UNIVERSIDAD NACIONAL DE SAN MARTIN

RCSI
https://revistas.unsm.edu.pe/index.php/rcsi
e-ISSN: 2709-992X

Review article
Artículo de revisión
Jan-Jun, 2025

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

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

Paolo Víctor Cuya-Chamilco[1], Pablo Saavedra-Villar[2], Lizeth Erly Mescua-Ampuero[1], José Alvarado-Flores[1], Alan Armando Cáceres-García[3*]

[1]Universidad César Vallejo. Lima, Perú
[2]Universidad Nacional de Huancavelica. Huancavelica, Perú
[3]Superintendencia Nacional de Educación Superior Universitaria. Lima, Perú

Received: 09 Oct. 2024 | **Accepted:** 27 Dec. 2024 | **Published:** 20 Jan. 2025

Corresponding author*: alancaceres@sunedu.gob.pe

How to cite this article: Cuya-Chamilco, P. V., Saavedra-Villar, P., Mescua-Ampuero, L. E., Alvarado-Flores, J., & Cáceres-García, A. A. (2025). Cybersecurity from the perspective of computer science: a bibliometric study on Peru and neighboring countries. *Revista Científica de Sistemas e Informática, 5*(1), e862. https://doi.org/10.51252/rcsi.v5i1.862

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

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

1. INTRODUCTION

Currently, the field of cybersecurity is facing various complex problems from multiple perspectives, specifically within the framework of computer science, which is a rapidly developing and evolving discipline. As technologies advance and innovate, risks and threats evolve in the digital cyberspace, generating a cycle of constant vulnerability that requires immediate attention to provide innovative and adaptive solutions to various social, business, and technological contexts (Ospina et al., 2023).

For Ampofo et al. (2024), it is important to recognize that there are still issues regarding privacy protection in information systems and that those remain very difficult to resolve. For their part, Arroyabe et al. (2024) state that the adoption of emerging technologies such as big data, cloud computing, artificial intelligence, machine learning, and blockchain has a significant impact on innovation and productivity in companies; the ability to connect to exchange and consume data entails a greater exposure to cyberattacks.

In cyberspace, the legal issue constitutes a critical area in the contemporary context, where the intersection between technology and law poses multifaceted challenges. In this scenario, the digital environment becomes a breeding ground for threats ranging from data theft to cyber intrusion (Arboleda-López et al., 2024; Jiménez-Almeira & López; Sharma et al., 2023). It is necessary to analyze the topic of cybersecurity as a basis for formulating actions supported by computer sciences to avoid information risks and vulnerabilities (Ullah & Babar, 2022; Diam et al., 2024).

Therefore, with the ongoing cyberattacks gaining momentum every day, no person or organization, public or private, is safe from these potential crimes (Flores et al., 2021). Consequently, cybersecurity is emerging as a competency for organizational survival and growth where computer systems are increasingly complex and interconnected, creating entry points for cyber attackers (García et al., 2024).

In this context, cybersecurity emerges in organizations as a key element to ensure the confidentiality and operability of these establishments in the current environment (Garces-Giraldo et al., 2022). In this sense, the bibliometric study should allow obtaining relevant information about the publications that address cybersecurity studies and related topics, highlighting the types of publications, their impact and trends in the scientific field, and the levels and networks of participation and collaboration among the authors (Lujan-Salamanca et al., 2024; Ramírez et al., 2023).

As a method, bibliometrics is a study that allows for understanding the historical and contemporary evolution of a field of knowledge or discipline, identifying trends, gaps, and strengths in research (Nobanee et al., 2024; Hamid & Nurul, 2024; Pejic-Bach et al., 2023), addressing in this case, the collaboration networks in cybersecurity research from the discipline of computer science (Mtsweni and Thaba, 2024). Bibliometric analysis contributes to planning future research and improving the efficiency of efforts based on bibliographic evidence (Sánchez-García et al., 2024).

Obando-Ibarra et al. (2022) recommend using the last five years of indexed publications as a reference to conduct a more precise bibliometric analysis in a specific discipline. Admass et al. (2024), in turn, state that cybersecurity is applicable in different areas of knowledge or economic

sectors, such as healthcare centers, financial institutions, smart cities, network systems, government organizations, education, or the military.

There are bibliometric studies addressing topics such as the protection of digital ecosystems and sustainable development (Benaichouba et al., 2024; Sulich et al., 2023), industry management for decision-making (Ahmed et al., 2024; Oliva et al., 2024), educational environments using artificial intelligence (Ambali et al., 2024; Orosco-Fabian, 2024; Kaur et al., 2023), the maritime commercial sector (Bolbot et al., 2022), aggression and victimization in adolescents (Fernández et al., 2024), the impact of 5G technology on telecommunications (Gamboa-Cruzado et al., 2024), organizational culture of cybersecurity for the financial sector (González et al., 2023), cybersecurity perspectives drawn from the world's religions (Renaud & Dupuis, 2023), and finally, trends in digital transformation during pandemic times (Wamba et al., 2023).

