International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(1s) 2026 pp. 403-419
https://doi.org/10.70917/ijcisim-2026-2525
Article

GOVERNANCE OF GENERATIVE ARTIFICIAL INTELLIGENCE IN HIGHER EDUCATION INSTITUTIONS: AN APPROACH FROM DIGITAL SECURITY AND DATA PROTECTION

Cesar Luis Vásquez Suarez[1], Elvecia Vásquez Suarez[2], María Ospina Figueroa[3]

[1] Universidad de Barranquilla, Barranquilla, Colombia.
Email: cvasquez@unibarranquilla.edu.co
ORCID: 0009-0007-9723-3562
[2] Universidad de Barranquilla, Barranquilla, Colombia.
Email: evasquez@unibarranquilla.edu.co
ORCID: 0009-0000-0373-7161
[3] Universidad de Barranquilla, Barranquilla, Colombia.
Email: mospina@unibarranquilla.edu.co
ORCID: 0009-0007-8394-1760

Abstract: The purpose of this research is to examine how generative artificial intelligence is managed in universities, focusing on digital security and data protection. This is done through an exhaustive review of the literature following the PRISMA protocol. To carry out this study, a thorough search was carried out in the Scopus and Web of Science databases, initially identifying 31 investigations. After eliminating duplicates and applying inclusion and exclusion criteria, 19 scientific articles were selected for further analysis. The findings show that generative AI governance is a new and complicated arena, combining technological, organizational, ethical, and regulatory factors. It was found that the implementation of these technologies in universities has exceeded the capacity of these institutions to create adequate regulations, which entails risks on digital security, data protection and the integrity of academic processes. Fragmentation was also noted in the scientific literature, with limited integration between governance, cybersecurity, and data management approaches, making it difficult to advance in the development of consistent institutional models.

Among the most important findings, it is highlighted that the most significant dangers are linked to the vulnerability of digital systems, the exposure of sensitive information, the lack of transparency in algorithms and the absence of digital skills in the academic community. It was also shown that artificial intelligence can act on two levels, being both a source of risk and a resource to improve information security. Therefore, generative AI governance needs a comprehensive approach that unites technological innovation with cybersecurity tactics, data protection policies, and digital skills training.

In conclusion, the study indicates that higher education institutions must work on creating governance frameworks that are dynamic, adaptable and context-specific, allowing them to balance the adoption of emerging technologies with the safeguarding of information and user rights. Practical implications are also suggested that seek to strengthen institutional capacities, especially in regional contexts such as Latin America, Colombia and Barranquilla, where important challenges persist in the management of artificial intelligence.

Keywords: Generative artificial intelligence, Digital governance, Higher education, Digital security, Data protection, Cybersecurity, Digital transformation.

1. Introduction

The rapid evolution of artificial intelligence (AI), particularly its generative aspect, has significantly impacted educational, research, and administrative environments in universities. Tools such as extensive language models, automatic content creation systems, and deep learning-based structures have facilitated not only the automation of complex cognitive activities, but have also created new spaces for interaction between people and machines. This phenomenon has drastically altered the traditional dynamics of knowledge creation, validation and dissemination, opening doors to innovative opportunities in education. However, at the same time, it has brought with it structural challenges in areas such as regulation, ethics and technological risk management, which forces universities to reconsider their governance frameworks in an environment marked by technological uncertainty and the rapid obsolescence of knowledge.

In education, generative AI has established itself as a revolutionary tool capable of changing teaching and learning methods, especially through the personalization of education, the automation of tutorials and the creation of adaptive content. These technologies allow the specific needs of each student to be more effectively addressed, promoting more inclusive and dynamic learning experiences. However, their integration also raises essential questions about the authenticity of learning, the assessment of academic performance, and authorship. The possibility of students using AI tools to produce academic papers without adequate supervision puts the principles of academic integrity at risk, which has led many institutions to review their internal regulations. In this context, the challenge is not only to incorporate technology, but also to establish mechanisms that regulate its use in a way that is aligned with educational values.

In this context, the governance of artificial intelligence is presented as a crucial aspect to guide the development, implementation and control of these technologies in universities. Governance encompasses more than creating rules, as it involves establishing an institutional ecosystem capable of comprehensively managing the effects of AI. According to Floridi et al. (2018), effective governance must link ethical principles, regulatory frameworks, and supervisory methods that ensure transparency, accountability, and equity in the use of technology. In the university environment, this implies the need to integrate various dimensions – technological, legal, pedagogical and organizational – in a systemic approach that allows innovation to be aligned with the strategic objectives of the institution. In addition, it requires the active participation of various actors, including managers, teachers, students, and technology specialists, in the formulation of institutional policies.

One of the essential elements in the regulation of generative artificial intelligence is cybersecurity, which refers to the ability to safeguard computer systems and institutional information against threats in the digital sphere. The adoption of AI-powered technologies has significantly increased the complexity of technological infrastructures in universities, creating new risks that can be exploited by malicious individuals (Kshetri, 2021). Such risks include AI-assisted social engineering attacks, data manipulation, unauthorized access to systems, and vulnerabilities in digital platforms. Therefore, higher education institutions must adopt cybersecurity strategies that are proactive, as well as reactive, adapting to changes through the integration of technologies for early detection, incident response protocols, and educational programs on digital culture for the entire academic community.

