International Journal of Safety and Security Engineering
Vol. 13, No. 1, February, 2023, pp. 97-106
Journal homepage: http://iieta.org/journals/ijsse

Information Security in the Banking Sector: A Systematic Literature Review on Current Trends, Issues, and Challenges

Alfredo Leonidas Vasquez Ubaldo[1], Vanessa Yeny Gutierrez Barreto[1], Juan Andres Berrios Albines[1], Laberiano Andrade-Arenas[2], Roberto Santiago Bellido-García[3*]

[1] Facultad de Ingeniería y Negocios, Universidad Privada Norbert Wiener, Lima 15046, Perú
[2] Facultad de Ingeniería, Universidad Tecnológica del Perú, Lima 15046, Perú
[3] Postgraduate School, Universidad San Ignacio de Loyola, Lima 15024, Perú

Corresponding Author Email: roberto.bellido@epg.usil.pe

https://doi.org/10.18280/ijsse.130111

Received: 31 December 2022
Accepted: 10 January 2023

Keywords:
banking sector, bibliometric analysis, cyberattacks, information security, PRISMA, systematic literature review

ABSTRACT

In recent years, information security has become a very important aspect, since it creates serious trouble for organizations that do not take it into consideration. In this regard, it was detected that many entities in the banking sector experience multiple problems that are mainly related to the way in which they protect their data, so it is necessary to pay close attention to this issue. For this reason, in this investigation it was decided to carry out a systematic review of the literature, obtaining 2,787 articles through searches in electronic databases. Likewise, the PRISMA method was used, which allowed the identification of 15 relevant articles to form the synthesis of the investigation. In the same way, a bibliometric analysis was carried out, which allowed knowing the gaps in knowledge. Finally, in the conclusions emphasis is placed on several aspects; for example, it is highlighted that cybercriminals constantly attack the banking sector and it is mentioned that all the research questions posed were successfully answered.

1. INTRODUCTION

As is well known, companies have different assets, such as infrastructure, machinery, cash, and means of transportation; however, the asset that sometimes goes unnoticed is information [1, 2]. In this sense, information, both physical and digital, plays a very important role in s, since, if they are not managed properly, they will be vulnerable to various risks that could lead to their end [3]. In consequence, s must manage their information efficiently to continue struggling to achieve their proposed objectives.

Following the above, to satisfactorily protect the information, human, al and technological aspects play a central integrating role in the security of this important asset. In other words, these aspects are critically important and closely related [4]. Likewise, most companies choose to invest in information systems as a tool for the proper management of their data. in order to make good strategic decisions that help them position themselves in the market, seek excellence in their operations, venture into new models of business, reach more customers and suppliers, and gain a competitive advantage over their competitors [5]. Therefore, it is evident that there is a concern for the efficient management of information within companies since it is a challenge that they must overcome to move forward.

But information management is not just about the correct use of data. It is also about the security of this valuable asset. In this sense, information security seeks to protect the information assets of companies from any unauthorized access, disclosure, or infringement [6]. It focuses on managing the various risks that threaten data confidentiality, integrity, and availability, these three being its goals [7, 8]. But these goals are not easy to meet. According to the authors [9], the domain of information security requires a multidisciplinary knowledge of a large amount of information, experience, and skill. In consequence, not having this multidisciplinary knowledge makes the fight of companies against risks, vulnerabilities, and threats more difficult.

Also, it should not be forgotten that, with the growing popularity of the Internet and its services, there is an increase in information security threats, such as social engineering, malware, and hacking, of which some users may not be aware [10]. Additionally, while many different security methods, such as intrusion detection systems and antivirus software, are used to protect IT systems from different attacks, the information security threat landscape continues to rapidly evolve and attackers are putting more effort into developing sophisticated and advanced malware and hacking methods [11]. Therefore, it is evident that there is an urgency on the part of companies to take new measures to face the wide variety of forms that cyberattacks are adopting.

In another line, there is little evidence that users are aware of the threats and forms of protection that revolve around information security, as well as that they practice mechanisms to deal with this problem [12-14]. In addition, there is evidence that users have difficulty understanding information security threats, as well as not knowing what to use and how to react to them [15-17]. In short, it is important that users are fully prepared to face the threats that revolve around information security.

On the other hand, it is necessary to mention the banking sector, which is an integral part of the economy. It plays a fundamental role in the well-being of the economy since a weak banking sector not only becomes a threat to maintaining

a sustainable economy in the long term but can also trigger financial instability that can lead to economic problems [18]. Therefore, the banking sector is crucial since it greatly influences the course of the economy of each country in the world. In this sense, entities in this sector must always take measures to safeguard their assets.

The banking sector suffers many cases of cyberattacks. For this reason, banks invest heavily in cybersecurity, with large budgets devoted to protecting their hardware and software [19]. Nevertheless, banking systems are susceptible to cyberattacks in several ways. This issue is due to the large number of access channels they provide and the economic gain obtained by the cybercriminal who successfully attacks [20]. But the problem does not end here. Due to the development of digital technology, this problem is also reflected in online banking, where the personal data of users in the banking sector have become more vulnerable to fraudulent attacks, so this problem requires the study and active use of new tools to protect everyone. confidential customer information [21]. In this sense, it is not enough for banks to invest only in ways to protect their hardware and software, as information threats are acquiring more entry points over time. Therefore, it is important to constantly update and look for new mechanisms to safeguard all information, with the aim of providing secure banking services to customers.

Based on everything mentioned above, it is justified that this study is very important since it aims to respond to the knowledge gaps, concerning information security in the banking sector, through the research questions raised. Likewise, the aim of this study is to present a systematic literature review in the field of information security that identifies the trends, issues, and challenges that revolve around the banking sector, worldwide today.

2. METHODOLOGY

For this research, it was decided to carry out a systematic literature review regarding information security in the banking sector. Likewise, it was decided to use the PRISMA method during the process. In the same way, it was decided to carry out a bibliometric analysis to complement the study by giving it a quantitative approach.

