Revista Científica
ANFIBIOS
ISSN: 2665-1513 (Impreso) | ISSN: 2711-0532 (En línea)

Cultura de Ciberseguridad en las Organizaciones: Un análisis cienciométrico de las Tendencias Globales y Empresariales

Cybersecurity Culture in Organizations: A Scientometric Analysis of Global and Business Trends

Karen Álvarez-Ballestas*
Universidad Tecnológica de Bolívar - Colombia
ORCID iD: https://orcid.org/0009-0006-0534-0743
karalvarez@utb.edu.co

Jhorquis Machado-Licona
Universidad Tecnológica de Bolívar - Colombia
ORCID iD: https://orcid.org/0000-0002-6987-7658
jmachado@utb.edu.co

Fecha de recepción: 11/08/2025
Fecha de evaluación: 26/08/2025
Fecha de aceptación: 12/10/2025

Cómo citar: *Álvarez-Ballestas, K., & Machado-Licona, J. (2025). Cultura de Ciberseguridad en las Organizaciones: Un análisis cienciométrico de las Tendencias Globales y Empresariales. Revista Científica Anfibios, 8(2), 11-21. https://doi.org/10.37979/afb.2025v8n2.178.*

*Autor a quien debe ser dirigida la correspondencia

Resumen

Introducción: La cultura de ciberseguridad se ha convertido en un componente clave en la protección de los activos digitales de las empresas, dado que a pesar de todos los controles técnicos que se puedan implementar para garantizar la seguridad de la información, la influencia del comportamiento humano frente a las amenazas informáticas es primordial. Objetivo: Analizar el comportamiento de la documentación e investigación sobre cultura de ciberseguridad en entornos empresariales durante el periodo 2005–2025. Metodología: Estudio bibliométrico y cienciométrico de 74 artículos obtenidos de la base de datos Scopus. Se aplicaron indicadores de productividad, colaboración, coocurrencia de palabras clave, redes de coautoría y análisis de citas. Resultados: Se evidencia una tendencia creciente en la producción científica a partir de 2017, con una línea de crecimiento exponencial ajustada a un $R^2 = 0.41$. Se identificó un enfoque temático centrado en tres ejes: cultura organizacional, comportamiento del usuario y estrategias de concienciación. Destacan autores como Da Veiga, L.V.; Hart, S.; y Rawindaran, N., así como instituciones del Reino Unido, Malasia y Estados Unidos. Conclusiones: La cultura de ciberseguridad es un ámbito en desarrollo que busca entender cómo los elementos humanos y organizacionales influyen en la gestión de riesgos digitales. Las investigaciones actuales se centran en la gamificación para la concientización, la evaluación de la madurez cultural y la cooperación internacional para mejorar las prácticas de seguridad digital en empresas.

Palabras clave

Cultura de Ciberseguridad; Análisis Bibliométrico; Ciberseguridad Organizacional; Comportamiento del Usuario; Concienciación en Seguridad.

Abstract

Introduction: Cybersecurity culture has become a key component in the protection of companies' digital assets, given that despite all the technical controls that can be implemented to guarantee information security, the influence of human behavior in the face of computer threats is paramount. Objective: To analyze the behavior of scientific production on cybersecurity culture in business environments during the period 2005–2025. Methodology: A bibliometric and scientometric study of 74 articles retrieved from the Scopus database. Indicators of productivity, collaboration, keyword co-occurrence, co-authorship

networks, and citation analysis were applied. Results: A growing trend in scientific output is evident beginning in 2017, with an exponential growth curve adjusted to an $R^2 = 0.41$. A thematic focus was identified around three main axes: organizational culture, user behavior, and awareness strategies. Notable authors include Da Veiga, L.V.; Hart, S.; and Rawindaran, N., along with institutions from the United Kingdom, Malaysia, and the United States. Conclusions: Cybersecurity culture is a developing field that seeks to understand how human and organizational factors influence digital risk management. Current research focuses on gamification for awareness, assessing cultural maturity, and international cooperation to improve digital security practices in companies.

Keywords
Cybersecurity Culture; Bibliometric Analysis; Organizational Cybersecurity; User Behavior; Security Awareness.

Introducción

Así como la tecnología es un apalancador del cambio en las organizaciones y en las últimas dos décadas, ha dejado de ser un asunto técnico exclusivo del área de Tecnologías de la Información (TI) para convertirse en un componente esencial de la gestión organizacional, así la ciberseguridad asociada a todo este avance tecnológico cobra mucho valor, debido a que es la capa que asegurará la continuidad operacional en las empresas, ya que cada vez más se soportan en plataformas tecnológicas. Desde 2005, el auge de la industria 4.0, la conectividad global y la sofisticación de los ciberataques han generado un crecimiento significativo en la literatura académica centrada en la cultura de la ciberseguridad organizacional, entendida como el conjunto de valores, actitudes, conocimientos y prácticas compartidas por los miembros de una organización en torno a la seguridad digital (Da Veiga & Eloff, 2010). A lo largo del periodo 2005-2025, esta línea ha evolucionado de forma notable. Al principio, predominaban los estudios centrados en el cumplimiento normativo y de allí que el enfoque consistía en el desarrollo de procedimientos, políticas, manuales y el cumplimiento de los mismos, así como la concienciación individual. Sin embargo, en los últimos 10 años se ha dado paso a un enfoque más integral donde se exploran variables como el liderazgo, la madurez cultural, centrándose en la necesidad de cada proceso de la organización, la resiliencia organizacional y el comportamiento humano dependiendo del rol que este ejerza frente a la complejidad de las amenazas cibernéticas (Parsons et al., 2014).

