Current cybersecurity landscape: threats, legislation, and structural gaps from a systematic review

Panorama actual de la ciberseguridad: amenazas, legislación y brechas estructurales desde una revisión sistemática

Néstor Torres Gamarra
https://orcid.org/0009-0007-5406-5482
ntorresg@ucsm.edu.pe
Universidad Católica de Santa María
Arequipa-Peru

Manuel Zúñiga Carnero
https://orcid.org/0000-0002-1091-9438
mzuñigac@ucsm.edu.pe
Universidad Católica de Santa María
Arequipa-Peru

REVISTA INVECOM ISSN: 2739-0063

Received: 05-03-2025 Accepted: 02-06-2025

2026. V6. N 1.

Abstract

Cybersecurity in Peru represents a growing strategic challenge, driven by the constant increase in digital attacks, the rapid digitalization of productive sectors, and existing regulatory gaps. In this context, this study examines the current landscape through a systematic review of scientific literature published between 2020 and 2024, based on Scopus and a historical-logical approach. To this end, 24 studies were selected that address aspects such as the most common types of cyberattacks, the level of cybersecurity maturity, current legislation, business investment, technological advances, and the specialized labor market. The findings indicate that the country faces a high volume of attacks, primarily phishing and electronic fraud, which generate growing economic losses and limit response capacity. Furthermore, it was evident that Peru is in an early stage of the Cybersecurity Capability Maturity Model (CMM), with outdated legislation and poor institutional coordination. Although investment in cybersecurity has increased, a critical shortage of specialized talent persists, affecting the effectiveness of digital defense policies. Therefore, it is essential to design a comprehensive national strategy that strengthens the regulatory framework, promotes specialized technical training, and fosters multisectoral cooperation. Only then will it be possible to resiliently confront the complex ecosystem of digital threats affecting the country.

Keywords: digital divide, cybersecurity, institutional maturity.

Resumen

La ciberseguridad en el Perú representa un desafío estratégico creciente, impulsado por el aumento constante de ataques digitales, la rápida digitalización de los sectores productivos y las brechas normativas existentes. En este contexto, este estudio examina el panorama actual mediante una revisión sistemática de literatura científica publicada entre 2020 y 2024, con base en Scopus y un enfoque histórico-lógico. Para ello, se seleccionaron 24 estudios que abordan aspectos como los tipos de ciberataques más comunes, el nivel de madurez en ciberseguridad, la legislación vigente, la inversión empresarial, los avances tecnológicos y el mercado laboral especializado. Los hallazgos indican que el país enfrenta un alto volumen de ataques, principalmente *phishing* y fraude electrónico, que generan pérdidas económicas crecientes y limitan la capacidad de respuesta. Además, se evidenció que Perú se encuentra en una etapa inicial del Modelo de Madurez de Capacidades en Ciberseguridad (CMM), con una legislación desactualizada y baja coordinación institucional. Aunque la inversión en ciberseguridad ha aumentado, persiste una escasez crítica de talento especializado, lo que afecta la eficacia de las políticas de defensa digital. Por ello, es fundamental diseñar una estrategia nacional integral que fortalezca el marco normativo, impulse la formación técnica especializada y fomente la cooperación multisectorial. Solo así será posible enfrentar con resiliencia el complejo ecosistema de amenazas digitales que afecta al país.

Palabras clave: brecha digital, ciberseguridad, madurez institucional.

Introduction

The increasing digitalization of productive, governmental, and social processes has significantly expanded the exposure to cyber risks, positioning cybersecurity as a strategic priority at a global level. In this regard, Peru faces important challenges that threaten its digital stability, critical infrastructure, and technological sovereignty. Although there has been a decrease in attack attempts—from 15 billion in 2022 to 5 billion in 2023—the economic losses associated with cybercrime reached S/ 40 million (BCRP, 2024; Forbes, 2024), indicating that the sophistication of threats surpasses the defensive advancements implemented.

Moreover, the country is still in the formative stage of the Cybersecurity Capability Maturity Model (CMM), ranking below the regional standard (Martín, 2023). This situation is exacerbated by outdated legislation that is poorly aligned with the emerging risks of the digital environment. While there are regulations such as the Personal Data Protection Law (Law No. 29733) and the Computer Crimes Law (Law No. 30096), both have lagged behind the rapid innovation of threats (Congress of the Republic, 2021; 2023). Additionally, the limited implementation of the National Cybersecurity Policy, approved in 2017, hampers effective coordination among the public, private, and academic sectors (Presidencia del Consejo de Ministros, 2017).

