eISSN 2310-290X
Vol. 14, No. 2, 2025

https://revistas.unitec.edu/innovare

INNOVARE
Revista de ciencia y tecnología

Original

OPEN ACCESS

Análisis bibliométrico sobre innovación y ciberseguridad: un enfoque estratégico para empresas digitalizadas en Latinoamérica

Bibliometric Analysis on Innovation and Cybersecurity: A Strategic Approach for Digitalized Companies in Latin America

Amalia Hernandez Bonilla*[1], Ángel Acevedo-Duque[2]

[1]Universidad Nacional Autónoma de Honduras, UNAH, San Pedro Sula, Honduras
[2]Grupo de Investigación de Estudios Organizacionales Sostenibles Universidad Autónoma de Chile, Chile

Resumen /**Introducción**. Esta investigación tiene como objetivo analizar la evolución, estructura intelectual y tendencias de la producción científica sobre innovación y ciberseguridad en empresas digitalizadas de América Latina mediante un enfoque bibliométrico. **Métodos.** Se realizó un análisis bibliométrico de publicaciones indexadas en Scopus y Web of Science correspondientes al período 2015–2025. Se analizaron indicadores de crecimiento temporal, autores, revistas, áreas temáticas y redes de colaboración utilizando técnicas de normalización y visualización mediante VOSviewer. **Resultados.** Los resultados evidencian un crecimiento exponencial de la literatura a partir de 2020, con un coeficiente de determinación $R^2 = 0{,}87$. La producción científica se concentra principalmente en ciencias de la computación e ingeniería, con predominio del idioma inglés y limitada colaboración intrarregional latinoamericana. Los mapas de co-ocurrencia identifican a la innovación como un eje articulador entre ciberseguridad y resiliencia empresarial. **Conclusión.** Se concluye que la innovación emerge como una variable mediadora clave para fortalecer la resiliencia organizacional frente a riesgos cibernéticos. No obstante, persisten brechas geográficas, lingüísticas y de financiamiento que limitan el desarrollo contextualizado del conocimiento en América Latina.

Palabras Clave América Latina, Bibliometría, Ciberseguridad, Empresas digitalizadas, Innovación

Abstract /**Introduction**. This research aims to analyze the evolution, intellectual structure, and trends in scientific production on innovation and cybersecurity in digitized companies in Latin America using a bibliometric approach. **Methods.** A bibliometric analysis was performed on publications indexed in Scopus and Web of Science for the period 2015–2025. Indicators of temporal growth, authors, journals, subject areas, and collaboration networks were analyzed using normalization and visualization techniques with VOSviewer. **Results.** The results show exponential growth in the literature since 2020, with a coefficient of determination $R^2 = 0.87$. Scientific production is mainly concentrated in computer science and engineering, with a predominance of the English language and limited intraregional collaboration in Latin America. Co-occurrence maps identify innovation as a connecting link between cybersecurity and business resilience. **Conclusion.** It is concluded that innovation emerges as a key mediating variable for strengthening organizational resilience to cyber risks. However, geographical, linguistic, and funding gaps persist, limiting the contextualized development of knowledge in Latin America.

Keywords Bibliometrics, Cybersecurity, Digitalized enterprises, Innovation, Latin America

Recepción: 11 de diciembre 2025 / Aceptación: 22 de diciembre 2025 / Publicación: 26 de diciembre 2025
Autor corresponsal: amalia.hernandez@unah.edu.hn
Cita: Hernandez-Bonilla, A. P., Acevedo-Duque, Á. (2025). Análisis bibliométrico sobre innovación y ciberseguridad: un enfoque estratégico para empresas digitalizadas en Latinoamérica. *Innovare, Revista de Ciencia y Tecnología, 14*(2), 1-9. https://doi.org/10.69845/innovare.v14i2.563

INTRODUCCIÓN

La transformación digital en América Latina ha impulsado de manera exponencial el comercio electrónico y la modernización de servicios gubernamentales, pero también ha dejado al descubierto profundas brechas de ciberseguridad (Kosevich, 2022a). Por un lado, solo unos pocos países como Brasil, México y Colombia han diseñado y puesto en marcha estrategias nacionales consolidadas; por el otro, existe una falta generalizada de normativas homogéneas, datos confiables sobre incidentes y capacidades técnicas en las empresas, lo que incrementa el riesgo de pérdidas económicas y daños reputacionales (Flores Cedeño & López Paz, 2024).

La innovación se define como la implementación de nuevos procesos o tecnologías que generan valor (OECD & Eurostat, 2018), mientras que la ciberseguridad abarca

las medidas para proteger sistemas digitales contra amenazas (ISO/IEC, 2020).

Se propone un modelo donde la innovación actúa como mediadora: una ciberseguridad robusta habilita la adopción de tecnologías innovadoras, lo que mejora la resiliencia frente a ciberataques (Purdon & Vera, 2020). Este marco guía el análisis bibliométrico y contextualiza los hallazgos en América Latina. El estado actual del campo revela posturas divergentes: algunos autores advierten que priorizar en exceso la seguridad puede ralentizar la innovación y el lanzamiento de nuevos productos al mercado (Purdon & Vera, 2020), mientras que otros sostienen que integrar la seguridad desde la fase de diseño impulsa la confianza de clientes y acelera la adopción tecnológica (Garay Canales et al., 2025).

Las conclusiones de algunos estudios sugieren que un enfoque holístico que combine infraestructura robusta, cumplimiento normativo, gobernanza ágil y capacitación continua es esencial para que las empresas digitalizadas maximicen su competitividad sin sacrificar su postura de Seguridad (Díaz-Piraquive et al., 2023).

El propósito de esta investigación es analizar sistemáticamente la producción científica sobre la relación entre innovación y ciberseguridad en empresas digitalizadas de la región para identificar tendencias, redes de colaboración, autores prolíficos, palabras clave dominantes y revistas relevantes, contribuyendo a una base teórica y estratégica que fomente enfoques integrados en la gestión empresarial. Por lo anterior se plantea la siguiente pregunta de investigación: ¿cómo se relacionan la innovación y la ciberseguridad en las estrategias de las empresas digitalizadas en Latinoamérica desde la perspectiva teórica?