El incremento de incidentes globales como el ataque a Sony (2014), WannaCry (2017) o SolarWinds (2020), junto con la masificación del teletrabajo durante la pandemia por COVID-19, motivaron a las organizaciones a adoptar estrategias centradas en las personas, reconociendo que la tecnología sin una cultura sólida es insuficiente para proteger activos digitales (Rocha Flores & Ekstedt, 2016). En consecuencia, el concepto de cultura de ciberseguridad ha ganado presencia en la agenda investigativa internacional, donde se han abordado aspectos como la evaluación de la madurez cultural (Da Veiga & Martins, 2015), el desarrollo de competencias conductuales (Kajzer et al., 2014) y los factores organizacionales que influyen en el cumplimiento de políticas establecidas en las diferentes compañías (Ifinedo, 2014).

Esta investigación tiene como objetivo principal analizar la evolución de la producción científica sobre cultura de ciberseguridad empresarial entre los años 2005 y 2025, a partir de un enfoque bibliométrico y cienciométrico. A través del uso de técnicas de análisis de datos como Excel y herramientas visuales como VOSviewer, el estudio busca identificar las principales tendencias temáticas, autores, instituciones, palabras clave y patrones de colaboración en este campo. El objetivo es ofrecer una visión integral del conocimiento existente, al tiempo que propone líneas futuras de investigación para fortalecer la seguridad organizacional desde una perspectiva humana y cultural.

Marco teórico

La cultura de ciberseguridad se refiere a los valores, creencias, actitudes y comportamientos compartidos dentro de una organización respecto a la protección de los sistemas de información. Este concecpto ha evolucionado desde una visión instrumental del cumplimiento normativo, hacia un enfoque holístico en el que los usuarios, sus hábitos y su contexto sociotécnico juegan un papel determinante en la defensa digital de las organizaciones (Da Veiga & Eloff, 2010). Autores como (Ifinedo, 2014) y (Tejay & Mohammed, 2023) han argumentado que una cultura sólida favorece el cumplimiento voluntario a las normas de seguridad, mientras que su ausencia incrementa los riesgos asociados al error humano y la negligencia. En esta

línea (Schlienger & Teufel, 2005) sugieren que la cultura debe gestionarse de forma similar a cualquier otro activo estratégico, mediante diagnósticos periódicos y programas de refuerzo conductual.

Entre los enfoques más citados se destaca el *Security Culture Maturity Model* (Da Veiga & Martins, 2015) que permite evaluar el nivel de desarrollo cultural, clave para tener un diagnóstico inicial de que tan consientes se encuentran los colaboradores respecto a la seguridad de la información y a partir de allí definir planes de acción. Otros marcos como los de (Furnell et al., 2010) clasifican la cultura en dimensiones cognitivas, actitudinales y conductuales.

Investigaciones como las (Vance et al., 2012) han resaltado que los comportamientos inseguros persisten incluso en organizaciones con políticas claras. Esta "brecha de comportamiento" puede mitigarse mediante estrategias como la gamificación (Hart et al., 2020), la segmentación del mensaje dependiendo de los roles y responsabilidades, y la alineación de incentivos organizacionales.

Desde 2010, han emergido modelos de diagnóstico que permiten evaluar la madurez de la cultura de ciberseguridad en las organizaciones. Uno de los más influyentes es el *Security Culture Framework*, que mide niveles de madurez desde la concienciación básica hasta el compromiso conductual (Alshaikh, 2020). Estos modelos se han aplicado en sectores como la banca, la educación superior y la administración pública (D'Arcy et al., 2014). El auge del enfoque *behavioral cybersecurity* ha impulsado estudios centrados en los factores cognitivos y emocionales que afectan la toma de decisiones en contextos de riesgo digital (Parsons et al., 2014). En particular, los trabajos de (Hadlington, 2017) resaltan que el exceso de confianza, el estrés laboral y la fatiga digital pueden disminuir la efectividad de las campañas de concienciación y fomentar errores involuntarios.

Además, se ha identificado una brecha persistente entre la conciencia y la acción: aunque muchos empleados conocen las políticas, no son aplicadas de manera consistente (Bada et al., 2019). Esta brecha es crítica y ha llevado al desarrollo de enfoques basados en nudges, gamificación y programas de refuerzo positivo como mecanismos de cambio de comportamiento.

En la etapa más reciente (2020–2025), la literatura ha comenzado a integrar la cultura de ciberseguridad con la transformación digital, el trabajo remoto y la adopción de nuevas tecnologías como la inteligencia artificial y el Internet de las cosas (IoT). (Alshaikh, 2020) advierte que los nuevos entornos laborales presentan desafíos particulares para sostener una cultura de seguridad sólida, resaltando en contextos híbridos o deslocalizados.

Asimismo, la internacionalización de los ciberataques y la evolución normativa (por ejemplo, el RGPD o la NIS2) han impulsado la necesidad de adaptar las culturas organizacionales a estándares de gobernanza global, donde el cumplimiento se combine con el compromiso genuino de los usuarios (Ifinedo, 2014; Tsohou et al., 2015).

