



Ciberseguridad desde las ciencias de la computación: un estudio bibliométrico sobre el Perú y los países limítrofes

Cybersecurity from the perspective of computer science: a bibliometric study on Peru and neighboring countries

Paolo Víctor Cuya-Chamilco¹, Pablo Saavedra-Villar², Lizeth Erly Mescua-Ampuero¹, José Alvarado-Flores¹, Alan Armando Cáceres-García^{3*}

¹Universidad César Vallejo. Lima, Perú

²Universidad Nacional de Huancavelica. Huancavelica, Perú

³Superintendencia Nacional de Educación Superior Universitaria. Lima, Perú

Recibido: 09 Oct. 2024 | Aceptado: 27 Dic. 2024 | Publicado: 20 Ene. 2025

Autor de correspondencia*: alancaceres@sunedu.gob.pe

Cómo citar este artículo: Cuya-Chamilco, P. V., Saavedra-Villar, P., Mescua-Ampuero, L. E., Alvarado-Flores, J., & Cáceres-García, A. A. (2025). Ciberseguridad desde las ciencias de la computación: un estudio bibliométrico sobre el Perú y los países limítrofes. *Revista Científica de Sistemas e Informática*, 5(1), e862. <https://doi.org/10.51252/rcsi.v5i1.862>

RESUMEN

El estudio en ciberseguridad ha generado una creciente dependencia de sistemas y redes interconectadas, siendo un tema de prioridad constante. El objetivo fue cuantificar y analizar la actividad científica disponible acerca de los estudios de ciberseguridad en el periodo 2020-2024. Se aplicó el método bibliométrico con enfoque cuantitativo de tipo descriptivo, de carácter transversal, usando la metodología PRISMA para analizar 612 publicaciones indexadas en las bases de datos WoS y con el análisis del software VOSviewer. Los resultados presentan un incremento en la producción de documentos en los últimos cinco años producto de las redes de colaboración entre autores e instituciones de diversos países, Perú se encuentra en el quinto lugar de productividad con 17 documentos indexados, el autor peruano con 12 citas recibidas es Edwin Hernan Ramirez-Asis y la Pontificia Universidad Católica el mayor número de publicaciones. La revista con mayor número de publicaciones e impacto pertenece IEEE Access con 131 documentos y el título publicado con el mayor número de citas de 186 pertenece a la revista Nature Machine Intelligence. Se concluye que la productividad y las redes de colaboración entre investigadores se vienen dando de manera articulada entre diversos países de América del Sur y otros continentes.

Palabras clave: delitos informáticos; protección de datos; seguridad de datos; seguridad informática

ABSTRACT

The study of cybersecurity has generated a growing dependence on interconnected systems and networks, being a topic of constant priority. The objective was to quantify and analyze the scientific activity available regarding cybersecurity studies in the period 2020-2024. The bibliometric method was applied with a quantitative, descriptive, cross-sectional approach, using the PRISMA methodology to analyze 612 publications indexed in the WoS databases and with the analysis of the VOSviewer software. The results show an increase in the production of documents in the last five years as a result of collaboration networks between authors and institutions from various countries, Peru is in fifth place in productivity with 17 indexed documents, the Peruvian author with 12 citations received is Edwin Hernan Ramirez-Asis and the Pontifical Catholic University has the highest number of publications. The journal with the highest number of publications and impact belongs to IEEE Access with 131 documents and the title published with the highest number of citations of 186 belongs to the journal Nature Machine Intelligence. It is concluded that productivity and collaboration networks between researchers are occurring in an articulated manner between various countries in South America and other continents.

Keywords: cyber-crimes; data protection; data security; information security



1. INTRODUCCIÓN

En la actualidad, el campo de la ciberseguridad atraviesa diversos problemas complejos desde varios puntos de vista, específicamente en el marco de las ciencias de la computación que es una disciplina de rápido desarrollo y evolución. A medida que avanzan y se innovan las tecnologías, los riesgos y amenazas evolucionan en el ciberespacio digital, generando un ciclo de constante vulnerabilidad que necesitan de atención inmediata para dar soluciones innovadoras y adaptativas a diversos contextos sociales, empresariales y tecnológicos (Ospina et al., 2023).

Para Ampofo et al. (2024) es importante reconocer que también aún existen problemas sobre la protección de la privacidad en los sistemas de información y que estas siguen siendo muy difíciles de resolver. Por su parte Arroyabe et al. (2024), afirman que la adopción de tecnologías emergentes como el big data, el cloud computing, la inteligencia artificial, el machine learning y el blockchain tiene un impacto significativo en la innovación y la productividad de las empresas, la capacidad de conectividad para intercambiar y consumir datos supone una mayor exposición a ciberataques.

En el ciberespacio el tema legal constituye un área crítica en el contexto contemporáneo, donde la intersección entre la tecnología y el derecho plantea desafíos multifacéticos, en este escenario, el entorno digital se convierte en un terreno propenso a amenazas que van desde el robo de datos hasta la intrusión cibernética (Arboleda-López et al., 2024; Jiménez-Almeira & López; Sharma et al., 2023). Es necesario analizar el tema de la ciberseguridad como base para formular acciones apoyado de las ciencias de la computación para evitar los riesgos y las vulnerabilidades de la información (Ullah & Babar, 2022; Diam et al., 2024).

Por lo tanto, con los ataques cibernéticos permanentes que van ganando impulso cada día, ninguna persona u organización, pública o privada, está a salvo de estos posibles delitos (Flores et al., 2021). En consecuencia, la ciberseguridad está emergiendo como una competencia para la supervivencia y el crecimiento organizacional donde los sistemas informáticos son cada vez más complejos y están más interconectados creando puntos de entrada para los atacantes cibernéticos (García et al., 2024).

En este contexto, la ciberseguridad aparece en las organizaciones como un elemento clave para asegurar la confidencialidad y operatividad de estos establecimientos en el entorno actual (Garces-Giraldo et al., 2022). En ese sentido, el estudio bibliométrico debe permitir obtener información relevante sobre las publicaciones que aborden los estudios de ciberseguridad y los temas relacionados, destacando los tipos de publicación, el impacto y tendencias que tienen en el campo científico y los niveles y redes de participación y colaboración de los autores (Lujan-Salamanca et al., 2024; Ramírez et al., 2023).

Como método, la bibliometría es un estudio que permite conocer la evolución histórica y contemporánea de un área del conocimiento o disciplina, identificando tendencias, brechas y fortalezas en la investigación (Nobanee et al., 2024; Hamid & Nurul, 2024; Pejic-Bach et al., 2023), abordando en este caso, las redes de colaboración en la investigación sobre ciberseguridad desde la disciplina ciencias de la computación (Mtsweni & Thaba, 2024). El análisis bibliométrico contribuye a planificar futuras investigaciones y mejorar la eficiencia de los esfuerzos basado en evidencia bibliográfica (Sánchez-García et al., 2024).

