TALENTO. Revista de administración ISSN: 2788 - 6565 / ISSN-L: 2788 - 6565

Volumen 4 No. 6 | Septiembre – diciembre 2022 | Pp. 01 - 15 | https://revistatalento.org/index.php/talento/

http://doi.org/10.62349/talento.v4i6.1

Ciberseguridad en empresas: Revisión sistemática sobre desafíos y estrategias para proteger activos digitales

Cybersecurity in companies: Systematic review of challenges and strategies to protect digital assets

Roger Dante Prado Lafuente

rpradol@univalle.edu

https://orcid.org/0000-0002-5560-3840

Universidad Privada del Valle

Cochabamba - Bolivia

Artículo recibido 08 de junio de 2022 / Arbitrado 25 de junio de 2022 / Aceptado 15 de agosto de 2022 / Publicado 01 de septiembre de 2022

RESUMEN

La ciberseguridad es importante en el entorno empresarial actual, dado el incremento de amenazas que afectan los activos digitales. Este artículo tiene como objetivo describir los desafíos y estrategias adoptadas por las empresas para salvaguardar su información mediante una revisión sistemática. Se sugieren variables como tipos de amenazas, niveles de seguridad implementados y la efectividad de diversas estrategias. Se utilizó el método PRISMA para recopilar información de bases de datos como SciELO, Dialnet, Redalyc, Scopus y Lantidex. Se incluyeron estudios publicados en inglés y español y se excluyeron aquellos que no estaban disponibles a texto completo. Se analizaron un total de 100 registros. Los descriptores booleanos incluyeron "ciberseguridad" y "estrategias". Los resultados revelan que las empresas enfrentan desafíos significativos, pero las estrategias basadas en formación continua y tecnologías avanzadas son relativamente efectivas. Las conclusiones destacan la necesidad de un enfoque integral para fortalecer la ciberseguridad en las empresas.

Palabras clave: Amenazas; desafíos; digitalización; empresas; estrategias, ciberseguridad.

ABSTRACT

Cybersecurity is important in today's business environment due to the increase in threats affecting digital assets. This article aims to describe the challenges and strategies adopted by companies to safeguard their information through a systematic review. Variables such as types of threats, levels of security implemented, and the effectiveness of various strategies are suggested. The PRISMA method was used to collect information from databases such as SciELO, Dialnet, Redalyc, Scopus, and Lantidex. Studies published in English and Spanish were included, while those not available in full text were excluded. A total of 100 records were analyzed. The Boolean descriptors included "cybersecurity" and "strategies." The results reveal that businesses face significant challenges, but strategies based on continuous training and advanced technologies are relatively effective. The conclusions highlight the need for a comprehensive approach to strengthen cybersecurity in businesses.

Keywords: Threats; challenges; digitalization; businesses; strategies; cybersecurity.

INTRODUCCIÓN

La ciberseguridad se ha convertido un tema recurrente en la política internacional del actual siglo, impactando de manera significativa áreas como la seguridad nacional y la política exterior de los Estados. Desde que el uso de Internet se popularizó y normalizó a finales de los años noventa, pasando por incidentes como el ciberataque en Tallin, Estonia (2007), hasta el reciente ataque cibernético que afectó a 18,000 agencias gubernamentales y empresas, detectado por el gobierno de Estados Unidos en diciembre de 2020, este campo ha surgido como una nueva área de influencia, conflicto y competencia en las relaciones internacionales (Aguilar, 2021).

La ciberseguridad es fundamental para organizaciones de diversas dimensiones y sectores, debido al aumento tanto en la cantidad como en la complejidad de las amenazas digitales. Con la rápida digitalización de los procesos, la necesidad de resguardar los activos digitales resulta más apremiante que nunca. Un estudio por parte del *Ponemon Institute* (2021) indica que las empresas enfrentan un costo promedio de 4.24 millones de dólares por cada violación de datos, enfatizando la urgencia de adoptar estrategias efectivas para la gestión de riesgos cibernéticos.

Además, Ojeda-Contreras (2020) señala que, en la actualidad, a medida que las instituciones financieras adopten sus operaciones digitales asumen mayores riesgos de ataques cibernéticos que tienen alta probabilidad de suceder, es así que, en los últimos diez años se ha incrementado la delincuencia cibernética, atacando a los negocios de los diferentes sectores de la economía.

A nivel global, la situación en torno a la ciberseguridad es preocupante; en 2022, se reportó un aumento del 31% en las ciberamenazas en comparación con el año anterior, según el informe de *Cybersecurity Ventures* (2022). Esta tendencia genera serias inquietudes sobre la idoneidad de los niveles de seguridad aplicados en las organizaciones y su capacidad para adaptarse a un entorno de amenazas en continua evolución. Las restricciones presupuestarias, la falta de formación en ciberseguridad y la creciente complejidad de las amenazas son algunos de los factores que restringen la efectividad de las distintas estrategias de protección disponibles.

En este artículo se analizan los tipos de amenazas que enfrentan las empresas, los niveles de seguridad implementados y la efectividad de las estrategias empleadas para mitigar estos riesgos. Asimismo, la necesidad de esta investigación radica en proporcionar a las empresas un marco teórico claro que les ayude a mejorar su posición en ciberseguridad y a salvaguardar más eficientemente sus activos digitales. La pregunta central que orienta el estudio consiste en conocer cuáles son los principales desafíos y estrategias que adoptan las empresas para proteger sus activos digitales en un entorno cibernético amenazante.

Por consiguiente, el objetivo principal de la investigación consiste en describir los desafíos que las empresas enfrentan en el ámbito de la ciberseguridad, así como las estrategias que han demostrado ser efectivas en la protección de sus activos digitales. Se considera un contexto en el que las organizaciones están cada vez más expuestas a incidentes de seguridad y donde las violaciones de datos son comunes, por lo que esta investigación se aborda de una manera teórica, ofreciendo información relevante para fortalecer la ciberseguridad en el ámbito empresarial.

