Espirales
Revista multidisciplinaria de investigación científica

Global Overview of Cybersecurity Research (2015–2024): Bibliometric Evidence from Developing Countries in the Americas, with a Focus on Ecuador

Panorama global de la investigación en ciberseguridad (2015–2024): evidencia bibliométrica desde países en desarrollo de América con enfoque en Ecuador

Juan Carlos Enrique Ortega Acosta*

Received: July 30, 2026
Approved: September 26, 2026

Ortega, J. (2026) Global Overview of Cybersecurity Research (2015–2024): Bibliometric Evidence from Developing Countries in the Americas, with a Focus on Ecuador. *Espirales Revista Multidisciplinaria de investigación científica*, 10 (59), 12-58

* Quevedo State Technical University, Faculty of Agricultural and Forestry Sciences, Quevedo, Ecuador
Email: juanceortega@uteq.edu.ec
OrcID: https://orcid.org/0000-0003-3125-361X

Abstract

Cybersecurity has established itself as a strategic field within global scientific research, driven by the growing impact of digital risks on economies, societies, and institutional systems. Despite sustained growth in academic output, significant inequalities persist across regions, particularly among developing countries in the Americas. This study analyzes 79 publications indexed in Scopus to describe how this field is taking shape: who is conducting research, with whom they collaborate, and on what specific problems. The analysis is organized into three levels. At the international level, it examines publication trends, co-authorship patterns, and the thematic clusters that account for the majority of citations. Building on this, the study reviews the contribution of developing countries in the Americas, comparing their relative weight within the broader scientific system. Finally, it delves into the case of Ecuador, examining its major publications, the collaborative networks in which its authors participate, and the research areas that appear to be emerging or still underdeveloped. The results reveal patterns of thematic convergence and divergence among regions, as well as critical research gaps in the Latin American context. This bibliometric analysis provides useful evidence to shape regional scientific agendas, strengthen international collaboration, and guide future research toward strategically relevant but still under-explored areas in the field of cybersecurity.

Keywords: cybersecurity; bibliometric analysis; Scopus; developing countries; Latin America; Ecuador; research gaps; scientific collaboration

Resumen

La ciberseguridad se ha consolidado como un campo estratégico dentro de la investigación científica global, impulsada por el creciente impacto de los riesgos digitales en las economías, las sociedades y los sistemas institucionales. A pesar del crecimiento sostenido en la producción académica, persisten notables desigualdades entre regiones, especialmente entre los países en desarrollo del continente americano. Este trabajo analiza 79 publicaciones indexadas en Scopus para describir cómo se está configurando ese campo: quién investiga, con quién colabora y sobre qué problemas concretos. El análisis se organiza en tres planos. En el nivel internacional se examinan las tendencias de producción, las coautorías y los núcleos temáticos que concentran la mayor parte de las citaciones. A partir de ahí se revisa la contribución de los países en desarrollo de América, poniendo en relación su peso específico con el resto del sistema científico. Finalmente, se profundiza en el caso de Ecuador, donde se revisan sus principales publicaciones, las redes de colaboración en las que participan sus autores y las líneas de investigación que aparecen como emergentes o todavía poco desarrolladas. Los resultados revelan patrones de convergencia y divergencia temática entre regiones, así como vacíos críticos de investigación en el contexto latinoamericano. Este diagnóstico bibliométrico proporciona evidencia útil para orientar las agendas científicas regionales, fortalecer la colaboración internacional y guiar futuras investigaciones hacia áreas estratégicamente relevantes, pero aún poco exploradas en el ámbito de la ciberseguridad.

Palabras clave: ciberseguridad; análisis bibliométrico; Scopus; países en desarrollo; América Latina; Ecuador; vacíos de investigación; colaboración científica

Introduction

The rapid digital transformation has enhanced the strategic role of cybersecurity in protecting critical infrastructure, personal data, and economic assets on a global scale. With the expansion of the Internet of Things, artificial intelligence, and remote work environments, cyberattacks have increased in frequency, sophistication, and scope. Recent reports agree that cybersecurity has become one of the primary concerns in the global context.

The World Economic Forum ranks cybersecurity incidents and failures among the most likely risks with the greatest short-term impact, in some scenarios placing them above economic or health-related threats (Mas, 2023). Consistent with this assessment, the 2023 Check Point Research report estimates that the number of cyberattacks worldwide grew by approximately 38% compared to the previous year (Valladarez González & Cadena Martínez, 2025).

This increase has led governments, companies, and international organizations to accelerate the development of national cybersecurity strategies, regulatory frameworks, and sector-specific plans, particularly in critical sectors such as healthcare, banking, telecommunications, and education (Goycochea Kcomt, 2025; Von Solms & Van Niekerk, 2013). This is not merely a technical problem: the way these risks are managed involves scientific, political, and social decisions.

Hence the need for academic research capable of anticipating new threats, discussing regulatory proposals, and providing evidence to strengthen response capabilities, particularly in regions with greater gaps in infrastructure and specialized human resources (Aguilar Antonio, 2020; Nowersztern et al., 2021).

In the academic sphere, cybersecurity has been gaining prominence as a distinct field of study, particularly over the past twenty years. Today, it draws on contributions from computer science, engineering, law, and various branches of the social sciences, which has given rise to an increasingly broad and diverse body of research. Bibliometric studies point to a sustained—and in some areas nearly exponential—increase in the number of articles on cybersecurity, with a strong concentration in Scopus-indexed journals, which are largely funded and led by institutions in the Global North (Xu et al., 2020).

In terms of topics, there has been a shift from a perspective focused almost exclusively on the technical protection of systems toward broader approaches that consider data governance, the protection of critical infrastructure, and the implications of digital ethics (AlMalki & Durugbo, 2023). In this context, bibliometric analyses have established themselves as a useful tool for tracking the evolution of a field, identifying leading authors and institutions, detecting emerging research trends, and describing how scientific collaboration networks are organized (Aria & Cuccurullo, 2017).

Despite this, few studies apply this type of analysis to regions and countries with a lesser presence in the mainstream literature, leaving a significant portion of cybersecurity research uncharted, with a focus on developed and developing countries (Onumo et al., 2017; Aljohani et al., 2025; Purdon et al., 2020).

In the case of Latin America, various studies agree that the region contributes only a small portion of the total number of publications on cybersecurity and that it often does so as a secondary partner to universities and research centers in the Global North (Solar, 2023). This situation is not explained solely by the lack of trained teams, but also by well-known structural conditions: limited R&D budgets, fragmented scientific systems, a lack of continuity in public policies, and difficulties in sustaining stable internationalization processes.

Given this scenario, identifying which topics are under-researched and which collaborations have yet to be established is essential for strengthening regional scientific integration and moving toward more autonomous technology policies. Similarly, conducting a specific mapping of cybersecurity research output in countries such as Ecuador allows for the recognition of achievements, gaps, and potential niches for the development of independent agendas better tailored to local needs.

Although systematic reviews and some case studies exist on leading countries in the region, such as Brazil or Mexico, most global studies tend to omit Latin America as a specific object of analysis (Onumo et al., 2017; Aljohani et al., 2025; Purdon et al., 2020; Solar, 2023; Matilde Espino & Valencia Pérez, 2022; García, 2025; Orosco Fabian, 2024). This academic omission prevents not only the identification of relevant actors and emerging lines of research but also an understanding of collaboration patterns among

Latin American institutions and their level of integration into international scientific networks.

Given this knowledge gap, the study aims to provide concrete data on the role of developing countries in the Americas in the construction of cybersecurity knowledge. The overall objective is to map cybersecurity research in from 2015 to 2024, combining a global perspective with a specific analysis of developing countries in the Americas and an in-depth case study on Ecuador.

Based on this approach, the study analyzes trends in scientific output, collaboration networks among institutions, and topics that are emerging or under-researched, with the aim of identifying strategic research gaps that can guide future lines of work.

Ecuador has received little attention in bibliometric studies on cybersecurity, despite facing significant challenges in terms of digital infrastructure, regulation, and technical capabilities. Examining its scientific output within a regional framework allows for an assessment of its level of academic development, its degree of integration into international networks, and the opportunities for collaboration that can be strengthened when the system is viewed from a comparative and structural perspective.

The article is organized into five sections. First, it presents a review of the state of the art and the theoretical foundation of the research. Second, it describes the bibliometric methodology used, based on data from Scopus, processed using tools such as VOSviewer. The third section presents the results of the analysis at the global, regional (developing Americas), and national (Ecuador) levels.

The fourth section is devoted to a critical discussion of the findings, with special emphasis on research gaps and patterns of thematic convergence and divergence. Finally, the conclusions, limitations of the study, and recommendations for future research are presented.

Materials and Methods

Analyzing the evolution of cybersecurity research, especially in countries with developing scientific systems, requires careful and systematic work that allows for a deeper understanding and organization of the available knowledge (Onumo et al., 2017; Aljohani et al., 2025; Purdon et al., 2020; Solar, 2023; Matilde Espino & Valencia Pérez, 2022; García, 2025; Orosco Fabian, 2024). To this end, rigorous and transparent procedures that can be replicated by other researchers are employed, such as systematic literature reviews and structured evidence syntheses.

Within this framework, bibliometric analysis has established itself as a key tool for examining scientific output and its performance by authors, countries, institutions, and publication sources (Aria & Cuccurullo, 2017; Donthu et al., 2021; Zupic, 2015; Linnenluecke et al., 2020; Wallin, 2005). By quantifying and characterizing publication patterns, bibliometrics makes it possible to describe the configuration of cybersecurity as an academic field and to compare the position of different regions—such as the

developing countries of the Americas and, in particular, Ecuador—within the global research landscape.

These analyses are often complemented by visualization techniques that generate bibliometric maps or science maps, which depict thematic clusters and collaboration networks among disciplines, institutions, and scientific communities (Cobo et al., 2011; van Eck & Waltman, 2010; Börner et al., 2005). When applied to cybersecurity, this combined approach of quantitative indicators and visual mapping offers an integrated view of the field's growth, the topics that are becoming established or emerging, and the ways in which peripheral regions connect with the core of international scientific output.

Therefore, this study is situated within the academic literature on cybersecurity in its broadest sense, which includes both the protection of infrastructure and information systems and the legal, organizational, educational, and ethical dimensions linked to the digital environment (Xu et al., 2020; AlMalki & Durugbo, 2023; Aria & Cuccurullo, 2017; Onumo et al., 2017; Aljohani et al., 2025; Purdon et al., 2020; Solar, 2023; Matilde Espino & Valencia Pérez, 2022; García, 2025; Orosco Fabian, 2024).

To this end, a search strategy was defined that combined terms related to "cybersecurity" and "information security" with specific descriptors regarding emerging technologies, governance, and sector-specific applications (e.g., "Internet of Things," "artificial intelligence," "critical infrastructure," "blockchain," "telemedicine").

