Journal of Ecohumanism
2024
Volume: 3, No: 8, pp. 6439 – 6448
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i8.5276

Computer Crime in the Digital Age Literature Review of Scientific Articles From 2019 to 2024

Mgs. Luis Antonio Villalta Gavilanes[1], Mgs. Leonardo Orleans Labre Villalta[2], Mgs. Adriana Mercedes Villalta Gavilanes[3], Dra. Cecilia Teresita de Jesús Carbajal Llauce[4]

Abstract

This systematic review study was conducted from 2019 to 2024 following the guidelines of the PRISMA protocol through an exhaustive search in Scopus, SciELO, Redalyc, Dialnet, Erih Plus, Latindex, the University César Vallejo library, and other databases, and aims to identify current trends and challenges in the prevention of cybercrime in Ecuador. The results show that, despite legislative efforts, cybercrime remains a growing problem in the country. The findings of this research have important implications for public policy formulation, investment in technology, and cybersecurity education in Ecuador. Lack of user awareness, insufficient resources for law enforcement, and the rapid evolution of technologies were identified as key factors. Public policies that promote cybersecurity education, investment in protection technologies, and collaboration between public and private institutions are recommended. In conclusion, this systematic review underscores the need to adopt a multidisciplinary and proactive approach to combat cybercrime in Ecuador.

Keywords: *Computer Fraud, Phishing, Cybercriminals, Cybersecurity Education and Protection Technologies.*

Introduction

In the digital era, computer crimes have emerged as one of the main threats to personal, business and government security (Rodríguez and Moreno, 2024). Due to the increased use of information and communication technologies, cybercriminals have found new opportunities to perpetrate illicit activities that transcend physical borders. This phenomenon has been driven by digital globalization, which has facilitated access to sensitive information and has allowed fraud, identity theft and other large-scale cybercrimes to be carried out (Ponce, 2024). The central problem lies in the difficulty of regulating and prosecuting these crimes, given their transnational nature and the rapid evolution of the technologies used to commit them.

This problem of computer crimes in the digital age has become a topic of growing concern at a national and international level. With the rise of technology and the digitalization of services, cybercriminals have found fertile ground to carry out their illicit activities, resulting in a significant increase in the frequency and sophistication of these crimes. According to a report by the United Nations Office on Drugs and Crime (UNODC, 2013), the fragmentation of national laws and the diversity of legal approaches complicate international cooperation in the fight against cybercrime, which limits the effectiveness of current legal responses.

At a global level, in Mexico by the end of 2019, cybercrimes increased by almost 40%, which represents economic losses that are difficult to overcome (Domínguez and Vera, 2022). This increase reflects how technology, although essential for development, also becomes a channel for illicit activities. Furthermore, it can be inferred that this growth is probably due to the increase in the adoption of digital technologies, combined with a lack of awareness or adequate preventive measures on the part of users and organizations.

Given the problem raised, the following research question is proposed: What are the main trends and

[1] César Vallejo University, Peru, Email: lvillaltag@ucvvirtual.edu.pe, https://orcid.org/0000-0001-8556-6529, (Corresponding Author)
[2] César Vallejo University, Peru, Email: llabre@ucvvirtual.edu.pe, https://orcid.org/0009-0000-2762-1091.
[3] Espíritu Santo University, Ecuador, Email: adriana.villalta@uess.edu.ec, https://orcid.org/0009-0002-2426-1478

[4] César Vallejo University, Peru, Email: cllaucect@ucvvirtual.edu.pe, https://orcid.org/0000-0002-1162- 8755

challenges in the legislation and prevention of computer crimes in the digital age? While, as a general objective, it is proposed to analyze current trends in computer crimes and their impact.

Previous bibliometric studies have examined climate change research using various databases and on contemporary society, as well as evaluate the legal and preventive responses implemented in different contexts. In the same way, the following specific objectives are formulated: identify the most common types of computer crimes reported in the last five years; list the countries that have studied cybercrimes in the last five years and propose recommendations to improve prevention and response strategies to these crimes.

At this point it should be noted that the literature on cybercrime has expanded significantly in recent years, reflecting the growing academic and practical interest in this field. According to Guaña (2023), cybercrimes, defined as illegal activities that use computer systems as a means or objective, include a variety of criminal actions such as phishing, malware, hacking and identity theft.

