



# Cybersecurity Risks in Businesses

Andrés Mauricio Quintero Londoño<sup>1\*</sup>, Laura arciniegas londoño<sup>2</sup>

## Abstract

A documentary review was carried out on the production and publication of research papers related to the study of the variable Cybersecurity Risks in companies in Latin America. The purpose of the bibliometric analysis proposed in this document is to know the main characteristics of the volume of publications registered in the Scopus database during the period 2016-2021 in Latin American countries, achieving the identification of 42 publications. The information provided by the said platform was organized through tables and figures categorizing the information by Year of Publication, Country of Origin, Area of Knowledge, and Type of Publication. Once these characteristics were described, a qualitative analysis was used to refer to the position of different authors on the proposed topic. Among the main findings of this research, it is found that Brazil, with 18 publications, is the Latin American country with the highest production. The area of knowledge that made the greatest contribution to the construction of bibliographic material referring to the study of cybersecurity risks in companies was computer science with 37 published documents, and the type of publication that was most used during the period indicated above was the conference proceedings, which represent 64% of the total scientific production.

**KeyWords:** Cybersecurity, Companies

**DOI Number:** 10.14704/nq.2022.20.8.NQ44317

**NeuroQuantology2022; 20(8):2858-2867**

2858

## 1. Introduction

Cybersecurity is all those mechanisms, systems, and programs that are used to safeguard important, sensitive, and classified information susceptible to digital crimes; this problem has increased in the last 5 years to be in the digital age and globalization so that companies increasingly use information and communication technologies (ICT) to innovate their processes making them more accessible and keep the company in line with what the market currently requires is facing new technological security challenges.

Cybersecurity Risks are all those made to an organization to subtract, destroy, obtain, or alter important information for its operation, so investing in Cybersecurity is essential for good business management and data protection; this applies to both large and medium and small companies since although to different degrees, all are exposed to these Risks and can mean great business losses in

both information and economic resources (Rea Guamán et al., 2018).

The Cybersecurity Risks to which companies are most exposed are the affectations of the cloud, where a large quantity of data is stored, and if many people have access to these platforms they can become cyber risks of information leakage. Another risk that companies face is identity theft, which was seen more frequently during quarantine when teleworking was the way to continue the business management and communication between workers was usually through emails, which could represent a risk of impersonation by cybercriminals giving them access to platforms and confidential documents putting at risk important information of the company. Thanks to the above, it can be said that cybersecurity is an important part of business management and it is necessary to implement good policies to reduce the risk of cybercrimes that affect the security of companies and the total or partial loss of relevant and classified information.

**Corresponding author:** Andrés Mauricio Quintero Londoño

**Address:** <sup>1</sup>Escuela de Inteligencia y Contrainteligencia "Brigadier General Ricardo Charry Solano" , <sup>2</sup>Magister en inteligencia estratégica Escuela de Inteligencia y Contrainteligencia "Brigadier General Ricardo Charry Solano"

E-mail: andres.quinterolo@buzonejercito.mil.co<sup>1</sup>,

lauritaarci@gmail.com<sup>2</sup>



Therefore, it is important to know in terms of bibliographic resources, the current state of research on Management Accounting for Decision Making in Latin American companies, so a bibliometric analysis of the scientific production registered in the Scopus database during the period 2016-2021 is proposed to answer the question: How has been the production and publication of research papers related to the study of the variable Cybersecurity Risks in companies in Latin America during the period 2016-2021?

## 2. General objective

To analyze from a bibliometric and bibliographic perspective, the production of high-impact research papers on the variable Cybersecurity Risks in Latin

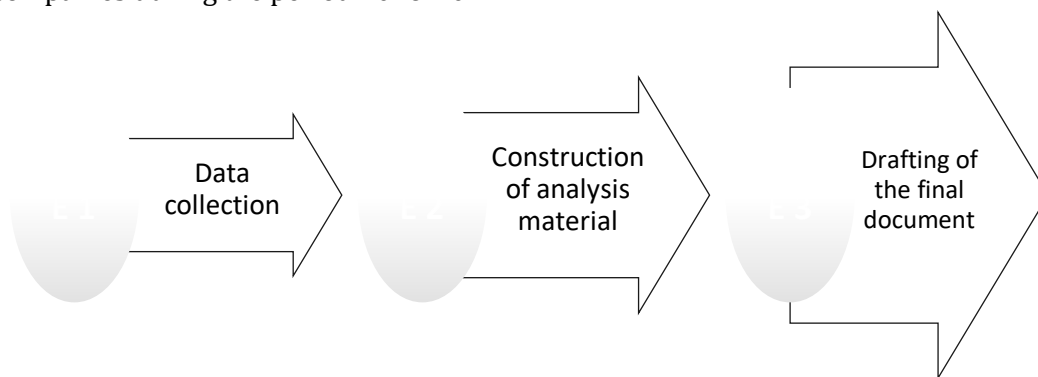
American companies during the period 2016-2021.