Likewise, the safeguarding of personal information has emerged as a crucial aspect in the debate on the use of generative artificial intelligence, given the heavy reliance on these tools on large volumes of data. The process of training and operating generative models requires access to information that, in many cases, may include sensitive or private data, which generates significant risks related to privacy and legal compliance (Voigt & Von dem Bussche, 2017). In the university environment, where academic, administrative, and research data are handled, the exposure of this information can have severe consequences for both the institution and individuals. For this reason, it is vital that higher education institutions adopt effective data protection policies that align with international standards, implementing anonymization measures, access control, and process auditing.

At the global level, growing concern about the effects of artificial intelligence has led to the creation of regulatory frameworks and recommendations by international organizations. UNESCO (2021) has highlighted the importance of developing ethical artificial intelligence that respects human rights, fosters inclusion, and ensures cultural diversity. Similarly, the OECD (2019) has established principles that seek to promote AI that is trustworthy, underscoring the relevance of transparency, accountability, and safety. These guidelines are critical for higher education institutions, as they provide a conceptual basis for the formulation of governance policies. However, its effective implementation requires a process that is tailored to the specific characteristics of each institution, which poses additional challenges in relation to technical and organizational capacities.

Current scientific research has critically examined the dangers linked to generative AI models, particularly those identified as fundamental models. Bommasani et al. (2021) point out that these systems face difficulties related to the lack of transparency in algorithms, the creation of biases, and the complexity of managing the results they generate. These properties can impact confidence in the information produced, which is especially tricky in educational settings, where accuracy and validity of knowledge are essential. In addition, the reliance of these models on large volumes of data can reinforce pre-existing inequalities, amplifying social and cultural biases unless adequate monitoring mechanisms are in place.

The incorporation of artificial intelligence in higher education institutions also presents considerable organizational challenges that require a profound change in the structures of these institutions. Williamson and Eynon (2020) indicate that universities need to cultivate strategic capabilities to manage the implementation of digital technologies, which includes staff training, process review, and the establishment of new areas of technology management. This change implies a cultural adjustment that transcends the mere addition of tools, demanding an institutional perspective that sees technology as a fundamental element of academic growth. In addition, AI management should include managing technology providers and assessing risks related to reliance on third-party services.

From an ethical approach, generative artificial intelligence presents significant complications linked to equity, justice and responsibility. Mittelstadt et al. (2016) argue that algorithmic systems can replicate and amplify existing biases, producing discriminatory outcomes if they are not properly designed and monitored. In the university environment, this can influence processes such as academic evaluation, student selection or the distribution of resources. For this reason, the governance of artificial intelligence must incorporate ethical principles that guide its application, as well as auditing and accountability mechanisms that allow detecting and correcting possible deviations.

In this framework, the governance of generative artificial intelligence should be considered as part of a broader process of digital transformation in higher education institutions. Selwyn (2019) states that digitalization in education entails a significant restructuring of teaching practices, organizational configurations, and power dynamics within institutions. Therefore, the implementation of artificial intelligence cannot be treated separately, but must be integrated into institutional plans that foster innovation, inclusion and sustainability. This requires a long-term perspective that links technology to the educational and social goals of universities.

The PRISMA methodology used in this study allows for a rigorous, clear and replicable systematic review of the scientific literature. This method helps identify patterns, trends, and gaps in research on generative AI governance, digital security, and data protection (Page et al., 2021). The final selection of 19 relevant studies facilitates an in-depth analysis of the current state of the topic, providing a solid basis for academic debate and the formulation of recommendations.

Therefore, this article aims to examine the governance of generative artificial intelligence in higher education institutions from a comprehensive view that relates digital security and data protection. Based on the available scientific evidence, it seeks to contribute to the creation of conceptual and practical frameworks that guide decision-making within institutions, promoting a responsible, safe and ethical use of artificial intelligence in the educational field.

In Latin America, the integration of artificial intelligence in higher education has shown significant progress, although it also presents major structural challenges linked to digital inequality, insufficient infrastructure, and the lack of solid regulatory frameworks. Cobo (2016) mentions that the region experiences a disparity between the adoption of new technologies and the ability of institutions to manage them properly, which restricts the use of their potential. In addition, recent research indicates that AI regulation in Latin America is still at an early stage, with little synergy between government policies, educational institutions, and ethical frameworks (Aguerre and Galperin, 2021).

In the Colombian scenario, the country has made progress in the creation of policies related to artificial intelligence, as reflected in the CONPES document 3975 of 2019, which proposes a national strategy to promote the development of AI. However, several researchers point out that obstacles persist in the application of these guidelines within the education sector, especially with regard to data protection and cybersecurity (González & Gómez, 2022). Universities in Colombia are going through a phase of adaptation that requires the strengthening of their institutional capacities and regulations.

Finally, in the local environment of Barranquilla, higher education institutions have shown a growing interest in digitization and the inclusion of innovative technologies in their educational and administrative activities. Despite this progress, the need to improve technology governance mechanisms has become apparent, particularly with regard

to data management and cybersecurity. Research in the region indicates that, although there are important initiatives, there are still gaps in the implementation of digital security policies (Pérez & Rodríguez, 2021), which emphasizes the importance of conducting research in this area.

2. Objectives

2.1 General objective

To analyze the governance of generative artificial intelligence in higher education institutions from the perspective of digital security and data protection, through a systematic review of the scientific literature based on the PRISMA methodology.

2.2 Specific objectives

- To identify the predominant theoretical and conceptual approaches in the scientific literature on the governance of generative artificial intelligence in higher education institutions.
- Examine the main risks, challenges and strategies associated with digital security and data protection in the use of generative artificial intelligence in the university environment.
- To synthesize the trends, research gaps, and governance proposals present in the selected studies, in order to provide guidelines for the development of institutional policies in higher education.

