Revista de Pensamiento Estratégico y Seguridad CISDE

Recibido: 26-02-2024 / Revisado: 11-05-2024
Aceptado: 15-05-2024 / Publicado: 30-11-2024

CISDE Journal, 9(2), 2024

La ciberseguridad en las empresas: estudio bibliométrico

Cybersecurity in companies: bibliometric study

Alberto Luján-Salamanca[1,2], Alfonso Infante-Moro[1], Juan Carlos Infante-Moro[1], Julia Gallardo-Pérez[1]

[1] Universidad de Huelva, España
[2] IES Ágora, Cáceres, España

alberto.lujan@alu.uhu.es , alfonso.infante@decd.uhu.es , juancarlos.infante@decd.uhu.es , julia.gallardo@decd.uhu.es

RESUMEN. Los ataques cibernéticos a empresas van en aumento en los últimos años y sus efectos pueden extenderse, no solo a las empresas que los sufren, sino que pueden llegar a afectar la seguridad nacional de un país o ser decisivos en época de conflicto o guerra. Esto hace que la ciberseguridad en las empresas sea un tema candente en la sociedad y, por tanto, deba ser un tema relevante en el ámbito científico. Por este motivo, este artículo realiza un estudio bibliométrico, a través de la herramienta Bibliometrix, que busca analizar los artículos publicados sobre esta temática, sus fuentes de publicación, sus autores y sus contenidos, señalando el impacto de estos artículos en el campo investigativo y la tendencia investigativa de estos. Estudio que confirma la relevancia investigativa de esta temática en el ámbito científico global y que condiciona sus investigaciones a las nuevas tecnologías o herramientas tecnológicas que van apareciendo, y a la aparición de nuevas formas de ataques cibernéticos. Aunque hay que señalar que toda esta investigación tiene más acogida en las revistas científicas de las áreas de Ciencias de la Computación y de Ingeniería, que en revistas científicas del área de Empresas, Gestión y Contabilidad.

ABSTRACT. Cyber attacks on companies have been increasing in recent years and their effects can extend, not only to the companies that suffer them, but can affect the national security of a country or be decisive in times of conflict or war. This makes cybersecurity in companies a hot topic in society and, therefore, it must be a relevant topic in the scientific field. For this reason, this article carries out a bibliometric study, through the Bibliometrix tool, which seeks to analyze the articles published on this topic, their publication sources, their authors and their contents, pointing out the impact of these articles in the research field and their investigative tendency. Study that confirms the investigative relevance of this topic in the global scientific field and that conditions its research to the new technologies or technological tools that appear, and to the appearance of new forms of cyber attacks. Although it should be noted that all this research is more popular in scientific journals in the areas of Computer Science and Engineering than in scientific journals in the area of Business, Management and Accounting.

PALABRAS CLAVE: Ciberseguridad, Empresas, Estudio bibliométrico, TIC.

KEYWORDS: Cybersecurity, Companies, Bibliometric study, ICT.

Luján-Salamanca, A.; Infante-Moro, A.; Infante-Moro, J. C.; Gallardo-Pérez, G. (2024). La ciberseguridad en las empresas: estudio bibliométrico. *Revista de Pensamiento Estratégico y Seguridad CISDE*, 9(2), 61-73. https://doi.org/10.54988/cisde.2024.2.1551

1. Introducción

Los ataques cibernéticos a las empresas no solo afectan a la empresas que lo reciben, ya que los efectos de estos ataques pueden llegar a suponer un ataque a la seguridad nacional de un país o ser decisivos en época de conflicto o guerra, afectando a infraestructuras críticas en el funcionamiento de un país o desestabilizando su economía y su sociedad.

Por ambos motivos, la ciberseguridad en las empresas es una temática que merecía ser estudiada en profundidad a través de un estudio bibliométrico que permitiera reflejar la relevancia de esta área en el ámbito científico, identificando y analizando los artículos publicados, las fuentes de publicación, los autores y el contenido, y señalando el impacto de estos artículos en el campo investigativo, lo que permitiría tener una ligera idea de cuál es el impacto de esta área en el mundo científico, dónde se está produciendo y cuál es su tendencia investigativa.

Para ello, en este estudio bibliométrico, se analizaron 1282 artículos que fueron publicados entre 2002 y 2023 y cuya temática trascendía al área de la ciberseguridad en las empresas, artículos que pertenecían a revistas científicas indexadas en la base de datos Scopus entre esas fechas, lo que les otorgaba una calidad y relevancia suficiente para ser tenidos en cuenta en el ámbito científico.

En la siguiente sección se contextualizó los delitos cibernéticos que sufren las empresas, la ciberseguridad en las empresas y el rol de la ciberseguridad en las empresas dentro la seguridad nacional de un país. Se continuó con el desarrollo de cómo se seleccionaron los artículos que formaron parte del estudio bibliométrico y cuál fue la herramienta utilizada, se presentaron los resultados a través de tablas y gráficos, y se concluyó señalando si realmente esta temática es relevante en el ámbito científico o no, y cuál es su tendencia investigativa.

2. Revisión literaria

Entre las últimas estadísticas sobre delitos cibernéticos se encuentran las siguientes (Kolesnikov, 2024):

- En el año 2022, las empresas a nivel mundial reportaron la detección de aproximadamente 493,33 millones de incidentes de ransomware (software malicioso que cifra archivos o bloquea el acceso a sistemas informáticos para exigir un rescate).
- El phishing (ciberataque en el que los delincuentes se hacen pasar por entidades confiables para engañar a personas/empresas y obtener información personal o confidencial) se mantuvo como el método de ataque cibernético más frecuente, con alrededor de 3.400 millones de correos electrónicos no deseados enviados diariamente.
- El promedio global de pérdidas por violaciones de datos alcanzó los 4,35 millones de dólares en 2022.
- El costo promedio de las brechas de seguridad derivadas de credenciales comprometidas o robadas fue de 4,50 millones de dólares en el mismo año.
- Y el sector de la salud se posicionó como el más afectado por filtraciones de datos durante 12 años consecutivos, con un costo promedio de filtración de datos que alcanzó los 10,10 millones de dólares en 2022.

Estas estadísticas convierten a la ciberseguridad en un problema serio dentro de las empresas e instituciones.

2.1. La ciberseguridad en las empresas

A día de hoy las empresas dependen cada vez más de las tecnologías para llevar a cabo toda su operativa (Zhao, Chen, Yuan, Yu, & Zhang, 2024; Infante-Moro et al., 2024; Rodríguez Pavón et al., 2024; Pla-García, Roman-Coy & Serradell-Lopez, 2024; Nguyen et al., 2024; Campos-Dávila et al, 2024; Estepa Maestre, Gutiérrez Sánchez & Vallejo Andrada, 2024; Lyulyov et al., 2024; Wang & He, 2024), por lo que proteger activos críticos ante posibles ataques cibernéticos, hacer una gestión proactiva de riesgos cibernéticos y

fomentar una cultura de ciberdefensa se ha vuelto esencial para garantizar la resistencia de las empresas a las amenazas cibernéticas.

