE y 3 de ACM. En la tabla 1 se encuentra los autores y años de publicación de los artículos.

Tabla 1. Artículos científicos analizados

Repositorios	Cant.	Referencias
IEEE	18	(Chaiwut & Rueangsirarak, 2022), (Alkhazi et al., 2022), (Tintin & Hidalgo, 2023), (Shaikh et al., 2024), (Tanovic & Marjanovic, 2020), (Guo et al., 2021), (Alves et al., 2024), (Suorsa & Helo, 2023), (Alwi & Zainol Ariffin, 2020), (Grishaeva & Borzov, 2022), (Yasin et al., 2020), (Jena & Padhy, 2022), (Juma et al., 2023), (Wicaksono et al., 2022), (Anang et al., 2021), (Putra et al., 2021), (Sun et al., 2020), (Yasin et al., 2020)
ACM	3	(Jajodia et al., 2022), (Al-Hamdani, 2021), (Kobiela, 2020)
Total	21	

Fuente: Autor.

En Microsoft Excel fueron organizados los datos de los artículos en orden alfabético por título y repositorio, se incluyó el año de publicación, el número de citas y las características que se encontraron. Las características se agruparon con forme a las preguntas de investigación presentadas en la Metodología. Si una característica es afirmativa se marca "X". Cada característica se encuentra en una columna con un total al final. Cada grupo engloba características y se calcula el porcentaje: la suma de la característica divida para el total del grupo al que pertenece. Es posible que un artículo cumpla con más de una característica en un mismo grupo. Es por ello que el porcentaje de cada característica no puede ser tomado como el porcentaje en artículos en el que estuvo presente. A modo de ejemplo, en el grupo "Prácticas en almacenamiento utilizadas", la primera característica "Actualizar regularmente los sistemas" representa el 7%: que es el resultado de la suma de la característica (2) y la división del total del grupo (27).

La facilidad y utilidad de este método es empleado para el desarrollo de gráficos y estadísticas; facilitando el entendimiento de la situación estudiada.

1. ¿Cuáles son las técnicas en manipulación de datos?

Las técnicas que se relacionan con la manipulación de datos son: manipulación de archivos y de dispositivos con 28% respectivamente, alteración de datos con 21%, phishing con 17% y modificación de código cuente con 7%. La manipulación de datos se refiere a acciones que modifique, elimine o corrompa archivos de un sistema (Alves et al., 2024; Grishaeva & Borzov, 2022; Tintin & Hidalgo, 2023): esto con el propósito de obtener acceso no autorizado o causar daños (Anang et al., 2021; Wicaksono et al., 2022). La manipulación de dispositivos se refiere

a las alteraciones físicas en dispositivos de almacenamiento o procesamiento tales como cámaras, computadoras (Chaiwut & Rueangsirarak, 2022; Guo et al., 2021). Estas técnicas son particularmente peligrosas pues al no haber monitoreos constantes es posible que pasen desapercibidas y causar daños en la integridad y la disponibilidad de datos.

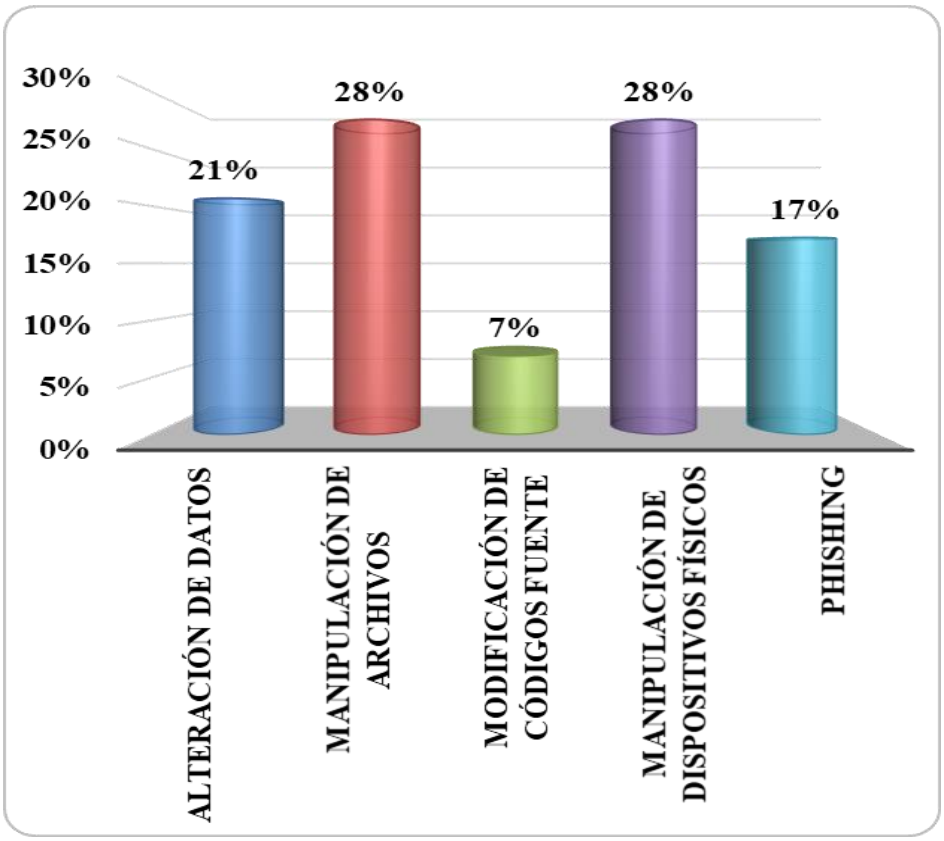


Figura 2. Técnicas de manipulación.

La alteración de datos implica cambios no autorizados, lo que conlleva a una corrupción de bases de datos, falsificación de información crítica, por consiguiente, a errores en tomas de decisiones (Al-Hamdani, 2021). Se da por medio de malware o explotación de vulnerabilidades del software. Esta técnica es más frecuente en sectores de salud, finanza y sistemas gubernamentales donde la precisión de datos es vital (Shaikh et al., 2024). Es debido a esta debilidad que investigadores proponen sistemas especialmente para estos ámbitos (Monev, 2020; Tanovic & Marjanovic, 2020).

Por otro lado, el phishing es una técnica que busca engañar a usuarios para que revelen información confidencial o que realicen acciones que comprometan sus datos (Putra et al., 2021). Es una trampa de ingeniería social en el que el usuario recibe correos electrónicos fraudulentos con links a sitios webs falsos o mensajes instantáneos que parezcan legítimos. En

(Alkhazi et al., 2022; Jajodia et al., 2022; Juma et al., 2023) se presentan casos de entidades financieras y gubernamentales que buscan educar a sus colaboradores y clientes y que no den datos sensibles.

La modificación de código es una técnica que tiene consecuencias duraderas y profundas, pues la alteración del código fuente de un software introduce vulnerabilidades, funciones maliciosas y cambia el comportamiento del programa. Los atacantes desactivan funciones de seguridad o recopilan datos encubiertamente. Esta compromete la seguridad de todo un software (Alwi & Zainol Ariffin, 2020; Yasin et al., 2020).

2. ¿Cuáles son las prácticas en almacenamiento de datos sensibles?