There are bibliometric studies on cybersecurity and other related topics in various parts of the world; however, are there any investigations that have analyzed the scientific production of Peru and neighboring countries on the subject? Although academic institutions and research groups interested in promoting information security (Matilde-Espino & Valencia-Pérez, 2022) have been keen on generating more knowledge, cybersecurity has not been researched from the perspective of computer sciences (Chuquitucto et al., 2024).

Therefore, the main objective of this research is to quantify and analyze the available scientific activity on cybersecurity studies in the last five years, 2020-2024. The specific objectives are: to analyze productivity and collaboration networks, to determine the journals with the highest number of publications and their impact on citations, to identify related topics and the most emerging and relevant co-occurrences.

2. MATERIALS AND METHODS

2.1 Study Design

The research used the bibliometric method and, by its nature, was a descriptive quantitative study, cross-sectional in character, through the analysis of scientific publications indexed in the bibliographic databases Web of Sciences (WoS) on the topic of cybersecurity. The sample period is taken as 2020-2024, with a cutoff date for downloads until August 3, 2024. To define the normalized search term, the UNESCO thesaurus was used to identify the hierarchical conceptual relationships of "Cybersecurity" with its related term. The specification of the descriptor was related to the term "Data protection" and its identified specific terms were:

- Computer Crime
- Computer Security
- Data security
- Data privacy

The search and retrieval of information were carried out considering the fields or metadata of the document title, abstract, and keywords or descriptors. The following query was used: (((((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).

To determine the collaboration networks in research, it was considered important to use the VOSviewer software to construct and visualize the leadership of researchers (Ampofo et al., 2024) specialized in Cybersecurity and networks of co-occurrence of important terms extracted from the scientific literature on the subject.

2.2 Procedures

From the search results in WoS, 612 documents related to the topic of Cybersecurity were obtained. For the exclusion of publications that are not related to the topic, the criterion used was that all documents must belong to the category or area of knowledge of computer sciences. In Figure 1, the steps followed for the acquisition and screening of the documents analyzed in this research through a systematic review using the PRISMA methodology (Valdiviezo et al., 2024) can be seen to ensure that the data from the journal publications are adequate and relevant.