On another note, the talent gap in the labor market is alarming. The demand for professionals in information technology, cybersecurity, and artificial intelligence has grown by 50% to 60% in the last three years (ProInnóvate, 2024), yet the supply remains insufficient to meet the needs of companies, public entities, and expanding digital platforms. This shortage leads to unfilled vacancies, team overload, and increased vulnerability to targeted attacks (OEA, 2023; Towhidi, 2023). Sectors such as transportation, health, and logistics have been particularly compromised due to their high dependency on interconnected systems (Bermúdez & Cano, 2023; Cervera & Alyson, 2024).

Simultaneously, the adoption of emerging technologies—such as the Internet of Things (IoT), cloud computing, and artificial intelligence systems—presents both opportunities and risks. Recent studies warn that, without proper governance and effective protection mechanisms, these technologies expand attack vectors and increase exposure to security incidents (Ortiz, 2023; Reyes, 2023). Therefore, managing these challenges requires more flexible regulatory frameworks, greater investment in infrastructure and control mechanisms, as well as continuous training of human capital. Although investment in cybersecurity in Peru has grown from 3% to 10% in recent years (Calderón, 2020), it remains insufficient compared to the average costs per attack, which can range from $13,000 to over $5 million (Gómez, 2023).

This scenario is situated within a regional reality marked by normative asymmetries and structural weaknesses. Compared to countries like the United States or Canada, which have consolidated active policies for cyber diplomacy and strategic alliances (Aguilar, 2024), Peru still relies heavily on international providers and lacks a robust national cyber defense model (Amasifuen, 2024). Thus, it is urgent to adopt a holistic and intersectoral approach that strengthens local capacities, promotes regulatory innovation, encourages multi-level cooperation, and articulates sustainable efforts for digital literacy.

In this context, the present study aims to analyze the current state of cybersecurity in Peru, considering the most frequent types of attacks, associated costs, institutional maturity levels, current legislation, technological trends, and labor market dynamics. To achieve this, a systematic review of academic and technical literature published between 2020 and 2024 is employed, selected from the Scopus database. The findings are expected to contribute to identifying the main structural gaps in the country and proposing strategic guidelines that reinforce its cybersecurity resilience in an increasingly complex and hostile global environment.

Methodology

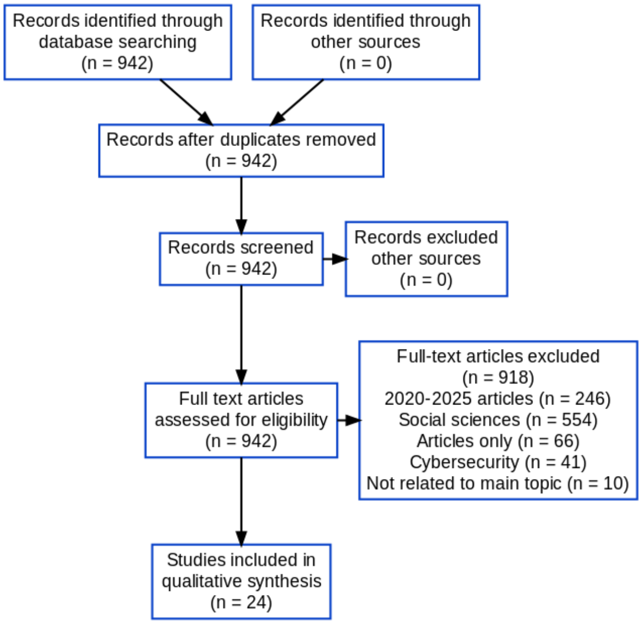
This study adopted a methodological approach based on a systematic literature review to rigorously examine the current state of cybersecurity in Peru between 2010 and 2024. The historical-logical method served as the analytical framework, allowing for the tracking of the evolution of policies, practices, trends, and challenges related to digital security in the national context.

In this process, the bibliographic search strategy was conducted in high-impact scientific databases, like Scopus, selected for their academic robustness and thematic relevance. The search equation was designed to maximize the relevance and accuracy of results, combining Boolean operators and key terms related to cybersecurity, such as: (*TITLE-ABS-KEY* ("*cybersecurity*" *OR* "*information security*" *OR* "*cyber resilience*" *OR* "*digital resilience*" *OR* "*resilience*")) *AND* (*TITLE-ABS-KEY* ("*cyber attacks*" *OR* "*cyber threats*" *OR* "*security incidents*" *OR* "*data breaches*" *OR* "*malware*" *OR* "*phishing*" *OR* "*ransomware*")) *AND* (*TITLE-ABS-KEY* ("*policy*" *OR* "*regulation*" *OR* "*law*" *OR* "*governance*" *OR* "*legal framework*" *OR* "*compliance*" *OR* "*normative framework*")) *AND* (*TITLE-ABS-KEY* ("*capacity building*" *OR* "*training*" *OR* "*skills development*" *OR* "*capabilities*" *OR* "*education*" *OR* "*awareness*")).