Metodología

El presente estudio se enmarca en un enfoque cuantitativo, de tipo exploratorio-descriptivo, orientado a realizar un análisis cienciométrico y bibliométrico de la producción científica relacionada con la cultura de ciberseguridad en contextos empresariales. La finalidad metodológica consiste en identificar las tendencias de publicación, los autores e instituciones más relevantes, las redes de colaboración, y los núcleos temáticos emergentes en torno a esta área de estudio, durante el periodo comprendido entre 2005 y 2025.

La recolección de datos se llevó a cabo en la base de datos Scopus, reconocida por su cobertura internacional y rigurosidad en la indexación de literatura científica. Para delimitar el corpus documental, se utilizó una estrategia de búsqueda avanzada con operadores booleanos, dirigida a identificar estudios que abordan la cultura de ciberseguridad desde una perspectiva organizacional o empresarial. El criterio aplicado fue el siguiente:

(TITLE-ABS-KEY ("cybersecurity culture" OR "information security culture" OR "cyber security awareness") AND TITLE-ABS-KEY (enterprise OR company OR business OR organization)) AND (LIMIT-TO (OA, "all"))

Esta búsqueda fue aplicada a los campos de título, resumen y palabras clave, con el fin de garantizar una adecuada cobertura temática. Como resultado, se obtuvo una muestra final de 74 documentos válidos para el análisis. Para el análisis de los datos, se siguieron los siguientes procedimientos metodológicos:

Revisión y depuración de datos

Se exportaron los registros bibliográficos en formato CSV desde Scopus y se procedió a la limpieza de datos para corregir inconsistencias, homogeneizar nombres de autores e instituciones, y consolidar palabras clave equivalentes.

Análisis bibliométrico descriptivo

Se calcularon indicadores cuantitativos clásicos como el número de publicaciones por año, productividad por país y autor, instituciones más activas, revistas más frecuentes y artículos más citados. Esta información se organizó y visualizó mediante gráficos y tablas elaborados en Microsoft Excel, permitiendo una visión cronológica y geográfica del desarrollo del campo.

Análisis cienciométrico relacional

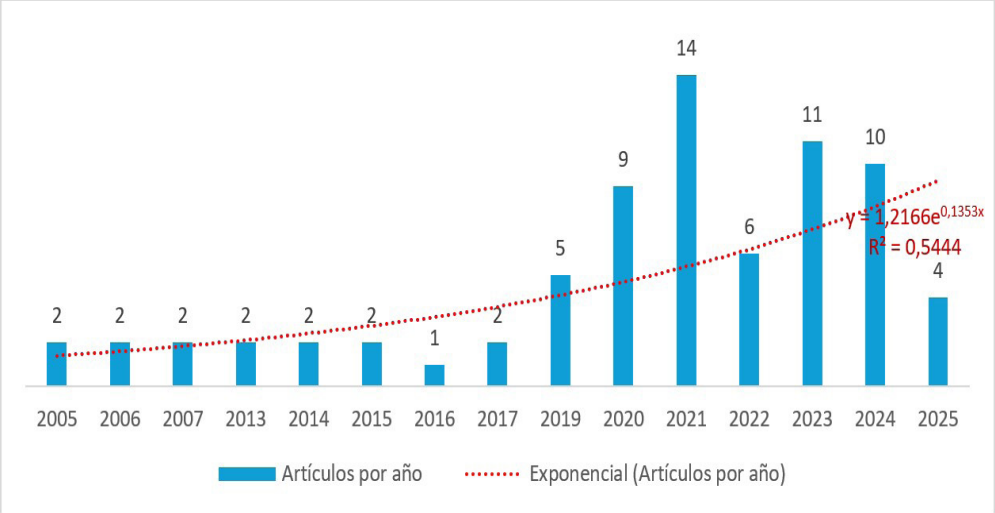
A través del software VOSviewer (v1.6.20), se generaron mapas de visualización para explorar redes de coautoría entre investigadores, colaboraciones internacionales entre países, coocurrencia de palabras clave y clústeres temáticos. Para ello, se establecieron umbrales mínimos de frecuencia para garantizar la solidez de las conexiones visualizadas. Este enfoque permitió identificar comunidades de investigación, estructuras colaborativas, y patrones semánticos que reflejan la evolución del discurso académico sobre cultura de ciberseguridad en entornos organizacionales. Los mapas de redes generados fueron con los siguientes criterios:

- Coautoría entre autores (mínimo 2 publicaciones por autor)
- Colaboración internacional entre países (mínimo 2 publicaciones por país)
- Coocurrencia de palabras clave (mínimo 3 ocurrencias por término)
- Clústeres temáticos agrupados por similitud semántica

Finalmente, los hallazgos fueron contrastados con el marco teórico y con estudios previos relevantes, con el fin de contextualizar los resultados y destacar aportes significativos, vacíos temáticos o posibles líneas de investigación futura. Toda la información utilizada proviene de fuentes académicas públicas y se procesó conforme a principios de integridad científica y respeto ético en el uso de datos bibliográficos.