The analysis was designed to cover the period 2015–2024, in line with the 10-year time frame adopted in other recent bibliometric studies (Arar & Yurdakul, 2023; Malanski et al., 2021; Pico Saltos et al., 2021). It is important to clarify that the data available for this study for the year 2015 includes only one record from a secondary source—the only one available in Scopus for that year based on the primary search term "cybersecurity" (Kononovich et al., 2015). To this was added 78 records downloaded from the database, all published between 2016 and 2024 (Cunha et al., 2018; Duo et al., 2019; Leal et al., 2019; Canuto et al., 2019; Monzelo & Nunes, 2019; Dzhalladova et al., 2019; Mejía Miranda, 2022; Ramirez Peña et al., 2020; Monzelo & Nunes, 2021; Sánchez Rodríguez et al., 2021; Giménez Gualdo et al., 2021; Martínez De Morentin et al., 2021; Yevseiev et al., 2021; Valente, 2021; Lena Acebo et al., 2022; Martins & Bruno, 2022; Azevedo et al., 2022; Monteiro et al., 2023; Sainz Raso et al., 2023; Jullian et al., 2023; Suárez García & Álvarez García, 2023; Nikolakopoulos et al., 2023; Gaspar et al., 2023; Shevchenko et al., 2023; Sivianes et al., 2023; Wilkinson et al., 2024; Oviedo et al., 2024; Salley et al., 2024; Lampropoulos et al., 2024; Gooder V, 2024; Raza & Moazeni, 2024; Leirmo et al., 2024; Narasimhan et al., 2024; Díaz-Cacho Medina et al., 2024; Moldovyan et al., 2024; De Guillén Gámez et al., 2024; Matos & Guerreiro, 2024; Safarpour et al., 2024; Raza et al., 2024; Pavão J., 2024; Reis et al., 2024; Aristizábal Correa et al., 2019; Astorga Aguilar & Schmidt Fonseca, 2019; Serna Valdivia & Mejía Miranda, 2020; Batista et al., 2020; Perafán del Campo et al., 2021; Saavedra et al., 2021; Flores Ccanto et al., 2021; Flores Montaño et al., 2021; Barria et al., 2021; Ojeda Castro, 2021; Lozano Blasco et al., 2022; Lay Lisboa et al., 2022; Pérez Morón, 2022; Ramírez et al., 2022; Álvarez, 2022; Badilla Quintana et al., 2022; Garcia et al., 2022; Ramírez Plascencia et al., 2022;

Capobianco Peña, 2023; Rioseco Pais et al., 2023; Waller et al., 2023; Delgado Alarcón et al., 2023; Riega Virú et al., 2023; Trejos Gil & Peláez Vélez, 2023; Iparraguirre Villanueva et al., 2023; Cano et al., 2023; Álvarez et al., 2023; Guerrero et al., 2024b; Heguiabehere & Pallero, 2024; Guerrero et al., 2024a; García, 2024; Riega Virú et al., 2024; Gavilanes Molina & Merchán, 2022; Romero Izurieta et al., 2021; Jiménez & Rivera, 2021; Roldán Molina et al., 2017; Olmo Parra et al., 2016).

The results should be interpreted as a synchronous snapshot (summarizing the current state of research at the end of the 2015–2024 period) rather than as a complete historical series. To this end, a phase-structured methodological framework (see Figure 1) was followed to conduct the systematic review and bibliometric analysis.

Phase I: Search Criteria for the Field

- Performance analysis.
- Scientific mapping.
- Search terms: "cybersecurity," "information security," "critical infrastructure," "IoT," "artificial intelligence."
- Study period: 2015–2024.
- Levels of analysis: global, developing countries in the Americas,

Phase II: Selection of Databases and Documents

- Bibliographic database: Scopus.
- Document types: articles, conference proceedings, reviews, book chapters.
- Initial records downloaded by level of analysis.
- Export of results in CSV format and initial cleaning in Excel.

Phase III: Selection Criteria

- Inclusion criteria: focus on cybersecurity or information security; 2015–2024 time period; document types; affiliation with countries/regions of interest.
- Exclusion criteria: editorials, notes, abstracts without full text; records without an abstract or without a country of affiliation.
- Final set after screening: n = 79

Phase IV: Software Selection and Data Processing

- Microsoft Excel: cleaning and standardization of authors, institutions, countries, and keywords; descriptive statistics on publication and citation.
- Bibliometric software (VOSviewer): analysis of bibliometric networks and creation of scientific maps (co-occurrence, co-authorship, co-citation).

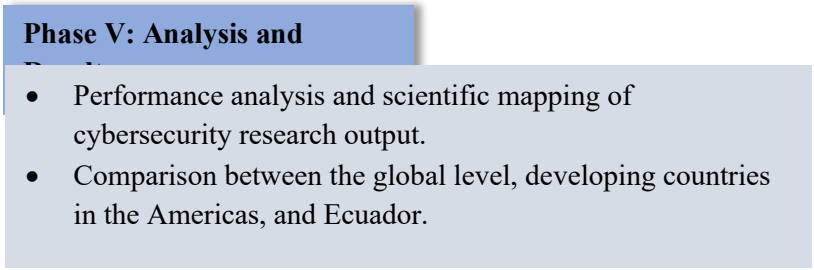

Figure 1. Methodological framework.

The study was organized into three levels of analysis:

1. Global level: international scientific output in cybersecurity without explicit geographic restrictions, used as a reference for the global landscape (Kononovich et al., 2015; Cunha et al., 2018; Duo et al., 2019; Leal et al., 2019; Canuto et al., 2019; Monzelo & Nunes, 2019; Dzhalladova et al., 2019; Mejía Miranda, 2022; Ramirez Peña et al., 2020; Monzelo & Nunes, 2021; Sánchez Rodríguez et al., 2021; Giménez Gualdo et al., 2021; Martínez De Morentin et al., 2021; Yevseiev et al., 2021; Valente, 2021; Lena Acebo et al., 2022; Martins & Bruno, 2022; Azevedo et al., 2022; Monteiro et al., 2023; Sainz Raso et al., 2023; Jullian et al., 2023; Suárez García & Álvarez García, 2023; Nikolakopoulos et al., 2023; Gaspar et al., 2023; Shevchenko et al., 2023; Sivianes et al., 2023; Wilkinson et al., 2024; Oviedo et al., 2024; Salley et al., 2024; Lampropoulos et al., 2024; Gooder V, 2024; Raza & Moazeni, 2024; Leirmo et al., 2024; Narasimhan et al., 2024; Díaz-Cacho Medina et al., 2024; Moldovyan et al., 2024; De Guillén Gámez et al., 2024; Matos & Guerreiro, 2024; Safarpour et al., 2024; Raza et al., 2024; Pavão J., 2024; Reis et al., 2024).
2. Regional level: output from developing countries in the Americas, estimated using records of institutional affiliations in Latin American countries, primarily Brazil, Colombia, Peru, and Mexico (Aristizábal Correa et al., 2019; Astorga Aguilar & Schmidt Fonseca, 2019; Serna Valdivia & Mejía Miranda, 2020; Batista et al., 2020; Perafán del Campo et al., 2021; Saavedra et al., 2021; Flores Ccanto et al., 2021; Flores Montaño et al., 2021; Barria et al., 2021; Ojeda Castro, 2021; Lozano Blasco et al., 2022; Lay Lisboa et al., 2022; Pérez Morón, 2022; Ramírez et al., 2022; Álvarez, 2022; Badilla Quintana et al., 2022; Garcia et al., 2022; Ramírez Plascencia et al., 2022; Capobianco Peña, 2023; Rioseco Pais et al., 2023; Waller et al., 2023; Delgado Alarcón et al., 2023; Riega Virú et al., 2023; Trejos Gil & Peláez Vélez, 2023; Iparraguirre Villanueva et al., 2023; Cano et al., 2023; Alvarez et al., 2023; Guerrero et al., 2024b; Heguiabehere & Pallero, 2024; Guerrero et al., 2024a; García, 2024; Riega Virú et al., 2024).
3. National level: research affiliated with Ecuadorian institutions, which allows for an assessment of Ecuador's specific position within the region (Gavilanes Molina & Merchán, 2022; Romero Izurieta et al., 2021; Jiménez & Rivera, 2021; Roldán Molina et al., 2017; Olmo Parra et al., 2016).

This three-tiered framework makes it possible to contrast the center and the periphery of the global scientific system and to examine the extent to which developing countries in the Americas—and Ecuador in particular—align with or diverge from international cybersecurity agendas (Aguilar Antonio, 2021; Israel's National Cybersecurity Authority, 2022a; Carvajal Bernal & Gómez Rodríguez, 2025; Giraldo Ríos & Gómez Rodríguez, 2025; Israel's National Cybersecurity Authority, 2022b).

In bibliometric studies, it is essential to work with a reliable and carefully curated information source that guarantees the coverage and quality of the records analyzed. For this study, the Scopus database was selected, as it is one of the largest international abstract and citation indexes and offers broad coverage of scientific journals, conference proceedings, and books in most fields of knowledge, including computer science, engineering, and the social sciences—areas where cybersecurity research is concentrated.

Various comparative studies have shown that Scopus ranks among the most widely used and reliable databases for conducting large-scale bibliometric analyses, due to its combination of broad coverage and strict content selection criteria overseen by independent committees (Pranckutė, 2021; Singh et al., 2021).

In addition to its thematic and geographic scope, Scopus incorporates established metrics (such as journal impact factors) and tools for data visualization and structured data export, which facilitate the construction of analysis matrices, the calculation of scientific performance indicators, and the subsequent creation of scientific maps using specialized software. These features explain its frequent use as a primary source in recent systematic reviews and bibliometric analyses across various fields of knowledge (Zupic, 2015; Linnenluecke et al., 2020).

In this study, data were extracted from Scopus in 2024 using the cybersecurity-related descriptors defined in the previous section. Searches were conducted using the TITLE-ABS-KEY option, such that the selected terms had to appear in the title, abstract, or keywords of the retrieved records. Subsequently, filters were applied by year of publication and by country of institutional affiliation to distinguish the different levels of analysis.

Based on these search strategies, three datasets were constructed:

1. Global dataset: 42 international documents related to cybersecurity (Kononovich et al., 2015; Cunha et al., 2018; Duo et al., 2019; Leal et al., 2019; Canuto et al., 2019; Monzelo & Nunes, 2019; Dzhalladova et al., 2019; Mejía Miranda, 2022; Ramirez Peña et al., 2020; Monzelo & Nunes, 2021; Sánchez Rodríguez et al., 2021; Giménez Gualdo et al., 2021; Martínez De Morentin et al., 2021; Yevseiev et al., 2021; Valente, 2021; Lena Acebo et al., 2022; Martins & Bruno, 2022; Azevedo et al., 2022; Monteiro et al., 2023; Sainz Raso et al., 2023; Jullian et al., 2023; Suárez García & Álvarez García, 2023; Nikolakopoulos et al., 2023; Gaspar et al., 2023; Shevchenko et al., 2023; Sivianes et al., 2023; Wilkinson et al., 2024; Oviedo et al., 2024; Salley et al., 2024; Lampropoulos et al., 2024; Gooder V, 2024; Raza & Moazeni, 2024; Leirmo et

al., 2024; Narasimhan et al., 2024; Díaz-Cacho Medina et al., 2024; Moldovyan et al., 2024; De Guillén Gámez et al., 2024; Matos & Guerreiro, 2024; Safarpour et al., 2024; Raza et al., 2024; Pavão J., 2024; Reis et al., 2024).

2. Regional group (developing countries in the Americas): 32 documents with primary affiliations at institutions in Latin America, particularly in Brazil and Colombia, with some co-authors affiliated with institutions in Europe and Oceania (Aristizábal Correa et al., 2019; Astorga Aguilar & Schmidt Fonseca, 2019; Serna Valdivia & Mejía Miranda, 2020; Batista et al., 2020; Perafán del Campo et al., 2021; Saavedra et al., 2021; Flores Ccanto et al., 2021; Flores Montaño et al., 2021; Barria et al., 2021; Ojeda Castro, 2021; Lozano Blasco et al., 2022; Lay Lisboa et al., 2022; Pérez Morón, 2022; Ramírez et al., 2022; Álvarez, 2022; Badilla Quintana et al., 2022; Garcia et al., 2022; Ramírez Plascencia et al., 2022; Capobianco Peña, 2023; Rioseco Pais et al., 2023; Waller et al., 2023; Delgado Alarcón et al., 2023; Riega Virú et al., 2023; Trejos Gil & Peláez Vélez, 2023; Iparraguirre Villanueva et al., 2023; Cano et al., 2023; Alvarez et al., 2023; Guerrero et al., 2024b; Heguiabehere & Pallero, 2024; Guerrero et al., 2024a; García, 2024; Riega Virú et al., 2024).
3. Ecuador Group: 5 papers with Ecuadorian affiliation, many of them involving additional collaborations with institutions in Spain, Mexico, the United Kingdom, and other countries (Gavilanes Molina & Merchán, 2022; Romero Izurieta et al., 2021; Jiménez & Rivera, 2021; Roldán Molina et al., 2017; Olmo Parra et al., 2016).