This advanced search, applied in the fields of title, abstract, and keywords (TITLE-ABS-KEY), allowed for the identification of relevant and updated articles addressing technical, regulatory, and training aspects of cybersecurity. Furthermore, the equation was iteratively refined to avoid irrelevant results and ensure adequate coverage of the phenomenon from a multidimensional perspective.

Figure 1

PRISMA flow diagram showing the article selection process


Records identified through database searching (n = 942)
Records identified through other sources (n = 0)
Records after duplicates removed (n = 942)
Records screened (n = 942)
Records excluded other sources (n = 0)
Full text articles assessed for eligibility (n = 942)
Full-text articles excluded (n = 918)
2020-2025 articles (n = 246)
Social sciences (n = 554)
Articles only (n = 66)
Cybersecurity (n = 41)
Not related to main topic (n = 10)
Studies included in qualitative synthesis (n = 24)

Note. Content generated from https://hollyhartman.shinyapps.io/PRISMAFlowDiagram/

The initial identification process yielded a total of 942 records after duplicate removal, with no additional sources found through other means. Subsequently, all records underwent a rigorous screening process, wherein titles, abstracts, and keywords were evaluated, retaining only those aligned with the study's objectives. Clearly defined inclusion criteria were applied: only studies in Spanish and English published between 2010 and 2024 that explicitly addressed topics related to cybersecurity, cyberattacks, legislation, costs, technological trends, or labor market dynamics were considered.

Following this, the full texts of the 942 articles were evaluated for their eligibility. From this set, 918 studies were excluded for various reasons: 246 did not meet the established temporal range (2020–2025), 554 belonged to the social sciences field without direct connection to cybersecurity, 66 were incomplete or not peer-reviewed articles, 41 lacked substantive contributions to the specific topic, and 10 had no relation to the central axis of the study. As a result of this systematic selection process, 24 studies were included in the final qualitative synthesis.

Data extraction and organization were carried out using thematic analysis and narrative synthesis techniques. Each study's addressed dimensions were examined in detail, including types of cyberattacks, current legal frameworks, institutional maturity levels, investment patterns, advancements in emerging technologies, and labor market gaps. This systematization allowed for the construction of a comprehensive, critical, and contextualized view of the challenges and opportunities Peru faces in cybersecurity, laying the groundwork for future research and strategic recommendations.

Results

As the digital environment gains prominence across all productive sectors, cybersecurity has solidified itself as a fundamental strategic axis within public policies and business development in Peru. However, various reports indicate that in 2023, the country was the target of over 5 billion cyberattack attempts—an alarming figure that reflects both the increasing sophistication of threats and the urgent need to strengthen protection systems (Forbes, 2024; PNP, 2024). According to the BCRP Report (2024), economic losses resulting from these cybercrimes reach multimillion-dollar figures, affecting companies that can incur losses ranging from $13,000 to over $5 million per incident, as highlighted by Gómez (2023).

Despite these concerning indicators, regulatory and technical delays persist in implementing a comprehensive national cybersecurity policy (Presidencia del Consejo de Ministros, 2017; Amasifuen, 2024), contrasting with advancements observed in neighboring countries or strategic allies such as the United States and Canada (Aguilar, 2024).

The global landscape demonstrates an urgent need for multilateral cooperation and regulatory harmonization in cybersecurity matters. In North America, for instance, a more cohesive regulatory ecosystem has emerged, facilitating system interoperability and intelligence sharing in the face of emerging threats (Aguilar, 2024). Meanwhile, in Peru, the legal framework has been strengthened in a fragmented manner, with regulations such as the Personal Data Protection Law (Congreso de la República, 2021) and the Computer Crimes Law (Congreso de la República, 2023). While these represent progress, they do not sufficiently align with the challenges posed by the current digital environment. As Bravo (2024) and Martín (2023) emphasize, the country still relies on a predominantly reactive response to cyberattacks, a situation also documented by Optiv (2019), which notes that many companies find themselves trapped in a cycle of response rather than prevention. This lack of anticipation is exacerbated by insufficient sustained investment in technology, infrastructure, and specialized human talent (Calderón, 2020; ProInnóvate, 2024).