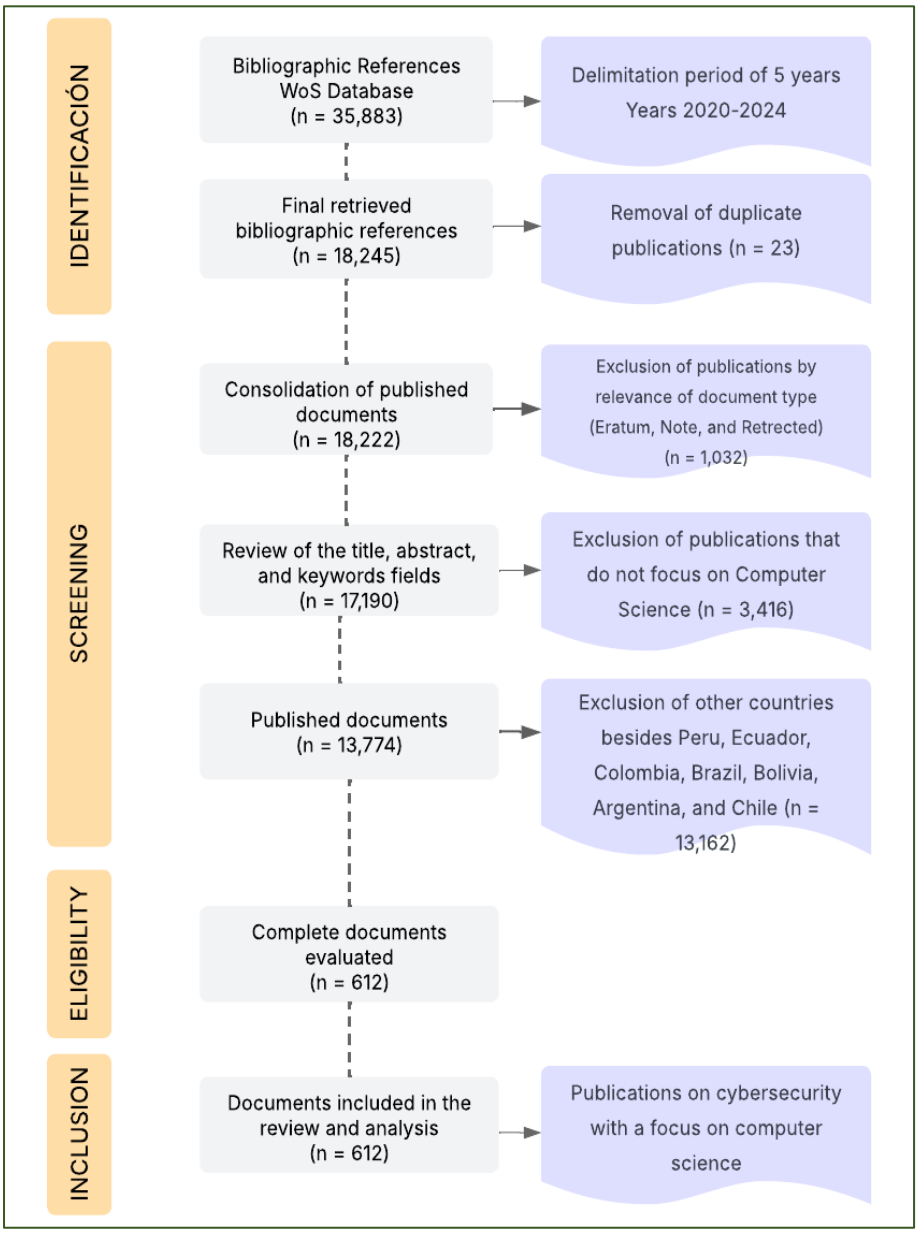

Figure 1. Flowchart of bibliographic records under the PRISMA model

3. RESULTS

3.1 Productivity and Collaboration Networks in Cybersecurity

The evolution of scientific production on cybersecurity in Peru, in recent years, including the pandemic period, compared to other neighboring countries, has not increased.According to Table 1, this country is in fifth place with only 2.7% productivity, and it is only ahead of Argentina and Bolivia by a minimal difference of two publications. However, it could be much better. A few years ago, the production of some countries in these areas was nascent. However, now they are beginning to generate a greater number of publications, as is the

case with Colombia at 10.2%, Ecuador at 8.8%, and Chile at 7.6%.

Table 1. Number of documents published on cybersecurity by country

Countries	Period						
	2020	2021	2022	2023	2024	Total	%
Brazil	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
Peru	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%

Note. The number of publications increases from 612 to 628 because some documents were prepared in collaboration with two or more countries.

Regarding Brazil, it has achieved a significant 68.2% productivity development in cybersecurity topics from the perspective of computer sciences. This increase has been sustained over the five years of analysis. Undoubtedly, its university population, fully dedicated to research to protect all types of information generated by society, plays a crucial role (Ambali et al., 2024). However, this positive development in research is also due to clear and sustainable public policies (Arboleda-López et al., 2024; Jiménez-Almeira & López, 2023; Sharma et al., 2023).

Before conducting a general analysis of all the countries in the sample, it is necessary to describe the productivity of Peruvian authors, or those affiliated with Peruvian institutions who have published on cybersecurity. In Table 2, it can be seen that Ramirez-Asis holds the first place with two publications and 12 citations; however, Casavilca Silva, with only one publication, has obtained 44 citations. The same applies to Bravo and Libaque-Saenz, who are co-authors and their publication has received 36 citations. This means that the publications of Peruvian authors have a significant impact in the scientific field.

Table 2. The ten Peruvian authors with the highest number of published documents on cybersecurity

Peruvian authors	Main affiliation	Peruvian authors		
		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=Number of publications, NC=Number of citations, and H-Index = Number of publications that have been cited at least h times (WoS).

From a general perspective, Table 3 presents the list of authors with the highest number of indexed publications, where the productivity of Joel Rodrigues stands out, with 45 documents, having so far achieved 898 citations, making him the researcher with the greatest impact in the field of cybersecurity, with an H-index of 80. Likewise, other authors follow in their footsteps. It is necessary to highlight the work carried out by Cristiano Andre Da Costa, who, with just 6 publications, has received 353 citations, demonstrating the quality of the content in his research.

Table 3. The ten authors with the highest number of published documents on cybersecurity

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

NP = Number of publications, %A = Percentage of articles of all publications, NC = Total citations received by all documents since their publication, and H-Index = Number of publications that have been cited at least h times (WoS).

The authors' high impact factor, evidenced by the substantial number of citations garnered from a relatively limited number of publications, underscores the growing interest of the scientific community in computer sciences and computer engineering. This trend is particularly notable in the study of cybercrime, which affects diverse sectors such as businesses, governments, and individuals, as highlighted by Chuquitucto et al. (2024). It is important to note that all authors featured in the ranking consistently publish in peer-reviewed journals, which are also referred to as refereed journals, ensuring the high quality of research content

Figure 2 shows the collaborative work of the researchers in 5 nodes, the most important one is led by Joel J. P. C. Rodrigues, who in turn collaborates permanently with the other three clusters represented by Victor Hugo C. De Albuquerque from the mustard node, Khan Muhammad from the blue node, and Mario Proenca from the purple node; in the case of the cluster led by Michele Nogueira, they are only in the research network collaborating with Paolo Bellavista, who is part of the blue cluster.