2.1 Study type

A systematic literature review (SLR) is a tool used to assess and interpret all available research related to a particular research question, topic area, or phenomenon of interest [22]. Likewise, SLR studies aim to identify relevant primary documents, extract the required data, and analyze and synthesize results to obtain a broader and deeper view of the investigated domain [23]. Additionally, regarding the usefulness of conducting SLR studies, there are several recent investigations [23-27], which show the benefits of this study type. In consequence, the importance of carrying out this SLR study lies in the need to know in depth about the state of information security in the banking sector.

2.2 Methodological approach

PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) is a method created in 2009 to help authors of systematic reviews and meta-analyses improve the presentation of their reports [28]. Likewise, the PRISMA method helps a lot in conducting SLR studies because it has a set of steps that allow exhaustively collecting all possible scientific production and analyzing the evidence in detail. Therefore, it can be proven that the PRISMA method is applicable to analyze this type of problem, since it allows organizing the literature found from start to finish by means of an algorithm.

2.3 Research questions

As part of the process of this systematic literature review study, it was decided to formulate some research questions to fill the knowledge gaps. These research questions can be observed in Table 1.

Table 1. Research questions

Codes	Denominations
RQ1	What are the most recurring cyberattacks that threaten information security in the banking sector?
RQ2	What are the most transcendental factors that favor information insecurity in the banking sector?
RQ3	What is the biggest negative impact generated by information insecurity in the banking sector?
RQ4	What are the most effective and feasible strategies that counter information insecurity in the banking sector?

2.4 Eligibility criteria

For the development of this study, eligibility criteria (inclusion and exclusion) were applied. These eligibility criteria can be observed in Table 2.

Table 2. Eligibility criteria

Criteria	Codes	Descriptions
Inclusion	IC1	Papers related to information security in the banking sector.
	IC2	Papers published between 2018 and 2022.
	IC3	Papers published in the English language.
	IC4	Papers of primary studies.
	IC5	Papers with full-text available.
Exclusion	EC1	Papers not related to information security in the banking sector.
	EC2	Papers not published between 2018 and 2022.
	EC3	Papers not published in the English language.
	EC4	Papers of secondary and tertiary studies.
	EC5	Papers without full-text available.

2.5 Information sources

To carry out the collection of articles for this RSL, we chose to use electronic databases that are reliable and known in the academic community. These selected information sources can be observed in Figure 1.

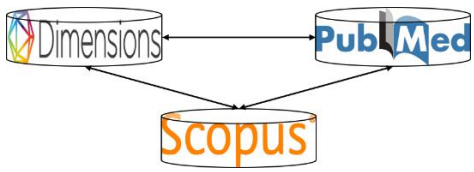

Figure 1. Information sources

2.6 Search strategy

As a search strategy for this systematic review of the literature, we chose to use a formula that contains the terms closest to the research, together with Boolean operators.

- ("information security" OR "information insecurity" OR "computer security" OR "cyber security" OR "cybersecurity" OR "cyber attack" OR "cyberattack" OR "cyber attacks" OR "cyberattacks" OR "cyber threat" OR "cyberthreat" OR "cyber threats" OR "cyberthreats") AND ("banking sector" OR "banking industry" OR "financial sector" OR "financial industry" OR "bank" OR "banks" OR "banking entity" OR "banking entities" OR "financial entity" OR "financial entities" OR "banking system")

2.7 Study selection process

The study selection process is divided into 4 phases:

2.7.1 Identification

It is the phase in which it is determined how many studies were identified in total, both through the search in databases and through the search in other sources.

2.7.2 Screening

It is the phase in which a preliminary selection of the studies is carried out, since those articles that will probably serve to fulfill the purposes of the investigation are distinguished.

2.7.3 Eligibility

It is the phase in which those studies that meet the necessary conditions to be accepted and form part of the investigation are analyzed.

2.7.4 Inclusion

It is the phase in which the accepted studies that will be part of the research synthesis (both qualitative and quantitative) are obtained.

2.8 Bibliometric analysis

Bibliometrics is the mathematical and statistical analysis of bibliographic records [29]. It is used to make intellectual links between articles and keywords, in order to get an overview of emerging trends and potential research opportunities [30, 31]. In this sense, it is very important to add bibliometrics to research because it helps to identify gaps in knowledge.

The bibliometric analysis focuses on analyzing statistical data related to each other [32]. It is an approach to measuring, tracking, and analyzing academic literature through a set of quantitative methods [33].

On the other hand, it was decided to use VOSviewer, which is a program that is freely available. It is a software that allows to build and visualize bibliometric maps. In the same way, it allows to visualize each map made in several different ways, changing its appearance. In addition, it has a viewer and zoom, scroll, and search functions that facilitate the detailed visualization of the maps [34]. Additionally, regarding the use of this computer program, there are several recent investigations [35-42], where not only the scientific production of topics and areas of knowledge are analyzed, but also of authors and journals, and with periods of years and predetermined databases. Therefore, it is notorious that VOSviewer is a very convenient tool for performing bibliometric analysis.

3. RESULTS

In this section, all the results of the RSL are explained.

3.1 About the search of studies

From the searches in electronic databases, 2,787 papers related to the topic of this research were identified and analyzed. Of this number of studies collected, 1,379 were found in Dimensions; 246, in PubMed; and 1,162, in Scopus. In addition, it is worth mentioning that the search was performed several times as the study progressed and ended on December 31, 2022. These search results of studies can be observed in Figure 2.

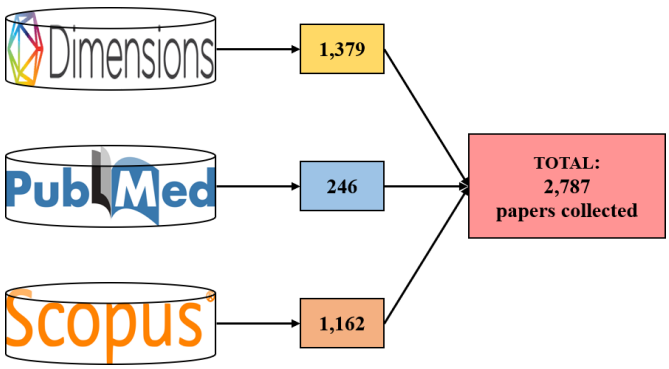

Figure 2. Search results of studies

3.2 About the selection of studies

Of the 2,787 studies obtained, 129 duplicate articles were eliminated, leaving 2,658. Subsequently, 1,981 studies were excluded and 677 remained. Finally, after an exhaustive review with particular criteria, 662 articles were eliminated and only 15 remained, which were selected to form part of the qualitative synthesis of this study. Likewise, the 2,787 studies obtained at the beginning will form part of the quantitative synthesis. This selection process can be observed in Figure 3.