Obando-Ibarra et al. (2022) recomiendan tomar de referencia los últimos cinco años de las publicaciones indexadas para realizar un análisis bibliométrico más preciso en una determinada

disciplina. Admass et al. (2024) a su vez, manifiestan que la ciberseguridad es aplicable en diferentes áreas de conocimiento o sectores económicos, como centros de salud, instituciones financieras, ciudades inteligentes, sistemas de red, organizaciones gubernamentales, educación o el ejército.

Existen estudios bibliométricos que abordan temas como protección de ecosistemas digitales y desarrollo sostenible (Benaichouba et al., 2024; Sulich et al., 2023), en la gestión de la industria para la toma de decisiones (Ahmed et al., 2024; Oliva et al., 2024), en entornos de la educación usando inteligencia artificial (Ambali et al., 2024; Orosco-Fabian, 2024; Kaur et al., 2023), en sector comercial marítimo (Bolbot et al., 2022), agresión y victimización en adolescentes (Fernández et al., 2024), impacto de la tecnología 5G en las telecomunicaciones (Gamboa-Cruzado et al., 2024), cultura organizacional de ciberseguridad para el sector financiero (González et al., 2023), perspectivas de ciberseguridad extraídas de las religiones del mundo (Renaud & Dupuis, 2023) y finalmente tendencias en transformación digital en tiempos de pandemia (Wamba et al., 2023).

Existen estudios bibliométricos sobre ciberseguridad y otros temas relacionados en diversas partes del mundo; sin embargo, ¿Se dispone de investigaciones que hayan analizado la producción científica peruana y de los países limítrofes sobre el tema? Si bien las instituciones académicas y grupos de investigación, interesados en promover la seguridad de la información (Matilde-Espino & Valencia-Pérez, 2022), se han interesado en generar mayor conocimiento no se ha investigado en el tema de ciberseguridad desde las ciencias de la computación (Chuquitucto et al., 2024).

Por ello, el objetivo principal de esta investigación es cuantificar y analizar la actividad científica disponible acerca de los estudios de ciberseguridad en los últimos cinco años, 2020-2024. Los objetivos específicos son: analizar la productividad y las redes de colaboración, determinar las revistas con mayor número de publicaciones y su impacto en citas, identificar los temas relacionados y las coocurrencias más emergentes y relevantes.

2. MATERIALES Y MÉTODOS

2.1 Diseño de estudio

La investigación utilizó el método bibliométrico y, por su naturaleza, fue un estudio de enfoque cuantitativo de tipo descriptivo, de carácter transversal, mediante el análisis de publicaciones científicas indexadas en las bases de datos bibliográfica Web of Sciences (WoS) sobre el tema de ciberseguridad. Se toma como muestra el rango de tiempo 2020-2024 con fecha de corte de la descarga hasta el 03 de agosto del 2024. Para definir el término normalizado de búsqueda, se hizo uso del tesoro de la UNESCO, con la finalidad de identificar las relaciones jerárquicas conceptuales de “Ciberseguridad” con su término relacionado. La especificación del descriptor estaba relacionado al término “Data protection” y sus términos específicos identificados fueron:

- Computer Crime (Delitos informáticos)
- Computer Security (Seguridad informática)
- Data security (Seguridad de datos)
- Data privacy (Privacidad de datos)

La búsqueda y recuperación de información se realizó considerando los campos o metadatos del título del documento, resumen y palabra clave o descriptores. Se utilizó el siguiente query: (((((TS=(Data protection)) OR TS=(Computer Crime)) OR TS=(Computer security)) OR TS=(Data

security)) OR TS=(Data privacy)) OR TS=(cybersecurity) and 2024 or 2023 or 2022 or 2021 or 2020 (Publication Years) and Computer Science (Research Areas) and ARGENTINA or BOLIVIA or BRAZIL or CHILE or COLOMBIA or ECUADOR or PERU (Countries/Regions).

Para determinar las redes de colaboración en la investigación, se consideró importante hacer uso del software VOSviewer para construir y visualizar el liderazgo de investigadores (Ampofo et al., 2024) especializados en Ciberseguridad y redes de coocurrencia de términos importantes extraídos de la literatura científica sobre el tema.

2.2 Procedimientos

De los resultados de búsqueda de información en WoS se obtuvieron 612 documentos relacionados al tema de Ciberseguridad. Para la exclusión de publicaciones que no están relacionadas al tema se utilizó el criterio de que todos los documentos formen parte de la categoría o área de conocimiento de las ciencias de la computación. En la figura 1 se puede apreciar los pasos seguidos para la obtención y cribado de los documentos analizados en esta investigación a través de una revisión sistémica utilizando la metodología PRISMA (Valdiviezo et al., 2024) para garantizar que los datos de las publicaciones de las revistas sean adecuados y pertinentes.

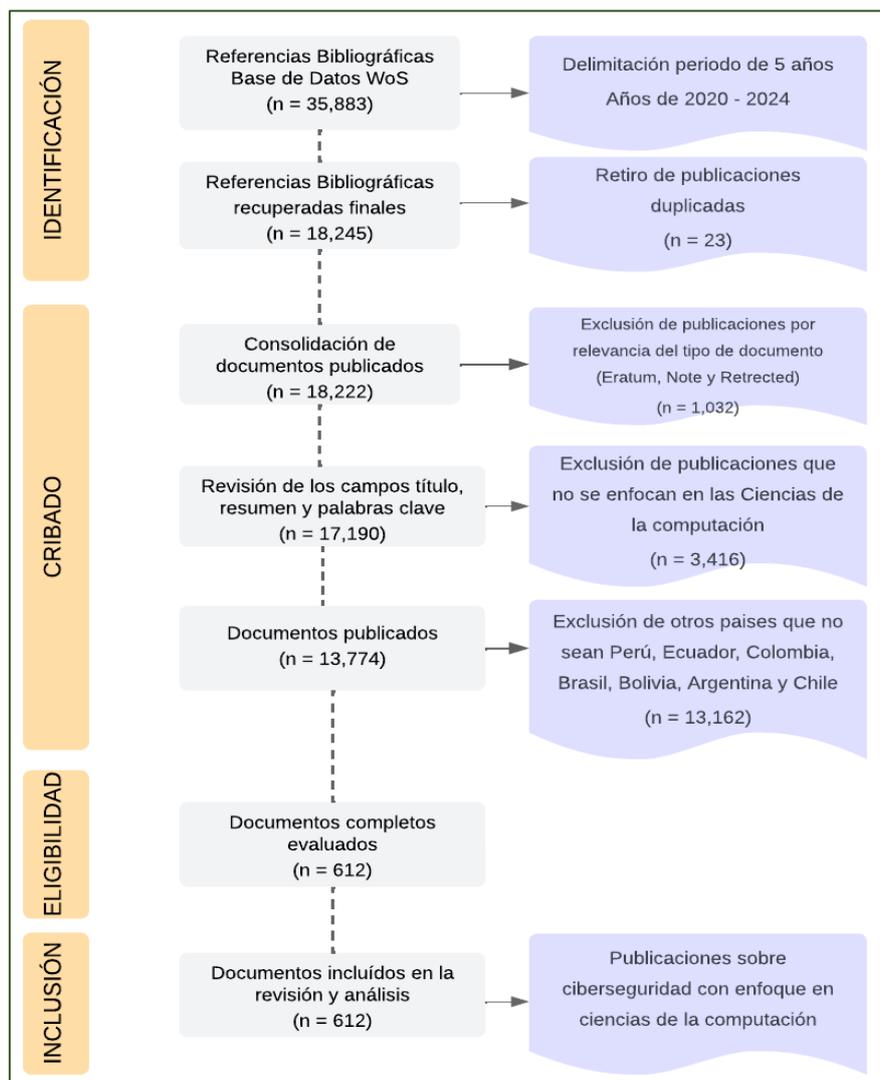


Figura 1. Diagrama de flujo de los registros bibliográficos bajo el modelo PRISMA