MÉTODO

La investigación se llevó a cabo como un estudio cualitativo de revisión sistemática, siguiendo el método PRISMA. Su objetivo fue analizar las principales amenazas a la ciberseguridad que enfrentan las empresas y las estrategias implementadas para mitigarlas. El diseño metodológico se fundamentó en la recolección y el análisis de información proveniente de literatura académica y técnica relevante, utilizando un enfoque estructurado que facilitó la identificación de patrones en el ámbito de la ciberseguridad empresarial.

La recolección de datos se realizó mediante una revisión de la literatura, empleando un protocolo que incluía criterios específicos para la selección de estudios. Este protocolo se caracterizó por su sistematicidad y replicabilidad, abarcando la definición de palabras clave, la selección de bases de datos y el establecimiento de criterios de inclusión y exclusión. Se consideraron artículos académicos y publicaciones relevantes en ciberseguridad de los últimos diez años, que abordaran temas relacionados con las amenazas digitales, los niveles de seguridad y las diversas estrategias utilizadas.

Los criterios de inclusión establecieron que los artículos debían haberse publicado en revistas científicas revisadas por pares y tratar sobre ciberseguridad en diferentes contextos, principalmente en el empresarial. En contraste, los criterios de exclusión descartaron estudios que no se centraran en la protección de activos digitales o que carecieran de datos empíricos. Se consultaron diversas bases de datos académicas, como SciELO, Dialnet, Redalyc, Scopus y Lantidex, garantizando así una cobertura amplia y representativa de los temas tratados.

Las variables de estudio se definieron como los principales tipos de amenazas, los niveles de seguridad implementados y la efectividad de las diversas estrategias utilizadas. Dentro de estas variables, se consideraron dimensiones como la clasificación de amenazas (malware, ransomware, phishing, entre otros), la categorización de los niveles de seguridad (bajo, medio, alto) y la evaluación de la efectividad de las estrategias, que incluyó tanto enfoques preventivos como reactivos. Se elaboró un cuadro de operacionalización que facilitó la organización y análisis de estos aspectos. El contexto de esta investigación se sitúa en el entorno empresarial actual, donde las organizaciones enfrentan constantes desafíos en materia de ciberseguridad. La población objeto de estudio incluyó empresas de diversos tamaños y sectores que implementan soluciones de ciberseguridad, seleccionando una muestra representativa de estudios que abordan la situación de la ciberseguridad empresarial a nivel global.

Para el análisis de los resultados, se aplicó una técnica de análisis cualitativo que permitió categorizar y sintetizar la información recolectada. El procesamiento de datos se realizó mediante un análisis temático, facilitando la identificación de patrones recurrentes y la extracción de conclusiones significativas sobre las amenazas, la seguridad y las estrategias en ciberseguridad. Este enfoque proporcionó una visión integral sobre el estado actual de la ciberseguridad en las empresas y su importancia en la protección de activos digitales.

RESULTADOS

Luego de aplicar el método PRISMA, en la primera etapa, como se refleja en la Figura 1, se identificaron 75 bases de datos que brindaron acceso a un total de 100 registros iniciales, lo que refleja

una búsqueda de información relevante. La diversidad de las fuentes consultadas demuestra que se llevó a cabo un enfoque amplio y sistemático, lo que aumentó así la probabilidad de encontrar datos significativos para la investigación. Sin embargo, en esta etapa se eliminaron 25 registros, compuestos por 15 duplicados, cinco que resultaron ser ilegibles y otros cinco eliminados por no estar disponibles a texto completo. Este proceso riguroso de depuración garantizó que la información seleccionada se basa en datos de calidad y relevantes, evitando que duplicaciones o datos inadecuados sesgaran los resultados.

Durante la etapa de cribado, los 75 registros restantes fueron analizados con un enfoque crítico. De esta selección, 30 informes fueron excluidos, lo que representa un 40% de aquellos que habían superado las fases iniciales, resaltando así la importancia del criterio de evaluación utilizado, ya que incluso registros previamente considerados válidos no cumplían con los estándares requeridos. Además, se realizaron solicitudes para recuperar 15 informes adicionales, señalando que se consideraba que existía información valiosa que merecía un análisis más profundo. Sin embargo, la exclusión de cinco informes que no pudieron ser recuperados plantea un reto, ya que limita la comprensión completa del tema en cuestión. Finalmente, se evaluaron 55 informes para determinar su adecuación y pertinencia, revelando un esfuerzo para asegurar la calidad de la información que se iba a utilizar. Las razones para la exclusión de los informes muestran un proceso transparente y estructurado, lo que favorece la credibilidad de la revisión.