3.3 About the designation of studies

Based on the articles selected to be part of this SLR study, it was decided to designate which ones would help answer each research question. This relevance of studies to research questions can be observed in Table 3.

Table 3. Designation of studies

Questions	Numbers of studies	Designated studies
RQ1	7	[43-49]
RQ2	5	[20, 46, 50-52]
RQ3	2	[43, 53]
RQ4	5	[20, 21, 50, 54, 55]

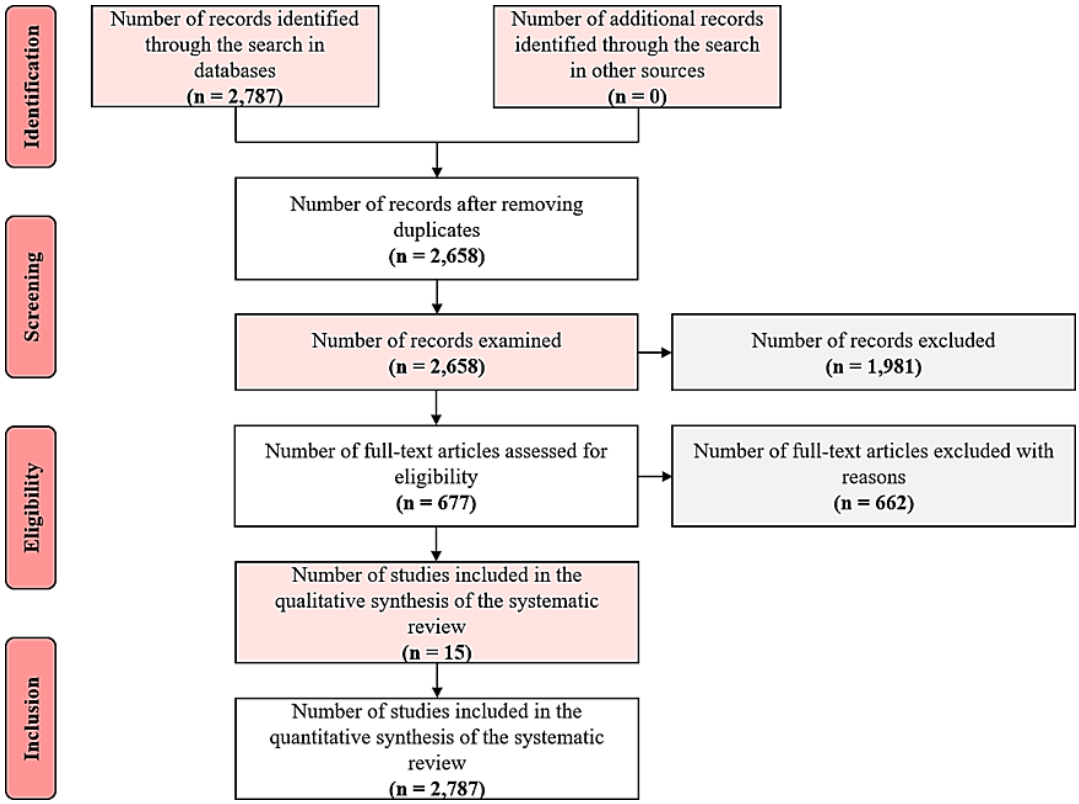

Figure 3. Search results of studies

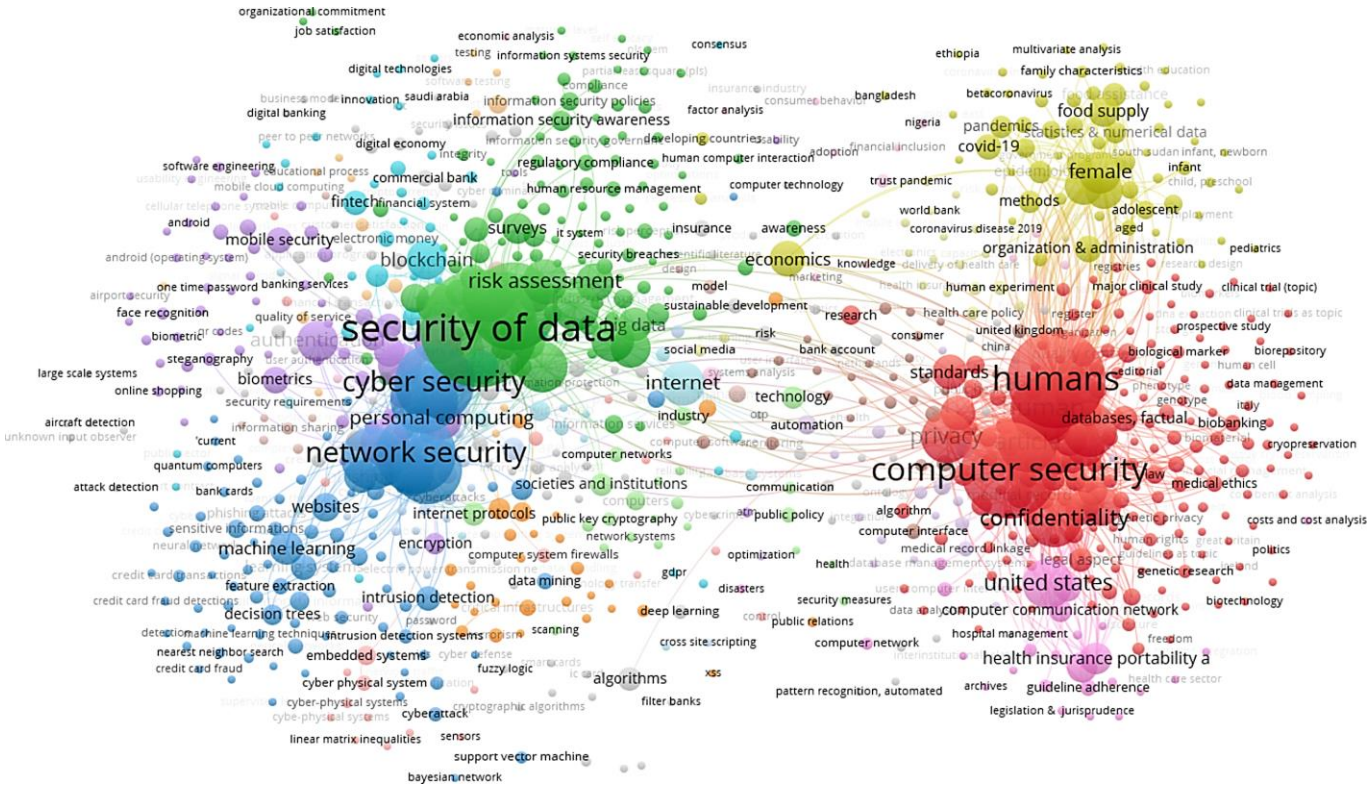

Figure 4. Network visualization

3.4 About the bibliometric analysis

Based on the 2,787 studies found, the bibliometric analysis was carried out with the help of the VOSviewer software.

3.4.1 Network visualization

This graph shows the weight of the themes, being that the larger the term, the larger the circle. This network visualization can be observed in Figure 4.

Referring to Figure 4, the node groups made up of green, blue and red clusters stand out more. The respective interpretations of these groups of nodes are described below:

- Green Cluster Nodegroup: Has its biggest point in security of data. It is closely related to other topics,