3. RESULTADOS

3.1 Productividad y redes de colaboración en ciberseguridad

La evolución de la producción científica sobre ciberseguridad en el Perú, en estos últimos años, incluyendo la época de pandemia, en comparación con otros países limítrofes, no se ha incrementado. Según la tabla 1, el país se encuentra en el quinto lugar con solo 2.7% de productividad y solo está sobre Argentina y Bolivia con la mínima diferencia de dos publicaciones. No obstante, podría ser mucho mejor. Hace algunos años la producción de algunos países era incipiente en estos temas, Sin embargo, ahora comienzan a generar un mayor número de publicaciones como es el caso de Colombia con 10.2%, Ecuador 8.8% y Chile con 7.6%.

Tabla 1. Número de documentos publicados sobre ciberseguridad por países

| Países | Periodo | | | | | Total | % |
|--------------|---------|------|------|------|------|-------|------|
| | 2020 | 2021 | 2022 | 2023 | 2024 | | |
| Brasil | 85 | 90 | 83 | 92 | 78 | 428 | 68.2 |
| Colombia | 12 | 13 | 16 | 9 | 14 | 64 | 10.2 |
| Ecuador | 13 | 5 | 9 | 14 | 14 | 55 | 8.8 |
| Chile | 5 | 5 | 7 | 9 | 22 | 48 | 7.6 |
| Perú | 1 | 1 | 8 | 3 | 4 | 17 | 2.7 |
| Argentina | 3 | 3 | 2 | 3 | 4 | 15 | 2.4 |
| Bolivia | 0 | 0 | 0 | 1 | 0 | 1 | 0.2 |
| Total | 119 | 117 | 125 | 131 | 136 | 628 | 100% |

Nota. El número de publicaciones se incrementa, de 612 a 628 porque algunos documentos fueron elaborados en colaboración con dos o más países.

Sobre Brasil se puede evidenciar que ha logrado un desarrollo significativo de 68.2% de productividad en temas de ciberseguridad desde el enfoque de las ciencias de la computación, con un aumento sostenido en los cinco años de análisis; sin duda influye su población universitaria que se abocan como todos a la investigación para proteger todo tipo de información que genera la sociedad (Ambali et al., 2024); sin embargo, este positivo desarrollo de la investigación en el tema responde a políticas públicas claras y sostenibles (Arboleda-López et al., 2024; Jiménez-Almeira & López; Sharma et al., 2023).

Antes de realizar un análisis general de todos los países de la muestra, es necesario describir la productividad de autores peruanos o que pertenecen a instituciones peruanas que hayan publicado sobre ciberseguridad. En la tabla 2 se aprecia que Ramirez-Asis ocupa el primer lugar con dos publicaciones y 12 citas; sin embargo, Casavilca Silva con solo una publicación ha obtenido 44 citas. Lo mismo pasa con Bravo y Libaque-Saenz que son coautores y su publicación ha obtenido 36 citas. Esto significa que las publicaciones de los autores peruanos tienen un impacto importante en el ámbito científico.

Tabla 2. Los diez autores peruanos con mayor número de documentos publicados sobre ciberseguridad

| Autores peruanos | Filiación principal | Indicadores bibliométricos | | |
|-----------------------------------|---|----------------------------|----|---------|
| | | NP | NC | H-Index |
| Ramirez-Asis, Edwin Hernan | Universidad Nacional Santiago Antúnez de Mayolo | 2 | 12 | 10 |
| Sanchez-Chero, Manuel | Universidad Nacional de Frontera | 2 | 6 | 9 |
| Arias Gonzales, Jose Luis | Pontificia Universidad Católica del Perú | 2 | 1 | 9 |
| Casavilca Silva, Juan C. | Pontificia Universidad Católica del Perú | 1 | 44 | 4 |
| Bravo, Edgardo R. | Universidad del Pacífico | 1 | 36 | 5 |
| Libaque-Saenz, Christian Fernando | Universidad del Pacífico | 1 | 36 | 0 |
| Sotelo Monge, Marco Antonio | Universidad de Lima | 1 | 17 | 10 |

| | | | | |
|-----------------------------|---|---|---|---|
| Esenarro, Doris | Universidad Ricardo Palma | 1 | 8 | 7 |
| Rodriguez, Ciro | Universidad Nacional Mayor de San Marcos | 1 | 8 | 6 |
| Delgado-del-Carpio, Marcelo | Universidad Nacional de San Agustín de Arequipa | 1 | 6 | 0 |

NP=Número de publicaciones, NC=Número de citas y H-Index = Número de publicaciones que han sido citados al menos h veces (WoS).

Desde el punto de vista general, en la tabla 3 se presenta la relación de autores con mayor número de publicaciones indexadas, donde se destaca la productividad de Joel Rodrigues, con 45 documentos, logra alcanzar hasta el momento 898 citas recibidas, siendo el investigador con mayor impacto en los temas de ciberseguridad, teniendo un índice H de 80. Asimismo, siguen sus pasos otros autores. Es necesario resaltar el trabajo realizado por Cristiano Andre Da Costa que tan solo con 6 publicaciones ha recibido 353 citas demostrando la calidad en los contenidos de sus investigaciones.