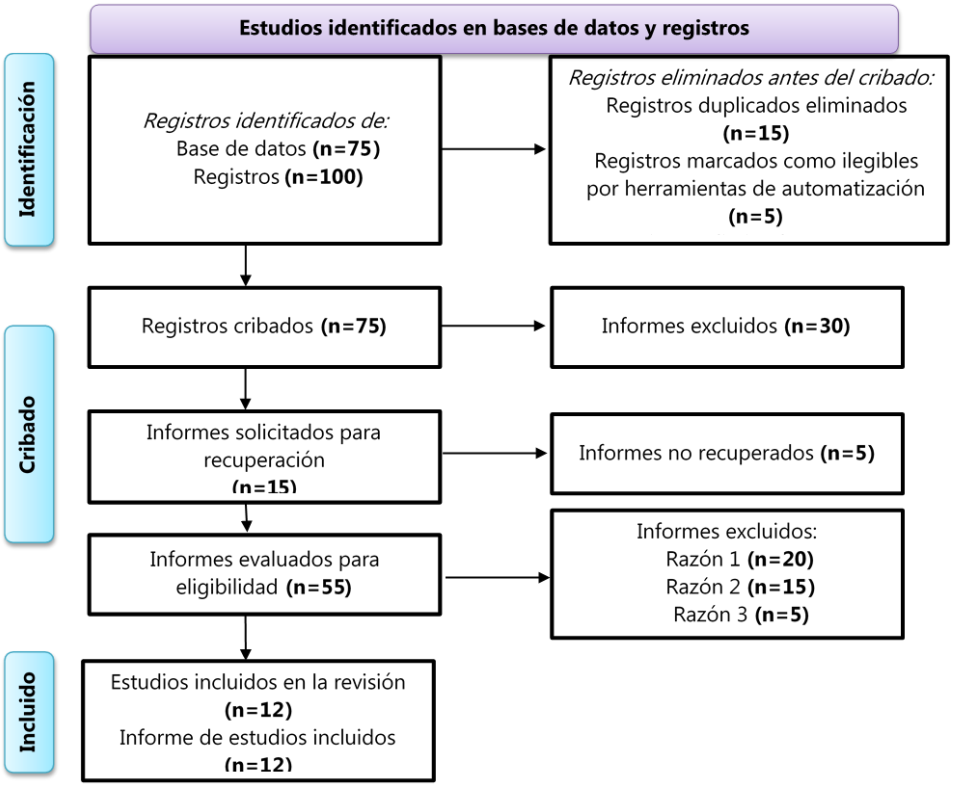
En la etapa de inclusión, se seleccionaron 12 estudios para formar parte de la revisión, demostrando que se llevó a cabo un proceso de identificación, cribado y evaluación, que asegura que solo los estudios más relevantes y de mayor calidad hayan sido considerados. La confirmación de 12 estudios permite a los investigadores contar con un conjunto de datos manejable y significativo, facilitando un análisis de los desafíos y estrategias en la protección de activos digitales.

Los resultados de cada etapa evidencian un proceso bien estructurado. Las decisiones tomadas a lo largo de las fases de identificación y cribado subrayan un significativo esfuerzo por filtrar información irrelevante, asegurando que las investigaciones incluidas ofrezcan una perspectiva clara y útil sobre los desafíos y estrategias existentes en el contexto de la ciberseguridad. Este enfoque sistemático no solo fortalece la base para la formulación de conclusiones y recomendaciones, sino que también proporciona un marco sólido para futuras investigaciones y prácticas en el área de protección de activos digitales.

Figura 1

Flujograma de PRISMA

Volumen 4 No. 6 | Septiembre – diciembre 2022 | ISSN: 2788 - 65650 / ISSN-L: 2788 – 6565 / https://revistatalento.org/index.php/talento/



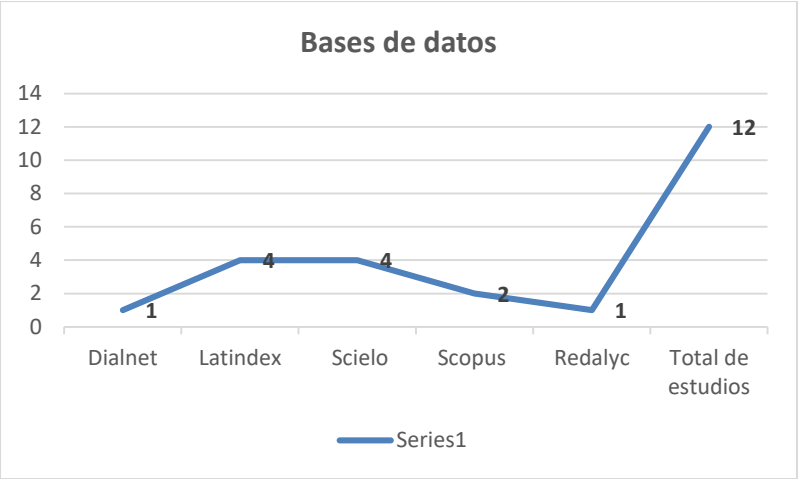
En la Figura 2 muestra que se han analizado un total de 12 estudios, que representan la suma de las investigaciones incluidas en la revisión. En lo que respecta a la distribución por bases de datos, se observa que Dialnet contiene únicamente un estudio. En cambio, Latindex y Scielo presentan cuatro estudios cada una, lo que indica que ambas bases de datos aportan de manera equitativa a la revisión. Por su parte, Scopus cuenta con dos estudios; aunque es una fuente menos utilizada en comparación con Latindex y Scielo, su relevancia como base de datos de alto nivel en la investigación científica es innegable. Finalmente, Redalyc también incluye un estudio, lo que indica que su contribución es similar a la de Dialnet.

Este análisis permite concluir que la mayoría de los estudios se concentran en Latindex y Scielo, lo que ha facilitado un mayor acceso a investigaciones en estas bases de datos sobre ciberseguridad en empresas. Además, la baja representación de Dialnet y Redalyc, cada una con un solo estudio, sugiere que fue difícil encontrar investigaciones relevantes en estas fuentes sobre el tema. Aunque Scopus tiene solo dos estudios, su presencia resalta su importancia en la revisión. La figura ofrece una visión clara de las fuentes de información utilizadas, destacando la relevancia de todas las bases de datos consultadas en el ámbito de la ciberseguridad en empresas.

