Análisis de los desafíos de ciberseguridad y los métodos de protección en los sistemas de información empresarial

Julián Steven Barrera Gutiérrez

Asesor

Jenny Fernanda Restrepo Santacruz

Universidad Nacional Abierta y a Distancia – Unad

Escuela De Ciencias Básicas, Tecnología e Ingeniería ECBTI

Especialización En Seguridad Informática

2026

Resumen

La transformación digital ha incrementado la importancia de los Sistemas de Información Empresariales y, al mismo tiempo, su exposición a amenazas que comprometen la seguridad de la información. Esta investigación tuvo como objetivo analizar los desafíos de ciberseguridad y los métodos de protección en estos sistemas mediante una revisión sistemática de literatura basada en la metodología PRISMA.

Bajo un enfoque cualitativo y documental, se analizaron estudios científicos relacionados con vulnerabilidades, amenazas, gestión del riesgo y estrategias de protección. Los resultados evidenciaron que los principales desafíos están asociados a factores tecnológicos, organizacionales y humanos, destacándose amenazas como la ingeniería social, las vulnerabilidades de acceso y las amenazas internas.

Se concluye que la ciberseguridad debe abordarse desde una perspectiva integral que combine gestión del riesgo, controles tecnológicos y cultura organizacional, fortaleciendo la resiliencia de las organizaciones frente a un entorno digital cada vez más complejo.

Palabras clave: Ciberseguridad, Sistemas de Información Empresariales, Gestión del Riesgo, Gobernanza de Seguridad, Factor Humano.

Abstrac

Digital transformation has increased the importance of Enterprise Information Systems and, at the same time, their exposure to threats that compromise information security. This research aimed to analyze cybersecurity challenges and protection methods in these systems through a systematic literature review based on the PRISMA methodology.

Using a qualitative and documentary approach, scientific studies related to vulnerabilities, threats, risk management, and protection strategies were analyzed. The results showed that the main challenges are associated with technological, organizational, and human factors, highlighting threats such as social engineering, access vulnerabilities, and insider threats.

It is concluded that cybersecurity must be addressed from a comprehensive perspective that combines risk management, technological controls, and organizational culture, strengthening the resilience of organizations in the face of an increasingly complex digital environment.

Keywords: Cybersecurity, Enterprise Information Systems, Risk Management, Security Governance, Human Factor.

Tabla de Contenido

Lista de Tablas

Introducción

El acelerado proceso de transformación digital ha redefinido la forma en que las organizaciones gestionan la información, integrando tecnologías que soportan operaciones críticas a través de los Sistemas de Información Empresariales (SIE). Estos sistemas, al constituirse como el núcleo operativo de las organizaciones, no solo facilitan la toma de decisiones y la automatización de procesos, sino que también incrementan de manera significativa la exposición a riesgos asociados a la ciberseguridad. En este contexto, la protección de los activos de información ha dejado de ser una función meramente técnica para convertirse en un componente estratégico dentro de la sostenibilidad organizacional.

El crecimiento de amenazas cibernéticas, caracterizadas por su sofisticación, persistencia y capacidad de adaptación, ha evidenciado que los modelos tradicionales de seguridad resultan insuficientes frente a entornos digitales dinámicos y altamente interconectados. Las vulnerabilidades en infraestructuras tecnológicas, las debilidades en los procesos organizacionales y la incidencia del factor humano configuran un escenario complejo en el que la seguridad de la información debe abordarse desde una perspectiva integral. En consecuencia, la ciberseguridad en los Sistemas de Información Empresariales se posiciona como un campo de estudio que articula dimensiones tecnológicas, organizacionales y estratégicas.

En este marco, la presente monografía tiene como propósito analizar los desafíos de ciberseguridad y los métodos de protección en los Sistemas de Información Empresariales, a partir de la revisión sistemática de literatura científica reciente. Para ello, se adopta un enfoque metodológico basado en el protocolo PRISMA, el cual permite garantizar la transparencia, trazabilidad y rigor en la selección, evaluación y síntesis de estudios académicos. Esta aproximación metodológica facilita la construcción de un análisis fundamentado en evidencia,

superando enfoques meramente descriptivos y permitiendo identificar patrones, tendencias y vacíos en el conocimiento existente.

El desarrollo del estudio se estructura a partir de tres ejes analíticos: en primer lugar, la identificación de los principales desafíos, vulnerabilidades y riesgos que afectan a los Sistemas de Información Empresariales; en segundo lugar, el análisis comparativo de las amenazas documentadas en la literatura, con el fin de reconocer regularidades y divergencias en su conceptualización; y, finalmente, la evaluación crítica de las estrategias, enfoques y prácticas de protección propuestas, valorando su aporte teórico y su aplicabilidad en el fortalecimiento de la seguridad organizacional.

De esta manera, la investigación busca contribuir a la comprensión del fenómeno de la ciberseguridad en entornos empresariales desde una perspectiva analítica y estructurada, aportando una síntesis crítica del estado del arte que permita no solo organizar el conocimiento existente, sino también evidenciar la necesidad de enfoques integradores que respondan a la complejidad de los Sistemas de Información Empresariales en contextos de riesgo creciente.

Definición del Problema

Antecedentes del Problema

La creación e implementación de tecnologías en muchas empresas permiten alcanzar altos niveles de optimización y efectividad en sus procesos, mejorando significativamente la calidad de los servicios ofrecidos a clientes potenciales. La sistematización, el estudio de datos y los esquemas digitales son instrumentos que, bien empleadas, pueden crear ventajas profesionales significativas. No obstante, estos progresos tecnológicos sobrellevan riesgos inherentes que no deben ser subestimados.

Regularmente, las compañías se encuentran exhibidas a diferentes riesgos en el ámbito de la seguridad informática. Los ciberataques pueden producir grandes detrimentos económicas y perjuicios a la notoriedad de la compañía. Entre los riesgos más frecuentes se hallan el robo de datos, la investigación industrial y las interrupciones del servicio. Los ciberdelincuentes emplean condiciones sofisticadas, como el phishing, el malware y los ataques de Ransomware, para consentir a información confidencial y emplearla con terminaciones maliciosos.

El progreso de las amenazas cibernéticas ha sido rápida y constante. Primeramente, las amenazas se precisaban en virus simples y gusanos, pero han desarrollado hacia formas más sofisticadas como los ataques de día cero, el Spear Phishing y las amenazas persistentes modernas (APT). Estas amenazas actuales son más dificultosas de manifestar y aminorar, lo que acrecienta la necesidad de esquemas de seguridad modernos y actualizados. La progresiva sofisticación de las agresiones, como los exploits de día cero que sirven vulnerabilidades desconocidas, y las agresiones de Spear Phishing, que son soberanamente personalizados para engañar a individuos específicos, manifiestan la necesidad urgente de tácticas de ciberseguridad más fuertes.

En el escenario de los esquemas de información empresarial, las organizaciones manipulan diferentes tipologías de representaciones como ERP (Enterprise Resource Planning), CRM (Customer Relationship Management), SCM (Supply Chain Management), y HCM (Human Capital Management). Estas representaciones son fundamentales para la orientación fuerte de los recursos, las relaciones con los clientes, la cadena de abastecimiento y el capital humano. Los esquemas ERP consienten una constitución completa de las automatizaciones empresariales, desde la producción hasta la orientación financiera. Los sistemas CRM optimizan la orientación de las relaciones con los clientes y despliegan las condiciones de ventas y marketing. Las estructuras SCM suministran la orientación eficaz de la cadena de abastecimiento, comprimiendo costos y mejorando la productividad. Posteriormente, las estructuras HCM gestionan el capital humano de manera integral, desde la contratación hasta la formación y el progreso profesional. Debido a su jerarquía estratégica, estos esquemas son objetivos fascinantes para los ciberdelincuentes, dado que cualquier impedimento o maniobra de estos esquemas puede tener derivaciones destructoras para una compañía.