## 3. Methodology

Quantitative analysis of the information provided by Scopus is performed under a bibliometric approach to the scientific production regarding Cybersecurity Risks in companies. Also, from a qualitative perspective, examples of some research papers published in the area of the study mentioned above are analyzed from a bibliographic approach to describe the position of different authors on the proposed topic.

The search is carried out through the tool provided by Scopus and the parameters referenced in Table 1 are established.

### 3.1 Methodological design



**Figure 1. Methodological design**  
Source: Own elaboration.

2859

### Phase 1: Data collection

Data was collected using the Scopus web page search tool, through which a total of 42 publications were identified. For this purpose, search filters were established consisting of:  
Published documents whose study variables are related to Cybersecurity Risks in companies.  
Imitated Latin American countries  
Without distinction of the area of knowledge.  
Without distinction of the type of publication.

### Phase 2: Construction of analysis material

The information identified in the previous phase is organized. The classification will be made through graphs, figures, and tables based on data provided by Scopus.  
Co-occurrence of words.  
Year of publication

Country of origin of the publication.  
Area of knowledge.  
Type of publication

### Phase 3: Drafting of conclusions and final document

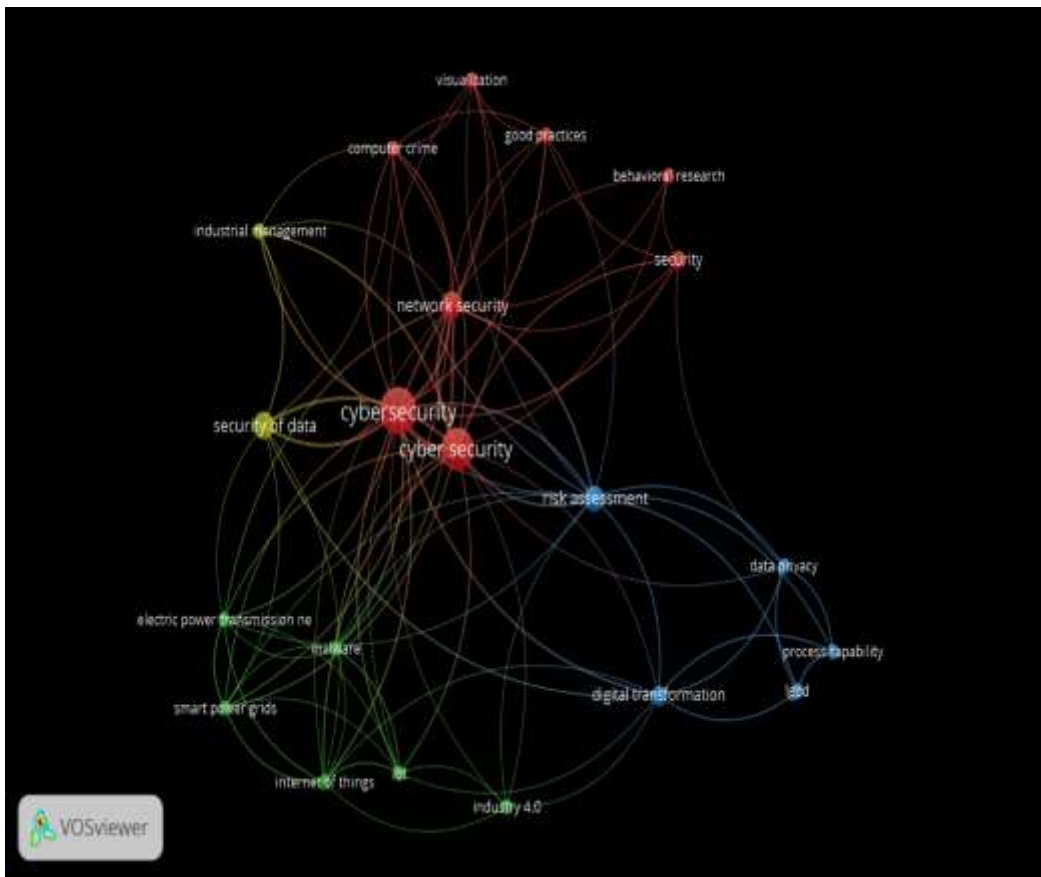
After the analysis carried out in the previous phase, the conclusions are drawn up and the final document is prepared.

## 4. Results

### 4.1 Co-occurrence of words

Figure 1 shows the co-occurrence of keywords within the publications identified in the Scopus database.





