Data and Metadata. 2025; 4:1109
doi: 10.56294/dm20251109

ORIGINAL

Strengthening cyber resilience in universities using artificial intelligence for proactive threat detection

Fortalecimiento de la resiliencia cibernética en universidades mediante inteligencia artificial para la detección proactiva de amenazas

Carina Del Rocio Cevallos Ramos[1], Fausto Francisco Navarrete Chávez[1], Fernando Ricardo Márquez Sañay[1], Mauro Patricio Andrade Romero[1]

[1]Escuela Superior Politécnica de Chimborazo (ESPOCH). Riobamba, Ecuador.

Cite as: Cevallos Ramos CDR, Navarrete Chávez FF, Márquez Sañay FR, Andrade Romero MP. Strengthening cyber resilience in universities using artificial intelligence for proactive threat detection. Data and Metadata. 2025; 4:1109. https://doi.org/10.56294/dm20251109

Submitted: 17-10-2024 **Revised:** 24-03-2025 **Accepted:** 11-07-2025 **Published:** 12-07-2025

Editor: Dr. Adrián Alejandro Vitón Castillo

Corresponding Author: Carina Del Rocio Cevallos Ramos

ABSTRACT

The data used by companies for decision making are exposed to various risks that can compromise their security. In this context, it is essential to identify tools to detect and manage these risks. Therefore, the main objective of this research was to conduct a bibliometric analysis aimed at assessing the development of scientific literature on the application of cyber resilience in universities using artificial intelligence for proactive threat detection. To achieve this purpose, the Scimago portal, specialized in the analysis of scientific production, was used. The study reviewed the distribution of quartiles using bibliometric indicators such as the H-index, journal impact factor, number of published documents, average citations per document, international scientific collaboration, and citations from public funding entities. Likewise, the number of articles cited in the most relevant journals of each quartile was evaluated in order to assess the importance of scientific innovation in improving proactive threat detection through cyber resilience. The results show that most of the scientific production is concentrated in journals belonging to countries with high technological development, especially in the areas of threat detection and application of artificial intelligence. However, there is a low diffusion of research related to cyber resilience in universities through artificial intelligence. which suggests the need to increase investment in science and technology, considering the high risk of cybersecurity attacks to which these institutions are exposed.

Keywords: Threats; Cybersecurity; Data; Artificial Intelligence; Resilience.

RESUMEN

Los datos utilizados por las empresas para la toma de decisiones están expuestos a diversos riesgos que pueden comprometer su seguridad. En este contexto, resulta indispensable identificar herramientas que permitan detectar y gestionar dichos riesgos. Por ello, el objetivo principal de esta investigación fue realizar un análisis bibliométrico orientado a conocer el avance de la producción científica sobre el uso de la resiliencia cibernética en universidades, mediante inteligencia artificial, para la detección proactiva de amenazas. Para alcanzar este propósito, se recurrió al portal Scimago, especializado en el análisis de producción científica, y se efectuó una revisión de la distribución de cuartiles utilizando indicadores bibliométricos como el índice H, el factor de impacto de las revistas, el número de documentos publicados, el promedio de citas por documento, la colaboración científica internacional y las citas de entidades financiadoras públicas. Asimismo, se evaluó el número de artículos citados en las revistas más relevantes de cada cuartil con el fin de valorar la importancia de la innovación científica en la mejora de la detección proactiva de amenazas mediante resiliencia cibernética. Los resultados muestran que la mayor parte de la producción científica se concentra en revistas pertenecientes a países con alto desarrollo tecnológico, destacando especialmente las áreas de detección de amenazas y aplicación de inteligencia artificial. Sin embargo, se observa una baja difusión de investigaciones relacionadas con la resiliencia cibernética en universidades a través de inteligencia artificial, lo cual evidencia la necesidad de incrementar la inversión en ciencia y tecnología, considerando el elevado riesgo de ataques a la ciberseguridad al que están expuestas estas instituciones.

Palabras clave: Amenazas; Ciberseguridad; Datos; Inteligencia Artificial; Resiliencia.

INTRODUCTION

Today, security threats are not limited to the physical realm, but include a growing variety of cyber-attacks, ranging from cyber-bullying and information theft to hacking of public domains. These actions represent a high risk for universities, as they compromise the integrity of their data and generate serious consequences both in the academic environment and in the security of the users of educational institutions. In view of this scenario, it is urgent to implement strategic actions aimed at minimizing these risks and strengthening the protection of university information systems.(1,2)

In the university context, this type of threat is increasingly recurrent, making it essential to implement cybersecurity measures, such as data encryption. Although these actions have proven to be effective, it is necessary to explore more innovative alternatives, such as cyber resilience. However, despite its relevance, scientific advances remain limited, especially considering the low number of publications in high-impact journals that specifically address this topic.(3,4)

Despite cybersecurity measures and legal actions, IT risks will always exist, so universities must have resilience, understood as the ability to recover from a disturbance, whose principles can be applied in the field of cybersecurity, so as to design strategies against actions that compromise data and make public and private institutions more vulnerable every day.(5,6)

Given that research attention on this topic has decreased, an effective way to evaluate measures to improve resilience at the university level and its impact on cybersecurity is to analyze how scientific production has evolved in this context. This is consistent with the social responsibility of universities, including their role in cybersecurity, as the derived innovations can serve as tools to strengthen IT security in public and private domains.(7,8)

To evaluate scientific production, one of the most appropriate tools is bibliometric analysis, since it provides quantitative information on the topic under study. This type of analysis makes it possible to review specialized databases, apply bibliometric indicators and perform systematic searches using keywords. Such a process is the first step in examining advances in technological innovations in the field of cybersecurity, where scientific production is often closely linked to the progress of such innovations.(9,10)

Considering the above, the objective of the research was to evaluate whether there is currently a strengthening of cyber resilience in universities through artificial intelligence for the proactive detection of threats, which was verified through a bibliometric analysis based on the premise that if there is indeed a consolidation of this tool for the detection of threats, it will be reflected in greater scientific productivity.