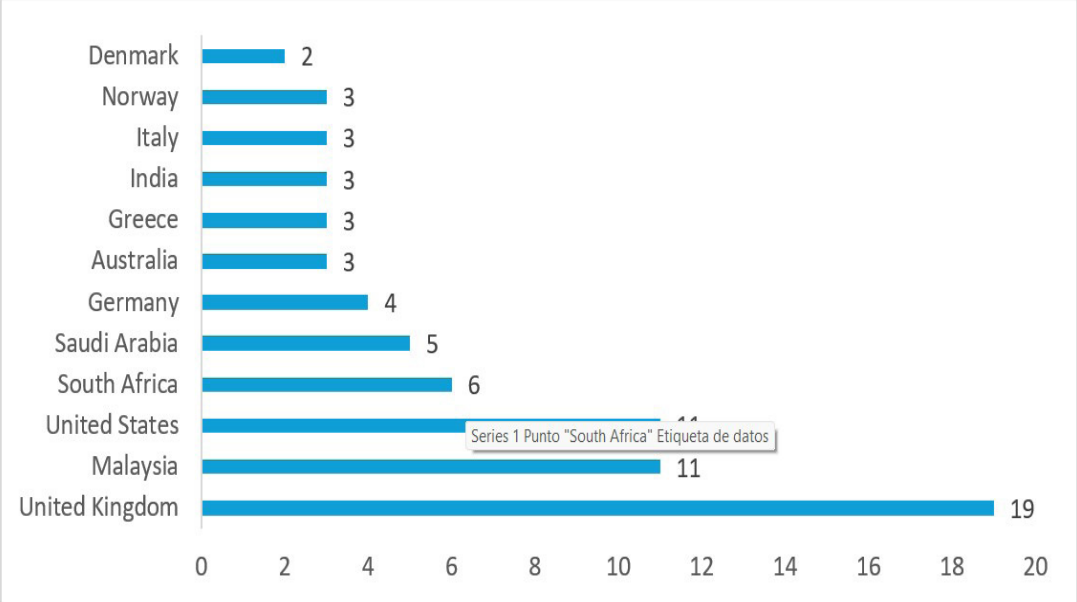
Resultados

En la gráfica 1, el análisis temporal muestra un crecimiento gradual en la producción científica sobre cultura de ciberseguridad desde 2005. Aunque los primeros años presentaron una baja frecuencia (entre 1 y 2 publicaciones anuales), a partir de 2017 se observa una tendencia sostenida al alza, alcanzando un pico de 14 artículos en 2021. La curva de crecimiento se ajusta a una progresión exponencial moderada ($R^2 = 0.41$), lo que refleja un interés emergente pero aún en consolidación en el campo. Cabe destacar que la publicación disminuye levemente hacia 2025, posiblemente debido a que el año aún no ha concluido al momento del análisis.



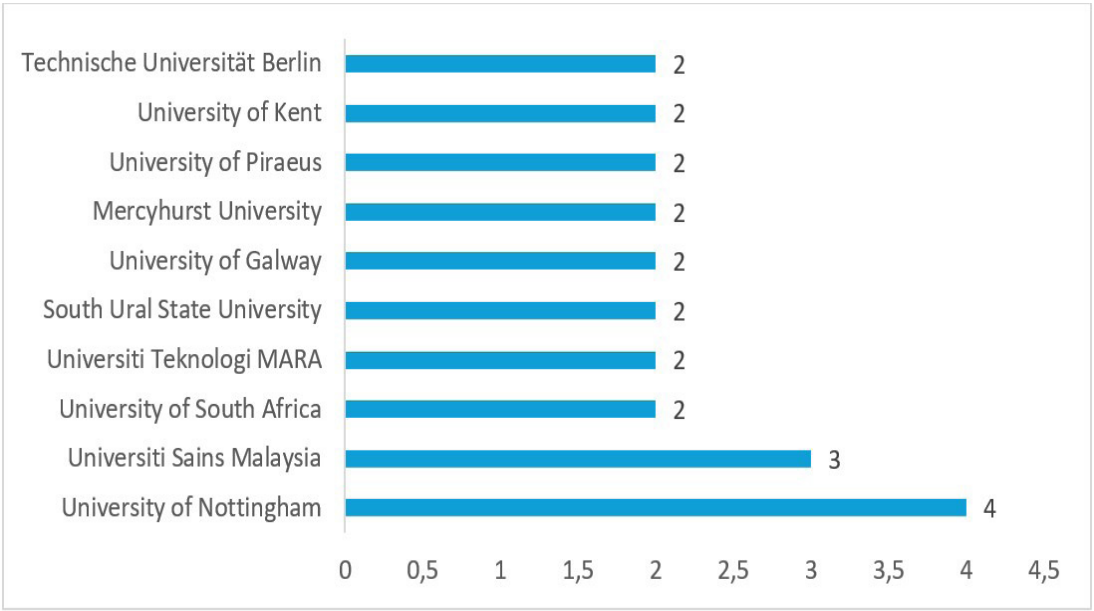
Gráfica 1. Publicación de artículos de ciberseguridad por año
Fuente: Elaboración propia con datos de Scopus

La producción científica está más concentrada en ciertos países, como se presenta en la gráfica 2. El Reino Unido lidera con 19 publicaciones, seguido de Malasia y Estados Unidos (ambos con 11), y Sudáfrica (6). Estos resultados indican que la investigación en cultura de ciberseguridad se ha desarrollado en contextos angloparlantes y en regiones con políticas activas en gestión de riesgos digitales. También es relevante la participación de países como Arabia Saudita, Alemania e India, lo que sugiere un interés global y transversal por el tema, aunque con menor densidad investigativa en América Latina.



