Indonesian Journal of Electrical Engineering and Computer Science
Vol. 31, No. 3, September 2023, pp. 1589~1604
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v31.i3.pp1589-1604

Enterprise information security risks: a systematic review of the literature

Jenner Lavalle Sandoval[1], Laberiano Andrade-Arenas[2], Domingo Hernández Celis[3], Michael Cabanillas-Carbonell[4]
[1]Faculty of Engineering and Business, Universidad Privada Norbert Wiener, Lima, Peru
[2]Faculty of Engineering, Universidad Tecnológica del Perú, Lima, Peru
[3]Faculty of Financial and Accounting Sciences, Universidad Nacional Federico Villarreal, Lima, Peru
[4]Faculty of Engineering, Universidad Privada del Norte, Lima, Peru

Article Info

Article history:

Received Dec 23, 2022
Revised Apr 27, 2023
Accepted May 6, 2023

Keywords:

Companies
Computer security
Cybersecurity
Information
Information technology infrastructure

ABSTRACT

Currently, computer security or cybersecurity is a relevant aspect in the area of networks and communications of a company, therefore, it is important to know the risks and computer security policies that allow a unified management of cyber threats that only seek to affect the reputation or profit from the confidential information of organizations in the business sector. The objective of the research is to conduct a systematic review of the literature through articles published in databases such as Scopus and Dimension. Thus, in order to perform a complete documentary analysis, inclusion and exclusion criteria were applied to evaluate the quality of each article. Then, using a quantitative scale, articles were filtered according to author, period and country of publication, leaving a total of 86 articles from both databases. The methodology used was the one proposed by Kitchenham, and the conclusion reached was that the vast majority of companies do not make a major investment in the purchase of equipment and improvement of information technology (IT) infrastructure, exposing themselves to cyber-attacks that continue to grow every day. This research provides an opportunity for researchers, companies and entrepreneurs to consult so that they can protect their organization's most important assets.

Corresponding Author:

Michael Cabanillas-Carbonell
Faculty of Engineering, Universidad Privada del Norte
Lima, Perú
Email: mcabanillas@ieee.org

1. INTRODUCTION

Information is a vital resource for an organization, so, worldwide, its real value depends on adequate management through a combination of actions, controls, and security policies based on human resources, hardware, and software. Security policies in the business sector pursue measures aimed at the protection, confidentiality, and integrity of the organizations' information. In this regard, state that companies face countless threats, violations, and intrusions on a daily basis because they do not have modern and adequate technology that allows them to protect and manage large amounts of customer data. Nor do they have information technology (IT) security audits to help detect possible risks and violations of the sensitive information handled by the organization in its day-to-day activities [1], [2].

On the other hand, digitalization in times of COVID-19 became especially relevant in several Latin American companies, forcing them to accelerate their digital transformation. In terms of information security, the pandemic crisis not only represented a challenge in terms of health but also in terms of information security,

since virtually all products or services offered by companies depended on technology. In this context, the use of technologies such as machine learning and deep learning helps companies to experience technological breakthroughs [3]. Two technologies that make it possible to extract characteristics from data, identify models, detect vulnerability patterns, and make better decisions as a result. Under this context of technological advances, attacks, and computer vulnerabilities in the business sector, cyber-attacks as of September 2021 increased by 600% in Latin America and the Caribbean. This is due to the fact that many companies did not have modern technology capable of counteracting cyberattacks, according to Fortinet, a world leader in cybersecurity. Likewise, the number of cyber-attacks has increased considerably in recent years, and worryingly so in Latin America [4]; either due to the intensive use of the network, the lack of investment in IT, or the lack of responsible personnel capable of responding to any eventuality of computer theft. In comparison with companies operating in the United States and China, two major powers are known worldwide for being the largest venture capital investors in cybersecurity.

In fact, the Peruvian business sector has been strongly affected, suffering economic losses derived from malicious computer programs. The massification of some agents such as ransomware, phishing, and cryptojacking has had an important activity, with attacks targeting large and small companies, due to their sophistication and the use of new criminal techniques. Given this scenario, states organizations should invest in IT security based on a comprehensive and automated security approach to prevent, detect and mitigate risks and threats. But also to save time and money, since when a computer or system has been breached or damaged, the time it takes to solve the problem is not immediate, on the contrary, it is prolonged, which could generate risks to the company's reputation [5].

For this reason, IT security has had a great impact on the business environment, especially in the face of immature knowledge or bad practices. Storage policies and backups are an effective and proven alternative to deal with risks and threats when the situation requires it. In this sense, in order to streamline process flows, an optimal and qualified infrastructure is required to provide an adequate quality of protection against different vulnerabilities, so it is not advisable to apply a standard architecture [6]. However, although it is important to forge a security culture in companies, investment in IT security protection is not always made, despite the real benefits it brings. Therefore, it is important to generate new theoretical contents that contribute to the scientific and community development of professionals working in the field of engineering and businessmen who are willing to delve into the subject of computer security risks and policies in companies. Therefore, the scope of the research only covers the risk of computer security focused on the private business sector.

The objective of this literature review is to analyze articles by other authors, both national and international, translated into English, in order to have a better understanding of the different parameters, attributes, characteristics, and emerging technologies of the study problem. Also, to know the risks and security policies in the business sector. But also, to understand the key principles and IT security policies that are applied in different organizations to ensure information security management. It is expected that after identifying the shortcomings in the development of cybersecurity policies, this study will provide organizations with a guideline of knowledge that, at the same time, will allow them to establish a guideline of action and protocols so that they can watch over the data and information of their clients and the company as a whole.

It should be noted that the bibliographic review, which consists of searching, obtaining, selecting, and consulting documentary sources, was developed from a unitary and global perspective on a particular topic. As this case study has required considering some fundamental topics in the compilation and purpose of this work. We can cite research such as "structure and challenges of a security policy in small and medium enterprises", "enterprise risk management a powerful management tool", "cyber risk and cybersecurity". However, this work has contemplated a literature search in different authors, who have contributed with targeted knowledge on the topic of study. The novelty of this research is that it has sought, from the beginning, to fill all the gaps found and not solved by other authors. In the proposed study, the use of graphic resources such as tables has been very helpful to present large amounts of data selected and presented in categories to make the information to be disclosed more concise and effective.

2. METHOD

For the present work, the methodology proposed has been used, which, its roots in literature reviews carried out in works of human sciences and medicine [7]. However, in recent years adaptations have been proposed for other disciplines such as engineering. It follows that this methodology has allowed us to find and identify the most suitable articles for this literature review (LR), in such a way that it has been structured in six items, six items: i) research questions, ii) research search process, iii) inclusion and exclusion criteria, vi) research quality assessment, v) data collection, and iv) data analysis. Moreover, the documentary-type research was complemented by a biometric analysis to help reveal which country did the most scientific research and production on the subject, or who or which documents were the most cited worldwide. On the other hand, an

in-depth analysis of the identified articles was made to extract the risk factors and the strengths and weaknesses of information security policies [8] based on the preservation of information assets in the companies of the sector, relating them to the results of the bibliometric analysis.

2.1. Research questions

The questions posed in the research seek to generate answers in accordance with the objectives set out in this research article, for which three questions have been defined. It should also be noted that all questions will be answered with information from the last 5 years of publication in the English language. The proposed research questions are:

- RQ1: how does IT security impact the business sector?
- RQ2: what are the most common computer crimes in the Peruvian business sector?
- RQ3: what type of computer security policies are applied in the business sector?

2.2. Search process

The process of locating the information consists of conducting a literature search to find documents related to the main research topic, which in this case is entitled: "risks and information security policies in the business sector: systematic review of the literature". So, in order to maintain the quality standard, a search was made in two sources of databases of greater approval and scientific reputation such as Scopus, part of one of the largest online collections of scientific research in the world, and Dimensions, which after Scopus is the most used platform by the scientific-academic.

Figure 1 shows the databases used, both Scopus and Dimensions, as well as the number of documents collected in each of them. Within which we worked with articles and conferences, which dealt with the subject of information security and the attacks and information theft modalities that many companies have been suffering. In addition, when applying the inclusion and exclusion criteria, 86 documents were obtained that coincided with the subject matter of the study community. This allows a more specific study, collected in each of them. For the research, 4 search terms were defined in English, since this language has generated more publications of research articles on the proposed topic. T1: computer, T2: security, T3: risks, T4: policies

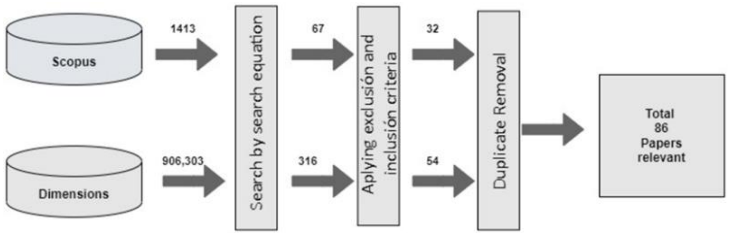

Figure 1. Table of article inclusion

2.3. Inclusion and exclusion criteria

The inclusion and exclusion criteria are intended to define the characteristics of the articles suitable for the analysis process and, subsequently, to answer the questions proposed for this research. In addition to strengthening the methodological quality of the research, by means of relevant studies that help to define the concepts and methodologies of the study. Thus, by means of obtaining relevant information, to establish the limits of the systematic review that will provide future researchers with well-founded information. At this point, it has been foreseen to consider that the pre-selected articles should have information that contributes to the objectives of the literature review, as well as describe the context in which the research was developed, the objectives, and consistent conclusions reached at the end of the process; finally, they should have contained at least 10 pages (see Table 1).