Tabla 3. Los diez autores con mayor número de documentos publicados sobre ciberseguridad

| Autores | Procedencia | Rank | Indicadores bibliométricos | | | |
|--------------------------------|-------------|------|----------------------------|-----|-----|---------|
| | | | NP | %A | NC | H-Index |
| Rodrigues, Joel J. P. C. | Brasil | 1 | 45 | 7.4 | 898 | 80 |
| de Albuquerque, Victor Hugo C. | Brasil | 2 | 26 | 4.2 | 739 | 64 |
| Muhammad, Khan | India | 3 | 13 | 2.1 | 481 | 60 |
| Nogueira, Michele | Brasil | 4 | 12 | 2.0 | 139 | 15 |
| Das, Ashok Kumar | India | 5 | 9 | 1.5 | 383 | 19 |
| Menegutte, Rodolfo Ipolito | Brasil | 6 | 7 | 1.1 | 64 | 19 |
| Righi, Rodrigo Da Rosa | Brasil | 7 | 7 | 1.1 | 205 | 27 |
| Carvalho, Luiz Fernando | Brasil | 8 | 6 | 1.0 | 172 | 9 |
| Da Costa, Cristiano Andre | Brasil | 9 | 6 | 1.0 | 353 | 27 |
| Moraes, Fernando Gehm | Brasil | 10 | 6 | 1.0 | 25 | 14 |

NP = Número de publicaciones, %A = Porcentaje de artículos de todas las publicaciones, NC = Total de citas recibidas por todos los documentos desde su publicación y H-Index = Número de publicaciones que han sido citados al menos h veces (WoS)

Queda en evidencia el alto factor de impacto de los autores con relación al número de citas obtenidas con tan solo un cierto número de publicaciones, lo cual demuestra la existencia de un creciente interés por parte de la comunidad científica de las ciencias de la computación e ingeniería informática en investigar sobre el cibercrimen que afecta a diversos sectores, incluidas las empresas, los gobiernos y las personas como lo sustenta Chuquitucto et al. (2024). Es necesario resaltar que todos los autores del ranking publican en revistas que cuentan con sistemas de revisión por pares, conocidas también como revistas arbitradas que permiten alcanzar mayor calidad de los contenidos de las investigaciones.

La figura 2 muestra el trabajo colaborativo de los investigadores en 5 nodos, el de mayor importancia está liderado por Joel J. P. C. Rodrigues quienes a su vez colabora de forma permanente con los otros tres clústeres que están representados por Victor Hugo C. De Albuquerque del nodo mostaza, de Khan Muhammad del nodo azul y Mario Proenca del color morado; para el caso del clúster liderado por Michele Nogueira, solo están en la red de investigadores colaborando con un Paolo Bellavista que forma parte del clúster azul.

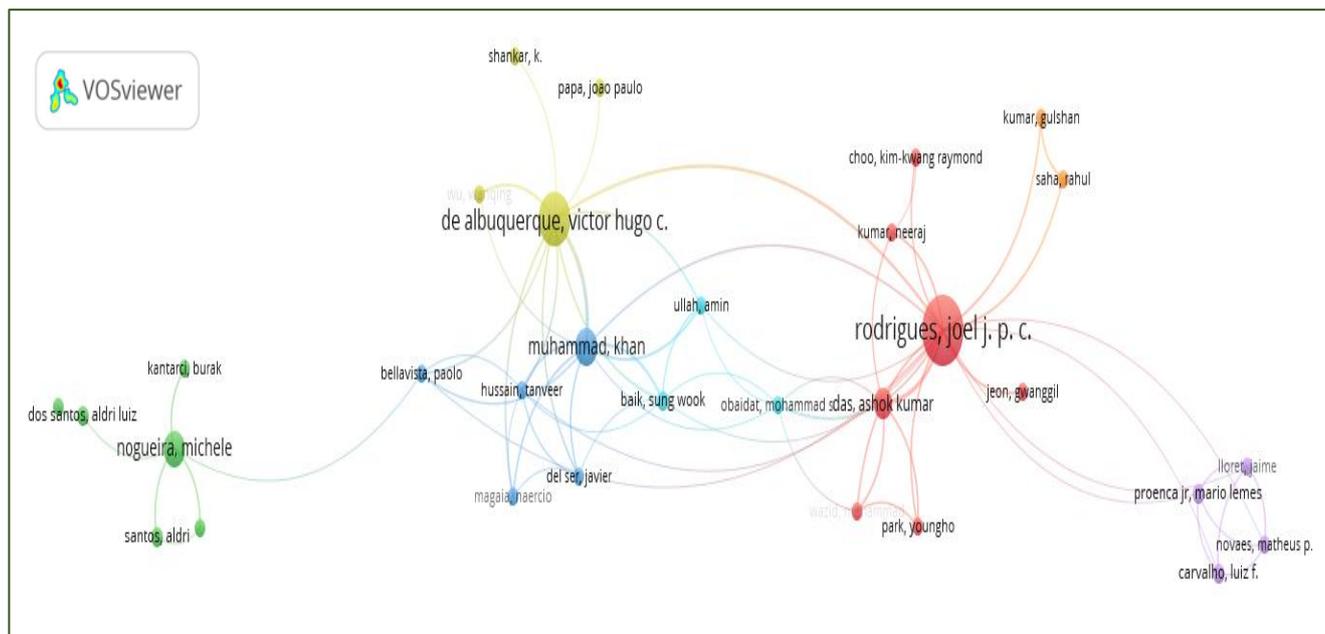


Figura 2. Mapa de coautoría personal de documentos publicados sobre Ciberseguridad

Las tendencias de las redes de colaboración están influenciando en el trabajo de los investigadores frente a los desafíos de internacionalizar su trabajo investigativo y buscan redefinir los procesos de investigación. Valencia-Arias et al. (2020) destaca la necesidad de una colaboración multidisciplinaria y transfronteriza, quiere decir que la participación en grupos de investigadores afines a estos temas de ciberseguridad debe permitir, entre varias cosas, desarrollar y reflexionar en conjunto para la producción de conocimiento científico.

Es por ello, que la colaboración internacional, que representa mayor interés entre los investigadores, articula los esfuerzos con países que cuentan con sistemas nacionales de ciencia y tecnología consolidados, esto es para el Perú y otros países de América Latina, un instrumento para optimizar los recursos y tener mayores oportunidades en el financiamiento y, en consecuencia, lograr mejores resultados de investigación en términos de cantidad e impacto aceptando lo planteado por Muñoz et al. (2023).

En el caso peruano, en la tabla 4, se aprecia que todas las instituciones que han publicado documentos indexados sobre ciberseguridad relacionados a las ciencias de la computación son todas universidades. Como menciona Matilde-Espino & Valencia-Pérez (2022) es en la academia que recae la responsabilidad de promover más en investigar y generar nuevos conocimientos en el proceso formativo de los estudiantes sobre esta materia, con mayor razón los programas de ingeniería.

Tabla 4. Instituciones peruanas con mayor número de publicaciones sobre ciberseguridad

| Instituciones peruanas | Publicaciones |
|---|---------------|
| Pontificia Universidad Católica del Perú | 3 |
| Universidad de Lima | 3 |
| Universidad Nacional de Ingeniería | 3 |
| Universidad Nacional Santiago Antúnez de Mayolo | 3 |
| Universidad del Pacífico | 2 |
| Universidad Nacional de Frontera | 2 |
| Universidad Autónoma del Perú | 1 |
| Universidad Nacional de Huancavelica | 1 |
| Universidad Nacional de San Agustín de Arequipa | 1 |

estudio. Se concuerda con esta afirmación puesto que el mayor número de instituciones que realizan este tipo de estudio son las universidades.