3. Methodology

This work is carried out through a systematic review of the scientific literature using the PRISMA protocol (Preferred Elements for Systematic Review Reports and Meta-Analyses) as a method. This approach enables the identification, selection, evaluation, and rigorous synthesis of evidence related to generative AI governance in universities, with a particular focus on digital security and data protection. The use of the PRISMA protocol ensures transparency in the research process, allows methodological decisions to be tracked, and makes it easier for other researchers to replicate the study, thus strengthening the validity and reliability of the findings (Page et al., 2021).

3.1 Collection of information

The information was obtained through a systematic search in the Scopus and Web of Science (WoS) databases, chosen for their international prestige and for containing indexed scientific literature of great impact in fields such as artificial intelligence, university education, digital governance, cybersecurity and data protection. These databases offer access to peer-reviewed publications, ensuring the methodological quality, scientific rigor and relevance of the documents considered in the review. In addition, its multidisciplinary approach is suitable for investigating a complex and broad phenomenon such as the governance of generative artificial intelligence.

3.2 Search strategy

The search was planned by combining keywords in English, since most of the scientific articles indexed in Scopus and WoS are in this language. The search equations were formulated based on the core concepts of the study: generative artificial intelligence, governance, higher education, digital security and data protection. The terms used included: "generative artificial intelligence", "AI governance", "artificial intelligence governance", "higher education", "universities", "digital security", "cybersecurity", "data protection", "data privacy", "ethical AI", "AI regulation" and "digital governance".

These terms were joined together using Boolean operators (AND/OR) to broaden the scope of the search and ensure that relevant studies were retrieved. The strategy made it possible to locate research that explores both the technical and organizational, ethical and regulatory aspects linked to the implementation of generative artificial intelligence in the university context.

3.3 Inclusion and exclusion criteria

In order to ensure the quality and relevance of the chosen studies, specific inclusion criteria were defined. Scientific articles published between 2025 and 2026 in journals indexed in Scopus and Web of Science that had gone through the peer review process were considered. Empirical and theoretical studies and systematic reviews that directly address the governance of generative artificial intelligence or its link with digital security and data protection in higher education institutions were also included. Only documents available in English or Spanish and offering access to the full text were selected, which facilitated a thorough analysis of their content.

In relation to the criteria for excluding documents, works such as theses, books, chapters, conference proceedings, technical reports and non-formal literature that had not gone through a peer review process were eliminated. Likewise, those studies that addressed artificial intelligence in a general way without a direct relationship with governance, cybersecurity or data protection in the field of education were rejected. Duplicate records found in the queried databases were also removed.

3.4 Study selection process

In the first stage of the search, a total of 31 records that could be relevant in the chosen databases were located. Then, a debugging process was carried out to eliminate duplicate documents, resulting in 28 unique records. In the next phase, an initial review of the titles and abstracts was carried out, in order to determine the thematic relevance of the studies in relation to the objectives of the research.

Articles that met the relevance criteria were then subjected to an eligibility test by reading the texts in full. This stage made it possible to check the adequacy of each study with respect to the established inclusion criteria, ensuring that they dealt directly with the governance of generative artificial intelligence and its relationship with cybersecurity and data protection in higher education institutions.

As a result of the selection process, a total of 19 academic articles were obtained, which constitute the basis for the analysis of this systematic review. These studies were examined from a qualitative approach, considering variables such as the methodological approach, the context in which they were applied, their main findings and their implications on governance, cybersecurity and data protection issues.

Finally, the process of identification, selection, eligibility evaluation and inclusion of the studies is illustrated through the PRISMA flow chart, which clearly summarizes each methodological stage carried out. This resource adds transparency to the study and facilitates its replication, which reinforces the scientific validity of the research.