La práctica más comúnmente adoptada para el almacenamiento de datos sensibles es la instalación de aplicaciones de ciberseguridad que obtuvo 48% como lo demuestra la figura 4. Entre las aplicaciones se incluye soluciones como firewalls, sistemas de detección de intrusiones y softwares de cifrado (Jena & Padhy, 2022; Monev, 2020). Dichos programas están diseñados para ser una barrera robusta contra vectores de ataque a la integridad y la confidencialidad de datos (Grishaeva & Borzov, 2022). Si no existen evaluaciones de riesgo, controles basados en riesgos, como criptografía, registro adecuado, medidas contra malware o una gestión de cambio, no se pueden implementar pruebas de seguridad del sistema. (Chaiwut & Rueangsirarak, 2022) complementa la instalación de una aplicación web dirigida a varios sectores industriales y gubernamentales con la formación que se le debe dar al personal.

La educación de los usuarios es la segunda práctica más común con un 22%. Tanto los colaboradores de una empresa como sus clientes/usuarios son la primera línea de defensa contra las amenazas de seguridad (Alwi & Zainol Ariffin, 2020; Suorsa & Helo, 2023). La capacitación y formación en ciberseguridad posee varias aristas que abordan temas como la identificación de correos de phishing, la importancia de contraseñas seguras, gestión de datos. Se busca aumentar la conciencia de los usuarios sobre mejores prácticas de seguridad (Alkhazi et al., 2022; Chaiwut & Rueangsirarak, 2022). La deficiencia en la concientización sobre la seguridad, la formación y educación del personal en empresas pueden causar confusiones o no saber qué se espera de ellos (Suorsa & Helo, 2023). Con una fuerza laboral bien informada, existen menos probabilidades de caer en trampas de ingeniería social. De esta forma las empresas pueden reducir significativamente el riego de que datos sensibles sean sustraídos por errores humanos.

La implementación de medidas de autenticación con el 22%, representan otro componente para la protección de datos sensibles. Esta medida incluye el uso de autenticación multifactor, sistemas biométricos y contraseñas fuertes (Monev, 2020; Shaikh et al., 2024). La autenticación multifactor añade una capa de seguridad adicional al requerir más de una forma de verificación antes de conceder el acceso. Esto dificulta a los atacantes comprometer cuentas, incluso si obtienen una contraseña (Jajodia et al., 2022). Por su parte, los sistemas biométricos con altamente seguros por ser difíciles de falsificar (huellas dactilares o rostro). En (Suorsa & Helo, 2023) se combinan las medidas de autenticación y la educación de los usuarios puesto que se encontraron inconsistencias en la calidad de los datos que condujeron a violaciones de confidencialidad, cuya mayor relación fue el etiquetado inadecuado de datos y el mal manejo de asuntos sensibles por parte de los empleados.

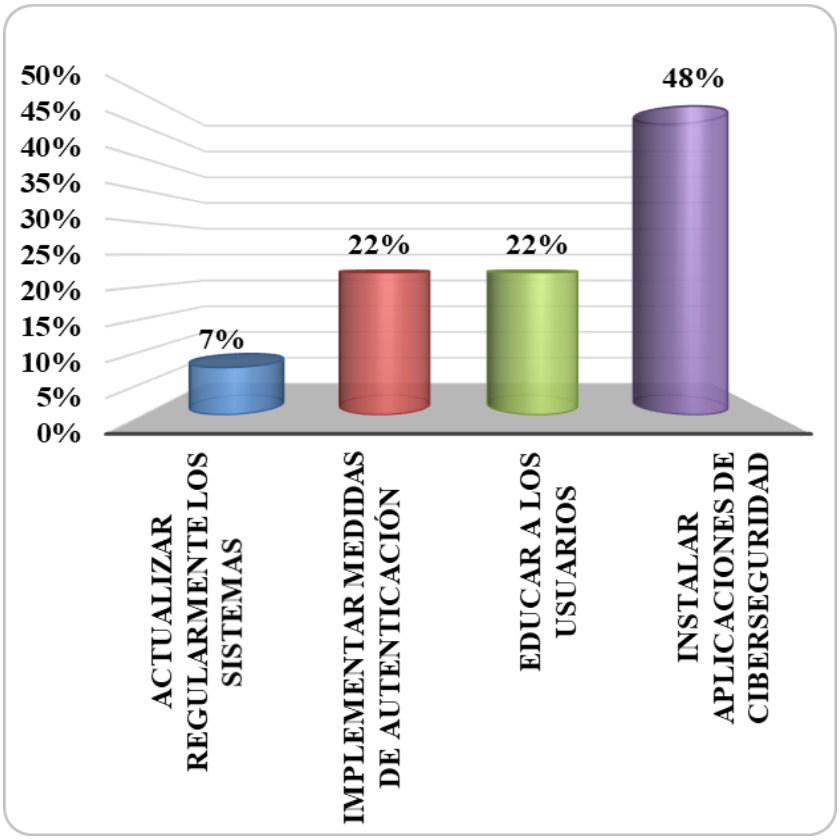


Figura 4. Prácticas en almacenamiento.

La actualización de sistemas de forma regular obtuvo un 7%. Esta es una práctica para la seguridad de los datos debido a las actualizaciones de software y parches abordan vulnerabilidades conocidas (Tintin & Hidalgo, 2023). Al mantener sistemas, aplicaciones y

dispositivos constantemente actualizados, se asegura que las ultimas defensas estén en su punto y que las brechas sean cerradas urgentemente(Anang et al., 2021).

Todas estas prácticas deben formar parte de una guía donde se da el fortalecimiento de la cultura de seguridad dentro una empresa u organización. La cultura de seguridad es vital para la sostenibilidad de estas prácticas que deben ser respaldadas por políticas claras y el compromiso desde los altos mandos para que se realice de manera efectiva.

3. ¿Cuáles son los riesgos en seguridad de información?

En la Figura 5 se puede observar que las amenazas de ciberseguridad con 33%, pérdida de datos con 27%, riesgos de terceros con 21% y fallos en la infraestructura con 18%. Las amenazas de ciberseguridad abarcan una amplia gama de actividades maliciosas como ransomware, phishing, malware y ataques de denegación de servicio (Juma et al., 2023). Dichas amenazas evolucionan rápidamente y obliga las organizaciones a estar en alerta, adoptar medidas proactivas como la implementación de sistemas de ciberseguridad, la educación de su personal en temas de seguridad de información, implementación de autenticación, entre otros (Alwi & Zainol Ariffin, 2020; Suorsa & Helo, 2023).

La pérdida de datos puede surgir de varias maneras entre ellas errores humanos, fallos técnicos y ataques cibernéticos y tiene consecuencias devastadoras como daños financieros e interrupción de las operaciones y corrupción de la información (Sun et al., 2020). Para minimizar el riesgo, existen estrategias para hacer copias de seguridad robustas, cifrado de datos y control de acceso son medidas esenciales (Guo et al., 2021; Putra et al., 2021).

Una organización puede caer en riesgos de terceros cuando depende de proveedores externos y socios comerciales para diversas funciones. Se introducen riesgos como vulnerabilidades en los sistemas de los proveedores, no cumplimiento de políticas de seguridad y la exposición a ataques a través de la cadena de suministro. Allí la reputación de una empresa u organización puede verse afectada (Kobiela, 2020; Sun et al., 2020). Esta característica también acoge otro significado cuando se habla de los riesgos que presenta para los usuarios de una organización o empresa. En este caso se refiere la manipulación de datos que compromete la privacidad de los clientes y expone información confidencial (Chaiwut & Rueangsirarak, 2022; Monev, 2020; Tintin & Hidalgo, 2023). En (Jajodia et al., 2022; Kobiela, 2020) tienen como caso de estudio

el sector gubernamental donde existieron numerosos casos de fuga de datos que afectaron a los usuarios.