Asimismo, la figura 4 permite observar la colaboración entre los países, en especial el Perú donde los autores vienen desarrollando sus investigaciones con sus similares extranjeros. En primer lugar, se presenta el clúster morado liderado por Brasil, la red de colaboración más grande, ésta la conforman entre varias con las instituciones de Corea del Sur; luego se encuentra el clúster rojo representado por estados Unidos que viene colaborando con Inglaterra, Nigeria, Jordán y Argentina; por su parte, Portugal del nodo azul, colabora con algunos países asiáticos como la India, Pakistán, Arabia Saudita como también con Perú; Para el caso del nodo verde, Es Colombia quien promueve esta red de investigadores incluyendo a más países de américa del sur como son Ecuador y Chile; finalmente el nodo mostaza que forman parte Canadá y Australia.

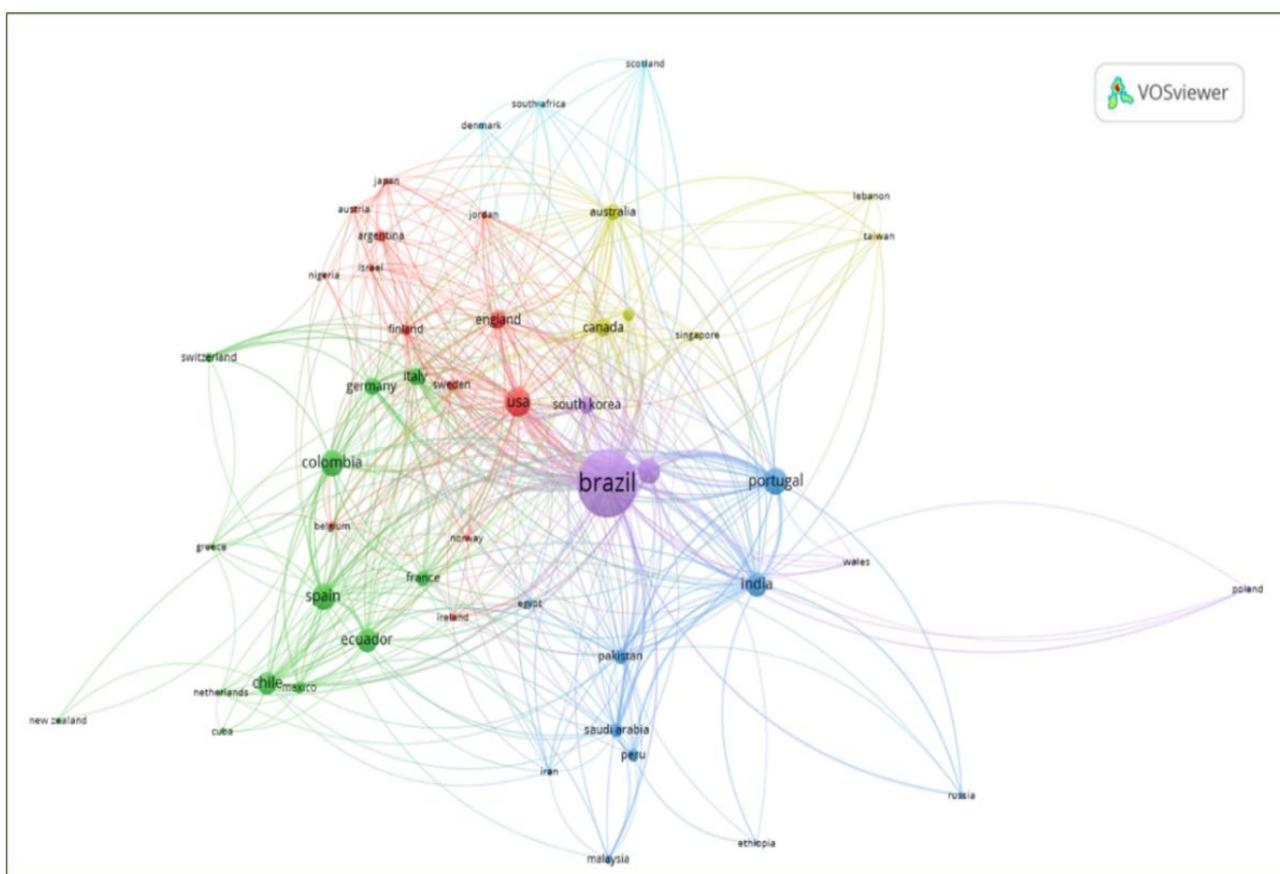


Figura 4. Mapa de coautoría institucional por países de documentos publicados sobre Ciberseguridad

Estos representan las afinidades de los autores para trabajar en equipo y las redes de colaboración ya establecidos o formados entre instituciones de diferentes países. Prümmer et al. (2024), afirma que los problemas que involucra a la ciberseguridad es similar o tienen las mismas características en todos los países, solo son contextos diferentes y la solución aplica para todas las realidades sin importar los aspectos geográficos. Esto queda corroborado por los resultados obtenidos.

3.2 Revistas científicas con mayor número de publicaciones y su impacto

Según la tabla 5 la revista con mayor número de publicaciones e impacto es la "IEEE Access" editado por IEEE-Inst Electrical Electronics Engineers Inc que opera en los Estados Unidos; con 131 publicaciones sobre ciberseguridad y 1475 citas recibidas, esta revista se posiciona en el primer lugar del ranking, con un número de autores promedio de 4 por cada publicación y de 11

citadas recibidas por cada documento. Es evidente que estos resultados demuestran que este tipo de revistas especializadas en el tema de las ciencias de la computación y que abordan el tema han logrado tener preferencia en la comunidad científica.

Tabla 5. Las quince revistas con mayor número de documentos publicados sobre Ciberseguridad

| Revista | Rank | Editorial | País | Indicadores bibliométricos | | | | | |
|--|------|--|----------------|----------------------------|-------|-----|------|------|-------|
| | | | | NP | % NP | NA | NAP | NC | NCP |
| IEEE Access | 1 | IEEE-Inst Electrical Electronics Engineers Inc | Estados Unidos | 131 | 21.41 | 644 | 4.92 | 1475 | 11.26 |
| IEEE Internet of Things Journal | 2 | IEEE-Inst Electrical Electronics Engineers Inc | Estados Unidos | 27 | 4.41 | 141 | 5.22 | 546 | 20.22 |
| Electronics | 3 | MDPI | Suiza | 21 | 3.43 | 115 | 5.48 | 132 | 6.29 |
| IEEE Latin America Transactions | 4 | IEEE-Inst Electrical Electronics Engineers Inc | Estados Unidos | 21 | 3.43 | 77 | 3.67 | 105 | 5.00 |
| IEEE Transactions on Network and Service Management | 5 | IEEE-Inst Electrical Electronics Engineers Inc | Estados Unidos | 18 | 2.94 | 93 | 5.17 | 176 | 9.78 |
| Computer Networks | 6 | Elsevier | Países Bajos | 16 | 2.61 | 86 | 5.38 | 248 | 15.50 |
| Computers & Security | 7 | Elsevier Advanced Technology | Inglaterra | 14 | 2.29 | 57 | 4.07 | 130 | 9.29 |
| Future Generation Computer Systems-The International Journal of Escience | 8 | Elsevier | Países Bajos | 13 | 2.12 | 76 | 5.85 | 308 | 23.69 |
| Computers and Electronics in Agriculture | 9 | Elsevier SCI Ltd | Inglaterra | 9 | 1.47 | 46 | 5.11 | 62 | 6.89 |
| Ad Hoc Networks | 10 | Elsevier | Países Bajos | 8 | 1.31 | 33 | 4.13 | 21 | 2.63 |

NP = Número de publicaciones, %NP = Porcentaje del total de publicaciones ($NP \cdot 100 / 612$), NA = Número de autores de todas las publicaciones, NAP = Número de autores por publicación (NA / NP), NC = Total de citas recibidas por todos los documentos desde su publicación y NCP = Número de citas por publicación (NC / NP).