According to Echeverría and Nivela (2024), computer crimes range from financial fraud to attacks on the integrity of computer systems. The most common classification includes: computer fraud, which is the illicit obtaining of personal or banking data. Also cyberbullying or the use of digital media to intimidate or harass. As well as computer sabotage or malicious interference with computer systems (Echeverría and Nivela, 2024).

In this sense, legislation on cybercrime varies significantly between countries. In many cases, criminal codes have been updated to include specific provisions on cybercrimes (Ordóñez, 2024). For example, the Comprehensive Organic Penal Code (COIP) in Ecuador addresses various forms of cybercrime, establishing penalties ranging from fines to years in prison. Despite the existing legal framework, significant challenges remain in the prevention and effective prosecution of these crimes. Since the anonymous nature of the digital environment makes it difficult to identify and capture cybercriminals, which requires a collaborative approach between governments, companies and citizens (Saltos et al., 2021). Furthermore, rapid technological evolution poses constant challenges to current regulations.

According to Juca and Medina (2023), cybercrime affects individuals in a particular way, but also represents a considerable risk for companies and national economies. Economic losses from cyber fraud are estimated in the billions annually, highlighting the urgent need for effective strategies to mitigate these risks. Therefore, the present systematic review of these aspects provides a critical context to understand how cybercrime is shaping our current digital reality and how it can be effectively addressed through appropriate policies and preventive initiatives.

Furthermore, the inherent characteristics of cybercrimes, such as their rapid execution, easy concealment, and transnational nature, make their prevention and prosecution especially complex. Likewise, the lack of institutional capacity in many countries to adequately investigate these crimes further aggravates the problem (Acosta et al., 2020). In summary, the problem of cybercrime is multifaceted and involves legal, technological and social challenges that require a coordinated and effective response at the international level. Therefore, the need for legislative harmonization and cooperation between countries is very necessary to address this growing phenomenon and protect both individuals and organizations from the threats of cybercrime.

Methodology and Materials

The present systematic review aims to identify the main trends in research on the use of artificial intelligence in the detection of computer crimes. In order to guarantee the rigor and transparency of this study, the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) method will be used. Since, this methodological approach will allow an exhaustive search to be carried out in various academic databases, evaluate the quality of the included studies and synthesize the results in a systematic way (Sánchez-Serrano et al., 2022). Thus, the findings of this review will contribute to a better understanding of the fight against cybercrime and to identifying future areas of research.

Como ya se indicó, la revisión se centra en la pregunta: ¿Cuáles son las principales tendencias y desafíos en la legislación y prevención de delitos informáticos en la era digital? Por lo tanto, se planteó una estrategia de búsqueda utilizando conectores booleanos para combinar términos relevantes, que permito formular la siguiente ecuación de búsqueda:

"delitos informáticos" AND "ciberdelincuencia" AND ("prevención" OR "legislación") AND ("tendencias" OR "desafíos") AND "era digital".

Furthermore, for an article to be considered in this work, the inclusion criteria were established:

- Studies published between 2019 and 2024.
- Articles that specifically address cybercrime, its legislation, prevention and trends.
- Research available in databases such as Scopus, SciELO, Redalyc, Dialnet, Erih Plus, Latindex and Universidad César Vallejo.
- Documents in Spanish and English.

Likewise, in order to exclude articles that did not contribute to this study, the following exclusion criteria were considered:

- Studies that do not focus on computer crimes or that do not address their legislative or preventive context.
- Duplicate articles or articles that are not available in full text.
- Publications that have not been peer reviewed.
- Studies that have information not relevant to the objectives of this review work.
- Duplicate articles.
- Work that does not present results.
- Works that are not scientific articles.
- Articles that are in a language other than Spanish or English.

Based on the above, an exhaustive search was carried out in the aforementioned databases, followed by a selection process based on the established criteria. Two independent reviewers assessed titles and abstracts for relevance, resolving any disagreements by discussion. Relevant data were then extracted from the selected studies, including information on the type of crime, legislative context, preventive approaches and results obtained. This extraction will be performed by the authors of this systematic review to ensure accuracy and minimize bias.