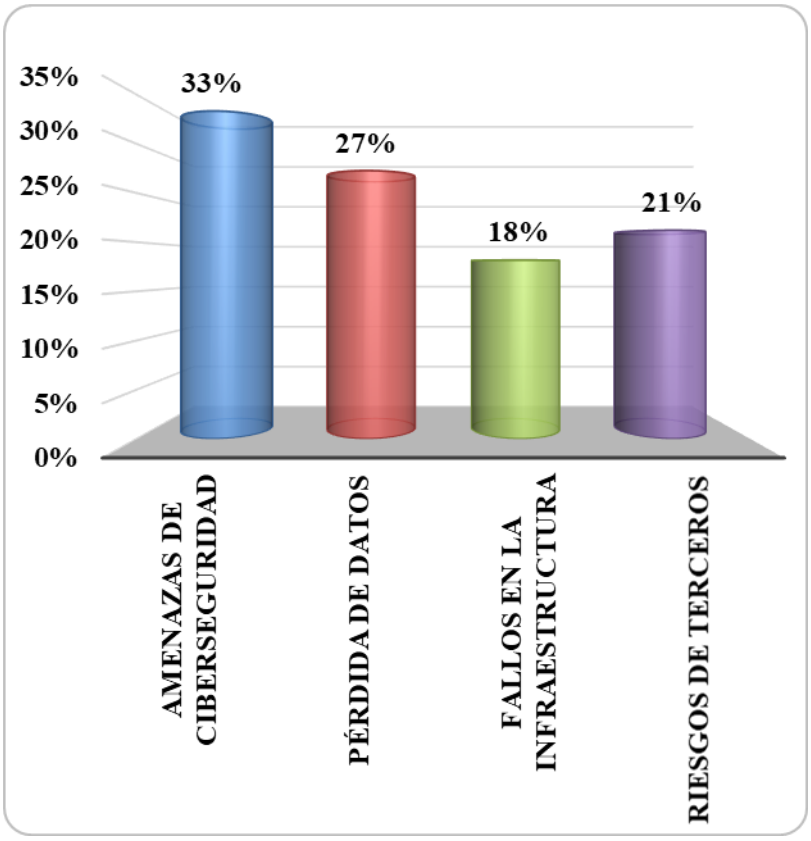


Figura 5. Riesgos en seguridad de información.

En cuanto a los fallos de infraestructura estos incluyen interrupciones en la red, fallas de energía, problemas con el hardware, todos estos causados por un o más personas con el fin de afectar la disponibilidad de datos e interrumpir las operaciones (Alves et al., 2024; Jena & Padhy, 2022; Wicaksono et al., 2022). (Tanovic & Marjanovic, 2020) toman como caso de estudio una empresa de telecomunicaciones donde los datos de los clientes y la infraestructura que poseen para brindar el servicio son los bienes más valiosos que tienen. Por ello, le ponen especial empeño en la protección de las conexiones de los sistemas con encriptación en tiempo real, monitoreo de intrusos, entre otros.

4. ¿Cuáles son las metodologías utilizadas en seguridad de información?

La gestión de la seguridad de la información debe ser un esfuerzo continuo y dinámico, donde el descubrimiento de nuevas amenazas a partir de investigación (privada o desde la academia) sea para el desarrollo de mejores prácticas de seguridad. Consecuentemente existen

metodologías que se utilizan en seguridad de la información, para enfocarse en métodos y técnicas que resuelvan las necesidades de diversos sectores. Se observa que NIST cuenta con 25%, PDCA con 29% seguido de MEHARI con 18%, OCTAVE con 12%.

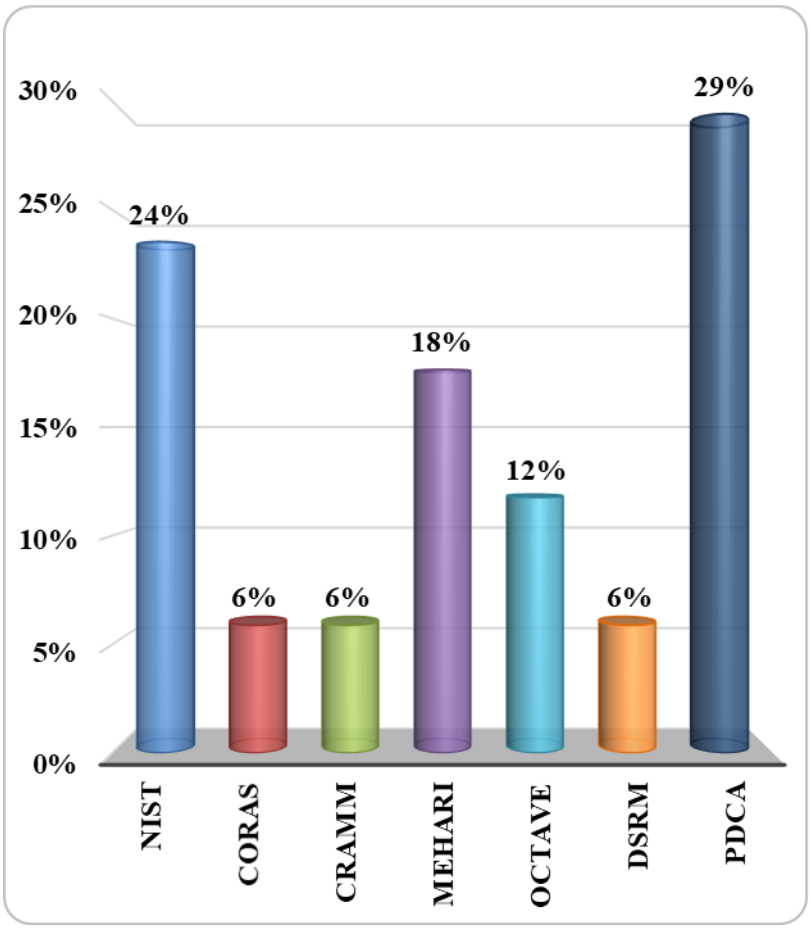


Figura 6. Metodologías utilizadas en SeIn.

El ciclo PDCA es una metodología que busca mejorar procesos empresariales. Consta de cuatro pasos: planificar, hacer, verificar y actuar o ajustar. Es conocido como un ciclo ya que se basa en la repetición de intentos para optimizar (Suorsa & Helo, 2023). En el primer paso es fundamental conocer los objetivos estratégicos para ponerlo en metas tangibles, las expectativas del cliente, detectar prioridades y crear un plan de acción con calendario de ejecución, asimismo definir indicadores de rendimiento para los siguientes pasos. El segundo paso, se debe contar con personal con formación específica para que se ejecuten correctamente las actividades definidas. Además, se debe recoger datos para medir resultados y controlar el proceso. El tercer paso es analizar los resultados, para ello se utilizan los parámetros objetivos y cuantitativos pensados con anterioridad. De esta forma se constata la mejora del proceso y la calidad, y se da la identificación de problemas. El cuarto paso es para implementar la corrección de fallas

detectadas, luego se rehace la planificación con los nuevos resultados (Grishaeva & Borzov, 2022). En (Putra et al., 2021) se hace uso de esta metodología por su flexibilidad y agilidad de adaptarse a los negocios contemporáneos. Sun et al. (2020) optan por PDCA debido a su estandarización de procesos que busquen la continua mejora del sistema de gestión de seguridad de la información propuesto, de igual forma por la utilidad de los indicadores de medición considerados.