Los desafíos presentes de ciberseguridad contienen una amplia gama de amenazas y vulnerabilidades habituales. Entre estas se hallan las brechas de datos, el malware, el Ransomware y los ataques DDOS (Distributed Denial Of Service). Las brechas de datos pueden trascender en la exhibición de información sensitivo, comprometiendo tanto a la compañía como a sus clientes. El malware, conteniendo virus, troyanos y spyware, puede inspirarse en los esquemas y robar información o causar daños. Las agresiones de Ransomware encriptan datos críticos, solicitando un rescate para su liberación, lo que puede suspender sistematizaciones empresariales. Los ataques DDOS saturan los servidores con tráfico monstruoso, produciendo interrupciones del servicio e impactando la disponibilidad de esquemas críticos. Las

vulnerabilidades pueden estar presentes en el software, las configuraciones de red, o debido a errores humanos. La defensa de los esquemas de información empresarial demanda una perspicacia integral de estas amenazas y la ejecución de medidas apropiadas para mitigarlas.

Para afrontar estos retos, las empresas deben ajustar normativas y esquemas examinados en el ámbito internacional. Entre los más notables se hallan la ISO/IEC 27001, que instituye requerimientos para un esquema de gestión de la seguridad de la información (SGSI), y el NIST Cybersecurity Framework, que suministra un enfoque fundado en modelos para optimizar la dirección de riesgos de ciberseguridad. La ISO/IEC 27001 favorece a las organizaciones a instituir, efectuar, conservar y optimizar un sistema de dirección de la seguridad de la información, respondiendo que se realicen inspecciones de seguridad apropiados para resguardar la información sensitiva. El NIST Cybersecurity Framework brinda un conjunto de pautas, esquemas y prácticas recomendadas para favorecer a las organizaciones a tramitar y comprimir los riesgos de ciberseguridad. Estas normativas ayudan a las organizaciones a efectuar experiencias de seguridad fuertes y a conservarse al día con las mejores experiencias de la industria. Asimismo, la adopción de estas normativas puede favorecer a las compañías a efectuar con requerimientos legales y regulatorios, así como a ganar la confianza de clientes y socios comerciales.

Se han reconocido numerosos casos en los que organizaciones que manejan redes y esquemas digitales para la realización de sus actividades han sido impactadas por estos ataques. Estas organizaciones pueden ser blanco de cibernautas malintencionados que buscan aprovecharse de vulnerabilidades en los esquemas de seguridad para detener datos sensitivos, como información financiera, personal o comercial. La infiltración de esta información no solo

complica la privacidad y la seguridad de los datos, sino que además puede trascender en ordenanzas legales y una pérdida de confianza por parte de los clientes.

Es esencial que las compañías ajusten medidas proactivas para aminorar estos riesgos. Esto contiene la ejecución de sistemas de seguridad fuertes, la formación continua del personal en experiencias de ciberseguridad, y la ejecución de auditorías normales para reconocer y corregir posibles vulnerabilidades. Las medidas de seguridad fuertes pueden contener firewalls, esquemas de localización y prevención de intrusiones, y cifrado de datos. La formación continua del personal es fundamental para afirmar que todos los colaboradores se encuentran al tanto de las últimas amenazas y de cómo resguardarse contra ellas. Las auditorías usuales admiten a las organizaciones valorar la efectividad de sus medidas de seguridad y hacer ajustes necesarios. Solo mediante una táctica integral de seguridad informática se puede certificar la defensa de los datos y el sustento de la integridad operativa en un ambiente cada vez más digitalizado.

Formulación del Problema

¿Cuáles son los principales desafíos de ciberseguridad y los métodos de protección identificados en la literatura científica reciente sobre los Sistemas de Información Empresarial?

Justificación

En los últimos años, las organizaciones han acelerado su transformación digital, integrando sistemas empresariales, plataformas en la nube y múltiples tecnologías que hacen más eficientes sus procesos. Sin embargo, este crecimiento también ha traído consigo nuevas amenazas de ciberseguridad que se vuelven cada vez más complejas y difíciles de detectar. Lo que antes eran ataques simples, hoy se ha convertido en técnicas más avanzadas como el spear phishing, los ataques de día cero, el Ransomware y otras formas de intrusión que pueden afectar seriamente la operación y los activos informáticos de cualquier empresa.

Esta situación ha despertado un interés académico importante por comprender cómo se originan estas amenazas, de qué manera afectan a los sistemas de información empresariales y qué estrategias de protección se han propuesto desde la investigación científica. Los sistemas como ERP, CRM, SCM o HCM manejan grandes volúmenes de información crítica, por lo que su vulneración no solo representa un problema técnico, sino también un riesgo para la continuidad del negocio, la reputación corporativa y el cumplimiento legal. Debido a ello, es fundamental analizar cómo la literatura académica describe estas amenazas y qué aportes ofrece para fortalecer la seguridad de la información.

Esta monografía surge precisamente de esa necesidad: revisar, organizar y analizar los estudios más recientes que abordan los desafíos de la ciberseguridad en entornos empresariales. Aunque existen numerosas publicaciones sobre ataques, vulnerabilidades, estándares y buenas prácticas, gran parte de esa información se encuentra dispersa o enfocada en casos particulares. Por eso resulta valioso realizar un análisis documental que permita identificar tendencias comunes, puntos críticos, enfoques teóricos y vacíos presentes en la investigación.

Además, es importante comprender que la ciberseguridad no depende únicamente de herramientas técnicas. La literatura destaca que factores como la gestión del riesgo, la capacitación del personal, la cultura organizacional y el cumplimiento de normativas también son esenciales para proteger los sistemas de información. Por ello, esta monografía busca integrar estas dimensiones y ofrecer una mirada más amplia, que ayude a entender cómo interactúan los elementos tecnológicos, humanos y administrativos en la construcción de un entorno seguro.

En este sentido, la justificación del estudio se basa en la importancia de analizar de forma rigurosa los retos actuales de la ciberseguridad y de consolidar el conocimiento existente para aportar claridad sobre los riesgos que enfrentan las organizaciones y las estrategias que propone la literatura para mitigarlos. Este trabajo contribuye a fortalecer la comprensión académica del tema y sirve como base para investigaciones futuras, en un contexto donde la protección de los sistemas de información es cada vez más esencial para la estabilidad y el crecimiento de las empresas.

Objetivos

Objetivo General

Analizar, desde la literatura científica reciente, los desafíos, vulnerabilidades y estrategias de protección en ciberseguridad que inciden en los Sistemas de Información Empresariales, mediante una revisión sistemática basada en la metodología PRISMA.

Objetivos Específicos

Identificar los principales desafíos y factores de riesgo de ciberseguridad reportados en la literatura científica sobre Sistemas de Información Empresariales.

Comparar las vulnerabilidades y amenazas documentadas en investigaciones académicas recientes, con el fin de establecer patrones y tendencias en el entorno organizacional.

Valorar críticamente las estrategias, enfoques y prácticas de protección propuestas en la literatura especializada, considerando su aporte teórico y su aplicabilidad en el fortalecimiento de la seguridad de la información.