Valencia-Arias et al. (2020) confirma que un proceso riguroso de revisión por pares también es importante para generar confianza en el proceso científico entre los formuladores de políticas científicas. La experiencia en revisión de artículos científicos produce un agudo sentido para la investigación novedosa, innovadora, rigurosa y de avance en el campo. Se suma Mtsweni & Thaba (2024) cuando sustenta que, para los autores, la publicación de sus investigaciones en revistas de prestigio, con métodos de evaluación con revisión de pares, reconoce el rigor y el impacto de su estudio y lo consideran necesaria para avanzar en su carrera investigativa y obtener financiamiento para la investigación. Se concuerda con ambos, ya que la revisión por pares está profundamente arraigada en el proceso científico y permite que las ideas, métodos, datos, hallazgos y conclusiones de los autores sean evaluados y calificados con carácter de calidad.

Se puede apreciar en la tabla 6, los documentos publicados que han obtenido el mayor número de citas sobre Ciberseguridad. El primer lugar del ranking, con 186 citas recibidas, se tiene al título "End-to-end privacy preserving deep learning on multi-institutional medical imaging" que viene a ser un artículo científico y que es publicado por la revista Nature Machine Intelligence de Alemania; esta publicación fue difundido en el año 2021. Un mayor recuento de citas aumenta la probabilidad de obtener mayor número de citación y señala el camino para futuras investigaciones en el trabajo de un autor.

Tabla 6. Los quince títulos más citados de los documentos publicados sobre Ciberseguridad

| Rank | NC | Título | Revista | Tipo de Publicación | País | Año |
|------|-----|---|--|---------------------|----------------|------|
| 1 | 186 | End-to-end privacy preserving deep learning on multi-institutional medical imaging | Nature Machine Intelligence | Article | Alemania | 2021 |
| 2 | 166 | Federated Learning for Healthcare: Systematic Review and Architecture Proposal | ACM Transactions on Intelligent Systems and Technology | Review | Estados Unidos | 2022 |
| 3 | 152 | Security in SDN: A comprehensive survey | Journal of Network and Computer Applications | Review | Inglaterra | 2020 |
| 4 | 148 | A Survey of 5G Technology Evolution, Standards, and Infrastructure Associated With Vehicle-to-Everything Communications by Internet of Vehicles | IEEE Access | Article | Estados Unidos | 2020 |
| 5 | 130 | Human action recognition using attention based LSTM network with dilated CNN features | Future Generation Computer Systems-The International Journal Of ESCIENCE | Article | Países Bajos | 2021 |
| 6 | 129 | A Survey of Blockchain-Based Strategies for Healthcare | ACM Computing Surveys | Article | Estados Unidos | 2020 |
| 7 | 126 | Intelligent personal assistants: A systematic literature review | Expert Systems With Applications | Review | Inglaterra | 2020 |
| 8 | 109 | Cloud Centric Authentication for Wearable Healthcare Monitoring System | IEEE Transactions on Dependable and Secure Computing | Article | Estados Unidos | 2020 |
| 9 | 108 | BAKMP-IoMT: Design of Blockchain Enabled Authenticated Key Management Protocol for Internet of Medical Things Deployment | IEEE Access | Article | Estados Unidos | 2020 |
| 10 | 97 | A Blockchain-Based Shamir's Threshold Cryptography Scheme for Data Protection in Industrial Internet of Things Settings | IEEE Internet Of Things Journal | Article | Estados Unidos | 2022 |

NC = Total de citas recibidas por el documento publicado.

El prestigio de sus investigadores, la rigurosidad de los estudios y la permanente publicación de los resultados, son un factor importante en la visibilidad e impacto de una revista. En términos actuales, asegura Hamid & Nurul (2024), esto se refleja en el número de citas con la que cuentan los artículos. Asimismo, el impacto que genera una publicación en la sociedad se traduce en cómo ha ido formando opinión pública y ha sido insumo para la generación de nuevos conocimientos, influyendo en la toma de decisiones de funcionarios y autoridades políticas.

3.3 Temáticas más relevantes que se vienen desarrollando en torno a Ciberseguridad

Con relación a los descriptores o palabras clave que hacen uso las publicaciones indexadas para describir su contenido, en la figura 5 se puede identificar el término principal o la mención con mayor frecuencia en el mapa temático que es Security que encabeza el clúster naranja y que está asociado con los términos de autenticación y encriptación en sistemas de información, control de accesos a bases de datos en compañías e industrias, dejando en evidencia que se encuentran en el marco de las ciencias de la computación; complementando lo mencionado con el nodo Machine Learning de color verde que relaciona el campo de la Inteligencia Artificial, desarrollo de

4. CONCLUSIONES

En cuanto a producción científica de Perú el número es mínimo y se requiere promover en las universidades la investigación en el tema. Las redes de colaboraciones de investigación con los autores personales e institucionales, se ha observado un trabajo conjunto pertenecientes a varios países, en especial de Brasil, cuyos resultados se reflejan en el número de publicaciones y citas recibidas a lo largo de los últimos 5 años. Se logró determinar las 10 primeras revistas con mayor número de publicaciones en el tema y las publicaciones como el mayor número de citas recibidas, demostrándose así, su impacto y posicionamiento en el campo científico. Se logró identificar la coocurrencia de palabras clave o descriptores de las diversas temáticas que giran alrededor de ciberseguridad, como la seguridad de los datos, uso de protocolos de seguridad para los accesos a sistemas de información, machine learning, blockchain, entre otros.

En este sentido, se sugiere ampliar el estudio haciendo uso de otras bases de datos bibliográficas, así como el uso de otras variables vinculadas que ayuden a entender las diversas temáticas y situaciones reveladas por el estudio. Es crucial que las investigaciones futuras sigan indagando sobre el desarrollo e impacto de ciberseguridad desde distintos enfoques, ya que el campo de la tecnología se va innovando a cada momento.

FINANCIAMIENTO

Los autores no recibieron ningún patrocinio para llevar a cabo este estudio-artículo.

CONFLICTO DE INTERESES

Los autores declaran no tener ningún tipo de conflicto de interés relacionado con el desarrollo del estudio.