- Protección de activos críticos ante posibles ataques cibernéticos. Las empresas deben identificar las amenazas potenciales que podrían afectar a sus activos críticos (datos confidenciales, propiedad intelectual, sistemas, procesos,…) y protegerse con la implementación de medidas de seguridad adecuadas para mitigar los riesgos (Kure, Islam & Mouratidis, 2022; Loonam, Zwiegelaar, Kumar & Booth, 2020).
- Gestión proactiva de riesgos cibernéticos. Las empresas deben analizar constantemente las posibles brechas de ciberseguridad y desarrollar estrategias para gestionar y mitigar sus posibles riesgos de una manera efectiva. Este proceso reduciría la probabilidad de ataques cibernéticos exitosos (Mattord, Kotwica, Whitman & Battaglia, 2023; Trim & Lee, 2022).
- Fomento de una cultura de ciberdefensa. Las amenazas cibernéticas suelen aprovechar en muchas ocasiones la falta de conciencia de los empleados y la negligencia de estos mismos para llevar a cabo sus ataques, por lo que una formación sobre ciberseguridad a estos empleados y la implementación de políticas de seguridad coherentes ayudaría de manera efectiva a reducir posibles ataques (Mijwil, Unogwu, Filali, Bala & Al-Shahwani, 2023; Infante-Moro, Infante-Moro & Gallardo-Pérez, 2022).

Y esto de la ciberseguridad no se queda solo en exigencias a nivel corporativo, ya que la seguridad exigida a nivel nacional e internacional implica cumplir con normativas y regulaciones globales que desempeñan un papel crucial en la ciberseguridad empresarial (Melaku, 2023; Djebbar & Nordström, 2023).

Algunos ejemplos de estas, si se actúan en sus respectivos mercados, pueden ser el Reglamento General de Protección de Datos (GDPR) de la Unión Europea o la Ley de Ciberseguridad de China.

Además, la cooperación y colaboración internacional son fundamentales para abordar las amenazas cibernéticas que trascienden las fronteras nacionales, intercambiando información sobre amenazas, colaborando con otras organizaciones y apoyando iniciativas internacionales para fortalecer la ciberseguridad a nivel internacional. Esto incluye compartir buenas prácticas, participar en ejercicios de simulación conjuntos y contribuir a la formulación de políticas internacionales de ciberseguridad (Flegontova, 2017; Park, 2016).

Por tanto, la ciberseguridad en las empresas debe abarcar a toda la empresa y plantearse como una cuestión estratégica, ya que es clave para la supervivencia y el éxito empresarial.

2.2. El rol de la ciberseguridad en las empresas dentro la seguridad nacional de un país

En la actual era digital, donde la mayoría de las actividades económicas, gubernamentales y militares dependen de las tecnologías, las amenazas cibernéticas pueden tener un alto impacto en la seguridad nacional de un país, de ahí la relevancia de la ciberseguridad en todos estos ámbitos (Aviv & Ferri, 2023; Ayala-Mora, Infante-Moro & Infante-Moro, 2023; Morales, Fletscher Bocanegra & Botero Vega, 2023; García-Río, Baena-Luna, Palos-Sánchez & Aguayo-Camacho, 2022).

En las empresas, la capacidad de protegerse contra ataques cibernéticos y de responder de manera efectiva ante estos cuando se producen se ha convertido en un elemento fundamental de preparación, ya que estos pueden actuar de una manera letal y acabar con estas de una manera rápida. Pero estos ataques, no solo podrían afectar a estas empresas, sino que también podrían llegar a afectar la seguridad nacional de un país.

Los ataques cibernéticos a empresas podrían llegar a afectar a la seguridad nacional de un país de las siguientes maneras:

- Dañando infraestructuras críticas: Un ataque cibernético contra empresas que gestionan sistema y servicios como la energía, el transporte, las finanzas y las comunicaciones, podría afectar al funcionamiento

de un país interrumpiendo servicios esenciales y afectando a la estabilidad nacional (Roshanaei, 2023; Mouratidis, Islam, Santos-Olmo, Sanchez & Ismail, 2023).

- Robando información sensible: Un ataque cibernético sobre una empresa que comprometa información sensible que esta almacene (secretos comerciales, información confidencial del gobierno, información financiera, información de propiedad intelectual, datos personales de ciudadanos,…) podría afectar a la seguridad nacional de un país (Mourtzis, Angelopoulos & Panopoulos, 2023; Mijwil, Unogwu, Filali, Bala & Al-Shahwani, 2023; Ferreira, Silva & Itzazelaia, 2023).

- Provocando un impacto económico: Los ataques cibernéticos sobre empresas podrían causar pérdidas económicas significativas a las empresas afectadas, y por ende debilitar la economía y la estabilidad financiera de un país (Grimwade, 2023; Smith, Smith, Burger & Boyle, 2023; Holovkin, Cherniavskyi & Tavolzhanskyi, 2023).

- Desestabilizando a la sociedad: Los ataques cibernéticos a empresas podrían generar descontento social y afectar a la confianza pública en las instituciones y en la seguridad general, afectando a la cohesión y seguridad nacional de un país (Al-Kumaim & Alshamsi, 2023; Carvalho, Carvalho, Silva, Casquilho & Santos, 2023; Carvalho, Carvalho, Silva, Santos & Bandeira, 2023).

En resumen, los ataques cibernéticos a empresas podrían tener consecuencias que trascienden el ámbito corporativo y afectar directamente a la seguridad nacional de un país.

3. Metodología

La herramienta que se utilizó para desarrollar este estudio bibliométrico es Bibliometrix, un software desarrollado en lenguaje R que permite el análisis cuantitativo de la producción científica y su visualización (Padilla Mesa, 2019).