In all three cases, priority was given to the most common document types in bibliometric literature: scientific articles, conference papers, reviews, and, to a lesser extent, book chapters, in line with methodological recommendations for systematic reviews and bibliometric analyses.

Abstracts, editorial notes, corrections, and other documents that did not provide basic data (publication year, title, institutional affiliation, or keywords) were excluded. Records whose subject matter clearly deviated from the study's core focus—cybersecurity and information security—were also discarded.

Since the available exports correspond to a filtered sample of records by level, the study does not aim to comprehensively reconstruct all existing output for the 2015–2024 period. Rather, it offers an initial comparative analysis based on documents representative of the recent cybersecurity agenda, which allows for the description of publication patterns, relevant topics, and collaborative relationships among the global arena, developing countries in the Americas, and the specific case of Ecuador.

Once the Scopus files were downloaded, a manual screening process was applied to ensure thematic relevance and consistency of the information (Maldonado-Erazo et al., 2021). The screening followed three main steps: (i) analysis of thematic relevance, (ii) review of geographic consistency, (iii) evaluation of record quality.

First, titles, abstracts, and keywords were reviewed to confirm that the main focus of each document was indeed related to cybersecurity, information security, or closely associated topics (e.g., IoT security, data protection, cyber risks, critical infrastructure, cybercrime).

The review of geographic relevance covered three levels:

1. At the global level, studies addressing conceptual frameworks, legal aspects, risk models, or technological applications with an international scope were retained.
2. At the regional level, it was verified that at least one of the primary affiliations corresponded to institutions in developing countries in the Americas; this made it possible to identify work with a Latin American focus, even though some articles included co-authors from developed countries.
3. At the Ecuadorian level, only documents with explicit affiliation to Ecuadorian institutions were retained, whether as the lead institution or as part of international consortia.

Finally, when evaluating the quality of the records, potential duplicates were discarded, and it was verified that each document contained minimum information regarding the year of publication, document type, publication source, and number of citations. The result of this process was a final sample of 79 documents: 42 global, 32 from developing countries in the Americas, and 5 with Ecuadorian affiliation, which constitute the empirical basis of the analysis.

The files exported from Scopus were initially processed in spreadsheets (Microsoft Excel or compatible software) to clean the fields, standardize names, and generate basic indicators of scientific output (number of documents by type, country, and source).

Subsequently, the data were organized by level of analysis (global, regional, national), and several matrices were prepared:

- Productivity (document–year, document–source type, document–country of affiliation).
- Collaboration (co-authorship matrices between institutions and between countries, based on affiliations reported in Scopus).
- Topics (co-occurrence matrices of keywords and title terms).

To explore themes and co-occurrence patterns, procedures were implemented that are compatible with bibliometric tools such as VOSviewer or statistical software packages that allow keywords to be grouped into thematic clusters (Ajibola & Cabral, 2024). Although the sample is small, this approach makes it easier to identify recurring thematic clusters and potential gaps, especially when comparing the global profile with the regional one and the case of Ecuador.

The "affiliation" field was also used to group documents by country and type of institution (universities, public agencies, research centers, law enforcement agencies) and, in this way, identify relevant actors at each level.

The analysis followed two main strands, drawing on classical bibliometric approaches (Donthu et al., 2021; Zupic, 2015; Linnenluecke et al., 2020; Wallin, 2005). First, through a performance analysis, research output was described in terms of the number of documents, publication types (articles, conference papers, reviews, book chapters), participating countries and institutions, and citations received. This section allows us to

assess the relative weight of developing countries in the Americas within the global landscape and to situate Ecuador within that regional context.

The second phase of the analysis involved structural analysis: the predominant themes and the relationships among them were studied through the co-occurrence of keywords, as well as the networks of scientific collaboration among authors, institutions, and countries. The objective was to identify thematic clusters, emerging areas, research gaps, and patterns of convergence or divergence among the global, regional, and national levels (Matilde Espino & Valencia Pérez, 2022; García, 2025; Orosco Fabian, 2024).

Given the characteristics of the sample, the emphasis was not on statistical inference but rather on a comparative qualitative analysis of the observed patterns, which are presented in the results section and discussed in terms of opportunities and challenges for the region and for Ecuador.

Results

Overall, the 79 documents retrieved from Scopus show a very sharp increase in cybersecurity output between 2015 and 2024. To better understand this trend, three stages were identified. The first corresponds to an introductory phase (2015–2018), during which the number of studies was still limited: only 4 publications were identified for the entire period (Kononovich et al., 2015; Cunha et al., 2018; Roldán Molina et al., 2017; Olmo Parra et al., 2016).

This was followed by a growth phase (2019–2021), during which the number of articles increased steadily, reaching a cumulative total of 25. Finally, between 2022 and 2024, a phase of consolidation and expansion takes place, during which 50 publications are concentrated and the sharpest annual increase in output volume is recorded.

This temporal segmentation confirms that the academic community's interest in cybersecurity has intensified, particularly over the last three years, as the topic has evolved from an emerging field to a clearly established area of research. It was noted that the majority of the works consist of scientific articles (53.8%) and conference papers (35.9%), while reviews, books, book chapters, and other types (notes and conference reviews) account for a minority

Given the interdisciplinary nature of the field, most of the works fall within computer science and engineering, although there are also relevant contributions from the social sciences, mathematics, and business management.

The geographic distribution of affiliations reveals clear leadership by European and industrialized countries. Spain is the country with the highest number of documents associated with the search, with 20 publications (25.6%), followed by Portugal, with 13 documents (16.7%). The United States ranks third, contributing 9 papers (11.5%), which confirms the importance of these scientific systems in the development of cybersecurity as a field of research.

The group of countries with intermediate output includes Colombia (8 documents), Peru (6), Mexico (6), and Chile (5). Taken together, these data indicate that Latin America is actively engaged in the international cybersecurity agenda, although its publication volumes still lag behind those of the countries leading the field.

Ecuador, with 5 papers, ranks just below these regional producers. In addition, the *corpus* includes contributions from Uruguay, Ukraine, Norway, Greece, the Russian Federation, Costa Rica, and other countries with one or a few papers, which helps to broaden the geographic diversity of the sample under consideration (see Table 1).

Table 1. *Top 14 countries with the highest number of documents.*

Rank	Country	Documents	Citations
1	Spain	20	332
2	Portugal	13	112
3	United States	9	23
4	Colombia	8	35
5	Mexico	6	6
6	Peru	6	14
7	Chile	5	20
8	Ecuador	5	47
9	Ukraine	3	30
10	Uruguay	3	4
11	Costa Rica	2	20
12	Greece	2	13
13	Norway	2	11
14	Russia	2	4

In addition to institutional affiliations, several particularly active academic hubs stand out. Among them are the University of Trás-os-Montes and Alto Douro (Portugal), the Pontifical Catholic University of Peru, and several engineering colleges at U.S. universities, each with four documents.

A second group includes institutions such as the Universidad Privada del Norte and the University of Castilla-La Mancha, among others. This pattern reveals a combination of European, North American, and Latin American universities that form the core of global output.

As for the most productive authors, the Scopus analysis identifies a small group of researchers with two or more publications during the study period. Among them, Rabadão stands out with three publications, followed by a group of authors with two publications each, as shown in Table 2.

Table 2. *Ranking of authors with the highest number of publications worldwide.*

Author	Institution	Country	Papers	Citations	H-index*
Rabadão, C.	School of Technology and Management, Polytechnic Institute of Leiria, Leiria	Portugal	3	42	2
Moazeni, F.	P.C. Rossin College of Engineering & Applied Science, Bethlehem, PA	United States	2	12	1
Raza, N.	P.C. Rossin College of Engineering & Applied Science, Bethlehem, PA	United States	2	12	1
Monzelo, P.	ISEG Lisbon School of Economics and Management, Lisbon	Portugal	2	10	2
Nunes, S.	ISEG Lisbon School of Economics and Management, Lisbon	Portugal	2	10	2
Santos, L.	School of Technology and Management, Polytechnic Institute of Leiria, Leiria	Portugal	2	7	2
Vieira, L.	School of Technology and Management, Polytechnic Institute of Leiria, Leiria	Portugal	2	7	2
Betarte, G.	Faculty of Engineering, University of the Republic, Montevideo	Uruguay	2	2	1
Campo, J.	Faculty of Engineering, University of the	Uruguay	2	2	1

Guerrero, G.	Republic, Montevideo Faculty of Engineering, University of the Republic, Montevideo	Uruguay	2	2	1
Nilupú, K.	Faculty of Law, Universidad Privada del Norte, Trujillo, La Libertad	Peru	2	2	1
Ninaquispe, M.	Universidad Privada del Norte, Trujillo, La Libertad	Peru	2	2	1
Riega, Y.	Universidad Privada del Norte, Trujillo, La Libertad	Peru	2	2	1
Salas, J.	n Pontifical Catholic University of Peru, Lima	Peru	2	2	1

* H-index calculated solely based on citations of works related to cybersecurity, not on the author's entire output in Scopus.

The relatively dispersed distribution of authorship, with no clearly dominant figures, suggests a field in the process of consolidation, with multiple research groups making complementary contributions to the development of knowledge in cybersecurity.

In the case of developing countries in the Americas, the analysis identified 37 publications linked to institutions in Latin America and the Caribbean during the 2015–2024 period. These contributions account for nearly half of the global output included in this study (79 documents), indicating that the region has been incorporating cybersecurity as an established line of research.

Most of these works are concentrated in the last four years of the analyzed period, suggesting a recent expansion and a process of progressive specialization in cybersecurity. The evolution of Latin American research output over time follows a phased pattern. Between 2016 and 2017, barely one article per year was published, and in 2018, no publications were identified in the sample—a sign of interest that was still in its infancy and scattered across the region.

Starting in 2019, a phase of moderate growth began, with two studies in 2019 and another two in 2020. Although the volume remains low, these years mark the transition from sporadic contributions to more continuous output, during which collaborations between institutions from different Latin American countries began to take hold.

The consolidation phase took place between 2021 and 2024, a period during which the majority of regional documents were produced and in which cybersecurity became more firmly established on the region's research agendas. In 2021, 8 documents were identified, a figure that rose to 9 publications in both 2022 and 2023, while in 2024, 5 papers were recorded.

Taken together, these four years account for 31 of the 37 Latin American publications, confirming that interest in cybersecurity in developing countries in the Americas is a recent and expanding phenomenon. Furthermore, in several of these years, the region's contributions accounted for between one-third and two-thirds of the global publications in *the corpus*, reinforcing its growing role on the international stage.

The analysis by country shows that cybersecurity research output is concentrated in a small group of scientific systems. Colombia tops the regional ranking with 8 documents and 35 citations, making it the country with the highest volume of publications in the sample (see Table 3); it is followed by Peru, with 7 papers and 18 citations, and Mexico, with 6 publications and 6 citations.

Table 3. Most-cited Colombian publications.