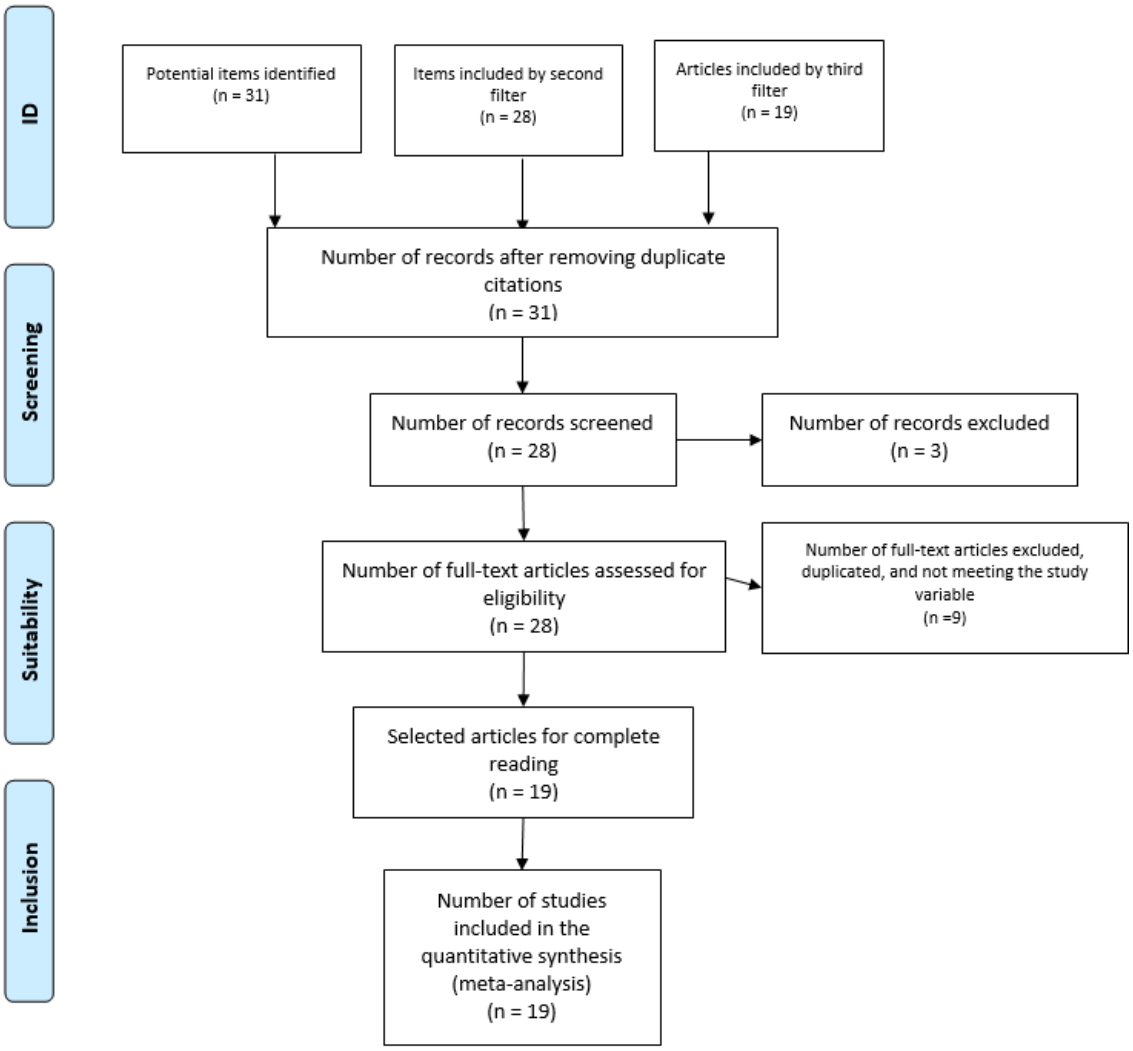

Figure 1. Flowchart of a systematic review carried out under the PRISMA technique (Moher, Liberati, Tetzlaff, Altman, & Group, 2009)

Source: Authors; Based on the proposal of the Prisma Group (Moher, Liberati, Tetzlaff, Altman, & Group, 2009)

4. Results

The findings of this systematic review are organized based on a thorough analysis of the 19 selected academic articles, which meet the inclusion criteria established in the PRISMA protocol. To facilitate the understanding and organization of the data, an analysis matrix was created that summarizes the main characteristics of each research, covering elements such as the authors, the year of publication, the methodological approach, the context in which it is applied, and the most relevant findings. This organization allows us to recognize patterns, trends and similarities in the literature related to the governance of generative artificial intelligence in higher education institutions, as well as its connection with digital security and data protection. From this analytical basis, a critical interpretation of the findings is made, with the aim of highlighting the most common approaches, the challenges that arise and the opportunities to advance in this area of research.

No.	RESEARCH TITLE	AUTHOR/YEAR	COUNTRY	TYPE OF STUDY	INDEXING
1	*Be Aware: Navigating Challenges in AI-Driven Higher Education*	Awashreh, R. (2025)	OMAN	QUALITATIVE	SCOPUS
2	*Artificial Intelligence Learning: Perceptions and Challenges in the Profile of Industrial Engineering Students*	de los Ángeles Martínez-Mercado, M., López-Bustamante, G. E., García-León, A. M., Puente-Aguilar, E. P., & del Carmen Bacre-Guzmán, D. (2025).	MEXICO, PERU	QUALITATIVE	SCOPUS
3	*Perceptions of AI-based tools among polish medical university students*	Ratajczak, P., Słowik, O., Cynar, J., Kopciuch, D., Paczkowska, A., Zaprutko, T., & Kus, K. (2025)	POLAND	QUALITATIVE	SCOPUS
4	*Securing data of real-world applications in society 5.0: research challenges and directions*	Sundarrajan, M., Choudhry, M. D., Jothi, A., & Biju, J. (2025).	INDIA	QUALITATIVE	WOS
5	*Integration of artificial intelligence in the digital preservation of academic repositories and scientific data in higher education libraries*	Sousa, N. M. T. (2025).	PORTUGAL	QUANTITATIVE	SCOPUS
6	*Advanced Research Trends in Sustainable Solutions, Data Analytics, and Security*	Radwan, A. G., Abd-El-Hafiz, S. K., Abdel Halim, I. T., Liu, Y., & Qiu, M. (2025).	EGYPT	QUALITATIVE	SCOPUS

7	*A Systematic Literature Review of Information Security Practices in Higher Education Contexts*	Bwiino, K., Mayoka, G. K., Nkamwesiga, L., & Nyamadi, M. (2026).	UGANDA	QUALITATIVE	WOS
8	*An integrated framework for the security of e-learning systems in higher education institutions*	AlKalbani, H. R., & Al-Busaidi, K. A. (2025).	OMAN	QUANTITATIVE/QUALITATIVE	WOS
9	*Artificial intelligence in information security policy management research: a scoping review*	Karlsson, F., Rostami, E., Gao, S., & Hanif, M. (2026).	SWITZERLAND	QUALITATIVE	WOS
10	*Behavioral and Cognitive Pathways to Information Security Outcomes in Smart Universities*	Phakaedam, C., Savithi, C., & Suttidee, A. (2026).	THAILAND	QUALITATIVE	WOS
11	*Comparative Analysis of Cybersecurity Frameworks in Educational Institutions: Towards a Tailored Security Model*	Hidayatulloh, S. (2025).	INDONESIA	QUALITATIVE	WOS
12	*Cybersecurity in Higher Education Institutions: A Systematic Review of Emerging Trends, Challenges and Solutions*	Afolalu, O., & Tsoeu, M. S. (2025).	SOUTH AFRICA	QUALITATIVE	WOS

