10.18004/ucsa/2409-8752/2024.011.02.0103

Artículo de Revisión

Impacto del uso de diversos marcos de seguridad en las auditorías informáticas dentro de las organizaciones: Revisión sistemática

Impact of using different security frameworks in it audits within organizations: systematic review

Marco Antonio Burgos-Rojas[1], *Carlos Isaac Haro-Polo[1], Alberto Carlos Mendoza-de los Santos[1]

[1]Universidad Nacional de Trujillo, Escuela de Ingeniera de Sistema. Trujillo, Perú

RESUMEN

En un mundo donde los ataques a la seguridad de la información en las organizaciones se han incrementado, surge la auditoría informática como una solución para prevenir estos sucesos no deseados. No obstante, para asegurar la efectividad de estas auditorías, es imprescindible el uso de un marco de seguridad adecuado. Este artículo de revisión proporciona un estudio completo sobre cómo distintos marcos de seguridad pueden impactar en la efectividad de las auditorías de sistemas en las organizaciones. Se llevó a cabo una revisión sistemática que comprende artículos originales, publicados en inglés y español desde 2018 hasta 2023, y accesibles en bases de datos reconocidas como Sciencedirect, Springerlink, JSTOR, Dialnet, Scielo, Scopus y Latinindex. El propósito principal del estudio es comprender cómo la implementación de un marco de seguridad específico, como COBIT, LCCI, NIST, CSF, ISG, D4I y ISO/IEC 27001, puede afectar las auditorías informáticas y su correspondiente impacto en las organizaciones. Adicionalmente, se ha encontrado que la selección del marco de seguridad puede impactar de manera importante en la habilidad de una organización para detectar y minimizar los riesgos de seguridad, mantener la conformidad con las regulaciones y asegurar la integridad y confidencialidad de los datos.

Palabras clave: Marco de seguridad, Auditoría informática, organizaciones.

ABSTRACT

In a world where attacks on the information security of organizations have increased, computer auditing emerges as a solution to prevent these unwanted incidents. However, to ensure the effectiveness of these audits, the use of an appropriate security framework is essential. This review article offers a comprehensive analysis of how different security frameworks can influence the effectiveness of computer audits in organizations. A systematic review has been conducted, which includes original articles published in English and Spanish between 2018 and 2023, and available in recognized databases such as Sciencedirect, Springerlink, JSTOR, Dialnet, Scielo, Scopus, and Latinindex.The main purpose of the study is to understand how the implementation of a specific security framework, such as COBIT, LCCI, NIST, CSF, ISG, D4I, and ISO/IEC 27001, can affect computer audits and their corresponding impact on organizations. In addition, it has been discovered that the choice of the security framework can have a significant repercussion on an organization's ability to identify and mitigate security risks, as well as to maintain regulatory compliance and ensure the integrity and confidentiality of data.

Keywords: Security framework, IT audit, organizations.

***Autor correspondiente: Carlos Isaac Haro Polo.** Universidad Nacional de Trujillo, Escuela de Ingeniera de Sistema. Trujillo , Perú. Email: charo@unitru.edu.pe*
Fecha de recepción: abril 2024. Fecha de aceptación: mayo 2024

***Editora responsable:** Graciela María Patricia Velázquez de Saldivar. Universidad del Cono Sur de las Américas, UCSA.*

Este es un artículo publicado en acceso abierto bajo una licencia Creative Commons

INTRODUCCIÓN

La auditoría informática se ha vuelto cada vez más relevante en el ámbito empresarial debido al crecimiento de la tecnología de la información y la creciente dependencia de las organizaciones en los sistemas informáticos para llevar a cabo sus actividades diarias (Antunes et al., 2022).

En este contexto, es crucial garantizar la privacidad, confidencialidad, coherencia y accesibilidad de los datos e información, al mismo tiempo que se cumple con las normativas y regulaciones aplicables en cuanto a la seguridad de la información (Politou et al., 2019).

La auditoría informática desempeña un rol fundamental en la evaluación y control de los sistemas informáticos y su entorno, siendo un proceso crucial para identificar riesgos, vulnerabilidades y oportunidades de mejora en el ámbito de la tecnología de la información. El objetivo principal de la auditoría informática es garantizar que los sistemas y las infraestructuras de TI estén diseñados, implementados y mantenidos de manera eficiente y efectiva, respaldando los objetivos y metas de la organización (Chifla et al., 2021).

La auditoría informática desempeña un papel crítico al evaluar y controlar los sistemas informáticos y su entorno, permitiendo la identificación de riesgos, debilidades y oportunidades de mejora en el ámbito de la tecnología de la información. Su objetivo principal es garantizar la eficiencia y efectividad en el diseño, implementación y mantenimiento de los sistemas informáticos y las infraestructuras de TI, de modo que respalden los objetivos y metas de la organización (Chifla et al., 2021).

Existen varios marcos de seguridad que pueden servir como referencia para el desarrollo de una auditoría informática en una organización, entre ellos se encuentran COBIT, LCCI, NIST, CSF, EPGA, ISG, D4I y el ampliamente conocido ISO/IEC 27001 (Sabillón et al., 2019).

COBIT (Objetivos de control para la información y tecnologías relacionadas) se enfoca en garantizar que los procesos y controles de TI sean adecuados, eficientes y estén alineados con los objetivos estratégicos de la organización (Schmitz et al., 2021). Las auditorías realizadas con el marco COBIT ayudan a verificar el cumplimiento de políticas y regulaciones aplicables, así como a proporcionar recomendaciones para fortalecer la seguridad y la gestión de riesgos en el entorno de TI (Paredes et al., 2018).