such as risk assessment, information security awareness, security breaches, regulatory compliance, human resource management, and computer networks.

- Blue Cluster Nodegroup: Has its biggest point in network security. It is closely related to other topics, such as personal computing, machine learning, intrusion detection, detection systems, credit card fraud, and data mining.
- Red Cluster Nodegroup: Has its biggest spike in computer security. It is closely related to other topics, such as confidentiality, privacy, humans, algorithm, standards, and data management.

3.4.2 Overlay visualization

This graph shows the evolution of terms over time. This overlay visualization can be observed in Figure 5.

Referring to Figure 5, it can be observed that the colors of the clusters vary in relation to the evolution of their terms over time. It is visualized that the yellow clusters are the ones that have had the greatest evolution in recent years, due to the fact that they have had a greater number of scientific productions.

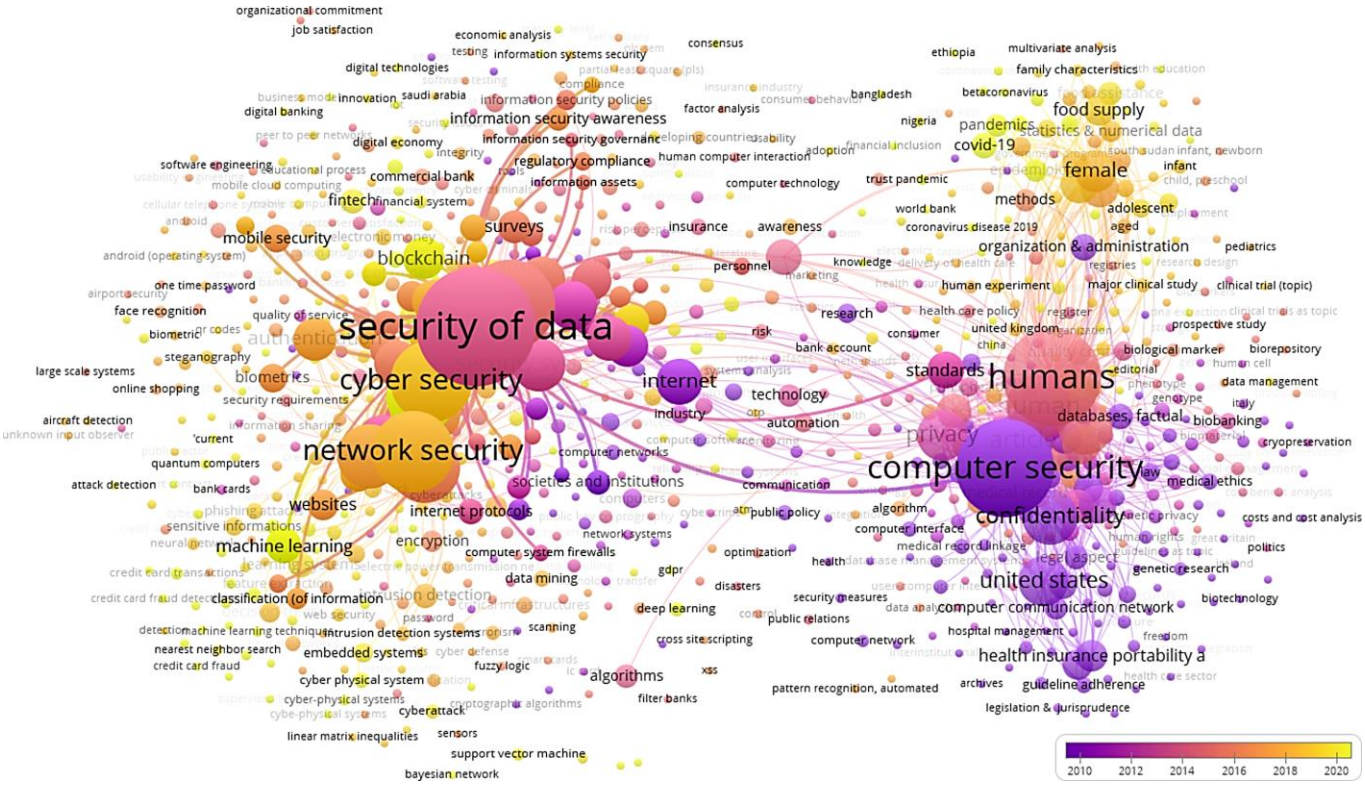

Figure 5. Overlay visualization

Figure 6. Density visualization

3.4.3 Density visualization

This graph shows the item density visualization, next to the group density visualization. This density visualization can be observed in Figure 6.