En respuesta a este panorama, el objeto de estudio se define como la relación entre los procesos de innovación y las estrategias de ciberseguridad en empresas digitalizadas en Latinoamérica. Por esta razón, la estructura del documento incluye, tras la introducción, una revisión bibliográfica que enmarca el estudio y define su propósito, una sección metodológica que busca explicar los procesos desde una perspectiva hermenéutica, una sección de resultados que presenta una nueva teoría, seguida de una discusión y una conclusión.

REVISIÓN DE LA LITERATURA

La transformación digital y las brechas regionales

La acelerada adopción de tecnologías digitales en América Latina ha impulsado el comercio electrónico y la modernización de servicios públicos, pero también ha evidenciado desigualdades en cobertura de red, infraestructura y capacidades técnicas entre los distintos países, lo que limita su competitividad y exposición a ciberamenazas (Garay Canales et al., 2025). Aunque Brasil, México y Colombia han establecido marcos nacionales de ciberseguridad que incluyen planes de respuesta y regulación de infraestructura crítica, la mayoría de los países de la región carece de políticas homogéneas, lo cual genera vacíos regulatorios y dificulta la protección efectiva de las empresas digitalizadas (Kosevich, 2022).

La Organización de los Estados Americanos (OEA) ha promovido la creación de Equipos Nacionales de Respuesta a Emergencias Informáticas y programas de capacitación, pero su implementación refleja a menudo las prioridades de proveedores externos, lo que subraya la necesidad de marcos de gobernanza adaptados a la realidad latinoamericana (Flores Cedeño & López Paz, 2024).

Las micro, pequeñas y medianas empresas de la región reconocen la importancia de la ciberseguridad, pero la carencia de personal especializado y de recursos económicos limita la adopción de controles básicos de gestión de riesgos, exponiéndolas a vulnerabilidades críticas (Díaz-Piraquive et al., 2023). El desarrollo de políticas internas alineadas con normas nacionales e internacionales de protección de datos incluyendo ISO/IEC 27001 y marcos regionales contribuye a generar confianza en clientes y socios, además de facilitar la anticipación a cambios regulatorios (Grisales Rendón, 2022).

La transformación digital y su impacto en la ciberseguridad

La transformación digital se refiere a la integración de tecnologías digitales en todos los aspectos de una organización, lo que implica cambios fundamentales en la forma en que operan y entregan valor a los clientes (Seabra Oliveira et al., 2019). La digitalización en la región creció exponencialmente post-COVID-19, con un aumento del 20% en el uso de plataformas digitales entre 2019 y 2021 (Jung & Katz, 2023).

Sin embargo, persisten brechas: Brasil lidera en infraestructura digital, mientras que Honduras enfrenta limitaciones severas (World Bank, 2022). En América Latina, la pandemia de COVID-19 aceleró este proceso, obligando a las empresas a apresurarse a adoptar soluciones digitales para mantener sus negocios (Grisales Rendón, 2022). Sin embargo, esta rápida digitalización ha aumentado la exposición a las ciberamenazas y la ciberseguridad se ha convertido en un componente crítico de la sostenibilidad empresarial.

La investigación de Kosevich (2022) afirma que las empresas latinoamericanas enfrentan problemas específicos de ciberseguridad debido a la falta de infraestructura tecnológica sofisticada y la escasez de personal calificado dentro de la región. Sin embargo, en América Latina, la adopción de estas tecnologías es desigual, lo que crea brechas en la capacidad de las empresas para innovar en esta dirección descubrieron que las empresas latinoamericanas que incorporan la innovación en sus estrategias de ciberseguridad logran una mayor resiliencia contra los ciberataques (Izycki, 2018).

La gestión de riesgos cibernéticos en empresas digitalizadas

La gestión de riesgos cibernéticos implica identificar, evaluar y mitigar las amenazas que pueden afectar la integridad, confidencialidad y disponibilidad de la información digital (Heierhoff & Reher, 2022). En el

contexto latinoamericano, las empresas deben considerar no solo las amenazas globales, como el *ransomware* o el *phishing*, sino también las particularidades regionales, como la diversidad regulatoria y las brechas en la adopción tecnológica. Metin et al. (2024) destacan que la mayoría de las empresas digitalizadas en América Latina subestiman las ciberamenazas y, como consecuencia, invierten menos en controles de seguridad.

El enfoque estratégico de ciberseguridad en América Latina

La brecha digital es un obstáculo crítico. Un enfoque estratégico en ciberseguridad implica alinear las políticas de seguridad con los objetivos de negocio, asegurando que la ciberseguridad sea un habilitador de la innovación y no un obstáculo (Goi et al., 2023). Esta transformación implica que la alta dirección y los especialistas en ciberseguridad colaboren para desarrollar estrategias de ciberseguridad alineadas con la innovación digital.

Varios países latinoamericanos, incluidos Brasil, Chile, Colombia, Costa Rica y México han desarrollado estrategias nacionales de ciberseguridad para proteger sus economías digitales y entornos comerciales. (Kosevich, 2022). La integración de la innovación tecnológica y la ciberseguridad exige que las organizaciones desarrollen nuevos recursos y capacidades (Bianchi et al., 2019).

MÉTODOS

Diseño del estudio

El estudio se desarrolló bajo un enfoque mixto con diseño bibliométrico, orientado a identificar la evolución temporal, estructura intelectual y redes de colaboración de la producción científica sobre innovación y ciberseguridad en empresas digitalizadas de América Latina. En la figura 1 se muestra el proceso de la metodología empleada.