La base de datos que se utilizó fue Scopus, una base de datos que por los criterios de indexación que aplica a sus revistas asegura una calidad y relevancia en los artículos que en ella se encuentran (Scopus, s.f.), y la consulta final realizada fue:

(TITLE-ABS-KEY (cybersecurity) OR TITLE-ABS-KEY (cyberterrorism) AND TITLE-ABS-KEY (business) OR TITLE-ABS-KEY (company) OR TITLE-ABS-KEY (companies)) AND PUBYEAR > 2001 AND PUBYEAR < 2024 AND (LIMIT-TO (SRCTYPE , "j")) AND (EXCLUDE (DOCTYPE , "ed") OR EXCLUDE (DOCTYPE , "no") OR EXCLUDE (DOCTYPE , "sh") OR EXCLUDE (DOCTYPE , "tb") OR EXCLUDE (DOCTYPE , "dp") OR EXCLUDE (DOCTYPE , "er") OR EXCLUDE (DOCTYPE , "cp"))

Primero se hizo una búsqueda previa con las siguientes palabras clave: (“cybersecurity” o "cyberterrorism") y (“business” o “company” o “companies”), y excluyendo los resultados de 2024 (ya que en este análisis solo se pretendía cubrir años completos), lo que arrojó un resultado de 3923 artículos. Y a este resultado se le hizo una criba para que solo quedaran artículos y revisiones literarias pertenecientes a revistas científicas (lo que aseguraría una mayor calidad y relevancia de los artículos analizados debido a las fuertes criterios exigidos por Scopus a este tipo de fuentes), quedando un total de 1294 artículos.

Posteriormente se hizo una revisión del contenido de los artículos (para eliminar todo artículo que no estuviera relacionado con la temática) y se eliminaron 12 artículos, siendo el resultado final de 1282 artículos.

Estos artículos fueron los que finalmente se procesaron a través del software Bibliometrix, y un resumen de esta información bibliográfica finalmente utilizada en este estudio bibliométrico se encuentra en la Tabla 1.

Descripción	Resultados
INFORMACIÓN PRINCIPAL SOBRE DATOS	
Espacio de tiempo	2002:2023
Fuentes	671
Documentos	1282
Media por año de publicaciones	3,29
Media de citas por documentos	14,44
CONTENIDO DEL DOCUMENTO	
Palabras clave de la base de datos	4857
Palabras clave del autor	3754
AUTORES	
Autores	3797
Autores de documentos de un solo autor	216
COLABORACIÓN DE AUTORES	
Documentos de un solo autor	231
Coautores por documento	3,32
Coautorías internacionales %	25,12
TIPOS DE DOCUMENTOS	
Artículos	1160
Revisiones literarias	122

Tabla 1. Resumen de información bibliográfica. Fuente: Elaboración propia.

4. Resultados

El número de artículos publicados a lo largo de estos años muestra un interés casi testimonial hasta 2011, pero esta situación cambia a partir de 2017 cuando el número de artículos que se publican sobre esta temática crece de manera vertiginosa año a año, siendo el número de artículos publicados a partir de ese año el 93,14% de los artículos publicados sobre esta temática en esta base se datos (Figura 1).

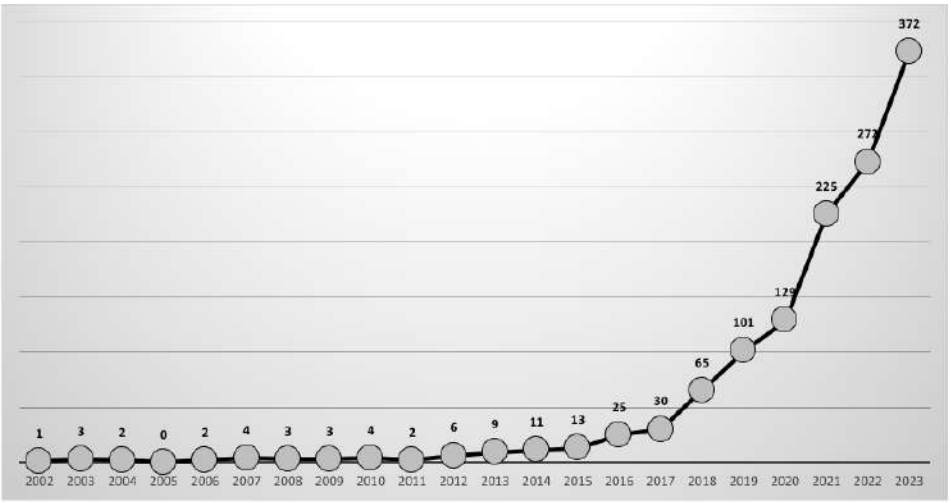

Figura 1. Evolución anual de las publicaciones. Fuente: Elaboración propia.

Y las principales fuentes de publicación fueron las que se pueden observar en la Figura 2, aunque realmente se publicaron en 671 revistas. Las 15 revistas que se pueden observar en esta figura acogieron el 22,93% de las publicaciones, destacando las revistas IEEE Access, Computers and Security, Sensors, Applied Sciences (Switzerland) y Issues in Information Systems, con 44, 34, 27, 25 y 25 artículos, respectivamente.

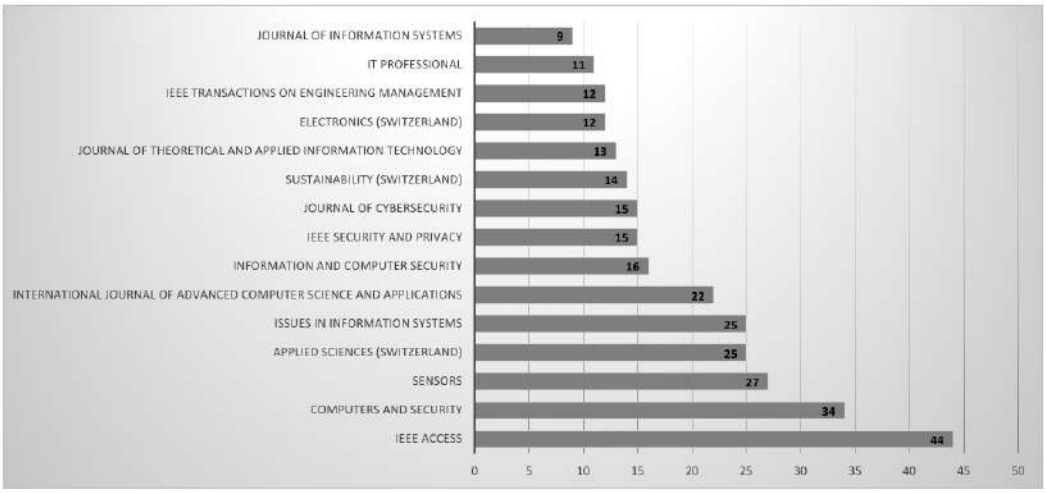

Figura 2. Fuentes con mayor número de publicaciones relacionadas. Fuente: Elaboración propia.

Esas 5 revistas que fueron las que más artículos publicaron sobre esta temática, comenzaron a publicarlos a partir de 2016, 2018, 2019 y 2021 (Figura 3). IEEE Access y Computers and Security, que son las revistas que más artículos publicaron, comenzaron a publicarlos en 2016. Y Sensors, que es la tercera revista con más artículos publicados sobre esta temática, comenzó a publicarlos en 2021.