Figura 2

Bases de datos de estudios incluidos

Volumen 4 No. 6 | Septiembre – diciembre 2022 | ISSN: 2788 - 65650 / ISSN-L: 2788 – 6565 / https://revistatalento.org/index.php/talento/



En el ámbito de la ciberseguridad, especialmente en el contexto empresarial, es primordial entender las diversas amenazas que pueden afectar la integridad de los activos digitales. La Tabla 1 de operacionalización de variables expone claramente las principales categorías de amenazas, que abarcan malware, ransomware, phishing y ataques DDoS. Stallings (2018) destaca que el malware representa una de las preocupaciones más significativas en el campo de la seguridad informática, debido a su capacidad para ocasionar daños severos.

Por su parte, Andress (2014) resalta el auge del ransomware, una amenaza que ha aumentado considerablemente en los últimos años y que tiene el potencial de interrumpir las operaciones empresariales al cifrar información esencial hasta recibir un pago. Asimismo, Vacca (2014) identifica el phishing como una técnica de engaño cada vez más elaborada, que emplea la manipulación psicológica para obtener datos sensibles. Finalmente, Kizza (2017) menciona los ataques DDoS como una táctica empleada por ciberdelincuentes para inhabilitar servicios en línea, lo que puede tener repercusiones serias en la reputación y funcionamiento de las organizaciones.

Por otra parte, la clasificación de los niveles de seguridad que las empresas implementan es igualmente importante. Peltier (2016) sugiere una segmentación que clasifica los niveles de seguridad en bajo, medio y alto. Esta categorización permite a las organizaciones evaluar de forma eficiente su nivel de preparación y su capacidad para responder a un ataque. Un nivel bajo de seguridad, por ejemplo, indica una vulnerabilidad significativa, mientras que un nivel alto, como indica Stallings (2018), refleja una infraestructura más sólida y capaz de resistir amenazas.

En lo que respecta a la efectividad de las estrategias de ciberseguridad, se pueden diferenciar enfoques preventivos y reactivos. Vacca (2014) subraya la relevancia de las estrategias preventivas, que comprenden la formación del personal y la instalación de firewalls, considerándolas básicas para establecer una defensa primordial contra las amenazas. Por otro lado, Andress (2014) aclara que los enfoques reactivos, que implican la creación de planes de respuesta ante incidentes, son igualmente críticos para reducir los daños una vez que se ha producido un ataque.

Tabla 1

Operacionalización de variables

Volumen 4 No. 6 | Septiembre – diciembre 2022 | ISSN: 2788 - 65650 / ISSN-L: 2788 – 6565 / https://revistatalento.org/index.php/talento/

Variables de Estudio	Dimensión	Indicador	Tipo de Medición
Tipos de Amenazas	Clasificación de Amenazas	Malware (Stallings, 2018)	Cualitativo
		Ransomware (Andress, 2014)	
		Phishing (Vacca, 2014)	
		Ataques DDoS (Kizza, 2017)	
Niveles de Seguridad	Categorización de Niveles de Seguridad	Bajo (Peltier, 2016)	Cualitativo
		Medio (Peltier, 2016)	
		Alto (Stallings, 2018)	
Efectividad de Estrategias	Evaluación de Estrategias	Enfoques Preventivos e.g., capacitación de personal, firewalls (Vacca, 2014)	Cualitativo / Cuantitativo
		Enfoques Reactivos e.g., planes de respuesta ante incidentes (Andress, 2014)	Cualitativo / Cuantitativo

Los estudios recientes sobre ciberseguridad y gestión de riesgos, analizados en esta revisión sistemática, revelan un panorama complejo donde cada nación enfrenta retos y oportunidades singulares en un contexto global marcado por un incremento en las ciberamenazas. La Tabla 2 presenta los estudios que se han incluido en esta revisión, cuyos resultados se describen a continuación.

En primer lugar, Aguilar (2021) señala que América Latina enfrenta carencias significativas en el desarrollo de capacidades cibernéticas y en la implementación de políticas nacionales efectivas. Estas deficiencias obstaculizan la creación de una Estrategia Nacional de Ciberseguridad, que es necesaria para proteger la seguridad nacional de las amenazas cibernéticas. La falta de base estructural adecuada es un problema común que se encuentra en numerosos países de la región, lo que indica una necesidad de fortalecer las capacidades institucionales y los marcos normativos en ciberseguridad.

En el contexto colombiano, Striseo y Striseo (2024) destacan la importancia de que las organizaciones adopten un enfoque proactivo y dinámico en la gestión de riesgos. Es decir, no solo se requiere inversión en innovación tecnológica, sino también el fomento de una cultura organizacional orientada a la resiliencia. De esta manera, las empresas no solo buscan mitigar riesgos potenciales, sino que también intentan aprovechar las oportunidades que ofrece la digitalización, lo que resulta esencial en un mundo cada vez más interconectado.

En cuanto al sector financiero en Ecuador, Ojeda-Contreras et al. (2020) subrayan la falta de estrategias claramente definidas para gestionar los riesgos cibernéticos en el sector popular y solidario. Ante este escenario, los autores proponen la implementación de estrategias basadas en el modelo COSO III, que integren la gestión del riesgo en los procesos institucionales, mejorando así la protección de la información y la seguridad general del sector. Por tanto, las entidades deben incorporar prácticas de evaluación y gestión de riesgos para asegurar una mayor resiliencia ante ciberamenazas.

Romero (2018), al referirse a México, enfatiza que la ciberseguridad debe considerarse una cuestión de seguridad nacional, dado su impacto directo sobre bienes públicos esenciales. La interrupción o el daño a estos servicios podría tener consecuencias devastadoras para la población, lo que resalta aún más la necesidad de implementar estrategias robustas y efectivas de ciberseguridad para salvaguardar los intereses nacionales.