**Figure 1. Co-occurrence of words**  
**Source: Own elaboration (2022); based on data provided by Scopus.**

2860

As shown in Figure 1, the most used keyword in the research related to the variables under study is Cybersecurity, which is the set of systems, platforms, and programs implemented by companies to protect information and reduce the risk of suffering cybercrimes that put their management at risk, making Cybersecurity an essential element for the proper functioning of organizations in the digital era, where actions are increasingly automated and information is stored on digital platforms with the ability to host a large amount of data.

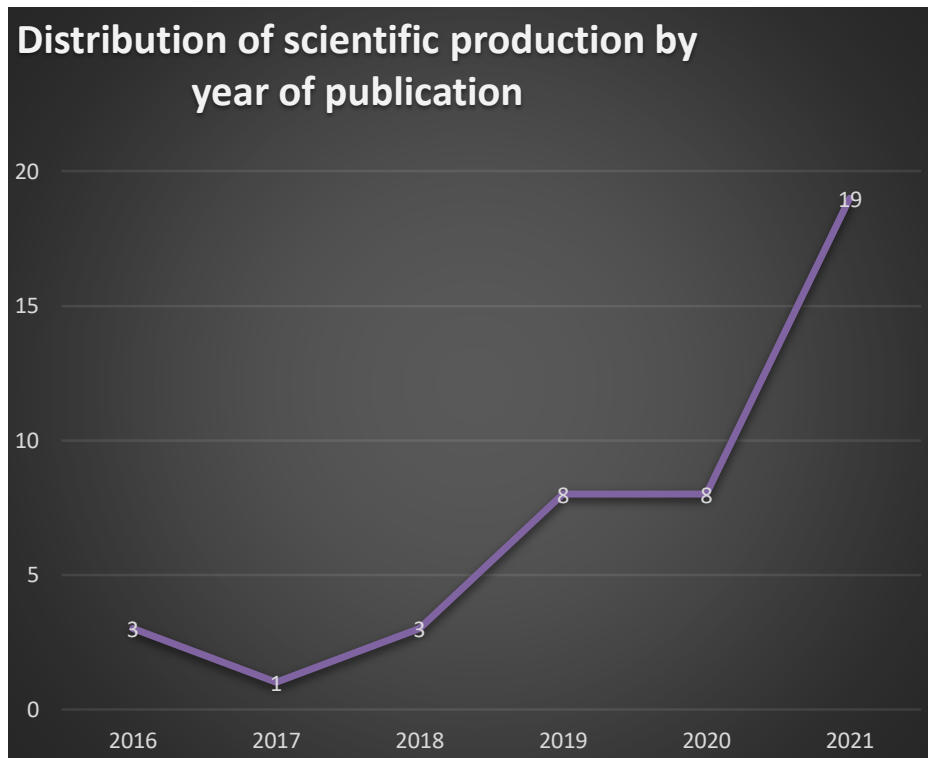
Digital transformation, industry 4.0, and ICT are keywords that refer to the social evolution that has been experienced with the application of technology in all areas, so that companies, to be in line with the industry have innovated their processes with the implementation of information and communication technologies that although

they represent a breakthrough by digitizing most processes, is also the creator of risk factors when facing a new class of crimes, cybercrimes, which put at risk the security and privacy of information. Finally, there is data security, assistance at risk, data privacy, and processability, which are the functions performed by cybersecurity to warn about possible risks to the security of clouds, platforms, or identity theft that jeopardize information and business management.

#### **4.2 Distribution of scientific production by year of publication.**

Figure 2 shows how the scientific production is distributed according to the year of publication, taking into account the period from 2016 to 2021.





**Figure 2. Distribution of scientific production by year of publication. Source: Own elaboration (2022); based on data provided by Scopus.**

2021 is the year with the highest number of publications related to the variables under study presenting 19 papers, within which you can find "A case study of the Capital One data breach: Why compliance requirements did not help prevent it" (Neto et al., 2021). The main objective of this paper is to understand whether compliance requirements would help prevent a major data breach incident at Capital One, one of the largest financial institutions in the U.S. The studies obtained in this study will help to improve cyber security controls, being this a latent danger for companies and their privacy policies, since although there is now a greater regulation against these crimes, it is still very important that companies implement security systems that warn about possible affectations to their databases.