La metodología NIST es valorada sobre todo por su profundidad y claridad al momento de proporcionar un conjunto de directrices y normas para la gestión de riesgos estructurados y adaptables. Al no ofrecer una lista de verificación para realizar una evaluación cibernética, esta metodología ofrece a las empresas una guía para que las mismas organizaciones construyan sus tácticas de ciberseguridad (Juma et al., 2023). Al estar conformado por una literatura que abarca cientos de documentos, NIST es fundamental para sustento metodológico que es ampliado y actualizado constantemente; con lo que estipulan fases para llevar a cabo en una prueba de intrusión, por ejemplo. En (Al-Hamdani, 2021), se presenta la guía para evaluaciones y pruebas de seguridad de la información. Anang et al. (2021) tiene la guía para la prevención y detección de intrusiones en sistemas. Wicaksono et al. (2022) acogen la guía para la gestión de incidente de ciberseguridad, con lo que NIST pone a disposición con tres temáticas centrales como planes de respuesta, gestión y coordinación.

La metodología MEHARI plantea analizar los intereses envueltos en la seguridad y utilizar un método de análisis de riesgos. Esta metodología desarrollada para apoya al personal responsable de la seguridad informática toma métodos de evaluación cuantitativos (Tintin & Hidalgo, 2023). Se empieza con un diagnóstico para averiguar el nivel de seguridad que tiene la organización. Tiene dos módulos: rápido y detallado. El rápido es menos preciso y el detallado lo supera su fiabilidad. En el rápido se identifican las principales debilidades, mientras que en el detallado se reconocen las posibles debilidades de los servicios. Claro que se pueden utilizar los dos como en (Chaiwut & Rueangsirarak, 2022). Jajodia et al. (2022) presentan una herramienta de seguridad de la información que combina muchos esquemas de seguridad existentes con el que puedan monitorear y evaluar unificadamente actividades desde un gobierno zonal.

La metodología OCTAVE se centra en los riesgos organizacionales, en sus activos. Consta de tres fases: construir perfiles de amenazas sobre los activos y recursos; identificar

vulnerabilidades en la infraestructura y desarrollar estrategias y planes. Toma importancia el conocimiento de los colaboradores sobre sus prácticas de seguridad y por consiguiente se evalúa la tecnología. Los activos, amenazas, vulnerabilidades se consideran como riesgo operacional. En (Anang et al., 2021) se toma en cuenta la parte de criterios que se conforman por principios, atributos y resultados. En los principios entran todos los conceptos fundamentales como la autodirección, los atributos describen, definen los principios. Los resultados de la evaluación conjunta entre personal de negocios y tecnología de la información destacan el enfoque de estructura y planeación. Kobiela (2020) propone el uso de esta metodología para implementar soluciones de seguridad en dispositivos móviles dentro de negocios debido a las amenazas que resultan del uso de aplicaciones empresariales en teléfonos inteligentes.

CRAMM es una metodología creada por el gobierno del Reino Unido para la gestión de riesgos. Esta consta de tres etapas respaldadas por directrices y cuestionarios objetivos. En la etapa 1 se establecen los objetivos, límites del estudio, valores de activos físicos, hacer una valoración de los datos conservados con respecto a los usuarios y se identifican los activos de software. Para la etapa 2 se identifican y evalúan los tipos de amenazas y sus niveles, se evalúa el alcance de las vulnerabilidades ante las amenazas y se calculan medidas de riesgos de los valores de activos. Para el último paso, se seleccionan las contramedidas de los riesgos calculados. CRAMM tiene más de 3000 contramedidas en su biblioteca. Monev (2020) coge como base esta metodología para proponer una que sea adecuada para sistemas de gestión de la información con estándar ISO 27001 y que dé como resultado una evaluación de madurez.

Sistema Consultivo de Análisis, o (CORAS) por sus siglas en inglés, es una metodología que se centra en el análisis de riesgos utilizando modelos y diagramas. CORAS tiene como objetivo facilitar el descubrimiento de vulnerabilidades y se basa en un lenguaje llamado UML. El enfoque visual ayuda a las organizaciones a comprender la relación entre riesgos y comunicarlos para su posterior tratamiento. La metodología posee ocho pasos: preparación para el análisis; junta inicial con el cliente para comprender cual es el Sistema a analiza, definir objetivos y las preocupaciones principales; descripción detalla del sistema que se analiza mediante diagramas activos; aprobación del cliente para coincidir con los criterios de evaluación para cada activo; identificación de riesgos mediante lluvia de ideas y diagramas de amenazas; estimación del nivel de riesgo por cada amenaza o incidente; evaluación de riesgos y tratamiento de los riesgos al considerar costo-beneficio. Ambos últimos pasos mediante diagramas de amenazas. Guo et al. (2021) utilizan esta metodología debido al enfoque de

interrelación de errores por ser la preferida en situaciones complejas donde los errores se encuentren intrincados, además de servir como soporte para el estándar ISO 27001.

DSRM consiste en identificar problemas, definir objetivos de solución, motivar al diseño, el desarrollo, la demostración, la evaluación y la comunicación. DSRM fomenta la creación de soluciones innovadoras, basada en problemas reales, con demostraciones empíricas y de relevancia práctica. Yasin et al. (2020) diseñan recomendaciones y una hoja de ruta sobre los sistemas de gestión de seguridad de la información basado en DSRM en una empresa en Indonesia. En la primera etapa de la metodología se busca obtener información puntual sobre el problema con la seguridad de la información. En la segunda etapa se determina el propósito que se espera sea mejor que la condición actual. En la tercera etapa se describe el diseño y creación de un modelo, método o rasgo de recursos técnicos necesarios.

5. ¿Cuáles son las tecnologías utilizadas en seguridad de información?

Entre las tecnologías más utilizadas está en primer lugar con 34% el análisis de vulnerabilidades, la ciberseguridad con 21%, la encriptación con 16% al igual que la detección de intrusos. El análisis de vulnerabilidades implica el escaneo de redes aplicaciones y sistemas operativos para ver posibles puntos de entrada de atacantes (Shaikh et al., 2024). La implementación de estos análisis de forma regular permite que las organizaciones estén en constante alerta y tomen medidas proactivas ante sus vulnerabilidades y las amenazas (Alkhazi et al., 2022; Chaiwut & Rueangsirarak, 2022). Alves et al. (2024) rescatan la trascendencia de las certificaciones que deben tener un software que maneje y garantice la seguridad, integridad y calidad de la información, especialmente si se toma en cuenta el estándar ISO 27001. (Al-Hamdani (2021) presenta un programa de seguridad basado en modo de diligencia para asegurar la información con un modelo de capas. Alkhazi et al. (2022) confirman que los análisis de vulnerabilidades se dan desde los mismos colaboradores cuando detectan errores o brechas, por ello afirma que los programas de concienciación sobre la seguridad son esenciales para la seguridad empresarial.

La ciberseguridad se refiere a varias prácticas y tecnologías para proteger dispositivos, programas y datos. Esta incluye la implementación de políticas de seguridad, educación y concientización de usuarios. Los planes de concientización y educación se ven entrelazados a menudo con el análisis de vulnerabilidades como se demuestra en (Alves et al., 2024; Anang et al., 2021; Chaiwut & Rueangsirarak, 2022; Guo et al., 2021; Monev, 2020). En (Kobiela, 2020)

se presenta un concepto para el análisis de amenazas por el uso de dispositivos móviles. La ciberseguridad es una prioridad estratégica para manejar datos sensibles. Tintin & Hidalgo (2023) plantean un diseño donde las normas nacionales emitidas por diferentes órganos de control de datos toman un papel importante para la seguridad de datos públicos de un cantón en Ecuador.