13	*Design and implementation of information security system for E-learning platform*	Junghare, S., & Dube, M. (2026).	INDIA	QUANTITATIVE	WOS
14	*Embracing Artificial Intelligence in Dental Practice: An Exploratory Study of Romanian Clinicians' Perspectives and Experiences*	Cozmescu, A. F., Cernega, A., Mincă, D. G., Didilescu, A. C., Imre, M. M., Totan, A. R., ... Pițuru, S. M. (2025)	ROMANIA	QUANTITATIVE	WOS
15	*Integrating Artificial Intelligence into the Cybersecurity Curriculum in Higher Education: A Systematic Literature Review*	Tian, J. (2025).	SINGAPORE	QUALITATIVE	WOS
16	*Integration of artificial intelligence with information security: a systematic literature review*	Negi, L., Ragiri, P. R., Bhatt, S., Garg, G., Sharma, K., & Bhatt, N. (2026).	INDIA	QUANTITATIVE	WOS
17	*INTRODUCING ARTIFICIAL INTELLIGENCE IN EDUCATION THREATS AND CHALLENGES (FOLLOWING THE EXAMPLE OF BULGARIA)*	Kazakova, M. (2025).	BULGARIA	QUALITATIVE	WOS

18	*Security, Privacy, and AI Integration in Educational Metaverse: A Comprehensive Review and Framework*	Salah, A. A., Jamil, N., Sulaiman, H., Cangelosi, A., Alyasseri, Z. A. A., & Hosseini, E. (2025)	MALAYSIA, IRAQ, UAE, QATAR, UNITED KINGDOM	QUANTITATIVE	WOS
19	*The position of technical competence in establishing digital data security awareness*	Keskin, H. K., Arıcı, E. Y., Papadakis, S., Kalogiannakis, M., & Baydar, I. Y. (2025)	TURKEY, GREECE	QUANTITATIVE	WOS

Table 1. List of articles analyzed

Source: Own elaboration

The detailed analysis of the 19 selected articles highlights that the management of generative artificial intelligence in educational institutions is presented as a new area, marked by its multiple complexity, where technological, organizational, ethical and regulatory elements are intertwined. In line with the purpose of this research, which seeks to examine the governance of generative AI from the perspective of digital security and data protection, the results indicate that the recent academic literature does not treat these aspects separately, but considers them as interrelated parts in the processes of digital transformation in universities. In this context, the studies reviewed agree that the rapid implementation of AI-powered technologies has outpaced the capacity of institutions to create effective regulatory frameworks, leading to vulnerable situations in both security and privacy (Awashreh, 2025; Karlsson et al., 2026; Negi et al., 2026).

First, a significant amount of research is devoted to examining how artificial intelligence is integrated into educational processes and the opinions of the different actors involved. The work of Awashreh (2025) highlights that the introduction of AI systems in higher education entails structural risks linked to information privacy, lack of transparency in algorithms, and lack of regulations within institutions, highlighting that the lack of well-defined governance frameworks can lead to an incorrect use of technology. In a similar vein, de los Ángeles Martínez-Mercado et al. (2025) show that students recognize the potential of artificial intelligence to enhance learning and academic productivity, but at the same time express concerns about technological dependence and the possible loss of cognitive skills. On the other hand, Ratajczak et al. (2025) reveal that university students consider AI tools useful, although they show doubts about the reliability of the information they produce and the potential ethical dilemmas. Additionally, Cozmescu et al. (2025) point out that in professional settings, such as dental practice, the use of artificial intelligence raises favorable expectations in terms of efficiency, but also raises concerns about the security of clinical information and accountability in decisions supported by technology. Together, these studies suggest that generative AI governance must integrate not only regulatory aspects, but also users' everyday perceptions and practices, given that these directly impact the effectiveness of institutional policies.

Second, the review shows a remarkable amount of research focused on digital security as a key aspect in the adoption of AI-powered technologies. Sundarrajan et al. (2025) underline that safeguarding data in real-world applications within contemporary digital society is one of the main current challenges, due to the increasing connectivity of systems and the complexity of digital environments. In this context, Radwan et al. (2025) highlight new trends in data analysis and security, indicating that the increase in the application of smart technologies requires the development of sustainable solutions that incorporate information protection from its initial design. Similarly, Negi et al. (2026) show that merging artificial intelligence with information security represents both an opportunity and a challenge, since, although it improves protection methods, it also introduces new vulnerabilities that need to be

addressed with appropriate policies. These contributions reinforce the idea that generative AI management must be based on advanced cybersecurity strategies, capable of adjusting to dynamic and complex environments.

In greater detail, the research of Bwiino et al. (2026) and Afolalu and Tsoeu (2025), both systematic studies, provide a comprehensive perspective on information security practices in higher education institutions. Bwiino et al. (2026) indicate that there is a considerable gap in the implementation of security policies, highlighting the lack of integrated strategies and the limited ability of institutions to manage digital risks effectively. In turn, Afolalu and Tsoeu (2025) identify that educational institutions face obstacles related to the protection of technological infrastructures, the response to security incidents, and the need to adopt novel solutions to address emerging threats. With respect to the objective of this study, these results demonstrate that generative AI governance cannot be developed without at the same time strengthening digital security capabilities in universities.