Al adentrarse en el marco normativo en Colombia, Jiménez-Almeira y Enrique (2023) analizan

que, aunque ha habido avances, el sistema actual de ciberseguridad todavía enfrenta limitaciones severas en términos de claridad y coordinación interinstitucional. De ahí que la creación de un plan nacional de ciberseguridad es importante para mejorar la implementación y eficacia de las medidas de prevención y respuesta ante riesgos cibernéticos. Complementando esta crítica, Aguilar-Antonio (2019) observa que las estrategias de ciberseguridad en América Latina y México tienden a estar desactualizadas en relación con las nuevas ciberamenazas. Dicha desconexión entre las estrategias existentes y la realidad del ciberespacio aumenta la vulnerabilidad frente a los ciberataques, resultando en altos índices de incidentes de ciberagresiones en la región.

Desde un enfoque práctico, Minaya et al. (2023) destacan el papel esencial de la auditoría informática como un instrumento que promueve la transparencia en el entorno digital y es fundamental para el establecimiento de normas y estándares que protejan los activos de información. De esta manera se resalta la necesidad de que las organizaciones establezcan mecanismos robustos que fortalezcan su ciberseguridad, garantizando que se cumplan las regulaciones pertinentes y se mantenga la integridad de los datos.

Además, Cusme et al. (2024) subrayan que el crecimiento del comercio electrónico en Ecuador plantea nuevos desafíos, especialmente en materia de ciberseguridad y protección de datos. Las empresas están bajo la presión de adaptarse a las crecientes expectativas de los consumidores en un entorno digital que exige rapidez y personalización en el servicio. Esta realidad exige un enfoque empresarial ágil, capaz de gestionar la complejidad del mercado actual y responder de manera efectiva a las amenazas.

Rolón (2024) complementa esta tendencia al examinar el impacto de la transformación tecnológica en la gestión de inventarios de las MIPYMES en Paraguay. Si bien la adopción de nuevas tecnologías ha modernizado estos procesos, también ha incrementado la vulnerabilidad a los ciberataques, ilustrando así los riesgos duales que conlleva la digitalización. Es fundamental que las MIPYMES implementen estrategias adecuadas para equilibrar la innovación con la ciberseguridad.

Así, se hace evidente que, en el contexto actual de una creciente digitalización, las empresas enfrentan nuevos riesgos y vulnerabilidades que afectan tanto sus recursos físicos como digitales. Trujillo-Avilés et al. (2024), resalta que el desarrollo tecnológico ha transformado significativamente el panorama de amenazas al que se enfrentan las organizaciones. Los autores identifican que entre los principales riesgos se encuentran los accesos no autorizados, los ciberataques, la sustracción de información confidencial, la alteración de datos y la exposición de información sensible. Estos riesgos están directamente relacionados con vulneraciones a la seguridad de la información, lo que hace imprescindible la implementación de estrategias de ciberseguridad efectivas que protejan los datos y garanticen la integridad de la operación empresarial.

Los autores también enfatizan la necesidad de que las empresas establezcan mecanismos claros dentro de sus estrategias digitales para asegurar el correcto uso, autorización y acceso a los datos personales de sus clientes. De esta manera, se está protegiendo la información y se genera confianza entre los consumidores, un factor esencial en el entorno competitivo actual. Además, el proceso de auditoría en ciberseguridad se presenta como un elemento clave. Los autores sugieren que enfocar las auditorías hacia los aspectos críticos de las organizaciones es fundamental, permitiendo así evaluar la efectividad de los controles de seguridad y el cumplimiento de normativas de protección existentes.

Es decir, el trabajo de Trujillo-Avilés et al. (2024) pone de relieve que, en un mundo cada vez más conectado, la ciberseguridad es un pilar fundamental para la sostenibilidad y el éxito de las empresas. La implementación de estrategias adecuadas y la realización de auditorías efectivas son pasos imprescindibles para mitigar riesgos y salvaguardar la información en un entorno digital en constante evolución. En el contexto de la creciente preocupación por la ciberseguridad en las empresas modernas, Said y Noha (2019) presentan una revisión de los métodos de medición y evaluación de la ciberseguridad. Este estudio, realizado en Egipto, destaca la importancia de estos métodos como estándares fundamentales para evaluar la postura de seguridad de una organización.

Los autores argumentan que los métodos de evaluación de seguridad garantizan la integridad de las redes, los sistemas y los datos. Sin una metodología adecuada para evaluar la seguridad, la alta dirección de las empresas se enfrenta a una pregunta crítica: "¿Estamos lo suficientemente seguros?". Esta interrogante es decisiva para la toma de decisiones informadas y permite identificar las áreas que requieren mejoras y determinar el tiempo, esfuerzo y recursos financieros necesarios para el desarrollo de la seguridad de la información.

Said y Noha (2019) enfatizan que la falta de un método de evaluación efectivo lleva a las organizaciones a subestimar sus vulnerabilidades, lo que puede ser peligroso ante ciberataques. Por lo tanto, los autores concluyen que implementar métodos de evaluación de seguridad robustos es vital para que las empresas puedan proteger sus activos con el fin de planificar de manera efectiva las inversiones en ciberseguridad. Finalmente, en el ámbito de la inteligencia artificial, Guerrero et al. (2024) destacan su potencial para revolucionar la toma de decisiones financieras. Sin embargo, enfatizan que su éxito depende de la supervisión humana y la capacitación, reconociendo que se requiere de inversión en tecnología para mejorar la gestión de riesgos.

Los estudios revisados subrayan que, aunque cada país presenta sus propios desafíos y oportunidades en ciberseguridad, existe una convergencia en la necesidad de establecer marcos estratégicos, normativos y de innovación que permitan a las organizaciones adaptarse y protegerse eficazmente en un entorno digital en constante evolución. La colaboración, la formación y la inversión en tecnologías emergentes son clave para fortalecer la capacidad de respuesta frente a las ciberamenazas.