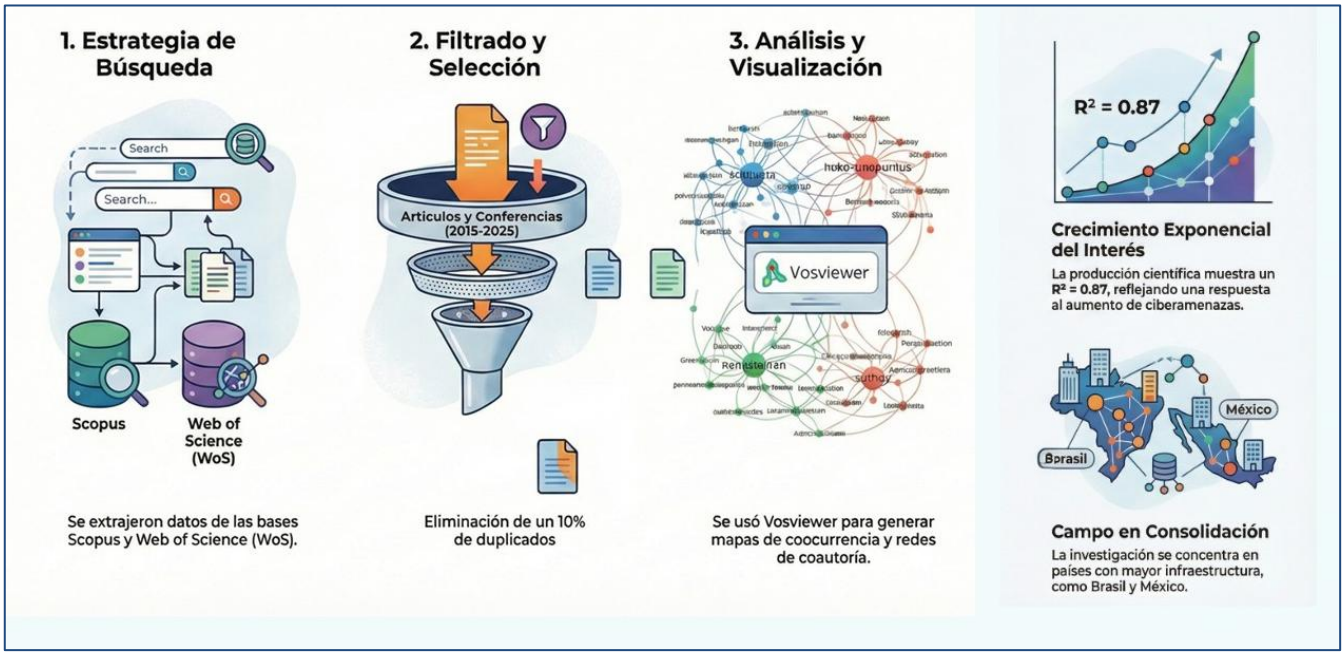

Figura 1. Metodología aplicada. Se describe el proceso sistemático utilizado para realizar el análisis bibliométrico.

Fuentes de información

Los datos se obtuvieron de las bases de datos Scopus y Web of Science (WoS), seleccionadas por su cobertura multidisciplinaria y por indexar literatura científica revisada por pares en ciencias de la computación, ingeniería y gestión. El estudio se centró en identificar patrones de publicación, autores clave, términos relevantes y colaboraciones internacionales relacionadas con el tema.

La distribución temporal de publicaciones se construyó a partir del corpus final de documentos seleccionados, y no del conjunto inicial de registros identificados. Partiendo de los resultados de la presente investigación los hallazgos reflejan tendencias globales donde la ciberseguridad es un habilitador clave de la innovación (Von Solms, R., & Von Solms, B, 2018), pero América Latina muestra desafíos únicos por brechas estructurales. La escasa colaboración intrarregional sugiere una oportunidad para redes de investigación. El crecimiento exponencial de la producción científica (R^2 = 0,85) refleja una respuesta académica al aumento de ciberamenazas post-pandemia, consistente con Kosevich (2022).

No obstante, la concentración de autores prolíficos y revistas núcleo indica que el campo aún está en consolidación, con un sesgo hacia países con mayor infraestructura de investigación (Brasil, México). Esto plantea un aporte teórico sobre la necesidad de marcos contextualizados que aborden las desigualdades regionales en adopción tecnológica y formación, un aspecto práctico relevante para MIPYMES.

Estrategia de búsqueda

Se aplicaron ecuaciones de búsqueda en los campos de título, resumen y palabras clave, de acuerdo con la sintaxis de cada base de datos (Acevedo Duque et al., 2023).

Scopus (TITLE-ABS-KEY):
("innovation" AND "cybersecurity" AND ("Latin America" OR "cyber resilience" OR "digital transformation"))
Web of Science (TS):
("innovation" AND "cybersecurity" AND ("Latin America" OR "cyber resilience"))

El periodo de análisis comprendió desde 2015 hasta enero de 2025, con fecha de corte el 11 de enero de 2025.

Proceso de selección

El proceso de selección de los documentos se realizó siguiendo una adaptación del enfoque PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses), aplicado al contexto de estudios bibliométricos como se muestra en la figura 2.