METHOD

The methodology, as already indicated, consists of the application of a bibliometric and bibliographic content analysis on the strengthening of cyber resilience in universities through artificial intelligence for the proactive detection of threats. The combination of both typologies allows to analyze, measure and identify bibliographic data and relevant aspects of scientific publications on a given topic. The methodology is based on several steps, such as: search of bibliographic references in databases and filtering by keywords and period.

Bibliometric analysis

The quantitative analysis of the information was carried out under a bibliometric approach of the scientific production on the strengthening of cyber resilience in universities through artificial intelligence for proactive threat detection. Also, from a qualitative perspective, examples of some research papers published in the aforementioned area of study are analyzed from a bibliographic approach to describe the position of different authors regarding the proposed topic. The search was carried out using the Scimago database to determine through keyword analysis the scientific productivity in terms of the number of article cited in the last year (figure 1).

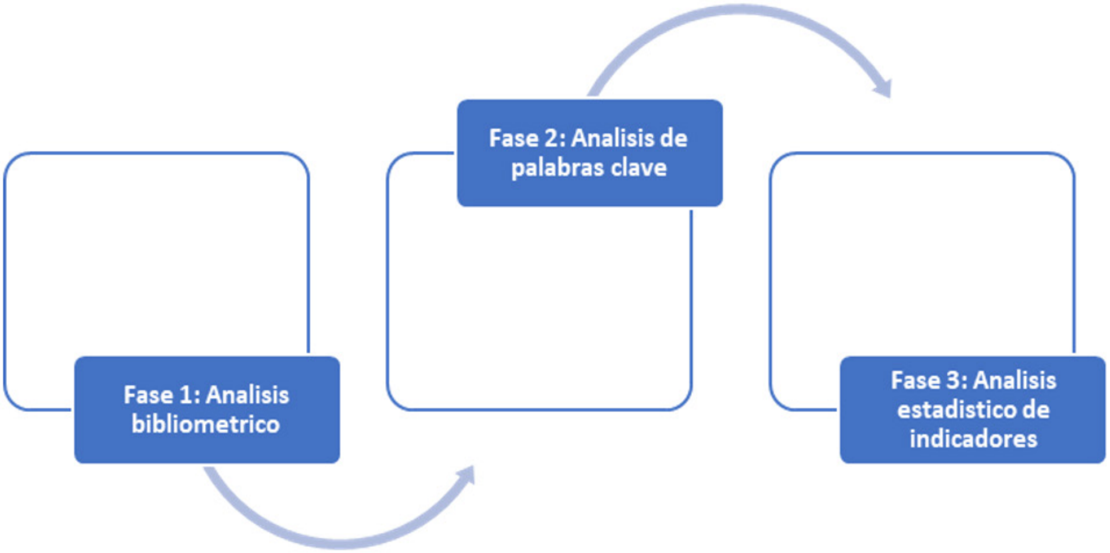
Fase 1: Analisis bibliometrico
Fase 2: Analisis de palabras clave
Fase 3: Analisis estadistico de indicadores

Figure 1. Methodological design

Search for information

For the development of the present research the documentary exploration, referring to the scientific production on the strengthening of cyber resilience in universities through artificial intelligence for the proactive detection of threats, was done by identifying the existence of similar works with objectives and other aspects of relevance, using artificial intelligence as search keywords in each journal, threats, risks, resilience and cybersecurity, whose concepts defined in table 1, are linked to the bibliometric indicators, given that they are generated from them, particularly in relation to the results that serve to compare the scientific production by search terms, carried out in the journals with the highest impact according to their bibliometric indicators.

Table 1. Definition of terms used to search for scientific information for bibliometric analysis

Term	Definition
Artificial intelligence	Refers to the ability of machines to simulate human intelligence, enabling them to perform tasks that normally require human intervention, such as learning, problem solving.
Threat	Physical or virtual event of natural origin, or caused, or accidentally induced by human action, occurring with suficient severity to cause loss of life, injury or other health impacts, as well as damage and loss to assets, infrastructure.
Risks	Probability that a hazardous event or situation will materialize and cause negative consequences.
Resilience	A person’s ability to adapt and recover from difficult, adverse or traumatic situations and emerge stronger from them.
Cybersecurity	Set of practices, technologies and processes designed to protect computer systems, networks, devices and data against digital attacks and unauthorized access.

To obtain the bibliographic data, the Scopus databases were used, since they are one of the main databases of academic information worldwide. This analysis is carried out in two stages: the first is a general search, and the second is a search by country. First, a search string was established within the “article title” field “abstract” and “keywords” with the following terms established in English and entered with quotation marks artificial intelligence, threats, risks, resilience, cybersecurity, cybersecurity (table 2).

Table 2. Parameters used in the analysis

Dimensions	Indicators
Database	Scopus
Time period	2019-2024
Search date	2025
Language	English - Spanish - Portuguese
Type of document	Journal articles, book chapters
Search field	Title of publication
Search term	artificial intelligence, threats, risks, resilience, cybersecurity, cybersecurity
Unit of study	Definitions, countries, authors, journals, documents, keywords and relevant topics.
Results	1500 documents.
Analysis parameters	Authors, Countries, Journals, Documents, Keywords, Relevant topics, Relevant topics

Techniques used to select journals for the bibliometric analysis

The bibliographic search and localization of journals was carried out by analyzing the main bibliometric indicators obtained from Scimago, such as H index, journal impact factor, number of documents, citations per document, international scientific collaboration and citations from public planners.