Tabla 2

Estudios incluidos en la revisión

Autor/año	Título del estudio	Contexto
Aguilar (2021)	Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior.	América Latina
Striseo y Striseo (2024)	Administración de riesgos en la era digital: Evaluar los desafíos y oportunidades que presenta la administración de riesgos en la era digital, y cómo las empresas pueden adatarse a estos cambios.	Colombia
Ojeda-Contreras et al. (2020)	Gestión del riesgo y la ciberseguridad en el sector financiero popular y solidario del Ecuador.	Ecuador

Volumen 4 No. 6 | Septiembre – diciembre 2022 | ISSN: 2788 - 65650 / ISSN-L: 2788 – 6565 / https://revistatalento.org/index.php/talento/

Romero (2018)	Conceptualización de una estrategia de ciberseguridad para la seguridad nacional de México.	México
Jiménez-Almeira y Enrique (2023)	Ciberseguridad y Seguridad Integral: un análisis reflexivo sobre el avance normativo en Colombia.	Colombia
Aguilar-Antonio (2019)	Hechos ciberfísicos: una propuesta de análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad.	México
Minaya et al. (2023)	Normas y estándares en auditoría: una revisión de su utilidad en la seguridad informática.	Ecuador
Cusme et al. (2024)	Comercio electrónico y gestión empresarial: retos y oportunidades en el mercado actual.	Ecuador
Rolón (2024)	Transformación Tecnológica en el Modelo de Gestión de Inventarios en las Mipymes, Revisión Bibliográfica.	Paraguay
Said & Noha (2019)	A Review of Cyber-security Measuring and Assessment Methods for Modern Enterprises.	Egipto
Trujillo-Avilés et al. (2024)	Estrategias de Auditoría en ciberseguridad y su importancia en las empresas una revisión bibliográfica.	Ecuador
Guerrero et al. (2024)	Impacto de la inteligencia artificial en la toma de decisiones financieras: Oportunidades y desafíos para los líderes empresariales.	México

Desafíos que enfrenta la ciberseguridad, asumidos de (Said & Noha, 2019)

La ciberseguridad enfrenta muchos desafíos, que están en constante aumento con el progreso tecnológico que se potencia en la actualidad. Entre los desafíos más prevalentes en las empresas modernas se encuentran:

Humano: El elemento humano es la parte más débil de la cadena de seguridad en cualquier empresa moderna. El éxito de los ciberataques es resultado de los errores que cometen. Las empresas modernas deben prestar especial atención a la capacitación del personal, especialmente de aquellos empleados no técnicos, con el fin de aumentar su conciencia de seguridad y evitar los errores que provocan violaciones de seguridad.

Entender la importancia de la ciberseguridad: La falta de comprensión por parte de la dirección y de los individuos en las empresas sobre la importancia de la ciberseguridad es uno de los desafíos para esta. La falta de conciencia de los gerentes acerca de la importancia de la ciberseguridad conduce a la falta de apoyo para sus sistemas de protección y a la actualización continua de los mismos, creando brechas, así como la falta de conciencia de los individuos sobre la importancia de la ciberseguridad, lo que conlleva a errores graves que provocan violaciones de seguridad.

Big Data: Los grandes datos provenientes del cibercrimen plantean desafíos; las empresas quieren extraer valor de esos datos, pero la naturaleza central de los grandes almacenes de datos crea nuevos desafíos de seguridad. Los datos deben garantizarse como seguros durante el proceso de procesamiento. Por lo tanto, se deben implementar controles alrededor de los mismos datos y también controles alrededor de las aplicaciones y sistemas que almacenan y procesan los datos.

IoT: Los electrodomésticos conectados a Internet representan un gran desafío para la ciberseguridad, pero carecen de los medios para protegerse, por lo que suponen una amenaza seria para la privacidad de los individuos y la seguridad de las empresas. Estos dispositivos, conocidos como objetos de Internet, representan un ejército de durmientes que pueden ser mal utilizados para atacar

los sistemas más poderosos en cuestión de momentos. En 2021 se estimó 27.1 mil millones de dispositivos conectados a nivel global, por lo que este problema empeoraró con el tiempo. Varias conferencias recientes sobre ciberseguridad revelan serias fallas de seguridad en el Internet de las cosas. Algunas mostraron cómo pueden ser secuestrados los coches autónomos y cómo se pueden controlar a distancia dispositivos médicos, como los marcapasos. Aunque esto es indudablemente preocupante, lo que lo hace aún más vulnerable ante ataques potenciales.

Evaluación de detección de virus: Se utilizan detectores de virus para evitar virus que se despliegan y se utilizan como un punto de acceso principal a la red, por lo que la herramienta se identifica de acuerdo con los requisitos de seguridad. La segunda parte es la evaluación de los posibles riesgos de seguridad de los elementos físicos circundantes.

Seguridad física, que puede evaluarse a través de cuatro métodos:

Método de evaluación de amenazas sociales: Es una evaluación del eslabón más débil de la cadena de seguridad, que es el elemento humano, mediante la realización de un conjunto de pruebas, como la ingeniería social, para identificar sus debilidades que pueden ser atacadas por los hackers.

Método de evaluación de amenazas de hardware: Identificar los riesgos potenciales que surgen de los elementos físicos de la computadora y la red e identificar los procedimientos más importantes que se deben seguir para evitar dicho tipo de riesgo.

Método de evaluación de políticas y medidas de contrarresto: Evaluar la eficiencia y efectividad de las políticas y medidas de contrarresto de la organización y su conformidad con las políticas internacionales de seguridad de la información.

Método de evaluación de amenazas naturales: Identificar riesgos potenciales derivados de desastres y factores naturales e identificar las acciones más importantes que deben tomarse para evitar dichos riesgos.