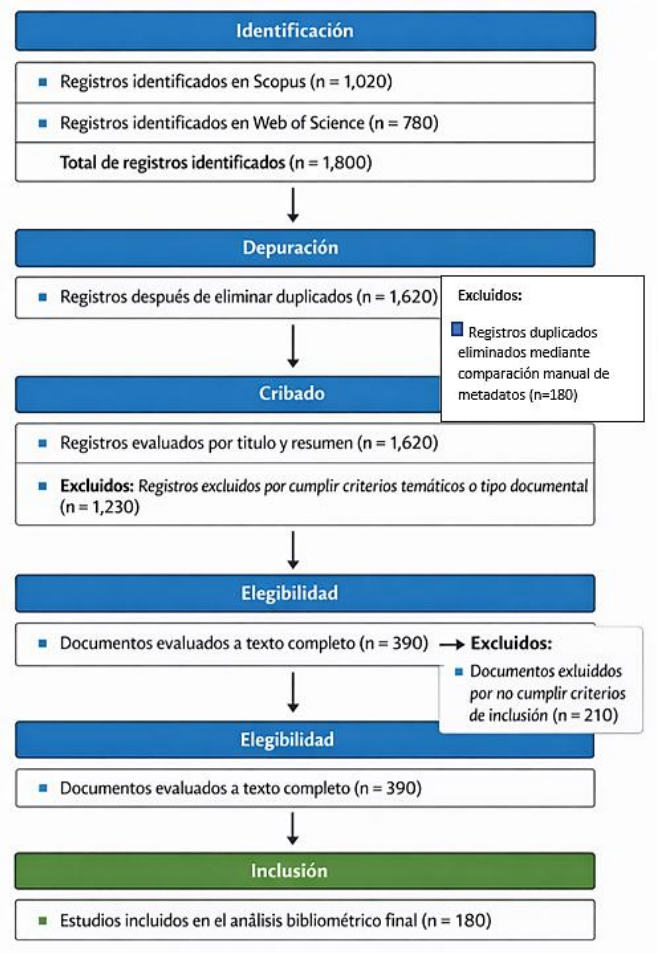

Figura 2. Diagrama de flujo del proceso de selección bibliométrica (adaptado de PRISMA).

En una primera fase de identificación, se recuperaron registros científicos desde las bases de datos Scopus y Web of Science (WoS) mediante ecuaciones de búsqueda estructuradas aplicadas a los campos de título, resumen y palabras clave, para el período comprendido entre 2015 y enero de 2025. Posteriormente, en la fase de depuración, se realizó una comparación manual de metadatos entre ambas bases de datos, lo que permitió identificar y eliminar aproximadamente un 10% de registros duplicados, conservando una única versión por documento.

En la fase de cribado, los registros restantes fueron evaluados a partir de sus títulos y resúmenes, excluyéndose aquellos que no presentaban una relación explícita con la temática de innovación y ciberseguridad en empresas digitalizadas, así como documentos que correspondían a literatura gris, tesis o informes técnicos no revisados por pares. Finalmente, en la fase de elegibilidad e inclusión, se seleccionó el conjunto final de documentos que cumplían con los criterios de inclusión establecidos (artículos, capítulos de libro y documentos de conferencia revisados por pares, en español o inglés), los cuales fueron utilizados para el análisis bibliométrico mediante VOSviewer.

Criterios de inclusión y exclusión

Los criterios de inclusión fueron: (i) Artículos revisados por pares. (ii) Periodo: 2015- enero 2025. (iii) Tipos: Artículos, capítulos de libro y documentos de conferencias. (iv) Idiomas: español e inglés. (v) Relación explícita entre innovación y ciberseguridad.

Los criterios de exclusión fueron: (i) Tesis e informes técnicos y literatura gris no arbitrada. (ii) Documentos duplicados entre Scopus y WoS. (iii) Estudios sin vínculo directo con empresas digitalizadas. (iv) Estudios sin relación explícita innovación–ciberseguridad.

Parámetros de VOSviewer

El análisis se efectuó utilizando VOSviewer, aplicando los siguientes parámetros: (i) Tipo de análisis: co-ocurrencia de palabras clave y coautoría. (ii) Método de conteo: *full counting*. (iii) Umbral mínimo: cinco ocurrencias por término o autor. (iv) Método de normalización: association strength. (v) Análisis de indicadores bibliométricos como número de documentos por año, autores más productivos, fuentes de publicación, áreas temáticas, idioma y patrocinadores de financiación.

Resultados y Análisis

Tendencias de crecimiento de la producción científica

La Figura 3 presenta la distribución temporal de las publicaciones sobre innovación y ciberseguridad en empresas digitalizadas para el período 2015–2025. Los resultados muestran un crecimiento progresivo hasta 2019, seguido de un incremento acelerado a partir de 2020.

Figura 3. Distribución temporal de publicaciones (2015–2025). Los datos presentados son parciales hasta enero de 2025. La tendencia muestra un crecimiento exponencial con $R^2 = 0,87$.

El coeficiente de determinación ($R^2 = 0,87$) indica un patrón de crecimiento exponencial de la producción científica en el periodo analizado. El mayor volumen de publicaciones se registra en 2024, mientras que los datos correspondientes a 2025 son parciales, debido al corte temporal del estudio.

Autores más productivos

La Tabla 1 muestra los diez autores con mayor número de publicaciones en el área. La producción se distribuye entre múltiples investigadores, sin una concentración extrema en uno o dos autores, lo que evidencia una autoría relativamente dispersa dentro del campo.

Tabla 1. Top 10 autores más productivos (Scopus–WoS)

Autor	N⁰. de publicaciones
Mohamed, N.	9
Ferrag, M. A.	8
Navarro Álvarez, A.	6
Fernández de María-Martínez	6
González de Ávila, E.	5
Abbas, H.	5
Abd El-Rahman, M.	4
Abdallah, A. B.	4
Aaron, R. E.	4
Saeed, S.	4

Fuentes y revistas de publicación

La Tabla 2 presenta las principales revistas y fuentes donde se concentran las publicaciones analizadas. Las fuentes más productivas corresponden a revistas y series orientadas a ingeniería, ciencias de la computación y tecnologías digitales, con predominio de publicaciones en actas de congresos y revistas de acceso abierto.

Tabla 2. Top 10 revistas y fuentes de publicación

Fuente / Revista	Documentos
IEEE Access	22
Lecture Notes in Networks and Systems	21
ACM International Conference Proceedings Series	18
Communications in Computer and Information Science	16
Lecture Notes in Computer Science	15
Sustainability	14
Computers & Security	12
Sensors	11
Information	10
Applied Sciences	9

Clústeres temáticos de investigación

El análisis de co-ocurrencia de palabras clave permitió identificar cinco clústeres temáticos principales, los cuales se resumen en la Tabla 3. Estos clústeres agrupan investigaciones relacionadas con ciberseguridad de redes, innovación y transformación digital, gestión de riesgos, tecnologías emergentes y estudios enfocados en pequeñas y medianas empresas.