Ranking	Author(s)	Year	Title	Citations	Reference
1	Pérez Morón, J.	2022	Eleven Years of Cyberattacks on Chinese Supply Chains in an Era of Cyber Warfare: A Review and Future Research Agenda	14	(Pérez Morón, 2022)
2	Ramírez, M.; Rodríguez Ariza, L.; Gómez Miranda, M.E.; Vartika, I	2022	The Disclosure of Cybersecurity Information by Listed Companies in Latin America—Proposal for a Cybersecurity Disclosure Index	12	(Ramírez et al., 2022)
3	Perafán del Campo, E.A.; Polo Alvis, S.; Sánchez Acevedo, M.E.; Miranda Aguirre, C.	2021	State and Sovereignty in Cyberspace	4	(Perafán del Campo et al., 2021)
4	Trejos Gil, C.A.; Peláez Vélez, Y.	2023	Cybercrimes Involving Minors on Facebook: A Systematic Literature Review	1	(Trejos Gil & Peláez Vélez, 2023)
5	Cano, J.J.; Almanza, A.R.	2023	The Information Security Function and the CISO in Colombia: 2010–2020	1	(Cano et al., 2023)

6	Ramírez Plascencia, D.; Alonzo González, R.M.; Marín Tapiero, J.I.	2022	Risks Faced by Underage YouTubers Due to Legislative Gaps in Mexico	1	(Ramírez Plascencia et al., 2022)
7	Ojeda Castro, F.A.	2021	Origin, Use, and Meaning of the Innovation Diamond	1	(Ojeda Castro, 2021)
8	Aristizábal Correa, J.M.; Marín Ramírez, L.; Álvarez Salazar, J.	2019	Identification of safety elements based on the C2M2 model for the textile manufacturing industry	1	(Aristizábal Correa et al., 2019)

Chile and Ecuador rank in a second tier, both with 5 publications, though with different impact profiles: while Chile has accumulated 20 citations, Ecuador has reached 47 citations during the period analyzed, indicating greater average visibility for its work. Uruguay contributes 3 publications and 4 citations, and Costa Rica stands out with only 2 documents but 20 citations, suggesting the existence of specific, high-impact contributions. Finally, there are countries with a still-emerging presence, such as Argentina, Brazil, Cuba, Honduras, and Jamaica, with one document each and varying citation levels.

When the data is broken down by institution, it becomes clear that regional output is concentrated in a few universities and research centers. In terms of volume, the Pontifical Catholic University of Peru (Lima) stands out, contributing 3 documents related to cybersecurity and accumulating 5 citations.

Next is the Faculty of Engineering at the University of the Republic (Uruguay), with 2 publications and 2 citations, along with the Universidad Privada del Norte (Trujillo, Peru), which also contributes 2 papers and 2 citations. The University of Guadalajara (Mexico) also has 2 publications and 3 citations, confirming its steady presence in regional output.

In addition, some institutions with fewer articles have made a striking impact. This is the case of the Business Department at the Technological University of Bolívar (Colombia), which has received 14 citations for a single paper, and the Cybersecurity Research Center (CICS) at Universidad Mayor (Chile), whose published work has garnered 3 citations. These cases illustrate how certain institutions have managed to position specific, high-visibility contributions, even though their volume of publications remains limited.

As for the most productive authors in developing countries in the Americas, the analysis identifies several researchers with two publications and a modest h-index during the period under consideration. From Uruguay, Gustavo Betarte, Juan Diego Campo, and

Guillermo Guerrero stand out—all affiliated with the Faculty of Engineering at the University of the Republic—while from Peru, Kiara Nilupú Moreno, Mario E. Ninaquispe Soto, Yasmina Beatriz Riega Virú, and Juan Luis Salas Riega, who are primarily affiliated with the Universidad Privada del Norte (Trujillo) and the Pontificia Universidad Católica del Perú (Lima).

In the case of Ecuador, the Scopus search identified five publications with at least one Ecuadorian affiliation during the 2016–2022 period. Although the number of works is lower than that of other countries in the region, the set of Ecuadorian publications has garnered 47 citations, indicating a notable impact relative to its volume. Furthermore, this output is strongly supported by international collaboration, with co-authorships linking Ecuadorian universities to institutions in Spain, Portugal, and Mexico, among other countries, which reinforces its visibility beyond the national sphere.

The timeline shows that Ecuador's presence in this field began to emerge in 2016 and 2017, with one article published each year. Both focus on the analysis and management of information security risks: one proposes a methodology associated with the ISO 27001 standard (9 citations), and the other compares different cybersecurity risk analysis tools, a study that has received 35 citations. In 2022, a new study on information technology governance in Ecuador was published

If we consider only the number of documents, Ecuador ranks second in regional scientific output, with 5 publications—a figure close to that of Chile (5) and slightly below that of Colombia (8) and Peru and Mexico (6 each). However, the picture changes when looking at the average number of citations per article: Ecuadorian works average about 9.4 citations per document, while Colombia averages around 4.4, Chile 4, Peru approximately 3, and Mexico around 1 citation per publication (see Table 3).

An examination of affiliations shows that Ecuadorian research output is concentrated in a small group of institutions. Among them, the University of the Armed Forces (ESPE) stands out, appearing in three of the records, primarily through its Department of Computer Science. This university participates in both methodological studies on risk analysis and articles co-authored with European universities, positioning it as one of the leading national institutions in this field.

The National Polytechnic School appears in two publications, related to cybersecurity in the Internet of Things (IoT) and engineering systems. Meanwhile, UTE University participates in at least one study related to information technology governance. Other institutions listed among the Ecuadorian affiliations include Milagro State University, Yachay Tech University, and the Salesian Polytechnic University.

Among the authors affiliated with Ecuadorian institutions, some names appear repeatedly and hold key positions on research teams. These include Roldán Molina, Almache Cueva, and Gavilanes Molina, along with other researchers associated with both the National Polytechnic School and the University of the Armed Forces (ESPE).

Within the analyzed set, the most influential paper is "A Comparison of Cybersecurity Risk Analysis Tools" (Roldán Molina et al., 2017), which has accumulated 35 citations. In

second place is "Methodology for Dynamic Analysis and Risk Management on ISO 27001," with 9 citations (Olmo Parra et al., 2016); both papers are closely related to the analysis and management of information security risks. The most recent articles, focusing on IT governance, information security in the public sector, and cybersecurity in the IoT, still have a lower number of citations.

An analysis of the "Author Keywords" identified 368 occurrences of keywords, grouped into 305 distinct terms. Most appear only once, while only a small group is repeated across multiple papers. Despite the wide range of terms, at least four major thematic blocks can be distinguished that organize global cybersecurity research.

A first group brings together studies on risks and protection on the Internet and social media; a second cluster focuses on cybersecurity applied to infrastructure, IoT environments, and Industry 4.0 initiatives; a third addresses educational dimensions and the development of digital competence; and a fourth concentrates on governance, corporate management, and financial reporting.

Viewed as a whole, cybersecurity functions as a cross-cutting theme that intersects with technical, organizational, educational, and social issues, rather than as an isolated or exclusively technological field. The keyword "Cybersecurity" (or its spelling variants in English and Spanish) is clearly dominant and is associated with terms that refer both to specific technologies (Internet, Internet of Things, network intrusion detection, cyber range) and to areas of application (education, healthcare, supply chain, public administration).

When grouping keywords into thematic families, the most frequently addressed research area in developing countries in the Americas is "Cybercrime and Risks on Social Media," which appears in 5 out of 37 documents. This category includes *keywords* such as *cyberbullying, cybercrime, social networks, online grooming, sexting, internet addiction, and young people.* The associated studies analyze, among other aspects, cybercrimes against minors on Facebook, addiction to new technologies and its relationship to cyberbullying in Costa Rica, and online interactions among Chilean youth during and after the pandemic.

Emerging Areas with Strategic Potential

Several emerging areas stand out which, although they are represented by only one or two studies, offer high strategic potential for future research:

AI, software quality, and cybersecurity: The appearance of keywords such as *"AI application quality," "AI data quality,"* and *"AI engineering"* alongside cybersecurity terms suggests an initial concern for the quality and security of AI-based applications.

Post-quantum cryptography and *blockchain* in security contexts: The isolated presence of *"post-quantum cryptography"* and *"blockchain technology"* foreshadows a line of research focused on protecting systems against quantum threats and using *blockchain* to ensure integrity, traceability, and identity management.

Security in Complex Supply Chains and Global Services: Although the keyword *"supply chain"* appears explicitly in several papers, the number of studies remains small. However, the intersection of logistics, services, and digital risk points to a line of research with room for further growth.

Cybersecurity in healthcare and clinical data supported by new technologies: Articles addressing the protection of health information and the processing of clinical data—through concepts such as *health information protection, clinical data, data privacy*, and *process mining*—confirm that cybersecurity in healthcare is an emerging issue.

Global South perspective and comparative North–South approaches: The isolated presence of keywords such as *"Global South"* and specific references to regions such as the Caribbean or Southeast Asia reveals that analyses remain, to a large extent, fragmented and lack comparative analysis.

First, there is a low number of studies on cybersecurity in critical economic sectors, despite its importance to the region. The sample includes occasional references to supply chains and maritime services, but there are almost no studies addressing the security of energy infrastructure, transportation networks, banking and financial services, telecommunications, or water systems from a Latin American perspective (Dzhalladova et al., 2019; Ramirez Peña et al., 2020). Most studies on the Internet of Things (IoT) focus on general technical aspects or experimental scenarios, without systematically delving into specific sectoral cases (Martínez De Morentin et al., 2021; Martins & Bruno, 2022; Jullian et al., 2023; Serna Valdivia & Mejía Miranda, 2020; Jiménez & Rivera, 2021).

A second gap lies at the intersection of cybersecurity, healthcare, and clinical data protection. Although there are some studies that analyze the protection of health information and the use of techniques such as *process mining*, their number remains small relative to the importance that the digitization of healthcare systems has acquired in Latin America. There are hardly any comparative analyses of security breaches, health data governance, or the impact of cybersecurity incidents on hospitals and clinics in the region (Cunha et al., 2018; Monteiro et al., 2023; Gooder V, 2024).

Research on the economic and financial dimensions of cybersecurity is also limited (Ramirez Peña et al., 2020). Apart from isolated mentions of the risks and costs associated with information security management, there is no significant body of studies analyzing the costs of incidents, investment in cybersecurity capabilities, or the impact on competitiveness or the attraction of foreign investment—neither from the perspective of companies nor of governments.

A fourth area that has barely been explored is that of ethics, digital rights, and inequalities. Keywords linked to *gender, the Global South, vulnerable groups*, or explicit rights-based approaches have a very limited presence in the sample (Suárez García & Álvarez García, 2023; Wilkinson et al., 2024). In general, technical or organizational analyses dominate, while topics such as digital surveillance, biases and mechanisms of discrimination, differences in access to protective measures, or the impact of cybersecurity on particularly vulnerable groups—such as rural populations, indigenous peoples, or migrants—are scarcely discussed.

Finally, the sample contains only very few references to artificial intelligence, advanced cryptography, or *blockchain* in relation to cybersecurity (Gaspar et al., 2023; Narasimhan et al., 2024; Giraldo Ríos & Gómez Rodríguez, 2025). These are topics that feature prominently on the international agenda but have yet to gain significant traction at the regional level.

The experience gained from some studies on maritime supply chains and global services could be expanded through regional consortia that develop comparative models, maturity indicators, and best practices applicable to different countries.

In the field of health, early studies on privacy and the management of clinical data pave the way for the formation of research networks that bring together hospitals, ministries of health, and universities from different countries. This type of collaboration would allow for a joint study of security incidents, data breaches, and the various forms of governance regarding health information.

From a social and legal perspective, the experience already gained from studies on cybercrime and risks on social media could be leveraged to launch regional observatories dedicated to closely monitoring phenomena such as digital violence, disinformation, surveillance practices, and inequalities in access to protective mechanisms.

Finally, the scarcity of research linking AI and cybersecurity opens up a strategic avenue for collaborative projects that bring together data science labs, cybersecurity groups, and public policy teams.

Based on an analysis of the keywords and titles of the five studies, several critical areas can be identified where Ecuadorian research output is virtually nonexistent during the period analyzed:

First, in the areas of cybercrime, social media, and child protection, no national studies were found that address phenomena such as cyberbullying, cybercrime, social media, or online grooming, even though these topics feature prominently in studies from neighboring countries and are part of the regional agenda on digital risks affecting children and adolescents (Suárez García & Álvarez García, 2023; Lozano Blasco et al., 2022; Riega Virú et al., 2023; Trejos Gil & Peláez Vélez, 2023).