La Cámara de Comercio e Industria de Londres (LCCI) es una institución que ofrece certificaciones y calificaciones en diversos campos, incluyendo la auditoría informática. La certificación LCCI en auditoría informática tiene como objetivo validar y reconocer las habilidades y competencias de los profesionales en la realización de auditorías de sistemas y seguridad informática. Esta certificación se basa en estándares y mejores prácticas reconocidos a nivel mundial y abarca aspectos fundamentales como la evaluación de riesgos, la detección de vulnerabilidades, la revisión de controles internos y la gestión de incidentes (Pawar et al., 2022).

El Marco Común de Seguridad (CSF) es un conjunto de directrices esenciales para la auditoría informática que ayuda a las organizaciones a establecer, implementar y mantener un sistema efectivo de seguridad de la información. El CSF proporciona una estructura para identificar y gestionar riesgos, garantizar el cumplimiento normativo, proteger los activos de información y fortalecer las políticas de seguridad (Alruwaili et al., 2018).

La gobernanza de seguridad de la información (ISG) es un componente integral en el ámbito de la auditoría informática. Se centra en establecer y mantener un marco para garantizar que la organización cumpla con los requisitos

internos y externos en materia de seguridad de la información (Sulistyowati et al., 2020).

El marco de Seguridad Cibernética del NIST utiliza una amplia variedad de criterios para evaluar las vulnerabilidades de seguridad en una organización, destacando su capacidad para realizar un control técnico exhaustivo y analizar registros e incidentes (Russell et al., 2018). Además, se centra tanto en la prevención como en la detección temprana y la respuesta rápida a posibles incidentes de seguridad (Asghar et al., 2019).

D4I es un enfoque que guía el proceso de auditoría informática desde la detección de problemas hasta la generación de informes, pasando por la investigación y la implementación de medidas correctivas. Proporciona una estructura integral para abordar los aspectos clave de la auditoría informática, asegurando una evaluación exhaustiva de los sistemas y tecnologías de la información (Dimitriadis et al., 2019).

Utilizando D4I, los auditores pueden eficientemente identificar y analizar riesgos y vulnerabilidades, investigar incidentes de seguridad, implementar soluciones adecuadas y documentar los resultados en informes detallados (Asghar et al., 2019).

Según Chifla (2020), la norma ISO/IEC 27001 es un estándar global que garantiza la protección, confiabilidad e integridad de la información, así como de los procesos involucrados en su creación. Además, proporciona a las empresas la capacidad de evaluar los riesgos y establecer los controles necesarios para mitigar o eliminar dichos riesgos.

La exploración reciente tiene como objetivo principal comprender los diversos efectos de la aplicación de varios marcos de seguridad en las auditorías de sistemas informáticos dentro de las organizaciones. Para lograrlo, se llevó a cabo una revisión bibliográfica que incorporó estudios de literatura científica entre 2018 y 2023.

Dada esta premisa, las cuestiones clave de la exploración son: ¿Qué marcos de seguridad se emplearon en las organizaciones para las auditorías de sistemas informáticos? ¿Cuáles son los impactos de la implementación de un marco de seguridad en estas auditorías dentro de las organizaciones?

Para responder a estas preguntas, se realizó una investigación en bases de datos académica reconocidas que contienen publicaciones relevantes para el tema en cuestión, lo que contribuirá a alcanzar el objetivo propuesto.

Se adoptó la metodología prisma para filtrar y analizar los hallazgos de los estudios seleccionados. Posteriormente, estos fueron organizados y examinados en la sección de discusión, concluyendo con las reflexiones finales.

MÉTODOS

Se llevó a cabo una revisión exhaustiva de la literatura empleando el método prisma como marco de referencia. La interrogante central que guio la aplicación de esta metodología fue: ¿Qué marcos de seguridad se implementaron en las organizaciones para las auditorías de sistemas informáticos y cuáles son las repercusiones de dicha implementación?

Para dar comienzo a la etapa de exploración, se utilizaron conectores lógicos relacionados con los elementos de investigación, que se desprenden de la pregunta de investigación: "marco de seguridad", "security framework", "Auditoría informática", "computer Audit".

En esta revisión, se consideraron artículos originales en inglés y español publicados en bases de datos científicas de renombre, como Sciencedirect, Springerlink, JSTOR, Dialnet, Scielo, Scopus y Latinindex, desde 2018 hasta 2023.

Estos artículos ofrecen un enfoque orientado a entender el impacto de la implementación de diversos marcos de seguridad en las auditorías de sistemas informáticos dentro de las organizaciones.

Los artículos seleccionados se registraron en una matriz especificando el repositorio, título, fecha de publicación, marco de seguridad empleado, empresa o organización que lo implementó, país y efecto. Los trabajos seleccionados debían incluir indicadores de marcos de seguridad, como COBIT, LCCI, NIST, CSF, EPGA, ISG, D4I y ISO/IEC 27001, y debían estar relacionados con la auditoría informática. La Tabla 1 presenta todos los criterios de exclusión.

Tabla 1: Tabla que detalla los criterios utilizados para excluir elementos.