Marco Referencial

Marco Conceptual

Evolución Conceptual de la Ciberseguridad en Entornos Empresariales

La conceptualización de la ciberseguridad ha experimentado una evolución significativa en las últimas décadas. Von Solms y Van Niekerk plantean la transición desde la seguridad de la información hacia un enfoque más amplio de ciberseguridad, destacando la necesidad de comprender el fenómeno más allá de la protección técnica tradicional. En esta misma línea, (Dan Craigen, 2014) proponen una estructura conceptual disciplinar que posiciona la ciberseguridad como un campo interdisciplinario que integra dimensiones tecnológicas, humanas y organizacionales.

Sin embargo, (Dhillon) advierten que la seguridad no puede analizarse exclusivamente desde un enfoque tecnológico, sino que debe entenderse como un fenómeno sociotécnico. Esta perspectiva resulta especialmente relevante en el contexto de los Sistemas de Información Empresariales (SIE), donde la interacción entre procesos organizacionales y plataformas tecnológicas determina el nivel real de exposición al riesgo.

Complementariamente, (Sultan AlGhamdi, 2020) demuestran empíricamente que la gobernanza de TI influye de manera significativa en la efectividad de la seguridad de la información. Este hallazgo refuerza la idea de que la ciberseguridad en entornos empresariales no depende únicamente de herramientas técnicas, sino de estructuras formales de gestión y supervisión estratégica.

Sistemas de Información Empresariales Como Activos Críticos y Estratégicos

Los Sistemas de Información Empresariales constituyen infraestructuras críticas que soportan funciones esenciales del negocio. La evidencia empírica demuestra que las brechas de

seguridad generan impactos económicos medibles. (Cavusoglu) y (Sanjay Goel, 2009) evidencian que los anuncios de incidentes de seguridad afectan negativamente el valor bursátil de las empresas. De manera complementaria, (Gordon, 2011) concluyen que las brechas de seguridad inciden directamente en el desempeño financiero organizacional.

Estos hallazgos confirman que la seguridad en los SIE no es únicamente un asunto técnico, sino un factor estratégico con implicaciones económicas. En este sentido, (Singer, 2014) argumentan que la ciberseguridad puede convertirse en una ventaja competitiva cuando se integra de manera estratégica en la gestión empresarial.

La convergencia de estos estudios permite afirmar que la protección de los SIE es un componente esencial de la sostenibilidad organizacional, ya que su vulnerabilidad compromete no solo la operación, sino también la confianza del mercado y la reputación corporativa.

Gestión del Riesgo en Sistemas de Información Empresariales

La gestión del riesgo emerge como un eje transversal en la literatura revisada. (Aven, 2015) propone una actualización conceptual del análisis y gestión del riesgo, destacando la importancia de enfoques estructurados y dinámicos. En concordancia, (Shameli-Sendi, 2015) desarrollan una taxonomía de métodos de evaluación de riesgos en seguridad de la información, lo que evidencia la necesidad de sistematización metodológica.

Desde una perspectiva organizacional, (Sánchez y otros, 2023) identifican factores críticos para la adopción efectiva de sistemas de gestión de seguridad de la información (SGSI), subrayando el papel del liderazgo y el compromiso institucional. Asimismo, (Kwon, 2014) comparan inversiones proactivas y reactivas en seguridad, concluyendo que las estrategias preventivas generan mejores resultados en términos de reducción de incidentes.

Factor Humano y Comportamiento Organizacional en la Seguridad de los SIE

Uno de los hallazgos más consistentes en la literatura analizada es la relevancia del factor humano como variable determinante en la seguridad organizacional. (Alshaikh, 2020) sostiene que el desarrollo de una cultura de ciberseguridad influye directamente en el comportamiento de los empleados. Esta postura es respaldada por (Bada, 2019) quienes demuestran que los programas de educación y concienciación mejoran significativamente las prácticas de seguridad.

Desde una perspectiva conductual, (Tejaswini Herath, 2009) evidencian que las sanciones y presiones organizacionales incrementan el cumplimiento de políticas de seguridad. Sin embargo, (Vance, 2012) advierten que las violaciones de políticas deben analizarse dentro de contextos específicos, considerando motivaciones individuales y estructuras organizacionales.

En relación con amenazas internas, (Posey, 2015) demuestran que el compromiso organizacional reduce la probabilidad de comportamientos riesgosos, mientras que (Jason R.C. Nurse, 2014) proponen un marco analítico para caracterizar y mitigar amenazas internas. Finalmente, (Robert E. Crossler, 2013) integran distintas perspectivas conductuales en un modelo que articula factores psicológicos, organizacionales y tecnológicos.

La convergencia de estos estudios evidencia que la protección de los SIE depende en gran medida de dinámicas organizacionales, cultura institucional y comportamiento individual, lo que refuerza la necesidad de estrategias integrales.

Tendencias Tecnológicas y Limitaciones Prácticas

En el ámbito tecnológico, la literatura destaca el uso creciente de técnicas de minería de datos y machine learning para la detección de intrusiones. Buczak y Guven (2016) presentan un análisis comparativo de métodos avanzados aplicados a la ciberseguridad, mientras que (Sarker, 2020) amplían esta perspectiva desde la ciencia de datos aplicada.

No obstante, (Sommer, 2010) advierten limitaciones prácticas en la implementación de modelos de aprendizaje automático en entornos reales, señalando problemas de generalización y alta tasa de falsos positivos. Este contraste evidencia que, aunque las tendencias tecnológicas ofrecen potencial significativo, su efectividad depende de la integración adecuada con procesos organizacionales y capacidades técnicas.

Por tanto, la innovación tecnológica debe evaluarse críticamente dentro del contexto operativo de los Sistemas de Información Empresariales.

Gestión de Incidentes y Resiliencia Organizacional

La gestión de incidentes constituye un componente esencial de la resiliencia organizacional. (Inger Anne Tøndel, 2014) identifican prácticas actuales en la gestión de incidentes, destacando la necesidad de procesos estructurados y coordinación interdepartamental. Estos hallazgos se complementan con la caracterización de amenazas internas propuesta por (Bada, 2019) que enfatiza la importancia de monitoreo continuo y análisis preventivo.

Metodología

Para desempeñar con los propósitos trazados en este estudio, se ha apartado una metodología fundada en la revisión metodología de la literatura (RSL), utilizando la habilidad PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses). PRISMA es una técnica validada que admite ejecutar exámenes estructuradas y transparentes de literatura académica, certificando el rigor metodológico solicitado para una monografía.

Este enfoque metodológico se fundamenta en la recopilación y análisis de estudios académicos sobre ciberseguridad, sistemas de información empresarial y estrategias de protección, asegurando la exclusión de fuentes no académicas como páginas web o blogs.

Enfoque Metodológico

Este estudio adopta un enfoque cualitativo y exploratorio, basado en una revisión sistemática de la literatura, con el objetivo de analizar los desafíos actuales en ciberseguridad y proponer estrategias de mitigación fundamentadas en evidencia científica. La revisión se estructura bajo la metodología PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses), garantizando el rigor académico en la selección y análisis de documentos.

Aplicación de la Metodología Prisma

Definir la Pregunta de Investigación

La pregunta de investigación guía el análisis y se formula de la siguiente manera:

¿Cómo aborda la literatura científica reciente los desafíos, vulnerabilidades y estrategias de protección en ciberseguridad asociados a los Sistemas de Información Empresariales?

Desarrollo del Protocolo

La búsqueda inicial realizada en las bases de datos académicas permitió identificar 313 artículos.

Después de eliminar 32 documentos duplicados, quedaron 281 estudios para revisión preliminar.