Table 1. Inclusion and exclusion criteria

Inclusión	Exclusión
– Research published from 2018 to 2022.	– Out-of-range research.
– Research in English language.	– Research that is not in English.
– Open access archives.	– Documents without full access.
– Original publications.	– Duplicated publications.
– Topics oriented to Information Security Risks and Policies in the Enterprise Sector.	– Topics not focused on the business sector.
– Research articles.	

2.4. Quality assessment

Regarding the quality assessment, it was necessary to reduce the bias of the literature analysis in order to achieve findings on its validity and some characteristics that influence the interpretation. It should be specified that, for the investigation of the pre-selected articles, these were judged by means of a quantitative scale defined on the basis of criteria that guarantee that the present literature review has achieved objective and truthful results (see Table 2). Furthermore, the determination of the quality of the research, from the beginning, has sought to evaluate the ability to communicate, the quality of the data generated, the suitability of the procedures chosen, and the consistency of the research.

Table 2. Quality assessment

Evaluation	Points
– Short-listed articles should describe the context through which they developed their research.	(2 Points)
– Shortlisted articles should describe the context in which they developed their research.	(1 Point)
– Shortlisted articles should present consistent objectives and conclusions.	(1 Point)
– Shortlisted articles should be at least 10 pages in length.	(1 Point)

2.5. Data collection

Based on the proposed terms and the AND and OR operators, a search string was formed and applied to the two databases. The collection of information from the different published articles came from the Scopus and Dimensions databases. Eighty-six scientific articles were collected using the inclusion and exclusion criteria. However, at the time of applying the general search for our research, we considered the formula with the words (("Computer" "security") AND ("risks" OR "policies")).

However, the search strings adapted to the syntax used by the search engine of each database were as:

- Scopus: TITLE-ABS-KEY (("Computadora" "seguridad") AND ("riesgos" "políticas")) Y (LIMIT-TO (PUBYEAR, 2023) O LIMIT-TO (PUBYEAR, 2022) O LIMIT-TO (PUBYEAR, 2022) O LIMIT-TO (PUBYEAR, 2022) O LIMIT-TO (PUBYEAR, 2021) O LIMITADO A (PUBYEAR, 2020) O LIMITADO A (PUBYEAR, 2019))
- Dimensions: (("Computer" "security") AND ("risks" "policies")), article publication type 2022 OR 2021 OR 2020 OR 2019 publication year ("Computer" "security") AND ("risks" OR "policies")) free text in title and abstract.

2.6. Data analysis

The first step in the analysis is to list the articles selected in the previous step. Next, consider answering research questions that will include data of interest, such as the country, the journal where the article was published, and the author. For practical purposes, in terms of country, consider the place where the article is finally published, not the country where the authors are located or the country where the research was conducted. This graph shows the number of documents related to cybersecurity in the financial sector, according to the most representative author (see Figure 2).

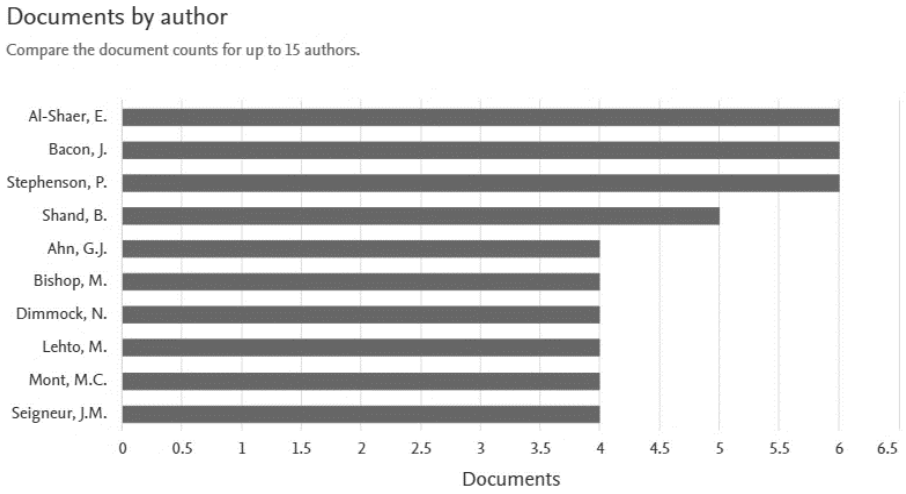

Figure 2. Documents by author

This graph shows that the United States is the country with the most research in the field of cybersecurity, leading the list with 450 published articles, followed by the United Kingdom and China with almost 150 published articles. The purpose of this research is to contribute to the scientific community and the business sector so that they can take precautions and invest in devices and training in the protection of information for the operation and stability of a community and its livelihood. Likewise, Figure 3 shows the papers by country or territory.

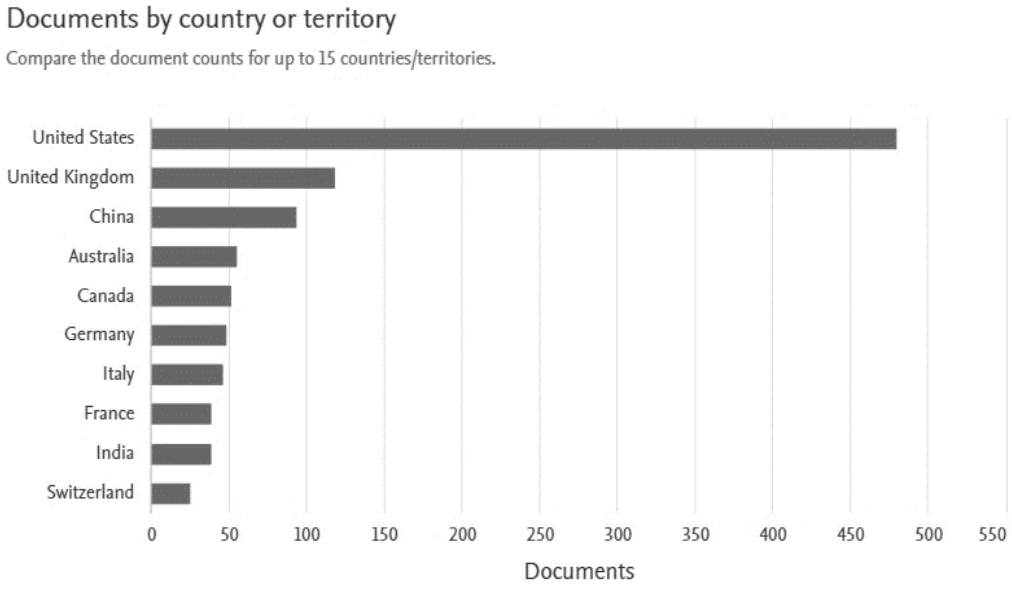

Figure 3. Papers by country or territory

3. RESULTS

After reviewing the articles, discarding those that were duplicated and did not meet the inclusion criteria, only 86 were selected from the Scopus and Dimensions databases. The following graph shows the automation that was carried out based on the Kitchenham methodology, which allowed a detailed and transparent explanation of the review of the articles based on the inclusion and exclusion criteria depending on the aspects to be considered. Likewise, the relevant results and issues that have emerged from previous work are shown below.

This flow chart shows the total number of quantified papers collected from the Scopus and Dimensions databases. Within which we worked with articles and conferences in English. Initially, 907,716 documents were found; however, not all of them corresponded to the topic of study. Thus, after applying search criteria such as year, language, open access, they were reduced to 250 documents (see Figure 4). Of these, 164 research papers unrelated to the topic were excluded as they did not effectively answer the questions posed in the research, obtaining a final result of 86 articles and conferences aligned with the study topic "Risks to corporate information security".

By means of the present figure we can indicate that the most outstanding words risk assessment, human, and computer security are the common terms, however, it should be specified that the human factor was the key piece for the management of the principles of cybersecurity within the business sector. Hence, states that there is a high degree of importance to the responsibility of information risks to the users of the system against social engineering so a culture of information security is of utmost importance for the protection of computer assets [9]. As mentioned by the author it is agreed that it is necessary to make companies aware of the need to avoid possible social engineering attacks; especially because by this means companies or even users are more vulnerable to information theft.