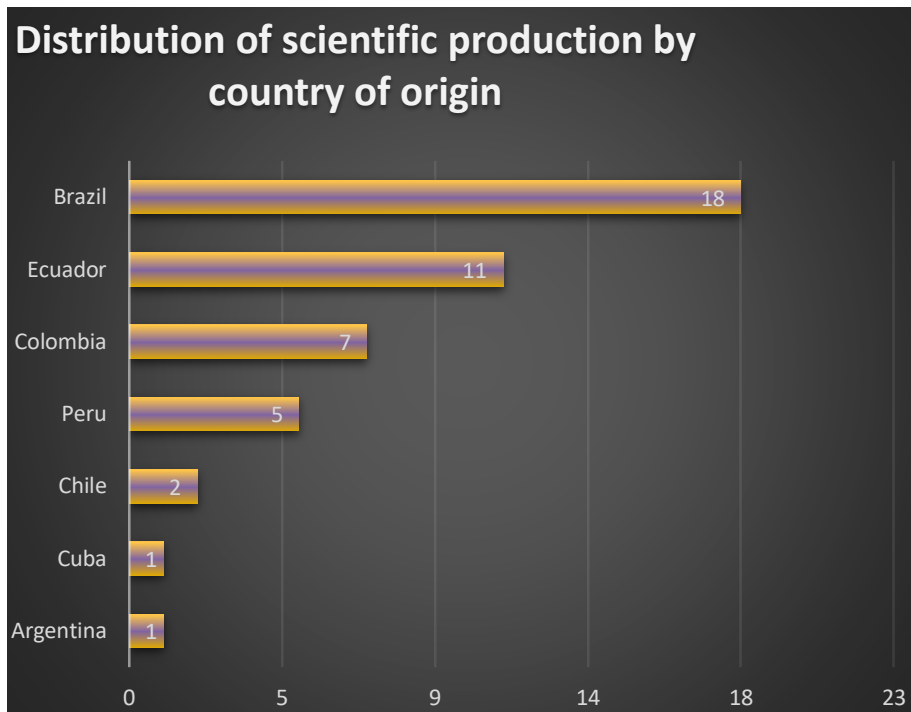
In second place are the years 2019 and 2020 with 8 publications registered in each one. Within the

publications of the year 2020 is the title "Platform for monitoring the maturity of Cybersecurity of micro and small enterprises" (Gallardo et al., 2020). This document aims to determine the cyber maturity of small and medium enterprises in Chile due to the low budget to hire qualified personnel, thus neglecting this aspect, which is increasingly important due to digital transformation. This is why this document presents the tools for micro and small companies to evaluate themselves, and potentially have the support for continuous improvement and ultimately mature digitally.

### 4.3 Distribution of scientific production by country of origin

Figure 3 shows the distribution of scientific production according to the nationality of the authors.





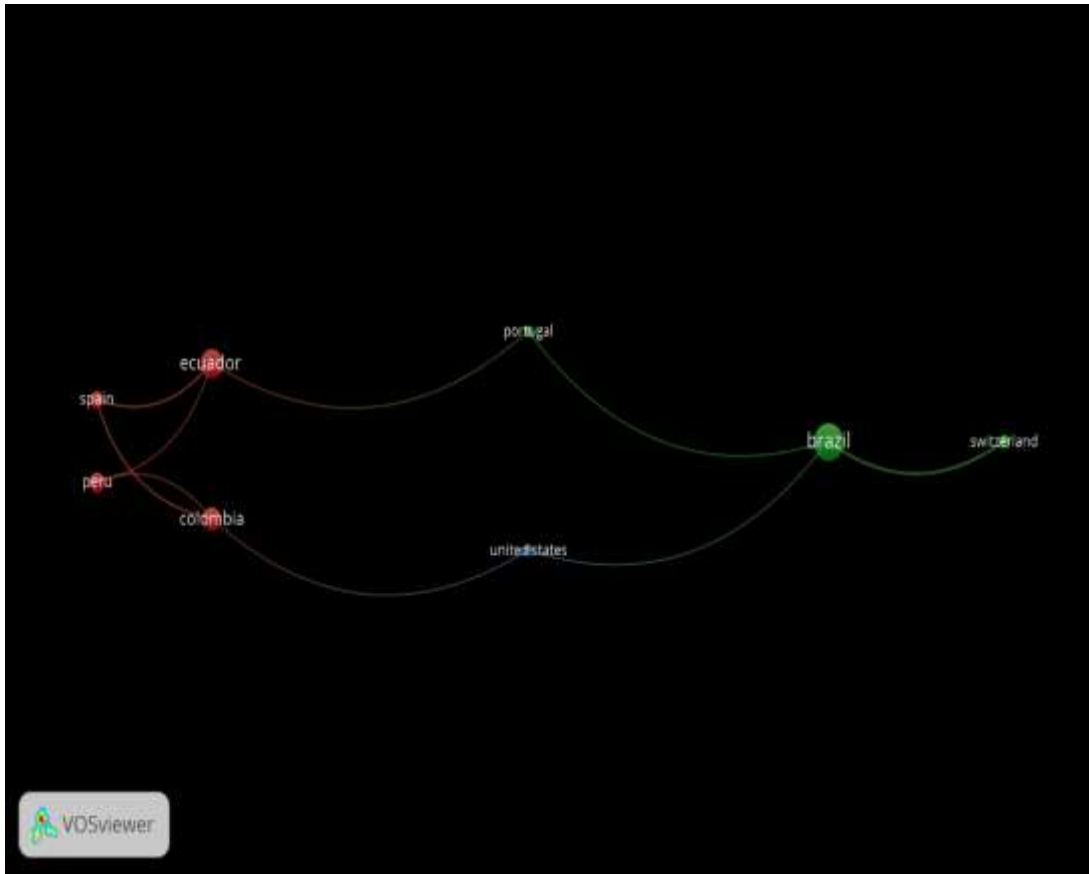
**Figure 3. Distribution of scientific production by country of origin.**  
Source: Own elaboration (2022); based on data provided by Scopus.