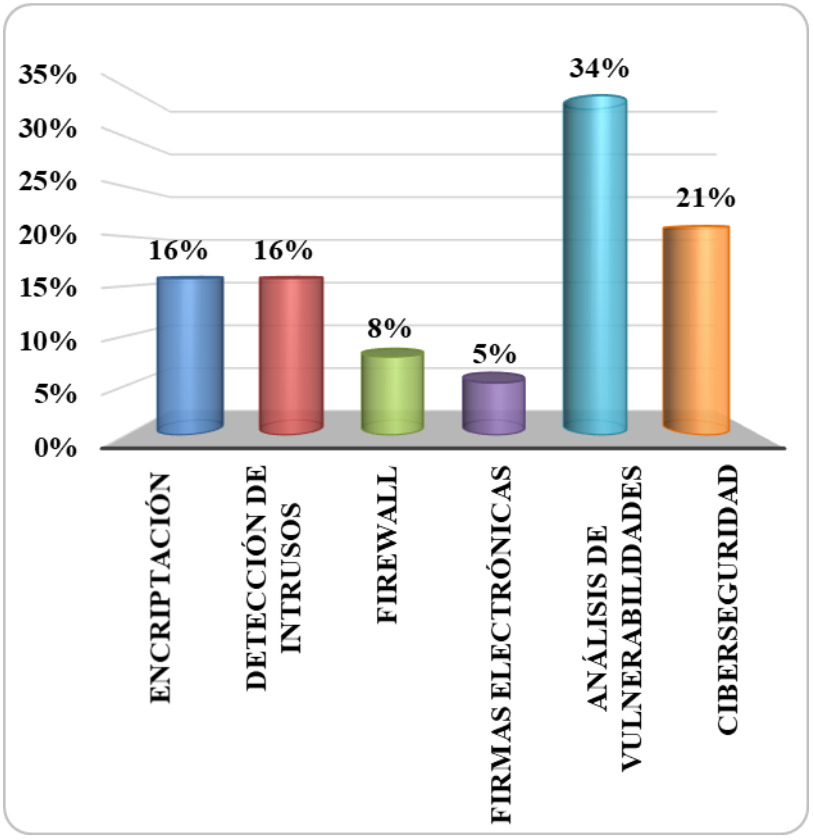


Figura 7. Tecnologías utilizadas en SeIn.

La encriptación convierte la información en un código que solo puede ser descifrado por personas con autorización. La encriptación se asegura de que los datos no sean leídos o utilizados por personas externas no autorizadas aun si los interceptan (Shaikh et al., 2024). Es la forma más optima en la que se resguarda datos y archivos que se encuentren en tránsito (navegadores, email, nube) (Tanovic & Marjanovic, 2020). De la misma forma sirve para datos que están en reposo (discos duros) (Guo et al., 2021; Suorsa & Helo, 2023). Putra et al. (2021) adoptan el encriptado como medida para cumplir con normativas de protección de datos establecidos de forma nacional, como es el caso de Indonesia, para salvaguardar información crítica.

Los sistemas de detección de intrusos monitorean el trafico de red en busca de patrones sospechosos, comportamientos anómalos que indiquen un intento de intrusión (Tanovic & Marjanovic, 2020). Continuo y pasivo, es la forma en la que operan estos sistemas que en ocasiones bloquean el tráfico, recopilan información y alertan a los administradores (Alves et al., 2024; Jena & Padhy, 2022). Putra et al., (2021) apuntan que es importante tener un plan de respuesta ante una violación de datos. Es decir, los sistemas de detección son parte de la solución. Debido a ello esta característica se la encuentra combinada con encriptación, políticas de seguridad, educación y concientización de usuarios (Jajodia et al., 2022).

El firewall es la primera línea de defensa contra ataques. Este controla el tráfico de red entrante y saliente basado en un conjunto de reglas de seguridad. Pueden presentarse como hardware o/y software. Su objetivo principal es bloquear el acceso no autorizado mientras permite la comunicación legítima (Jajodia et al., 2022). Al implementar un firewall evita que información sensible como datos confidenciales y contraseñas salgan como se utiliza en (Suorsa & Helo, 2023).

Las firmas electrónicas fueron las menos utilizadas. Una firma electrónica permite verificar la identidad del remitente, la autenticidad y la integridad de los documentos digitales. Utilizan métodos criptográficos para proporcionar dichas pruebas. Es utilizada en transacciones comerciales, contratos legales, acelera procesos de negocio (Tintin & Hidalgo, 2023). Juma et al. (2023) nombra el uso de esta tecnología para la verificación de identidad del beneficiario del servicio público referenciado.

Contrastar los resultados obtenidos para el cumplimiento de estándares y normativas en la gestión de información mediante una tabla comparativa de requisitos de infraestructura, diseño de implementación y metodologías de mejora continua.

Se construyó una tabla comparativa de infraestructura, diseño e implementación como parte del cumplimiento de los objetivos específicos. Los datos fueron organizados en orden alfabético por título y repositorio, se incluyó el año de publicación, el número de citas y las características. Se tomó en cuenta 16 artículos que presentaban metodología y se realizó un cotejo con las características antes expuestas. Se marca una “X” si una característica es afirmativa. Cada característica se presenta en una columna y se proporciona un total. El porcentaje correspondiente se calcula dividiendo la suma de la característica entre el total del grupo. Cabe señalar que un artículo puede cumplir con múltiples características, lo que implica que el

porcentaje de cada característica no puede interpretarse como el porcentaje de artículos en los que estuvo presente. Por ejemplo, la característica “Implementación” representa el 19%, que se obtiene de la suma de la característica (4) y la división del total del grupo (21)

ITEM	AÑO DE PUBLICACIÓN	TÍTULO DEL ARTÍCULO	REVISTA	NÚMERO DE CITAS	Infraestructura	Diseño	Implementación
1	2024	A New Trend in Cryptographic Information Security for Industry 5.0: A Systematic Review ZAFFAR	IEEE Access	103		X	
2	2022	An Online Gap Analysis on Cyber Security Principles for Thailand Organizations Based on ISO/IEC 27001:2013 Standard	IEEE Access	16			X
3	2022	Assessment of the Impact of Information Security Awareness Training Methods on Knowledge, Attitude, and Behavior	IEEE Access	86			
4	2023	Could an ISMS Model (ISO/IEC 27001:2013 Standard) Implementation Really Protect Public Data?	IEEE Access	11	X	X	X
5	2019	Development of a new improved model of ISO 20000 standard based on recommendations from ISO 27001 standard	IEEE Access	15			
6	2021	Enhance Enterprise Security through Implementing ISO/IEC 27001 Standard	IEEE Access	9		X	
7	2024	Evolutionary analysis of adherence to the ISO 27001:2013 standard in Portugal: Regional and sectoral study	IEEE Access	12			
8	2023	Information Security Failures Measured and ISO/IEC 27001:2022 Controls Ranked by General Data Protection Regulation Penalty Analysis	IEEE Access	28		X	
9	2018	Information Security Risk Assessment for the Malaysian Aeronautical Information Management System	IEEE Access	13			
10	2022	Information Security Risk Management	IEEE Access	27		X	
11	2020	Organisational Information Security Maturity Assessment Based on ISO 27001 and ISO 27002	IEEE Access	3		X	X
12	2022	Resilient Operation of BESS in a Cooperative DC Microgrid under Data Manipulation Attacks	IEEE Access	29			
13	2019	Cybersecurity Assessment Framework: A Systematic Review	IEEE Access	41		X	
14	2022	Risk and security measurament	IEEE Access	12		X	X
15	2021	The Design of Information Security Risk Management: A Case Study Human Resources Information System at XYZ University	IEEE Access	15		X	
16	2021	The Use of ISO/IEC 27001 Family of Standards in Regulatory Requirements in Some Countries	IEEE Access	41		X	
17	2020	Research on the Effectiveness Analysis of Information Security Controls	IEEE Access	15		X	
18	2020	Designing Information Security Governance Recommendations and Roadmap Using COBIT 2019 Framework and ISO 27001:2013 (Case Study Ditreskrimsus Polda XYZ)	IEEE Access	10		X	
19	2020	Information Security Governance Framework	ACM	11		X	
20	2022	Non Risk Assessment Information Security Assurance Model	ACM	21		X	
21	2020	The security of mobile business applications based on mCRM	ACM	28	X	X	
					2	15	4
					10%	71%	19%

Figura 8. Cumplimientos de estándares.