N°	Criterios de Exclusión
N1	Eliminar los artículos duplicados.
N2	Eliminar los artículos que no estén dentro del periodo comprendido entre los 2018 y 2023.
N3	Eliminar aquellos elementos que no sean documentos científicos
N4	Eliminar los artículos que no estén relacionados con los marcos de seguridad.
N5	Eliminar los artículos que no están disponibles de forma gratuita.

En la Tabla 2 se presenta la cantidad de artículos obtenidos de cada base de datos académica y motor de búsqueda utilizados como referencia en este estudio.

Para la primera depuración se consideraron los criterios de inclusión además de los criterios de exclusión N1, N2 y N3 como se muestran en la Tabla 1. Mientras que para la segunda depuración se consideraron los criterios de exclusión N4 y N5.

Tabla 2: Cantidad de Artículos filtrados utilizando los criterios de inclusión y exclusión

Base de Datos Académico	Cantidad total de artículos encontrados.	Realizando el primer proceso de filtrado.	Realizando el segundo proceso de filtrado
Sciencedirect	75	23	11
Springerlink	48	17	9
JSTOR	56	16	9
Dialnet	68	13	7
Scielo	43	26	6
Scopus	186	27	4
Latinindex	36	17	4
Total	**512**	**139**	**50**

La Figura 1 proporciona una representación visual completa del proceso de la metodología prisma. Este gráfico comienza destacando el proceso de identificación, incluyendo su respectiva sintaxis de búsqueda. Luego se ilustran los dos niveles de filtrado aplicados. Finalmente, el diagrama culmina con la inclusión de los resultados seleccionados, que abarcan un total de 50 artículos.

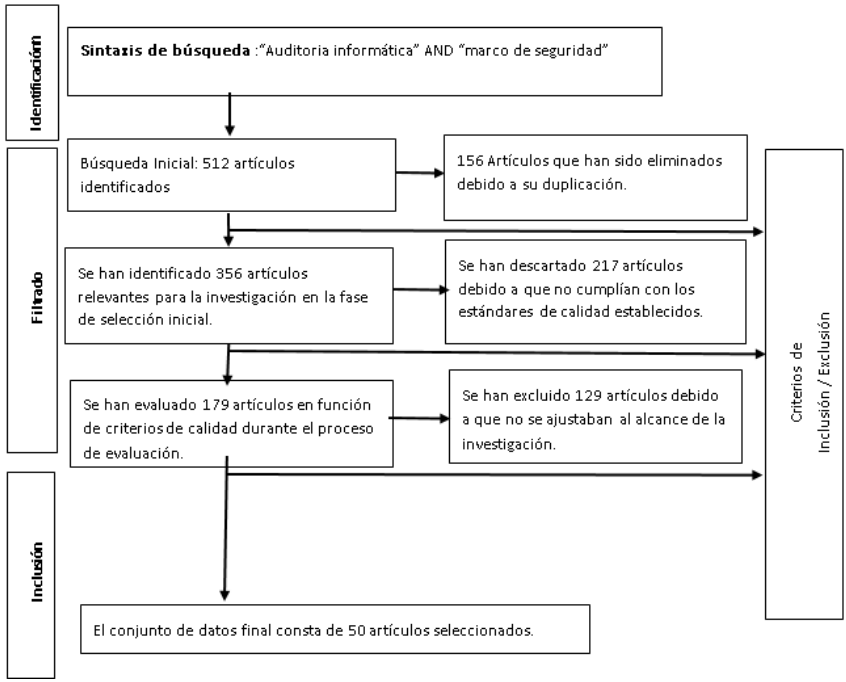

Figura 1: El procedimiento de obtención de artículos mediante el enfoque prisma.

RESULTADOS

Los artículos seleccionados que se ha recopilado en los diferentes tipos de bases de datos muestra la cantidad de artículos que se obtuvieron de cada país siendo Estados Unidos y Ecuador los países con una cantidad de 13 y 10 artículos respectivamente, además de manera porcentual Estados Unidos presenta el 26% siendo el país con la mayor cantidad de artículos (Figura 2).

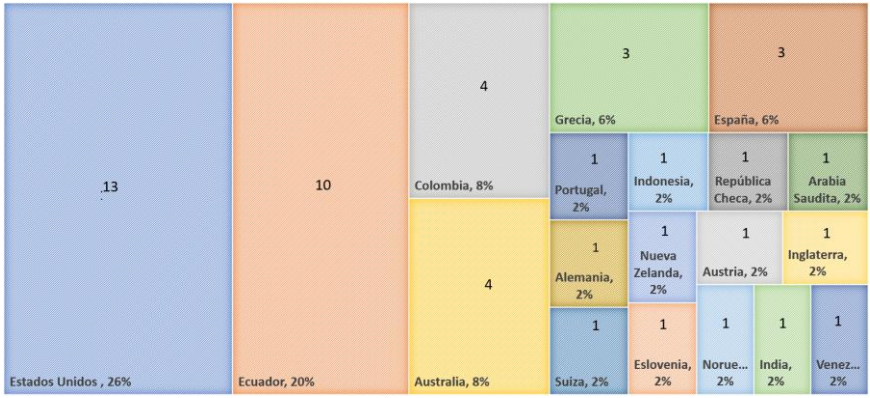

Figura 2: Referencias bibliográficas por país.