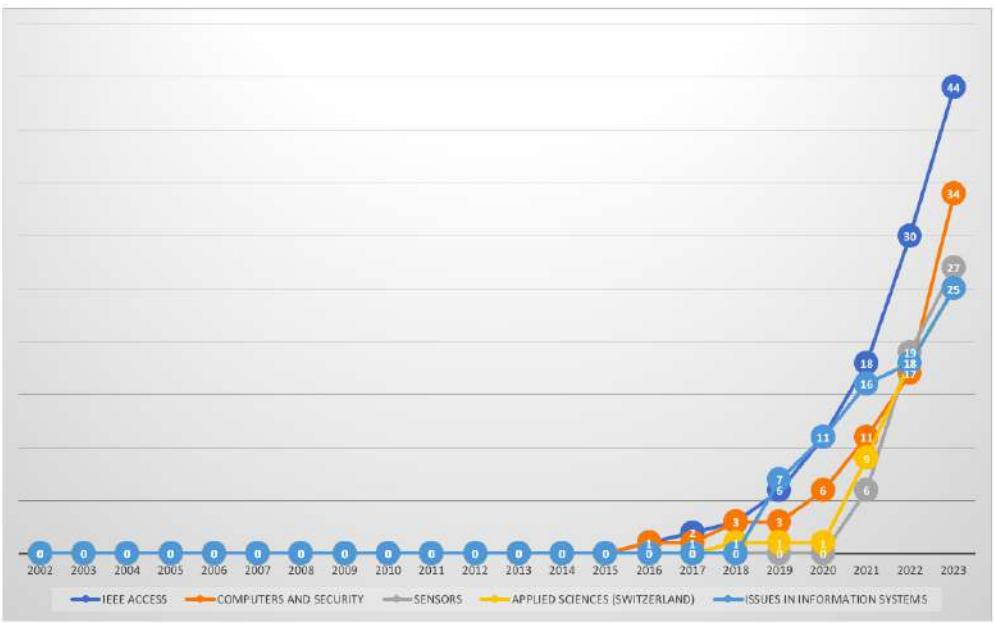

Figura 3. Producción de las principales fuentes de producción a lo largo del tiempo. Fuente: Elaboración propia.

El factor de impacto de las principales fuentes de publicación se puede observar en la Tabla 2, donde 4 de las 5 principales fuentes de producción se encuentran entre las 5 con mayor factor de impacto, solo Issues in Information Systems sale de esta lista, ya que se encuentra en el número 22.

Luján-Salamanca, A.; Infante-Moro, A.; Infante-Moro, J. C.; Gallardo-Pérez, G. (2024). La ciberseguridad en las empresas: estudio bibliométrico. *Revista de Pensamiento Estratégico y Seguridad CISDE*, 9(2), 61-73. https://doi.org/10.54988/cisde.2024.2.1551

Nombre de la revista	h_index	g_index	m_index	TC	NP	Inicio
COMPUTERS AND SECURITY	13	28	1,444	804	33	2016
IEEE ACCESS	13	26	1,444	732	44	2016
APPLIED SCIENCES (SWITZERLAND)	10	17	1,429	297	25	2018
IEEE SECURITY AND PRIVACY	7	13	0,318	169	15	2003
SENSORS	7	14	1,75	223	27	2021
COMPUTERS IN INDUSTRY	6	6	0,667	859	6	2016
IEEE TRANSACTIONS ON ENGINEERING MANAGEMENT	6	10	1,2	118	11	2020
IT PROFESSIONAL	6	11	0,333	169	11	2007
JOURNAL OF CYBERSECURITY	6	12	0,75	157	15	2017
SUSTAINABILITY (SWITZERLAND)	6	11	0,75	129	13	2017
TECHNOLOGICAL FORECASTING AND SOCIAL CHANGE	6	8	1,2	230	8	2020
BUSINESS HORIZONS	5	7	0,385	150	7	2012
ELECTRONICS (SWITZERLAND)	5	12	0,714	270	12	2018
INFORMATION AND COMPUTER SECURITY	5	10	0,833	111	15	2019
INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS	5	7	0,714	81	21	2018

Tabla 2. Principales fuentes de publicación en función a su factor de impacto. Fuente: Elaboración propia.

Respecto a los autores de estas publicaciones, son un total de 3797 autores, donde los 10 principales autores por número de publicaciones se pueden observar en la Figura 4. N. Kshetri es el autor con más publicaciones relacionadas y pertenece a la The University of North Carolina en Greensboro (Estados Unidos).

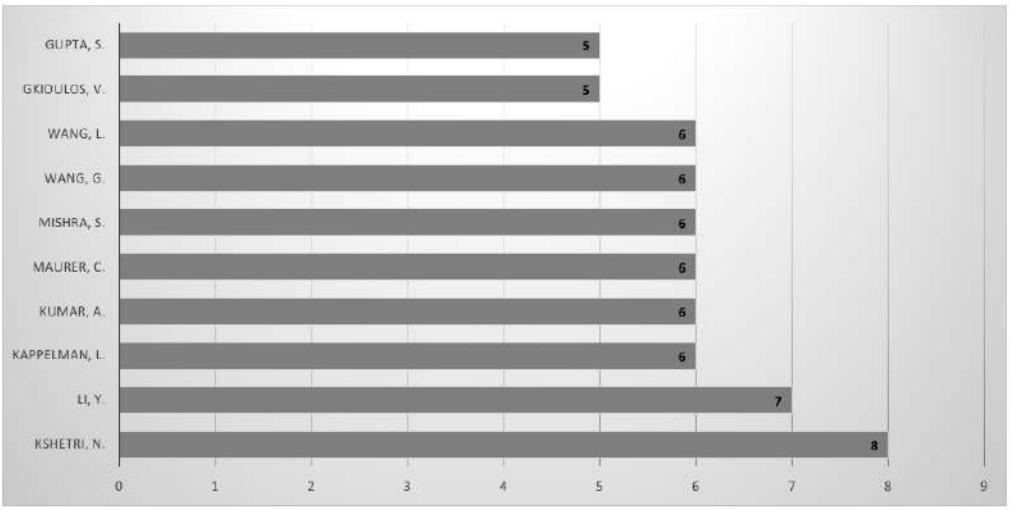

Figura 4. Autores con mayor número de publicaciones relacionadas. Fuente: Elaboración propia.

Los autores con mayor factor de impacto se pueden observar en la Tabla 3, donde 5 de los 10 autores con más publicaciones relacionadas se encuentran entre los 10 autores con mayor factor impacto. En esta lista, el autor con mayor número de publicaciones es el autor con mayor factor de impacto, aunque no es el autor más citado (ya que el autor más citado es I. H. Sarker, de la Swinburne University of Technology en Australia, con 1316 citas).