Durante la evaluación de títulos y resúmenes, se excluyeron 85 artículos por no ajustarse a los criterios establecidos.

Como resultado, 24 estudios cumplieron los criterios de inclusión y fueron seleccionados para su lectura completa y posterior análisis cualitativo.

Criterios de Inclusión:

Artículos científicos y conferencias indexadas en bases de datos reconocidas (Scopus, IEEE Xplore, Web of Science, Springer, ACM Digital Library).

Documentos publicados entre 2009 y 2024:

Estudios que aborden desafíos y estrategias en ciberseguridad empresarial.

Criterios de Exclusión

- Publicaciones sin revisión por pares (blogs, noticias, informes no académicos).
- Artículos sin acceso al texto completo.
- Estudios centrados únicamente en aspectos técnicos sin relación con entornos empresariales.
- Documentos que no aportaran información relevante para la caracterización del problema.

Se utilizarán términos de búsqueda como:

"Cybersecurity challenges in business information systems"

"Cybersecurity risk management in enterprises"

"Threats and mitigation strategies in corporate cybersecurity"

"Cybersecurity frameworks and enterprise protection"

Se realizará la búsqueda en bases de datos académicas y se documentará el número de estudios encontrados, seleccionados y descartados.

Selección de Estudios

Los estudios serán filtrados en dos etapas:

Revisión de títulos y resúmenes para verificar alineación con los objetivos del estudio.

Revisión del texto completo para confirmar su pertinencia en el análisis.

Extracción de Datos

Se diseñará una tabla de extracción de datos con los siguientes campos:

- Autor y año.
- Título del articulo
- Tipo
- Diseño metodológico
- Categoría
- Hallazgos Principales

Evaluación de Calidad

Cada estudio será evaluado con base en:

- Relevancia científica (¿Aporta información clave para la investigación?).
- Rigor metodológico (¿Utiliza un enfoque sólido y validado?).
- Impacto en el campo (¿Es un estudio ampliamente citado o innovador?).

Síntesis de la Evidencia

Se realizará un análisis comparativo de los estudios seleccionados para identificar patrones, tendencias y vacíos de investigación. Los hallazgos se organizarán en categorías temáticas.

Presentación de Resultados

Los resultados se presentarán una discusión narrativa que sintetice las tendencias clave en ciberseguridad empresarial.

Matriz de Extracción y Análisis De Datos

Con el fin de garantizar rigor metodológico y coherencia entre el proceso de revisión sistemática y los objetivos planteados en la investigación, se diseñó una matriz de extracción y análisis de datos como instrumento estructurador del estudio.

Esta matriz permitió sistematizar de manera organizada y comparativa la información relevante de los 24 artículos científicos seleccionados bajo el protocolo PRISMA. Más allá de una simple compilación bibliográfica, la matriz constituyó una herramienta analítica que facilitó la identificación de patrones, tendencias investigativas, enfoques metodológicos predominantes y vacíos conceptuales en el campo de la ciberseguridad organizacional.

Para cada estudio se registraron variables estratégicamente definidas, tales como: autor y año de publicación, título del artículo, tipo y diseño metodológico, categoría analítica, principales hallazgos reconocidas por los autores y contribución específica a los objetivos de la presente investigación. Esta estructura permitió establecer una relación directa entre la evidencia científica recopilada y las preguntas que orientan el estudio.

Tabla 1

Matriz de Extracción y Análisis de los Estudios Científicos Incluidos en la Revisión Sistemática

Autor / Año	Título del artículo	Tipo	Diseño metodológico	Categoría	Hallazgos principales
Von Solms & Van Niekerk	From information security to cyber security	Conceptual	Análisis teórico	Gobernanza	Evolución hacia enfoque estratégico
Craigen et al. (2014)	Defining cybersecurity	Revisión conceptual	Análisis documental	Gobernanza	Estructura conceptual disciplinar
Buczak & Guven (2016)	A survey of data mining and machine learning methods for cybersecurity intrusion detection	Revisión sistemática	Análisis comparativo	Tendencias tecnológicas	Complejidad implementación
Sommer & Paxson (2010)	Outside the closed world: On using machine learning for network intrusion detection	Empírico	Evaluación experimental	Tendencias tecnológicas	Limitaciones prácticas ML
Alshaikh (2020)	Developing cybersecurity culture to influence employee behavior	Revisión	Análisis organizacional	Factor humano	Cultura reduce incidentes
Sarker et al. (2021)	Cybersecurity data science: an overview from machine learning perspective	Científico	Modelado analítico	Tendencias tecnológicas	Analítica avanzada

Autor / Año	Título del artículo	Tipo	Diseño metodológico	Categoría	Hallazgos principales
Bada & Nurse (2019)	Developing cybersecurity education and awareness programmes: A literature review	Revisión sistemática	Síntesis cualitativa	Factor humano	Programas mejoran comportamiento
Ahmad, Maynard & Park (2014)	Information security strategies: towards an organizational multi-strategy perspective	Empírico	Estudio organizacional	Factor humano	Estrategias múltiples efectivas
Dhillon & Backhouse (2001)	Current directions in IS security research: towards socio-organizational perspectives	Teórico	Marco sociotécnico	Gestión del riesgo	Seguridad como fenómeno organizacional
Siponen & Willison (2009)	Information security policy violations: A rational choice perspective	Empírico	Modelo cuantitativo	Factor humano	Contexto específico
Herath & Rao (2009)	Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness	Empírico	Encuestas cuantitativas	Factor humano	Disuasión mejora cumplimiento

Autor / Año	Título del artículo	Tipo	Diseño metodológico	Categoría	Hallazgos principales
Posey et al. (2015)	The impact of organizational commitment on insiders' motivation to protect information assets	Empírico	Modelado estructural	Factor humano	Compromiso reduce riesgo interno
Aven (2016)	Risk assessment and risk management: Review of recent advances	Teórico	Revisión conceptual	Gestión del riesgo	Marco actualizado evaluación riesgo
Shameli-Sendi et al. (2016)	Taxonomy of information security risk assessment methods	Revisión sistemática	Clasificación metodológica	Gestión del riesgo	Clasificación IRM estructurada
Tøndel et al. (2014)	Information security incident management: Current practice as reported in the literature	Revisión sistemática	Análisis procesos	Riesgos y amenazas	Mejora gestión incidentes
Behl & Behl (2017)	Cybersecurity and cyberwar: What everyone needs to know	Empírico	Análisis estratégico	Impacto organizacional	Seguridad como ventaja competitiva
Lee, Lee & Kim (2013)	Determinants of adoption of information security management systems	Empírico	Modelo adopción	Gestión del riesgo	Factores críticos SGSI
Gordon et al. (2011)	The impact of information security breaches on firm performance	Empírico	Análisis financiero	Impacto económico	Brechas afectan desempeño

Autor / Año	Título del artículo	Tipo	Diseño metodológico	Categoría	Hallazgos principales
Cavusoglu et al. (2004)	The effect of Internet security breach announcements on market value	Empírico	Análisis mercado	Impacto económico	Reducción valor bursátil
Goel & Shawky (2009)	Estimating the market impact of security breach announcements on firm values	Empírico	Estudio econométrico	Impacto económico	Mercado reacciona negativamente
Kwon & Johnson (2014)	Proactive versus reactive security investments in information security	Empírico	Modelo comparativo	Gestión del riesgo	Inversión proactiva superior
Crossler et al. (2013)	Future directions for behavioral information security research	Revisión sistemática	Integración teórica	Factor humano	Modelo conductual integrador
Kim & Kim (2017)	The effects of IT governance on information security effectiveness	Empírico	Análisis estructural	Gobernanza TI	Gobernanza mejora efectividad
Nurse et al. (2017)	Understanding insider threat: A framework for characterization and mitigation	Revisión científica	Marco analítico	Riesgos y amenazas	Caracterización amenazas internas

Nota. Matriz de que permitió categorizar y organizar los artículos evaluados para posterior análisis alineado al cumplimiento y desarrollo de los objetivos específicos.