Referring to Figure 6, the density of the keywords obtained from the bibliometric analysis can be observed. It is visualized that the yellow areas represent the importance and concurrence of investigations related to information security in the banking sector. Meanwhile, in the other areas of lower density, the terms referring to the main themes are located. In this sense, the words "security of data" is the most predominant of all. Likewise, "humans", "network security", "cyber security" and "computer security" also stand out, observing a relationship between information security and the human part.

3.5 Proposed model

Apart from everything previously presented, for this investigation it was decided to develop a model that helps companies belonging to the banking sector in the face of the increase in threats to information security. This proposed model can be observed in Figure 7.

Figure 7. Proposed model: APVA cycle

The proposed model was applied in an industrial company. In this regard, before and after the application was compared, considering the update, protection, surveillance and action, which are part of the cycle of the proposed model. Likewise, a survey was carried out among the managers involved in the company in question, obtaining a significant improvement (in percentages) among the results. This improvement can be observed in Table 4.

Table 4. Applicability of the proposed model

Cycles	Start	Final
Actualization	40%	75%
Protection	28%	63%
Vigilance	37%	71%
Action	39%	81%

4. DISCUSSIONS

In this section, it is intended to answer the research questions posed, as well as address other equally important aspects.

4.1 About the research questions

4.1.1 RQ1: What are the most recurring cyberattacks that threaten information security in the banking sector?

The study [43] mentions that data breaches and fraud have increased, especially in the banking, healthcare, and government sectors. In this sense, it is stated that phishing is a threat that has gained great relevance.

From another perspective, the study [44] exposes that distributed denial-of-service (DDoS) is another cyberattack that commonly threatens information security in banks.

From another approach, the study [45] indicates that malware is a highly preferred way for cybercriminals to attack banks and other financial institutions. In addition, this study mentions that malware is a cyberattack that has evolved to great levels, acquiring new forms, such as the use of encrypted payloads and obfuscation techniques, making it difficult to detect.

In another line, the study [46], which was strictly based on the Hungarian financial sector, found that phishing and denial-of-service (DoS) are the most common cyberattacks in that country. In addition, it can be verified that phishing is indeed a very common term in relation to this subject, due to the bibliometric analysis carried out, which can be observed in Figure 4, Figure 5, and Figure 6.

Seen in another way, the study [47] also mentions phishing; however, cyberstalking, hacking, cross-site scripting (XSS) and denial-of-service (DoS) are other very popular cyberattacks in the banking sector.

Similarly, the study [48] is yet another piece of research that mentions phishing. In this regard, this study indicates that phishing has become one of the most common methods to commit fraudulent acts since it allows the theft of passwords and other confidential data by deceiving the victims.

Lastly, the study [49] warns that cybercriminals use malware-based tools or tactics, as well as distributed denial-of-service (DDoS), phishing, and trojans to breach the security of banking systems and commit illegal acts.

Based on the studies presented above, it is evident that phishing is one of the main cyberattacks that threaten the

security of information in the banking sector. Therefore, in this research, banking entities are urged to take preventive measures in this regard, in order to avoid negative impacts in the future.

4.1.2 RQ2: What are the most transcendental factors that favor information insecurity in the banking sector?

The study [20] indicates that banking security systems must be designed very carefully, considering many different factors in the process, not only internal to the banking infrastructure but also external systems (such as the procedures of the telecom operator).

On the other side, the study [46] identified inadequate physical security, which refers to the protection of ICT systems. In addition, it mentions that physical access to the ICT infrastructure by third parties generates risks of destruction or theft of its elements, risks of attacks on communication connections and conversations, and even the takeover of ICT systems. Likewise, it indicates that the risk of the supply chain must be taken into account, referring to criminals who try to insert malware into ICT systems through the access supply chain.

From another perspective, the study [50] exposes that the technological measures of the banks have been insufficient to handle the attacks on cybersecurity. Likewise, this study mentions that the fact that banks have unethical or unethical employees makes it more likely that the number of attacks within them will increase.

From another approach, the study [51] identified 27 associated factors, of which 5 stand out as the most critical to consider. The first is the lack of a backup electric generator, of which it is indicated that not having at least one creates vulnerability in the digital infrastructure. This is followed by

failures in firewall protection, lack of information security audits, lack of encryption control management, and lack of protection of the true identity of users, in that order.

Lastly, the study [52] mentions that there is a lack of awareness about information security on the part of the employees of the entities belonging to the banking sector.

Based on the studies presented above, it is evident that there are many factors related to both physical and digital security. In this regard, it is necessary for banking entities to consider both aspects when taking preventive measures, in order to avoid a host of negative impacts that may appear.

4.1.3 RQ3: What is the biggest negative impact generated by information insecurity in the banking sector?

The insecurity of information has negative consequences of different kinds. For example, the study [43] mentions that cyberattacks allow cybercriminals to steal financial data through access to machines and networks. However, none of these consequences would be the biggest negative impact that a company can have due to the insecurity of information. In this regard, the study [53] maintains that the breach in information security is quite reflected in the economy of the company because cyberattacks cause problems mainly in operations. Therefore, this is reflected in the company's loss of money, often in excess of millions of dollars.

Based on the studies presented above, it is evident that the most common negative impact caused by cyberattacks in the banking sector is reflected in the economy of the company. However, none of the studies mention points about the prestige of entities in the banking sector, as well as other negative impacts.

4.1.4 RQ4: What are the most effective strategies to protect information security in the banking sector?

The study [20] indicates that banking security systems need to be designed very carefully, considering many different factors in the process, not only within the banking infrastructure but also outside of it. In addition, this study mentions more aspects related to how to improve banking security, among them that biometrics could be very useful to reconcile security and ergonomics; It also exposes other strategies that could help to significantly increase the level of security, such as introducing software and hardware tokens and using biometric channels.