Next, the methodological quality of the included studies was evaluated using appropriate tools, such as the Newcastle-Ottawa scale or the GRADE (Grading of Recommendations Assessment, Development and Evaluation Working Group) system, depending on the type of study, because, according to González (2024) is a resource used to analyze the quality of evidence and determine the strength of recommendations during the development of clinical practice guidelines.

In the end, the extracted data were synthesized qualitatively and quantitatively as necessary, presenting a clear analysis on the trends and challenges identified in the literature regarding cybercrime. Therefore, a PRISMA flowchart was developed to illustrate the study selection and exclusion process, as well as a table summarizing the key characteristics of each included study. This systematic approach will allow readers to have a deeper understanding of the current state of cybercrime and will contribute to the formulation of recommendations to improve legislative and preventive strategies against this growing phenomenon.

Results and Discussion

Table 1. Data Extraction

Author(s)	**Year**	**Objective of the Study**	**Methodology**	**Main Results**	**Conclusions**
Eslava-Zapata et al.	2024	Examine the variables related to computer crimes in Latin America.	Quantitative research with a transectional design, based on data from the Latin American Computer Crime Observatory (ODILA) corresponding to the period 2015-2017, with a sample of 5,310 people.	The findings show that, in terms of the relationship between complaints by country and gender, men have a total representation in Argentina, while women have a greater presence in Mexico (22.38%), Colombia (20.23%). and Guatemala (8.54%). Regarding the level of education and the action of reporting, a high percentage of those who have not reported have a university level (81.35%).	It is concluded that computer crimes violate the privacy of individuals and organizations, and that cybercriminals take advantage of this environment to commit information theft, illicitly enrich themselves, and affect the integrity of those affected.
Sarmiento-Chamba & Maldonado-Ruiz	2024	Analyze the growing problem of computer crimes in Ecuador, evaluating its impact from economic, psychological and social perspectives.	Detailed qualitative analysis of current legislation.	A widespread lack of knowledge about the illegality of certain behaviors, such as the violation of privacy and the manipulation of mobile IDs, is revealed, which has led to serious consequences, including cases of suicide. The	In conclusion, a call is made to strengthen education and awareness about these crimes, while promoting more effective measures to prevent and punish these behaviors, thus guaranteeing the protection of digital rights in

				urgent need to reform the Comprehensive Organic Penal Code (COIP) is pointed out, given that the current sanctions are disproportionate and lack adequate economic components.	Ecuadorian society.
Cuenca y Núñez	2024	Comparatively analyze the types of computer crimes recorded between 2018 and 2021.	Document analysis on computer crimes and their impact on legal security.	The research provides valuable data that can contribute to the prevention of cybercrime, including a quantitative description of the types of computer crimes recorded between 2018 and 2021. Based on the comparative analysis of the information collected, the most common computer crimes have been identified, providing a key information base to face this growing challenge.	The study highlights the need to strengthen education and awareness about the importance of computer security in Ecuador, highlighting the importance of both individuals and organizations adopting preventive measures to protect themselves against this type of crime.
Buch	2024	Determine the relationship between digital literacy and variables related to digital inclusion in a group of master's level students.	Postpositivist paradigm with a quantitative approach, using a non-experimental cross-sectional correlational design. An online survey was applied as a data collection instrument. The sample was made up of 35 university	In the final model, the variables: number of ICT training (less than 40 hours), knowledge about computer crimes, knowledge of security protocols and digital literacy were identified as significant, with a 95% confidence level. The model presented an adjusted	There is a direct relationship between digital literacy and digital inclusion. The coefficient of 0.152 was significant at the 5% level, indicating that an increase of one unit in digital literacy generates a proportional increase of 0.152 units in digital inclusion. This