A similar situation exists in the area of digital competencies and cybersecurity education. Documents with Ecuadorian affiliation do not include keywords such as "digital competence," "teachers in training," "primary/secondary education," or "teacher training," whereas in countries such as Chile, Peru, and Costa Rica, analyses have been published on the digital competencies of students and teachers at these educational levels (De Guillén Gámez et al., 2024; Rioseco Pais et al., 2023).

There is also a gap in cybersecurity related to healthcare and clinical data. Although studies on "health information protection," "clinical data," and "data privacy" do appear in the global body of research, none of the studies linked to Ecuador address

the protection of health data, the security of electronic health records, or incident management in hospitals and other healthcare services.

As for strategic productive sectors and essential services, no Ecuadorian research has been identified in areas such as energy, transportation, banking, telecommunications, agriculture, or supply chains. Nor are there any specific studies on tax administration, the justice system, public safety, or local governments from a cybersecurity perspective.

Finally, in the field of cutting-edge cybersecurity technologies, none of the five studies with Ecuadorian affiliation explicitly incorporates keywords related to artificial intelligence, machine learning, *blockchain,* advanced cryptography, or "zero-trust" architectures. Although the article on IoT touches on technical security issues, the corpus as a whole does not yet address the convergence between cybersecurity and emerging technologies, a topic that is beginning to emerge in other contexts (Martínez De Morentin et al., 2021; Shevchenko et al., 2023; Sivianes et al., 2023; García, 2024; Jiménez & Rivera, 2021).

The thematic gaps described are related to several structural challenges that emerge from the analysis of the Ecuadorian corpus:

Low volume and high institutional concentration: Publications are identified only in connection with a small set of institutions (primarily universities in the Sierra region and collaborations with European centers) (Roldán Molina et al., 2017; Olmo Parra et al., 2016).

Reliance on external collaborations for advanced topics: The only study that explicitly addresses cybersecurity in the Internet of Things (IoT) is conducted in a comparative context with European Union countries and involves significant participation from foreign institutions (Jiménez & Rivera, 2021).

Clear preference for standards and models: Several studies focus on risk analysis and *IT governance*, concentrating on discussing methodologies, reference frameworks, and decision-making structures (Jiménez & Rivera, 2021; Roldán Molina et al., 2017; Olmo Parra et al., 2016), whereas studies applied to concrete situations or specific sectors are scarce.

Precisely for this reason, several opportunities for future work are emerging: conducting empirical research on social media, education, and vulnerable groups; studying cybersecurity in key productive sectors and public services; systematically incorporating emerging technologies into the national cybersecurity agenda; and strengthening both regional collaboration networks and advanced training programs.

A pattern of co-authorship based on small and medium-sized teams is evident: the average is approximately 3.5 authors per article, ranging from 1 to 10 authors (see Figure 11). In most cases, between 2 and 4 researchers are involved, suggesting working groups typical of university-level research projects.

Looking at the distribution by country, co-authorship is predominantly national. Approximately three out of every four articles (59 out of 79) were authored solely by

institutions from the same country, with no external participation. Only 19 papers include affiliations from at least two countries, and in only one case do four countries appear in the same article.

At the global level, the countries most involved in co-authorship are Spain, Portugal, and the United States, which frequently serve as partners in international teams. Spain appears as a collaborating country in several articles with Colombia, Ecuador, Chile, and Costa Rica, and Portugal is particularly linked to Ecuador and Macao, as well as to the United States.

At the regional level, the Latin American countries with the strongest presence in co-authorship are Colombia, Peru, Mexico, Chile, Ecuador, Uruguay, Costa Rica, Honduras, Cuba, and Jamaica, although a significant portion of their articles continue to be authored solely by researchers with national affiliations.

In Ecuador, co-authorship follows this general pattern but with a relatively high degree of international openness. The five articles with Ecuadorian affiliations are written by teams of between 2 and 5 authors and combine exclusively domestic work with publications produced in collaboration with institutions in Spain, Portugal, Mexico, and Peru.

Based on the co-occurrences of countries in the affiliations, several clearly recognizable collaboration clusters can be distinguished:

Iberian–Latin American cluster: Spain is frequently linked with Colombia, Ecuador, Chile, and Costa Rica, while Portugal maintains collaborations with Ecuador and other European partners, such as Macau and Italy. In practice, this forms a network in which several Iberian research groups serve as a bridge between European and Latin American universities, particularly in studies on IT governance, cybersecurity in the IoT, digital skills, and risk analysis.

Intra-regional Latin American cluster: Teams comprising institutions from Colombia, Mexico, Peru, and Ecuador have been identified, with frequent combinations such as Colombia–Mexico, Ecuador–Mexico, Ecuador–Peru, and Mexico–Peru. The publications primarily address issues of organizational cybersecurity, the design and evaluation of cybersecurity policies and programs, as well as studies on risks in social media and digital skills at various educational and professional levels.

English-speaking and Caribbean cluster: A third set of collaborations is organized around Jamaica, the United States, and the United Kingdom. This cluster includes works that analyze the challenges associated with the *dark web*, global digital services, and various aspects of cybersecurity in the Caribbean. In these collaborations, Caribbean universities and research centers work as co-authors with British and American institutions, reinforcing the region's connection to the English-speaking tradition of studies in this field.

Eastern European and Euro-Eastern Cluster: More specifically, there are collaborations linking Cuba with the Russian Federation and Ukraine with the Czech Republic. The work

in this cluster focuses primarily on the protection of critical infrastructure, the design of intrusion detection models, and cybersecurity challenges at the state level, offering a unique perspective on the role of cybersecurity in contexts marked by heightened geopolitical tensions.

Within the collaboration network, Ecuador occupies a middle ground between several clusters. On the one hand, it is part of the Iberian–Latin American axis through work carried out alongside teams from Spain and Portugal; on the other hand, it is integrated into the Latin American cluster through co-authored publications with institutions in Peru and Mexico. At the same time, it maintains a small but consistent body of exclusively domestic research. This combination of external links and independent research gives Ecuador a potentially significant role as a connecting node between different regional subnetworks.

To assess the impact of a field of study, the citation patterns of documents are typically analyzed. In this study, the scientific output on cybersecurity identified in the sample (79 documents) has accumulated a total of 582 citations in Scopus. Table 5 presents the 10 most-cited articles at each level of analysis (global, developing countries in the Americas, and Ecuador), which together account for a considerable proportion of the impact observed during the 2015–2024 period.

Table 5. Ranking of Authors and Articles with the Greatest Impact.

R	Authors	Year	Title	Citations	Reference
1	Ramirez Peña, M.; Sánchez Sotano, A.J.; Pérez Fernández, V.; Abad, F.J.; Batista Ponce, M.	2020	Achieving a Sustainable Shipbuilding Supply Chain from an Industry 4.0 Perspective	135	(Ramirez Peña et al., 2020)
2	Jullian, O.; Otero, B.; Rodríguez, E.; Gutierrez, N.; Antona, H.; Canal, R.	2023	Deep-Learning-Based Detection of Cyberattacks in IoT Networks: A Distributed Attack Detection Framework	79	(Jullian et al., 2023)
3	Gaspar, J.; Cruz, T.; Lam, C.T.; Simoes, P.	2023	Smart Substation Communications and Cybersecurity: A Comprehensive Survey	53	(Gaspar et al., 2023)
4	Roldán Molina, G.; Almache Cueva, M.; Rabado Silva, C.; Yevseyeva, I.; Basto Fernandes, V.	2017	A Comparison of Cybersecurity Risk Analysis Tools	35	(Roldán Molina et al., 2017)
5	Duo, A.; Basagoiti, R.; Arrazola, P.J.; Aperribay, J.; Cuesta, M.	2019	The capacity of statistical features extracted from multiple signals to predict tool wear in the drilling process	27	(Duo et al., 2019)

6	Pérez Morón, J.	2022	Eleven Years of Cyberattacks on Chinese Supply Chains in an Era of Cyber Warfare: A Review and Future Research Agenda	14	(Pérez Morón, 2022)
7	Dzhalladova, I.; Škapa, S.; Novotná, V.; Babynyuk, A.	2019	Design and Analysis of a Model for Detecting Information Attacks in Computer Networks	14	(Dzhalladova et al., 2019)
8	Martínez De Morentin, J.I.; Lareki, A.; Altuna Urdin, J.	2021	Risks Associated with Posting Content on Social Media	13	(Martínez De Morentin et al., 2021)
9	Astorga Aguilar, C.; Schmidt Fonseca, I.	2019	Social Media Dangers: How to Educate Our Children About Cybersecurity	13	(Astorga Aguilar & Schmidt Fonseca, 2019)
10	Ramírez, M.; Rodríguez Ariza, L.; Gómez Miranda, M.E.; Vartika, I.	2022	The Disclosure of Cybersecurity Information by Listed Companies in Latin America—Proposal for a Cybersecurity Disclosure Index	12	(Ramírez et al., 2022)

3.5.2. Authors with the greatest scientific impact

The cybersecurity information corpus considered in this study includes 258 authors, of whom 61 have at least 10 citations within the *corpus.* Table 6 lists the 10 authors with the highest number of citations in the sample, along with their total link strength and their country and primary affiliated institution.

Table 6. Top 10 authors.

R	Author	Citations	Total Link Strength	Country	Primary affiliation
1	Ramirez Peña, M.	135	4	Spain	University of Cádiz, Cádiz
2	Sánchez Sotano, A.J.	135	4	Spain	University of Cádiz, Cádiz
3	Pérez Fernández, V.	135	4	Spain	University of Cádiz, Cádiz
4	Abad, F.J.	135	4	Spain	Navantia S.A., Cádiz
5	Batista Ponce, M.	135	4	Spain	University of Cádiz, Cádiz
6	Jullian, O.	79	5	Spain	Polytechnic University of Catalonia, Barcelona
7	Otero, B.	79	5	Spain	Polytechnic University of Catalonia, Barcelona

8	Rodríguez, E.	79	5	Spain	Polytechnic University of Catalonia, Barcelona
9	Gutierrez, N.	79	5	Spain	Polytechnic University of Catalonia, Barcelona
10	Antona, H.	79	5	Spain	Polytechnic University of Catalonia, Barcelona

Table 7 lists the 10 sources with the highest number of citations in the sample, along with their total link strength, approximated here by the number of documents published in each source within the corpus. It can be observed that high-impact international journals, such as *the Journal of Cleaner Production*, account for a high volume of citations with a single article, while other sources combine a more frequent presence in the sample with a significant impact on topics such as education, digital skills, and social cybersecurity.

Table 7. Leading journals in cybersecurity publications in the analyzed sample.

Ranking	Source	Citations	Total Link Strength*
1	*Journal of Cleaner Production*	135	1
2	*Journal of Network and Systems Management*	79	1
3	*IEEE Communications Surveys and Tutorials*	53	1
4	*Procedia Computer Science*	35	1
5	*International Journal of Advanced Manufacturing Technology*	27	1
6	*Educare Electronic Journal*	20	2
7	*Journal of Asia Business Studies*	14	1
8	*Economic Computation and Economic Cybernetics Studies and Research*	14	1
9	*Educational Sciences*	14	2
10	*Ibero-American Journal of Learning Technologies*	13	1

* In this study, total link strength is approximated by the number of documents in the sample published in each source (a higher number of articles implies a greater degree of connection between the journal and the rest of the publication network).

A joint analysis of the three levels considered (global, developing countries in the Americas, and Ecuador) reveals a shared thematic core that structures cybersecurity research. In all three cases, at least four cross-cutting themes emerge, with varying degrees of emphasis: (i) risk management and information security in organizations; (ii) the protection of infrastructure and connected systems (especially the Internet of Things and Industry 4.0); (iii) risks associated with the use of the Internet and social media; and (iv) concerns regarding cybersecurity training and skills.

On a global scale, these themes are reflected in studies on industrial supply chains, smart substations, advanced methods for detecting attacks on IoT networks, and analyses of the risks associated with posting content on social media.