Tras llevar a cabo la revisión sistemática, se recopilaron resultados relacionados con los diferentes marcos de seguridad utilizados por diversas organizaciones, clasificados por países. Además, se recopiló información relevante de cada referencia consultada, necesaria para responder a la primera pregunta: ¿Qué marcos de seguridad se utilizaron en las organizaciones para los procesos de auditorías informática?, A continuación, se presentarán en la Tabla 3 los 13 artículos más relevantes de los 50 encontrados.

Tabla 3: Resumen de los marcos utilizados en las organizaciones.

Nº	**Título**	**Marcos**
1	A security review of local government using NIST CSF: a case study(Ibrahim et al.,2018).	NIST CSF
2	A Customizable Web Platform to Manage Standards Compliance of Information Security and Cybersecurity Auditing(Antunes et al., 2022).	ISO/IEC 27001
3	Cybersecurity vulnerability mitigation framework through empirical paradigm: Enhanced prioritized gap analysis(Gupta et al., 2019).	NIST CSF
4	Information security governance challenges and critical success factors: Systematic review(AlGhamdi et al., 2020).	ISG,NIST CSF
5	Cloud Adoption Framework(Zboril et al., 2022).	CAF
6	Maturity level assessments of information security controls: An empirical analysis of practitioners assessment capabilities(Schmitz et al., 2021).	COBIT,
		ISO/IEC 27002
7	LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs)(Pawar et al., 2022).	LCCI
8	D4I - Digital forensics framework for reviewing and investigating cyber attacks(Dimitriadis et al., 2019).	D4I
9	Desarrollo de un sistema de gestión para la seguridad de la información basado en metodología de identificación y análisis de riesgo en bibliotecas universitarias(Guerra et al., 2021).	ISO/IEC 27001
10	Gestión de seguridad de la información con la norma ISO 27001:2013 Information security management with ISO 27001: 2013 (Rubén et al., 2018).	ISO/IEC 27001:2013
11	Auditoría Informática soportada por COBIT E ISO 27001 en las Instituciones Financieras públicas de la ciudad de Guayaquil(Paredes et al., 2018).	ISO/IEC 27001,
		COBIT
12	Efectos de la implementación de una Auditoría Informática a las Empresas de seguros a través de la ISO 27001 :2013 ubicadas en el norte de DMQ(Alejandro et al., 2021).	ISO/IEC 27001
13	Marco de trabajo de gobierno de TI orientado a la ciberseguridad para el sector bancario bajo COBIT 2019(Cabrera et al., 2022).	COBIT,NIST CSF

De los artículos seleccionados abarcan diferentes marcos de seguridad que se han implementado en las diferentes organizaciones en los últimos 6 años, de los cuales 3 de ellos tienen mayor cantidad y son los siguientes: NIST CSF (7),ISO 27001 (6) y COBIT (4) (Figura 3).

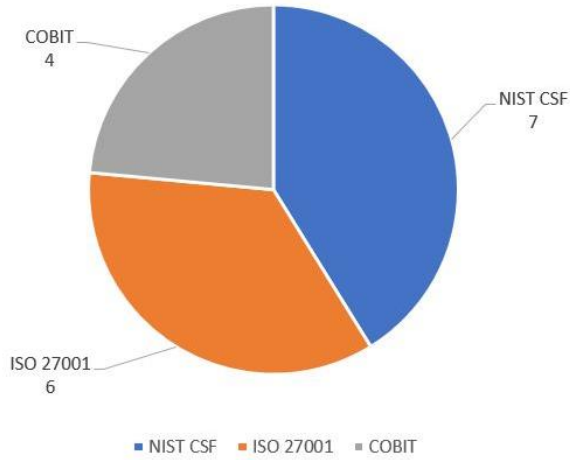

Figura 3. Implementación de marcos de seguridad en diferentes organizaciones

De los resultados obtenidos se puede ver que las referencias abarcan diferentes tipos de organizaciones al implementar diversos marcos de seguridad (Figura 4) en los últimos 6 años que se muestra la cantidad de artículos publicados por sector.

Figura 4. Organizaciones donde se utilizaron diferentes Marcos de Seguridad

Se recolectaron datos sobre la implementación de varios marcos de seguridad en distintas organizaciones, clasificados por país, para responder a la segunda pregunta: ¿Cuáles son los impactos al implementar un marco de seguridad en las auditorias informáticas dentro de las organizaciones? A continuación, se mostrarán en la Tabla 4 los 13 artículos más relevantes de los 50 encontrados, los cuales son los mismos que se presentaron en la Tabla 3.

Tabla 4: resumen de los efectos al implementar los diferentes marcos de seguridad.