In light of this context, various studies concur on the urgency to transition toward proactive and adaptive models of digital risk management. The use of endpoint protection platforms, as described by Evgeny et al. (2023), along with the implementation of technological governance frameworks in strategic sectors such as health (Cervera & Alyson, 2024), transportation (Bermúdez & Cano, 2023), and higher education (Towhidi, 2023), are emerging as essential components of a coherent national strategy. Additionally, developing capabilities in machine learning for threat detection (Reyes et al., 2023) and analyzing IoT architectures (Ausecha et al., 2022) opens up new possibilities for enhancing digital resilience. The OEA (2023) warns of the shortage of trained cybersecurity professionals in the region, necessitating an inter-institutional commitment to talent training, while authors like Sánchez (2022) and Tapia (2021) emphasize that the phenomenon must also be addressed from a sociocultural and rights-based perspective. Thus, cybersecurity involves not only technological improvement but also a structural, ethical, and educational transformation that ensures a protected and aware digital citizenry.

Peru has established itself as one of the primary targets of cyberattacks in Latin America. Although the number of intrusion attempts has decreased compared to the previous year, the figures remain alarming and continue to generate significant economic losses. In this context, modalities such as phishing, electronic fraud, and identity theft—which together represent over 80% of economic-related cybercrimes—highlight the sophistication and frequency of these threats.

This situation is exacerbated by the structural weaknesses of the Peruvian digital ecosystem, including legislative gaps, obsolete technological infrastructures, and a limited capacity to respond to attacks targeting critical sectors like transportation, health, and logistics. Indeed, the country is still in the formative stage of the Cybersecurity Capability Maturity Model (CMM), reflecting a restricted institutional capacity to effectively tackle cyber risks.

Furthermore, this condition not only generates operational vulnerabilities but also reveals a disconnect between current regulations and the dynamic nature of the digital environment. While key laws related to data protection and computer crimes have been enacted, their scope is insufficient given the rapid technological evolution and the constant emergence of new attack vectors. On the other hand, although corporate investment in cybersecurity has shown progressive growth, it still fails to compensate for deficiencies in digital governance or close the risk gap threatening the sustainability of national critical systems.

One of the most pressing challenges facing Peru is the shortage of specialized cybersecurity talent. Despite the demand for professionals in this area increasing by 50% to 60% in recent years, organizations continue to face significant difficulties in filling strategic vacancies. This disparity between supply and demand results in an overload on technical teams and weakens the country's ability to implement effective preventive policies.

Moreover, factors such as accelerated digitalization, the proliferation of the Internet of Things (IoT), and the mass adoption of cloud services increase the complexity of threats, necessitating a highly skilled professional workforce. Therefore, without a coordinated strategy among the government, academia, and industry to strengthen human capital, Peru risks further entrenching its structural vulnerability in an increasingly hostile digital ecosystem.

Table 1
Systematization of articles on cybersecurity

Author and Year	Theme	Findings
Dumchikov et al. (2025)	Use of artificial intelligence in cybercrime	AI represents a growing risk in cybercrime but is also a useful tool for digital forensic investigation; highlights the need for ethical and legal frameworks.
Mahyoub et al. (2025)	Cybersecurity in the remote work model (WFA)	Lack of training in cybersecurity and communication strategies in the WFA model; recommendations proposed to mitigate cyber risks.
Lukáč et al. (2025)	Socioeconomic factors in digital literacy and security	Educational level and access to resources are linked to response capacity against digital threats; differentiated educational programs proposed.
Serini (2024)	Situational cyber awareness in the European Union	Cybersecurity information exchange faces legal obstacles; greater institutional cooperation and protection of sensitive data required.
Chidukwani et al. (2024)	Cybersecurity in small and medium enterprises (SMBs)	Budget constraints and limited knowledge hinder cybersecurity in SMBs; Google is the most used source but is unreliable for these needs.
Zanke et al. (2024)	Organizational culture in information security	A mixed approach reveals deficiencies in communication and training on security; validates the usefulness of qualitative methods in organizational diagnosis.
Orosco-Fabian (2024)	Cybersecurity in higher education	Sustained increase in studies on educational cybersecurity since 2003; central topics include GDPR, cyber threats, and cybersecurity awareness.
Ricci et al. (2024)	Gaps in cybersecurity education in Europe	Lack of social awareness and certifications at the EU level limits training effectiveness; strategies proposed to adapt to each country.
Koolen et al. (2024)	Technical and organizational measures based on maturity models	Proposes using maturity models to evaluate 'appropriate' security measures according to GDPR; aims to shift from technical understanding to legal compliance.