CONTRIBUCIÓN DE LOS AUTORES

Conceptualización: Cuya-Chamilco, P. V.; Metodología: Mescua-Ampuero, L. E.; Software: Saavedra-Villar, P.; Curación de datos: Cáceres-García, A. A.; Validación: Alvarado-Flores, J.; Análisis formal: Cuya-Chamilco, P. V., Mescua-Ampuero, L. E., Saavedra-Villar, P., Cáceres-García, A. A., & Alvarado-Flores, J.; Redacción - borrador original: Cuya-Chamilco, P. V.

REFERENCIAS BIBLIOGRÁFICAS

- Admass, W., Munaye, Y. & Diro, A. (2024). Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications*, 2,100031.
<https://doi.org/10.1016/j.csa.2023.100031>
- Ahmed, I., Hossain, N., Fazio, S., Lezzi, M. & Islam, S. (2024). A decision support model for assessing and prioritization of industry 5.0 cybersecurity challenges. *Sustainable Manufacturing and Service Economics*, 3, 100018.
<https://doi.org/10.1016/j.smse.2024.100018>
- Ambali, M., Rustamov, J., Ahmed, S., Rustamov, Z., Awad, A., Zaki, N. & Alnajjar, F. (2024). Integrating AI-based and conventional cybersecurity measures into online higher education settings: Challenges, opportunities, and prospects. *Computers and Education: Artificial*

Intelligence, 7, 100327. <https://doi.org/10.1016/j.caeai.2024.100327>

Ampofo, I., Kobina, E., Badzongoly, E., Buabeng, S., Oppong-Twum, F., Amoah, P., Ampofo, I., Afriyie, G., Obiribea, L. & Yeboah, M. (2024). Bibliometric and Visualized Analysis of Scientific Publications on Blockchain Technology in Cybersecurity. En: Arai, K. (eds) *Intelligent Computing. SAI 2024. Lecture Notes in Networks and Systems*, vol 1016. Springer, Cham. https://doi.org/10.1007/978-3-031-62281-6_36

Arboleda-López, A., Valencia-Arias, J., Garcés-Giraldo, L., Flores, E. & León, A. (2024). Legal defense in cyberspace: a bibliometric approach from Scopus and Web of Science. *Revista Ibérica de Sistemas e Tecnologías De Informação*, E72, 180-191. <https://www.proquest.com/scholarly-journals/defensa-legal-en-el-ciberespacio-una-aproximación/docview/3118075948/se-2>

Arroyabe, M., Arranz, C., Fernandez de Arroyabe, J. & Fernandez, I. (2024). Digitalization and Cybersecurity in SMEs: A Bibliometric Analysis. *Procedia Computer Science*, 237, 80-87. <https://doi.org/10.1016/j.procs.2024.05.082>

Bolbot, V., Kulkarni, K., Brunou, P. Valdez, O. & Musharraf, M. (2022). Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis. *International Journal of Critical Infrastructure Protection*, 39, 100571. <https://doi.org/10.1016/j.ijcip.2022.100571>

Benaichouba, R., Brahmi, M. & Adala, L. (2024). Economic of cyber-security and society databases: protecting the digital ecosystem from cyber-attacks. *International Journal of Professional Business Review*, 9(7), 1-26. <https://doi.org/10.26668/busincssreview/2024.v9i7.4803>

Chuquitucto, L., Silva, P., Reyes, C., Arbulú, M., Ángeles, M., Arbulú, J., Martel, R. & Paredes, A. (2024). Cyber Crimes: A Systematic Review of Evolution, Trends, and Research Approaches. *Journal of Educational and Social Research*, 14(5), 96. <https://doi.org/10.36941/jesr-2024-0124>

Daim, T., Yalcin, H., Mermoud, A. & Mulder, V. (2024). Exploring cyber technology standards through bibliometrics: Case of National Institute of Standards and Technology. *World Patent Information*, 77, 102278. <https://doi.org/10.1016/j.wpi.2024.102278>

Fernández, A., Jiménez, M., Dúo, P. & Moreno, A. (2024). Cyberaggression and cybervictimisation in adolescents: Bibliometric analysis in web of science. *Heliyon*, 10(1), e23329. <https://doi.org/10.1016/j.heliyon.2023.e23329>

Flores, F., Pozo, C., Flores, L., Aduato, W. (2021). Challenges of transformational leadership in organizational cybersecurity matters. *Revista Venezolana de Gerencia*, 26(5), 417 – 429. <https://doi.org/10.52080/rvgluz.26.e5.27>

Gamboa-Cruzado, J., Cuya-Chuica, L., López-Goycochea, J., Núñez-Meza, Á & Valle, C. (2024). Impact of 5G Technology on Cybersecurity: A Comprehensive Systematic and Bibliometric Review. *Computación y Sistemas*, 28(2), 367–386. <https://doi.org/10.13053/CyS-28-2-4734>

Garcés-Giraldo, L., Benjumea-Arias, M., Vélez, O., Valencia-Arias, A., Celi, L., Bermeo-Giraldo, C. & Quiroz-Fabra, J. (2022). Research trends in the use of Big Data technologies in cybersecurity systems. *RISTI - Revista Iberica de Sistemas e Tecnologías de Informacao*, 2022(E49), 410 –

420. <https://www.proquest.com/scholarly-journals/tendencias-investigativas-en-el-uso-de/docview/2714753949/se-2>
- García, F., Donoso, Í. Flores, A. Pon, C. Flores, V. & Martínez-Peláez, R. (2024). Examining cybersecurity culture in Leon city organizations: Insights from 2022. *Ingeniare: Revista Chilena de Ingeniería*, 32, 1-16. <https://www.proquest.com/scholarly-journals/examining-cybersecurity-culture-leon-city/docview/3102955924/se-2>
- González, D., Soto, D., Peláez, L., Villamizar, A., Delgado, I. & Vidal, F. (2023). Modelo de madurez de cultura organizacional de ciberseguridad para el sector financiero basado en buenas prácticas. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, 2023(E62), 362-375. <https://www.risti.xyz/issues/ristie62.pdf>
- Hamid, S. & Nurul, M. (2024). Mapping the landscape of government data breaches: A bibliometric analysis of literature from 2006 to 2023. *Social Sciences & Humanities Open*, 11, 101234. <https://doi.org/10.1016/j.ssaho.2024.101234>
- Jiménez-Almeira, G. & López, D. (2023). Ciberseguridad y Seguridad Integral: un análisis reflexivo sobre el avance normativo en Colombia. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, 2023(E62), 16-31. <https://www.risti.xyz/issues/ristie62.pdf>
- Kaur, R., Gabrijelčič, D. & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, 97, 101804. <https://doi.org/10.1016/j.inffus.2023.101804>
- Luján-Salamanca, A., Infante-Moro, A., Infante-Moro, J. & 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>
- Matilde-Espino Y. & Valencia-Pérez L. (2022). Análisis bibliométrico de la producción científica sobre México en temas de Ciberseguridad (2015-2020). *CIENCIA ergo-sum*, 29(3). <https://doi.org/10.30878/ces.v29n3a11>
- Mtsweni, J. & Thaba, M. (2024). Bibliometric Analysis of Cyber Warfare Research in Africa: Landscape and Trends. Academic Conferences International Limited. *Proceedings of the 19th International Conference on Cyber Warfare and Security, ICCWS 2024*. <https://www.proquest.com/conference-papers-proceedings/bibliometric-analysis-cyber-warfare-research/docview/3082337474/se-2>
- Muñoz, A., Garibay, A. & Wong, L. (20-23 de junio de 2023). Cybersecurity framework for SMEs in Peru based on ISO/IEC 27001 and CSF NIST controls. *18th Iberian Conference on Information Systems and Technologies (CISTI)*, Aveiro, Portugal, pp. 1-7, <https://doi.org/10.23919/CISTI58278.2023.10211874>
- Nobanee, H., Alodat, A., Bajodah, R., Al-Ali, M. & Al Darmaki, A. (2023). Bibliometric analysis of cybercrime and cybersecurity risks literature. *Journal of Financial Crime*, 30(6), 1736-1754. <https://doi.org/10.1108/JFC-11-2022-0287>
- Obando-Ibarra, C., Garcés-Giraldo, L., Quiroz-Fabra, J., Benjumea-Arias, M., Valencia-Arias, A., Zavala, L. & Patiño-Vanegas, C. (2022). Evaluación de riesgos en ciberseguridad: una revisión bibliométrica. *RISTI - Revista Iberica de Sistemas de Tecnologias de Informacao*, 2022(E49), 396-409. <https://www.proquest.com/scholarly-journals/evaluación-de-riesgos-en->