Tabla 3. Principales clústeres temáticos identificados (VOSviewer)

Clúster	Temas dominantes
Clúster 1	Cybersecurity, network security, digital infrastructure
Clúster 2	Innovation, digital transformation, organizational resilience
Clúster 3	Risk management, cyber resilience, governance
Clúster 4	Artificial intelligence, machine learning, blockchain
Clúster 5	SMEs, digital economy, Latin America

Redes de colaboración científica

El análisis de coautoría revela la existencia de redes de colaboración internacionales como se muestra en la Figura 4, con una participación predominante de investigadores afiliados a instituciones fuera de América Latina. Las colaboraciones intrarregionales se presentan de manera limitada dentro del conjunto de datos analizado.

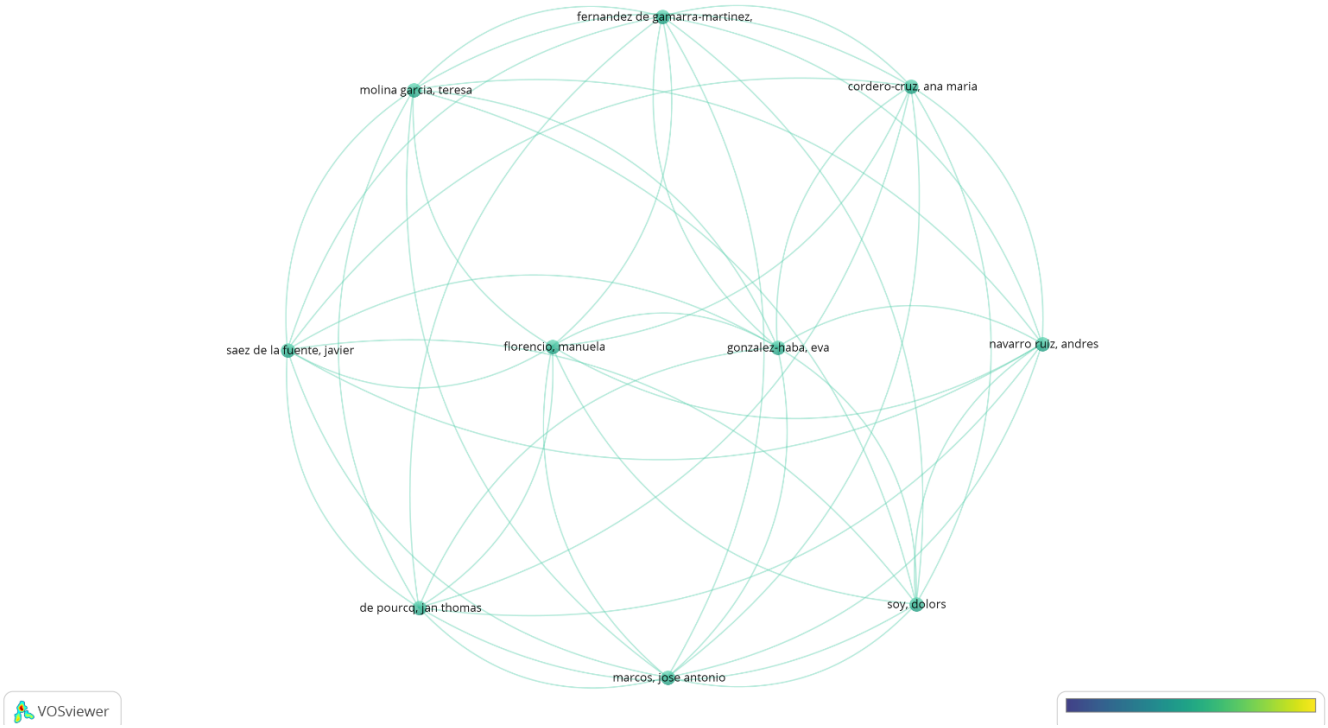

Figura 4. Redes de colaboración científica utilizando VOSviewer.

DISCUSIÓN

Los resultados evidencian un crecimiento acelerado de la producción científica sobre innovación y ciberseguridad a partir de 2020, lo cual coincide con el proceso de digitalización intensificada posterior a la pandemia. Este comportamiento es consistente con la Ley de Price y con estudios previos que identifican la ciberseguridad como un habilitador clave de la innovación digital.

La concentración temática en ciencias de la computación e ingeniería refleja un enfoque predominantemente tecnológico, mientras que los aspectos organizacionales, regulatorios y estratégicos presentan una menor representación. Esta asimetría sugiere una oportunidad para investigaciones interdisciplinarias que integren la gestión empresarial y las políticas públicas, particularmente en el contexto latinoamericano.

Asimismo, la limitada colaboración intrarregional y la escasa presencia de instituciones latinoamericanas entre las afiliaciones más productivas evidencian brechas estructurales en capacidades de investigación y financiamiento. Estos hallazgos coinciden con estudios que señalan la dependencia de fondos internacionales y la necesidad de fortalecer ecosistemas científicos locales.

El análisis de clústeres confirma el papel de la innovación como un eje articulador entre la ciberseguridad y la resiliencia empresarial. La convergencia entre tecnologías emergentes como inteligencia artificial y blockchain y estrategias de gestión de riesgos refuerza la idea de que la innovación no solo coexiste con la ciberseguridad, sino que actúa como una variable mediadora que potencia la capacidad de adaptación organizacional.

Con el propósito de integrar y sintetizar los hallazgos derivados del análisis de la literatura y de los resultados obtenidos, la Tabla 4 presenta una estructuración sistemática de las principales dimensiones, subdimensiones, vacíos de investigación y oportunidades emergentes en el ámbito de la ciberseguridad y la transformación digital en MIPYMES.

Esta síntesis permite visualizar de manera comparativa las áreas donde existe mayor consenso teórico, así como aquellas en las que persisten limitaciones empíricas, particularmente en el contexto latinoamericano. En consecuencia, la tabla no solo consolida los resultados del estudio, sino que también establece una base analítica para la discusión y la formulación de futuras líneas de investigación orientadas a fortalecer la gestión del riesgo, la resiliencia organizacional y el desempeño sostenible en la región.