Brazil is the Latin American country with the largest contribution to research related to the variables under study during the period 2016-2021 presenting 18 papers, within which is the title "Development of a conceptual model for process capability in the context of Brazilian data protection regulation" (Muncinelli et al., 2021). This article has as its main objective to analyze the areas of contribution to the evaluation of process capability for digital transformation in Cybersecurity in the context of personal data protection legislation from the implementation of a capability model that allows companies to have Cybersecurity systems that allow them to have favorable business management and in line with industry 4.0 from the digitalization of

their processes.

At this point, it is worth noting that the production of scientific publications, when classified by country of origin, presents a special feature and that is the collaboration between authors with different affiliations to both public and private institutions, and these institutions may be from the same country or different nationalities, so the production of an article co-authored by different authors from different countries of origin allows each of the countries to add up as a unit in the general publications. This is best explained in Figure 4, which shows the flow of collaborative work from different countries.





**Figure 4. Co-citations between countries.**  
**Source: Own elaboration (2022); based on data provided by Scopus.**

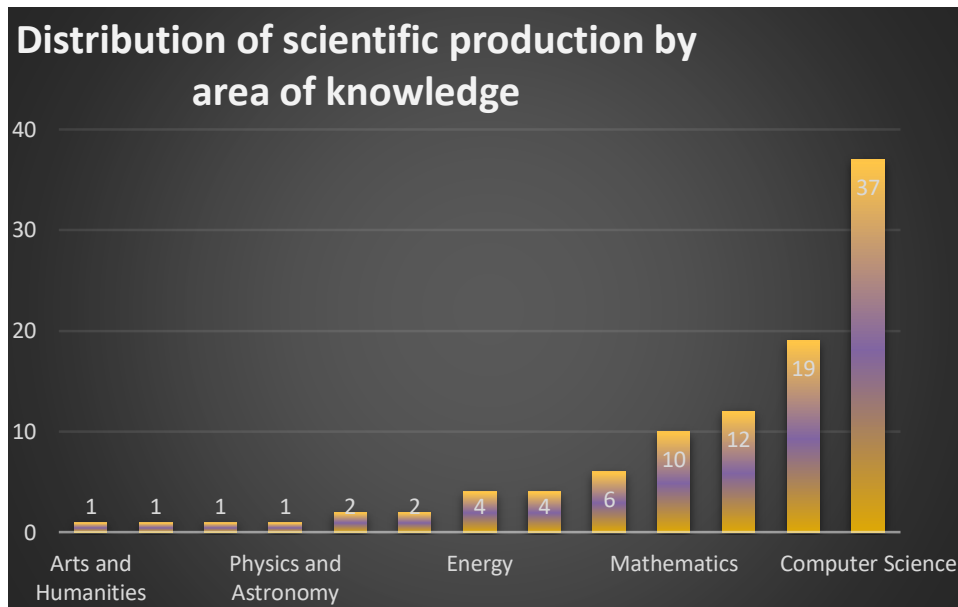
As mentioned above, Brazil is the Latin American country with the highest number of scientific production in research related to Cybersecurity Risks that are exposed to companies, having documents in collaboration with authors affiliated to institutions belonging to countries such as Switzerland, the United States, and Portugal, which shows the interest of countries outside Latin America to learn about the cyber risks that organizations face and what systems and platforms are used to alert them about these risks. In second place is Ecuador with 11 documents, including publications co-authored with countries such as Spain, Peru, and Colombia. Peru and Colombia, where through comparative studies, the progress made by one country in cybersecurity compared to another is determined. Among these documents is the paper entitled "Comparative analysis of

cybersecurity mechanisms in SD-WAN architectures: Preliminary results" (Bustamante & Avila-Pesantez, 2021). The main objective of this document is to present a software solution that provides a cost-benefit balance, given the high cost of WAN connections by conducting a comparative study between a commercial and an open-source alternative. Thanks to this study, it was found that the commercial alternative provides greater security and confidentiality while the open source offers adaptability in the future.