Along the same lines, the studies by AlKalbani and Al-Busaidi (2025), Hidayatulloh (2025) and Junghare and Dube (2026) focus on the design and implementation of security models in digital educational contexts, especially in e-learning platforms. AlKalbani and Al-Busaidi (2025) suggest an integrated security framework that combines technological and organizational elements, highlighting the relevance of adopting holistic approaches to the protection of education systems. Hidayatulloh (2025) conducts a comparative analysis of cybersecurity frameworks, concluding that educational institutions need models that adapt to their specific requirements, avoiding generic solutions. In turn, Junghare and Dube (2026) point out that it is essential to implement security systems in virtual learning platforms to ensure the confidentiality, integrity, and availability of information. This research reinforces the notion that AI governance must include the protection of the digital environments in which it operates, which implies the integration of risk management policies, technologies, and practices.

On the other hand, research by Karlsson et al. (2026) and Negi et al. (2026) offers key insight into the link between artificial intelligence and information security management. Karlsson et al. (2026) stress that artificial intelligence can be leveraged to improve security policy management, helping to identify threats and make decisions based on accurate information. In addition, Negi et al. (2026) point out that by integrating AI into security systems, the effectiveness of protection processes can be increased, although this also requires creating regulatory frameworks that regulate its use. These studies demonstrate that generative AI governance should be seen as a two-way process, where AI acts both as a subject of governance and as a tool for it.

With regard to the human dimension, research by Phakaedam et al. (2026) and Keskin et al. (2025) highlights the relevance of digital skills and security awareness as essential elements for safeguarding information. Phakaedam et al. (2026) highlight that user behavior has a considerable impact on security outcomes in smart universities, underscoring the urgency of improving cybersecurity education. On the other hand, Keskin et al. (2025) indicate that technical skills are crucial to building a digital security culture, which requires digital skills training to be part of institutional strategies. In this framework, generative AI governance should include educational programs that allow users to interact safely and responsibly with the technology.

In addition, the research by Sousa (2025) and Salah et al. (2025) expands the debate to new digital environments, showing that the application of artificial intelligence in academic repositories and educational metaverses presents new challenges related to privacy and security. Sousa (2025) highlights the relevance of digital preservation and data defense in university libraries, while Salah et al. (2025) offer a framework to address security and privacy in educational environments in the metaverse. These findings suggest that AI governance needs to adapt to technological contexts that are constantly changing, which demands agile and flexible approaches.

On the other hand, Tian's (2025) analysis underscores the need to include artificial intelligence in cybersecurity curricula, indicating that training trained professionals is crucial to face the difficulties arising from digital transformation. In this context, generative AI governance is not only about regulating the current situation, but also about preparing institutions for the future, developing both human and technical capabilities.

Finally, the joint examination of the studies allows us to affirm that the management of generative artificial intelligence in the field of higher education needs a global approach that combines technological innovation, security in the digital environment and information protection. The articles analyzed agree that the implementation of AI must be accompanied by clear policies within institutions, appropriate regulations, and training strategies that help manage the risks involved. In this sense, the purpose of this study is supported by the reviewed evidence, which confirms that the management of generative AI represents a key challenge for higher education institutions in the framework of digital transformation (Awashreh, 2025; Bwiino et al., 2026; Karlsson et al., 2026; Salah et al., 2025).

5. Discussion

The current systematic review offers an interpretation of how generative AI governance is handled in universities as a complicated phenomenon that goes beyond mere technology, embedded in a structural context that includes organizational, ethical, pedagogical, and normative elements. The results obtained show that the current scientific literature coincides in highlighting that the incorporation of artificial intelligence systems has progressed faster than the capacity of institutions to supervise their use, thus generating important gaps in areas such as digital security and information protection. This discrepancy between technological advancement and effective governance is identified as one of the main dangers in digitally integrated educational environments, where the absence of defined policies can result in uncontrolled practices, misuse of information, and exposure to severe vulnerabilities (Awashreh, 2025; Karlsson et al., 2026).

From an analytical approach, the results allow us to conclude that the governance of generative artificial intelligence in higher education should not be considered a linear or only technical process, but rather as a creation that encompasses multiple dimensions and requires the collaboration of different levels of intervention. In this context, research based on users' perceptions and experiences shows that the application of artificial intelligence is influenced by cultural, cognitive, and ethical factors that affect its use and acceptance. Studies such as those by Ángeles Martínez-Mercado et al. (2025), Ratajczak et al. (2025) and Cozmescu et al. (2025) indicate that, although there is a positive assessment of the potential of artificial intelligence, there are still concerns regarding the loss of autonomy in cognition, the reliability of the content generated and the ambiguity regarding the ethical limits in its use. This finding underscores that governance should not be restricted to formal regulation, but should include approaches that promote critical ownership, advanced digital education, and the building of technological trust within academia.

With regard to digital security, the analysis of the results reveals that educational institutions are dealing with a landscape of increasing vulnerability, as a result of the expansion of their digital environments and the incorporation of smart technologies in various institutional processes. Studies by Sundarrajan et al. (2025), Radwan et al. (2025) and Negi et al. (2026) agree that the complexity of systems that use artificial intelligence multiplies exposure to cyber risks, particularly those linked to automated attacks, data manipulation and unauthorized access. In this context, generative artificial intelligence governance should be seen as a fundamental element within the cybersecurity strategies of institutions, as it regulates both technological behavior and the protection of data and critical infrastructures.