CONCLUSIÓN

El análisis revela un crecimiento exponencial en la literatura sobre innovación y ciberseguridad desde 2020, con un pico de 719 documentos en 2024 (Scopus), reflejando el impacto de la transformación digital acelerada en América Latina tras la pandemia (CEPAL, 2020). El R^2 de 0,87 confirma esta tendencia según la Ley de Price. Los términos "cybersecurity" e "innovation" son centrales en los mapas de coocurrencias, con 50 coocurrencias, y se

relacionan con tecnologías emergentes como "artificial Intelligence" (30 coocurrencias) y "blockchain" (25 coocurrencias), validando su papel como mediadores de resiliencia empresarial (Purdon & Vera, 2020).

Brasil emerge como el líder regional en producción científica (20 documentos, WoS), pero la colaboración intrarregional es limitada, con países como Honduras y Argentina mostrando menos de 5 documentos cada uno. Autores globales como Mohamed, N. (9 documentos) y Ferrag, MA (8 documentos) dominan, destacando una brecha en el liderazgo local. La financiación externa, liderada por la Comisión Europea (80 documentos), y la afiliación de universidades como Chitkara University, Punjab (27,5 documentos), subrayan la dependencia de recursos internacionales, mientras que el idioma inglés (300 documentos) predomina sobre el español (<10 documentos). Estos hallazgos amplían el modelo de Von Solms & Von Solms (2018) al incluir la innovación como mediadora en contextos latinoamericanos, sugiriendo que las empresas deben adoptar soluciones como autenticación multifactor (MFA) e IA para fortalecer su resiliencia.

Tabla 4. Matriz de Análisis de la Literatura sobre Innovación y Ciberseguridad

Dimensión	Subdimensión	Evidencia en la literatura	Vacío de investigación	Oportunidad de investigación en Latinoamérica
I. Factores humanos y culturales	Cultura de ciberseguridad y comportamiento del empleado.	La cultura de ciberseguridad incide en el comportamiento del empleado y el desempeño sostenible. El enfoque de Transformación Digital Sostenible (SDT) resalta liderazgo y participación active (Alshaikh, 2020; Martínez-Peláez et al., 2024).	Limitada evidencia empírica sobre la operacionalización de culturas de ciberseguridad y SDT en MIPYMES.	Validar el marco SDT en MIPYMES latinoamericanas y su impacto en desempeño sostenible.
	Concienciación y capacitación en ciberseguridad (SETA).	El trabajo remoto incrementó ataques de ingeniería social. Marcos como CAT fortalecen la concienciación (Hijji & Alam, 2022; Rawindaran et al., 2021; Sadik et al., 2020)	Escasez de modelos SETA adaptados a entornos remotos e híbridos.	Adaptar y validar marcos SETA (CAT) en MIPYMES de LATAM.
II. Gobernanza y cumplimiento normativo	Gobernanza corporativa y divulgación de riesgos.	La divulgación de riesgos de ciberseguridad en LATAM es limitada; el CDI permite evaluar transparencia (Al-Mohareb, 2025; Ramírez et al., 2022).	Investigación incipiente sobre efectos financieros del riesgo cibernético.	Aplicar el CDI en empresas latinoamericanas.
	Regulación y cyberworthiness.	Los sistemas ciberfísicos requieren gobernanza integrada; la regulación es fragmentada (Van Zomeren et al., 2025).	Ausencia de marcos regulatorios integrales para CPS.	Proponer marcos de cyberworthiness en infraestructuras críticas de LATAM.
III. Riesgo y resiliencia operacional	Gestión de riesgos y madurez.	Los marcos ISO y NIST son complejos para MIPYMES; se proponen enfoques adaptativos (El-Hajj & Mirza, 2024; Melaku, 2023; Saeed et al., 2023; Stefani et al., 2025)	Falta de taxonomías de riesgos específicas para DT.	Validar marcos simples de gestión de riesgos en LATAM.
	Resiliencia cibernética y respuesta.	La resiliencia cibernética mejora sostenibilidad y reduce tiempos de recuperación (Aghazadeh Ardebili et al., 2024; Annarelli & Palombi, 2021; Choi et al., 2023; Morales-Sáenz et al., 2024; Shahim, 2021)	Los métodos tradicionales no capturan adecuadamente la resiliencia.	Implementar modelos de evaluación de resiliencia basados en RTO.
IV. Tecnología e implicaciones económicas	Tecnologías habilitadoras (IA, ML, blockchain, IoT).	Industria 5.0 amplía la superficie de ataque; faltan soluciones accesibles para MIPYMES (Ascue et al., 2025; Ayodele & Buttigieg, 2024; Jeršič et al., 2025; Kour et al., 2024; Ukwandu et al., 2022).	Escasez de herramientas y datasets adecuados para ML/DL.	Desarrollar soluciones tecnológicas adaptadas a MIPYMES de LATAM.
	Economía, costos e inversión.	El costo del ciberdelito es elevado; el ciberseguro es clave para la gestión del riesgo (Kianpour et al., 2021; Taskin et al., 2025).	Evidencia limitada sobre adopción de ciberseguros en MIPYMES.	Analizar adopción de ciberseguros en LATAM.

Limitaciones

Esta sección identifica las restricciones del estudio y su impacto en los resultados. El corte temporal del 11 de enero de 2025 excluye literatura posterior, potencialmente subestimando tendencias recientes en 2025 (317 documentos hasta la fecha). La dependencia de bases de datos como Scopus y WoS, con un sesgo hacia publicaciones en inglés (300 documentos vs. <10 en español), pudo haber omitido perspectivas locales disponibles en literatura gris (eg, informes de la OEA) o bases regionales como SciELO. La estrategia de búsqueda, aunque ampliada con términos como "transformación digital", podría no haber capturado toda la literatura relevante debido a variaciones en la terminología (por ejemplo, "seguridad informática" en español).

Implicancias

Los resultados amplían el marco teórico de la ciberseguridad al integrar la innovación como mediadora de la resiliencia, ofreciendo un modelo adaptable a contextos en desarrollo como América Latina. Esto invita a futuras investigaciones para validar el modelo con datos cualitativos. Se recomienda fomentar la colaboración intrarregional, conectando universidades y apoyando el financiamiento local para reducir la dependencia de recursos externos. Políticas como las de Brasil podrían servir de modelo para Honduras y otros países.