Figures 5 and 6 are visual representations of network diagrams and density diagrams that help to visualize the relationships between the most common words that appear most frequently in the documents used, where the largest node represents the word with the highest frequency in the document. According to the resulting nodes, it stands out that the words risk assessment, human and computer security stand out from the rest, in this regard the use of ISO 27001, which reduces the level of risk in companies through adequate controls for security equipment, as well as for the risk culture within an entity. Hence, it would also be advisable to

improve the implementation of ISO 27001 by establishing cybersecurity policies in the face of possible attacks and information use violations [10], [11].

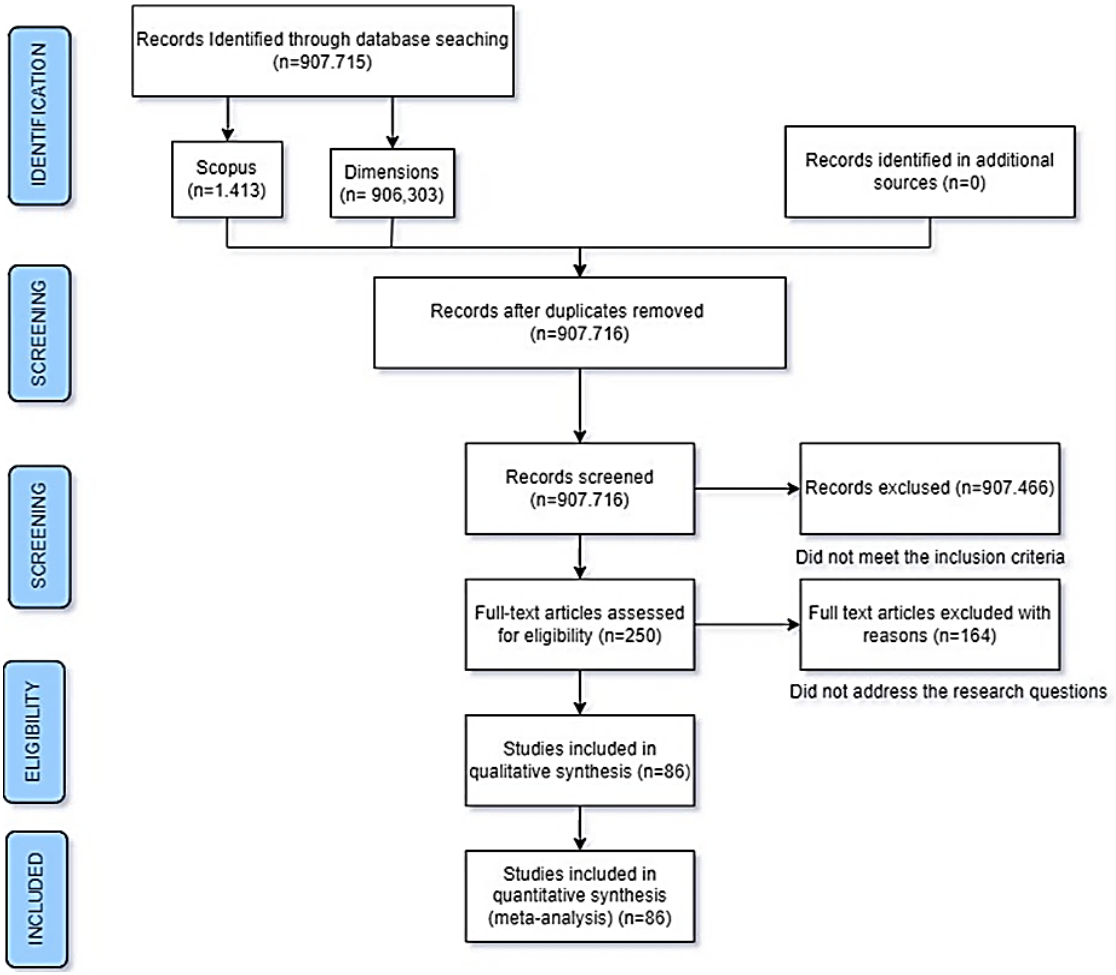

Figure 4. Flowchart of inclusion and exclusion of articles

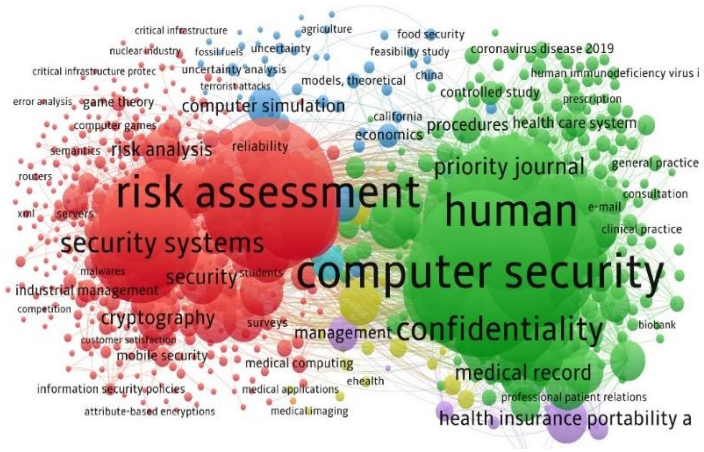

Figure 5. Relationships between the common terms using the bibliometric map

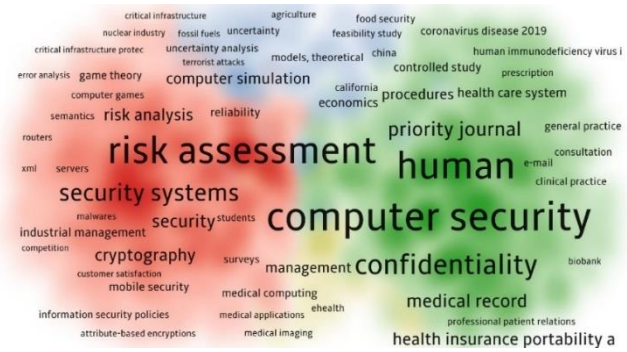

Figure 6. Visualization of density

This graph shows the results of the countries with the highest scientific production on the topics of IT security risks and policies in the business sector. After performing a bibliometric analysis, it can be established that India was one of the countries with the greatest scientific commitment to research on the topic since it had 28 published articles. That is why, as can be seen in Figure 7, the country was represented by the strongest blue color. It was followed by Greece with 11 published articles, the United States with 7, the United Kingdom with 6 articles, Egypt with 5 articles, Spain and Germany with 4 published researches each. On the other hand, China, Australia, Indonesia, and Saudi Arabia only contributed with 3 individually published papers. In the same vein, Iraq and Pakistan, represented by the slightly lighter blue color, only published 2 papers separately.

In contrast to these results, the group of countries with the lowest scientific output on the topic of security risks and policies in the business sector was led by Peru, Finland, Ukraine, New Zealand, and France, which only published one paper per country. For this reason, this group was represented by the lighter blue color. The total number of papers published and at the same time consulted for this research was 86 papers and conferences together. It should be noted that the countries shown in lead color are those that did not record any scientific publications on the subject.

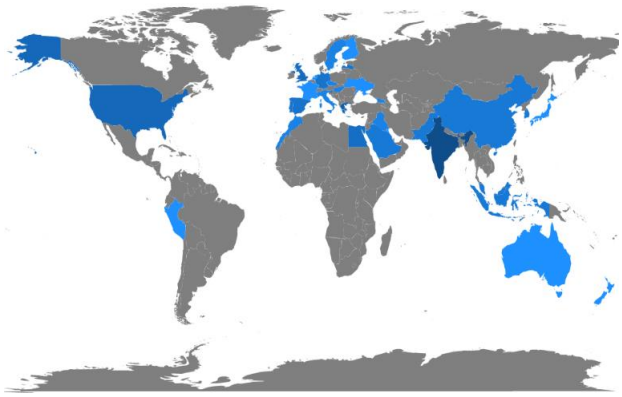

Figure 7. Country scientific production

As can be seen in Figure 8, 82 are the most referenced papers in other works; being the main authors of those papers, followed with 60 papers relevant to delve into the cybersecurity field. In Figure 9 it is possible to interpret the attacks in real-time that occur worldwide from the country of origin where the cyberattack is launched to a destination country affected by the cyberattack. On the other hand, by means of this map of cyber-attacks in real time it is possible to know which countries are the most attacked and most vulnerable by cyber-criminals. Also, in Figure 10 and Figure 10 it is possible to observe, the possible cyber attacks in real-time and worldwide based on Kaspersky data, a tool that allows to know the approximation of cyber attacks that occur globally and differentiated between countries. Likewise, the typology of the cyber attack as for example, the detection of distributed denial-of-service (DDoS) attacks and Botnet servers, also the detection of malware and ransomware as pointed out [12]. Since they are a very harmful threat to the company and its collaborators as well as for the users who acquire the company's service.