Nº	Autor	Efecto
1	Ibrahim et al.(2018)	Mejoras en la planificación de la recuperación. Baja garantía de integridad de datos. Baja identificación de gestión de activos.
2	Antunes et al.(2022)	Adaptabilidad a diferentes organizaciones. Mejora del cumplimiento de los estándares de seguridad. Falta de coherencia en la implementación de los controles de seguridad. Baja mitigación de los controles.
3	Gupta et al.(2019)	Baja Mitigación de vulnerabilidades. Protección Mejorada de Infraestructura Crítica.
4	AlGhamdi et al.(2020)	Identificación de dominios y factores críticos de éxito. Mejora de la alineación entre las políticas de seguridad y los objetivos de la organización. Bajo monitoreo continuo de los controles internos.
5	Zbořil et al.(2022)	Determinación de la madurez de adopción en la nube. Reducción de costos. Éxito en la Migración. Implementación exitosa del marco de gobernanza de la nube. Nula eliminación de datos en la nube. Falta de Implementación de copia de seguridad.
6	Schmitz et al.(2021)	Mejora de Resultados con Certificaciones de Seguridad. Bajo nivel de madurez hacia los controles.
7	Pawar et al.(2022)	Buena Protección contra Amenazas Cibernéticas. Falta de implementación de controles de línea base.
8	Dimitriadis et al.(2019)	Mejora de la Comprensión de los Ciberataques. Identificación del Modus Operandi. Conceptualización de Ataques Mediante Artefactos.
9	Guerra et al.(2021)	Mejora la gestión de riesgos. Falta de identificación de amenazas. Falta de identificación de vulnerabilidades.
10	Rubén et al.(2018)	Mejora en la seguridad de los recursos humanos. Mejora en el control de accesos. Mejora la seguridad de operaciones. Baja gestión de incidentes de seguridad de la información. Poco análisis en los procesos críticos.
11	Paredes et al.(2018)	Mejora de la Gestión de la Seguridad de la Información. Aumento de la Eficiencia Operativa. Incremento de confianza. Bajo seguimiento de controles.
12	Alejandro et al.(2021)	Aumento de Ingresos. Mayor Eficiencia en la Toma de Decisiones. Rendimiento de Activos. Mejora de la Seguridad de la Información. Mejora de Gobernanza de TI. Mejora la Gestión de riesgos.
13	Cabrera et al.(2022)	Mejora de la seguridad de la información. Optimización de recursos. Armonización de procesos y comunicaciones. Aumento de confianza. Dependencia tecnológica.

DISCUSIÓN

Al finalizar el proceso de investigación, que tiene como objetivo determinar el impacto que genera al implementar un marco de seguridad en las auditorias informáticas dentro de las organizaciones, se realizó la siguiente pregunta ¿Qué marcos de seguridad se utilizaron en las organizaciones?, dada la pregunta de investigación hay información recopilada que orienta a una respuesta afirmativa ,aprovechando los antecedentes seleccionados, entre los cuales se encuentra el

autor para dar respuesta a la pregunta, En su investigación, Ibrahim et al. (2020) aplicó el Marco de Ciberseguridad de NIST (NIST CSF) para estimar los riesgos de ciberseguridad en una entidad gubernamental a nivel local en Australia Occidental.

Este método, según el autor, es útil en la obtención de indicadores cuantificables para cada función principal del marco y sus correspondientes categorías. Esto contribuye a que las organizaciones sean capaces de calibrar su nivel de preparación frente a los auténticos riesgos de ciberseguridad.

En su trabajo, Antunes et al. (2022) introdujeron un Sistema de Información (IS) de auditoría de seguridad de la información, que es genérico, accesible a través de la web y de código abierto. A pesar de que su caso de estudio se basó en una auditoría ISO-27001:2013 y se utilizó una lista de verificación predefinida en la plataforma, argumentan que su modelo de datos posee la flexibilidad para adaptarse de manera autónoma a diversas listas de verificación.

Según Zboril & Svatá (2022), el marco que han desarrollado se considera una herramienta valiosa para ayudar a las organizaciones a garantizar que no se omita ninguna actividad o paso necesario. Aunque reconocen que su marco puede no ser aplicable en todos los casos, sostienen que esta característica es común a cualquier marco diseñado para respaldar la gestión o gobierno de una organización.

Schmitz et al. (2021) se propusieron examinar la habilidad de los profesionales para determinar con exactitud el grado de madurez de los controles de seguridad en su estudio. Este estudio se distingue de otros en que no se centró en comparar el nivel de acuerdo entre los participantes. En lugar de ello, crearon un escenario en el cual definieron el nivel de madurez para cada control de seguridad, siguiendo los estándares pertinentes, es decir, ISO/IEC 27002 y COBIT.

Finalmente, una pregunta que surge de esta discusión es: ¿Cuáles son los impactos al implementar un marco de seguridad en las auditorias informáticas dentro de las organizaciones? Frente a esta interrogativa, disponemos de información recopilada que nos orienta hacia una respuesta. Basándonos en los antecedentes, uno relevante para esta pregunta es, Guerra et al. (2021) menciona que es esencial evaluar el efecto de un sistema de seguridad de la información en comparación con los sistemas actuales de las instituciones.

Este proceso implica identificar y analizar las vulnerabilidades y amenazas existentes, permitiendo así la identificación de varios riesgos dentro de los procesos de calidad institucional. Mantilla (2018) mencionó que la implementación de la norma ISO27001:2013 influye eficazmente para administrar un Sistema de Gestión de Seguridad de la Información en cualquier tipo de organización, dado su carácter universal y la posibilidad de certificación. Resaltan la importancia de que la seguridad de la información se integre en la cultura de la organización.

Además, propone la incorporación consciente de los beneficios y los riesgos asociados a dicha cultura en los miembros de la organización. Paredes & Gonzales (2018) mencionan que se identificaron los procesos financieros críticos de la empresa, centrándose en un área de gran relevancia, y demostró cómo las normas internacionales pueden contribuir a la gestión eficaz de riesgos y a la integración de TI en las estrategias clave para la toma de decisiones en la organización.