Una vez sistematizada la información mediante la matriz de extracción, se desarrolló un análisis orientado al cumplimiento de los objetivos específicos del estudio. Este proceso permitió organizar la evidencia científica recopilada, establecer relaciones entre los distintos enfoques encontrados y construir una interpretación crítica sobre el estado actual de la ciberseguridad en sistemas de información empresariales.

En relación con el primer objetivo específico, el análisis evidenció que los desafíos y factores de riesgo más recurrentes en la literatura están asociados al crecimiento de infraestructuras digitales complejas, la exposición constante a amenazas externas y la limitada cultura organizacional en materia de seguridad. Los autores coinciden en que la transformación digital ha incrementado significativamente la superficie de ataque, lo que exige enfoques integrales de gestión del riesgo.

Respecto al segundo objetivo, el examen comparativo de vulnerabilidades y amenazas permitió identificar patrones comunes en distintos contextos organizacionales. Entre los aspectos más destacados se encuentran las fallas en la configuración de sistemas, el uso inadecuado de credenciales, la ingeniería social y la explotación de vulnerabilidades conocidas. No obstante, se observan diferencias en la forma en que los estudios clasifican y priorizan dichas amenazas, lo que refleja la diversidad metodológica existente en el campo.

En cuanto al tercer objetivo específico, la revisión permitió analizar las estrategias y prácticas de protección propuestas en la literatura especializada. De manera general, se observa una tendencia hacia la adopción de marcos de gestión basados en estándares internacionales, acompañados de controles técnicos y medidas de concienciación organizacional. Sin embargo, varios estudios advierten que la efectividad de estas estrategias depende del nivel de compromiso institucional, la asignación de recursos y la madurez de los procesos internos.

De manera transversal, el análisis permitió no solo identificar coincidencias entre autores, sino también reconocer limitaciones y vacíos en la investigación actual. Esta síntesis fortalece la coherencia entre los objetivos planteados, la metodología empleada y las conclusiones derivadas, consolidando el carácter documental y analítico propio de una monografía de especialización.

Análisis

El análisis de la literatura se estructura en tres ejes analíticos, definidos en correspondencia directa con los objetivos específicos de la investigación. Esta organización permite garantizar la trazabilidad metodológica entre la revisión sistemática basada en PRISMA y la interpretación de los hallazgos, articulando el proceso en tres niveles: identificación y caracterización de desafíos y factores de riesgo, comparación de vulnerabilidades y amenazas, y valoración crítica de estrategias de protección. De esta manera, se busca superar una aproximación meramente descriptiva y avanzar hacia una integración analítica de la evidencia científica revisada.

Identificación y Caracterización De Desafíos y Factores de Riesgo en los Sistemas de Información Empresariales

En el contexto de la transformación digital y la creciente dependencia de las organizaciones respecto a los sistemas de información empresariales, la identificación y análisis de vulnerabilidades, amenazas y riesgos se ha consolidado como un elemento central dentro de la seguridad de la información. Las investigaciones recientes destacan que los sistemas de información que soportan procesos críticos de negocio se encuentran expuestos a múltiples riesgos derivados tanto de factores tecnológicos como organizacionales, lo que exige una comprensión integral de los elementos que configuran el panorama actual de la ciberseguridad.

Desde una perspectiva conceptual, la literatura especializada ha señalado que la seguridad de la información ha evolucionado hacia un enfoque más amplio que integra dimensiones técnicas, organizacionales y humanas. (Rossouw von Solms, 2013) plantean que la ciberseguridad debe entenderse como un componente estratégico dentro de la gestión organizacional, en la medida en que los sistemas de información empresariales constituyen

infraestructuras críticas para el desarrollo de las actividades corporativas. En esta misma línea, (Dan Craigen, 2014) sostienen que el concepto de ciberseguridad ha adquirido un carácter multidisciplinario, en el cual convergen aspectos relacionados con la protección tecnológica, la gobernanza de la información y la gestión de riesgos organizacionales.

Dentro de este panorama, las vulnerabilidades representan debilidades presentes en los sistemas tecnológicos, en los procesos organizacionales o en el comportamiento de los usuarios que pueden ser explotadas por actores malintencionados. Diversos estudios han señalado que muchas de estas vulnerabilidades no se originan exclusivamente en fallas técnicas, sino también en deficiencias en las políticas organizacionales, en los procesos de gestión de seguridad o en el comportamiento de los individuos dentro de las organizaciones. (Dhillon) destacan que la seguridad de los sistemas de información debe analizarse desde una perspectiva socio-organizacional, dado que las decisiones humanas, las prácticas institucionales y las estructuras organizativas influyen significativamente en la exposición al riesgo.

De manera complementaria, investigaciones orientadas al análisis del comportamiento organizacional han evidenciado que el factor humano constituye uno de los elementos más relevantes en la aparición de vulnerabilidades dentro de los sistemas de información empresariales. Estudios como los desarrollados por (Vance, 2012), así como por (Tejaswini Herath, 2009), muestran que el incumplimiento de las políticas de seguridad y la percepción limitada del riesgo por parte de los usuarios pueden facilitar la ocurrencia de incidentes de seguridad. En este sentido, la literatura coincide en que la seguridad de la información no puede abordarse únicamente mediante soluciones tecnológicas, sino que requiere integrar dimensiones culturales y organizacionales dentro de las estrategias de protección.

En cuanto a las amenazas, el crecimiento de los entornos digitales ha favorecido la aparición de nuevos vectores de ataque que afectan directamente a los sistemas de información empresariales. Investigaciones orientadas al análisis de intrusiones y ataques informáticos señalan que las organizaciones enfrentan un panorama dinámico de riesgos asociado al incremento de actividades maliciosas, tales como ataques de malware, explotación de vulnerabilidades en redes y sistemas, así como amenazas internas provenientes de usuarios con acceso privilegiado a la información. En este contexto, estudios como los desarrollados por (Buczak, 2016) han explorado el uso de técnicas de minería de datos y aprendizaje automático para la detección de intrusiones, evidenciando tanto el potencial como las limitaciones de estas tecnologías en entornos organizacionales reales.

No obstante, algunos autores han advertido que la aplicación de tecnologías avanzadas de detección de amenazas presenta desafíos significativos en términos de implementación y efectividad. (Sommer, 2010) señalan que los sistemas de detección basados en aprendizaje automático pueden enfrentar limitaciones prácticas relacionadas con la calidad de los datos, la adaptabilidad de los modelos y la complejidad de los entornos operativos, lo que pone de manifiesto la necesidad de complementar los enfoques tecnológicos con estrategias organizacionales de gestión de seguridad.

Frente a este escenario, la gestión del riesgo se posiciona como un componente fundamental para la administración de la seguridad de la información en los sistemas empresariales. (Aven, 2015) destaca que la gestión del riesgo constituye un proceso sistemático orientado a identificar, analizar y tratar los riesgos que pueden afectar los activos de información de una organización. Este enfoque permite priorizar las vulnerabilidades más críticas y orientar la toma de decisiones estratégicas en materia de seguridad.