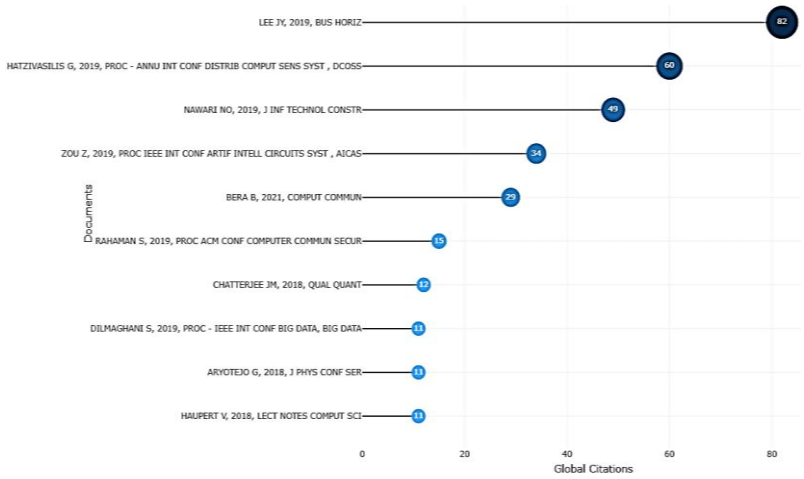

Figure 8. Most cited papers worldwide

Figure 9. Real-time map of cyberattacks occurring in the world

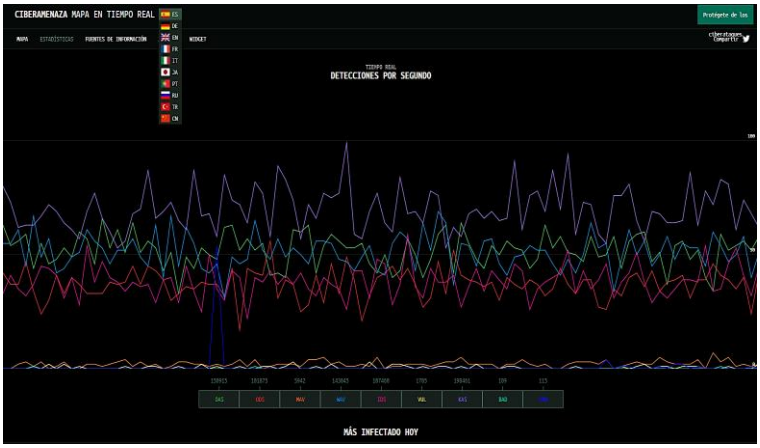

Figure 10. Statistics of cyber-attacks in the world

Table 3 contemplates an analysis of all the articles and conferences used in this research, which is strategically presented through a subdivision of clusters, which also include a breakdown of various parts of the phenomenon under study so that more detailed knowledge can be produced in this regard. Cluster 1 presents the papers, articles, and conferences that have served to define and substantiate the phenomenon under study, with titles such as: threats, violations and intrusions, integral security, and optimal infrastructure. Then, in cluster 2,

we have considered those works that have allowed to establish and explain the methodology used and that at the same time have helped to know a series of concepts, principles, norms, and laws of great utility in the process of the investigation. On the other hand, cluster 3 presents all the materialization of the study that has been used to reach a significant and relevant result, to the extent that it supports or refutes the proposed research.

Table 3. Classification of analyzed articles and conferences

Study phenomenon	Article
Cluster 1	
Threats violations and intrusions	[1], [2]
Machine learning deep learning	Nguyen *et al.* [3]
Cyber attacks	Orozco [4]
Comprehensive security	Shorten and Khoshgoftaar [5]
Optimal infrastructure	Vinayakumar *et al.* [6]
Methodology	Article
Cluster 2	
Barbara Kitchenham	Kitchenham *et al.* [13]
Informatic security	Shappie *et al.* [7]
Results	Article
Cluster 3	
Information risks	Bhaharin *et al.* [9]
ISO 27001	[10], [11]
Ransomware detection	Berrueta *et al.* [12]
Digital technologies	Articles
Cluster 4	
Artificial Intelligence	[14]–[17]
Big Data	Liu and Huang [18]
Blockchain	[19]–[27]
Biometric	[28], [29]
Internet of things	Vedaei *et al.* [30]
Riskiu	Hart *et al.* [31]
Biometric Face	Shaban *et al.* [32]
Security politics	Articles
Cluster 5	
Access control	[33]–[40]
Zero trust	AlQadheeb *et al.* [41]
Multicriteria (MCDM)	Alyami *et al.* [42]
Audit	Ndife *et al.* [43]
Cybersecurity culture	[44]–[46]
Risk assessment	[47], [48]
Programming	Abdali and Nia [49]
Modalities of attacks	Articles
Cluster 6	
Phising	[50], [51]
Smishing	[52], [53]
Malware	[54]–[56]
Social Engineering	Aycock [57]
Virus	Articles
Cluster 7	
Trojan	Hameed *et al.* [58]
Worm	Kumar *et al.* [59]
Xploit	Shandler and Gomez [60]
Ramsomware	[61]–[64]
Analysis	Articles
Cluster 8	
Informatic security	[65], [66]
Train IT managers	Shafi [67]
Security decision support	Razikin and Soewito [68]
Cost of cybercrime	Cremer *et al.* [69]
Security controls	Aslan *et al.* [70]
Mass digitization	Jara *et al.* [71]
Technology evolution	Chentouf and Bouchkaren [72]
Policies and preventive actions	Pardhi *et al.* [73]
Methods to generate strong passwords	Alhamed and Bhatia [74]
Cybersecurity systems modeling	Shulha *et al.* [75]
Comprehensive model for cyber risk	Zeller and Scherer [76]
Investments in security strategies	Martín [77]
Network security threat design	[78], [79]
Firewall implementation	[80], [81]
Fingerprint mechanisms and digital signatures	[82], [83]
Reverse engineering application	[84], [85]
Denial of service	Scanlan [86]

Cluster 4 shows the research related to the classification of the different digital technologies since these works have allowed to deepen the analysis of the subject of study, from different concepts that encompass infinite emerging possibilities, which in turn serve the proposed objective. Likewise, cluster 5 shows the articles and conferences used in the classification of the different security policies, which has allowed a broader vision of how organizations apply their policies. Cluster 6 shows the papers that support the classification of the different cyber attacks to which organizations are exposed today as a result of the large volumes of information they handle on their servers.

On the other hand, cluster 7 shows the classification of the different cybernetic viruses that can cause all kinds of problems in organizations. Likewise, articles and referential conferences on the effects and security policies applied by different organizations are presented, based on a comparative study among the different authors who have analyzed the subject. Finally, in cluster 8 and in particular, specific research that has helped to develop a comprehensive analysis in order to answer the questions posed in this research are presented.

4. DISCUSSION

In this research, studies on IT security risks and policies in the business sector in different countries from 2019 to 2022 have been reviewed. Finding 86 scientific articles based on authors' own research. Scopus and Dimensions were the two main sources considered for this research. According to the treatment of the information, we proceeded to answer the three questions proposed for this work.

4.1. Analysis of the questions

4.1.1. RQ1: how does IT security impact the business sector?

According to Figure 6, with the emergence and global opening of the Internet, computer security has had a great impact on different organizations, regardless of their size, because the information has become a very relevant resource, and although at the beginning it only addressed aspects of computer infrastructures, the truth is that little by little it has become established in different areas such as medical records, health insurance portability, security systems, and industrial management. Computer security has occupied a preponderant position in the organizational structure of a company, significantly affecting the provision of care in different organizations [66].

Now, the impact of computer security in the business sector has been both positive and negative, however, in the face of this dilemma, organizations have sought to respond with some preventive policies to protect their information [67] makes known when he describes the reason for cyber attacks and the need to train IT managers and personnel in the new modalities of cyber theft. Likewise suggests in his research a recommendation model for IT security decision support in order not to generate data losses that can affect the company [68]. This point specifies that cybersecurity cost the world economy, a little less than 1 trillion dollars in 2020, which indicates an increased difference between the years 2019 and 2018 [69]. In this regard, the security controls and countermeasures allow security managers such as IT managers of different organizations to make the right decisions in any context of cyber attack that may occur, either to adapt the deployment, configuration, or use of controls for good protection of the company's information, in parallel to the use of all the necessary technology to protect the company's data [70].

According to Figure 4, the issue of cybersecurity has become a priority not only for the private business sector but also at different levels of government. It should be noted that, for decades, strategies have been sought to safeguard information, starting from the scientific aspect, as can be seen in this figure, where the country that has studied cybersecurity, the most has been the United States. Likewise, Figure 5 shows the relationships between the most common and used terms, which give a reference to the impact of information security in the business sector.