Houichi et al. (2024)	Cyber threats in smart cities	Smart cities face complex threats due to technological dependency; specific countermeasures proposed for sectors such as health, mobility, and smart governance.
Nastjuk et al. (2024)	Security policy training for employees	The use of deterrence arguments improves learning retention and compliance with security policies among employees, with sustained effects over time.
Song & Park (2024)	Cost-benefit simulation for cybersecurity policies in SMEs	Tax incentives are more effective than regulation for strengthening cybersecurity resilience in SMEs; proposes a dynamic model with government scenarios.
Dodge et al. (2023)	User motivation to adopt cybersecurity practices	Perceived cost, self-efficacy, and threat severity influence user intention to adopt cybersecurity practices; personalized approaches recommended.
Rawindaran et al. (2023)	Cybersecurity in SMEs in Wales and relation with government	SMEs collaborate with the government to overcome cybersecurity challenges; study highlights financial barriers and lack of trained personnel as central issues.
Tok & Chattopadhyay (2023)	Cybercrime and forensic opportunities in smart cities	Proposes STRIDE threat model for investigating digital crimes in urban infrastructures; emphasizes the need for forensic capabilities and international cooperation.
Alsharida et al. (2023)	Human behavior regarding cybersecurity	Systematic review shows dominance of theories like PMT and TPB; identifies methodological gaps and emphasizes the role of students and social networks in studying behavior.
Smikle (2023)	Cybersecurity in Jamaica's financial sector	Cybersecurity is a national policy issue; Jamaica requires greater capacity to respond to financial cyberattacks and specific legislation.
Alhumud et al. (2023)	Cybersecurity performance assessment in Saudi universities	Universities show partial compliance with cybersecurity regulations; weaknesses identified in policies, training, and ongoing monitoring.
Wong et al. (2022)	Awareness of cybersecurity policies and compliance in employees	Awareness of policies and cybersecurity hygiene among staff impacts response capability to cyberattacks in SMEs; highlights the importance of a preventive approach.
Pravdiuk (2022)	Legal regulation of cybersecurity in Ukraine	Ukrainian legislation shows advances and limitations in national cyberspace protection; emphasizes the need for coordination among public, private, and civil society sectors.
Mat et al. (2022)	Emerging cybersecurity challenges	Cyber resilience measures in Malaysia are limited by a lack of experts, fragmented legislation, and poor public-private collaboration; highlights the urgency of improving cybersecurity education.
Zhang et al. (2022)	Threats from open information in critical infrastructure	The use of OSINT allows malicious actors to access sensitive data from critical infrastructure; recommends greater control over public information and awareness programs.
Gibbs (2020)	Economic cybersecurity in the United Arab Emirates	Despite the legal framework, the human factor remains the greatest vulnerability; education in cybersecurity and public awareness are key for a secure digital culture in the region.

Finally, the analysis of trends and projections reveals a paradigm shift in how organizations approach cybersecurity, highlighting the incorporation of emerging technologies such as artificial intelligence and the Internet of Things. These innovations provide significant advantages, especially in automated threat detection and real-time response capabilities; however, they also considerably expand the attack surface.

Torres Gamarra, N., & Zúñiga Carnero, M. (2026). Current cybersecurity landscape: threats, legislation, and structural gaps from a systematic review. *Revista InveCom, 6*(1). 1-10. https://zenodo.org/records/15605545

Structural challenges persist, such as the complexity in configuring cloud services, the lack of data sovereignty, and vulnerability to human errors. The combination of these factors underscores that digital transformation in Peru cannot be sustained without a robust, transversal, and articulated cybersecurity policy that recognizes both technological risks and human and institutional weaknesses.

Discussion

The systematic analysis of 24 recent studies allows for the identification of key trends in cybersecurity from various perspectives: technological, organizational, legal, and educational. First, one of the most significant findings is the duality of artificial intelligence in cyberspace. On one hand, Dumchikov et al. (2025) and Tok & Chattopadhyay (2023) highlight its use in both criminal activities and forensic investigation processes; on the other hand, Houichi et al. (2024) and Zhang et al. (2022) warn of its contribution to increasing vulnerabilities in smart cities and critical infrastructures. Collectively, these studies agree that technological adoption must be accompanied by adaptive defense capabilities and robust ethical frameworks.

Secondly, cybersecurity in small and medium enterprises (SMEs) emerges as an especially vulnerable area. Research by Chidukwani et al. (2024), Song & Park (2024), Rawindaran et al. (2023), and Wong et al. (2022) shows that factors such as low budgets, limited training, and a lack of a preventive culture negatively impact their digital resilience. In response, the most effective proposals revolve around tax incentives, strengthening staff awareness, and an active government role in post-incident response management.