Se sugiere explorar la literatura gris y bases regionales (por ejemplo, Redalyc) para capturar perspectivas locales. Los estudios longitudinales post-2025 podrían evaluar el impacto de las políticas actuales, mientras que los análisis cualitativos podrían profundizar en las barreras culturales y económicas.

Contribución de los autores

Ambos autores contribuyeron de manera equitativa en la conceptualización del estudio, el diseño metodológico, la recopilación y depuración de los datos bibliométricos, el análisis e interpretación de los resultados, así como en la redacción, revisión crítica y aprobación de la versión final del manuscrito.

Conflictos de interés

Los autores declaran no tener conflictos de interés financieros, institucionales ni personales que pudieran influir en los resultados o en la interpretación de esta investigación.

Financiamiento

No aplicable

Uso de IA

En la elaboración del presente manuscrito se emplearon herramientas de inteligencia artificial como apoyo en tareas de revisión de estilo, mejora de la redacción académica y organización del contenido.

REFERENCIAS

Acevedo Duque, Á., Álvarez Herranz, A., & Marinao Artigas, E. (2023). Scientometrics study of country branding and its contribution to sustainable development in nations. *Data and Metadata*, *2*, 163. https://doi.org/10.56294/dm2023163

Aghazadeh Ardebili, A., Lezzi, M., & Pourmadadkar, M. (2024). Risk Assessment for Cyber Resilience of Critical Infrastructures: Methods, Governance, and Standards. *Applied Sciences*, *14*(24), 11807. https://doi.org/10.3390/app142411807

Al-Mohareb, M. (2025). The Impact of Cyber Governance Quality on Dividend Policy in Mitigating Cybersecurity Breaches. *Risks*, *13*(2), 34. https://doi.org/10.3390/risks13020034

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security*, *98*, 102003. https://doi.org/10.1016/j.cose.2020.102003

Annarelli, A., & Palombi, G. (2021). Digitalization Capabilities for Sustainable Cyber Resilience: A Conceptual Framework. *Sustainability*, *13*(23), 13065. https://doi.org/10.3390/su132313065

Ascue, O., Valle, O., & Santisteban, J. (2025). BLOCKSAGE: Blockchain-Based Cloud Architecture for Sensitive Data Management in SMEs. *Sustainability*, *17*(4), 1352. https://doi.org/10.3390/su17041352

Ayodele, B., & Buttigieg, V. (2024). The VNF Cybersecurity Dataset for Research (VNFCYBERDATA). *Data*, *9*(11), 132. https://doi.org/10.3390/data9110132

Bianchi, C., Mingo, S., & Fernandez, V. (2019). Strategic management in Latin America: Challenges in a changing world. *Journal of Business Research*, *105*, 306-309. Scopus. https://doi.org/10.1016/j.jbusres.2018.10.022

Choi, S.-H., Youn, J., Kim, K., Lee, S., Kwon, O.-J., & Shin, D. (2023). Cyber-Resilience Evaluation Methods Focusing on Response Time to Cyber Infringement. *Sustainability*, *15*(18), 13404. https://doi.org/10.3390/su151813404

Díaz-Piraquive, F. N., de Jesús Muriel-Perea, Y., & González-Crespo, R. (2023). Cybersecurity Management in Micro, Small, and Medium Enterprises in Colombia. En Uden L. & Ting I.-H. (Eds.), *Commun. Comput. Info. Sci.: Vol. 1825 CCIS* (pp. 74-85). Springer Science and Business Media Deutschland GmbH; Scopus. https://doi.org/10.1007/978-3-031-34045-1_8

El-Hajj, M., & Mirza, Z. A. (2024). ProtectingSmall and Medium Enterprises: A Specialized Cybersecurity Risk Assessment Framework and Tool. *Electronics*, *13*(19), 3910. https://doi.org/10.3390/electronics13193910

Flores Cedeño, P. R., & López Paz, C. R. (2024). Government Management of Information Technology in the Latin American Context. *Salud, Ciencia y Tecnología - Serie de Conferencias*, *3*, 682. https://doi.org/10.56294/sctconf2024682

Garay Canales, H. B., Casas Luna, S. A., Malaga Davila, C. P., Aponte Cajavilca, J. M., Cano Ccoa, D. M., Vilca Tantapoma, M. E., Alvarado Arbildo, G. R., & Aguirre López, H. M. (2025). The Digital Economy in Latin American Foreign Trade: Post-Pandemic Challenges for Sustainable Development. *Qubahan Academic Journal*, *5*(1), 580-597. Scopus. https://doi.org/10.48161/qaj.v5n1a1514

Goi, V., Ahieieva, I., Mamonov, K., Pavliuk, S., & Dligach, A. (2023). The Impact of Digital Technologies on the Companies' Strategic Management. *Economic Affairs (New Delhi)*, *68*(2), 1291-1299. Scopus. https://doi.org/10.46852/0424-2513.2.2023.33

Grisales Rendón, L. (2022). Latin American eGovernance and data protection: The EU model. *ACM Int. Conf. Proc. Ser.*, 100-105. Scopus. https://doi.org/10.1145/3551504.3551558

Heierhoff, S., & Reher, A. (2022). Balancing Digital Innovation and Cybersecurity Capabilities through Organizational Ambidexterity—An Investigation in the Automotive Industry. En Bui T.X. (Ed.), *Proc. Annu. Hawaii Int. Conf. Syst. Sci.* (Vols. 2022-January, pp. 6393-6402). IEEE Computer Society; Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85152234519&partnerID=40&md5=06a107f493a731809f91d71404b0e997

Hijji, M., & Alam, G. (2022). Cybersecurity Awareness and Training (CAT) Framework for Remote Working Employees. *Sensors*, *22*(22), 8663. https://doi.org/10.3390/s22228663

ISO/IEC. (2020). *Information technology. Security techniques. Information security management systems. Overview and vocabulary* (Onternational Organization for Standardization.). British Standards Institution.