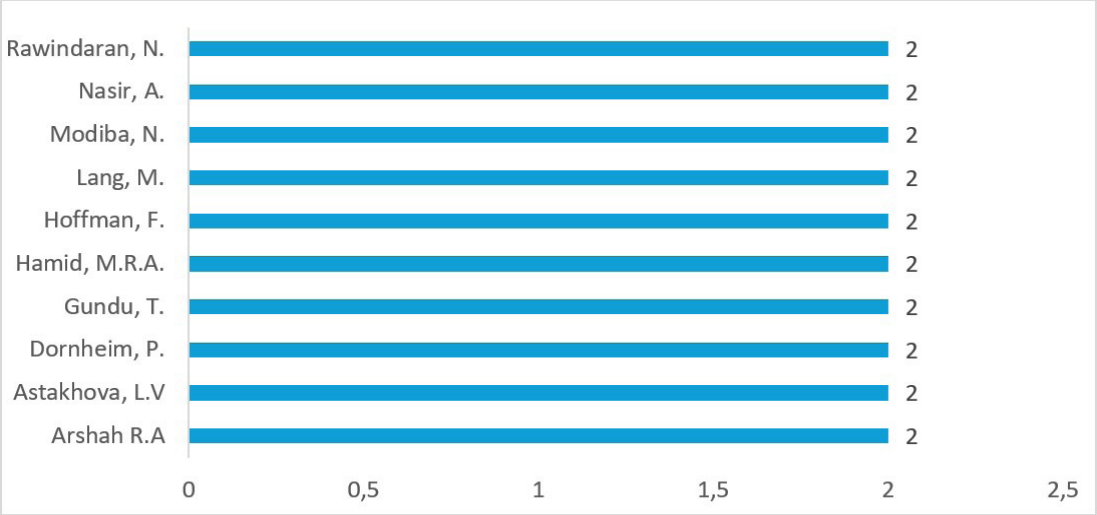
Gráfica 2. Publicación de artículos de ciberseguridad por país
Fuente: Elaboración propia con datos de Scopus

En la gráfica 3 se observa la publicación por organizaciones, entre las más activas se encuentran la University of Nottingham (4 artículos), Universiti Sains Malaysia (3), y otras universidades con 2 artículos cada una, como Technische Universität Berlin, University of Piraeus, University of Kent y University of South Africa, indicando que, si bien el tema es de interés mundial, no existe aún una concentración excesiva de producción en pocos centros de excelencia, sino una dispersión moderada entre instituciones.



Gráfica 3. Publicación de artículos de ciberseguridad por organización
Fuente: Elaboración propia con datos de Scopus

Los investigadores con mayor número de publicaciones como se muestra en la gráfica 4. (2 cada uno) son: Rawindaran, N., Nasir, A., Modiba, N., Lang, M., entre otros. Esta homogeneidad sugiere un campo en desarrollo, sin figuras dominantes, pero con varios autores recurrentes que han contribuido de forma significativa al debate sobre cultura de ciberseguridad. La mayoría proviene de instituciones asiáticas, europeas y africanas, lo que también respalda la visión de una red de producción internacional.



Gráfica 4. Publicación de artículos de ciberseguridad por autor
Fuente: Elaboración propia con datos de Scopus

El análisis de coocurrencia de palabras clave realizado en VOSviewer (v1.6.20) mostrado en la Figura 1 revela tres grandes clústeres temáticos interrelacionados:

- El primer clúster (rojo) gira en torno a "cybersecurity", "cyber security" y "security of data".
- El segundo clúster (azul) agrupa términos como "information security culture", "information systems" y "security awareness".
- El tercer clúster (verde y morado) integra conceptos como "organizational culture", "compliance", "trust", "decision making" y "employee behavior".

Este mapa semántico evidencia que el discurso académico está centrado en la intersección entre tecnología, comportamiento humano y cultura organizacional. Destaca además la emergencia de términos como cybersecurity culture y information security culture como ejes semánticos predominantes.

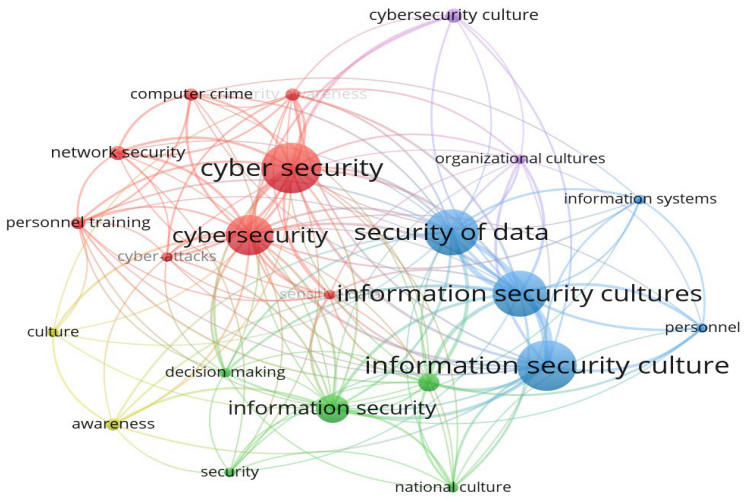


Figura 1. Coocurrencia en el uso de palabras clave.
Fuente: Elaboración propia con datos de Scopus

En la Figura 2 se evidencia que las redes de colaboración internacional muestran una fuerte centralidad de países como el Reino Unido, Malasia y Estados Unidos, que actúan como nodos de alta conectividad entre autores de diversas regiones. El Reino Unido mantiene vínculos directos con países como Grecia, India, Estados Unidos, y Noruega, mientras que Malasia se conecta activamente con Sudáfrica, China y Arabia Saudita. Estas redes sugieren una interdependencia académica global, con ciertos hubs regionales que impulsan la investigación transnacional sobre el tema.