Autor	h_index	g_index	m_index	TC	NP	Inicio
Kshetri, N	5	8	0,417	131	8	2013
Maurer, C.	5	6	0,714	238	6	2018
Corallo, A.	4	4	0,571	453	4	2018
Gupta, S.	4	5	0,8	219	5	2020
Islam, S.	4	5	0,571	139	5	2018
Kappelman, L.	4	6	0,571	207	6	2018
Kim, K.	4	5	0,571	81	5	2018
Kumar, A.	4	6	0,8	66	6	2020
Lazoi, M.	4	4	0,571	453	4	2018
Lezzi, M.	4	4	0,571	453	4	2018

Tabla 3. Autores con mayor factor de impacto. Fuente: Elaboración propia.

Los autores de todos estos artículos pertenecen a 94 países diferentes, Estados Unidos es el país que más autores aporta en estos artículos (aparecen en el 51,64% del total de artículos, 662 de 1282 artículos), Reino Unido en el 16,30% (209 de 1282 artículos), India en el 14,51% (186 de 1282 artículos), China en el 12,48% (160 de 1282 artículos) y Arabia Saudí en el 11,31% (145 de 1282 artículos). España se sitúa en séptimo lugar con un 7,25% (93 de 1282 artículos) (Figure 5):

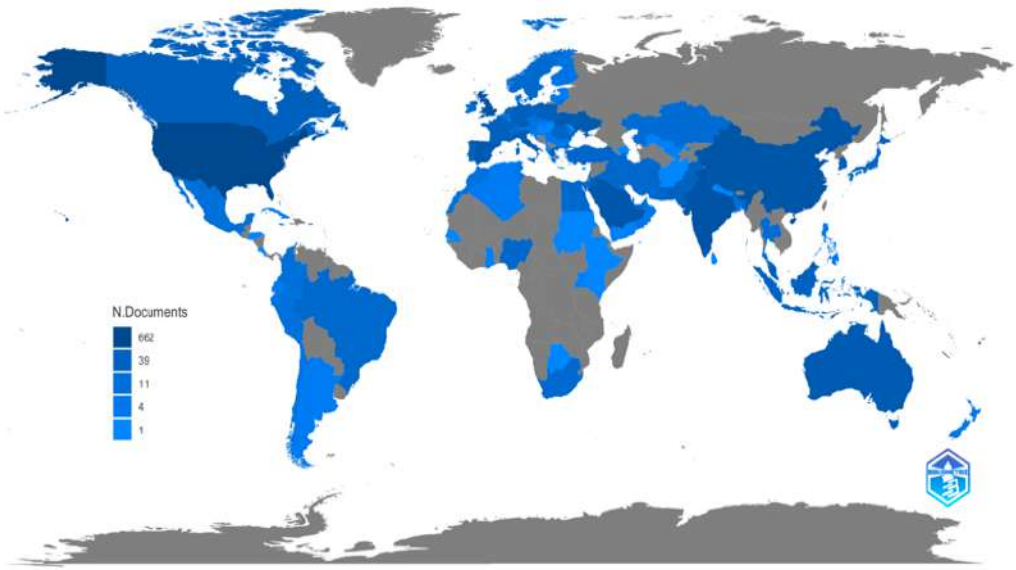

Figura 5. Producción científica por países. Fuente: Elaboración propia.

Y las colaboraciones entre autores de diferentes países son múltiples (804 colaboraciones) (Figura 6), produciéndose las mayores colaboraciones entre Estados Unidos - China (16 colaboraciones), Estados Unidos - India (15 colaboraciones), India - Arabia Saudí (11 colaboraciones), Arabia Saudí - Pakistán (11 colaboraciones) y Estados Unidos - Arabia Saudí (11 colaboraciones).

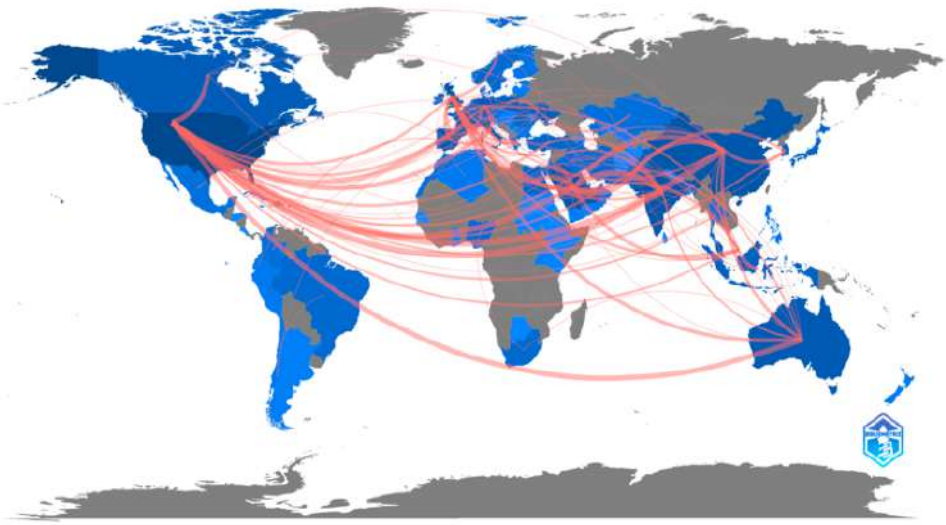

Figura 6. Mapa mundial de colaboraciones entre países. Fuente: Elaboración propia.

En los 1282 artículos, las palabras claves más predominantes son (Figura 7): cyber security (378 veces), cybersecurity (347 veces), network security (209 veces), computer crime (112 veces), internet of things (95 veces), risk assessment (92 veces), security of data (91 veces), computer security (85 veces), crime (81 veces) y cyber-attacks (72 veces).

Figura 7. Nube de palabras clave más utilizadas. Fuente: Elaboración propia.

Aunque la tendencia de estas palabras ha ido cambiando a lo largo de estos años en función a la temática investigativa de cada periodo, como se puede observar en la Tabla 4. En esta tabla se ha reseñado las palabras clave más utilizadas hasta antes de que comenzara a crecer de manera más incrementada el número de publicaciones sobre esta temática (a partir de 2017), las palabras clave desde ese periodo hasta 2022 y las palabras clave de cada uno de los dos últimos años analizados.

2002-2017	2018-2021	2022-2022	2023-2023
resilience	cybersecurity	cyber security	digitalization
cloud computing	industry 4.0	cybersecurity	cyber security
security	risk management	cyber-attacks	cybersecurity
cybersecurity	machine learning	digital transformation	information security
cybercrime		cyber risks	covid-19
		digitalization	ransomware
		information security	machine learning

Tabla 4. Palabras clave más utilizadas en función al periodo. Fuente: Elaboración propia.