In Latin America, these same topics take on a different nuance: risk management and security policies are combined with research on cyberbullying, cybercoexistence, and problematic social media use among adolescents. At the same time, cybersecurity training is primarily addressed through the development of digital skills among teachers and students. In the case of Ecuador, the predominant areas of focus are directly aligned with this common core.

The analysis also reveals significant differences in how research is structured at each level. On a global scale, highly technologically complex studies predominate, and the emphasis is on the sophistication of technical solutions and the handling of critical infrastructure with a strong industrial component.

In developing countries in the Americas, the agenda is more hybrid, but the region exhibits a specific profile in which cybersecurity is closely intertwined with educational and social issues. Ecuador, for its part, shows a specialization more focused on process engineering and organizational management.

A combined analysis of convergences and divergences allows us to outline several strategic perspectives to guide future research in cybersecurity, particularly from the perspective of developing countries and the Ecuadorian case:

International research accounts for a significant portion of the most technical advances, particularly in intrusion detection, security in IoT environments, and the protection of critical infrastructure. In contrast, Latin American research contributes more heavily to studies on social media, adolescents and youth, educational processes, and inequalities, thereby enriching the field with distinct questions and contexts.

A promising approach is to promote work that combines both perspectives: for example, technologically sophisticated detection and prevention models applied to socially sensitive issues such as cyberbullying, misinformation, or the protection of vulnerable groups.

In Ecuador, the evidence points to a well-established track record in risk analysis and IT governance, although there are still few direct applications to specific sectors. Applying this methodological expertise to empirical studies in fields such as health, energy, transportation, finance, or local government would help better align national research output with the sectoral priorities already being discussed in the international literature.

The contrast between global, regional, and national agendas highlights the need to promote comparative research that allows for a joint analysis of capacity gaps, resource asymmetries, and regulatory differences that shape how each context approaches cybersecurity. This includes comparisons both among countries in the region and between Latin American countries and economies with high technological capacity, incorporating shared indicators of risk, resilience, and governance.

Topics such as artificial intelligence applied to cybersecurity, post-quantum cryptography, blockchain for data protection and traceability, and zero-trust architectures barely feature on the regional and national agendas. Given their growing

importance in the global debate, they represent fertile ground for collaborative projects that combine external technical expertise with local contextual knowledge.

Research on cybersecurity has grown steadily over the past two decades, but in this study we have focused on the period 2015–2024 (specifically on 79 documents), when the field took on a more systematic structure and clearly recognizable lines of research began to take shape.

Three distinct phases in the field's evolution can be clearly identified: an initial phase between 2015 and 2018, an intermediate phase in 2019–2020, and a more intense period between 2021 and 2024. Taken together, these stages show that cybersecurity has evolved from appearing sporadically and in a fragmented manner to establishing itself as a recognizable field of research, with a conceptual and empirical foundation sufficient to begin discussing relatively stable trends and specializations.

When mapping the data by country, 26 nations are identified with at least one contribution, with Spain and Portugal playing a particularly prominent role, followed by the United States and a group of Latin American countries led by Colombia, Peru, Mexico, Chile, and Ecuador. This research output is disseminated through a wide variety of channels: journals with high international visibility in engineering and management coexist with journals focused on education and the social sciences, confirming that cybersecurity is grounded in a dual disciplinary foundation, straddling information technology and the applied social sciences.

The intellectual structure of the field was reconstructed using various bibliometric maps. The keyword co-occurrence map (Figure 5) identifies "Cybersecurity" as the central term: it appears in 28 documents and is associated with more than 300 different terms, reflecting the diversity of approaches and contexts in which it is used. Based on these connections, several thematic clusters emerge, grouping issues of a technical nature (infrastructure, IoT, attack detection), organizational (risk analysis, governance, policies), and social (social media, education, digital skills) nature.

An analysis of citations and the most influential authors helps identify which research areas carry the most weight at each level. Globally, research on supply chains and resilience in Industry 4.0, the detection of cyberattacks on IoT networks, and studies examining cyberattacks on supply chains from a risk and geopolitical perspective stand out.

In Latin America, the focus is on studies regarding risks on social media and cybersecurity education for children and adolescents, the disclosure of cybersecurity information by publicly traded companies, and research centered on teachers' digital skills. In Ecuador, the impact is concentrated in articles comparing risk analysis tools and the methodology for dynamic risk analysis and management according to ISO 27001, which have become essential references in the country's academic output.

The co-citation map of sources helps identify which journals serve as true hubs for the dissemination of knowledge in this field. Among the most prominent are, on a global level, the *Journal of Cleaner Production* and, on a regional level, the *Revista

Electrónica Educare*. The former contributes only one article to the corpus, but that single paper accounts for 135 citations, while the latter includes two publications totaling 20 citations. Although the number of documents is small, the volume of citations associated with these sources demonstrates their central role in the circulation of cybersecurity findings within the analyzed contexts.

Conclusions

This study offers a comprehensive overview of cybersecurity research from 2015 to 2024, combining three levels of analysis: global, developing countries in the Americas, and Ecuador. Based on a set of documents indexed in Scopus, the study examined the evolution of research output, the main themes, research gaps, collaboration networks, and the publication sources that shape the field. The comparative approach adopted in this study goes beyond a simple count of articles and citations and offers a comprehensive analysis of how the field is shaped at different levels.

In general terms, the results show that cybersecurity is a rapidly expanding field, with a set of well-established research lines centered on risk management, the protection of connected infrastructure (IoT, smart substations, supply chains), and information security in organizations.

This core is clearly evident in global research output and, with some nuances, also in much of the regional and national research (Lampropoulos et al., 2024; Gooder V, 2024; Raza & Moazeni, 2024; Leirmo et al., 2024; Narasimhan et al., 2024; Díaz-Cacho Medina et al., 2024; Moldovyan et al., 2024; De Guillén Gámez et al., 2024; Matos & Guerreiro, 2024; Safarpour et al., 2024; Raza et al., 2024; Pavão J., 2024; Reis et al., 2024; Aristizábal Correa et al., 2019; Astorga Aguilar & Schmidt Fonseca, 2019; Serna Valdivia & Mejía Miranda, 2020; Batista et al., 2020; Perafán del Campo et al., 2021; Saavedra et al., 2021; Flores Ccanto et al., 2021; Flores Montaño et al., 2021; Barria et al., 2021; Ojeda Castro, 2021; Lozano Blasco et al., 2022; Lay Lisboa et al., 2022; Pérez Morón, 2022; Ramírez et al., 2022; Álvarez, 2022; Badilla Quintana et al., 2022; Garcia et al., 2022; Ramírez Plascencia et al., 2022; Capobianco Peña, 2023; Rioseco Pais et al., 2023; Waller et al., 2023; Delgado Alarcón et al., 2023; Riega Virú et al., 2023; Trejos Gil & Peláez Vélez, 2023; Iparraguirre Villanueva et al., 2023; Cano et al., 2023; Álvarez et al., 2023; Guerrero et al., 2024b; Heguiabehere & Pallero, 2024; Guerrero et al., 2024a; García, 2024; Riega Virú et al., 2024; Gavilanes Molina & Merchán, 2022; Romero Izurieta et al., 2021; Jiménez & Rivera, 2021; Roldán Molina et al., 2017; Olmo Parra et al., 2016). At the same time, the concentration of a large number of citations in a few highly influential articles suggests that the field still relies heavily on certain landmark contributions.

There is a distinct body of work emerging from developing countries in the Americas that is not always captured in global studies: cybersecurity is being vigorously addressed as a social and educational issue, linked to social media, cyberbullying, digital coexistence, digital literacy, and inequalities. This perspective explicitly incorporates issues of rights, child protection, and teacher training, and opens up fertile ground for research that combines technical solutions with public policies and concrete pedagogical practices.

Within this landscape, Ecuador emerges as a rising player with a distinct thematic profile. Although the number of publications is small, the works are published in high-visibility journals and conference proceedings and focus on key topics for the region: , risk analysis methodologies, implementation of ISO standards in cybersecurity, IT governance in the public sector, and an initial line of research on IoT security (Jiménez & Rivera, 2021).

When considering the average number of citations per document, performance is high, suggesting a certain "efficiency" in national research output. However, clear gaps persist in areas such as social media, cybersecurity education, and health data protection. An analysis of co-authorship and publication sources also confirms that the field is supported by a diverse network of collaborations.

The Iberian–Latin American axis plays a central role, alongside intra-regional and Caribbean clusters that, although still sparse, provide a foundation for moving toward more stable research consortia. The journals that account for the bulk of this output combine well-established titles in engineering and management with specialized publications in education and the social sciences, reflecting the distinctly interdisciplinary nature of the field and opening up various channels for developing countries to disseminate their findings.

Finally, it is worth noting that these conclusions are based on a limited sample and a single database. Even so, the analytical framework developed offers a solid starting point for deepening, updating, and expanding the study in future research, incorporating new time periods, other databases, and greater detail in the analysis of networks and themes.

For researchers, policymakers, and stakeholders in the innovation system, the evidence presented can serve as a basis for prioritizing investments, designing training programs, and guiding national and regional cybersecurity strategies, with special attention to the needs and capabilities of developing countries—and, in particular, Ecuador.

References

Aguilar Antonio, J. M. (2020). The Cybersecurity Gap in Latin America in the Context of Global Threats. Journal of International Security Studies, 6(2), 17–43.

Aguilar, Antonio, J. M. (2021). Cybersecurity challenges and opportunities in Latin America in the global context of cyberthreats to national security and foreign policy.

International Studies, 53(198), 169–197.

Ajibola, S., & Cabral, P. (2024). A systematic literature review and bibliometric analysis of semantic segmentation models in land cover mapping. Remote Sens, 16(12):2222.

Aljohani, M., Furnell, S., Carpent, X., Gervassis, N. Examining the Influence of Cultural Diversity on Cybersecurity Culture. In: Praça, I., Bernardi, S., & Inácio, P. R. (eds). (2025). Cybersecurity. EICC 2025. Communications in Computer and Information Science.

AlMalki, H. A., & Durugbo, C. M. (2023). Systematic review of institutional innovation literature: toward a multi-level management model. Manag Rev Q 73, 731–785.

Alvarez, C., Hinojosa, C., Gonzalez, S., Rojas, L. "Towards Cybersecure Maritime Supply Chains in Latin America and the Caribbean." In: García Alcaraz, J. L., Manotas Duque, D. F., González Ramírez, R. G., Chong Chong, M. G., & de Brito Junior, I. (eds.) Supply Chain Management Strategies and Methodologies. (2023). Lecture Notes in Logistics. Springer, Cham.

Arar, T., & Yurdakul, G. (2023). Bibliometric review on the business management field. Sci Ann Econ Bus, 70(2), 301–334.

Aria, M., & Cuccurullo, C. (2017). Bibliometrix: An R-tool for comprehensive science mapping analysis. Journal of Informetrics, 11(4), 959–975.

Aristizábal Correa, J. M., Marín Ramírez, L., & Álvarez Salazar, J. (2019). Identification of security elements based on the C2M2 model for the textile manufacturing industry. Revista Colombiana de Computación, 20(2), 56–67.

Astorga Aguilar, C., & Schmidt Fonseca, I. (2019). Dangers of Social Networks: How to Educate Our Children on Cybersecurity. Revista Electrónica Educare, 23(3), 1–24.

Azevedo, Â.S., Oliveira, Í. M., & Dias, P. C. (2022). Parental Mediation of Internet Use: A Psychometric Study with Portuguese Pre-adolescents. In: Mesquita, A., Abreu, A., Carvalho, J.V. (eds.) Perspectives and Trends in Education and Technology. Smart Innovation, Systems and Technologies, vol. 256. Springer, Singapore.