#### **4.4 Distribution of scientific production by area of knowledge**

Figure 5 shows how the production of scientific publications is distributed according to the area of knowledge through which the different research methodologies are executed.





**Figure 5. Distribution of scientific production by area of knowledge.**  
**Source: Own elaboration (2022); based on data provided by Scopus.**

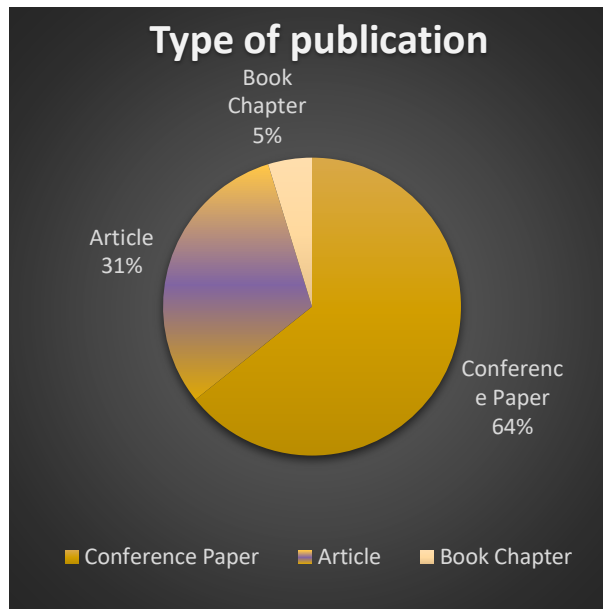
Computer Science is the area of knowledge with the largest number of contributions through the theories that are framed in it, in the search for new knowledge about Cybersecurity Risks in companies presenting 37 papers, within which is the title "SecGrid: A visual system for ML-based analysis and classification of cyber attack traffic" (Franco et al., 2021 ). This paper presents a platform powered by Machine Learning (ML) to analyze, classify, and visualize cyber attacks which is called SecGrid and through miners that inspect network traces with malicious traffic thus alerting about possible cyber criminals protecting confidential information and data the results show high overall usability, scalability in terms of the platform's ability to extract information from large files and high performance and accuracy during the classification of cyber attacks. In second place is engineering where 19 documents

were written following the guidelines of the topics related to this area within which you can find "Financial quantification model oriented to ransomware scenarios for the financial sector" (Ochoa et al., 2021) with the main objective of presenting a model with a quantitative approach so that organizations can express in financial terms the potential impact of a ransomware attack being cyber-attacks more and more common, so it is necessary to invest in cybersecurity. With this model, it was possible to increase investment in this aspect to safeguard relevant information.

#### 4.5 Type of publication

Figure 6 shows how the bibliographic production is distributed according to the type of publication chosen by the authors.





**Figure 6. Type of publication**  
**Source: Own elaboration (2022); based on data provided by Scopus.**

As shown in Figure 6, within the different types of publications, 64% of the total documents identified through Phase 1 of the Methodological Design, correspond to conference proceedings, among which is the "Guide of principles and good practices for software security testing in web applications for a private sector company" (Bautista & Parada, 2021). In this document, the methods that a private sector company in Colombia uses to safeguard its information from possible cybercrimes are analyzed, taking into account the boom that this has as more and more electronic devices are used. As a result, it was found that the company does not have a component that focuses on security, so it is necessary to promote the use of authorized, dynamic and static tools, among others, for the evaluation of software quality in the security component.

In second place are the journal articles which represent 31% of the total number of documents identified in this study within which is the paper entitled "Exploratory data analysis for Cybersecurity" (Miranda-Calle et al., 2021). This article has as its main objective to establish the use of data science in data analysis and provide a more detailed view of the most common Cybersecurity attacks where in addition to identifying them it was possible to determine the different pages that could be used to avoid these cyber attacks and also suggest policies so that if an attack is carried out on a specific machine.

### 5. Conclusions

Thanks to the bibliometric analysis proposed in this research, it can be determined that Brazil is the Latin American country with the highest number of bibliographic records in the Scopus database during the period between 2016 and 2022 with a total of 18 documents. The scientific production related to the study of Cybersecurity Risks in companies has presented a significant growth during the period previously indicated, going from 3 publications in 2016 to 19 units in 2021, i.e., it was possible to increase the creation of bibliographic records in 5 years in a great way being a situation that since the pandemic was seen a strong increase of cybercrimes and the need to invest in Cybersecurity, which indicates the importance of researching on Cybersecurity Risks in companies to determine the systems that allow safeguarding important and classified information relevant to the company and its operation.