Por último, destacar que los 10 artículos más citados sobre esta temática se encuentran en la Tabla 5, el número total de citas que recibieron los artículos relacionados con la ciberseguridad en las empresas fue de 18506 citas en Scopus.

Artículo	DOI	Citas	Citas por año
SARKER IH, 2021, SN COMPUT SCI	10.1007/s42979-021-00592-x	1220	305,00
NG ICL, 2017, INT J RES MARK	10.1016/j.ijresmar.2016.11.003	411	51,38
BABICEANU RF, 2016, COMPUT IND	10.1016/j.compind.2016.02.004	386	42,89
WESTERLUND M, 2019, TECHNOLOG INNOV MANAG REV	10.22215/TIMREVIEW/1282	348	58,00
ABESHU A, 2018, IEEE COMMUN MAG	10.1109/MCOM.2018.1700332	269	38,43
NISHANT R, 2020, INT J INF MANAGE	10.1016/j.ijinfomgt.2020.102104	266	53,20
YANG H, 2019, IISE TRANS	10.1080/24725854.2018.1555383	254	42,33
AL-RIMY BAS, 2018, COMPUT SECUR	10.1016/j.cose.2018.01.001	236	33,71
LEZZI M, 2018, COMPUT IND	10.1016/j.compind.2018.09.004	222	31,71
FRAGA-LAMAS P, 2019, IEEE ACCESS	10.1109/ACCESS.2019.2895302	220	36,67

Tabla 5. Artículos más citados. Fuente: Elaboración propia.

El artículo más citado (Sarker, 2021), Machine learning: Algorithms, real-world applications and research directions, examina el papel crucial del aprendizaje automático en la era de la Cuarta Revolución Industrial, destacando algoritmos y aplicaciones en áreas como ciberseguridad, ciudades inteligentes, salud y comercio electrónico, además de señalar desafíos y futuras direcciones de investigación.

El segundo artículo más citado (Ng & Wakenshaw, 2017), The Internet-of-Things: Review and research directions, revisa el Internet de las Cosas (IoT) a través de diferentes enfoques conceptuales y propone una definición junto con implicaciones para la investigación futura en áreas como marketing, sistemas de información, diseño, ciencia de datos, ciberseguridad, estudios organizacionales y economía.

El tercer artículo más citado (Babiceanu & Seker, 2016), Big Data and virtualization for manufacturing cyber-physical systems: A survey of the current status and future outlook, examina la integración del Big Data y la virtualización en los sistemas ciberfísicos de manufactura, destacando la necesidad de la seguridad cibernética. Propone un marco para el desarrollo de sistemas predictivos de manufactura ciberfísica con capacidades IoT, procesamiento de eventos y análisis algorítmico de Big Data.

El cuarto artículo más citado (Westerlund, 2019), The Emergence of Deepfake Technology: A Review, examina la aparición de la tecnología deepfake, analizando su impacto en la sociedad, la política y los negocios. Proporciona recomendaciones para combatir las amenazas que representa, destacando la importancia de la legislación, la educación y el desarrollo tecnológico en la detección y prevención de deepfakes.

El quinto artículo más citado (Abeshu & Chilamkurti, 2018), Deep Learning: The Frontier for Distributed Attack Detection in Fog-to-Things Computing, presenta un enfoque innovador utilizando Deep Learning para la detección distribuida de ataques en Fog-to-Things Computing. Destaca la necesidad de controles de ciberseguridad distribuidos en el borde de la red y demuestra la superioridad de los modelos profundos en precisión y escalabilidad para la detección de ataques cibernéticos en entornos distribuidos.

El sexto artículo más citado (Nishant, Kennedy & Corbett, 2020), Artificial intelligence for sustainability: Challenges, opportunities, and a research agenda, explora el potencial del aprendizaje profundo en la inteligencia artificial para abordar desafíos de sostenibilidad. Destaca la necesidad de enfoques interdisciplinarios para mitigar riesgos y maximizar beneficios en la aplicación de la inteligencia artificial en la gestión ambiental y propone una agenda de investigación para avanzar en este campo.

El séptimo artículo más citado (Yang, Kumara, Bukkapatnam & Tsung, 2019), The internet of things for smart manufacturing: A review, revisa el papel fundamental del Internet de las Cosas (IoT) en la manufactura inteligente, destacando su impacto en la eficiencia de la producción, la seguridad cibernética y la innovación. Propone un marco para el desarrollo de sistemas ciberfísicos en la manufactura y señala desafíos y oportunidades futuras.

El octavo artículo más citado (Al-Rimy, Maarof, & Shaid, 2018), Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions, examina el ransomware, destacando su creciente amenaza y los desafíos asociados con la detección y prevención. Proporciona una taxonomía de ransomware y revisa investigaciones sobre contramedidas, incluyendo análisis, prevención, detección y predicción, además de señalar direcciones futuras de investigación.

El noveno artículo más citado (Lezzi, Lazoi & Corallo, 2018), Cybersecurity for Industry 4.0 in the current literature: A reference framework, propone un marco de referencia para analizar la ciberseguridad en el contexto de la Industria 4.0, mediante una revisión sistemática de la literatura. Examina elementos como activos, vulnerabilidades, amenazas y contramedidas, ofreciendo una guía para futuras investigaciones y aplicaciones en este campo.

Y el décimo artículo más citado (Fraga-Lamas & Fernández-Caramés, 2019), A Review on Blockchain

Technologies for an Advanced and Cyber-Resilient Automotive Industry, revisa el potencial de las tecnologías blockchain en la industria automotriz, destacando su capacidad para mejorar la seguridad cibernética y la eficiencia operativa. Analiza desafíos actuales, casos de uso relevantes y recomienda acciones para futuros desarrollos en la industria automotriz resiliente a ciberataques.

5. Conclusiones

Tras el estudio bibliométrico queda constancia que la ciberseguridad en las empresas es una temática en auge dentro del ámbito científico desde 2017, fecha a partir de la cual el número de publicaciones anuales relacionadas comenzó a aumentar año a año hasta llegar en 2023 a multiplicar por 10 el número de publicaciones de 2017.

La gama de revistas que publican artículos sobre esta temática es muy amplia, destacando las revistas de las áreas de Ciencias de la Computación y de Ingeniería, y en muy menor medida las de las áreas de Ciencias Sociales y de Empresas, Gestión y Contabilidad. Este hecho resulta insólito debido a la importancia que tienen hoy día las tecnologías y la ciberseguridad en las empresas.

Y el disperso origen de los autores señala la preocupación de la ciberseguridad en las empresas a nivel mundial (exceptuando algunas regiones de África, hecho que se debe más a la ausencia de publicaciones de autores de esos países que a su interés), un problema que añade muchas colaboraciones a nivel global ya que son los mismos problemas de ciberseguridad para todas las empresas del mundo.