Likewise, the systematic research analyzed (Bwiino et al., 2026; Afolalu & Tsoeu, 2025) help to deepen the understanding of the structural limitations suffered by educational institutions in terms of information security. Specifically, there is a lack of cohesion in security management, marked by the absence of inclusive policies, poor coordination between different units, and limited capacity to deal with complicated incidents. This situation indicates that generative AI governance should be conceived as a comprehensive process that connects different areas of the organization, such as academic, technological, and administrative administration, to ensure a coherent and effective response to the risks that arise.

On the other hand, the debate reveals that the relationship between artificial intelligence and information security is not linear, but has a dual dynamic in which AI serves both as a risk and as a solution. Research by Karlsson et al. (2026) and Negi et al. (2026) underscores that artificial intelligence can improve security systems by automating threat identification and optimizing response processes. However, this same skill presents new challenges related to the lack of transparency of algorithms, the monitoring of automated decisions and the dependence on technology. In this regard, generative AI governance should be fixed in mixed control models, where human supervision and technological automation are integrated to ensure appropriate levels of security and transparency.

Regarding the organizational dimension, the findings suggest that the governance of artificial intelligence needs to strengthen institutional capacities, both in technical and human aspects. Studies by Phakaedam et al. (2026) and Keskin et al. (2025) show that user behavior and their level of digital skills significantly affect information security. This means that governance strategies should include continuing education programs, not only in the use of technologies, but also in the understanding of their risks, limitations, and associated responsibilities. Thus, security ceases to be a purely technical matter and becomes a socio-technical phenomenon that encompasses human practices, decisions and behaviors.

Similarly, the analysis allows us to recognize that the creation of new digital environments, such as the educational metaverse and digital preservation systems, poses additional challenges for the governance of artificial intelligence. Research by Sousa (2025) and Salah et al. (2025) shows that these environments increase complexity in the management of privacy, digital identity, and data protection, due to their immersive, distributed, and highly interconnected nature. In this framework, generative AI governance must move towards flexible and predictive models, capable of anticipating risks and adapting to constantly evolving technological scenarios.

Another important element that emerges in the discussion is the crucial role of education as a method of long-term governance. Tian's (2025) research underlines that the inclusion of artificial intelligence in cybersecurity programs favors the development of fundamental skills in the professionals of the future, which improves the ability of institutions to manage technological risks. This approach indicates that governance should go beyond regulatory standards, incorporating an educational dimension that ensures the durability of security and data protection strategies over time.

In this line, the discussion allows for a broader understanding of generative AI governance as a dynamic socio-technical system that encompasses the interaction between technologies, regulations, actors, and institutional contexts. The studies reviewed show that higher education institutions are in a phase of change, where the implementation of advanced technologies is not always accompanied by sufficiently robust governance frameworks. This situation creates tensions between innovation and control, efficiency and security, as well as between automation and responsibility, which requires a revision of the traditional models of technological management in the university environment.

Finally, the discussion reinforces the notion that the governance of generative artificial intelligence in educational institutions should be considered a strategic, comprehensive and evolving process, which seeks not only to reduce risks, but also to maximize the value of technology in educational environments. The studies analyzed agree that the lack of strong governance frameworks can put the integrity of education systems at risk, affect institutional trust, and cause adverse effects on the quality of learning and knowledge management (Awashreh, 2025; Bwiino et al., 2026; Karlsson et al., 2026; Salah et al., 2025).

From this perspective, this study offers a comprehensive view that helps to understand the governance of generative AI as a key element in the digital transformation of higher education. Beyond the mere adoption of technologies, it is essential to design coherent policies at the institutional level, establish strong security systems, develop digital competencies and promote an organizational culture that prioritizes responsible information management. Thus, generative AI governance should be seen not as a simple control mechanism, but as a complex institutional structure that connects innovation, security, and ethics in the context of today's higher education.

6. Conclusions

The current systematic review, conducted using the PRISMA methodology, facilitated a comprehensive analysis of generative AI governance in universities, focusing on its connection to digital security and data protection. After examining 19 selected studies, it is evident that this area of research is in a state of both theoretical and practical development, marked by the coexistence of outstanding technological advances together with structural limitations in the capacity of institutions to regulate their use. In this context, one of the main contributions of this research is to highlight that the governance of generative artificial intelligence should not be seen as an isolated element within the digital transformation, but as a key axis that accompanies various dimensions of university functioning, including technological management, information security, the ethics of the institution and academic training.

In relation to the proposed general objective, the results allow us to deduce that the governance of generative artificial intelligence in universities is configured as a flexible, complex and multifaceted process, where technological, organizational, human and regulatory aspects are intertwined. The evidence collected indicates that although the adoption of AI tools has grown rapidly in the education sector, this increase has not been supported by the establishment of sufficiently robust governance frameworks, which has created a critical discrepancy between innovation and regulation. This mismatch translates into significant risks related to digital security, data protection and the integrity of academic processes, highlighting the urgent need to strengthen institutional capacities in the field of technological governance.