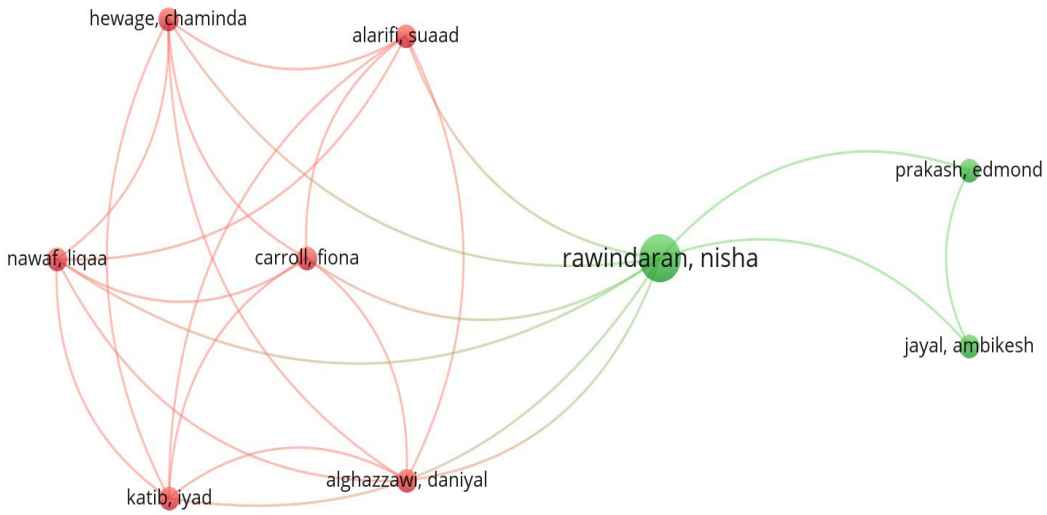


Figura 2. Coautorías de artículos en ciberseguridad
Fuente: Elaboración propia con datos de Scopus

El análisis de coautoría a nivel individual analizado en la Figura 3 permite identificar comunidades científicas activas. El nodo de mayor conexión es Rawindaran, Nisha, quien aparece colaborando con autores como Prakash, Edmond y Jayal, Abikesh, lo cual sugiere un grupo de investigación consolidado en torno a cultura de ciberseguridad. Otros clústeres relevantes involucran a autores de Medio Oriente y África, evidenciando la descentralización temática del campo.

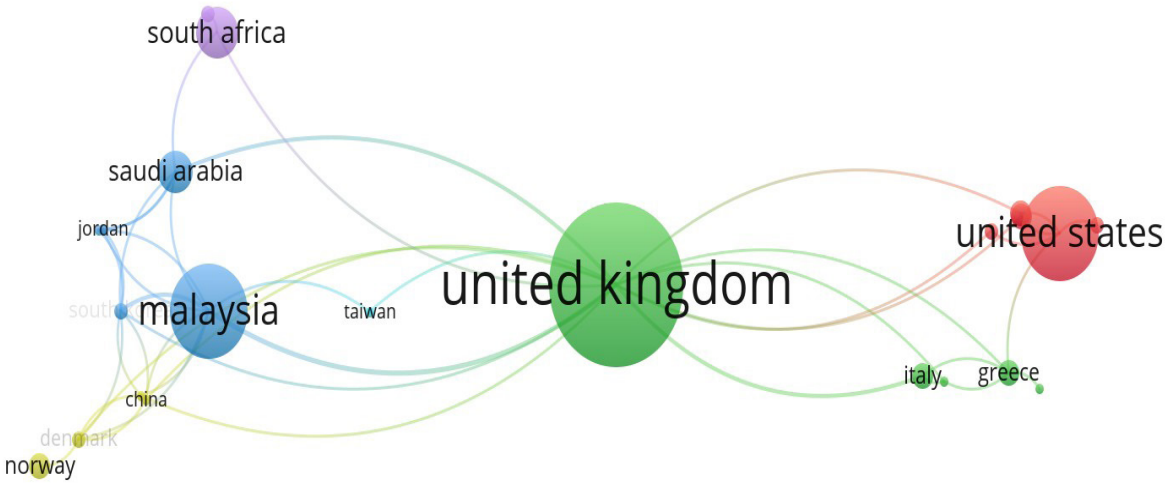


Figura 3. Coautorías entre países de artículos en ciberseguridad
Fuente: Elaboración propia con datos de Scopus

Los artículos con mayor impacto se relacionan directamente con el diseño de programas de concienciación, el uso de gamificación para educación en ciberseguridad, y la evaluación de culturas organizacionales en contextos académicos y empresariales. El artículo más citado (Cose et al., 2007) acumula 185 citas, pionero en introducir el uso de videojuegos como herramienta de formación en seguridad informática. Estableció un precedente en la relación entre cultura, comportamiento y

tecnologías interactivas. Seguido por Hart et al. (2020) con 171 que profundiza en la gamificación como estrategia para mejorar la retención de conocimientos en usuarios no técnicos, especialmente en sectores educativos y pymes. Estos trabajos comparten una visión aplicada de la ciberseguridad desde lo conductual y educativo, consolidando la idea de que el usuario es tanto el eslabón más débil como el más importante en el ecosistema de ciberseguridad.