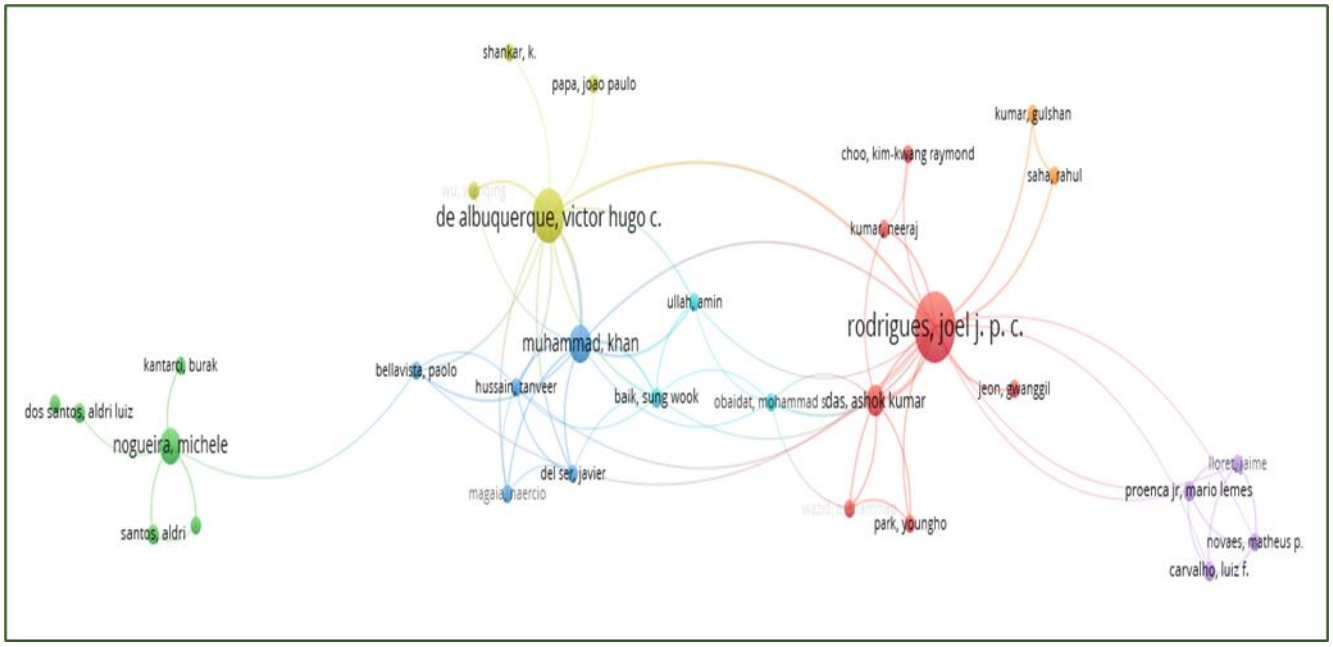

Figure 2. Personal co-authorship map of published documents on Cybersecurity

The trends in collaboration networks are influencing the work of researchers in the face of the challenges of internationalizing their research work and seek to redefine research processes. Valencia-Arias et al. (2020) highlight the need for multidisciplinary and cross-border collaboration, meaning that participation in groups of researchers aligned with these cybersecurity topics should allow, among other things, to develop and reflect together for the production of scientific knowledge.

That is why international collaboration, which represents greater interest among researchers, coordinates efforts with countries that have consolidated national science and technology systems. For Peru and other Latin American countries, this is a tool to optimize resources and have greater opportunities in funding and, consequently, achieve better research results in terms of quantity and impact, as proposed by Muñoz et al. (2023).

In the Peruvian context, Table 4 reveals that all institutions publishing indexed documents on cybersecurity related to computer sciences are universities. As Matilde-Espino and Valencia-Pérez (2022) emphasize, academia bears the responsibility to further promote research, and generate new knowledge within the educational process of students on this subject, particularly in engineering programs.

Table 4. Peruvian institutions with the highest number of publications on cybersecurity

Peruvian institutions	Publications
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
Universidad Nacional Federico Villarreal	1
Universidad Nacional Hermilio Valdizan	1
Universidad Nacional Mayor de San Marcos	1

Universidad Nacional Pedro Ruiz Gallo	1
Universidad Peruana Cayetano Heredia	1
Universidad Peruana de Ciencias Aplicadas	1
Universidad San Ignacio de Loyola	1
Universidad señor de Sipán	1
Universidad Tecnológica del Perú	1

In this regard, Figure 3 shows a map of cooperation between institutions, mainly Brazilian universities that, in most of the clusters, take the lead in collaboration networks with other universities in South America and Europe. Among the most representative clusters are the University of Sao Paulo (mustard color), Federal University of Minas Gerais (pink) which collaborates as the Polytechnic University of Valencia, Federal University of Ceara, which has been publishing with authors affiliated with the Pontifical Catholic University of Chile; Federal University of Rio de Janeiro, which publishes its research with the University of Salamanca and University of Alicante, and finally, the Federal University of Santa Catarina, which works in collaboration with authors from the National University of Colombia.