Cybersecurity is a concept increasingly used and relevant in companies to be all the mechanisms that are used to prevent cybercrimes that put at risk the data that the company stores in a classified manner to protect customer data, suppliers, and company officials. Cybersecurity mechanisms are born of the transformation that companies have implemented in recent years to be in line with what the industry 4.0 requests, all this brings with it new challenges such as data protection in the clouds and in financial and big data systems that help in the decision-making process. Investing in cybersecurity



is essential for any company to ensure data privacy for its customers and good business management. One of the greatest risks that companies face concerning cybersecurity is identity theft, which can lead cybercriminals to obtain relevant information or usurp passwords and platforms, slowing down their proper functioning. All the above allows this article to conclude, highlighting the importance of knowing the theory or bibliographic resources that seek to awaken the interest in organizations, to manage policies that allow you to implement systems against Cybersecurity Risks in companies taking into account that they can lose or usurp very important information. That is why the need for studies such as the one presented in this document is highlighted, which make a tour of those texts that address the aforementioned topic, to give the reader a broad view of the current situation of the literature on Cybersecurity Risks in companies.

## References

- Bautista, E. C., & Parada, H. D. (2021). Guide of principles and good practices for software security testing in web applications for a private sector company. 2021 7th Congreso Internacional de Innovación y Tendencias en Ingeniería, CONIITI 2021 - Conference Proceedings. Bogota: 7th Congreso Internacional de Innovación y Tendencias en Ingeniería, CONIITI 2021.
- Bustamante, J. R., & Avila-Pesantez, D. (2021). Comparative analysis of Cybersecurity mechanisms in SD-WAN architectures: A preliminary results. Proceedings of the 2021 IEEE Engineering International Research Conference, EIRCON 2021.
- Franco, M., Von Der Assen, J., Boillat, L., Killer, C., Rodrigues, B., Scheid, E. J., & Granvi. (2021). SecGrid: A visual system for the analysis and ML-based classification of cyberattack traffic. Proceedings - Conference on Local Computer Networks, LCN, (págs. 140 - 147).
- Gallardo, J., Torres, R., & Tessini, O. (2020). Surveillance Platform of cybersecurity maturity of micro and small enterprises. Proceedings - International Conference of the Chilean Computer Science Society, SCCC. Coquimbo: 39th International Conference of the Chilean Computer Science Society, SCCC 2020.
- Miranda-Calle, J. D., Reddy C, V., Dhawan, P., & Churi, P. (2021). Exploratory data analysis for cybersecurity. World Journal of Engineering, 734 - 749.
- Muncinelli, G., De Lima, E. P., Cestari, J. M., Deschamps, F. .., & Da Costa, S. E. (2021). Developing a conceptual model for process capability in the Brazilian data protection regulation context. Journal of Industrial Integration and Management, 407 - 427.
- Neto, N. N., Madnick, S., de Paula, A. M., & Borges, N. M. (2021). A case study of the capital one data breach: Why didn't compliance requirements help prevent it? Journal of Information Systems Security, 49 - 78.
- Ochoa, R., Ticse, D., Herrera, E., & Vargas, J. (2021). Ransomware scenario oriented financial quantification model for the financial sector. Proceedings of the 2021 IEEE Sciences and Humanities International Research Conference, SHIRCON 2021. Lima.
- Rea Guamán, M., Calvo-Manzano Villalón, J. A., & San Feliu Gilabert, T. (2018). A prototype to manage cybersecurity in small companies. *archivo digital UPM*.
- Andrea Vaca, H., Reyes Ch, R. P., Vaca, H. P., & Paredes, M. (2018). Empirical study of the application of business intelligence (BI) in cybersecurity within Ecuador: A trend away from reality doi:10.1007/978-3-319-78605-6\_1 Retrieved from www.scopus.com
- Armenia, S., Ferreira Franco, E., Nonino, F., Spagnoli, E., & Medaglia, C. M. (2019). Towards the definition of a dynamic and systemic assessment for cybersecurity risks. *Systems Research and Behavioral Science*, 36(4), 404-423. doi:10.1002/sres.2556
- Bautista, E. C. R., & Parada, H. D. J. (2021). Guide of principles and good practices for software security testing in web applications for a private sector company. Paper presented at the 2021 7th Congreso Internacional De Innovación y Tendencias en Ingeniería, CONIITI 2021 - Conference Proceedings, doi:10.1109/CONIITI53815.2021.9619664 Retrieved from www.scopus.com
- Bruderer, R., Villena, M., Tupia, M., & Bruzza, M. (2018). A cybersecurity model for mobile devices aimed at SMEs that use freelancers and BYOD schemes. Paper presented at the Proceedings of the 11th IADIS International Conference Information Systems 2018, IS 2018, 129-136. Retrieved from www.scopus.com
- Bustamante, J. R., & Avila-Pesantez, D. (2021). Comparative analysis of cybersecurity mechanisms in SD-WAN architectures: A preliminary results. Paper presented at the Proceedings of the 2021 IEEE Engineering International Research Conference, EIRCON 2021, doi:10.1109/EIRCON52903.2021.9613418 Retrieved from www.scopus.com
- Cardenas, I. P., Espinoza, M., Armas-Aguirre, J., & Aguirre-Mayorga, H. (2021). Security of the information model on process mining: Case study of the surgery block. Paper presented at the 2021 7th Congreso Internacional De Innovación y Tendencias en Ingeniería, CONIITI 2021 - Conference Proceedings, doi:10.1109/CONIITI53815.2021.9619668 Retrieved from www.scopus.com
- Chenou, J. -. (2021). The contested meanings of cybersecurity: Evidence from post-conflict Colombia. *Conflict, Security and Development*, 21(1), 1-19. doi:10.1080/14678802.2021.1888512
- Dalmarco, G., Ramalho, F. R., Barros, A. C., & Soares, A. L. (2019). Providing industry 4.0 technologies: The case of a production technology cluster. *Journal of High Technology Management Research*, 30(2) doi:10.1016/j.hitech.2019.100355
- Espinosa, D. M., Vidal, D. C., & Huidobro, C. B. (2021). Methodological proposal for privilege escalation in Windows systems doi:10.1007/978-3-030-89586-0\_11 Retrieved from www.scopus.com
- Florentino, A. C. B., Barbalho, S. C. M., & MacHado, R. C. S. (2021). Proposal and validation of a standard protection profile for homologation of commercial videoconferencing equipment. *IEEE Access*, 9, 24288-24304. doi:10.1109/ACCESS.2021.3056491
- França, R. P., Monteiro, A. C. B., Arthur, R., & Iano, Y. (2021). The fundamentals and potential for cybersecurity of big data in the modern world doi:10.1007/978-3-030-57024-8\_3