			students selected through voluntary non-probabilistic sampling.	correlation coefficient of 0.673. The average digital inclusion index was 0.46, with 0.48 for women and 0.45 for men.	suggests that higher levels of digital literacy among students are positively associated with higher levels of digital inclusion.
Valverde-Ramos et al.	2024	Respond if it is necessary to include the crime of pornographic deepfake as a specific criminal type in the special part of the Comprehensive Organic Penal Code (COIP) of Ecuador, to strengthen citizen security based on the principles of legality and typicality.	From the qualitative approach, methods such as logical, exegetical, comparative, bibliographic review, case analysis and hypothetical-deductive methods were used.	The results indicate that this emerging criminal modality requires an effective legal response that not only punishes those responsible, but also repairs the serious consequences derived from these acts and prevents future violations.	The urgent need to classify pornographic deepfakes as a specific crime in Ecuadorian legislation is evident, providing authorities with robust legal tools to confront this form of digital sexual violence.
Avila and Rincón	2023	Develop a strategy so that the aspiring patrol officers of the Rafael Reyes Police School could acquire knowledge and adopt good practices aimed at preventing damage from computer crimes, such as phishing, vishing, smishing, impersonation or fraud.	Mixed approach, combining qualitative and quantitative elements. It began with a survey applied to 220 students of the professional technician in police service, identifying the most frequent computer crimes that affect the academic community.	The results of the study highlight the importance of educational institutions, especially those focused on police training, to prioritize cybersecurity and include it in their curricula, incorporating topics on prevention and digital care.	Based on these findings, a mobile application was designed for applicants, which includes information on computer crimes, protection measures, online tools and guides for making complaints.
Gomero-Cuadra and Sánchez-Calle	2024	Evaluate the cybersecurity practices implemented in the Occupational	A cross-sectional descriptive study was conducted in 11 SAMOs, using a questionnaire	The results reveal that the majority of SAMOs surveyed have contingency plans for cyber	The findings of this study underscore the importance of strengthening cybersecurity in SAMOs to protect

		Physician Support Services (SAMO) that provide services to a major construction project in Metropolitan Lima.	designed to evaluate the information security measures implemented in each institution.	incidents, perform regular backups and keep their operating systems updated. However, opportunities for improvement were identified in the implementation of some security measures.	the confidentiality and integrity of medical information. It is recommended to implement proactive security measures, such as conducting risk assessments and training staff.
López-Pincay et al.	2024	Analyze the various control strategies implemented to mitigate the risks associated with this type of crime.	Comprehensive qualitative literature review.	The results show that while sophisticated cybersecurity systems have been developed, the changing nature of cybercrime poses constant challenges.	It is concluded that an effective response requires multidisciplinary collaboration and the adoption of proactive measures to protect the financial infrastructure.
Arapa et al.	2024	Describe the current situation of cybercrime in the city of Puno, identifying its underlying causes and consequences.	Quantitative, explanatory and descriptive research.	The results show that lack of awareness and vulnerabilities in computer systems expose an increasing number of people, especially those between 27 and 59 years old, to risks such as identity theft, fraud and extortion.	Factors such as misinformation, the sophistication of attack techniques and deficiencies in computer security have been found to be the main drivers of this phenomenon, disproportionately affecting a specific segment of the population.
Jimenez	2023	Analyze the risks that legal assets face when Internet providers do not implement preventive mechanisms, such as artificial intelligence systems, to combat these threats.	Bibliographic literature review.	Although the Peruvian State has established standards to punish computer crimes, a lack of specific regulation for its prevention is evident, in contrast to countries like Germany.	The study concludes that self-regulation and compliance measures are appropriate strategies to control digital platforms as possible sources of danger. Likewise, it is proposed to the Peruvian legislator to establish a regulation that forces service providers to monitor their

					platforms to prevent the violation of legal rights in cyberspace.