Tabla 1. 10 artículos más citados en la base de datos Scopus

Artículo	Autor	Año	Citas
A video game for cyber security training and awareness	Cone B.D.; Irvine C.E.; Thompson M.F.; Nguyen T.D.	2007	185
Riskio: A Serious Game for Cyber Security Awareness and Education	Hart S.; Margheri A.; Paci F.; Sassone V.	2020	171
Defining organisational information security culture—Perspectives from academia and industry	da Veiga A.; Astakhova L.V.; Botha A.; Herselman M.	2020	144
Developing a cyber security culture: Current practices and future needs	Uchendu B.; Nurse J.R.C.; Bada M.; Furnell S.	2021	119
The least secure places in the universe? A systematic literature review on information security management in higher education	Bongiovanni I.	2019	61
Machine learning cybersecurity adoption in small and medium enterprises in developed countries	Rawindaran N.; Jayal A.; Prakash E.	2021	49
Institutional Strategies for Cybersecurity in Higher Education Institutions	Cheng E.C.K.; Wang T.	2022	47
Towards understanding cybersecurity capability in Australian healthcare organisations: a systematic review of recent trends, threats and mitigation	Offner K.L.; Sitnikova E.; Joiner K.; MacIntyre C.R.	2020	47
Cyber physical systems security for maritime assets	Progoulakis I.; Rohmeyer P.; Nikitakos N.	2021	43
Human factors in information leakage: mitigation strategies for information sharing integrity	Wong W.P.; Tan H.C.; Tan K.H.; Tseng M.-L.	2019	41

Fuente: Elaboración propia con datos de Scopus.

Discusión

Los resultados obtenidos en este estudio permiten identificar una evolución sostenida en la atención académica hacia la cultura de ciberseguridad en contextos organizacionales durante el periodo 2005–2025. Este crecimiento progresivo, especialmente acentuado a partir de 2017, se alinea con los postulados de autores como Da Veiga y Martins (2015) y Parsons et al. (2017), quienes señalan que la cultura de seguridad ha ganado relevancia en respuesta al aumento de incidentes vinculados al comportamiento humano en el entorno digital.

La diversidad geográfica observada, con liderazgos marcados por países como Reino Unido, Malasia y Estados Unidos, sugiere que la preocupación por la ciberseguridad cultural es transversal a contextos con niveles de desarrollo y digitalización distintos. Sin embargo, se evidencian brechas regionales, especialmente en América Latina y África, donde se ve la necesidad de fortalecer la infraestructura investigativa en regiones en vías de consolidación digital.

En términos institucionales, el hallazgo de una producción moderadamente dispersa entre uni-

versidades refuerza la idea de un campo académico en expansión, pero aún sin centros de influencia. Esto es coherente con el carácter emergente de los estudios sobre cultura de ciberseguridad, que aún no presentan comunidades científicas consolidadas de forma sistemática, como reflejan las redes de coautoría entre autores, relativamente fragmentadas, pero en crecimiento.

Desde el punto de vista temático, el análisis de coocurrencia de palabras clave confirma la articulación de tres ejes conceptuales dominantes: el técnico *(cybersecurity, data security),* el conductual *(awareness, behavior, trust)* y el organizacional *(compliance, culture, decision-making)*. Esta distribución valida que la cultura de ciberseguridad debe entenderse como un fenómeno multidimensional que integra lo humano, lo estructural y lo tecnológico.

Particularmente revelador es el hecho de que los artículos más citados no solo abordan la seguridad desde la dimensión técnica, sino que enfatizan estrategias educativas innovadoras, como la gamificación, para mejorar la concienciación y el comportamiento de los usuarios. Existe la necesidad de estrategias adaptativas que cierren la brecha entre conocimiento y acción. Asimismo, los estudios consultados han contribuido de manera significativa a la consolidación conceptual del campo, proporcionando marcos analíticos para evaluar la madurez de la cultura organizacional en ciberseguridad.

Finalmente, las redes de colaboración entre países y autores reflejan un sistema científico más interconectado. La existencia de clústeres colaborativos en regiones como Europa y Asia señala una tendencia a la conformación de comunidades de práctica, aunque todavía incipientes. Esto coincide con quienes destacan que la cultura de ciberseguridad también requiere un enfoque colaborativo en la producción de conocimiento.

Conclusiones

Este estudio permitió trazar un panorama estructurado sobre la evolución y el estado actual de la producción científica en cultura de ciberseguridad empresarial, mediante un análisis cienciométrico y bibliométrico de publicaciones indexadas en Scopus entre 2005 y 2025. Los hallazgos indican que esta área ha experimentado un crecimiento sostenido en las últimas dos décadas, impulsado por la necesidad de comprender y transformar el comportamiento humano ante las amenazas digitales.

Se identificaron tres líneas temáticas predominantes: la dimensión técnica de la seguridad de datos, la dimensión organizacional centrada en políticas y cumplimiento, y la dimensión conductual orientada a la conciencia y el cambio de hábitos. Estas dimensiones, lejos de estar aisladas, interactúan en la configuración de una cultura de seguridad integral, como lo sugiere la literatura revisada.