H-index: the H-index expresses the number of journal articles (H) that have received at least H citations. It quantifies both the scientific output and the scientific impact of the journal; it also applies to scientists and countries.

Journal impact factor: represents the weighted average number of citations received in the selected year for papers published in the chosen journal during the previous three years.

Number of papers: number of papers published by a journal in the selected year. All types of documents are considered, both citable and non-citable.

Citations per paper: number of citable papers published by a journal in the three years prior to the selected year (papers from the selected year are excluded). Only articles, reviews and conference papers are considered.

International scientific collaboration: list of papers whose affiliation includes more than one country address.

Public planner citations: number of documents cited by public policy documents according to the Overton database .

Subsequently, a comparative and bibliometric analysis was carried out to assess the relevance of the main journals in the area of economic sciences, with the purpose of determining their impact on scientific production related to topics such as artificial intelligence, threats, risks, resilience and cybersecurity.

Inclusion criteria

The journals indexed in Scimago were considered, taking into account the key terminology used during the information search. For this purpose, words such as *artificial intelligence*, *threats*, *risks*, *resilience* and *cybersecurity* were used, limiting the results to English-language articles related to scientific production on strengthening cyber resilience in universities through the use of artificial intelligence for proactive threat detection. The analysis focused exclusively on digital journals included in the Scopus database, considering active publications in the period between 2019 and 2024.

Exclusion criteria.

Publications that deviated from the content of this study or were not indexed in Scopus were not considered. Publications that lacked a scientific base and reference databases derived from products that did not correspond to publications during the search period or that by the time of analysis were not active in Scopus were excluded.

Analysis of the information

Once the clusters were identified, six journals were randomly selected for each quartile, which are presented in table 1. These journals were subsequently analyzed according to the bibliometric indicators provided by the Scimago database. To evaluate possible differences between quartiles, an analysis of variance (ANOVA) was applied. In cases where significant differences were identified with a probability level of 5 %, mean comparison tests were performed using Tukey's test, using InfoStat statistical software.

Additionally, multivariate statistical techniques were used, specifically principal component analysis (PCA), in order to contrast the results obtained with the quartile classification reported in Scimago, which is a technique used to describe a set of data in terms of new uncorrelated variables ("components"), which are ordered by the amount of original variance they describe, so the technique is useful to reduce the dimensionality of a set of data and explain which are the factors that explain such variation in this case the bibliometric indicators.

Journal selection process

As a result of the visualization of Vosiewer, the clusters formed according to the importance of the journals stored in this program are shown in figure 2, where 6 clusters can be distinguished, with the yellow color representing the most relevant journals.

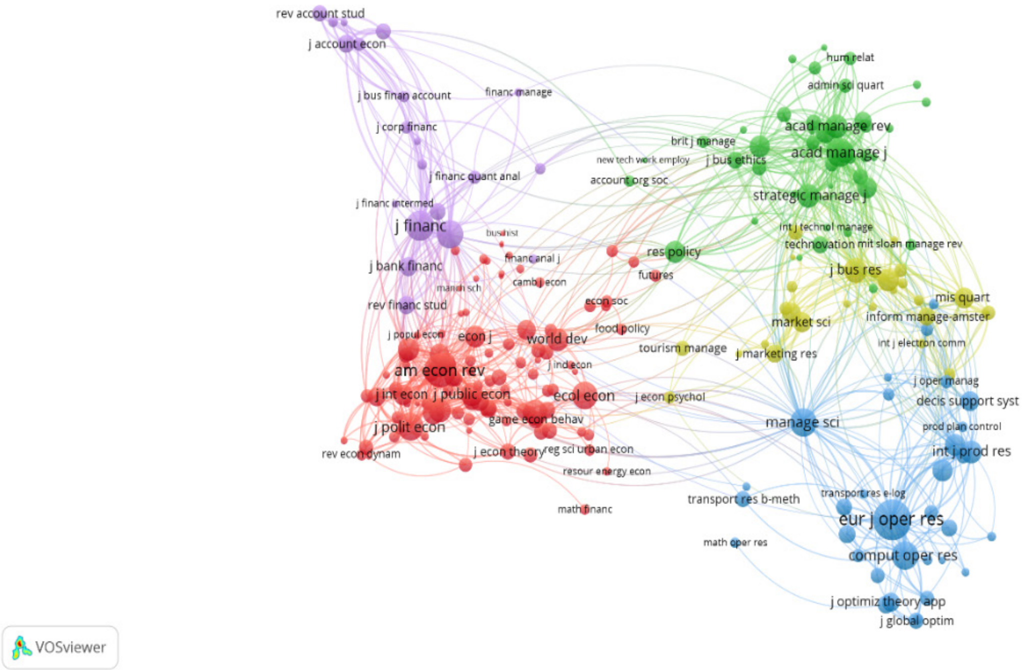

Figure 2. Clusters visualized in VOSwiewer program

Once the clusters were identified, 4 journals were selected for each cluster. The screening process is described below, which was based on a selection from the 272 journals visualized in VOSviewer, which constitutes the size of the population according to their impact factor, and from which 24 were selected to constitute the sample to which the bibliometric analysis was performed.