Source: Own elaboration

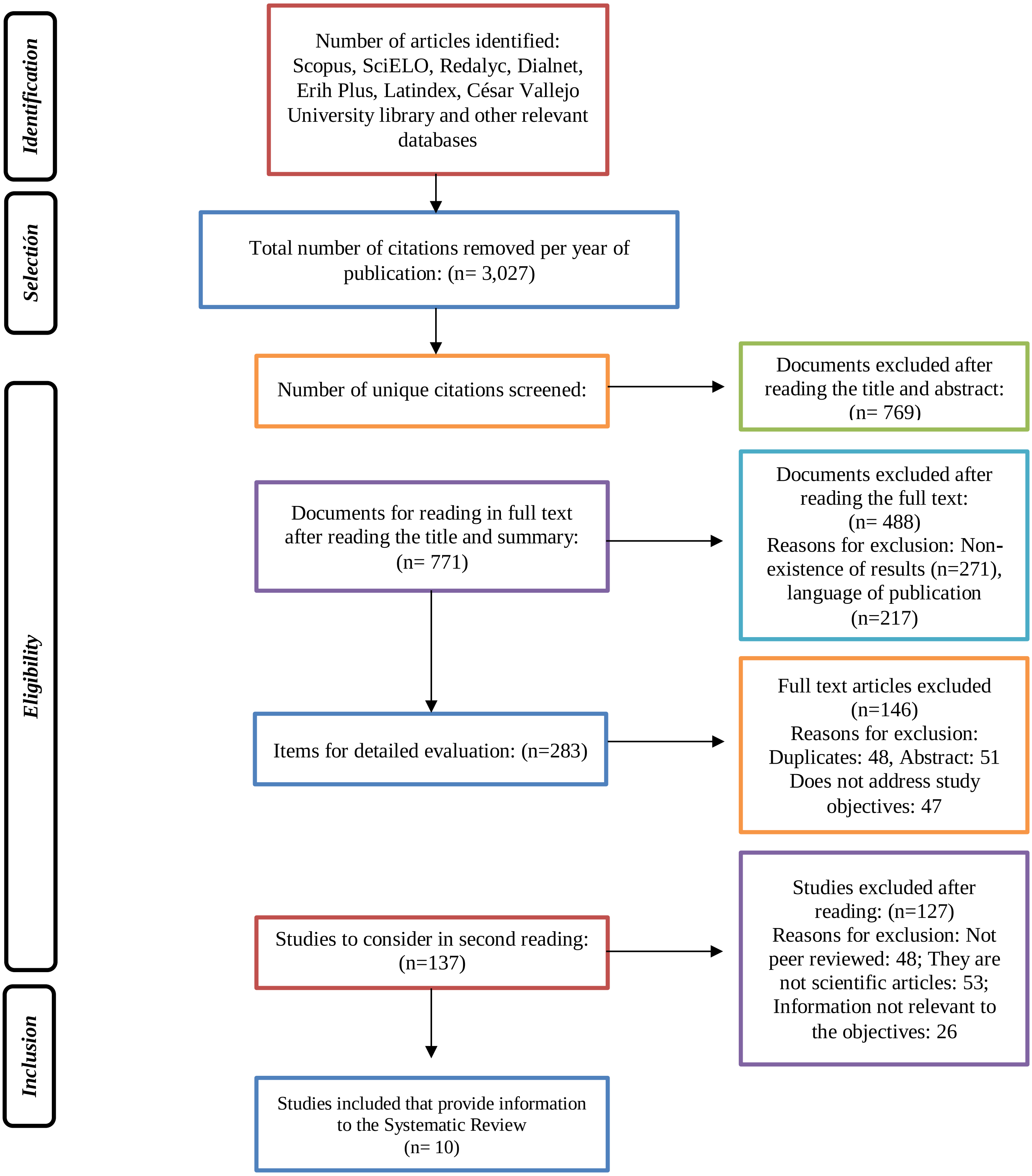
Identification
Selectión
Eligibility
Inclusion
Number of articles identified: Scopus, SciELO, Redalyc, Dialnet, Erih Plus, Latindex, César Vallejo University library and other relevant databases
Total number of citations removed per year of publication: (n= 3,027)
Number of unique citations screened:
Documents excluded after reading the title and abstract: (n= 769)
Documents for reading in full text after reading the title and summary: (n= 771)
Documents excluded after reading the full text: (n= 488) Reasons for exclusion: Non-existence of results (n=271), language of publication (n=217)
Items for detailed evaluation: (n=283)
Full text articles excluded (n=146) Reasons for exclusion: Duplicates: 48, Abstract: 51 Does not address study objectives: 47
Studies to consider in second reading: (n=137)
Studies excluded after reading: (n=127) Reasons for exclusion: Not peer reviewed: 48; They are not scientific articles: 53; Information not relevant to the objectives: 26
Studies included that provide information to the Systematic Review (n= 10)

Figure 1. Search Diagram

Source: Own elaboration

The literature review reveals a complex and constantly evolving landscape surrounding cybercrime. Several key themes emerge from the studies reviewed. To begin with, the growing reliance on digital technologies has created an environment conducive to the proliferation of cybercrime (Valencia-Sandoval et al., 2022). As evidenced by the studies presented in Table 1, cyberattacks have become more sophisticated, affecting individuals, organizations, and governments alike.