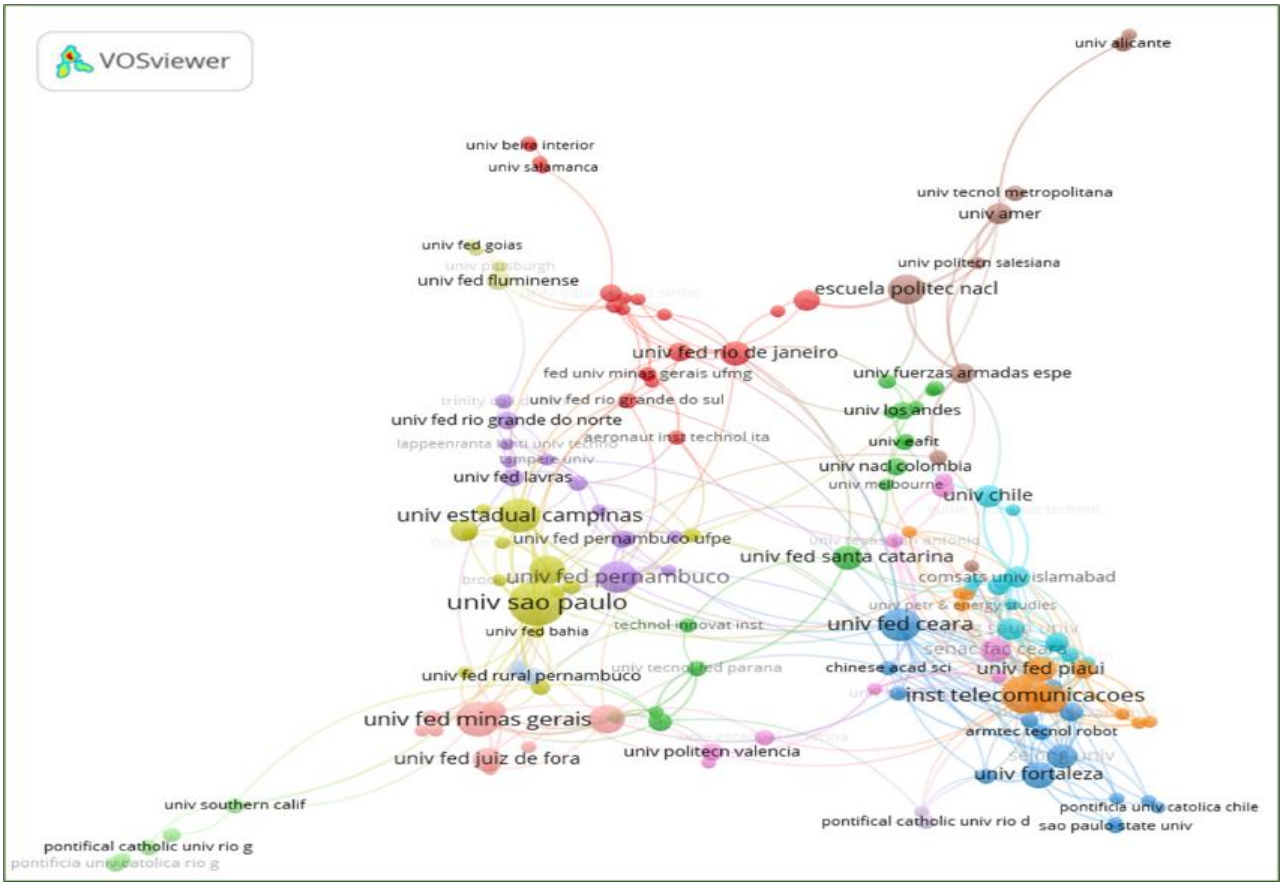

Figure 3. Institutional co-authorship map of documents published on Cybersecurity

One of the requirements set by indexing databases for inclusion in their collections is that publications have international collaborations. Truong & Nguyen (2024) argue that, to achieve a considerable increase in scientific production on the topic of cybersecurity, academic institutions must give greater importance in their various curricula to those disciplines where technology is the subject of study. This statement is agreed upon since the majority of institutions conducting this type of study are universities.