4.1.2. RQ2: what are the most common computer crimes in the Peruvian business sector?

In times of pandemic massive digitalization was a great help, but with it appeared many computer crimes, which greatly affected the private business sector, violating their information, supplanting identities, and violating the bank accounts of different users. The states in his article, there is currently an increase in interactions between technology and, for example, sectors such as the health sector, and as a result, there are new risks such as data theft and cyber-attacks on company information [71]. Although they state in their article that technology has evolved significantly, generating a positive impact on a global level, the truth is that they agree that during the pandemic several companies have been victims of cyber attacks and information theft by hackers who, using methods such as phishing, vishing, smishing, ransomware, malware, spear phishing, and whaling phishing, have caused serious damage to the productivity of companies, even leading to the total closure of the company [72].

According to Cluster 6, phishing has been presented as an infallible social engineering technique to damage the reputation of the company; this virus acts by sending an email in which cybercriminals impersonate the identity of a known company to request personal and banking information of its users, which reaches it through a link attached to an email, which supposedly redirects to the company's website, when in fact it directs you to a fraudulent website to appropriate your money. With vishing something similar happens, however, this modality acts by means of a phone call, and the criminals try to deceive the victim, impersonating the identity of another person or of some organization. Smishing attacks are also aimed at damaging a company's reputation; this type of attack uses the messaging service to appropriate private information or charge the user money.

4.1.3. RQ3: what kind of IT security policies are applied in the business sector?

There are currently a number of IT security policies and preventive actions such as, for example, the implementation of a malware scanner to analyze and detect the severity of threats present in Android devices [73]. As well as a signature-based scheme to scan applications on mobile devices. Such signatures are installed through the legal vulnerability market store or third-party market that classifies such applications as safe, medium, and high applications. In this regard, Alhamed and Bhatia [74] in his research article argues that companies have decided to implement a method that generates secure and memorable passwords that comply with best practices and capabilities to remember and regenerate passwords, allowing to protect the organization's information from any attack or information vulnerability.

For his part, proposes a modeling of the cybersecurity system for the rapid development of the computerization process and refers to a comprehensive model for cyber risk by proposing a new approach to model cyber risk using marked point processes [76]. By this, the key co-variable is identified, resulting in the ability to detect non-redirected and targeted malicious attacks, as well as accidents and failures. For his part his article mentions that currently, the increase in cyber-attacks has made organizations invest in strategies such as management systems based on the ISO/IEC 27001:2014 standard [77]. Which allows to ensure the confidentiality, availability, and integrity of information and information systems. Thus, providing the requirements to establish, implement, maintain, and continuously improve an information security management system for the company. Hence, it is important that such a security management system is part of all activities performed by the company and is integrated with all processes and areas of the organization.

4.2. Proposed information security model

The research allowed the development of a proposed model based on the topic of information security risks and policies in the business sector; for this purpose, the data collected were extracted from two important databases, Scopus and Dimensions. The implementation of a collaborative architecture and a security threat design of industrial control networks allows the security assessment of the control system [78], [79], the standardization of the system's operational behavior, and the design of the security control system architecture. Along these lines, the implementation of firewalls acts as a first line of defense, protecting private networks from unauthorized and unverified access to an Internet connection [80], [81].

As for the recommended defense-in-depth architecture, this strategy includes firewalls, the use of demilitarized zones, and intrusion detection capabilities in the event of an attempt to breach company information. In this regard, suggest implementing fingerprinting and digital signature mechanisms in enterprise architectures for all kinds of devices, through passive packet capture techniques and an optimal selection of filtering criteria and machine learning algorithms, in addition to a device identification mechanism for both network administrators and ordinary users [82], [83]. From another approach, the application of reverse engineering, a botnet that uses domain name system (DNS) as an operator for command and control, detecting several hosts, and at least 14 million transactions within them [84], [85]; as well as some malicious malware capable of severely damaging a company's computer systems. Under these premises, Figure 11 shows the proposed model, which reveals the strategy for protecting the data and information of organizations.

The Figure 11 shows that many companies are interconnecting to external networks in order to expand their business; however, it can also be observed that the vast majority of these companies do not have secure computer security architectures to protect their data and sensitive information, a situation that could have a series of effects such as unstable connectivity to external networks, use of technologies with vulnerabilities, deficient technologies and control system communication protocols that lack security functionality. Hence, sought to assess the impact of denial of service distributing attacks and malicious software on computer systems, in addition to the likely increase in cyber attacks on ill-prepared industries due to the rapid adoption of high-speed Internet, through these proposed constellations and the Starlink satellite constellations [86].

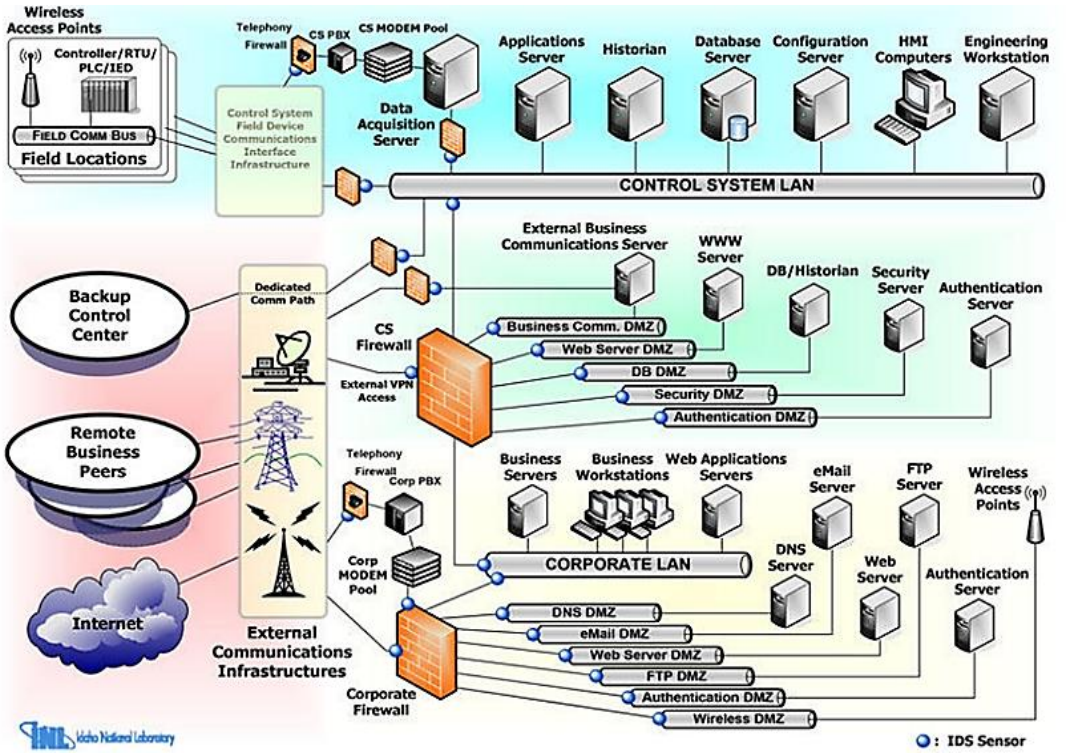

Figure 11. Recommended defense-in-depth architecture

5. CONCLUSION

After having carried out a systematic review of the literature on the subject in question, it is concluded that historical and recent events in the world have shown that the combination of cyber-attacks and attacks on traditional physical terrain can become the perfect strategy to paralyze or destroy the essential and civil infrastructures of an entire country. In relation to the objective posed for this systematic review sought to: "To analyze articles by other authors, both national and international, translated into the English language, as well as to achieve a better understanding of the different parameters, attributes, characteristics and emerging technologies of the problem under study", it can be concluded that, computer security management is a well regarded concept within the organizational environment; therefore, knowing the reality of the principles and the main standards applied by the different companies or organizations in the sector is relevant to generate new guidelines that contribute to technological ethics and mitigate computer crimes that prevail in the business sector. In addition, it has a drastic impact on the economic, legal, social, and reputational aspects of a company, through a series of actions such as: loss of daily working hours, interruption of networks and devices; also, ransom payments or emergency attention that generally seek to generate significant damage and eventually the total inactivity of the company.

Consequently, among the most used modalities are: Phishing, spear phishing, whaling phishing, vishing, smishing, and malware. The most common types of viruses are: trojan, worm, Xploit and ransomware; however, the variant known as ransomware has recently become one of the most lethal and dangerous threats to corporate networks worldwide. Likewise, after analyzing each of the articles in this paper, it is concluded that the security policies that companies apply, nowadays, to prevent cyberattacks and information theft are mainly focused on cybersecurity algorithms that can be applied in the development of applications, protection measures to avoid social engineering attacks and prevention strategies. The study also reveals that there is still a large percentage of companies or organizations that believe they are unattractive to cybercriminals or consider that security software that very little investment has required, is sufficient to stop all future threats. This makes IT security management essential when trying to reduce risks to an organization's communication and IT infrastructures. Therefore, it is recommended that businessmen implement security policies that allow them to detect illegitimate intrusions, malicious attacks, and malicious traffic on networks, among other types of cyber-attacks that may threaten the company's information.