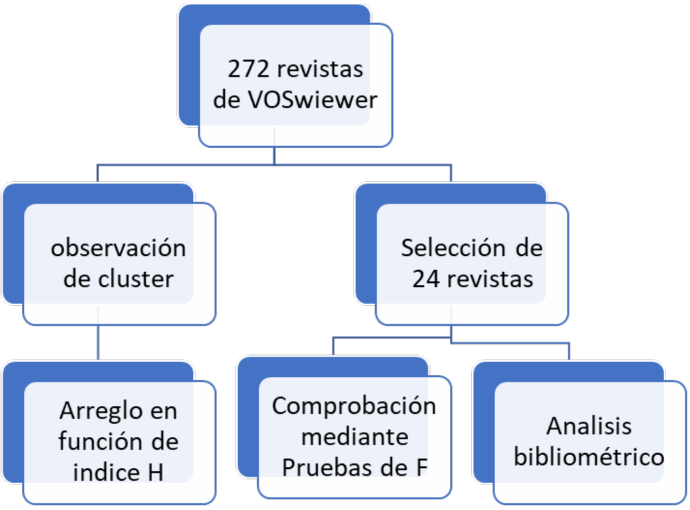
272 revistas de VOSwiewer
observación de cluster
Selección de 24 revistas
Arreglo en función de indice H
Comprobación mediante Pruebas de F
Analisis bibliométrico

Figure 3. Journal selection process for bibliometric analysis

After the selection of the sample of 24 journals out of the 272 observed in VOSviewer, which were subsequently analyzed, F tests were carried out based on the bibliometric indicators derived from Scimago such as H index, journal impact factor, number of documents, citations per document, international scientific collaboration and citations from public planners, which prove that there are differences by country and quartile, which ratifies that the screening process was adequate (table 3).

Table 3. Statistical analysis based on F-value to verify the screening process

Factor	Quartile	Country
SJR	0,035*	0,0043**
IH	0,808	0,0001**
DT	0,8886	0,0597
CPD	0,045*	0,0001**
CI	0,7230	0,2744
OV	0,6607	0,0001**

(SJR): journal Impact Factor (IH): H. index, DT: number of papers: number of papers published by a journal in the selected year, (CPD): citations per paper: number of citable papers published by a journal in the three years prior to the selected year, (IC): international scientific collaboration: list of papers whose affiliation includes more than one country address, (OV): citations of public planners according to the Overton database.

RESULTS

When analyzing the scientific production on strengthening cyber resilience in universities through artificial intelligence for proactive threat detection, in terms of journals in the area of computer science indexed in Scopus, the results show in figure 4, that the majority correspond to Europe and North America with 929 and 576 journals, while less production was observed in Latin America with 28 journals and Africa with less than 10 publications.

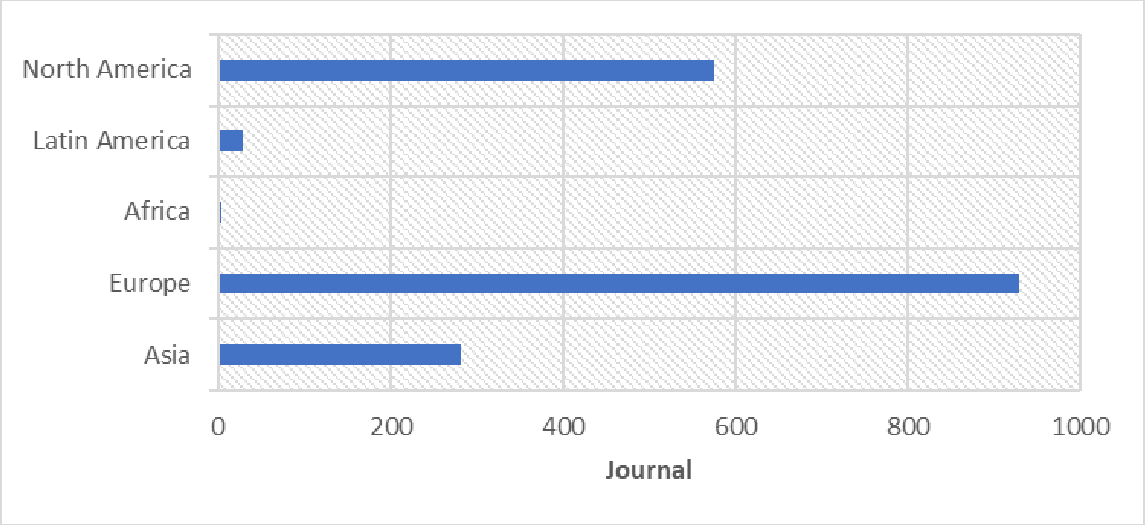

Figure 4. Scientific production on Strengthening cyber resilience in universities through artificial intelligence for proactive threat detection

Once the scientific production was randomly identified, 6 journals were selected for each cluster, as shown in Table 4, which were subsequently analyzed according to bibliometric indicators derived from Scimago, such as H index, journal impact factor, number of documents, citations per document, international scientific collaboration and citations from public planners.

When analyzing scientific production by region, figure 5 shows that most of the Q1 journals (higher H index) are concentrated in the USA and China, which correspond to the journals with the highest visibility in the area of computer science, while the lowest scientific relevance (lower H index) are located in African countries such as Egypt, South Africa, Tunisia, Morocco and Algeria and in Latin America such as Brazil, Mexico, Chile, Colombia and Argentina.