Similarly, Figure 4 illustrates the collaboration between countries, particularly Peru, where authors are conducting research with their international counterparts. The largest collaboration network is represented by the purple cluster led by Brazil, which includes several institutions from South Korea. Next is the red cluster represented by the United States, which collaborates with England, Nigeria, Jordan, and Argentina. Portugal, from the blue node, collaborates with several Asian countries such as India, Pakistan, and Saudi Arabia, as well as with Peru. The green node, led by Colombia, promotes a network of researchers that includes other South American countries such as Ecuador and Chile. Finally, the mustard node encompasses Canada and Australia.

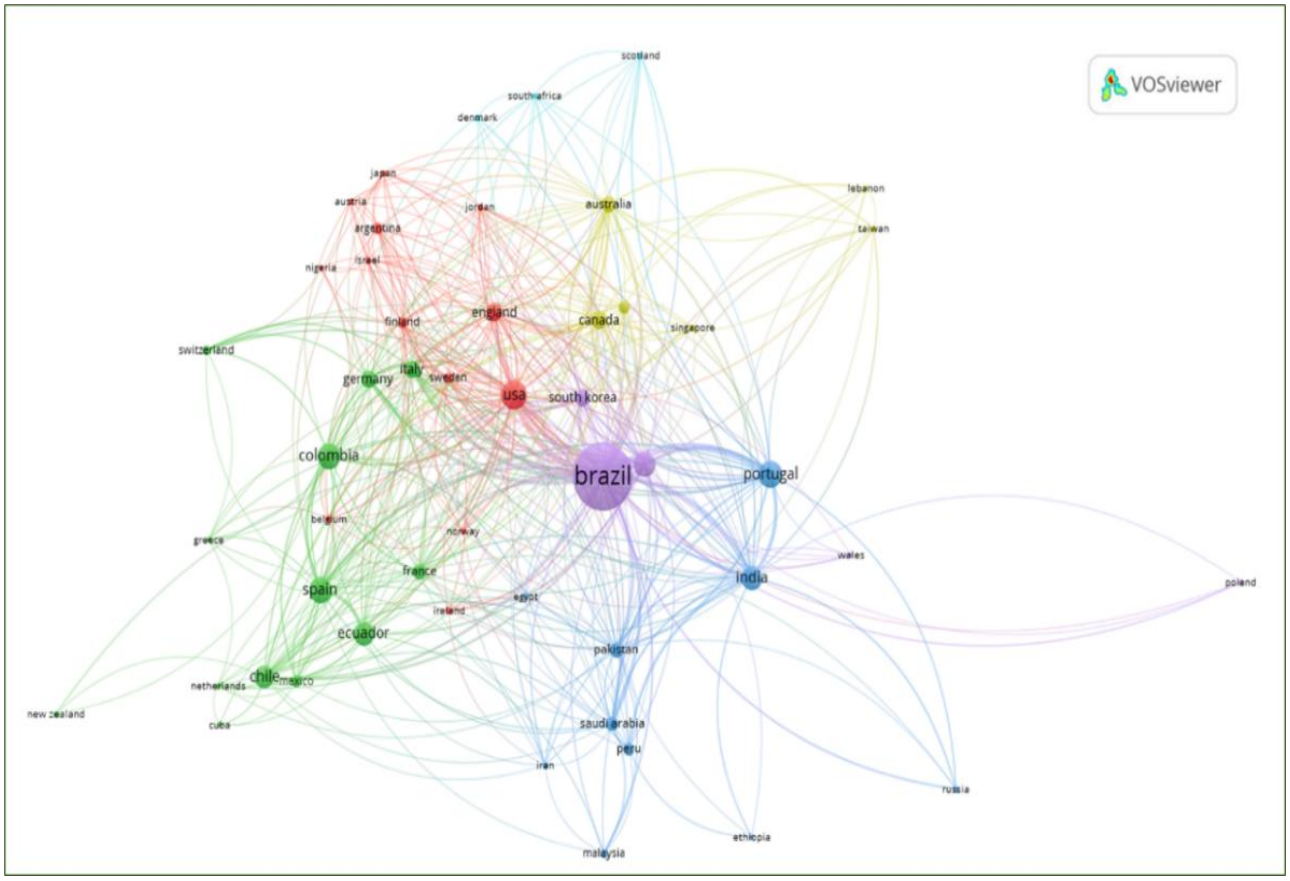

Figure 4. Map of institutional co-authorship by countries of documents published on Cybersecurity

These represent the authors' affinities for teamwork and the already established or formed collaboration networks between institutions from different countries. Prümmer et al. (2024) state that the problems involving cybersecurity are similar or have the same characteristics in all countries; they are just different contexts, and the solution applies to all realities regardless of geographical aspects. This is corroborated by the results obtained.