Una de las mejores maneras de prevenir ciberataques es aumentar la conciencia de seguridad sobre la importancia de la ciberseguridad para los individuos y la administración, y capacitarlos en las medidas de seguridad más simples posibles para enfrentar los riesgos potenciales que pueden surgir en el contexto del progreso tecnológico que ha transformado todas las transacciones diarias a nivel personal y empresarial.

DISCUSIÓN

El análisis crítico de los resultados presentados en esta revisión sistemática revela una realidad compleja y multifacética, donde cada país enfrenta sus propios desafíos y oportunidades en un entorno global marcado por el aumento de las ciberamenazas.

Una de las contribuciones más significativas de los estudios es el reconocimiento de las carencias en la capacidad cibernética en América Latina, planteado por (Aguilar, 2021). Este resultado resalta la necesidad de establecer políticas nacionales efectivas y desarrollar una Estrategia Nacional de Ciberseguridad que, según el autor, es importante para proteger la seguridad nacional. Este enfoque es corroborado por otros estudios que sugieren la necesidad de estrategias proactivas y dinámicas,

como lo proponen Striseo y Striseo (2024), quienes destacan la importancia de invertir en tecnología y fomentar una cultura organizacional resiliente.

No obstante, el estudio presenta limitaciones al no profundizar en las estrategias metodológicas implementadas por distintas organizaciones en sus respectivas naciones. Aunque Ojeda-Contreras et al. (2020) señalan la falta de estrategias en el sector financiero de Ecuador, no se aborda en detalle cómo estas iniciativas podrían adaptarse a las particularidades del contexto ecuatoriano ni se discuten ejemplos concretos de implementación.

Asimismo, Romero (2018) subraya que la ciberseguridad es un tema de seguridad nacional en México, enfatizando las consecuencias que la interrupción de servicios esenciales puede conducir. Esta afirmación revela la interdependencia entre la seguridad nacional y la ciberseguridad, pero también plantea la cuestión de cómo se puede traducir esta importancia en acciones concretas y coordinadas a nivel gubernamental y empresarial.

El marco normativo abordado por Jiménez-Almeira y Enrique (2023) también puede considerarse una contribución valiosa, debido a la necesidad de claridad y cohesión en las políticas de ciberseguridad. Sin embargo, el análisis crítico indica que, a pesar del progreso, aún persisten limitaciones significativas que obstaculizan la implementación efectiva de estas políticas.

Aguilar-Antonio (2019) destaca la desconexión entre las estrategias de ciberseguridad y las nuevas ciberamenazas, un aspecto que es necesario tener en cuenta ya que resalta cómo las organizaciones pueden quedar expuestas ante amenazas emergentes. La falta de actualización contínua detectada constituye un riesgo que necesita ser objeto de atención prioritaria por parte de las empresas y los gobiernos.

En un contexto práctico, las observaciones de Minaya et al. (2023) sobre el papel de la auditoría informática como herramienta para promover la transparencia resaltan la importancia de establecer mecanismos robustos en las organizaciones. No obstante, el estudio podría haberse beneficiado de ejemplos concretos sobre cómo estas auditorías se han implementado y los resultados que han producido en diversas industrias.

El análisis de Cusme et al. (2024) sobre los retos planteados por el crecimiento del comercio electrónico en Ecuador añade una dimensión importante a la discusión, subrayando la necesidad de adaptaciones rápidas en ciberseguridad. Sin embargo, sería útil contar con más información sobre cómo las empresas están respondiendo a estas demandas, así como las efectivas mejores prácticas implementadas.

Finalmente, el trabajo de Trujillo-Avilés et al. (2024) y la revisión de Said y Noha (2024) en relación con los métodos de evaluación de la ciberseguridad presentan un enfoque para comprender la postura de seguridad de las organizaciones. La necesidad de una metodología adecuada constituye elemental en el debate contemporáneo sobre la ciberseguridad, pero se debe reconocer que el proceso de evaluación y su implementación efectiva son complejos y requieren un compromiso continuo de todas las partes interesadas.

Aunque esta revisión sistemática destaca una serie de contribuciones valiosas sobre la ciberseguridad y la gestión de riesgos en diferentes contextos nacionales, también pone de manifiesto varias limitaciones en los enfoques existentes. Para afrontar la creciente realidad de las ciberamenazas.

Por esta razón las empresas deben adaptar sus estrategias y marcos normativos, así como deben aprender de las experiencias de otros países y sectores. La colaboración, la educación y la inversión en tecnología emergente fortalecen la capacidad de las empresas de enfrentar desafíos en un entorno digital cada vez más complejo.

CONCLUSIONES

La revisión sistemática ha permitido identificar y comprender los principales desafíos que enfrentan las empresas en la protección de sus activos digitales. Se describe que las amenazas cibernéticas, como el malware, el ransomware y el phishing, presentan un riesgo creciente cuya complejidad y frecuencia continúan aumentando.

Asimismo, se observó que la implementación de niveles de seguridad varía significativamente. Muchas empresas, a pesar de ser conscientes de los riesgos, tienden a adoptar enfoques reactivos en lugar de preventivos, lo que las deja expuestas a violaciones de datos y otros incidentes cibernéticos. La falta de capacitación y conciencia sobre ciberseguridad entre los empleados también se identifica como un factor crítico que contribuye a la vulnerabilidad de las organizaciones. Es esencial que las empresas integren la educación continua en ciberseguridad como parte de su cultura organizacional para fomentar un entorno más seguro.