Moreover, in the educational and organizational realm, the importance of training and culture in cybersecurity is reaffirmed. Zanke et al. (2024), Nastjuk et al. (2024), and Dodge et al. (2023) emphasize that training policies should be aligned with user profiles to achieve sustained impact. Likewise, Orosco-Fabian (2024), Alhumud et al. (2023), and Ricci et al. (2024) raise concerns about the lack of clear international standards in higher education, while Alsharida et al. (2023) stress the need to adapt behavioral theories to new digital contexts.

Regarding legal aspects, studies by Serini (2024), Pravdiuk (2022), Smikle (2023), Mat et al. (2022), and Gibbs (2020) highlight the lack of regulatory articulation and the need for coherence between national and international regulatory frameworks. In this regard, Koolen et al. (2024) propose maturity models that translate legal obligations into sustainable operational actions. This proposal is complemented by the demand for greater coordination between public and private sectors to ensure robust digital governance.

Finally, the role of individual and contextual factors in cybersecurity cannot be underestimated. Lukáč et al. (2025) and Dodge et al. (2023) demonstrate that digital literacy, self-efficacy, and threat perception directly influence the adoption of secure practices. Collectively, the reviewed studies indicate that cybersecurity requires a comprehensive and intersectoral vision that integrates technology, training, regulation, and individual motivation to effectively and equitably address emerging risks.

Conclusions

The reviewed studies demonstrate that cybersecurity is a multidimensional phenomenon that must be approached through integrated and intersectoral strategies. Indeed, digital threats are not confined solely to the technological realm; they also impact legal, educational, social, and organizational dimensions. Therefore, it is essential to strengthen regulatory frameworks, promote digital education, foster resilient organizational cultures, and adapt strategies to various sociotechnical profiles to confront the challenges of a constantly evolving digital environment.

Thus, it is concluded that cybersecurity policies must be based on a coordinated vision among public and private actors, where continuous training, end-user awareness, risk assessment, and context-specific application of emerging technologies occupy a priority place. In an increasingly interconnected world, building strong and inclusive cyber capabilities not only protects digital assets but also ensures sustainability, institutional trust, and the secure development of societies.

References

Aguilar, A. J. M. (2024). Rezago y asimetrías de las política nacional e internacional de ciberseguridad de México frente a Estados Unidos y Canadá: Retos de cooperación para Norteamérica. *Revista Académica del CISAN-UNAM, 19*(1), 38. https://dialnet.unirioja.es/descarga/articulo/9396821.pdf

Alhumud, T. A. A., Omar, A., & Altohami, W. M. A. (2023). An assessment of cybersecurity performance in the Saudi universities: A Total Quality Management approach. *Cogent Education, 10*(2), 2265227. https://doi.org/10.1080/2331186X.2023.2265227

Alsharida, R. A., Al-Rimy, B. A. S., Al-Emran, M., & Zainal, A. (2023). A systematic review of multi-prospects on human cybersecurity behavior. *Technology in Society, 73*, 102258. https://doi.org/10.1016/j.techsoc.2023.102258

Amasifuen, M. G. (2024). La ciberseguridad en el Perú. *El Peruano*.

BCRP. (2024). Informe anual sobre el impacto económico de los delitos cibernéticos en Perú (p. 58). https://www.bcrp.gob.pe/publicaciones/memoria-anual/memoria-2024.html

Bermúdez, C., & Cano, J. J. (2023). Cybersecurity model for the logistics and land transportation sectors. *Infosys, 8*. https://esdegrepositorio.edu.co/handle/20.500.14205/11147

Calderón, J. J. (2020). Crece inversión en seguridad tecnológica en empresas peruanas. *El Peruano*. https://elperuano.pe/noticia/89401-crece-inversion-en-seguridad-tecnologica-en-empresas-peruanas

Cervera, A., & Alyson, G. (2024). Cybersecurity and use of ICT in the health sector. *Atención Primaria, 56*(3). https://pubmed.ncbi.nlm.nih.gov/38219392/

Chidukwani, A., Zander, S., & Koutsakis, P. (2024). Cybersecurity preparedness of small-to-medium businesses: A Western Australia study with broader implications. *Computers & Security, 145*, 104026. https://doi.org/10.1016/j.cose.2024.104026

Congreso de la República del Perú (2021). Ley de Protección de Datos Personales peruana. *El Peruano*. https://www.leyes.congreso.gob.pe/documentos/leyes/29733.pdf

Congreso de la República del Perú (2023). Ley de Delitos Informáticos. *El Peruano*. https://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/C5F98BB564E5CCCF05258316006064AB/$FILE/6_Ley_30096.pdf