REFERENCES

[1] M. Sigala, A. Beer, L. Hodgson, and A. O'Connor, "Big data for measuring the impact of tourism economic development programmes: a process and quality criteria framework for using big data," in *Big Data and Innovation in Tourism, Travel, and Hospitality: Managerial Approaches, Techniques, and Applications*, Singapore: Springer Singapore, 2019, pp. 57–73, doi: 10.1007/978-981-13-6339-9_4.

[2] L. C. Ruiz, M. L. Amado, J. R. Carrasco, and L. Andrade-Arenas, "Implementation of information security audit for the sales system in a peruvian company," *International Journal on Advanced Science, Engineering and Information Technology*, vol. 12, no. 3, pp. 1189–1195, Jun. 2022, doi: 10.18517/ijaseit.12.3.13969.

[3] G. Nguyen *et al.*, "Machine learning and deep learning frameworks and libraries for large-scale data mining: a survey," *Artificial Intelligence Review*, vol. 52, no. 1, pp. 77–124, Jun. 2019, doi: 10.1007/s10462-018-09679-z.

[4] G. A. P. Orozco, "Chinese and American Cyber Security Models: A Comparative," *Oasis*, no. 34, pp. 107–126, Sep. 2021, doi: 10.18601/16577558.n34.07.

[5] C. Shorten and T. M. Khoshgoftaar, "A survey on image data augmentation for deep learning," *Journal of Big Data*, vol. 6, no. 1, p. 60, Dec. 2019, doi: 10.1186/s40537-019-0197-0.

[6] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, "Deep learning approach for intelligent intrusion detection system," *IEEE Access*, vol. 7, pp. 41525–41550, 2019, doi: 10.1109/ACCESS.2019.2895334.

[7] A. T. Shappie, C. A. Dawson, and S. M. Debb, "Personality as a predictor of cybersecurity behavior.," *Psychology of Popular Media*, vol. 9, no. 4, pp. 475–480, Oct. 2020, doi: 10.1037/ppm0000247.

[8] V. Villegas and J. Carlos. "Cybersecurity and information theft: A systematic review of the literature," (*in Spanish: Ciberseguridad y robo de información: Una revisión sistemática de la literatura*), *Santo Toribio de Mogrovejo Catholic University*, 2022, .

[9] S. H. Bhaharin, U. A. Mokhtar, R. Sulaiman, and M. M. Yusof, "Issues and trends in information security policy compliance," in *International Conference on Research and Innovation in Information Systems, ICRIIS*, Dec. 2019, vol. December-2019, pp. 1–6, doi: 10.1109/ICRIIS48246.2019.9073645.

[10] M. Podrecca, G. Culot, G. Nassimbeni, and M. Sartor, "Information security and value creation: the performance implications of ISO/IEC 27001," *Computers in Industry*, vol. 142, p. 103744, Nov. 2022, doi: 10.1016/j.compind.2022.103744.

[11] N. Legowo and Y. Juhartoyo, "Risk management; risk assessment of information technology security system at bank using ISO 27001," *Journal of System and Management Sciences*, vol. 12, no. 3, pp. 181–199, 2022, doi: 10.33168/JSMS.2022.0310.

[12] E. Berrueta, D. Morato, E. Magaña, and M. Izal, "Crypto-ransomware detection using machine learning models in file-sharing network scenarios with encrypted traffic," *Expert Systems with Applications*, vol. 209, p. 118299, Dec. 2022, doi: 10.1016/j.eswa.2022.118299.

[13] B. Kitchenham, O. Pearl Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering–a systematic literature review," *Information and Software Technology*, vol. 51, no. 1, pp. 7-15, 2009, doi: 10.1016/j.infsof.2008.09.009.

[14] T. F. Blauth, O. J. Gstrein, and A. Zwitter, "Artificial intelligence crime: an overview of malicious use and abuse of AI," *IEEE Access*, vol. 10, pp. 77110–77122, 2022, doi: 10.1109/ACCESS.2022.3191790.

[15] A. A. Khan, A. A. Laghari, P. Li, M. A. Dootio, and S. Karim, "The collaborative role of blockchain, artificial intelligence, and industrial internet of things in digitalization of small and medium-size enterprises," *Scientific Reports*, vol. 13, no. 1, p. 1656, Jan. 2023, doi: 10.1038/s41598-023-28707-9.

[16] J. Cho, "Efficient autonomous defense system using machine learning on edge device," *Computers, Materials and Continua*, vol. 70, no. 2, pp. 3565–3588, 2022, doi: 10.32604/cmc.2022.020826.

[17] D. Schiff, "Out of the laboratory and into the classroom: the future of artificial intelligence in education," *AI and Society*, vol. 36, no. 1, pp. 331–348, Mar. 2021, doi: 10.1007/s00146-020-01033-8.

[18] Q. Liu and Z. Huang, "Research on intelligent prevention and control of COVID-19 in China's urban rail transit based on artificial intelligence and big data," *Journal of Intelligent and Fuzzy Systems*, vol. 39, no. 6, pp. 9085–9090, 2020, doi: 10.3233/JIFS-189307.

[19] D. Wang, Y. Zhu, Y. Zhang, and G. Liu, "Security assessment of blockchain in Chinese classified protection of cybersecurity," *IEEE Access*, vol. 8, pp. 203440–203456, 2020, doi: 10.1109/ACCESS.2020.3036004.

[20] J. L. Gonzalez-Compean, O. Telles, I. Lopez-Arevalo, M. Morales-Sandoval, V. J. Sosa-Sosa, and J. Carretero, "A policy-based containerized filter for secure information sharing in organizational environments," *Future Generation Computer Systems*, vol. 95, pp. 430–444, Jun. 2019, doi: 10.1016/j.future.2019.01.002.

[21] H. Wu and X. Zhu, "Developing a reliable service system of charity donation during the COVID-19 outbreak," *IEEE Access*, vol. 8, pp. 154848–154860, 2020, doi: 10.1109/ACCESS.2020.3017654.

[22] L. Garg, E. Chukwu, N. Nasser, C. Chakraborty, and G. Garg, "Anonymity preserving IoT-based COVID-19 and other infectious disease contact tracing model," *IEEE Access*, vol. 8, pp. 159402–159414, 2020, doi: 10.1109/ACCESS.2020.3020513.

[23] L. Ricci, D. D. F. Maesa, A. Favenza, and E. Ferro, "Blockchains for covid-19 contact tracing and vaccine support: A systematic review," *IEEE Access*, vol. 9, pp. 37936–37950, 2021, doi: 10.1109/ACCESS.2021.3063152.

[24] R. W. Ahmad, K. Salah, R. Jayaraman, I. Yaqoob, M. Omar, and S. Ellahham, "Blockchain-based forward supply chain and waste management for COVID-19 medical equipment and supplies," *IEEE Access*, vol. 9, pp. 44905–44927, 2021, doi: 10.1109/ACCESS.2021.3066503.

[25] H. R. Hasan, K. Salah, R. Jayaraman, I. Yaqoob, M. Omar, and S. Ellahham, "COVID-19 contact tracing using blockchain," *IEEE Access*, vol. 9, pp. 62956–62971, 2021, doi: 10.1109/ACCESS.2021.3074753.

[26] D. C. Nguyen, M. Ding, P. N. Pathirana, and A. Seneviratne, "Blockchain and AI-based solutions to combat Coronavirus (COVID-19)-like epidemics: a survey," *IEEE Access*, vol. 9, pp. 95730–95753, 2021, doi: 10.1109/ACCESS.2021.3093633.

[27] W. Alkhader, K. Salah, A. Sleptchenko, R. Jayaraman, I. Yaqoob, and M. Omar, "Blockchain-based decentralized digital manufacturing and supply for COVID-19 medical devices and supplies," *IEEE Access*, vol. 9, pp. 137923–137940, 2021, doi: 10.1109/ACCESS.2021.3118085.

[28] M. Kolhar, F. Al-Turjman, A. Alameen, and M. M. Abualhaj, "A three layered decentralized IoT biometric architecture for city lockdown during covid-19 outbreak," *IEEE Access*, vol. 8, pp. 163608–163617, 2020, doi: 10.1109/ACCESS.2020.3021983.

[29] A. M. A. Ali, A. M. M. N. Musaed, and R. B. Alias, "The effect of cyber security knowledge on employees' personal growth: an empirical study in private hospitals in Libya and Yemen," *Health Education and Health Promotion*, vol. 10, no. 2, 2022.

[30] S. S. Vedaei *et al.*, "COVID-SAFE: An IoT-based system for automated health monitoring and surveillance in post-pandemic life," *IEEE Access*, vol. 8, pp. 188538–188551, 2020, doi: 10.1109/ACCESS.2020.3030194.