In another line, the study [21], in which both the international and Russian contexts were examined, maintains that biometrics is a very helpful tool in the security of information in the banking sector. However, this study mentions that the introduction of biometric identification systems also entails aspects and risks of use to consider. Furthermore, this study raises the importance of increasing the transparency of the data provided by banking entities and indicates that measures must be taken to minimize the risk of unauthorized transactions, such as improving the financial situation of people, for example.

From another perspective, the study [50] exposes that the fact that banks have employees with temperance traits helps prevent cybersecurity breaches within them since temperance promotes ethical behavior. Likewise, it indicates that this ethical behavior can be identified through a personnel selection process or a background investigation that interprets its approach to ethical challenges; therefore, examining the ethical behaviors of employees helps to understand how to improve cybersecurity and can make banks more resilient to various attacks. Likewise, this study recommends that banks hire people willing to accept innovation and change, especially when implementing strategic technology and cybersecurity plans.

In another instance, the study [54] argues that paperless office technology is a strategy that not only makes it possible to secure information and financial transactions, but also to optimize labor costs, minimize operational risks, and many other benefits. In addition, it mentions other strategies that also help in information security and provide more benefits. These strategies are social engineering, which helps prevent embezzlement of funds from customer accounts; biometric identification, which helps prevent and block threats; information security psychology, which allows testing the processes of identification and timely response to suspicious files, calls, and messages; and RegTech and SupTech, which are regulatory and supervisory technologies that enable banks to comply with state regulatory requirements faster, more efficiently, and with minimal risk and cost.

Seen in another way, the study [55] indicates that proactive behavior and collaboration among all the actors directly involved in the financial industry is of the utmost importance to discover new emerging risks and the measures and regulations to be adopted to mitigate them. It also mentions other measures that entities in the banking sector must apply, such as constantly updating themselves on technological advances and continuing to invest in cybersecurity.

Based on the studies presented above, it is evident that security methods are important since they allow the protection of banking systems from various threats. However, none of the investigations found mention other strategies, such as the use of antivirus and constant password changes. For this reason, it is essential that banking entities be at the forefront with respect to new strategies to safeguard information.

4.2 About the proposed model

The proposed model presented in Figure 7 was called "APVA Cycle (Actualization-Protection-Vigilance-Action)" and consists of 4 stages. Regarding this proposed model, it is explained below:

4.2.1 Actualization

It is the phase where the entities of the banking sector must be constantly updated on the new modalities of cyberattacks and new solution alternatives so that they are prepared for threats.

4.2.2 Protection

It is the phase in which entities in the banking sector must take preventive measures in terms of hardware and software since this would prevent many latent threats.

4.2.3 Vigilance

It is the phase in which employees of banking sector entities must carefully observe if there are signs of attacks on information security in order to take appropriate measures.

4.2.4 Action

It is the phase in which entities in the banking sector must take timely measures as soon as vulnerabilities to information security are detected, in order to avoid negative impacts.

5. CONCLUSIONS

In this paper, a systematic literature review on current trends, issues, and challenges that revolve around information security in the banking sector was presented. In this regard, after systematically recognizing and reviewing 15 primary studies of many relevant papers in this domain, great results were obtained. According to the findings obtained in this research, it is concluded that the banking sector presents great vulnerabilities in the protection of its information. It was evidenced that cybercrime is increasing since cybercriminals constantly devise new practices to illegally access information from entities belonging to the banking sector.

Based on the research questions answered, it is concluded that phishing is a very popular type of cyberattack in the banking sector. In addition, it was identified that there are physical and digital factors that predominate; in this sense, banks must protect both hardware and software for the sake of their future. Also, it is observed that the most negative impact caused by cyberattacks is reflected in the economic aspect, due to the multiple problems that prevent the proper functioning of the processes of banking entities. In the same way, it is evident that attacks on the information of banking entities skimp on borders, since there are cybercriminals all over the world ready to enter the system of any bank.

On the other hand, regarding the methodology used, it can be observed that carrying out a systematic literature review was an ideal decision since there were too many articles in the databases. Likewise, the use of the PRISMA method helped to systematize the studies found and the bibliometric analysis allowed to analyze all this information in depth.

In another line, the APVA model was proposed based on the findings obtained, in which it is recommended how the cycle of confrontation with cyberthreats by entities in the banking sector should be.

Finally, it is recommended that further research be carried out on the subject, considering emerging technologies and applying the model proposed in this study.

REFERENCES

[1] Zhao, Q., Chen, S., Liu, Z., Baker, T., Zhang, Y. (2020). Blockchain-based privacy-preserving remote data integrity checking scheme for IoT information systems. Information Processing & Management, 57(6): 102355. https://doi.org/10.1016/j.ipm.2020.102355

[2] Zhang, X. (2021). Corporate accounting information disclosure based on FPGA and neural network. Microprocessors and Microsystems, 83: 103973. https://doi.org/10.1016/j.micpro.2021.103973

[3] Meneses, F.E.G., Segura, D.F.C. (2010). Relación de la presentación de información de negocios on-line con las variables financieras en las empresas colombianas. Revista de la Facultad de Ciencias Económicas: Investigación y Reflexión, 18(1): 205-224. https://doi.org/10.18359/rfce.2289

[4] Safa, N.S., Von Solms, R., Futcher, L. (2016). Human aspects of information security in organisations. Computer Fraud & Security, 2016(2): 15-18. https://doi.org/10.1016/S1361-3723(16)30017-3

[5] Calder, A., Watkins, S.G. (2010). Information Security Risk Management for ISO 27001/ISO 27002, third edition (3rd ed.). IT Governance Publishing. https://doi.org/10.2307/j.ctvndv9kx

[6] Ghazvini, A., Shukur, Z., Hood, Z. (2018). Review of information security policy based on content coverage and online presentation in higher education. International Journal of Advanced Computer Science and Applications, 9(8): 410-423 https://doi.org/10.14569/IJACSA.2018.090853

[7] Tripton, H.F., Krause, M. (2007). Information Security Management Handbook, sixth edition (6th ed.). CRC Press.