Table 4. Journals selected for bibliometric analysis quartiles visualized in Scimago portal

Q1	Q2	Q3	Q4
International journal of information management	Journal of the Brazilian computer society	Chilean journal of law and technology	South African computer Journal
ACM computing service	Online learnign journal	Journal of internet service and Applications	Menoufa Journal of electronic engineering research
Journal of Operation management	Journal of cryptology	Uniciencia	Journal of machine and computing
Nature computational Science	EPJ data Science	Inteligence and robotics	Free text
Computer Science Review	Joournla of information system	Formla aspext of computing	Transinformatica
Information Fusion	Journal of artificial inteligence and tecbologies	Journal of computing sccioence and tecbhology	Data anbd metada

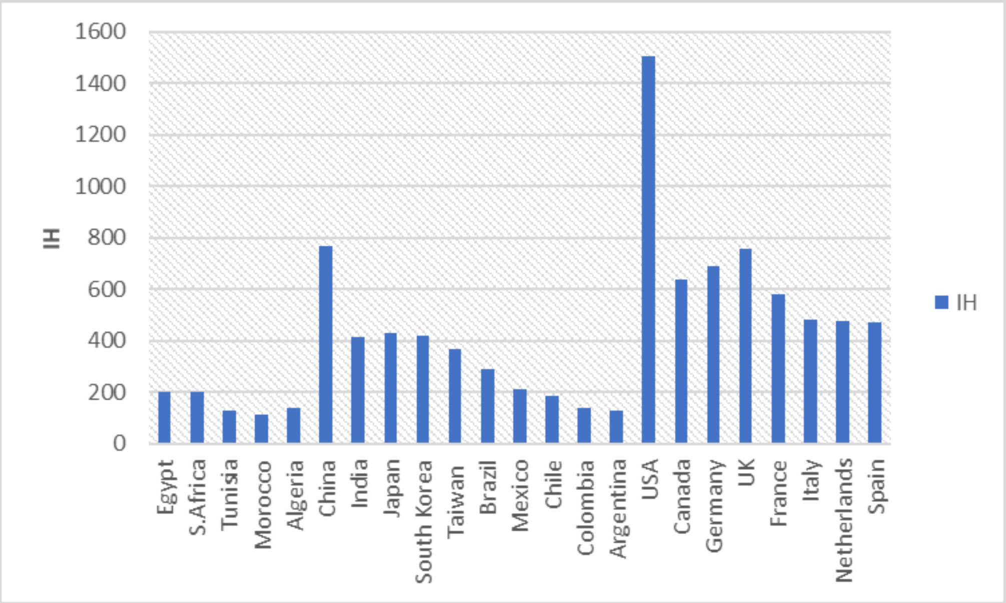

Figure 5. Distribution of scientific publications by regions and countries according to the H index

The results obtained confirm, as previous research has shown, the relevance of computer sciences in high-impact scientific production. This finding highlights the growing importance of cyber resilience in universities, especially when artificial intelligence is applied for proactive threat detection. To deepen this line of analysis, a bibliometric study was conducted based on information collected from the Scimago portal, considering indicators such as H-index, journal impact factor, number of published papers, average number of citations per paper, international scientific collaboration and citations from public funding entities. The results of this analysis are presented in table 5.

Table 5. Summary of bibliometric analysis of selected journals

Journal	Quartile	SJR	IH	DT	CPD	CI	OV	Country	Classi
1	1	6,26	196	334	33,30	44,71	2	UK	Q1
2	1	5,79	232	424	39,89	47,17	8	USA	Q1
3	1	452	228	61	11,05	54,10	0	NET	Q1
4	1	3,47	40	160	6,81	23,13	0	US	Q1
5	1	327	68	59	18,39	45,76	1	US	Q1
6	1	413	179	510	22,65	45,49	2	NET	Q1
7	2	0,36	25	43	2,52	11,63	0	BRA	Q2
8	2	0,82	75	74	3,03	13,51	0	US	Q2
9	2	0,79	85	39	2,5	64,1	0	US	Q2
10	2	0,74	50	75	3,17	40	0	US	Q2

11	2	0,73	48	22	2,46	54,55	0	US	Q2
12	2	0,71	19	39	6,82	25,64	0	US	Q2
13	3	0,41	7	19	0,48	0	0	CHI	Q3
14	3	0,41	34	39	1,41	12,82	0	BRA	Q3
15	3	0,24	9	34	0,73	23,53	0	CR	Q3
16	3	0,55	10	22	2,81	19,18	0	US	Q3
17	3	0,46	45	26	1,59	42,31	0	US	Q3
18	3	0,46	63	64	1,64	23,44	0	US	Q3
19	4	0,19	12	15	1,2	18,33	0	SA	Q4
20	4	0,18	6	11	0,87	45,45	0	EGYP	Q4
21	4	0,15	20	111	7,8	27,93	0	KENY	Q4
22	4	0,22	10	44	0,73	27,27	0	BRA	Q4
23	4	0,20	15	30	0,65	21,05	0	BRA	Q4
24	4	0,21	20	240	1,28	19,58	1	ARG	Q4

(SJR): journal impact factor (IH): H index, DT: Number of papers: number of papers published by a journal in the selected year, (CPD): citations per paper: number of citable papers published by a journal in the three years prior to the selected year, (IC): international scientific collaboration: list of papers whose affiliation includes more than one country address, (OV): citations from public planners according to the Overton database.

The results in table 5 confirm the relevance of the scientific publications that were visualized as Q1 by Scimago and are from the United States and the European Union, which agrees with other authors that high-level scientific production is generated more frequently in countries with a higher technological level. The reason for this productivity is due to a higher level of human talent in the formation of V level studies, a high investment in the area of science and technology and a more advanced technological infrastructure compared to Latin American and African countries.

Once the most relevant journals in the area of computer science were selected, we proceeded to evaluate the relevance of their scientific production around cyber resilience in universities, specifically through the use of artificial intelligence for proactive threat detection. With this objective, a systematic search was conducted within each journal using keywords such as artificial intelligence, threats, risks, resilience and cybersecurity, focusing on the academic field of cybersecurity. The summary of the results obtained is presented in table 6.