De manera similar, (Shameli-Sendi, 2015) y sus colaboradores han propuesto taxonomías de métodos de evaluación de riesgos en seguridad de la información que permiten clasificar las diferentes aproximaciones metodológicas utilizadas en el análisis de riesgos organizacionales. Estas clasificaciones evidencian la evolución de los enfoques de gestión de riesgos hacia modelos más estructurados que integran análisis cualitativos y cuantitativos para la evaluación de amenazas en los sistemas de información.

Finalmente, la literatura también ha resaltado la importancia de comprender el impacto organizacional de los incidentes de seguridad. Investigaciones como las desarrolladas por (Gordon, 2011) (Cavusoglu) y (Sanjay Goel, 2009) evidencian que las brechas de seguridad pueden generar consecuencias significativas en el desempeño organizacional, afectando tanto la reputación como el valor económico de las empresas. Estos hallazgos refuerzan la necesidad de abordar la ciberseguridad como un elemento estratégico dentro de la gestión de los sistemas de información empresariales.

En conjunto, los estudios analizados permiten afirmar que las vulnerabilidades, amenazas y riesgos asociados a los sistemas de información empresariales deben comprenderse desde una perspectiva integral que combine dimensiones tecnológicas, organizacionales y humanas. Esta visión sistémica resulta fundamental para interpretar el fenómeno de la ciberseguridad en el contexto empresarial contemporáneo y constituye un punto de partida para el desarrollo de estrategias de protección más efectivas dentro de las organizaciones.

Comparación de Vulnerabilidades y Amenazas en Entornos Organizacionales

En el contexto de la seguridad de los sistemas de información empresariales, los activos informacionales han sido ampliamente reconocidos en la literatura como elementos críticos para el funcionamiento organizacional, debido a su papel en el almacenamiento, procesamiento y

transmisión de información estratégica. No obstante, más allá de su importancia conceptual, diversos estudios han abordado de manera diferenciada las vulnerabilidades y amenazas que los afectan, evidenciando la necesidad de un análisis comparativo que permita identificar patrones y tendencias en el entorno organizacional.

Desde una perspectiva evolutiva, (Rossouw von Solms, 2013) plantean que la seguridad de la información ha transitado desde un enfoque técnico hacia una visión integral de ciberseguridad organizacional, en la cual los activos informacionales se encuentran expuestos a amenazas no solo tecnológicas, sino también organizacionales y humanas. Este planteamiento coincide con lo expuesto por (Jason R.C. Nurse, 2014) quienes destacan que las vulnerabilidades en los sistemas empresariales no se limitan a fallas en la infraestructura tecnológica, sino que están estrechamente relacionadas con el comportamiento de los usuarios y las prácticas organizacionales.

En contraste, desde el enfoque de la gestión del riesgo, (Aven, 2015) propone una aproximación más estructurada basada en la identificación, evaluación y priorización de riesgos asociados a los activos de información. Mientras que los enfoques sociotécnicos enfatizan la interacción entre factores humanos y organizacionales, el enfoque de gestión del riesgo introduce una visión sistemática que permite establecer niveles de criticidad y probabilidad de impacto frente a diferentes amenazas. Esta diferencia evidencia una complementariedad entre los enfoques analizados, donde uno prioriza la comprensión del contexto organizacional y el otro la estructuración metodológica del riesgo.

Adicionalmente, los estudios centrados en el impacto de los incidentes de ciberseguridad aportan una dimensión relevante al análisis comparativo. Investigaciones desarrolladas por (Gordon, 2011), (Cavusoglu) y (Sanjay Goel, 2009) coinciden en que las brechas de seguridad

que afectan los activos informacionales generan efectos negativos significativos en el desempeño organizacional y el valor empresarial. A diferencia de los enfoques anteriores, estos estudios no se centran únicamente en la identificación de vulnerabilidades, sino en las consecuencias económicas derivadas de su materialización, lo que amplía la comprensión del problema desde una perspectiva estratégica.

A partir de la revisión comparativa de la literatura, es posible identificar un patrón común en los diferentes enfoques analizados: la convergencia en reconocer que las vulnerabilidades en los sistemas de información empresariales son el resultado de la interacción entre factores tecnológicos, humanos y organizacionales. Asimismo, se evidencia una tendencia hacia la integración de modelos de gestión del riesgo con enfoques de gobernanza y cultura organizacional, lo que refleja una evolución hacia estrategias más holísticas de ciberseguridad.

En este sentido, la literatura reciente muestra una transición desde modelos reactivos, centrados en la respuesta a incidentes, hacia enfoques proactivos orientados a la prevención, la gestión del riesgo y el fortalecimiento de la resiliencia organizacional. Esta tendencia responde al aumento en la complejidad de las amenazas y a la necesidad de proteger de manera integral los activos informacionales dentro de los sistemas empresariales.

El análisis comparativo de los estudios revisados permite establecer que las vulnerabilidades y amenazas en los sistemas de información empresariales no pueden ser abordadas desde una única perspectiva, sino que requieren la integración de enfoques tecnológicos, organizacionales y de gestión del riesgo. Esta convergencia teórica evidencia que la ciberseguridad trasciende el ámbito técnico y se configura como un desafío estratégico para las organizaciones, en el cual la protección de los activos informacionales adquiere un papel central

en la sostenibilidad operativa, la mitigación de riesgos y la preservación del valor organizacional en entornos digitales cada vez más complejos.

Valoración Crítica de Estrategias de Protección en Ciberseguridad

El fortalecimiento de la ciberseguridad en los sistemas de información empresariales ha sido abordado en la literatura especializada mediante diversos enfoques estratégicos que buscan responder a la creciente complejidad de las amenazas digitales. No obstante, más allá de la identificación de dichas estrategias, resulta fundamental evaluar críticamente su alcance, limitaciones y aplicabilidad dentro de los entornos organizacionales.

Desde una perspectiva conceptual, (Rossouw von Solms, 2013) plantean que la evolución hacia un enfoque de ciberseguridad organizacional ha permitido integrar la seguridad de la información dentro de la gobernanza empresarial. Este planteamiento es complementado por (Ahmad, 2014), quienes sostienen que las estrategias de seguridad más efectivas son aquellas que combinan múltiples enfoques organizacionales, en lugar de depender exclusivamente de soluciones tecnológicas aisladas. No obstante, la implementación de este tipo de estrategias integrales suele enfrentar limitaciones asociadas a la falta de alineación entre los objetivos de negocio y las políticas de seguridad.

En relación con la gestión del riesgo, (Aven, 2015) propone un enfoque estructurado que facilita la identificación, análisis y priorización de amenazas sobre los sistemas de información. Este modelo aporta un marco metodológico sólido; sin embargo, su aplicabilidad puede verse restringida por la dificultad de anticipar amenazas emergentes y por la complejidad de estimar impactos en entornos altamente dinámicos. En esta misma línea, (Singer, 2014) evidencian que las organizaciones que adoptan enfoques proactivos de inversión en seguridad logran mejores

resultados que aquellas que reaccionan únicamente ante incidentes, lo que refuerza la importancia de integrar la gestión del riesgo dentro de la planificación estratégica.

Por otra parte, las estrategias basadas en controles tecnológicos han sido ampliamente reconocidas por su capacidad para mitigar vulnerabilidades técnicas. No obstante, estudios como los de (Sommer, 2010) y (Buczak, 2016) evidencian que la incorporación de tecnologías avanzadas, particularmente aquellas basadas en aprendizaje automático, presenta limitaciones relacionadas con la complejidad de implementación, la generación de falsos positivos y la dificultad de adaptación a contextos organizacionales reales. Estos hallazgos sugieren que, aunque las soluciones tecnológicas son necesarias, no resultan suficientes cuando se aplican de manera aislada.