La característica infraestructura se refiere activos físicos, redes, edificios, redes en la nube. El diseño representa a arquitectura, modelos, recomendaciones, guías. Mientras que implementación alude a la aplicación de arquitecturas, recomendaciones, guías e

infraestructura. La figura 9 muestra la estadística de la tabla comparativa de los cumplimientos de estándares. Ilustra que el diseño son lo que los artículos más presentan con un 71%. Seguido por la implementación con 19% e infraestructura con 10%. Se da el caso de que un artículo presente las tres características como en (Tintin & Hidalgo, 2023). De igual forma, se casos en el que los investigadores no solo diseñaron la arquitectura de un sistema, sino que también la implementaron (Monev, 2020). En (Wicaksono et al., 2022) se recopilan recomendaciones y estrategias y se presenta su posterior implementación. Por otra parte, en (Kobiela, 2020) se presentan infraestructura y diseño.

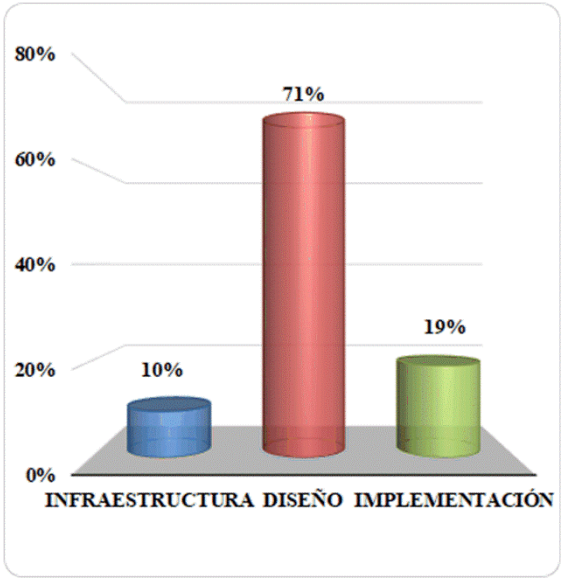


Figura 9. Cumplimientos de estándares.

A continuación, se contrastan los resultados obtenidos a través de un análisis cualitativo que muestra el cumplimiento de estándares y normativas de información por los siguientes artículos.

(Chaiwut & Rueangsirarak, 2022) proporciona un análisis de brechas en línea para orientar el refuerzo de políticas de ciberseguridad en diferentes organizaciones. La aplicación web genera la puntuación y el nivel de seguridad de las organizaciones de diversos sectores de la industria y el gobierno. Se concluye que el sistema es práctico como parte del sistema de gestión de seguridad de la información. Utiliza la metodología PDCA por el principio central de la norma ISO 27001 versión del 2013. Este es presentado como un ciclo cuyo enfoque iterativo y sistemático asegura que los cambios previstos se implementen efectivamente y de forma sostenible.

(Tintin & Hidalgo, 2023) presenta el diseño e implementación de un sistema de gestión de seguridad de la información bajo la norma ISO 270001 para la seguridad de datos públicos. El estudio utilizó la metodología MEHARI para la construcción de un plan de contingencia ante cualquier ataque, perdida de información y dificultades de operatividad. Adicionalmente, se instaló infraestructura de tipo servidores y nube. Se determinó que la institución analizada alcanzó un alto nivel de seguridad de los datos para garantizar procesos y contratos de ciudadanos. Los autores recomiendan la actualización de normativas para que las entidades que manejen datos públicos estén obligados a implementar seguridad de la información bajo estándares internacionales.

(Guo et al., 2021) presenta políticas, clausulas y categorías diseñadas para cumplir con requisitos del ISO 27001 y ayudar a organizaciones a mejorar la seguridad empresarial mediante el desarrollo de un sistema de gestión de seguridad de la información. Utiliza CORAS porque proporciona una forma sistemática de identificar, analizar y gestionar riesgos por técnicas de modela gráfico. Mediante esta metodología se reducen las vulnerabilidades y los riesgos a través de todos los requerimientos, clausulas y categorías.

(Suorsa & Helo, 2023) se enfoca en los fallos más frecuentes y más caros de seguridad de la información correspondientes al estándar ISO 27001 del 2022. Por ello acoge el PDCA para diseñar controles efectivos y mitigar riesgos en las organizaciones. Se orienta también en las supervisiones de varias autoridades de la Unión Europea.

(Grishaeva & Borzov, 2022) proponen medidas preventivas para mejorar procesos de gestión de seguridad de la información y reducir daños a las empresas. De igual forma basa en la metodología PDCA para la protección de activos de información reconociéndoles como aspecto importante en los negocios. Toma como referencia los estándares ISO 27001 del 2013 y otras como la 27002 (código de prácticas para la gestión de la seguridad de la información).

En (Monev, 2020) se diseña una metodología que utiliza el estándar ISO 27001 Y 27002, además del estándar COBIT para evaluar el nivel de madurez de los controles de seguridad, clausulas y directrices. Se basaron en la metodología CRAMM para realizar la suya. El diseño fue implementado con éxito en un sistema de gestión de información. Los autores concluyen que organizaciones de varios tamaños y naturaleza pueden utilizarlas. El producto final son las métricas y recomendaciones para la mejora del sistema, decisiones tácticas y estrategias.

(Juma et al., 2023) hace uso de la metodología NIST y evalúan los estándares ISO 27001 y COBIT. Estos marcos abordan tecnología, necesidades de gobernanza, culturales y específicas de países y organizaciones. Se expone el diseño que contribuye a una investigación de los marcos de ciberseguridad, formuladores de políticas y desarrollo de estrategias efectivas de ciberseguridad.

(Wicaksono et al., 2022) realiza evaluación de riesgos de seguridad y determina la mitigación adecuad, de acuerdo con las normas ISO 27001 y 27002. Hace uso de la metodología NIST para producir el número de prioridad de riesgo, el listado de riesgos y los resultados de que será tratado o mitigado para mejorar los aspectos de la gestión.

(Anang et al., 2021) el estudio tuvo como propósito hacer un diseño de gestión de riesgos de seguridad de la información para un sistema de recursos humanos. Se utilizó ISO 27001 y 27005 para la evaluación de riesgos y recomendaciones. Las metodologías implementadas para la construcción del diseño fueron NIST y OCTAVE.

(Putra et al., 2021) formula un diseño que aplica ISO 27001 para gestiona los riesgos de seguridad de la información para diversos tipos de organizaciones. Hace uso de la metodología PDCA para verificar como los estándares afectan el rango de gestión de seguridad que se encuentra en las medidas legales en Indonesia.

(Sun et al., 2020) plantea un sistema de gestión de seguridad basado en PDCA para controlar el modelo de análisis de los controles de la información. Combina indicadores de medición y los resultados del cumplimiento, lo orienta a corregir y mejorar los objetivos para una mejora continua. Esto lo logra porque se guía con las practicas del ISO 27001 para construir el análisis.