Table 6. Summary of scientific production on cyber resilience in universities using artificial intelligence for proactive threat detection

Journal	Quartile	IA	DA	CR	IAU	DAU	RCU
1	1	487	1452	133	458	1370	124
2	1	1482	4579	4006	1442	125	419
3	1	24	655	22	3	625	15
4	1	227	130	23	184	109	19
5	1	226	261	93	69	228	86
6	1	966	969	186	905	887	172
7	2	19	0	7	0	0	0
8	2	8292	40499	4468	7430	34260	3954
9	2	332	3622	3065	241	1348	1096
10	2	1482	4579	4006	14427	125	419
11	2	355	436	36	298	370	28
12	2	600	51	9	550	47	8
13	3	53	84	7	63	84	7
14	3	412	1194	713	2837	33	97
15	3	3	32	13	2	1	1
16	3	122	0	1	0	0	1
17	3	332	3622	3075	241	1348	1096
18	3	460	176	827	1528	16	5

19	4	5	5	0	4	5	0
20	4	6	4	0	0	4	0
21	4	263	751	3	2	9	29
22	4	8	0	0	7	0	0
23	4	5	5	0	0	0	0
24	4	53	29	9	21	18	0

(AI); artificial intelligence, (DA); threat detection; (CR): cyber resilience, (IAU); artificial intelligence in universities, (DAU); threat detection in universities; (RCU): cyber resilience in universities.

In general, the results show that there is a greater scientific production in articles related to cyber resilience in universities through artificial intelligence for proactive threat detection, which demonstrates that the trend in science is the production of scientific innovations, which is aligned with the advance of articulated intelligence and cybersecurity, which must be accompanied by an adequate management of data protection and user integrity.

The trend observed by the analysis of the quartiles generated by the Scimago portal was ratified by the principal component analysis (PCA), shown in figure 6, where two groups are clearly observed: group 1, which corresponds to the journals with the highest impact (Q1) and with international collaborative works, and group 2, which groups the journals with the highest number of publications that address the topics of artificial intelligence, threats, risks, resilience and cybersecurity, both in the global and academic spheres.

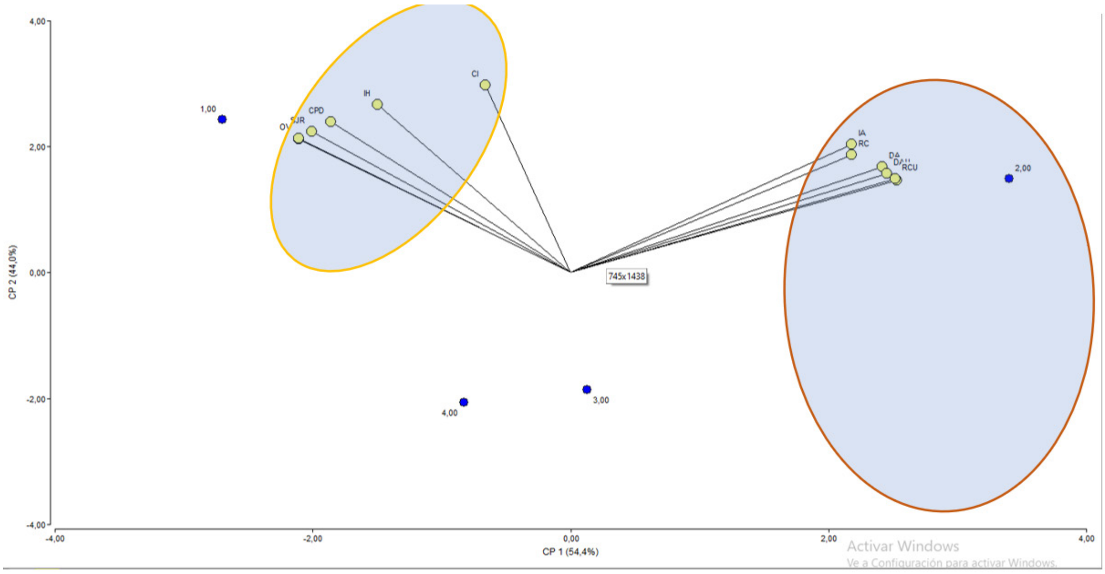

Figure 6. Distribution of scientific publications by principal component analysis

The results of the PCA are ratified by the mean comparison tests of bibliometric indicators generated by Scimago, firstly, by those presented in table 7 referring to the quality of the journals, where it is observed that the journals in quartile 1 have on average a higher citation index (H), total documents cited (DT), citations per documents (CPD) and citations from public bodies (OV) compared to these same indicators for quartiles 2, 3 and 4.

Table 7. Mean comparisons of bibliometric indicators generated by Scimago

Quartile	SJR	IH	DT	CPD	CI	OV
1	201,25	150,17	258,00	22,02	43,39	2,17
2	0,69	50,33	75,17	3,42	34,91	0,00
3	0,42	28,00	48,67	2,09	20,21	0,00
4	0,19	13,33	34	1,44	26,60	0,17

(SJR): Journal Impact Factor (IH): H index, DT: Number of papers: number of papers published by a journal in the selected year, (CPD): Citations per paper: number of citable papers published by a journal in the three years prior to the selected year, (IC): International Scientific Collaboration: list of papers whose affiliation includes more than one country address, (OV): Citations of public planners according to the Overton database.

Likewise, in table 8, it is observed in relation to the number of publications, referring to the search terms used as, both generally and in the field of cybersecurity in universities, artificial intelligence, threats, risks and resilience, where the mean comparison tests show that the journals grouped in quartiles 1 and 2 present the highest number of publications compared to clusters 3 and 4.