En contraste, los enfoques centrados en el factor humano han cobrado relevancia en la literatura reciente. Investigaciones como las de (Bada, 2019), (Jason R.C. Nurse, 2014) y (Tejaswini Herath, 2009) coinciden en que la formación, la concienciación y los mecanismos de disuasión influyen significativamente en el comportamiento de los usuarios frente a la seguridad de la información. Asimismo, estudios como los de (Vance, 2012) y (Posey, 2015) destacan que el cumplimiento de las políticas de seguridad y el compromiso organizacional son determinantes para reducir los riesgos internos. Sin embargo, estas estrategias presentan limitaciones relacionadas con la variabilidad del comportamiento humano y la dificultad de sostener cambios culturales en el largo plazo.

Adicionalmente, los estudios sobre impacto organizacional evidencian que, a pesar de la adopción de diversas estrategias de protección, las brechas de seguridad continúan generando efectos negativos en las organizaciones. Investigaciones desarrolladas por (Gordon, 2011), (Cavusoglu) y (Sanjay Goel, 2009) demuestran que los incidentes de ciberseguridad afectan el

desempeño financiero y la reputación corporativa, lo que sugiere que las estrategias actuales, aunque relevantes, no logran eliminar completamente los riesgos asociados a los sistemas de información empresariales.

De manera complementaria, (Robert E. Crossler, 2013) plantean la necesidad de integrar los distintos enfoques de seguridad dentro de modelos teóricos más amplios que permitan comprender el comportamiento organizacional frente a la ciberseguridad. Esta perspectiva refuerza la idea de que la efectividad de las estrategias no depende únicamente de su diseño, sino de su capacidad de adaptación al contexto organizacional.

El análisis crítico de la literatura permite establecer que las estrategias de ciberseguridad más efectivas son aquellas que integran de manera coherente la gestión del riesgo, los controles tecnológicos y el factor humano. No obstante, su aplicabilidad en los sistemas de información empresariales se encuentra condicionada por variables como el nivel de madurez organizacional, la disponibilidad de recursos y la capacidad de articulación entre los diferentes enfoques. En este sentido, la ciberseguridad se consolida como un proceso dinámico que requiere una adaptación constante frente a la evolución de las amenazas y a las particularidades de cada organización.

Discusión de los Hallazgos

El examen de la literatura científica reciente sobre ciberseguridad en Sistemas de Información Empresariales permite interpretar los hallazgos más allá de su descripción individual, evidenciando relaciones, tensiones y convergencias entre los enfoques analizados.

En primer lugar, la revisión pone de manifiesto que los desafíos en ciberseguridad no responden a una única dimensión analítica. Mientras algunos enfoques privilegian el desarrollo de soluciones tecnológicas avanzadas, otros resaltan el peso de las estructuras organizacionales y del comportamiento humano en la configuración del riesgo. Esta dualidad ha sido ampliamente abordada desde perspectivas sociotécnicas, las cuales sostienen que la seguridad no puede ser garantizada exclusivamente mediante controles técnicos, sino que depende de la articulación entre tecnología, procesos y usuarios dentro de las organizaciones. En consecuencia, la literatura converge en señalar que la fragmentación de estos elementos limita la efectividad de las estrategias de protección.

En esta misma línea, el análisis comparativo de vulnerabilidades y amenazas permite observar que, aunque existe consenso en la identificación de ciertos patrones recurrentes —como la explotación de credenciales, la ingeniería social o las fallas de configuración—, persisten diferencias significativas en la manera en que estos riesgos son clasificados y priorizados. Algunos estudios adoptan enfoques centrados en el impacto técnico de las amenazas, mientras que otros incorporan variables organizacionales o conductuales en su análisis. Esta diversidad metodológica, si bien enriquece el campo, también introduce dificultades para establecer marcos comparativos estandarizados, lo que evidencia una falta de consolidación teórica en torno a la gestión del riesgo en entornos empresariales.

Por otra parte, el desarrollo de estrategias de protección ha experimentado una evolución significativa en la literatura. Los enfoques tradicionales, basados en la implementación de controles técnicos aislados, han dado paso a modelos más integrales que incorporan principios de gobernanza, gestión del riesgo y cultura organizacional. Sin embargo, la revisión evidencia que esta evolución no ha sido homogénea. Algunos estudios destacan el potencial de estos modelos para fortalecer la seguridad organizacional, mientras que otros advierten sobre las dificultades asociadas a su implementación, particularmente en contextos donde no existe una alineación clara entre la estrategia de seguridad y los objetivos corporativos.

De forma complementaria, los avances en tecnologías como el aprendizaje automático y la analítica de datos han sido presentados como herramientas clave para la detección y prevención de amenazas. No obstante, diversos autores coinciden en señalar que su efectividad se encuentra condicionada por factores como la calidad de los datos, la complejidad de los entornos organizacionales y la capacidad de adaptación de los modelos a escenarios dinámicos. Esta situación introduce una tensión entre el potencial teórico de estas tecnologías y su aplicabilidad real, lo que refuerza la necesidad de evaluar críticamente su implementación en contextos empresariales.

A su vez, el papel del factor humano emerge de manera consistente como uno de los elementos más críticos dentro del análisis de la ciberseguridad. La literatura revisada evidencia que las prácticas inadecuadas, la falta de concienciación y el incumplimiento de políticas de seguridad constituyen fuentes recurrentes de vulnerabilidad. En este sentido, los enfoques que integran la dimensión conductual dentro de las estrategias de protección muestran una mayor capacidad para abordar los riesgos de manera integral, lo que sugiere la necesidad de superar visiones centradas exclusivamente en la tecnología.

En cuanto al impacto organizacional de los incidentes de seguridad, los estudios analizados coinciden en señalar consecuencias significativas tanto en el desempeño financiero como en la reputación corporativa. No obstante, se identifican diferencias en la manera en que estos impactos son medidos y analizados, lo que limita la comparabilidad de los resultados y plantea la necesidad de desarrollar metodologías más consistentes para evaluar los efectos de las brechas de seguridad en las organizaciones.

Finalmente, la revisión permite identificar vacíos relevantes en la literatura, especialmente en lo relacionado con la validación empírica de los modelos de gobernanza en ciberseguridad y la medición de la resiliencia organizacional. Aunque existen avances conceptuales importantes, la evidencia empírica aún resulta limitada, lo que restringe la posibilidad de generalizar los hallazgos y aplicar de manera uniforme las estrategias propuestas.

En conjunto, estos elementos permiten interpretar la ciberseguridad en los Sistemas de Información Empresariales como un campo en evolución, caracterizado por la coexistencia de múltiples enfoques teóricos y metodológicos. Esta diversidad, lejos de ser una limitación, constituye una oportunidad para el desarrollo de marcos integradores que permitan articular de manera más coherente las dimensiones tecnológicas, organizacionales y humanas del fenómeno.

Conclusiones

La presente monografía, desarrollada mediante una revisión sistemática bajo el enfoque PRISMA, permitió construir una síntesis analítica del estado del conocimiento en torno a la ciberseguridad en los Sistemas de Información Empresariales, evidenciando no solo tendencias dominantes en la literatura, sino también tensiones conceptuales y vacíos investigativos relevantes. El proceso metodológico adoptado garantizó consistencia en la selección y análisis de fuentes, lo que posibilitó trascender una aproximación descriptiva hacia una interpretación estructurada de los hallazgos.