Respecto al impacto de los artículos publicados sobre esta temática, hay que decir que el número de citas de estos es bastante alto, alcanzando los 1282 artículos un total de 18506 citas, un índice h de 60 y un índice i10 de 370, por lo que el interés del ámbito científico en estas investigaciones queda patente con estos datos.

Pero esta temática no cierra su camino con este número de investigaciones, ya que es una temática en constante evolución por los nuevos riesgos que atrae la evolución de las tecnologías y la aparición de nuevas formas de ataques cibernéticos, algo que se puede observar en la evolución de las palabras clave a lo largo de estos años (que no se han mantenido constantes, sino que han sido cambiantes). Hay palabras que se han repetido a lo largo de los años, pero hay otras que van apareciendo por los nuevos problemas a los que se enfrentan las empresas (ransomware, phishing, machine learning, artificial intelligence, blockchain e industry 4.0, entre otras). Por tanto, el futuro de estas investigaciones, irá siempre de la mano de la evolución de los ataques cibernéticos y de la evolución de las tecnologías.

Financiación

Esta investigación no recibió financiación externa.

Cómo citar este artículo / How to cite this paper

Luján-Salamanca, A.; Infante-Moro, A.; Infante-Moro, J. C.; Gallardo-Pérez, G. (2024). La ciberseguridad en las empresas: estudio bibliométrico. *Revista de Pensamiento Estratégico y Seguridad CISDE*, 9(2), 61-73. https://doi.org/10.54988/cisde.2024.2.1551

Referencias

Abeshu, A.; Chilamkurti, N. (2018). Deep learning: The frontier for distributed attack detection in fog-to-things computing. IEEE Communications Magazine, 56(2), 169-175. https://doi.org/10.1109/MCOM.2018.1700332.

Al-Kumaim, N. H.; Alshamsi, S. K. (2023). Determinants of cyberattack prevention in UAE financial organizations: assessing the mediating role of cybersecurity leadership. Applied Sciences, 13(10), 5839. https://doi.org/10.3390/app13105839.

Al-Rimy, B. A. S.; Maarof, M. A.; Shaid, S. Z. M. (2018). Ransomware threat success factors, taxonomy, and countermeasures: A

survey and research directions. Computers & Security, 74, 144-166. https://doi.org/10.1016/j.cose.2018.01.001.
Aviv, I.; Ferri, U. (2023). Russian-Ukraine armed conflict: Lessons learned on the digital ecosystem. International Journal of Critical Infrastructure Protection, 43, 100637. https://doi.org/10.1016/j.ijcip.2023.100637.
Ayala-Mora, J.; Infante-Moro, A.; Infante-Moro, J. C. (2023). Electronic administration in the Council of the Judiciary of Ecuador [La administración electrónica en el Consejo de la Judicatura de Ecuador]. RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao, (E60), 511-523.
Babiceanu, R. F.; Seker, R. (2016). Big Data and virtualization for manufacturing cyber-physical systems: A survey of the current status and future outlook. Computers in industry, 81, 128-137. https://doi.org/10.1016/j.compind.2016.02.004.
Campos-Dávila, J. E.; Choque-Yarasca, C. L.; Olmos, S. D.; Uribe Hernández, Y. C. (2024). Estrategias de transformación digital en empresas tradicionales. Revista Venezolana de Gerencia, 29(105), 289-302. https://doi.org/10.52080/rvgluz.29.105.19.
Carvalho, S.; Carvalho, J. V.; Silva, J. C.; Casquilho, M.; Santos, G. (2023). The use of ICT in today's society from the perspective of citizens and businesses: security risks and their influence on the quality of life of the portuguese population. International Journal for Quality Research, 17(3), 795-814. https://doi.org/10.24874/IJQR17.03-11.
Carvalho, S.; Carvalho, J. V.; Silva, J. C.; Santos, G.; Bandeira, G. S. (2023). Concerns about Cybersecurity: The Implications of the use of ICT for Citizens and Companies. Journal of Information Systems Engineering and Management, 8(2), 20713. https://doi.org/10.55267/iadt.07.13226.
Djebbar, F.; Nordström, K. (2023). A Comparative Analysis of Industrial Cybersecurity Standards. IEEE Access, 11, 85315-85332. https://doi.org/10.1109/ACCESS.2023.3303205.
Estepa Maestre, F.; Gutiérrez Sánchez, J. D.; Vallejo Andrada, A. (2024). Herramientas cualitativas y TICs en la enseñanza universitaria: una experiencia desde las Ciencias Sociales. Campus Virtuales, 13(1), 35-46. https://doi.org/10.54988/cv.2024.1.1137.
Ferreira, L.; Silva, D. C.; Itzazelaia, M. U. (2023). Recommender systems in cybersecurity. Knowledge and Information Systems, 65(12), 5523-5559. https://doi.org/10.1007/s10115-023-01906-6.
Flegontova, T. (2017). E-commerce Regulation in China: Risks and Opportunities for International Cooperation. Vestnik Mezhdunarodnykh Organizatsii-International Organisations Research Journal, 12(4), 150-168.
Fraga-Lamas, P.; Fernández-Caramés, T. M. (2019). A review on blockchain technologies for an advanced and cyber-resilient automotive industry. IEEE access, 7, 17578-17598. https://doi.org/10.1109/ACCESS.2019.2895302.
García-Río, E.; Baena-Luna, P.; Palos-Sánchez, P. R.; Aguayo-Camacho, M. (2022). Amenazas de los gobiernos electrónicos: el desafío de la e-seguridad. Revista de Pensamiento Estratégico y Seguridad CISDE, 7(2), 87-107.
Grimwade, M. (2023). The potential impacts of the digital revolution on the operational risk profiles of banks. Journal of Risk Management in Financial Institutions, 17(1), 71-88.
Holovkin, B.; Cherniavskyi, S.; Tavolzhanskyi, O. (2023). Factors of cybercrime in Ukraine. Relações Internacionais no Mundo Atual, 3(41), 464-488. https://doi.org/10.21902/Revrima.v3i41.6401.
Infante-Moro, A.; Infante-Moro, J. C.; Gallardo-Pérez, J. (2022). Factores claves para concienciar la ciberseguridad en los empleados. Revista de pensamiento estratégico y seguridad CISDE, 7(1), 69-79.
Infante-Moro, A.; Infante-Moro, J. C.; Gallardo-Pérez, J.; Nguyen, T. L. (2024). Aspects to be taken into account by teachers for the correct use of Moodle as a support tool for face-to-face teaching. Campus Virtuales, 13(2), 215-224. https://doi.org/10.54988/cv.2024.2.1587.
Kolesnikov, N. (2024). 50 Estadísticas Clave de Ciberseguridad para Marzo de 2024. (https://www.techopedia.com/es/estadisticas-ciberseguridad).
Kure, H. I.; Islam, S.; Mouratidis, H. (2022). An integrated cyber security risk management framework and risk predication for the critical infrastructure protection. Neural Computing and Applications, 34(18), 15241-15271. https://doi.org/10.1007/s00521-022-06959-2.
Lezzi, M.; Lazoi, M.; Corallo, A. (2018). Cybersecurity for Industry 4.0 in the current literature: A reference framework. Computers in Industry, 103, 97-110. https://doi.org/10.1016/j.compind.2018.09.004.
Lyulyov, O.; Pimonenko, T.; Infante-Moro, A.; Kwilinski, A. (2024). Perception of Artificial Intelligence: GSR Analysis and Face Detection. Virtual Economics, 7(2), 7-30. https://doi.org/10.34021/ve.2024.07.02(1).
Loonam, J.; Zwiegelaar, J.; Kumar, V.; Booth, C. (2020). Cyber-resiliency for digital enterprises: a strategic leadership perspective. IEEE Transactions on Engineering Management, 69(6), 3757-3770. https://doi.org/10.1109/TEM.2020.2996175.
Mattord, H.; Kotwica, K.; Whitman, M.; Battaglia, E. (2023). Organizational perspectives on converged security operations. Information & Computer Security. https://doi.org/10.1108/ICS-03-2023-0029.
Melaku, H. M. (2023). A dynamic and adaptive cybersecurity governance framework. Journal of Cybersecurity and Privacy, 3(3), 327-350. https://doi.org/10.3390/jcp3030017.
Mijwil, M.; Unogwu, O. J.; Filali, Y.; Bala, I.; Al-Shahwani, H. (2023). Exploring the top five evolving threats in cybersecurity: an in-depth overview. Mesopotamian journal of cybersecurity, 2023, 57-63. https://doi.org/10.58496/MJCS/2023/010.
Morales, O. M.; Fletscher Bocanegra, L. A.; Botero Vega, J. F. (2023). La Inteligencia Artificial como apoyo a la gestión de la seguridad ciudadana: un estado del arte. Revista de Pensamiento Estratégico y Seguridad CISDE, 8(2), 55-72.
Mouratidis, H.; Islam, S.; Santos-Olmo, A.; Sanchez, L. E.; Ismail, U. M. (2023). Modelling language for cyber security incident handling for critical infrastructures. Computers & Security, 128, 103139. https://doi.org/10.1016/j.cose.2023.103139.
Mourtzis, D.; Angelopoulos, J.; Panopoulos, N. (2023). Blockchain integration in the era of industrial metaverse. Applied Sciences, 13(3), 1353. https://doi.org/10.3390/app13031353.
Ng, I. C.; Wakenshaw, S. Y. (2017). The Internet-of-Things: Review and research directions. International Journal of Research in Marketing, 34(1), 3-21. https://doi.org/10.1016/j.ijresmar.2016.11.003.