[31] S. Hart, A. Margheri, F. Paci, and V. Sassone, "Riskio: A serious game for cyber security awareness and education," *Computers and Security*, vol. 95, p. 101827, Aug. 2020, doi: 10.1016/j.cose.2020.101827.

[32] S. A. Shaban, H. M. M. Ahmed, and D. L. Elsheweikh, "A novel fusion system based on iris and ear biometrics for e-exams," *Intelligent Automation and Soft Computing*, vol. 35, no. 3, pp. 3295–3315, 2023, doi: 10.32604/iasc.2023.030237.
[33] S. Parkinson and S. Khana, "Identifying high-risk over-entitlement in access control policies using fuzzy logic," *Cybersecurity*, vol. 5, no. 1, p. 6, Dec. 2022, doi: 10.1186/s42400-022-00112-1.
[34] M. Calvo and M. Beltrán, "A model for risk-based adaptive security controls," *Computers and Security*, vol. 115, p. 102612, Apr. 2022, doi: 10.1016/j.cose.2022.102612.
[35] A. Vulpe, R. Crăciunescu, A.-M. Drăgulinescu, S. Kyriazakos, A. Paikan, and P. Ziafati, "Enabling security services in socially assistive robot scenarios for healthcare applications," *Sensors*, vol. 21, no. 20, p. 6912, Oct. 2021, doi: 10.3390/s21206912.
[36] M. A. Elshabka, H. A. Hassan, W. M. Sheta, and H. M. Harb, "Security-aware dynamic VM consolidation," *Egyptian Informatics Journal*, vol. 22, no. 3, pp. 277–284, Sep. 2021, doi: 10.1016/j.eij.2020.10.002.
[37] M. B. M. Kamel, Y. Yan, P. Ligeti, and C. Reich, "Attred: attribute based resource discovery for IoT," *Sensors*, vol. 21, no. 14, p. 4721, Jul. 2021, doi: 10.3390/s21144721.
[38] S. V. Bezzateev, T. N. Elina, V. A. Mylnikov, and I. I. Livshitz, "Risk assessment methodology for information systems, based on the user behavior and it-security incidents analysis," *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, vol. 21, no. 4, pp. 553–561, Aug. 2021, doi: 10.17586/2226-1494-2021-21-4-553-561.
[39] H. Liu, H. Xue, and H. Lu, "A sensitive file abnormal access detection method based on application classification," *Security and Communication Networks*, vol. 2021, pp. 1–7, Mar. 2021, doi: 10.1155/2021/6684456.
[40] C. Zhou, X. Li, S. Yang, and Y. C. Tian, "Risk-based scheduling of security tasks in industrial control systems with consideration of safety," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 5, pp. 3112–3123, May 2020, doi: 10.1109/TII.2019.2903224.
[41] A. AlQadheeb, S. Bhattacharyya, and S. Perl, "Enhancing cybersecurity by generating user-specific security policy through the formal modeling of user behavior," *Array*, vol. 14, p. 100146, Jul. 2022, doi: 10.1016/j.array.2022.100146.
[42] H. Alyami *et al.*, "Effectiveness evaluation of different IDSs using integrated fuzzy MCDM Model," *Electronics (Switzerland)*, vol. 11, no. 6, p. 859, Mar. 2022, doi: 10.3390/electronics11060859.
[43] A. N. Ndife, Y. Mensin, W. Rakwichian, and P. Muneesawang, "Cyber-security audit for smart grid networks: an optimized detection technique based on bayesian deep learning," *Journal of Internet Services and Information Security*, vol. 12, no. 2, pp. 95–114, 2022, doi: 10.22667/JISIS.2022.05.31.095.
[44] V. Bernal, "The cultural construction of cybersecurity: digital threats and dangerous rhetoric," *Anthropological Quarterly*, vol. 94, no. 4, pp. 611–638, 2022, doi: 10.1353/anq.2021.0037.
[45] A. Georgiadou, A. Michalitsi-Psarrou, and D. Askounis, "Cyber-security culture assessment in Academia: A COVID-19 study: Applying a cyber-security culture framework to assess the Academia's resilience and readiness," in *ACM International Conference Proceeding Series*, Aug. 2022, pp. 1–8, doi: 10.1145/3538969.3544467.
[46] A. Georgiadou, A. Michalitsi-Psarrou, and D. Askounis, "Evaluating the cyber-security culture of the EPES sector: Applying a cyber-security culture framework to assess the EPES sector's resilience and readiness," in *ACM International Conference Proceeding Series*, Aug. 2022, pp. 1–10, doi: 10.1145/3538969.3543813.
[47] O. Shmatko *et al.*, "Development of methodological foundations for designing a classifier of threats to cyberphysical systems," *Eastern-European Journal of Enterprise Technologies*, vol. 3, no. 9–105, pp. 6–19, Jun. 2020, doi: 10.15587/1729-4061.2020.205702.
[48] D. Kim, "Decision-making method for estimating malware risk index," *Applied Sciences (Switzerland)*, vol. 9, no. 22, p. 4943, Nov. 2019, doi: 10.3390/APP9224943.
[49] A. Abdali and S. M. Nia, "A new optimization method for security-constrained workflow scheduling," *Indian Journal of Computer Science and Engineering*, vol. 10, no. 1, pp. 8–25, Feb. 2019, doi: 10.21817/indjcse/2019/v10i1/191001002.
[50] W. Priestman, T. Anstis, I. G. Sebire, S. Sridharan, and N. J. Sebire, "Phishing in healthcare organisations: threats, mitigation and approaches," *BMJ Health and Care Informatics*, vol. 26, no. 1, p. e100031, Sep. 2019, doi: 10.1136/bmjhci-2019-100031.
[51] M. Hijji and G. Alam, "A multivocal literature review on growing social engineering based cyber-attacks/threats during the COVID-19 pandemic: challenges and prospective solutions," *IEEE Access*, vol. 9, pp. 7152–7169, 2021, doi: 10.1109/ACCESS.2020.3048839.
[52] M. L. Martin, B. Carro, and A. S. Esguevillas, "Application of deep reinforcement learning to intrusion detection for supervised problems," *Expert Systems with Applications*, vol. 141, p. 112963, Mar. 2020, doi: 10.1016/j.eswa.2019.112963.
[53] S. Hakak, W. Z. Khan, M. Imran, K. K. R. Choo, and M. Shoaib, "Have you been a victim of COVID-19-related cyber incidents? survey, taxonomy, and mitigation strategies," *IEEE Access*, vol. 8, pp. 124134–124144, 2020, doi: 10.1109/ACCESS.2020.3006172.
[54] H. H. Al-Khshali and M. Ilyas, "Impact of portable executable header features on malware detection accuracy," *Computers, Materials and Continua*, vol. 74, no. 1, pp. 153–178, 2023, doi: 10.32604/cmc.2023.032182.
[55] J. A. Mata-Torres, E. Tello-Leal, J. D. Hernandez-Resendiz, and U. M. Ramirez-Alcocer, "Evaluation of machine learning techniques for malware detection," in *Intelligent Systems Reference Library*, vol. 226, 2023, pp. 121–140, doi: 10.1007/978-3-031-08246-7_6.
[56] A. K. Jha, A. Vaish, and S. Patil, "A novel framework for metamorphic malware detection," *SN Computer Science*, vol. 4, no. 1, p. 10, Oct. 2023, doi: 10.1007/s42979-022-01433-1.
[57] J. Aycock, "Teaching social engineering using improv," in *Proceedings of the 26th ACM Conference on Innovation and Technology in Computer Science Education V. 2*, Jun. 2021, pp. 629–630, doi: 10.1145/3456565.3460037.
[58] S. S. Hameed, A. Selamat, L. A. Latiff, S. A. Razak, and O. Krejcar, "Multi-classification of imbalance worm ransomware in the IoMT system," in *Frontiers in Artificial Intelligence and Applications*, vol. 355, 2022, pp. 531–541, doi: 10.3233/FAIA220282.
[59] A. Kumar, B. J. Choi, K. S. Kuppusamy, and G. Aghila, "Malware attacks: dimensions, impact, and defenses," in *Frontiers in Artificial Intelligence and Applications*, vol. 355, 2022, pp. 157–179.
[60] R. Shandler and M. A. Gomez, "The hidden threat of cyber-attacks–undermining public confidence in government," *Journal of Information Technology and Politics*, pp. 1–16, Aug. 2022, doi: 10.1080/19331681.2022.2112796.
[61] T. McIntosh, A. S. M. Kayes, Y. P. P. Chen, A. Ng, and P. Watters, "Ransomware mitigation in the modern era: a comprehensive review, research challenges, and future directions," *ACM Computing Surveys*, vol. 54, no. 9, pp. 1–36, Dec. 2022, doi: 10.1145/3479393.
[62] L. A. Kong, K. N. Yeo, R. X. Ng, and S. H. Kok, "Ransomware attack and remedial: a survey," *International Journal of Innovative Research in Applied Sciences and Engineering*, vol. 3, no. 7, p. 490, Jan. 2020, doi: 10.29027/ijirase.v3.i7.2020.490-497.
[63] S. H. Kok, A. Azween, and N. Z. Jhanjhi, "Evaluation metric for crypto-ransomware detection using machine learning," *Journal of Information Security and Applications*, vol. 55, p. 102646, Dec. 2020, doi: 10.1016/j.jisa.2020.102646.