Según Montalvo (2021), la implementación de una auditoría informática basada en la norma ISO puede tener un impacto positivo en el rendimiento de una organización al mejorar la gestión de sus activos. Este avance contribuye a una mejora integral en el funcionamiento de la organización. Además, se destaca

que un Sistema de Gestión de Información eficiente puede potenciar la toma de decisiones. A través de las fluctuaciones en los resultados clave, se observaron efectos positivos en las estrategias de acción, como un aumento en las ventas, atribuido al uso y desarrollo de tecnología, como la venta a través de portales y otros servicios de comunicación electrónica.

CONCLUSIÓN

El análisis del impacto del uso de diversos marcos de seguridad en las auditorias informáticas dentro de las organizaciones, muestra que hay mayor cantidad de efectos positivos. La mayor cantidad de tipos de organizaciones donde se implementó los marcos de seguridad fueron los siguientes: Pyme, Financiero, Educativo, Gubernamental, Seguros, Salud y Energía.

La revisión sistemática reveló que los siguientes marcos de seguridad se utilizaron en mayor cantidad en las auditorías informáticas dentro de las organizaciones y estos fueron: NIST CSF, ISO-27001,COBIT.Además el impacto positivo que tuvo el marco de seguridad ISO/IEC 207001 utilizado en las bibliotecas de una universidad fue la mejora en la gestión de riesgos esto implica que logra una mayor eficacia y eficiencia al identificar, evaluar, controlar y mitigar los riesgos asociados con la seguridad de la información.

Así mismo otro efecto positivo que tuvo la ISO/IEC 27001 fue la adaptabilidad de los marcos de seguridad a diferentes organizaciones esto implica que el marco de seguridad tiene la capacidad de ser utilizado y ajustado en diferentes tipos de organizaciones, sin importar su tamaño, sector o estructura. Por otro lado, el marco de seguridad NIST CSF utilizado en una organización financiera tuvo un efecto positivo que fue la mejora de la seguridad de la información esto significa la protección de los activos de información de la organización frente a amenazas y riesgos.

Por otro lado, al utilizar el marco de seguridad ISO 27001 en una entidad financiera tuvo un impacto negativo que fue el bajo seguimiento de controles esto significa que la organización presenta deficiencias o debilidades en el monitoreo y seguimiento de los controles de seguridad implementados.

En futuras investigaciones, se pueden examinar los resultados derivados de implementar distintos marcos de seguridad en auditorías informáticas dentro de diversas organizaciones. Estos marcos, como el marco de seguridad HIPAA para entidades de salud, los CIS Controls para la protección de sistemas de información y el marco de seguridad PCI DSS aplicable a organizaciones que manejan información de tarjetas de crédito, no fueron incluidos en esta revisión sistemática, pero son ejemplos de marcos que pueden ser considerados. Se puede indagar sobre los efectos generados por dichos marcos en aspectos cruciales como la confidencialidad, integridad y disponibilidad de los datos, así como en la mitigación de riesgos y el cumplimiento de regulaciones específicas.

Además, Es crucial realizar una evaluación de la adaptabilidad de estos marcos de seguridad a diversos entornos organizacionales, así como analizar su impacto en la planificación de la recuperación y la gestión de incidentes de seguridad. Además, es necesario investigar cómo estos marcos pueden optimizar la asignación de recursos y mejorar la eficiencia operativa en las organizaciones. También es importante investigar los aspectos relacionados con la incorporación de tecnologías emergentes, como la inteligencia artificial y el Internet de las cosas, y cómo los marcos de seguridad pueden abordar los desafíos y riesgos asociados con la adopción de estas nuevas tecnologías.

Contribución del autor: Como autor principal, Carlos Isaac Haro Polo ha encabezado la conceptualización, metodología y supervisión general de la investigación, participando activamente en la selección y revisión sistemática de los artículos originales, una labor compartida con Marco Antonio Burgos Rojas. Burgos Rojas, por su parte, se ha concentrado en la interpretación de los resultados obtenidos y en la redacción de las conclusiones de la investigación. Alberto Carlos Mendoza de los Santos, reconocido por su prolífica carrera académica y sus numerosas publicaciones, ha ejercido un papel fundamental en la corrección y mejora de la estructura del informe, además de brindar un apoyo invaluable para la culminación exitosa del proyecto. Todos los autores han revisado y aprobado la versión final del manuscrito.

Financiación: El estudio ha sido financiado con recursos propios además de tener el apoyo de la universidad nacional de Trujillo.

Conflicto de interés: Los autores no tienen ningún conflicto de intereses y han colaborado de forma coordinada en todas sus contribuciones.

REFERENCIAS BIBLIOGRAFICAS

Abstracts of the MASCC/ISOO Annual Meeting 2018. (2018). Supportive Care in Cancer : Official Journal of the Multinational Association of Supportive Care in Cancer, 26(2), 39–364. https://doi.org/10.1007/S00520-018-4193-2/METRICS

AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: Systematic review. Computers and Security, 99. https://doi.org/10.1016/j.cose.2020.102030

Antunes, M., Maximiano, M., & Gomes, R. (2022). A Customizable Web Platform to Manage Standards Compliance of Information Security and Cybersecurity Auditing. Procedia Computer Science, 196, 36–43. https://doi.org/10.1016/J.PROCS.2021.11.070

Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M. V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J. M., O'Leary, C., Eshaya-Chauvin, B., & Flahault, A. (2020). Cybersecurity of Hospitals: Discussing the challenges and working towards mitigating the risks. BMC Medical Informatics and Decision Making, 20(1), 1–10. https://doi.org/10.1186/S12911-020-01161-7/PEER-REVIEW