[8] Merkow, M.S., Breithaupt, J. (2014). Information security: Principles and practices, second edition (2nd ed.). Pearson Education.

[9] Whitman, M.E., Mattord, H.J. (2012). Principles of Information Security, fourth edition (4th ed.). Cengage Learning.

[10] Bawazir, M.A., Mahmud, M., Molok, N.N.A., Ibrahim, J. (2016). Persuasive technology for improving information security awareness and behavior: Literature review. In 2016 6th International Conference on Information and Communication Technology for The Muslim World (ICT4M), Jakarta, Indonesia, pp. 228-233. https://doi.org/10.1109/ICT4M.2016.054

[11] Alohali, M., Clarke, N., Furnell, S. (2018). The design and evaluation of a user-centric information security risk assessment and response framework. International Journal of Advanced Computer Science and Applications, 9(10): 148-163. https://doi.org/10.14569/IJACSA.2018.091018

[12] Talib, S., Clarke, N.L., Furnell, S.M. (2010). An analysis of information security awareness within home and work environments. In 2010 International Conference on Availability, Reliability and Security, Krakow, Poland, pp. 196-203. https://doi.org/10.1109/ARES.2010.27

[13] Xavier, U.H.R., Pati, B.P. (2012). Study of internet security threats among home users. In 2012 Fourth International Conference on Computational Aspects of Social Networks (CASoN), Sao Carlos, Brazil, pp. 217-221. https://doi.org/10.1109/CASoN.2012.6412405

[14] Kritzinger, E., Von Solms, S.H. (2013). Home user security-from thick security-oriented home users to thin security-oriented home users. In 2013 Science and Information Conference, London, UK, pp. 340-345.

[15] Zaaba, Z.F., Furnell, S., Dowland, P. (2011). End-user perception and usability of information security. In HAISA, pp. 97-107.

[16] Mensch, S., Wilkie, L. (2011). Information security activities of college students: An exploratory study. Academy of Information and Management Sciences Journal, 14(2): 91-116.

[17] Komatsu, A., Takagi, D., Takemura, T. (2013). Human aspects of information security: An empirical study of intentional versus actual behavior. Information Management & Computer Security, 21(1): 5-15. https://doi.org/10.1108/09685221311314383

[18] Mhadhbi, K., Terzi, C., Bouchrika, A. (2020). Banking sector development and economic growth in developing countries: a bootstrap panel Granger causality analysis. Empirical Economics, 58(6): 2817-2836. https://doi.org/10.1007/s00181-019-01670-z

[19] Hammour, R.A., Gharaibeh, Y.A., Qasaimeh, M., Al-Qassas, R.S. (2019). The status of information security systems in banking sector from social engineering perspective. In Proceedings of the Second International