3.2 Scientific journals with the highest number of publications and their impact

According to Table 5, the journal with the highest number of publications and impact is "IEEE Access," published by IEEE-Inst Electrical Electronics Engineers Inc, which operates in the United States with 131 publications on cybersecurity and 1475 citations received, this journal ranks first, with an average of 4 authors per publication and 11 citations received per document. It is evident that these results demonstrate that this type of journal specialized in the field of computer science, and addressing the topic has gained preference in the scientific community.

Table 5. The fifteen journals with the highest number of published documents on Cybersecurity

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

NP = Number of publications, %NP = Percentage of the total publications (NP*100/612), NA = Number of authors of all publications, NAP = Number of authors per publication (NA/NP), NC = Total citations received by all documents since their publication and NCP = Number of citations per publication (NC/NP).

Valencia-Arias et al. (2020) confirm that a rigorous peer review process is also important to generate trust in the scientific process among science policy makers. The experience in reviewing scientific articles produces a keen sense for novel, innovative, rigorous, and advancing research in the field. Mtsweni & Thaba (2024) add that, for authors, publishing their research in prestigious journals, with peer review evaluation methods, recognizes the rigor and impact of their study, and they consider it necessary to advance their research career, and obtain funding for their research. Both are agreed upon, as peer review is deeply rooted in the scientific process, and allows the authors' ideas, methods, data, findings, and conclusions to be evaluated and rated with a quality standard.

Table 6 shows the published documents that have received the highest number of citations on Cybersecurity. The first place in the ranking, with 186 citations received, is held by is held by the one tittled "End-to-end privacy preserving deep learning on multi-institutional medical imaging," which is a scientific article published by the journal Nature Machine Intelligence from Germany; this publication was disseminated in the year 2021. A higher citation count increases the likelihood of receiving more citations and paves the way for future research in an author's work.

Table 6. The fifteen most cited titles of documents published on Cybersecurity

Rank	NC	Title	Journal	Type of Publication	Country	Year
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 citations received by the published document.

The prestige of their researchers, the rigor of the studies, and the continuous publication of results are important factors in the visibility and impact of a journal. In current terms, Hamid & Nurul (2024) assert, this is reflected in the number of citations that the articles receive. Likewise, the impact a publication has on society is reflected in how it has shaped public opinion and contributed to the generation of new knowledge, influencing the decision-making of officials and political authorities.

3.3 Most relevant topics currently being developed around Cybersecurity

Regarding the descriptors or keywords used by indexed publications to describe their content, Figure 5 shows that the main term, or the most frequently mentioned term in the thematic map, is 'Security.' This term heads the orange cluster and is associated with authentication and encryption in information systems, as well as access control to databases in companies and industries, emphasizing their relevance within the framework of computer science. Complementing this is the green node 'Machine Learning,' which relates to the field of Artificial Intelligence. It involves the

development of algorithms in computers capable of identifying patterns in massive data, making predictions, and analyzing Big Data, in agreement with Kaur et al. (2023).

Then there is the red cluster led by the term Cybersecurity, which encompasses subtopics such as computer protocols, intrusion detection, and information system security, among others. Finally, the term Blockchain, which frames the topics of mathematical formulas, data storage, and security patterns, where Ampofo et al. (2024) revealed the research trends and the future direction of blockchain technology in cybersecurity, asserting that interdisciplinary collaboration will be key for future advancements in this technology.

By mapping the existing literature, identifying emerging themes, highlighting frequently cited works, and identifying research gaps, it inspires new similar studies, ensuring they are based on solid work while simultaneously they are opening new thematic pathways fundamental to the development of the discipline. This also allows new researchers in the field to understand the landscape or context, meet and connect with leading researchers in the field, and identify potential collaboration opportunities (Chuquitucto et al., 2024; Matilde-Espino & Valencia-Pérez, 2022; Valencia-Arias et al., 2020).