Asghar, M. R., Hu, Q., & Zeadally, S. (2019). Cybersecurity in industrial control systems: Issues, technologies, and challenges. Computer Networks, 165, 106946. doi=https://doi.org/10.1016/J.COMNET.2019.106946

Bailon Lourido, W. A. (2019). Auditoria informática al control y mantenimiento de una infraestructura tecnológica. CIENCIAMATRIA, 5(1), 73–87. https://doi.org/10.35381/cm.v5i1.248

Blažič, B. J. (2022). Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills? Education and Information Technologies, 27(3), 3011–3036.doi=https://doi.org/10.1007/s10639-021-10704-y

CALDER, A. (2020). The Cyber Security Handbook: Prepare for, respond to and recover from cyber attacks with the IT Governance Cyber Resilience Framework (CRF). IT Governance Publishing.doi=https://doi.org/10.2307/j.ctv19shhms

Checco, J. C. (2022). Cyber-Physical Coordinated Attacks: The Emerging Complexity of Crisis Management. The Cyber Defense Review, 7(4), 69–90. https://www.jstor.org/stable/48703292

Chidukwani, A., Zander, S., & Koutsakis, P. (2022). A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations. IEEE Access, 10, 85701–85719.doi=https://doi.org/10.1109/ACCESS.2022.3197899

CYBERSECURITY CERTIFICATION VALIDATES PROGRAMS. (2020). Computer Security Update, 21(2), 2–4.doi=https://www.jstor.org/stable/48597909

CYNET LAUNCHES THE SECURITY FOR MANAGEMENT TEMPLATE. (2019). Computer Security Update, 20(9), 1–2.doi=https://www.jstor.org/stable/485978866

Montalvo Cisneros, OAUNIVERSIDAD POLITÉCNICA SALESIANA SEDE QUITO Efectos de la implementación de una auditoría informática a las empresas de seguros a través de la ISO 27001 :2013 ubicadas en el Norte del DMQ

3 http://dspace.ups.edu.ec/handle/123456789/19918

Dimitriadis, A., Ivezic, N., Kulvatunyou, B., & Mavridis, I. (2020). D4I - Digital forensics framework for reviewing and investigating cyber attacks. Array, 5, 100015. https://doi.org/10.1016/j.array.2019.100015

Enfoque, U. (2018). Un modelo práctico para realizar auditorías exhaustivas de Ciberseguridad (A Practical Model to Perform Comprehensive Cybersecurity Audits). Enfoque UTE, 1, 127–137. http://ingenieria.ute.edu.ec/enfoqueute/

FAIRVIEW HEALTH SELECTS CYNERGISTEK SECURITY. (2020). Computer Security Update, 21(11), 7–8. https://www.jstor.org/stable/48597898

Frayssinet Delgado, M., Esenarro, D., Juárez Regalado, F. F., & Díaz Reátegui, M. (2021). Methodology based on the NIST cybersecurity framework as a proposal for cybersecurity management in government organizations. 3C TIC: Cuadernos de Desarrollo Aplicados a Las TIC, 10(2), 123–141. https://doi.org/10.17993/3ctic.2021.102.123-141

Gourisetti, S. N. G., Mylrea, M., & Patangia, H. (2020). Cybersecurity vulnerability mitigation framework through empirical paradigm: Enhanced prioritized gap analysis. Future Generation Computer Systems, 105, 410–431. https://doi.org/10.1016/j.future.2019.12.018

Guerra, E., Neira, H., Díaz, J. L., & Patiño, J. (2021). Desarrollo de un sistema de gestión para la seguridad de la información basado en metodología de identificación y análisis de riesgo en bibliotecas universitarias. Información Tecnológica, 32(5), 145–156.doi=https://doi.org/10.4067/s0718-07642021000500145

Ibrahim, A., Valli, C., McAteer, I., & Chaudhry, J. (2018). A security review of local government using NIST CSF: a case study. Journal of Supercomputing, 74(10), 5171–5186. https://doi.org/10.1007/s11227-018-2479-2

Ibrahim, E., & Greenberg, M. R. (2018). Managing the Cybersecurity Risks of an Increasingly Digital Power System. In V. Sivaram (Ed.), Digital Decarbonization: Promoting Digital Innovations to Advance Clean Energy Systems (pp. 91–97). Council on Foreign Relations.doi= http://www.jstor.org/stable/resrep21838.12

Levite, A. E., Kannry, S., & Hoffman, W. (2018). Complementary Efforts by Governments and the Insurance Industry. In Addressing the Private Sector Cybersecurity Predicament: The Indispensable Role of Insurance (pp. 19–23). Carnegie Endowment for International Peace. http://www.jstor.org/stable/resrep20984.7

Negrín Sosa, E., López García, L., Rodríguez Cabrera, K., & Martínez Guerra, D. (2017). Facultad de Ciencias Administrativas y Económicas. In UTM Diciembre (Vol. 8).

Orellana Cabrera, X. E., & Álvarez Galarza, M. D. (2022). Marco de trabajo de gobierno de TI orientado a la ciberseguridad para el sector bancario bajo COBIT 2019. Universidad Católica de Cuenca, Ecuador.