(Yasin et al., 2020) proporciona recomendaciones y una hoja de ruta para la gobernanza de la información basada en ISO 27001 versión 2013 y COBIT. El diseño se basa en las seis etapas de DSRM para la identificación de problemas, promover el desarrollo, evaluación y comunicación. Se produjo un modelo de estructura organizacional con políticas y procedimiento a aplicarse.

(Jajodia et al., 2022) propone un marco que combina muchos esquemas de seguridad de la información ya existente. Dicho marco está basado en la metodología MEHARI para que los ejecutivos corporativos dirijan, monitoreen y evalúen las actividades relacionadas con la seguridad de la información. Se refiere con ISO 27001 versión 2005.

(Kobiela, 2020) usa OCTAVE para detectar vulnerabilidades en la seguridad de software. El estudio propone la modificación de esta metodología para diseñar e implementar mejores soluciones para la seguridad de dispositivos móviles.

(Al-Hamdani, 2021) presenta un modelo de aseguramiento de la información basado en la metodología NIST para construir un modelo de diligencia. La arquitectura del sistema mCRM es una solución en la nube. Se describe que los datos almacenados en los dispositivos móviles utilizados por la empresa se sincronizan con el servidor de base de datos mCRM. De esta forma los datos están disponibles en la aplicación con los sistemas backend de la empresa. Se sugiere el uso de ISO 27001; 2005, 17799, 10007-2003, 122007, IEEE P1700.

5. DISCUSIÓN

Este proyecto tiene como objetivo evaluar la gestión y las técnicas en la manipulación de datos en el área de seguridad de la información por medio de una revisión sistemática de la literatura. Se identificaron dos bases de datos: IEEE y ACM, la investigación desarrollada proporciona a otros investigadores la noción del estado actual de las soluciones que se adapten fácilmente y sean fiables ante situaciones de riesgo, procesos y practicas perjudiciales para el almacenamiento de datos sensibles. Para la revisión se consiguieron artículos científicos, en inglés, de libre acceso, publicados desde el 2018 hasta 2024 que se centran en técnicas de manipulación de datos y seguridad de la información. 21 artículos cumplieron con los criterios establecidos. Esta es una investigación que apunta a ser una revisión bibliográfica por lo que no se cuenta con pruebas experimentales de lo encontrado en los artículos. Por medio de una tabla de Microsoft Excel se inspeccionó características destacadas; se continuó con el análisis cuantitativo, cualitativo y descriptivo; el resultado fue un informe apoyado en gráficos estadísticos y una tabla comparativa.

Entre los resultados se destaca que la manipulación de archivos y de dispositivos físicos son las técnicas más comunes en la manipulación de datos. La práctica de almacenamiento más nombrada es instalar aplicaciones de ciberseguridad. El riesgo más frecuente es la amenaza a la ciberseguridad. PDCA es la metodología más aplicada /referenciada. Los sistemas de análisis de vulnerabilidades son los más utilizados. Resulta notable que, a pesar de que la manipulación de dispositivos constituye uno de los principales desafíos para la seguridad de la información, es el aspecto al que los investigadores toman menos atención.

El articulo excluye tiempos de desarrollo, recursos humanos, costos financieros o el desarrollo prototipo. No se analizaron las implementaciones de ningún artículo seleccionado dentro de la revisión. Entre las limitaciones se cuenta la selección de dos repositorios; no obstante, el uso de IEEE y ACM proporcionan una información valiosa a ser bases de datos grandes, relacionadas a ciencia de la computación y con acceso abierto. Otra limitación es la no evaluación práctica experimental de lo propuesto en los artículos revisado sobre la gestión de manipulación de datos sensibles.

Como trabajo futuro se proyecta una arquitectura para un sistema de gestión de seguridad de la información que se tome como caso de estudio una empresa privada y se hagan posibles la integración de diferentes tecnologías revisadas en este documento.

6. CONCLUSIÓN

Se asegura que los artículos científicos seleccionados cumplan criterios estrictos al aplicar el método PRISMA. Se realizó la identificación de las técnicas de manipulación que resultan perjudiciales para las empresas y organizaciones públicas o privadas: Alteración de datos, Manipulación de archivos, Modificación de códigos fuente, Manipulación de dispositivos físicos y Phishing. Adicionalmente, se reconocieron las prácticas de almacenamiento: Actualizar regularmente los sistemas, Implementar medidas de autenticación, Educar a los usuarios, Instalar aplicaciones de ciberseguridad. Los hallazgos sugieren que las empresas implementan diversas medidas de seguridad y existe una necesidad de enfoques integrales en la gestión de riesgos.

Se determinaron los riesgos en seguridad de la información: Amenazas de ciberseguridad, Pérdida de datos, Fallos en la infraestructura y Riesgos de terceros. Así como se hallaron las metodologías emergentes: NIST, CORAS, CRAMM, MEHARI, OCTAVE, DSRM y PDCA. Del mismo modo, se limitaron las tecnologías adoptadas para la aplicación del estándar ISO 27001: Encriptación, Detección de intrusos Firewall, Firmas electrónicas, Análisis de vulnerabilidades y Ciberseguridad.

Los resultados de la tabla comparativa arrojaron que el uso de normativas o estándares como el ISO 27001 en sus diferentes versiones se adopta en diferentes contextos nacionales y de empresas u organizaciones. Aunque el estándar es una guía internacional, tiene su preferencia en metodología que es la PDCA. Resalta que la mayoría de los artículos presenten diseños, arquitecturas, recomendaciones, guías, y no las implementen. El estudio contribuye al entendimiento de prácticas actuales y ofrece base para futuras investigaciones.

REFERENCIAS

Al-Hamdani, W. A. (2021). Non risk assessment information security assurance model. *Proceedings of the 2009 Information Security Curriculum Development Annual Conference, InfoSecCD'09*, 84–90. https://doi.org/10.1145/1940976.1940993

Alkhazi, B., Alshaikh, M., Alkhezi, S., & Labbaci, H. (2022). Assessment of the Impact of Information Security Awareness Training Methods on Knowledge, Attitude, and Behavior. *IEEE Access*, *10*(December), 132132–132143. https://doi.org/10.1109/ACCESS.2022.3230286

Alves, I., Teixeira, P., & Lopes, N. (2024). Evolutionary analysis of adherence to the ISO 27001 standard in Portugal: Regional and sectoral study. *2024 12th International Symposium on Digital Forensics and Security (ISDFS)*, 1–5. https://doi.org/10.1109/ISDFS60797.2024.10527273

Alwi, A., & Zainol Ariffin, K. A. (2020). Information Security Risk Assessment for the Malaysian Aeronautical Information Management System. *Proceedings of the 2018 Cyber Resilience Conference, CRC 2018*, 1–4. https://doi.org/10.1109/CR.2018.8626841

Anang, A., Gandhi, A., & Sucahyo, Y. G. (2021). The Design of Information Security Risk Management: A Case Study Human Resources Information System at XYZ University. *Proceedings - 2021 4th International Conference on Computer and Informatics Engineering: IT-Based Digital Industrial Innovation for the Welfare of Society, IC2IE 2021*, 198–203. https://doi.org/10.1109/IC2IE53219.2021.9649035

Angelo Edu, M. L., Alexis, G. P., & Lenis, W. P. (2023). Cybersecurity framework for SMEs in Peru based on ISO/IEC 27001 and CSF NIST controls. *Iberian Conference on Information Systems and Technologies, CISTI*, *2023-June*. https://doi.org/10.23919/CISTI58278.2023.10211874