Dodge, C. E., Fisk, N., Burruss, G. W., Moule, R. K., & Jaynes, C. M. (2023). What motivates users to adopt cybersecurity practices? A survey experiment assessing protection motivation theory. *Criminology & Public Policy, 22*(4), 849–868. https://doi.org/10.1111/1745-9133.12641

Dumchikov, M., Maletova, O., Mishchenko, T., & Lytvynenko, Y. (2025). Artificial intelligence in cyberspace: Between danger and innovation. *Revista de Direito, Estado e Telecomunicacoes, 17*(1), 117–142. https://doi.org/10.26512/lstr.v17i1.53386

Forbes, S. (2024). El Perú sufrió 5.000 millones de intentos de ciberataques en 2023. *Forbes Perú*. https://forbes.pe/tecnologia/2024-03-25/el-peru-sufrio-5-000-millones-de-intentos-de-ciberataques-en-2023-reporto-fortinet/

Gibbs, T. (2020). Seeking economic cyber security: A Middle Eastern example. *Journal of Money Laundering Control, 23*(2), 493–507. https://www.emerald.com/insight/content/doi/10.1108/jmlc-09-2019-0076/full/html

Gomez, A. (2023). Ciberseguridad: Empresas pueden perder desde US$ 13 mil hasta más de US$ 5 millones por ataque. *El Peruano*. https://elcomercio.pe/tecnologia/ciberseguridad/ciberseguridad-empresas-pueden-perder-desde-us-13-mil-hasta-mas-de-us-5-millones-por-ataque-ciberdelincuencia-malware-phishing-suplantacion-de-identidad-noticia/

Houichi, M., Jaidi, F., & Bouhoula, A. (2024). A comprehensive and in-depth study of the threats faced by smart cities and the countermeasures implemented in their key areas. *Journal of Infrastructure, Policy and Development, 8*(10), 8629. https://systems.enpress-publisher.com/index.php/jipd/article/view/8629

ICEX España Exportación e Inversiones. (2023). Ficha sector: Ciberseguridad en Perú 2023. https://www.icex.es/es/quienes-somos/donde-estamos/red-exterior-de-comercio/PE/documentos-y-estadisticas/estudios-e-informes/visor-de-documentos.ficha-sector--ciberseguridad-en-per%C3%BA-2023.doc065202312

Koolen, C., Wuyts, K., Joosen, W., & Valcke, P. (2024). From insight to compliance: Appropriate technical and organisational security measures through the lens of cybersecurity maturity models. *Computer Law & Security Review, 52*, 105914. https://doi.org/10.1016/j.clsr.2023.105914

Lukáč, J., Kudlová, Z., Kopčáková, J., & Gallo, P. (2025). Impact of socio-economic factors on digital literacy and security. *TEM Journal, 14*(1), 925–932. https://www.temjournal.com/content/141/TEMJournalFebruary2025_925_932.pdf

Mahyoub, M., Matrawy, A., Isleem, K., & Ibitoye, O. (2025). Cybersecurity challenge analysis of work-from-anywhere (WFA) and recommendations guided by a user study. *IEEE Transactions on Human-Machine Systems*. https://arxiv.org/abs/2409.07567

Martín, M. V. (2023). Ciberseguridad en Perú. (O. E. Comercial, Ed.). *ICEX, 8*.

Mat, B., Pero, S. D. M., Zengeni, K. T., & Fakhrorazi, A. (2022). Towards an understanding of emerging cybersecurity challenges of a small state: A case study of Malaysia. *Tamkang Journal of International Affairs, 25*(3), 45–108. https://doi.org/10.6185/TJIA.V.202201_25(3).0002

Nastjuk, I., Rampold, F., Trang, S., & Benitez, J. (2024). A field experiment on ISP training designs for enhancing employee information security compliance. *European Journal of Information Systems*. https://doi.org/10.1080/0960085X.2024.2359460

OEA (2023). Fuerza laboral de ciberseguridad. Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo. Organización de los Estados Americanos. https://www.oas.org/es/sms/cicte/docs/Reporte_sobre_el_desarrollo_de_la_fuerza_laboral_de_ciberseguridad_en_una_era_de_escasez_de_talento_y_habilidades.pdf

Optiv Security (2019). Empresas atrapadas en un ciclo de respuesta de ciberseguridad continuamente reactivo. *El Economista*. https://www.eleconomista.es/empresas-finanzas/noticias/9731425/02/19/Empresas-atrapadas-en-un-ciclo-de-respuesta-de-ciberseguridad-continuamente-reactivo-segun-un-informe-de-Optiv-Security.html