Badilla Quintana, M. G., González López, G., Sandoval Henríquez, F. J., Moreno Fernández, O., Moreno Crespo, P., & Revuelta Domínguez, F. (2022). Psychometric validation of an instrument to measure cybercoexistence among Chilean youth during and after the pandemic. Aloma: Journal of Psychology, Educational Sciences, and Sports, 40(1), 23–24.

Barria, C., Cordero, D., Galeazzi, L., Acuña, A. Proposal of a Multi-standard Model for Measuring Business Maturity Levels with Reference to Information Security Standards and Controls. In Dzitac, I., Dzitac, S., Filip, F., Kacprzyk, J., Manolescu, MJ, & Oros, H. (eds.) Intelligent Methods in Computing, Communications and Control.

(2021). ICCCC 2020. Advances in Intelligent Systems and Computing, vol. 1243. Springer, Cham.

Batista, R., Villar, O., González Diez, H., & Milián Núñez, V. (2020). Cultural challenges of the malicious use of artificial intelligence in Latin American regional balance. Proc. Eur. Conf. Impact Artif. Intell. Robot., ECIAIR, 7–13.

Börner, K., Chen, C., & Boyack, K. W. (2005). Visualizing knowledge domains. Annu. Rev. Inf. Sci. Technol., 37(1), 179–255.

Cano, J. J., Almanza, A. R. The Information Security Function and the CISO in Colombia: 2010–2020. In: Rocha, Á., Ferrás, C., & Ibarra, W. (eds.) Information Technology and Systems. (2023). ICITS 2023. Lecture Notes in Networks and Systems, vol. 691. Springer, Cham.

Canuto, L., Santos, L., Vieira, L., Gonçalves, R., & Rabadão, C. (2019). CoAP flow signatures for the Internet of Things. Iberian Conference on Information Systems and Technologies, CISTI, 1–6.

Capobianco Peña, J. (2023). The New Era of Global Services: A Framework for Successful Enterprises in Business Services and IT. Emerald Publishing Limited.

Carvajal Bernal, M. Guide to Adopting a Cybersecurity Culture on Boards of Directors. In Realpe Díaz, M. E., & Gómez Rodríguez, G. A. (Eds.). (2025). Cybersecurity at the Digital Frontier: Challenges and Opportunities in New Business

Technology Ecosystems. 157–196. ESDEG Publishing.

Cobo, M. J., López Herrera, A. G., Herrera Viedma, E., & Herrera, F. (2011). Science mapping software tools: Review, analysis, and cooperative study among tools. J Am Soc Inf Sci Technol, 62(7), 1382–1402.

Cunha, J., Mealha, F. Shedding light on the Portuguese health IT architecture. In Macedo, M., Kommers, P. (Eds.). MCCSIS - Multi-Conference on Computer Science and Information Systems, & Proceedings (2018). International Conference on e-Health, ICT, Society, Human Beings, Web-Based Communication, and Social Media, 61–68.

De Guillén Gámez, F., Martínez García, I., Alastor, E., & Tomczyk, Ł. (2024). Digital Competences in Cybersecurity of Teachers in Training. Computers in the Schools, 41(3), 281–306.

Delgado Alarcón, A.I., Aguirre Anaya, E. A., Cortez Duarte, N. A., & Gallegos García, G. (2023). Multilevel functional quantification of movements for EDR in cloud-based and on-premises systems. Mexican International Conference on Computer Science, ENC.

Israel's National Cybersecurity Authority. (2022a). Cybersecurity Methodology for Organizations: Version 2.0: Best Practices in Cybersecurity.

Israel's National Cybersecurity Authority. (2022b). Defense Recommendations: The Internal Threat: Organizational Adaptation

in Cyberspace: Best Practices in Cybersecurity.

Donthu, N., Kumar, S., Mukherjee, D., Pandey, N., & Lim, W. M.. (2021). How to conduct a bibliometric analysis: An overview and guidelines. J Bus Res, 133, 285–296.

Duo, A., Basagoiti, R., Arrazola, P. J., Aperribay, J., & Cuesta, M. (2019). The capacity of statistical features extracted from multiple signals to predict tool wear in the drilling process. International Journal of Advanced Manufacturing Technology, 102(5)8, 2133–2146.

Dzhalladova, I., Škapa, S., Novotná, V., & Babynyuk, A. (2019). Design and analysis of a model for detecting information attacks in computer networks. Economic Computation and Economic Cybernetics Studies and Research, 53(3), 95–112.

Díaz-Cacho Medina, M., Falcón, P., Marcos Acevedo, J., & Pereira Domínguez, A. (2024). Educational project for remote access to industrial networks. IEEE Global Engineering Education Conference, EDUCON.

Flores Ccanto, F., Pozo, C., Flores Conislla, L. D., & Adauto Medina, W. A. (2021). Challenges of transformational leadership in organizational cybersecurity matters. Revista Venezolana de Gerencia, 26(5), 417–429.

Flores Montaño, L. A., Herrera Lozada, J. C., Sandoval Gutierrez, J., Vazquez Lopez, R., & Martinez Vazquez, D.. (2021). Cybersecurity in the Internet of Robotics Things: An Experimental Platform. DYNA, 96, 540–545.

Garcia, M., De Mendonca, F., & Albuquerque, R. (2022). Assessments of National Cyber Capability: A Brazilian Perspective in Comparison with Spain. Iberian Conference on Information Systems and Technologies (CISTI), 1–6.

García, J. A.. (2024). Securing Clinical Data in Honduras: Exploring Cybersecurity Regulations and the Role of Blockchain. JBBBE [Internet], 66, 105–116.

García, A. (2025). Bibliometric Study on Cybersecurity. Mendeley Data, V1.

Gaspar, J., Cruz, T., Lam, C. T., & Simoes, P. (2023). Smart Substation Communications and Cybersecurity: A Comprehensive Survey. IEEE Communications Surveys and Tutorials, 25(4), 2456–2493.

Gavilanes Molina, A., & Merchán, V. (2022). Information technology governance: an analysis of the approach in Ecuador. Bulletin of Electrical Engineering and Informatics, 11(1), 466–476.

Giménez Gualdo, A. M., Galán Casado, D. A., & Moraleda, Á. (2021). Key Competencies for Developing Cybercoexistence in Schools: The "ICT Peer Support" Program. Education in the Knowledge Society, 22.

Giraldo Ríos, L. A. Artificial intelligence and digital transformation in the field of cybersecurity. In Realpe Díaz, M. E., & Gómez Rodríguez, G. A. (Eds.). (2025). Cybersecurity at the Digital Frontier: Challenges and Opportunities in New Business Technology Ecosystems. 79–118. ESDEG Publishing.

Gooder, V., & Lowe, L. (2024). Implementation of a COVID-19 Closed/Open POD Partnership: A Creative Professional Practice Exemplar for Occupational and Environmental Health Nurses. *Workplace Health & Safety*, 72(5):196–201.

Goycochea Kcomt, S. P. (2025). Behavioral Economics and Economic Growth in Times of a Pandemic. Lima 2020–2025. *Ciencia Latina: Multidisciplinary Scientific Journal*, 9(4), 1296–1311.

Guerrero, G., Betarte, G., & Campo, J. D.. (2024a). Process Mining-Based Assessment of Cyber Range Trainings. Latin American Computer Conference (CLEI), Buenos Aires, Argentina, 1–10.

Guerrero, G., Betarte, G., & Campo, J.D. (2024b). Tectonic: An Academic Cyber Range. IEEE Biennial Congress of Argentina (ARGENCON), 1–8.

Heguiabehere, J., & Pallero, M. (2024). Cybersecurity and Academia. IEEE Biennial Congress of Argentina (ARGENCON), 1–4.

Iparraguirre Villanueva, O., Obregon Palomino, L., Pujay Iglesias, W., & Cabanillas Carbonell, M. (2023). Intelligent agent for incident management. RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação, (e51), 99–115.

Jiménez, C., & Rivera, R. (2021). IoT Cybersecurity: An Analysis of European Union Countries. RISTI - Revista Ibérica de Sistemas e

Tecnologias de Informação, E39, 461–476.

Jullian, O., Otero, B., Rodríguez, E., Gutierrez, N., Antona, H., & Canal, R. (2023). Deep-Learning-Based Detection for Cyberattacks in IoT Networks: A Distributed Attack Detection Framework. Journal of Network and Systems Management, 31(2).

Kononovich, I., Mayevskiy, D., & Podobniy, R. (2015). Models of Cybersecurity Systems with Delayed Response to Incidents. Inf Math Methods Simul, 5(4), 339–346.

Lampropoulos, G., Larrucea, X., & Colomo-Palacios, R. (2024). Digital Twins in Critical Infrastructure. Information, 15, 454.

Lay Lisboa, S., Armijo Rodríguez, F., Calderón Olivares, C., & Flores Acuña, J., Mercado Guerra, J. (2022). In-depth Analysis of Adultcentrism in the Educational Field: Tensions in the Face of Childhood Protagonism. Revista Electrónica Educare, 26(3), 463–489.

Leal, R., Santos, L., Vieira, L., Gonaalves, R., & Rabadão, C. (2019). MQTT flow signatures for the Internet of Things. 14th Iberian Conference on Information Systems and Technologies (CISTI), Coimbra, Portugal, 1–5.

Leirmo, J. L. Cybersecurity Awareness in Critical Sectors – a Systematic Literature Review. In Wang, Y. C., Chan, S. H., & Wang, Z. H. (eds.). (2024). Flexible Automation and Intelligent Manufacturing: Manufacturing Innovation and Preparedness for the Changing

World Order. FAIM 2024. Lecture Notes in Mechanical Engineering. Springer, Cham.

Lena Acebo, F.J., Renés Arellano, P., Hernández Serrano, M.J., & Caldeiro Pedreira, M. C.. (2022). Knowing how to share and protect oneself: key factors in digital cybercritical education for children. Profesional de la Información, 31(6).

Linnenluecke, M. K., Marrone, M., & Singh, A. K. (2020). Conducting systematic literature reviews and bibliometric analyses. Aust J Manag, 45(2), 175–194.

Lozano Blasco, R., Quilez Robres, A., Rodriguez Araya, R., & Casanovas López, R. (2022). Addiction to New Technologies and Cyberbullying in the Costa Rican Context. Educ. Sci., 12, 876.

Malanski, P. D., Dedieu, B., & Schiavi, S. (2021). Mapping the research domains on work in agriculture: A bibliometric review from the Scopus database. J Rural Stud, 81, 305–314.

Maldonado-Erazo, C. P., Álvarez García, J., del Río Rama, M. C., & de la Durán Sánchez, A. (2021). Scientific Mapping on the Impact of Climate Change on Cultural and Natural Heritage: A Systematic Scientometric Analysis. Land, 10, 76.

Martins, M. A., & Bruno, L. C. (2022). Monitoring Security Risks of Teleworker Devices in Hospital Institutions. 17th Iberian Conference on Information Systems and Technologies (CISTI), 1–6.

Martínez De Morentin, J. I., Lareki, A., & Altuna Urdin, J. (2021). Risks

Associated with Posting Content on Social Media. Ibero-American Journal of Learning Technologies, 16(1), 77–83.

Mas, F. F. (2023). The World Economic Forum and Productivity: Historical Foundations of Competitiveness. *Perspectives on Economic and Legal Sciences*, 13(2), 201–212.

Matilde Espino, Y., & Valencia Pérez, L. (2022). Bibliometric Analysis of Scientific Output on Cybersecurity in Mexico (2015–2020). CIENCIA ergo-sum, 29(3).

Matos, T., & Guerreiro, J. (2024). Development of a Remote Secure Online Voting System. In Universal Access in Human-Computer Interaction: 18th International Conference, UAHCI 2024, Held as Part of the 26th HCI International Conference, 51–65.

Mejía Miranda, J. (Ed.). (2022). Proceedings of the 11th International Conference on Software Process Improvement (CIMPS 2022): Applications in Software Engineering, Acapulco, Guerrero, Mexico, October 19–21, 2022. IEEE.