Table 8. Mean comparisons for analyzed publications

Quartile	IA	DA	CR	IAU	DAU	RCU
1	568,67	1341	743,83	510,17	557,33	137,19
2	1845,67	8197,83	1931,83	3824,33	6025	917,50
3	230,33	851,33	772,67	778,60	247	211,17
4	50,.67	132,33	2,00	5,67	6	4,83

AI); artificial intelligence, (DA); threat detection; (CR): cyber resilience, (IAU); artificial intelligence in universities, (DAU); threat detection in universities; (RCU): cyber resilience in universities.

From a graphical point of view, figure 7 shows that according to search terms such as artificial intelligence, threat detection, and cyber resilience, the majority is concentrated in journals in the Q1 and Q2 quartiles, with a tendency to a lower number of publications in the university context, especially when addressing the topic of cyber resilience, so that despite the importance of this cybersecurity strategy, it has been little studied.

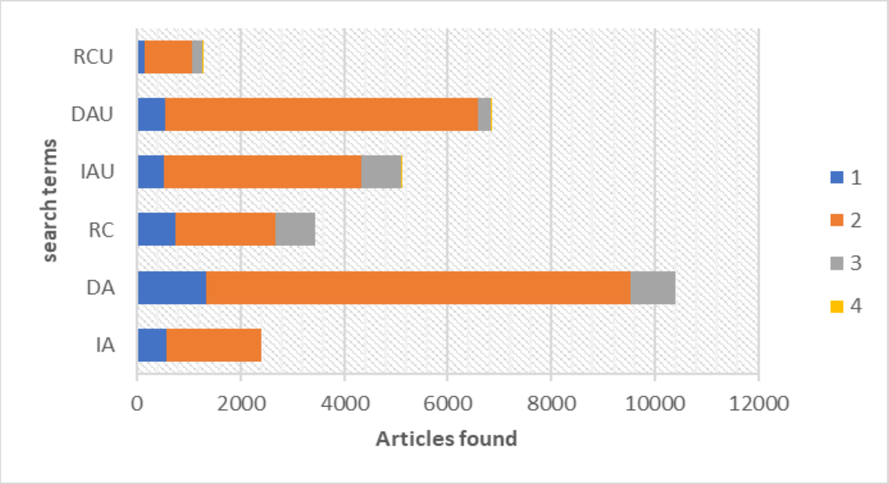

Figure 7. Comparison of scientific production by search terms

DISCUSSION

The findings also demonstrate the low capacity for action in the context of cybersecurity especially in Latin American, Southeast Asian and African countries, where technological limitations prevent the development of strategies such as cyber resilience. The situation described in these countries is more vulnerable to hacker attacks that hinder the capacity to respond to the consequences generated by this type of actions, putting at risk the operability of the institutions.(11,12)

Despite the fact that Latin American countries have increased their scientific production, there is still an inequality between the production of developed countries and those of the regions in the context of research in informatics and in this case in the development of cybersecurity tools, especially due to the dominance of prestigious databases such as Scopus, Nevertheless, there is an abundance of repositories exclusively in Spanish, and there is also an internal lag among the countries with the highest academic level, given that the results observed in countries such as Brazil, Mexico, Colombia and Argentina have the largest number of journals in certified indexes.(13,14)

There are results that contradict the fact that a scientific publication is one of the most valued activities within the academic world, given its importance to disseminate knowledge at the level of the global scientific community, as a mechanism of evaluation of university professionals and research institutions to leverage technological development, which is why every day they are required to publish in journals of higher quality and prestige, which will allow their evaluation according to the impact of the journals and through the use of bibliometric indicators based on the number of citations that highlight the importance of the same, a situation that does not happen when addressing the study of cyber resilience in academia, which refers to the ability of an organization to anticipate, resist, recover and adapt to cyber incidents, maintaining business continuity. It involves the prevention, detection and effective response to attacks, as well as the rapid restoration of operations after an incident.(15,16)

The principal components study (PCA) shows that the analysis of quartiles generated by Scimago allows discriminating scientific journals according to their importance and that such analysis facilitates the bibliometric analysis of the data, being a valuable tool for this type of studies, as shown by previous research, and which are proven through the statistical analysis of the bibliometric indicators considered in this research in relation to the strengthening of cyber resilience in universities through artificial intelligence for proactive threat detection.(17,18)

The results obtained are key, since impact indexes help the accessibility of scientific information, allow the visibility of publications and facilitate the improvement of bibliometric indicators of national journals, the findings reveal a lag of Latin American publications with respect to their European and North American peers, highlighting that the best positioned journals belong to the area of computer science, The results suggest that an increase in scientific investment is required through incentives that promote publication in high impact journals and thus allow Latin American publications to have a greater reach in the international scientific community and improve their position in the most prestigious impact indexes, for which journal publishers must also comply with demanding quality standards. Regional scientific production has decreased considerably, as a result of less scientific activity, lack of investment in science and technology and the exodus of many Latin American scientists to other countries.(19,20)

In order to know the positioning of scientific production, impact indexes are a derivation of databases and institutional repositories whose main purpose is the digital preservation of scientific information and at the same time to guarantee its visibility, accessibility and finally to be a tool of quality of scientific information through bibliometric indexes generated from the number of citations, the lower presence of Latin American journals in the impact indexes does not necessarily affect the qualification of scientists in the region and research institutions, since despite this lag, researchers continue to maintain a high number of citations despite the low number of publications.(21)

CONCLUSIONS

In conclusion, cybersecurity according to the bibliometric analysis performed is concentrated on the development of technology for data protection, where cutting-edge research is carried out by countries with high technological level, however resilience is an underdeveloped mechanism to address the consequences of cybersecurity threats, Therefore, given the scarce research on resilience in the context of cybersecurity, there are few existing strategies for strengthening this quality in public and private organizations, especially universities.