It is also evident from the studies reviewed that cybercrime has far-reaching consequences, affecting individuals, organizations, and societies in general (Martínez et al., 2024). Therefore, financial losses, reputational damage, and social disruption are some of the most significant impacts. In addition, cyberattacks can compromise critical infrastructure and national security.

López-Pincay et al. (2024) notes that, to effectively combat cybercrime, a multifaceted approach is required that involves collaboration between governments, law enforcement agencies, the private sector and international organizations. This includes strengthening legal frameworks, improving cybersecurity measures, raising public awareness and fostering international cooperation.

According to Saltos et al., (2021) cited in the introduction of this article, technological advances can be used to both facilitate and combat cybercrime. Therefore, the development of sophisticated cybersecurity tools and techniques is essential to protect against cyberattacks. However, it is also important to address the ethical implications of these technologies and ensure that they are used for beneficial purposes. Hence, it is necessary to educate people and organizations about cyber threats and best practices in cybersecurity (Orosco-Fabian, 2024). Because by increasing awareness, individuals can protect themselves from becoming victims of cybercrime.

Conclusions

Based on the extensive literature review and discussion of results that has been conducted, solid conclusions can be drawn to respond to the general and specific objectives of this research. To begin with, the increasing dependence on digital technologies has made cybercrime an omnipresent threat, affecting individuals, organizations and governments around the world. Therefore, combating cybercrime requires the collaboration of various actors, such as governments, companies, academia and civil society, to develop comprehensive strategies that address legal, technological and social challenges.

In addition, the most common cybercrimes identified in the literature include computer fraud, cyberbullying, computer sabotage and identity theft. On the other hand, in response to the second specific objective, a growing interest in cybercrime research has been observed worldwide, with a significant number of studies published in recent years.

The final conclusion of this systematic review is that the main challenges include the rapid evolution of technologies, the cross-border nature of cybercrime, lack of resources and the difficulty of identifying and capturing cybercriminals. Cybercrime represents a growing and complex threat that requires a coordinated response at a global level. By understanding current trends, challenges and best practices, we can develop more effective strategies to protect individuals and organizations from cyberattacks.

Recommendations call for measures such as strengthening international cooperation, investing in research and development of security technologies, improving user education and awareness, and updating legislation to address new forms of cybercrime. Specific case studies of cyberattacks are also encouraged to identify the tactics, techniques and procedures used by cybercriminals.

ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i8.5276

References

Acosta, M., Benavides, M., & García, N. (2020). Computer crimes: Organizational impunity and its complexity in the business world. Revista Venezolana De Gerencia, 25(89), 351-368. https://doi.org/10.37960/revista.v25i89.31534

Arapa, J., Cari, K., Laura, J., Laura, M., Merma, R., Tarapa, H., & Condori, N. (2024). Causes and Consequences of the Increase in Cybercrime in the City of Puno 2023. Revista de Derecho, 9(1). https://doi.org/10.47712/rd.2024.v9i1.262

Avila, F., & Rincón, P. (2023). Inclusion of training in prevention and attention to computer crimes in police education. Revista Educación, 47(2), 1–28. https://doi.org/10.15517/revedu.v47i2.53905

Buch, I. (2024). Deciphering digital inclusion: exploring its relationship with digital literacy and other related variables. Revista Científica Internacional, 7(1), 269–286. https://doi.org/10.46734/revcientifica.v7i1.96

Cuenca, A. & Núñez, J. (2024). Documentary analysis: impact of legal security in computer crime. LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades, 5(4), 2541 – 2551. https://doi.org/10.56712/latam.v5i4.2437

Domínguez, R. & Vera, R. (2022). Spatial analysis of cyber fraud in electronic commerce: considerations on the Tamaulipeca political agenda. PODIUM, (41), 21–40. https://doi.org/10.31095/podium.2022.41.2

Echeverría, S., & Nivela, M. (2024). Comprehensive analysis of key technologies in Industry 4.0. Polo del Conocimiento, 9(8), 945-965. https://doi.org/10.23857/pc.v9i8.7736

Eslava-Zapata, R., Rojas-Hermida, C. J., & García-Peñaloza, J. E. (2024). Variables associated with computer crimes in Latin America. Revista Academia & Derecho, 15(28), 1-21. https://doi.org/10.18041/2215-8944/academia.28.11822