Jeršič, N., Turkanović, M., & Beranič, T. (2025). Towards a Sustainable Cybersecurity Governance: Threat Modelling with Large Language Models. *Sustainability*, *17*(23), 10569. https://doi.org/10.3390/su172310569

Jung, J., & Katz, R. (2023). *Impacto del COVID-19 en la digitalización de América Latina*.

Kianpour, M., Kowalski, S. J., & Øverby, H. (2021). Systematically Understanding Cybersecurity Economics: A Survey. *Sustainability*, *13*(24), 13677. https://doi.org/10.3390/su132413677

Kosevich, E. Yu. (2022a). CYBERSPACE SECURITY IN LATIN AMERICAN COUNTRIES. *Polis. Political Studies*, *3*, 108-123. Scopus. https://doi.org/10.17976/jpps/2022.03.09

Kosevich, E. Yu. (2022b). CYBERSPACE SECURITY IN LATIN AMERICAN COUNTRIES. *Polis. Political Studies*, *3*, 108-123. Scopus. https://doi.org/10.17976/jpps/2022.03.09

Kour, R., Karim, R., Dersin, P., & Venkatesh, N. (2024). Cybersecurity for Industry 5.0: Trends and gaps. *Frontiers in Computer Science*, *6*, 1434436. https://doi.org/10.3389/fcomp.2024.1434436

Martínez-Peláez, R., Escobar, M. A., Félix, V. G., Ostos, R., Parra-Michel, J., García, V., Ochoa-Brust, A., Velarde-Alvarado, P., Félix, R. A., Olivares-Bautista, S., Flores, V., & Mena, L. J. (2024). Sustainable Digital Transformation for SMEs: A Comprehensive Framework for Informed Decision-Making. *Sustainability*, *16*(11), 4447. https://doi.org/10.3390/su16114447

Melaku, H. M. (2023). Context-Based and Adaptive Cybersecurity Risk Management Framework. *Risks*, *11*(6), 101. https://doi.org/10.3390/risks11060101

Metin, B., Özhan, F. G., & Wynn, M. (2024). Digitalisation and Cybersecurity: Towards an Operational Framework. *Electronics (Switzerland)*, *13*(21). Scopus. https://doi.org/10.3390/electronics13214226

Morales-Sáenz, F. I., Medina-Quintero, J. M., & Reyna-Castillo, M. (2024). Beyond Data Protection: Exploring the Convergence between Cybersecurity and Sustainable Development in Business. *Sustainability*, *16*(14), 5884. https://doi.org/10.3390/su16145884

OECD & Eurostat. (2018). *Oslo Manual 2018: Guidelines for Collecting, Reporting and Using Data on Innovation, 4th Edition*. OECD. https://doi.org/10.1787/9789264304604-en

Purdon, L., & Vera, F. (2020). Regional cybersecurity approaches in Africa and Latin America. En *Routledge Handb. Of International Cybersecur.* (pp. 234-246). Taylor and Francis; Scopus. https://doi.org/10.4324/9781351038904-23

Ramírez, M., Rodríguez Ariza, L., Gómez Miranda, M. E., & Vartika. (2022). The Disclosures of Information on Cybersecurity in Listed Companies in Latin America—Proposal for a Cybersecurity Disclosure Index. *Sustainability*, *14*(3), 1390. https://doi.org/10.3390/su14031390

Rawindaran, N., Jayal, A., Prakash, E., & Hewage, C. (2021). Cost Benefits of Using Machine Learning Features in NIDS for Cyber Security in UK Small Medium Enterprises (SME). *Future Internet*, *13*(8), 186. https://doi.org/10.3390/fi13080186

Sadik, S., Ahmed, M., Sikos, L. F., & Islam, A. K. M. N. (2020). Toward a Sustainable Cybersecurity Ecosystem. *Computers*, *9*(3), 74. https://doi.org/10.3390/computers9030074

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. *Sensors*, *23*(15), 6666. https://doi.org/10.3390/s23156666

Seabra Oliveira, D., Epstein, J., Kurose, J., & Rocha, A. (2019). Cybersecurity and Privacy Issues in Brazil: Back, Now, and Then [Guest Editors' Introduction]. *IEEE Security and Privacy*, *16*(6), 10-12. Scopus. https://doi.org/10.1109/MSEC.2018.2874824

Shahim, A. (2021). Security of the digital transformation. *Computers & Security*, *108*, 102345. https://doi.org/10.1016/j.cose.2021.102345

Stefani, E., Costa, I., Gaspar, M. A., Goes, R. D. S., Monteiro, R. C., Petrili, B. R., & Pereira, A. D. P. (2025). Information Security Risk Framework for Digital Transformation Technologies. *Systems*, *13*(1), 37. https://doi.org/10.3390/systems13010037

Taskin, N., Özkeleş Yıldırım, A., Ercan, H. D., Wynn, M., & Metin, B. (2025). Cyber Insurance Adoption and Digitalisation in Small and Medium-Sized Enterprises. *Information*, *16*(1), 66. https://doi.org/10.3390/info16010066

Ukwandu, E., Ben-Farah, M. A., Hindy, H., Bures, M., Atkinson, R., Tachtatzis, C., Andonovic, I., & Bellekens, X. (2022). Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends. *Information*, *13*(3), 146. https://doi.org/10.3390/info13030146

Van Zomeren, M., Deane, F., Joiner, K. F., Qiao, L., Horne, R., & Suprun, E. (2025). Regulating Cyberworthiness: Governance Frameworks for Safety-Critical Cyber-Physical Systems. *Systems*, *13*(10), 862. https://doi.org/10.3390/systems13100862

Von Solms, R., & Von Solms, B. (2018). Issue Information. *Information Systems Journal*, *28*(5), 28(2)123-145. https://doi.org/10.1111/isj.12165

World Bank. (2022). *Digital Economy for Latin America and the Caribbean: Country Diagnostic: El Salvador.* 150. Report No. AUS0002748.