En relación con el primer objetivo específico, se identificó que los desafíos y factores de riesgo en los Sistemas de Información Empresariales se configuran como fenómenos de naturaleza estructural y no meramente técnica. La literatura converge en reconocer que la exposición al riesgo emerge de la interacción dinámica entre componentes tecnológicos, procesos organizacionales y comportamiento humano, lo que posiciona la ciberseguridad dentro de una lógica sociotécnica. Esta perspectiva implica un desplazamiento conceptual desde enfoques instrumentales hacia una comprensión estratégica de la seguridad como parte constitutiva de la gobernanza organizacional.

Respecto al segundo objetivo específico, el análisis comparativo de vulnerabilidades y amenazas permitió establecer patrones recurrentes asociados a la explotación de debilidades en la gestión de accesos, la sofisticación de la ingeniería social y la persistencia de amenazas internas. No obstante, se evidenció una fragmentación en los marcos de clasificación y priorización del riesgo, lo que sugiere una falta de consolidación epistemológica en el campo. Esta heterogeneidad limita la posibilidad de construir modelos comparativos robustos y refuerza la necesidad de avanzar hacia esquemas analíticos más integradores y contextualizados.

En cuanto al tercer objetivo específico, la valoración crítica de las estrategias de protección evidenció una transición progresiva desde enfoques reactivos centrados en controles tecnológicos hacia modelos integrales sustentados en gobernanza, gestión del riesgo y cultura organizacional. Sin embargo, el análisis permite inferir que la efectividad de dichas estrategias no radica únicamente en su formulación, sino en su nivel de institucionalización y articulación con los objetivos estratégicos de la organización. En este sentido, la literatura sugiere que las aproximaciones fragmentadas tienden a generar resultados limitados, mientras que los enfoques sistémicos presentan mayores niveles de coherencia y sostenibilidad.

Desde una perspectiva transversal, el estudio permitió establecer que la ciberseguridad en los Sistemas de Información Empresariales debe ser entendida como un constructo multidimensional que articula dimensiones tecnológicas, organizacionales y humanas. Esta concepción redefine la seguridad de la información como un componente estructural de la sostenibilidad organizacional en entornos digitales, superando visiones reduccionistas centradas exclusivamente en la protección técnica de los sistemas.

Recomendaciones

A partir del análisis desarrollado, se plantean las siguientes recomendaciones orientadas al fortalecimiento del campo desde una perspectiva teórica y de investigación:

Se sugiere avanzar en la construcción de marcos conceptuales integradores que permitan articular de manera coherente las dimensiones sociotécnicas de la ciberseguridad en los Sistemas de Información Empresariales, superando las aproximaciones fragmentadas que limitan la comprensión del fenómeno.

Resulta pertinente profundizar en la estandarización de categorías analíticas como vulnerabilidad, amenaza y riesgo, con el propósito de reducir la dispersión conceptual identificada en la literatura y facilitar el desarrollo de estudios comparativos con mayor rigor metodológico.

Se recomienda fortalecer las líneas de investigación orientadas a la evaluación empírica de modelos de gobernanza y gestión del riesgo en ciberseguridad, particularmente en lo relacionado con su impacto en la resiliencia organizacional y la capacidad adaptativa frente a entornos de amenaza dinámica.

Asimismo, se considera necesario ampliar los estudios centrados en el factor humano, incorporando enfoques interdisciplinarios que integren elementos de comportamiento organizacional, cultura de seguridad y toma de decisiones, dada su incidencia estructural en la configuración del riesgo.

Finalmente, se sugiere promover investigaciones que analicen la relación entre ciberseguridad y desempeño organizacional desde enfoques longitudinales, con el fin de comprender de manera más profunda los efectos sostenidos de la gestión de la seguridad sobre la competitividad y sostenibilidad empresarial.

Referencias Bibliográficas

Ahmad, A. a. (2014). Information security strategies: Towards an organizational multi-strategy perspective. *Journal of Intelligent Manufacturing, 25*. https://doi.org/10.1007/s10845-012-0683-0

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security, 98*. https://doi.org/10.1016/j.cose.2020.102003

Aven, T. (2015). Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research, 253*. https://doi.org/10.1016/j.ejor.2015.12.023

Bada, M. a. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). *Information and Computer Security*. https://doi.org/10.1108/ICS-07-2018-0080

Buczak, A. L. (2016). A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. *IEEE Communications Surveys & Tutorials, 18*(2), 1153-1176. https://doi.org/10.1109/COMST.2015.2494502

Cavusoglu, H. a. (s.f.). he Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. *International Journal of Electronic Commerce, 9*. https://doi.org/10.1080/10864415.2004.11044320

Dan Craigen, N. D.-T. (2014). Defining Cybersecurity. *Technology Innovation Management Review, 4*, 13-21. https://doi.org/10.22215/timreview/835

Dhillon, G. a. (s.f.). Current directions in IS security research: Towards socioorganizational perspectives. *Information Systems Journal*. https://doi.org/10.1046/j.1365-2575.2001.00099.x

Gordon, L. a. (2011). The Impact of Information Security Breaches: Has There Been a Downward Shift in Costs? *Journal of Computer Security, 19*, 33-56. https://doi.org/10.3233/JCS-2009-0398

Inger Anne Tøndel, M. B. (2014). Information security incident management: Current practice as reported in the literature. *Computers & Security, 45*, 42-57. https://doi.org/10.1016/j.cose.2014.05.003

Jason R.C. Nurse, O. B. (2014). Understanding insider threat: A framework for characterization and mitigation. *IEEE Security and Privacy Workshops*, 214-228.

Kwon, J. a. (2014). Proactive Versus Reactive Security Investments in the Healthcare Sector. *MIS Quarterly, 38*, 451-471. https://doi.org/10.25300/MISQ/2014/38.2.06

Posey, C. a. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems, 32*, 179-214.

Robert E. Crossler, A. C. (2013). Future directions for behavioral information security research. *Computers & Security, 32*, 90-101. https://doi.org/10.1016/j.cose.2012.09.010.

Rossouw von Solms, J. v. (2013). From information security to cyber security. *Computers & Security*, págs. 97-102. https://doi.org/https://doi.org/10.1016/j.cose.2013.04.004

Sánchez, D. A., Duran, D. E., Valencia, L. E., Jaimes, A. E., González, I. A., & Alegría, F. A. (2023). Maturity model of cybersecurity organizational culture for the financial sector

based on good practices. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, 362-375.

Sanjay Goel, H. A. (2009). Estimating the market impact of security breach announcements on firm values. *Information & Management, 46*, 404-410. https://doi.org/10.1016/j.im.2009.06.005

Sarker, I. a. (2020). Cybersecurity data science: an overview from machine learning perspective. *Journal of Big Data, 7*. https://doi.org/10.1186/s40537-020-00318-5

Shameli-Sendi, A. a.-B. (2015). Taxonomy of Information Security Risk Assessment . *Computers & Security, 57*. https://doi.org/10.1016/j.cose.2015.11.001

Singer, P. a. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. https://doi.org/10.1093/wentk/9780199918096.001.0001

Sommer, R. a. (2010). Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. *2010 IEEE Symposium on Security and Privacy*, 305-316. https://doi.org/10.1109/SP.2010.25

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

Tejaswini Herath, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154-165. https://doi.org/10.1016/j.dss.2009.02.005.

Vance, A. a. (2012). IS Security Policy Violations. *Journal of Organizational and End User Computing, 24*, 21-41. https://doi.org/10.4018/joeuc.2012010102