Retrieved from [www.scopus.com](http://www.scopus.com)

- Franceschett, A. L., De Souza, P. R. A., Pereira De Barros, F. L., & De Carvalho, V. R. (2019). A holistic approach - how to achieve the state-of-art in cybersecurity for a secondary distribution automation energy system applying the IEC 62443 standard. Paper presented at the 2019 IEEE PES Conference on Innovative Smart Grid Technologies, ISGT Latin America 2019, doi:10.1109/ISGT-LA.2019.8895368 Retrieved from [www.scopus.com](http://www.scopus.com)
- Franco, M., Von Der Assen, J., Boillat, L., Killer, C., Rodrigues, B., Scheid, E., . . . Stiller, B. (2021). Poster: DDoSGrid: A platform for the post-mortem analysis and visualization of DDoS attacks. Paper presented at the 2021 IFIP Networking Conference, IFIP Networking 2021, doi:10.23919/IFIPNetworking52078.2021.9472850 Retrieved from [www.scopus.com](http://www.scopus.com)
- Franco, M., Von Der Assen, J., Boillat, L., Killer, C., Rodrigues, B., Scheid, E. J., . . . Stiller, B. (2021). SecGrid: A visual system for the analysis and ML-based classification of cyberattack traffic. Paper presented at the Proceedings - Conference on Local Computer Networks, LCN, , 2021-October 140-147. doi:10.1109/LCN52139.2021.9524932 Retrieved from [www.scopus.com](http://www.scopus.com)
- Franco, M. F., Rodrigues, B., Scheid, E. J., Jacobs, A., Killer, C., Granville, L. Z., & Stiller, B. (2020). SecBot: A business-driven conversational agent for cybersecurity planning and management. Paper presented at the 16th International Conference on Network and Service Management, CNSM 2020, 2nd International Workshop on Analytics for Service and Application Management, AnServApp 2020 and 1st International Workshop on the Future Evolution of Internet Protocols, IPFuture 2020, doi:10.23919/CNSM50824.2020.9269037 Retrieved from [www.scopus.com](http://www.scopus.com)
- Gallardo, J., Torres, R., & Tessini, O. (2020). Surveillance platform of cybersecurity maturity of micro and small enterprises. Paper presented at the Proceedings - International Conference of the Chilean Computer Science Society, SCCC, , 2020-November doi:10.1109/SCCC51225.2020.9281264 Retrieved from [www.scopus.com](http://www.scopus.com)
- Gerard Machado, T., De Assis Mota, A., Toledo Moreira Mota, L., Fabius Henriques De Carvalho, M., & CotrimPezzuto, C. (2016). Methodology for identifying the cybersecurity maturity level of smart grids. *IEEE Latin America Transactions*, 14(11), 4512-4519. doi:10.1109/TLA.2016.7795822