Orosco-Fabian, J. R. (2024). Cybersecurity in higher education: A bibliometric review. *Revista Digital de Investigación en Docencia Universitaria, 18*(2), e1933. http://www.scielo.org.pe/pdf/ridu/v18n2/2223-2516-ridu-18-02-e1933.pdf

Pravdiuk, A. (2022). The state and current issues of legal regulation of cyber security in Ukraine. *Evropsky Politicky a Pravni Diskurz, 9*(3), 19–28. http://repository.vsau.org/card.php?lang=en&id=31305

Presidencia del Consejo de Ministros (2017). Política Nacional de Ciberseguridad. *Diario El Peruano*. https://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/A36311FB344A1DC7052583160057706D/$FILE/Pol%C3%ADtica_Nacional_de_Ciberseguridad_peru.pdf

ProInnóvate (2024). Los perfiles profesionales tecnológicos más demandados en el Perú. Ministerio de la Producción. https://www.gob.pe/institucion/proinnovate/noticias/913473-los-perfiles-profesionales-tecnologicos-mas-demandados-en-el-peru-desarrolladores-ia-y-ciberseguridad-lideran-la-lista

Rawindaran, N., Jayal, A., Prakash, E., & Hewage, C. (2023). Perspective of small and medium enterprise (SMEs) and their relationship with government in overcoming cybersecurity challenges and barriers in Wales. *International Journal of Information Management Data Insights, 3*(2), 100191. https://doi.org/10.1016/j.jjimei.2023.100191

Reyes, E. (2023). Técnicas de aprendizaje automático para la detección y prevención de amenazas de ciberseguridad. Proyecciones futuras. *Revista Cubana de Ciencias Informáticas, 17*, 15–27. https://rcci.uci.cu/index.php/RCCI

Ricci, S., Parker, S., Jerabek, J., Lendak, I., & Janout, V. (2024). Understanding cybersecurity education gaps in Europe. *IEEE Transactions on Education, 67*(2), 190–201. https://ieeexplore.ieee.org/document/10380620

Sánchez, F. M. (2022). La seguridad en el ciberespacio desde una perspectiva sociocultural. *Revista de Ciencias Sociales, 2*, 243–258.

Serini, F. (2024). Collective cyber situational awareness in EU. A political project of difficult legal realisation? *Computer Law & Security Review, 55*, 106055. https://doi.org/10.1016/j.clsr.2024.106055

Smikle, L. (2023). The impact of cybersecurity on the financial sector in Jamaica. *Journal of Financial Crime, 30*(1), 86–96. https://ideas.repec.org/a/eme/jfcpps/jfc-12-2021-0259.html

Song, J., & Park, M. J. (2024). A system dynamics approach for cost-benefit simulation in designing policies to enhance the cybersecurity resilience of small and medium-sized enterprises. *Information Development*. https://doi.org/10.1177/02666669241252996

Tapia, E., & Canizales, R. (2021). La importancia de la ciberseguridad y los derechos. *Misión Jurídica, 14*(20), 142–158. https://www.revistamisionjuridica.com/wp-content/uploads/2021/06/08-20-La-importancia-de-la-ciberseguridad-y-los-derechos-humanos-en-el-entorno-virtual.pdf

Tok, Y. C., & Chattopadhyay, S. (2023). Identifying threats, cybercrime and digital forensic opportunities in smart city infrastructure via threat modeling. *Forensic Science International: Digital Investigation, 45*, 301540. https://doi.org/10.1016/j.fsidi.2023.301540

Towhidi, G. P. J. (2023). Aligning cybersecurity in higher education with industry. *Journal of Information Systems Education, 34*(1), 70–83. https://jise.org/Volume34/n1/JISE2023v34n1pp70-83.pdf

Wong, L.-W., Lee, V.-H., Tan, G. W.-H., Ooi, K.-B., & Sohal, A. (2022). The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. *International Journal of Information Management, 66*, 102520. https://doi.org/10.1016/j.ijinfomgt.2022.102520

Zanke, A., Weber, T., Dornheim, P., & Engel, M. (2024). Assessing information security culture: A mixed-methods approach to navigating challenges in international corporate IT departments. *Computers & Security, 144*, 103938. https://doi.org/10.1016/j.cose.2024.103938

Zhang, Y., Frank, R., Warkentin, N., & Zakimi, N. (2022). Accessible from the open web: A qualitative analysis of the available open-source information involving cyber security and critical infrastructure. *Journal of Cybersecurity, 8*(1), tyac003. https://doi.org/10.1093/cybsec/tyac003