Nguyen, T. L.; Infante-Moro, A.; Infante-Moro, J. C. (2024). Generation Z's followers on hotel' social networking sites: Motivational factors from a theory of planned behavior approach [Seguidores de la generación Z en los sitios de redes sociales del hotel: factores motivacionales desde el enfoque de la teoría del comportamiento planificado]. RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao, (E66), 340-354.
Nishant, R.; Kennedy, M.; Corbett, J. (2020). Artificial intelligence for sustainability: Challenges, opportunities, and a research agenda. International Journal of Information Management, 53, 102104. https://doi.org/10.1016/j.ijinfomgt.2020.102104.
Padilla Mesa, J. A. (2019). Bibliometrix: Análisis bibliométrico con RStudio. (Tesis Fin de Grado). Granada (España): Universidad de Granada.
Park, D. W. (2016). Research on Cooperation Platform for the Cybersecurity Industry World Markets. International Information Institute (Tokyo). Information, 19(11A), 4969.
Pla-García, C.; Roman-Coy, D.; Serradell-Lopez, E. (2024). Blended Learning: ¿es importante la presencialidad en programas de formación online?. Campus Virtuales, 13(1), 183-198. https://doi.org/10.54988/cv.2024.1.1442.
Rodríguez Pavón, P. R.; Morales Salas, R. E.; Infante Moro, A.; Infante Moro, J. C. (2024). The Nominal Group Technique as a tool to select items that measure the level of digital skills in postgraduate students [La Técnica de Grupo Nominal como herramienta para seleccionar ítems que miden el nivel de competencias digitales en estudiantes de posgrado]. International Journal of Educational Research and Innovation, (21), 1-17. https://doi.org/10.46661/ijeri.9393.
Roshanaei, M. (2023). Cybersecurity Preparedness of Critical Infrastructure—A National Review. Journal of Critical Infrastructure Policy, 4(1), 21-50. https://doi.org/10.18278/jcip.4.1.4.
Sarker, I. H. (2021). Machine learning: Algorithms, real-world applications and research directions. SN computer science, 2(3), 160. https://doi.org/10.1007/s42979-021-00592-x.
Scopus (s.f.). Content policy and selection. (https://www.elsevier.com/es-es/products/scopus/content/content-policy-and-selection).
Smith, K. T.; Smith, L. M.; Burger, M.; Boyle, E. S. (2023). Cyber terrorism cases and stock market valuation effects. Information & Computer Security, 31(4), 385-403. https://doi.org/10.1108/ICS-09-2022-0147.
Trim, P. R.; Lee, Y. I. (2022). Combining sociocultural intelligence with Artificial Intelligence to increase organizational cyber security provision through enhanced resilience. Big Data and Cognitive Computing, 6(4), 110. https://doi.org/10.3390/bdcc6040110.
Wang, Y.; He, Z. (2024). CEO discretion and enterprise digital transformation. Heliyon, 10(1), e23468. https://doi.org/10.1016/j.heliyon.2023.e23468.
Westerlund, M. (2019). The emergence of deepfake technology: A review. Technology innovation management review, 9(11). https://doi.org/10.22215/TIMREVIEW/1282.
Yang, H.; Kumara, S.; Bukkapatnam, S. T.; Tsung, F. (2019). The internet of things for smart manufacturing: A review. IISE transactions, 51(11), 1190-1216. https://doi.org/10.1080/24725854.2018.1555383.
Zhao, X.; Chen, Q. A.; Yuan, X.; Yu, Y.; Zhang, H. (2024). Study on the impact of digital transformation on the innovation potential based on evidence from Chinese listed companies. Scientific Reports, 14(1), 6183. https://doi.org/10.1038/s41598-024-56345-2.