Los artículos más citados, con enfoques aplicados en gamificación, concienciación y evaluación de madurez cultural, refuerzan la idea de que el éxito de la ciberseguridad organizacional depende, en gran medida, de las personas y su entorno. Asimismo, las redes de colaboración científica revelan una progresiva internacionalización del campo, aunque con desequilibrios geográficos aún presentes.

Entre las principales limitaciones del estudio se encuentra la restricción a una sola base de datos (Scopus), lo cual puede excluir literatura relevante de otras fuentes. También se reconoce la dificultad de estandarizar términos clave debido a la variabilidad semántica en el campo.

Como proyección futura, se sugiere ampliar el análisis a otras bases como *Web of Science o Dimensions*, e incorporar análisis cualitativos que profundicen en cómo las organizaciones aplican en la práctica los modelos culturales identificados en la literatura. Asimismo, se recomienda fortalecer la investigación en regiones subrepresentadas y explorar las interacciones entre cultura de ciberseguridad, liderazgo digital y resiliencia organizacional.

Referencias

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

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? https://arxiv.org/pdf/1901.02672

Bongiovanni, I. (2019). The least secure places in the universe? A systematic literature review on information security management in higher education. Computers & Security, 86, 350–357. https://doi.org/10.1016/J.COSE.2019.07.003

Cheng, E. C. K. ;, Wang, T., Cheng, E. C. K., & Wang, T. (2022). Institutional Strategies for Cybersecurity in Higher Education Institutions. Information 2022, Vol. 13, Page 192, 13(4), 192. https://doi.org/10.3390/INFO13040192

Cone, B. D., Irvine, C. E., Thompson, M. F., & Nguyen, T. D. (2007). A video game for cyber security training and awareness. Computers & Security, 26(1), 63–72. https://doi.org/10.1016/J.COSE.2006.10.005

Da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. Computers & Security, 92, 101713. https://doi.org/10.1016/J.COSE.2020.101713

Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. Computers & Security, 29(2), 196–207. https://doi.org/10.1016/J.COSE.2009.09.002

Da Veiga, A., & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. Computers & Security, 49, 162–176. https://doi.org/10.1016/J.COSE.2014.12.006

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. Journal of Management Information Systems, 31(2), 285–318. https://doi.org/10.2753/MIS0742-1222310210

Furnell, S. M., Clarke, N., & Lacey, D. (2010). Understanding and transforming organizational security culture. Information Management & Computer Security, 18(1), 4–13. https://doi.org/10.1108/09685221011035223

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon, 3(7), e00346. https://doi.org/10.1016/J.HELIYON.2017.E00346

Hart, S., Margheri, A., Paci, F., & Sassone, V. (2020). Riskio: A Serious Game for Cyber Security Awareness and Education. Computers & Security, 95, 101827. https://doi.org/10.1016/J.COSE.2020.101827

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. Information & Management, 51(1), 69–79. https://doi.org/10.1016/J.IM.2013.10.001

Kajzer, M., Darcy, J., Crowell, C. R., Striegel, A., & Van Bruggen, D. (2014). An exploratory investigation of message-person congruence in information security awareness campaigns. Computers & Security, 43, 64–76. https://doi.org/10.1016/J.COSE.2014.03.003

Offner, K. L., Sitnikova, E., Joiner, K., & MacIntyre, C. R. (2020). Towards understanding cybersecurity capability in Australian healthcare organisations: a systematic review of recent trends, threats and mitigation. Intelligence and National Security, 35(4), 556–585. https://doi.org/10.1080/02684527.2020.1752459

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Computers & Security, 42, 165–176. https://doi.org/10.1016/J.COSE.2013.12.003

Progoulakis, I., Rohmeyer, P., & Nikitakos, N. (2021). Cyber Physical Systems Security for Maritime Assets. Journal of Marine Science and Engineering 2021, Vol. 9, Page 1384, 9(12), 1384. https://doi.org/10.3390/JMSE9121384

Rawindaran, N., Jayal, A., & Prakash, E. (2021). Machine Learning Cybersecurity Adoption in Small and Medium Enterprises in Developed Countries. Computers 2021, Vol. 10, Page 150, 10(11), 150. https://doi.org/10.3390/COMPUTERS10110150

Rocha Flores, W., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. Computers & Security, 59, 26–44. https://doi.org/10.1016/J.COSE.2016.01.004

Schlienger, T., & Teufel, S. (2005). Tool Supported Management of Information Security Culture. IFIP Advances in Information and Communication Technology, 181, 65–77. https://doi.org/10.1007/0-387-25660-1_5

Tejay, G. P. S., & Mohammed, Z. A. (2023). Cultivating security culture for information security success: A mixed-methods study based on anthropological perspective. Information & Management, 60(3), 103751. https://doi.org/10.1016/J.IM.2022.103751

Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. Computers & Security, 109, 102387. https://doi.org/10.1016/J.COSE.2021.102387

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. Information & Management, 49(3–4), 190–198. https://doi.org/10.1016/J.IM.2012.04.002

Wong, W. P., Tan, H. C., Tan, K. H., & Tseng, M. L. (2019). Human factors in information leakage: mitigation strategies for information sharing integrity. Industrial Management & Data Systems, 119(6), 1242–1267. https://doi.org/10.1108/IMDS-12-2018-0546