BIBLIOGRAPHIC REFERENCES

1. Ulven JB, Wangen G. A systematic review of cybersecurity risks in higher education. Future Internet. 2021;13(2):39.

2. Florackis C, Louca C, Michaely R, Weber M. Cybersecurity risk. Rev Financ Stud. 2023;36(1):351–407.

3. Alqahtani MA. Factors affecting cybersecurity awareness among university students. Appl Sci. 2022;12(5):2589.

4. Alharbi T, Tassaddiq A. Assessment of cybersecurity awareness among students of Majmaah University. Big Data Cogn Comput. 2021;5(2):23.

5. Saeed S, Suayyid SA, Al-Ghamdi MS, Al-Muhaisen H, Almuhaideb AM. A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience. Sensors. 2023;23(16):7273.

6. Hong WCH, Chi C, Liu J, Zhang Y, Lei VNL, Xu X. The influence of social education level on cybersecurity awareness and behaviour: a comparative study of university students and working graduates. Educ Inf Technol. enero de 2023;28(1):439–70.

7. Mai PT, Tick A. Cyber Security Awareness and behavior of youth in smartphone usage: A comparative study between university students in Hungary and Vietnam. Acta Polytech Hung. 2021;18(8):67–89.

8. Bolbot V, Kulkarni K, Brunou P, Banda OV, Musharraf M. Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis. Int J Crit Infrastruct Prot. 2022;39:100571.

9. Nobanee H, Alodat A, Bajodah R, Al-Ali M, Al Darmaki A. Bibliometric analysis of cybercrime and

cybersecurity risks literature. J Financ Crime. 1 de diciembre de 2023;30(6):1736-54.

10. In-Vehicle Communication and Cyber Security. En: Automotive Cyber Security [Internet]. Singapore: Springer Singapore; 2020 [citado 9 de julio de 2025]. p. 67-96. Disponible en: https://link.springer.com/10.1007/978-981-15-8053-6_4

11. Flor-Unda O, Simbaña F, Larriva-Novo X, Acuña Á, Tipán R, Acosta-Vargas P. A comprehensive analysis of the worst cybersecurity vulnerabilities in latin america. En: Informatics [Internet]. MDPI; 2023 [citado 9 de julio de 2025]. p. 71. Disponible en: https://www.mdpi.com/2227-9709/10/3/71

12. Urbanovics A. Cybersecurity Policy-Related Developments in Latin America. AARMS–Academic Appl Res Mil Public Manag Sci. 2022;21(1):79-94.

13. Carapeto R, Calil AL. Cybersecurity regulation in Brazil and Latin America: an overview. Int Cybersecurity Law Rev. diciembre de 2022;3(2):385-410.

14. Aguilar Antonio JM. Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior. Estud Int Santiago. 2021;53(198):169-97.

15. Pourmadadkar M, Lezzi M, Corallo A. Cyber Security for Cyber-Physical Systems in Critical Infrastructures: Bibliometrics Analysis and Future Directions. IEEE Trans Eng Manag [Internet]. 2024 [citado 9 de julio de 2025]; Disponible en: https://ieeexplore.ieee.org/abstract/document/10740034/

16. Cibu B, Delcea C, Domenteanu A, Dumitrescu G. Mapping the evolution of cybernetics: A bibliometric perspective. Computers. 2023;12(11):237.

17. Nica I. Bibliometric mapping in the landscape of cybernetics: insights into global research networks. Kybernetes. 2025;54(6):3322-57.

18. Rodriguez WJM, Girón DCA, Ramirez ETS, Rojas MZ. Investigación sobre computación en nube en ciencias de la computación e ingeniería: análisis de resultados de Scopus. Rev Científica Sist E Informática. 2025;5(1):e908-e908.

19. Restrepo-Betancur LF. Evaluation of the number of publications in computer science in South America in a period of 20 years. Tecnura. 2022;26(74):149-64.

20. Talla AJC, Huapaya DCT, Pérez VEA. Análisis bibliométrico de la producción científica de la Deep Web en Ciencias Computacionales: Bibliometric analysis of the scientific production of the Deep Web in Computer Science. LATAM Rev Latinoam Cienc Soc Humanidades. 2024;5(4):2846-65.

21. Peng P, Xie X, Claramunt C, Lu F, Gong F, Yan R. Bibliometric analysis of maritime cybersecurity: Research status, focus, and perspectives. Transp Res Part E Logist Transp Rev. 2025;195:103971.

FINANCING

None.

CONFLICT OF INTEREST

Authors declare that there is no conflict of interest.

AUTHORSHIP CONTRIBUTION

Conceptualization: Carina Del Rocio Cevallos Ramos, Fausto Francisco Navarrete Chávez, Fernando Ricardo Márquez Sañay, Mauro Patricio Andrade Romero.

Data curation: Carina Del Rocio Cevallos Ramos, Fausto Francisco Navarrete Chávez, Fernando Ricardo Márquez Sañay, Mauro Patricio Andrade Romero.

Formal analysis: Carina Del Rocio Cevallos Ramos, Fausto Francisco Navarrete Chávez, Fernando Ricardo Márquez Sañay, Mauro Patricio Andrade Romero.

Drafting - original draft: Carina Del Rocio Cevallos Ramos, Fausto Francisco Navarrete Chávez, Fernando Ricardo Márquez Sañay, Mauro Patricio Andrade Romero.

Writing - proofreading and editing: Carina Del Rocio Cevallos Ramos, Fausto Francisco Navarrete Chávez, Fernando Ricardo Márquez Sañay, Mauro Patricio Andrade Romero.