ciberseguridad-una/docview/2714752808/se-2

- Oliva, A., Llanos, C., Alarcón, S. & León-Velarde, C. (2024). Cybersecurity for the Protection of IOT Devices in the Industrial Sector [Presentación principal]. *22nd LACCEI International Multi-Conference for Engineering, Education, and Technology: Sustainable Engineering for a Diverse, Equitable, and Inclusive Future at the Service of Education, Research, and Industry for a Society 5.0*. Hybrid Event, San José – Costa Rica.
<https://doi.org/10.18687/LACCEI2024.1.1.1206>
- Orosco-Fabian, J. (2024). Cybersecurity in higher education: a bibliometric review. *Revista Digital de Investigación en Docencia Universitaria*, 18(2), e1933.
<https://doi.org/10.19083/ridu.2024.1933>
- Ospina, A., Garcés-Giraldo, L., Valencia-Arias, A., Bermeo-Giraldo, M., Gómez-Bayona, L., Patiño-Vanegas, J. & García, R. (2023). Tendencias investigativas en ciberseguridad del Internet de las Cosas (IoT). *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, 2023(E62), 73-86. <https://www.risti.xyz/issues/ristie62.pdf>
- Pejić-Bach, M., Jajić, I. & Kamenjarska, T. (2023). A Bibliometric Analysis of Phishing in the Big Data Era: High Focus on Algorithms and Low Focus on People. *Procedia Computer Science*, 219, 91-98. <https://doi.org/10.1016/j.procs.2023.01.268>
- Prümmer, J., Steen, T. & Berg, B. (2024). A systematic review of current cybersecurity training methods. *Computers & Security*, 136, 103585. <https://doi.org/10.1016/j.cose.2023.103585>
- Ramírez, D., Garcés-Giraldo, L., Doria-Orozco, T., Franco-Castaño, S., Valencia-Arias, A., Rodríguez-Correa, P & Espinoza, J. (2023). Bibliometric analysis on the use of Machine Learning in cybersecurity. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, 2023(E62), 60-72. <https://www.risti.xyz/issues/ristie62.pdf>
- Renaud, K. & Dupuis, M. (2023). Cybersecurity Insights Gleaned from World Religions. *Computers & Security*, 132, 103326. <https://doi.org/10.1016/j.cose.2023.103326>
- Sánchez-García, I., Rea-Guaman, A., Feliu, T. & Calvo-Manzano, J. (2024). Auditoría de riesgos de ciberseguridad: Revisión de Literatura, propuesta y aplicación. *RISTI - Revista Iberica De Sistemas e Tecnologias De Informaçãõ*, (53), 69-86. <https://doi.org/10.17013/risti.53.69-87>
- Sharma, D., Mittal, R., Sekhar, R., Shah, P. & Renz, M. (2023). A bibliometric analysis of cyber security and cyber forensics research. *Results in Control and Optimization*, 10, 100204. <https://doi.org/10.1016/j.rico.2023.100204>
- Sulich, A., Zemasz, T. & Kulhanek, L. (2023). Towards a Secure Future: A Bibliometric Analysis of the Relations Between Cybersecurity and Sustainable Development. *Procedia Computer Science*, 225, 1448-1457. <https://doi.org/10.1016/j.procs.2023.10.133>
- Truong, T. & Nguyen, H. (2024). Cybersecurity in Small and Medium-Sized Enterprises: A Bibliometric Analysis. En: Pagac, M., Hajnys, J., Kozior, T., Nguyen, H., Nguyen, V., Nag, A. (eds) *From Smart City to Smart Factory for Sustainable Future: Conceptual Framework, Scenarios, and Multidiscipline Perspectives. Lecture Notes in Networks and Systems*, vol 1062. Springer, Cham. https://doi.org/10.1007/978-3-031-65656-9_39
- Valdiviezo, M., Huilca, F. & Alarcón, S. (2024). Machine Learning in Cybersecurity: Systematic

Literature Review [Presentación principal]. *22nd LACCEI International Multi-Conference for Engineering, Education, and Technology: Sustainable Engineering for a Diverse, Equitable, and Inclusive Future at the Service of Education, Research, and Industry for a Society 5.0*. Hybrid Event, San José – Costa Rica. <https://doi.org/10.18687/LACCEI2024.1.1.723>

Valencia-Arias, A., Patiño-Toro, O., Arenas-Fernández, A., Garcés-Giraldo, L., Umba-López, A. & Benjumea-Arias, M. (2020). Tendencias investigativas en el estudio de la ciberdefensa: un análisis bibliométrico. *Revista Ibérica De Sistemas e Tecnologias De Informação*, E29, 366-379. <https://www.proquest.com/scholarly-journals/tendencias-investigativas-en-el-estudio-de-la/docview/2394538000/se-2>

Ullah, F. & Babar, M. (2022). On the scalability of Big Data Cyber Security Analytics systems. *Journal of Network and Computer Applications*, 198, 103294. <https://doi.org/10.1016/j.jnca.2021.103294>

Wamba, S., Gumbo, S., Twinomurinzi, H., Bwalya, K. & Mpinganjira, M. (2023). Digital transformation under Covid-19: A Bibliometric Study and future research agenda. *Procedia Computer Science*, 219, 271-278. <https://doi.org/10.1016/j.procs.2023.01.290>