Oswaldo Chuquimarca-Espinoza, M. I., Edwin Ormaza-Andrade III, J., & Carlos Erazo-Álvarez, J. I. (n.d.). El futuro de la auditoría y las innovaciones tecnológicas El futuro de la auditoría y las innovaciones tecnológicas The future of auditing and technological innovations O futuro da auditoria e das inovações tecnológicas. Especial, 6(1), 316–339. doi=https://doi.org/10.23857/dc.v6i1.1149

Pawar, S., & Palivela, D. H. (2022). LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs). International Journal of Information Management Data Insights, 2(1). https://doi.org/10.1016/j.jjimei.2022.100080

Politou, E., Michota, A., Alepis, E., Pocs, M., & Patsakis, C. (2018). Backups and the right to be forgotten in the GDPR: An uneasy relationship. Computer Law and Security Review, 34(6), 1247–1257. https://doi.org/10.1016/j.clsr.2018.08.006

Proaño Escalante, R. A., Saguay Chafla, C. N., Jácome Canchig, S. B., & Sandoval Zambrano, F. (2017). Sistemas basados en conocimiento como herramienta de ayuda en la auditoría de sistemas de información. Enfoque UTE.

Progoulakis, I., Rohmeyer, P., & Nikitakos, N. (2021). Cyber physical systems security for maritime assets. Journal of Marine Science and Engineering, 9(12). https://doi.org/10.3390/JMSE9121384

Radanliev, P. (2023). Review and Comparison of US, EU, and UK Regulations on Cyber Risk/Security of the Current Blockchain Technologies: Viewpoint from 2023. The Review of Socionetwork Strategies 2023, 1–25. https://doi.org/10.1007/S12626-023-00139-X

Randall, R. G., & Allen, S. (2021). Cybersecurity professionals information sharing sources and networks in the U.S. electrical power industry. International Journal of Critical Infrastructure Protection, 34, 100454. https://doi.org/10.1016/J.IJCIP.2021.100454

Rubén, A., & Guerra, M. (n.d.). Gestión de seguridad de la información con la norma ISO 27001:2013 Information security management with ISO 27001: 2013 standard (Vol. 39).

Russell, S., & Jackson, S. (2018). Operating in the Dark: Cyber Decision-Making from First Principles. Journal of Information Warfare, 17(1), 1–15. https://www.jstor.org/stable/26504126

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

Sánchez-García, I. D., Feliu Gilabert, T. S., & Calvo-Manzano, J. A. (2023). Countermeasures and their taxonomies for risk treatment in cybersecurity: A systematic mapping review. Computers & Security, 128, 103170. https://doi.org/10.1016/j.cose.2023.103170

Schmitz, C., Schmid, M., Harborth, D., & Pape, S. (2021). Maturity level assessments of information security controls: An empirical analysis of practitioners assessment capabilities. Computers and Security, 108. https://doi.org/10.1016/j.cose.2021.102306

Serna Ramírez, S., Montoya Londoño, Á., Quintero Barco, Y. A., Henao Villa, C. F., & Castro Ramírez, F. D. J. (2022). Desarrollo de un sistema de seguridad informática a partir de una auditoría sobre una red empresarial. INGENIERÍA: Ciencia, Tecnología e Innovación, 9(2), 135–151. https://doi.org/10.26495/icti.v9i2.2267

Sulistyowati, D., Handayani, F., & Suryanto, Y. (2020). Comparative analysis and design of cybersecurity maturity assessment methodology using nist csf, cobit, iso/iec 27002 and pci dss. International Journal on Informatics Visualization, 4(4), 225–230. https://doi.org/10.30630/JOIV.4.4.482

Tsohou, A., Diamantopoulou, V., Stefanos Gritzalis, ·, & Lambrinoudakis, · Costas. (2023). Cyber insurance: state of the art, trends and future directions. International Journal of Information Security, 22, 737–48. https://doi.org/10.1007/s10207-023-00660-8

Wylde, V., Rawindaran, N., Lawrence, J., Balasubramanian, R., Prakash, · Edmond, Jayal, A., Khan, I., Hewage, C., & Platts, J. (2022). Cybersecurity, Data Privacy and Blockchain: A Review. SN Computer Science, 3, 127. https://doi.org/10.1007/s42979-022-01020-4

Yadav, A., Kumar, A., & Singh, V. (2023). Open-source intelligence: a comprehensive review of the current state, applications and future perspectives in cyber security. Artificial Intelligence Review, 1–32. https://doi.org/10.1007/S10462-023-10454-Y/TABLES/17

Zboril, M., & Svatá, V. (2022). Cloud Adoption Framework. Procedia Computer Science, 207, 483–493. https://doi.org/10.1016/j.procs.2022.09.103

Zhu, P., & Liyanage, J. P. (123 C.E.). Cybersecurity of Offshore Oil and Gas Production Assets Under Trending Asset Digitalization Contexts: A Specific Review of Issues and Challenges in Safety Instrumented Systems. European Journal for Security Research, 6, 125–149. https://doi.org/10.1007/s41125-021-00076-2

Mero Paredes, G. D., & Zambrano González, S. K. (2018). Auditoría informática soportada por COBIT e ISO 27001 en las instituciones financieras públicas de la ciudad de Guayaquil. Universidad Católica de Santiago de Guayaquil. Recuperado de http://repositorio.ucsg.edu.ec/handle/3317/10431

Gourisetti, S. N. G., Mylrea, M., & Patangia, H. (2020). Cybersecurity vulnerability mitigation framework through empirical paradigm: Enhanced prioritized gap analysis. Future Generation Computer Systems. Elsevier. https://doi.org/10.1016/j.future.2019.12.018