Chaiwut, N., & Rueangsirarak, W. (2022). An Online Gap Analysis on Cyber Security Principles for Thailand Organizations Based on ISO/IEC 27001:2013 Standard. *6th International Conference on Information Technology, InCIT 2022*, 479–484. https://doi.org/10.1109/InCIT56086.2022.10067572

Coello Ochoa, I. N. (2021). *Análisis de ciberataques en organizaciones públicas del Ecuador y sus impactos administrativos*. http://dspace.ups.edu.ec/handle/123456789/20738

Grishaeva, S. A., & Borzov, V. I. (2022). Information security risk management. *Proceedings of the 2022 IEEE International Conference "Quality Management, Transport and Information Security, Information Technologies", IT and QM and IS 2022*, 96–98. https://doi.org/10.1109/ITQMIS51053.2020.9322901

Guaranda Lara, S. N. (2021). *Modelo de gestión para el alineamiento de estrategias corporativas en pymes mediante las tecnologías de la información y comunicación*. http://dspace.ups.edu.ec/handle/123456789/20911

Guo, H., Wei, M., Huang, P., & Chekole, E. G. (2021). Enhance Enterprise Security through Implementing ISO/IEC 27001 Standard. *2021 IEEE International Conference on Service Operations and Logistics, and Informatics, SOLI 2021*, 1–6. https://doi.org/10.1109/SOLI54607.2021.9672401

Jajodia, S., Kudo, M., & ACM Digital Library. (2022). *Information Security Governance Framework*. 64.

Jena, S., & Padhy, N. P. (2022). Resilient Operation of BESS in a Cooperative DC Microgrid under Data Manipulation Attacks. *2022 IEEE Global Conference on Computing, Power and Communication Technologies, GlobConPT 2022*, 1–7. https://doi.org/10.1109/GlobConPT57482.2022.9938340

Juma, A. H., Arman, A. A., & Hidayat, F. (2023). Cybersecurity Assessment Framework: A Systematic Review. *10th International Conference on ICT for Smart Society, ICISS 2023 - Proceeding*, 1–6. https://doi.org/10.1109/ICISS59129.2023.10291832

Kobiela, J. (2020). The security of mobile business applications based on mCRM. *ACM International Conference Proceeding Series*, 179–186. https://doi.org/10.1145/3428690.3429155

Llerena-Izquierdo, J., & Ayala-Carabajo, R. (2022). Inventory of ICTs for learning in engineering for emergency virtual teaching by COVID-19. *2022 IEEE World Engineering Education Conference (EDUNINE)*, 1–6. https://doi.org/10.1109/EDUNINE53672.2022.9782389

Mcafee. (2024). *Manipulación de datos: causas, riesgos y cómo prevenirla*. Mcafee.

Melendrez-Caicedo, G., & Llerena-Izquierdo, J. (2022). Secure Data Model for the Healthcare Industry in Ecuador Using Blockchain Technology. *Smart Innovation, Systems and Technologies*, *252*, 479–489. https://doi.org/10.1007/978-981-16-4126-8_43

Moncayo Ronquillo, K. C. (2021). *Seguridades de la información bases de datos distribuidas: Un mapeo sistemático*. http://dspace.ups.edu.ec/handle/123456789/21701

Monev, V. (2020). Organisational Information Security Maturity Assessment Based on ISO 27001 and ISO 27002. *2020 International Conference on Information Technologies (InfoTech), September*, 1–5. https://doi.org/10.1109/InfoTech49733.2020.9211066

Muñoz Campuzano, P. S. (2021). *Modelos de seguridad para prevenir riesgos de ataques Informáticos: Una revisión sistemática*. http://dspace.ups.edu.ec/handle/123456789/20932

Pérez González, R. F. (2021). *Softwares de penetración utilizados por los piratas informáticos: Una revisión sistemática (2015-2020)*. http://dspace.ups.edu.ec/handle/123456789/20936

Ponce Larreategui, J. G. (2021). *Indicadores de compromiso (IOC) para detección de amenazas en la seguridad informática con enfoque en el código malicioso*. http://dspace.ups.edu.ec/handle/123456789/20937

Putra, D. S. K., Tistiyani, S., & Sunaringtyas, S. U. (2021). The Use of ISO/IEC 27001 Family of Standards in Regulatory Requirements in Some Countries. *Proceeding - 2021 2nd International Conference on ICT for Rural Development, IC-ICTRuDev 2021*, 1–6. https://doi.org/10.1109/IC-ICTRuDev50538.2021.9656529

RGLOPD-Ecuador. (2023). *Reglamento General De Ley Orgánica De Protección De Datos Personales*.

Rosero Tejada, L. F. (2021). *El Phishing como riesgo informático, técnicas y prevención en los canales electrónicos: Un mapeo sistemático*.

Shaikh, Z. A., Hajjej, F., Uslu, Y. D., Yuksel, S., Dincer, H., Alroobaea, R., Baqasah, A. M., & Chinta, U. (2024). A New Trend in Cryptographic Information Security for Industry 5.0: A Systematic Review. *IEEE Access*, *12*(December 2023), 7156–7169. https://doi.org/10.1109/ACCESS.2024.3351485

Sun, Z., Zhang, J., Yang, H., & Li, J. (2020). Research on the Effectiveness Analysis of Information Security Controls. *Proceedings of 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference, ITNEC 2020*, *Itnec*, 894–897. https://doi.org/10.1109/ITNEC48623.2020.9084809

Suorsa, M., & Helo, P. (2023). Information Security Failures Measured and ISO/IEC 27001:2022 Controls Ranked by General Data Protection Regulation Penalty Analysis. *2023 11th International Conference on Cyber and IT Service Management, CITSM 2023*, 1–5. https://doi.org/10.1109/CITSM60085.2023.10455413

Tanovic, A., & Marjanovic, I. S. (2020). Development of a new improved model of ISO 20000

standard based on recommendations from ISO 27001 standard. *International Symposium on Aware Computing, ISAC*, 1503–1508. https://doi.org/10.23919/MIPRO.2019.8756843

Tintin, R., & Hidalgo, M. (2023). Could an ISMS Model (ISO/IEC 27001:2013 Standard) Implementation Really Protect Public Data? *2023 9th International Conference on EDemocracy and EGovernment, ICEDEG 2023*, 1–5. https://doi.org/10.1109/ICEDEG58167.2023.10122109

WEF. (2024). *Ciberamenazas*.

Wicaksono, A. C., Prabowo, S., & Oktaria, D. (2022). Risk and Security Measurement Based on ISO 27001 Using FMEA Methodology Case Study: National Government Agency. *2022 1st International Conference on Software Engineering and Information Technology, ICoSEIT 2022*, *95*, 6–11. https://doi.org/10.1109/ICoSEIT55604.2022.10029988

Yasin, M., Akhmad Arman, A., Edward, I. J. M., & Shalannanda, W. (2020). Designing information security governance recommendations and roadmap using COBIT 2019 Framework and ISO 27001:2013 (Case Study Ditreskrimsus Polda XYZ). *Proceeding of 14th International Conference on Telecommunication Systems, Services, and Applications, TSSA 2020*, *2013*(95), 3–7. https://doi.org/10.1109/TSSA51342.2020.9310875

Zapata-Martínez, J., & Llerena-Izquierdo, J. (2023). Las TIC después del COVID-19: la perspectiva de los profesores universitarios. *Congreso de Docencia En Educación Superior CODES*, *5*.

Zerega-Prado, J., & Llerena-Izquierdo, J. (2022). Arquitectura de consolidación de la información para seguros de la salud mediante Big Data. *Memoria Investigaciones En Ingeniería*, *0*(23 SE-Artículos). https://doi.org/10.36561/ING.23.3