Moldovyan, A., Moldovyan, D., & Moldovyan, N. (2024). Post-Quantum Public-Key Cryptoschemes on Finite Algebras. *Informatics and Automation*, 23(4), 1246–1276. 10.15622/ia.23.4.12.

Monteiro, F., Simões, M., & Relva, I. C. (2023). Internet Addiction, Sleep Habits, and Family Communication: The Perspectives of a Sample of Adolescents. Healthcare, 11, 3194.

Monzelo, P., & Nunes, S. (2019). The Role of the Chief Information Security Officer (CISO) in Organizations. Proceedings of the Conference of the Portuguese Association of Information Systems.

Monzelo, P., & Nunes, S. (2021). Information Security Awareness and Its Impact on the CISO's Responsibilities—A Study of the Portuguese Environment. Journal of Information Systems Security, 17(2), 81–102.

Narasimhan, S., El-Farra, N. H., & Ellis, M.J. (2024). A Set-Based Control Mode Selection Approach for Active Detection of False Data Injection Cyberattacks. Proceedings of the American Control Conference, 1726–1731.

Nikolakopoulos, K., Mpelogianni, V., Groumpos, P., Kyriou, A., Ganas, A., Charalampopoulou, V., & Athanasopoulos, T. (2023). Soft computing algorithms for infrastructure monitoring. Preliminary results of the PROION project. Proc. SPIE 12786, Ninth International Conference on Remote Sensing and Geoinformation of the Environment.

Nowersztern, A., Paz, S., Kagelmacher, D., Cabral Berenfus, F., Libedinsky, P., Ribagorda, A., Tapiador, J., De Fuentes, J. M., & González, L. (2021). Cybersecurity training program for Latin America and the Caribbean.

Ojeda Castro, F. A. (2021). Origin, Use, and Meaning of the Innovation Diamond. *Business Ethics and Leadership*, 5(4):48–58.

Olmo Parra, A. S., Sánchez Crespo, L. E., Álvarez, E., Huerta, M., & Fernández Medina Paton, E. (2016). Methodology for Dynamic Analysis and Risk Management under ISO 27001. IEEE Latin America Transactions, 14(6), 2897–2911.

Onumo, A., Cullen, A., & Ullah-Awan, I. (2017). An empirical study of cultural dimensions and cybersecurity development. In 2017 IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud), 70–76.

Orosco Fabian, J. R. (2024). Cybersecurity in higher education: a bibliometric review. Digital Journal of Research in University Teaching, 18(2).

Oviedo, J., Rodríguez, M., Trenta, A., Cannas, D., Natale, D., & Piattini, M. (2024). ISO/IEC quality standards for AI engineering. *Computer Science Review*, 54.

Pavão, J., Bastardo, R., Carreira, D., & Rocha, N. P. (2024). Cyber-Resilience in the Context of National Security and Defense. RISTI: Iberian Journal of Information Systems and Technologies, 65, 359–371.

Perafán del Campo, E. A., Polo Alvis, S., Sánchez Acevedo, M. E., & Miranda Aguirre, C.. (2021). State and Sovereignty in Cyberspace. Via Inveniendi Et Iudicandi, 16(1).

Pico Saltos, R., Carrión Mero, P., Montalván Burbano, N., Garzás, J., & Redchuk, A. (2021). Research Trends in Career Success: A Bibliometric Review. Sustainability, 13, 4625.

Pranckutė, R. (2021). Web of Science (WoS) and Scopus: The Titans of

Bibliographic Information in Today's Academic World. Publications, 9(1), 12.

Purdon, L., Vera, F. Regional Cybersecurity Approaches in Africa and Latin America. In Tikk, E., & Kerttunen, M. (eds.). (2020). Routledge Handbook of International Cybersecurity.

Pérez Morón, J. (2022). Eleven years of cyberattacks on Chinese supply chains in an era of cyber warfare: A review and future research agenda. Journal of Asia Business Studies, 16(2), 371–395.

Ramírez Peña, M., Sánchez Sotano, A. J., Pérez Fernández, V., Abad, F. J., & Batista Ponce, M. (2020). Achieving a sustainable shipbuilding supply chain from an Industry 4.0 perspective. Journal of Cleaner Production, 244.

Ramírez, M., Rodríguez Ariza, L., Gómez Miranda, M. E., & Vartika, I. (2022). The Disclosure of Cybersecurity Information by Listed Companies in Latin America—Proposal for a Cybersecurity Disclosure Index. Sustainability, 14, 1390.

Ramírez Plascencia, D., Alonzo González, R. M., & Marín Tapiero, J. I. (2022). Risks Faced by Underage YouTubers Due to Legislative Gaps in Mexico. Revista Mediterránea De Comunicación, 13(1), 65–77.

Raza, N., Moazeni, F., & Khazaei, J. (2024). A Holistic Cybersecurity Framework against False Data Injection Attacks in Smart Water Distribution Systems Employing Auto-Encoders. World Environmental and Water Resources Congress 2024, 1087–1098.

Raza, N., & Moazeni, F. (2024). Chance-constrained vulnerability assessment of smart water distribution systems against stealthy false data injection attacks. International Journal of Critical Infrastructure Protection, 44.

Reis, C., Barbosa, A. R., Baptista, M. A., Lopes, M., & Clain, S. (2024). A numerical methodology for estimating site-specific cascading earthquake and tsunami dynamic loading on critical infrastructure. International Journal of Disaster Risk Reduction, 100.

Riega Virú, Y., Nilupú Moreno, K., Salas Riega, J., & Ninaquispe Soto, M.. (2023). High school girls' knowledge of cybersecurity against social cybercrime. Proc. IEEE Int. Conf. on Adv. Learn. Technol. Educ. Res., ICALTER.

Riega Virú, Y., Ninaquispe Soto, M., Salas Riega, J., Nilupú Moreno, K., Miguel Salas Riega, J., & Puga Ayala, E. (2024). Cybersecurity, State, and Law: A look from the scientific literature. Proceedings of the LACCEI International Multi-Conference on Engineering, Education, and Technology.

Rioseco Pais, M., Silva Quiroz, J., & Carrasco Manríquez, C. (2023). Development of Digital Competencies in Students at a Public, State-Owned Chilean University with a Focus on Safety. Educ. Sci., 13, 710.

Roldán Molina, G., Almache Cueva, M., Rabado Silva, C., Yevseyeva, I., & Basto Fernandes, V. (2017). A Comparison of Cybersecurity Risk

Analysis Tools. *Procedia Comput. Sci.*, 121, 568–575.

Romero Izurieta, R., Caucha Morales, L. J., Toapanta Toapanta, S. M., Mafla Gallegos, S. E., & Orizaga Trejo, J. A. (2021). Analysis of Information Security in Public Organizations in Ecuador. International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 823–829.

Saavedra, S., Llatas, J., & Armas Aguirre, J. (2021). Process Mining Model to Guarantee the Privacy of Personal Data in the Healthcare Sector. CEUR Workshop Proceedings, 3037, 34–43.

Safarpour, H., Acero, P., & Spearing, L. A. (2024). How Are Alaskan Water Systems Interdependent with Other Infrastructure? A Systematic Literature Review. World Environmental and Water Resources Congress 2024, 1039–1047.

Sainz Raso, J., Martin Gutierrez, S., Díaz, G., & Castro, M. (2023). Security Management on Arduino-Based Electronic Devices. IEEE Consumer Electronics Magazine, 12(3), 72–84.

Salley, C., Mohammadi, N., & Taylor, J. E. (2024). Protecting Critical Infrastructure from Disasters: NLP-Based Automated Information Retrieval to Generate Hypothetical Cyberattack Scenarios. Journal of Infrastructure Systems, 30(3).

Serna Valdivia, J. E., & Mejía Miranda, J. (2020). Proposal for an Intelligent Agent for the Management and Mitigation of Cybersecurity Risks in IoT Environments. 9th International

Conference on Software Process Improvement (CIMPS), 158–158.

Shevchenko, S., Zhdanova, Y., Shevchenko, H., Nehodenko, O., & Spasiteleva, S.. (2023). Conflict Analysis in the "Subject-to-Subject" Security System. CEUR Workshop Proceedings, 3421, 56–66.

Singh, V. K., Singh, P., Karmakar, M., Leta, J., & Mayr, P. (2021). The journal coverage of Web of Science, Scopus, and Dimensions: A comparative analysis. Scientometrics, 126, 5113–5142.

Sivianes, M., Arauz, T., Marín, E., & Maestre, J. M. (2023). Reputation-Based Consensus on a Secure Blockchain Network. In: Maleh, Y., Alazab, M., Romdhani, I. (eds.) Blockchain for Cybersecurity in Cyber-Physical Systems. Advances in Information Security, vol. 102. Springer, Cham.

Solar, C. (2023). Cybersecurity Governance in Latin America: States, Threats, and Alliances. Albany: State University of New York Press.

Suárez García, Z., & Álvarez García, D. (2023). Use of social networks in preadolescence: gender differences. Psychology, Society and Education, 15(1), 30–39.

Sánchez Rodríguez, M. Á., Bermejo Higuera, J., Bermejo Higuera, J. R., Sicilia Montalvo, J. A., & González Crespo, R. (2021). A systematic approach to analysis for assessing the security level of cyber-physical systems in the electricity sector. Microprocessors and Microsystems, 87.

Trejos Gil, C. A., & Peláez Vélez, Y. (2023). Cybercrimes Involving Minors on the Facebook Social Network: A Systematic Literature Review. Nuevo Derecho, 19(32).

Valente, J. (2021). From Online Platforms to Digital Monopolies: Technology, Information, and Power.

Valladarez González, V. I., & Cadena Martínez, R. (2025). Big Data Techniques and Methodologies for Analyzing Cybercrime Behavior During and After the Pandemic. Ciencia Latina: Multidisciplinary Scientific Journal, 9(3), 5952–5970.

van Eck, N. J., & Waltman, L. (2010). Software survey: VOSviewer, a computer program for bibliometric mapping. Scientometrics, 84(2):523–538.

Von Solms, R., & Van Niekerk, J. (2013). Cybercrime in the Digital Economy. Computers & Security, 38, 97–102.

Waller, L., Johnson, S. C., Satchell, N., Gordon, D., Kirkpatrick Daley, G. L., Reid, H., Fender, K., Llewellyn, P., Smyle, L., & Linton, P. (2023). Woe is the Dark Web: The Main Challenges That Governments of the Commonwealth Caribbean Will Face in Combating Dark Web-Facilitated Criminal Activities. Transforming Government: People, Process, and Policy, 17(1), 87–100.

Wallin, J. A. (2005). Bibliometric methods: Pitfalls and possibilities. Basic Clin Pharmacol Toxicol, 97(5), 261–275.

Wilkinson, D., Hanley, E., & Knijnenburg, B. P. (2024). A Comparative Analysis of Legislative Protections for Online Safety in the Global South: A Case

Study of the Caribbean. Proceedings of the ACM on Human-Computer Interaction, 8(CSCW2), 1–29.

Xu, C., Zhang, C., & Xu, J. (2020). Verifiable Cloud Computing. In: Shen, X., Lin, X., & Zhang, K. (eds.), Encyclopedia of Wireless Networks. Springer, Cham.

Yevseiev, S., Pohasii, S., Milevskyi, S., Milov, O., Melenti, Y., Grod, I., Berestov, D., Fedorenko, R., & Kurchenko, O. (2021). "Development of a Method for Assessing the Security of Cyber-Physical Systems Based on the Lotka–Volterra Model," Eastern-European Journal of Enterprise Technologies, 5(9), 30–47.

Zupic, I. (2015). Čater, T. "Bibliometric methods in management and organization." Organ Res Methods, 18(3), 429–472.

Álvarez, C. L. (2022). Standard for triggering the obligation to report significant cyber incidents in public institutions. Revista Chilena de Derecho y Tecnología, 11(2), 183–210.