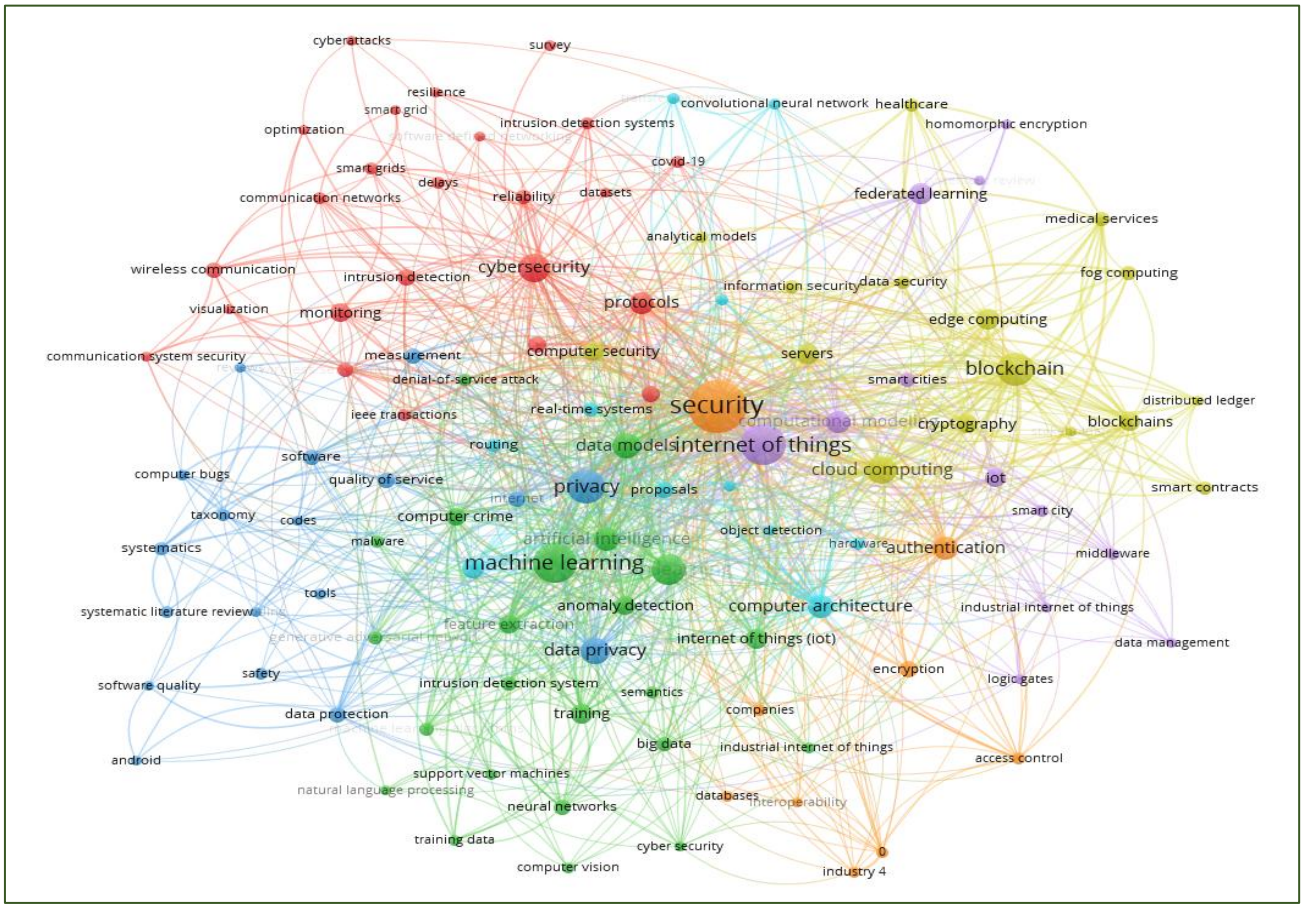

Figure 5. Co-occurrence map of topics in documents published on Cybersecurity

Finally, regarding the limitations of the study, the obtained results should be interpreted considering that the only source of information was the WoS bibliographic database. Other databases such as Scopus, Scielo, PubMed, among others, were not used, and they could have provided results with greater scope or coverage of productivity and collaboration networks in cybersecurity.

CONCLUSIONS

Regarding Peru's scientific production, the number is minimal, and it is necessary to promote research on this topic in universities. The research collaboration networks with individual and institutional authors have shown joint work belonging to several countries, especially Brazil, whose results are reflected in the number of publications and citations received over the past 5 years. The top 10 journals with the highest number of publications on the topic and the publications with the highest number of citations were identified, thus demonstrating their impact and positioning in the scientific field. The co-occurrence of keywords or descriptors of the various themes surrounding cybersecurity was identified, such as data security, the use of security protocols for access to information systems, machine learning, blockchain, among others.

In this sense, it is suggested to expand the study by using other bibliographic databases, as well as the use of other related variables that help to understand the various themes and situations revealed by the study. It is crucial that future research continues to investigate the development and impact of cybersecurity from different approaches, as the field of technology is constantly innovating.

FINANCING

The authors did not receive any funding to conduct this study-article.

CONFLICT OF INTEREST

The authors declare that they have no conflicts of interest related to the development of the study.

AUTHORSHIP CONTRIBUTION

Conceptualization: Cuya-Chamilco, P. V.; Methodology: Mescua-Ampuero, L. E.; Software: Saavedra-Villar, P.; Data curation: Cáceres-García, A. A.; Validation: Alvarado-Flores, J.; Formal analysis: Cuya-Chamilco, P. V., Mescua-Ampuero, L. E., Saavedra-Villar, P., Cáceres-García, A. A., & Alvarado-Flores, J.; Writing - original draft: Cuya-Chamilco, P. V.

REFERENCES

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 Tecnologias 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/businessreview/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 cybertechnology 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., Adauto, 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 Tecnologias 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 Informação*, (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., Huillca, 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