[64] A. Wani and S. Revathi, "Ransomware protection in IoT using software defined networking," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 3, pp. 3166–3174, Jun. 2020, doi: 10.11591/ijece.v10i3.pp3166-3175.
[65] A. S. Edu, D. Agozie, and M. Agoyi, "Digital security vulnerabilities and threats implications for financial institutions deploying digital technology platforms and application: FMEA and FTOPSIS analysis," *PeerJ Computer Science*, vol. 7, pp. 1–26, Aug. 2021, doi: 10.7717/PEERJ-CS.658.
[66] C. J. Nelson *et al.*, "Impact of and response to cyberattacks in radiation oncology," *Advances in Radiation Oncology*, vol. 7, no. 5, p. 100897, Sep. 2022, doi: 10.1016/j.adro.2022.100897.
[67] E. Shafi, "Vulnerability of Saudi private sector organisations to cyber threats and methods to reduce the vulnerability," *Pertanika Journal of Science and Technology*, vol. 30, no. 3, pp. 1909–1926, Apr. 2022, doi: 10.47836/pjst.30.3.08.
[68] K. Razikin and B. Soewito, "Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework," *Egyptian Informatics Journal*, vol. 23, no. 3, pp. 383–404, Sep. 2022, doi: 10.1016/j.eij.2022.03.001.
[69] F. Cremer *et al.*, "Cyber risk and cybersecurity: a systematic review of data availability," *The Geneva Papers on Risk and Insurance - Issues and Practice*, vol. 47, no. 3, pp. 698–736, Jul. 2022, doi: 10.1057/s41288-022-00266-6.
[70] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, "A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions," *Electronics*, vol. 12, no. 6, p. 1333, Mar. 2023, doi: 10.3390/electronics12061333.
[71] H. L. S. Jara, H. B. P. Navarro, and J. Armas-Aguirre, "Cybersecurity and privacy capabilities model for data management against cyber-attacks in the health sector," *Smart Innovation, Systems and Technologies*, vol. 233, pp. 359–367, 2021, doi: 10.1007/978-3-030-75680-2_40.
[72] F. Z. Chentouf and S. Bouchkaren, "Security and privacy in smart city: a secure e-voting system based on blockchain," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 13, no. 2, pp. 1848–1857, 2023, doi: 10.11591/ijece.v13i2.pp1848-1857.
[73] P. R. Pardhi, J. K. Rout, and N. K. Ray, "Implementation of a malware scanner using signature-based approach for android applications," in *2021 19th OITS International Conference on Information Technology (OCIT)*, Dec. 2022, pp. 14–19, doi: 10.1109/ocit53463.2021.00015.
[74] A. Alhamed and S. Bhatia, "VowPass: novel method to generate secure and memorable passwords," in *2021 4th International Conference on Signal Processing and Information Security, ICSPIS 2021*, Nov. 2021, pp. 45–48, doi: 10.1109/ICSPIS53734.2021.9652188.
[75] O. Shulha, I. Yanenkova, M. Kuzub, I. Muda, and V. Nazarenko, "Banking information resource cybersecurity system modeling," *Journal of Open Innovation: Technology, Market, and Complexity*, vol. 8, no. 2, p. 80, Jun. 2022, doi: 10.3390/joitmc8020080.
[76] G. Zeller and M. A. Scherer, "A comprehensive model for cyber risk based on marked point processes and its application to insurance," *SSRN Electronic Journal*, 2020, doi: 10.2139/ssrn.3668228.
[77] T. R. Martín, "Automation of an information security management system based on the iso / iec 27001 standard," *Universidad y Sociedad*, vol. 13, no. 5, pp. 495–506, 2021.
[78] Y. Jiang, J. Qian, and C. Zhang, "Design and practice of industrial control network security threat model," in *ACM International Conference Proceeding Series*, Sep. 2021, pp. 2106–2109, doi: 10.1145/3482632.3484108.
[79] H. Qusa and J. Tarazi, "Collaborative fog computing architecture for privacy-preserving data aggregation," in *2021 IEEE World AI IoT Congress, AIIoT 2021*, May 2021, pp. 86–91, doi: 10.1109/AIIoT52608.2021.9454198.
[80] P. Ambhore and A. Wankhade, "Firewall for intranet security," in *ICMCSI 2020: International Conference on Mobile Computing and Sustainable Informatics*, 2021, pp. 653–659, doi: 10.1007/978-3-030-49795-8_62.
[81] C. Aktürk and C. Cubukcu, "A decision making model proposal for firewall selection," *KSII Transactions on Internet and Information Systems*, vol. 15, no. 10, pp. 3588–3607, Oct. 2021, doi: 10.3837/tiis.2021.10.007.
[82] L. Babun, H. Aksu, L. Ryan, K. Akkaya, E. S. Bentley, and A. S. Uluagac, "Z-IoT: passive device-class fingerprinting of ZigBee and Z-Wave IoT devices," *IEEE International Conference on Communications*, vol. 2020-June, 2020, doi: 10.1109/ICC40277.2020.9149285.
[83] L. Yu, B. Luo, J. Ma, Z. Zhou, and Q. Liu, "You are what you broadcast: Identification of mobile and iot devices from (public) WiFi," in *Proceedings of the 29th USENIX Security Symposium*, 2020, pp. 55–72.
[84] C. J. Dietrich, C. Rossow, F. C. Freiling, H. Bos, M. V. Steen, and N. Pohlmann, "On botnets that use DNS for command and control," in *Proceedings - 2011 7th European Conference on Computer Network Defense, EC2ND 2011*, Sep. 2012, pp. 9–16, doi: 10.1109/EC2ND.2011.16.
[85] S. Sheridan and A. Keane, "Detection of DNS based covert channels," in *European Conference on Information Warfare and Security, ECCWS*, 2015, pp. 267–275.
[86] J. D. Scanlan, J. M. Styles, D. Lyneham, and M. H. Lützhöft, "New internet satellite constellations to increase cyber risk in ill-prepared industries," in *Proceedings of the International Astronautical Congress, IAC*, 2019.

BIOGRAPHIES OF AUTHORS

Jenner Lavalle Sandoval is a junior in engineering and research, currently studying the ninth cycle of systems engineering and computer science at Norbert Wiener University, focused on development with the aim of making a continuous contribution to the problems that arise in society. With publications in magazines indexed in Scopus. He can be contacted at email: a2020104377@uwiener.edu.pe.

Laberiano Andrade-Arenas Doctor in Systems and Computer Engineering. Master in Systems Engineering. Graduated with the Master's Degree in University Teaching. Graduated with the Master's degree in accreditation and evaluation of educational quality. Systems Engineer. ITILV3 Fundamentals International Course (Zonngo - Peru / IMLAD - Mexico). Scrum fundamentals certified, Research Professor with publications in Scopus indexed journals. He has extensive experience in the University Chair in face-to-face and blended classes at different undergraduate and postgraduate universities in Lima. He can be contacted at email: laberiano.andrade@uwiener.edu.pe.

Domingo Hernández Celis Doctor of Accounting; Doctor of Economics; Doctor of Administration; Master in Accounting and Financial Auditing; Certified Public Accountant; Independent Auditor. General Manager of Microconsult-DHC Associates. Normal, remote and virtual undergraduate teacher; master's teacher; doctoral professor; Financial Advisor. In research, I am a teacher, advisor, reviewer, jury. More than 30 years of professional practice and more than 20 years of teaching work. Teaching experience at: Federico Villarreal National University; University of San Mart´ın de Porre. He can be contacted at email: dhernandez@unfv.edu.pe.

Michael Cabanillas-Carbonell Engineer and Master in Systems Engineering from the National University of Callao - Peru, a Ph.D. candidate in Systems Engineering and Telecommunications at the Polytechnic University of Madrid. President of the chapter of the Education Society IEEE-Peru. Conference Chair of the Engineering International Research Conference IEEE Peru EIRCON. Research Professor at Norbert Wiener University, Professor at Universidad Privada del Norte, Universidad Autónoma del Perú. Advisor and Jury of Engineering Thesis in different universities in Peru. International lecturer in Spain, the United Kingdom, South Africa, Romania, Argentina, Chile, and China. Specialization in software development, artificial intelligence, and machine learning. He can be contacted at email: mcabanillas@ieee.org.