En términos de estrategias, se encontró que las soluciones de ciberseguridad más efectivas combinan tecnología avanzada y políticas bien definidas. La adopción de tecnologías como inteligencia artificial ha demostrado ser importante en la mitigación de riesgos. Además, las estrategias colaborativas y el intercambio de información sobre amenazas entre empresas pueden fortalecer aún más las defensas cibernéticas, permitiendo una mejor adaptación a un entorno de amenazas en evolución.

Finalmente, esta revisión ha resaltado la importancia de un enfoque integrador hacia la ciberseguridad que incluya no solo soluciones técnicas, sino también una cultura organizacional que valore la seguridad. Las recomendaciones derivadas de este estudio proporcionan un marco claro para que las empresas evalúen y mejoren sus prácticas de ciberseguridad, protegiendo así de manera más efectiva sus activos digitales ante un panorama de amenazas cada vez más complejo. La ciberseguridad no es solo una responsabilidad del departamento de tecnología, sino una prioridad estratégica que debe ser adoptada y fomentada por todas las empresas.

REFERENCIAS

Aguilar, A.J.M. (2021). Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior. Estudios internacionales (Santiago), 53(198), 169-197. https://dx.doi.org/10.5354/0719-3769.2021.57067

Aguilar-Antonio, J.M. (2019). Hechos ciberfísicos: una propuesta de análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad. Revista Latinoamericana de Estudios de Seguridad, 25, 24-40. https://dx.doi.org/10.17141/urvio.25.2019.4007

Andress, J. (2014). The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. Syngress.

Cusme, P.C.M., Recalde, A.L.M., Rodríguez, M.M.E., Rodríguez, M.K.A. et al. (2024). Comercio electrónico y gestión empresarial: retos y oportunidades en el mercado actual. South Florida Journal of Development, Miami, v.5(9), 01-17. https://dx.doi.org/10.46932/sfjdv5n9-041

Cybersecurity Ventures. (2022). Cybercrime Report. https://s3.ca-central-1.amazonaws.com/esentire-dot-com-assets/assets/resourcefiles/2022-Official-Cybercrime-Report.pdf

Guerrero, W.A., Camacho-Galindo, S., Guerrero-Martin, L.E., Arévalo, J.C., de Freitas, P.P., Gómes, V.J.C., Fernandes, F.A.S., and Guerrero-Martin, C.A. (2024). Impacto de la inteligencia artificial en la toma de decisiones financieras: Oportunidades y desafíos para los líderes empresariales. DYNA, 91(233), 168-177. https://doi.org/10.15446/dyna.v91n233.114660

Jiménez-Almeira, G.A., & Enrique, L.D. (2023). Ciberseguridad y Seguridad Integral: un análisis reflexivo sobre el avance normativo en Colombia. Revista Ibérica de Sistemas e Tecnologias de Informação 62(10), 16-31. https://media.proquest.com/media/hms/PFT/1/CMtxV?_s=tiPJWYKwbWX4wPQIq1ftCgEWmxk%3D

Kizza, J. M. (2017). Guide to Computer Network Security. Springer.

Minaya, M.M.M., Minaya, M.R.W. Intriago, N.M.L., & Intriago, N.J.A. (2023). Normas y estándares en auditoría: una revisión de su utilidad en la seguridad informática. Revista Científica Arbitrada Multidisciplinaria PENTACIENCIAS, 5(4), 584–599. https://doi.org/10.59169/pentaciencias.v5i4.700

Ojeda-Contreras, F.I., Moreno-Narváez, V.P., Torres-Palacios, M.M. (2020). Gestión del riesgo y la ciberseguridad en el sector financiero popular y solidario del Ecuador. Revista Interdisciplinaria de Humanidades, Educación, Ciencia y Tecnología, VI(2), 192-2019. https://doi.org/10.35381/cm.v6i2.366

Peltier, T. R. (2016). Information Security Risk Analysis. Auerbach Publications.

Ponemon Institute. (2021). Cost of a Data Breach Report 2021. https://www.dataendure.com/wp-content/uploads/2021_Cost_of_a_Data_Breach_-2.pdf

Rolón, R.D.A. (2024). Transformación Tecnológica en el Modelo de Gestión de Inventarios en las Mipymes, Revisión Bibliográfica. Ciencia Latina Revista Científica Multidisciplinar, 8(1), 3551-3566. https://doi.org/10.37811/cl_rcm.v8i1.9701

Romero, G.J. (2018). Conceptualización de una estrategia de ciberseguridad para la seguridad nacional de México. Revista Internacional de Ciencias Sociales y Humanidades SOCIOTAM XXVIII (2), 69-93. Recuperado de https://www.redalyc.org/journal/654/65458498003/html/

Said, F.A., Noha, A.H. (2019). A Review of Cyber-security Measuring and Assessment Methods for Modern Enterprises. International Journal on Informatics Visualization, 3(2), 157-176. https://joiv.org/index.php/joiv/article/view/239/202

Stallings, W. (2018). Cryptography and Network Security: Principles and Practice. Pearson.

Striseo, M.D.A., & Striseo, M.S.J. (2024). Administración de riesgos en la era digital: Evaluar los desafíos y oportunidades que presenta la administración de riesgos en la era digital, y cómo las empresas pueden adaptarse a estos cambios. Sapiens International Multidisciplinary Journal, 1(1), 61-76. https://revistasapiensec.com/index.php/sapiens/article/view/5

Trujillo-Avilés, M.N., Morales-López, D.A., Taipe-Yanez, J.F., Pallo-Tulmo, P.A. (2024). Estrategias de Auditoría en ciberseguridad y su importancia en las empresas una revisión bibliográfica. Journal Scientific MQRInvestigar, 8(2), 3889-3913 https://doi.org/10.56048/MQR20225.8.2.2024.3889-3913

Vacca, J. R. (2014). Computer and Information Security Handbook. Morgan Kaufmann.