Gomero-Cuadra, R. & Sánchez-Calle, D. (2024). Cybersecurity in support services for the occupational doctor in the city of Lima. Pilot study. Revista Médica Herediana, 35 (1), 38-43. https://doi.org/10.20453/rmh.v35i1.5298

González, M. (2024). Methods: search system, levels of evidence, degree of recommendation. In: Bajares de Lilue M, González Blanco M, Pizzi La Veglia R, editors. Consensus: Hormonal contraception. Rev Obstet Ginecol Venez. 84(1), 1-4. https://doi.org/10.51288/0084S101

Guaña Moya, J. (2023). Cybersecurity revolution in the fourth industrial revolution. Revista Ingeniería E Innovación Del Futuro, 2(2), 6–20. https://doi.org/10.62465/riif.v2n2.2023.11

Jimenez, L. (2023). The current state of cybercrime in Peru and German law. Boletín mexicano de derecho comparado, 56(167), 197-219. https://doi.org/10.22201/iij.24484873e.2023.167.18367

Juca, F., & Medina, R. (2023). Cybercrimes in Ecuador and its social impact; current panorama and future perspectives. Portal De La Ciencia, 4(3), 325–337. https://doi.org/10.51247/pdlc.v4i3.394

López-Pincay, P., Mendoza-Lino, K., Yagual-Tomalá, E., & Blum-Alcívar, H. (2024). Control mechanisms to prevent the increase in financial cybercrime. MQRInvestigar, 8(3), 1802–1818. https://doi.org/10.56048/MQR20225.8.3.2024.1802-1818

Martínez, Y., Cerezo, J., y Quirós, A. (2024). How does cybercrime affect companies and banking institutions in Panama? Revista Semilla Científica, (5), 196–210. https://doi.org/10.37594/sc.v1i5.1380

Ordóñez, L. (2024). The Legal Framework of Cybercrimes in Ecuador. Reincisol., 3(5), 1447–1469. https://doi.org/10.59282/reincisol.V3(5)1447-1469

Orosco-Fabian, J. (2024). Cybersecurity in higher education: a bibliometric review. Revista Digital de Investigación en Docencia Universitaria, 18(2), e1933. https://doi.org/10.19083/ridu.2024.1933

Ponce, M. (2024). Computer crimes: Ecuador Case. Revista San Gregorio, 1(58), 119-123. http://dx.doi.org/10.36097/rsan.v1i58.2667

Rodríguez, H., & Moreno, C. (2024). Information security and cybersecurity: its importance for States, companies and people, a systematic review. Estudios y Perspectivas Revista Científica y Académica, 4(1), 159–178. https://doi.org/10.61384/r.c.a.v4i1.90

Saltos, M., Robalino, J., & Pazmiño, L. (2021). Conceptual analysis of computer crime in Ecuador. Conrado, 17(78), 343-351. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1990-86442021000100343&lng=es&tlng=es

Sánchez-Serrano, S., Pedraza-Navarro, I., & Donoso-González, M. (2022). How to do a systematic review following the PRISMA protocol? Fundamental uses and strategies for their application in the educational field through a practical case. Bordón. Revista de Pedagogía, 74(3), 51–66. https://doi.org/10.13042/Bordon.2022.95090

Valencia-Sandoval, K., Sánchez-Leyva, J., & Duana-Avila, D. (2022). Cyber Dependency and Competitiveness. Investigación administrativa, 51(129), 00009. https://doi.org/10.35426/iav51n129.09

Sarmiento-Chamba, J., & Maldonado-Ruiz, L. (2024). Computer crimes and cyber attacks: legal analysis in the criminal law of Ecuador. MQRInvestigar, 8(3), 1753–1781. https://doi.org/10.56048/MQR20225.8.3.2024.1753-1781

United Nations Office on Drugs and Crime. (2013). Comprehensive study on cybercrime. https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Spanish.pdf

Valverde-Ramos, M., Armijos-González, M., & Martínez-Pérez, O. (2024). The classification of the Pornographic Deepfake crime in Ecuador and the era of artificial intelligence. MQRInvestigar, 8(2), 1950–1970. https://doi.org/10.56048/MQR20225.8.2.2024.1950-1970.