Conference on Data Science, E-Learning and Information Systems, pp. 1-7. https://doi.org/10.1145/3368691.3368705
[20] Wodo, W., Stygar, D., Blaskiewicz, P. (2021). Security issues of electronic and mobile banking. In SECRYPT, pp. 631-638.
[21] Bakunova, T.V., Trofimova, E.A., Lapteva, E.V. (2019). Biometrics as a method of information security in the banking sector digitalization. In International Scientific and Practical Conference on Digital Economy (ISCDE 2019). Atlantis Press. pp. 929-934. https://doi.org/10.2991/iscde-19.2019.50
[22] Kitchenham, B., Charters, S. (2007). Guidelines for performing systematic literature reviews in software engineering.
[23] Falade, A., Azeta, A., Oni, A., Odun-ayo, I. (2019). Systematic literature review of crime prediction and data mining. Review of Computer Engineering Studies, 6(3): 56-63. https://doi.org/10.18280/rces.060302
[24] Van Dinter, R., Tekinerdogan, B., Catal, C. (2021). Automation of systematic literature reviews: A systematic literature review. Information and Software Technology, 136: 106589. https://doi.org/10.1016/j.infsof.2021.106589
[25] Siddiqui, S.A., Parahoo, S., Sadi, M.A.N., Afzal, M.N.I. (2021). Rural tourism as a transformative service of community well-being: A systematic literature review. International Journal of Sustainable Development and Planning, 16(6): 1081-1090. https://doi.org/10.18280/ijsdp.160609
[26] Weber, B., Fischer, T., Riedl, R. (2021). Brain and autonomic nervous system activity measurement in software engineering: A systematic literature review. Journal of Systems and Software, 178: 110946. https://doi.org/10.1016/j.jss.2021.110946
[27] Aini, N., Modjo, R., Lestari, F. (2022). Hospital preparedness in facing COVID-19 pandemic: A systematic literature review. International Journal of Design & Nature and Ecodynamics, 17(2): 311-317. https://doi.org/10.18280/ijdne.170219
[28] Moher, D., Liberati, A., Tetzlaff, J., Altman, D.G., PRISMA Group*. (2009). Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. Annals of Internal Medicine, 151(4): 264-269. https://doi.org/10.7326/0003-4819-151-4-200908180-00135
[29] Pritchard, A. (1969). Statistical bibliography or bibliometrics. Journal of Documentation, 25: 348.
[30] Boyack, K.W., Klavans, R. (2010). Co-citation analysis, bibliographic coupling, and direct citation: Which citation approach represents the research front most accurately? Journal of the American Society for Information Science and Technology, 61(12): 2389-2404. https://doi.org/10.1002/asi.21419
[31] Marchiori, D., Franco, M. (2020). Knowledge transfer in the context of inter-organizational networks: Foundations and intellectual structures. Journal of Innovation & Knowledge, 5(2): 130-139. https://doi.org/10.1016/j.jik.2019.02.001
[32] Ellegaard, O., Wallin, J.A. (2015). The bibliometric analysis of scholarly production: How great is the impact? Scientometrics, 105(3): 1809-1831. https://doi.org/10.1007/s11192-015-1645-z
[33] Roemer, R.C., Borchardt, R. (2015). Meaningful metrics: A 21st century librarian's guide to bibliometrics, altmetrics, and research impact. Amer Library Assn. https://doi.org/10.7710/2162-3309.2290
[34] Van Eck, N., Waltman, L. (2010). Software survey: VOSviewer, a computer program for bibliometric mapping. Scientometrics, 84(2): 523-538. https://doi.org/10.1007/s11192-009-0146-3
[35] Garcés-Gómez, Y.A., Henao-Céspedes, V. (2022). International Journal of Electrical and Computer Engineering: A bibliometric analysis. International Journal of Electrical & Computer Engineering, 12(6): 5667-5673. http://doi.org/10.11591/ijece.v12i6.pp5667-5673
[36] Krauskopf, E. (2018). A bibiliometric analysis of the Journal of Infection and Public Health: 2008–2016. Journal of Infection and Public Health, 11(2): 224-229. https://doi.org/10.1016/j.jiph.2017.12.011
[37] Koo, M. (2017). A bibliometric analysis of two decades of aromatherapy research. BMC Research Notes, 10(1): 1-9. https://doi.org/10.1186/s13104-016-2371-1
[38] Zyoud, S.E.H., Waring, W.S., Al-Jabi, S.W., Sweileh, W.M. (2017). Global cocaine intoxication research trends during 1975–2015: A bibliometric analysis of Web of Science publications. Substance Abuse Treatment, Prevention, and Policy, 12: 6. https://doi.org/10.1186/s13011-017-0090-9
[39] Merigó, J.M., Gil-Lafuente, A.M., Kacprzyk, J. (2017). A bibliometric analysis of the publications of Ronald R. Yager. In Granular, Soft and Fuzzy Approaches for Intelligent Systems (pp. 233-248). Springer, Cham. https://doi.org/10.1007/978-3-319-40314-4_12
[40] Sweileh, W.M., Zyoud, S.E.H., Al-Jabi, S.W., Sawalha, A.F., Shraim, N.Y. (2016). Drinking and recreational water-related diseases: A bibliometric analysis (1980–2015). Annals of Occupational and Environmental Medicine, 28: 40. https://doi.org/10.1186/s40557-016-0128-x
[41] Mesdaghinia, A., Mahvi, A.H., Nasseri, S., Nodehi, R.N., Hadi, M. (2015). A bibliometric analysis on the solid waste-related research from 1982 to 2013 in Iran. International Journal of Recycling of Organic Waste in Agriculture, 4(3): 185-195. https://doi.org/10.1007/s40093-015-0098-y
[42] Zhu, Q., Kong, X., Hong, S., Li, J., He, Z. (2015). Global ontology research progress: A bibliometric analysis. Aslib Journal of Information Management, 67(1): 27-54. https://doi.org/10.1108/AJIM-05-2014-0061
[43] Quadir Md, A., Jaiswal, D., Daftari, J., Haneef, S., Iwendi, C., Jain, S.K. (2022). Efficient dynamic phishing safeguard system using neural boost phishing protection. Electronics, 11(19): 3133. https://doi.org/10.3390/electronics11193133
[44] Islam, U., Muhammad, A., Mansoor, R., Hossain Md, S., Ahmad, I., Eldin, E.T., Khan, J.A., Rehman, A.U., Shafiq, M. (2022). Detection of distributed denial of service (DDoS) attacks in IOT based monitoring system of banking sector using machine learning models. Sustainability, 14(14): 8374. https://doi.org/10.3390/su14148374
[45] Zimba, A. (2022). A Bayesian attack-network modeling approach to mitigating malware-based banking cyberattacks. International Journal of Computer Network & Information Security, 14(1): 25-39. https://doi.org/10.5815/ijcnis.2022.01.03

[46] Somogyi, T., Nagy, R. (2022). Cyber threats and security challenges in the Hungarian financial sector. Sodobni Vojaški Izzivi, 24(3): 15-30. https://doi.org/10.33179/BSV.99.SVI.11.CMC.24.3.1
[47] Hasan, M.F., Al-Ramadan, N.S. (2021). Cyber-attacks and cyber security readiness: iraqi private banks case. Social Science and Humanities Journal, 5(8): 2312-2323.
[48] Revenkov, P.V., Oshmankevich, K.R., Berdyugin, A.A. (2021). Phishing schemes in the banking sector: Recommendations to internet users on protection and development of regulatory tasks. Finance: Theory and Practice, 25(6): 212-226. https://doi.org/10.26794/2587-5671-2021-25-6-212-226
[49] Tariq, N. (2018). Impact of cyberattacks on financial institutions. Journal of Internet Banking and Commerce, 23(2): 317.
[50] Ruth, N., Kituyi, M., Kaggwa, F. (2022). Establishing the influences of cardinal virtues on employees' cyber security ethical behavior in the banking sector in Uganda. European Journal of Technology, 26(1): 1-13. https://doi.org/10.47672/ejt.896
[51] Edu, A.S., Agoyi, M., Agozie, D. (2021). Digital security vulnerabilities and threats implications for financial institutions deploying digital technology platforms and application: FMEA and FTOPSIS analysis. PeerJ Computer Science, 7: e658. https://doi.org/10.7717/peerj-cs.658
[52] Woretaw, A., Lessa, L., Negash, S. (2019). Factors hindering full-fledged information security in banking sector in Ethiopia: Emphasis on information security culture. In 25th Americas Conference on Information Systems, AMCIS 2019, Cancún, Mexico, August 15-17, 2019, pp. 1-10.
[53] Stanikzai, A.Q., Shah, M.A. (2021). Evaluation of cyber security threats in banking systems. In 2021 IEEE Symposium Series on Computational Intelligence (SSCI), rlando, FL, USA, pp. 1-4. https://doi.org/10.1109/SSCI50451.2021.9659862
[54] Kondratyeva, M.N., Svirina, D.D., Tsvetkov, A.I. (2021). The role of information technologies in ensuring banking security. In IOP Conference Series: Materials Science and Engineering, 1047(1): 012069. https://dx.doi.org/10.1088/1757-899X/1047/1/012069
[55] Boitan, I.A. (2019). Cyber security challenges through the lens of financial industry. International Journal of Applied Research in Management and Economics, 2(4): 33-38. https://doi.org/10.33422/ijarme.v2i4.275