With regard to the first specific objective, which seeks to identify the most relevant theoretical and conceptual approaches in the literature, it is observed that the governance of generative artificial intelligence has been treated from various perspectives, including technological ethics, information security management, digital transformation

and educational innovation. However, a significant conceptual fragmentation can be noted, since most studies address these elements in isolation, without integrating them into holistic governance models. This lack of connection limits the understanding of the phenomenon and makes it difficult to implement coherent institutional policies. In this sense, the studies analysed agree on the need to move towards integrative conceptual frameworks that relate the governance of artificial intelligence with digital security and data protection, recognising their interdependent nature within education systems.

Regarding the second specific objective, which focuses on analyzing the dangers, obstacles and methods related to digital security and data safeguarding, the findings indicate that universities face an environment with high vulnerability to cyber threats and risks linked to the handling of confidential information. The increasing incorporation of artificial intelligence in educational platforms, digital archives and virtual learning spaces has significantly increased the area of risk, which increases the possibility of security incidents. In addition, the need for large volumes of data for generative models to work presents additional challenges in terms of privacy, confidentiality, and compliance. In this sense, the reviewed literature points out that digital security should be seen as a key element in the governance of artificial intelligence, rather than considered as a secondary or additional aspect (Sundarrajan et al., 2025; Negi et al., 2026; Hidayatulloh, 2025).

Similarly, it is recognized that one of the main obstacles to implementing digital security strategies is due to the lack of coordination between the institution's policies, technological solutions, and risk management practices. This disarticulation complicates the creation of effective protection systems and reduces the ability to react to security incidents. The studies analyzed suggest that institutions should implement comprehensive approaches that merge advanced technological tools, precise regulatory frameworks, and digital skills training strategies. In this context, the governance of generative artificial intelligence must encompass not only the regulation of technological systems, but also the strengthening of the organizational culture regarding information security (Phakaedam et al., 2026; Keskin et al., 2025).

With regard to the third specific objective, which seeks to synthesize the trends, gaps and proposals of the literature, it is observed that current research focuses on the creation of adaptive security models, the incorporation of artificial intelligence in security management and the analysis of perceptions and digital skills in educational contexts. However, significant gaps are also identified, especially with regard to the design of governance models that clearly integrate generative artificial intelligence, digital security and data protection in the field of higher education. This lack represents an important opportunity to develop new research that offers more complete conceptual and methodological frameworks applicable to the institutional reality.

From a broader angle, the results of this research allow us to affirm that generative artificial intelligence management should be seen as a socio-technical whole that encompasses the relationship between technologies, participants, regulations, and organizational contexts. In this set, technology does not operate in isolation, but depends on human decisions, institutional structures and regulatory frameworks. Proper management of artificial intelligence therefore requires a holistic approach that combines technological innovation with ethical responsibility, digital security and safeguarding users' rights.

Similarly, it concludes that training in digital skills is essential to improve the governance of artificial intelligence in higher education institutions. The studies reviewed show that the shortage of knowledge and skills to handle digital technologies increases vulnerability to security risks and restricts users' ability to interact critically and responsibly with artificial intelligence. In this context, universities must include training in digital skills and cybersecurity as part of their institutional strategies, both in specific academic programs and in the comprehensive training of students, teachers, and administrative staff.

On the other hand, the findings of this research highlight the urgency of establishing clear and consistent institutional policies that guide the implementation of generative artificial intelligence in higher education. These policies should address aspects such as data management, information security, transparency in algorithms, and accountability in the use of technology. In addition, it is essential that they are flexible and adaptable, which will allow them to respond to technological changes and new challenges that arise in constantly evolving digital environments.

In conclusion, this research contributes to the scientific literature by offering a systematic and critical analysis on the governance of generative artificial intelligence in higher education institutions, emphasizing the relevance of including digital security and data protection as essential elements in this process. However, its limitations are also recognized, especially in terms of the lack of empirical studies that directly address the application of governance

models in specific contexts. Therefore, it is suggested that future research focus on an empirical analysis of these processes and on the creation of applied models that can be used in different institutional contexts.

In summary, the governance of generative artificial intelligence becomes one of the main strategic challenges for higher education institutions in the 21st century. Proper management will not only maximize the potential of technology to improve education, but also safeguard the security, privacy, and integrity of information in increasingly complex digital environments. It is therefore crucial that universities play an active role in creating governance frameworks that unite technological innovation with institutional accountability, which will contribute to the development of safer, more ethical and sustainable education systems.

7. Recommendations

The results obtained from this systematic review provide a set of practical suggestions that seek to improve the governance of generative artificial intelligence in higher education institutions, especially in those regional and local environments where institutional capacities are still under development. In this framework, the recommendations presented should not be considered absolute rules, but rather as strategic guidelines that can be adjusted to the particular circumstances of each situation, considering the technological, regulatory and organizational gaps that have been pointed out in the scientific literature (Bwiino et al., 2026; Afolalu & Tsoeu, 2025).

First, from a strategic perspective, it is advisable for higher education institutions to create institutional frameworks for the governance of artificial intelligence that explicitly include digital security and data protection as fundamental pillars of technological transformation. The studies reviewed show that one of the main shortcomings in the implementation of artificial intelligence is the lack of clear and coherent policies, which entails risks associated with the unregulated use of these technologies (Awashreh, 2025; Karlsson et al., 2026). Therefore, universities must progress towards establishing institutional policies that define principles of use, obligations, supervision protocols and control mechanisms, ensuring that the adoption of artificial intelligence is carried out under criteria of transparency, ethics and security.

Second, when it comes to digital security, it is crucial for institutions to implement flexible cybersecurity models that adapt to the increasing complexity of educational digital spaces. The studies analyzed indicate that the incorporation of artificial intelligence systems increases vulnerability to cyber threats, which is why the implementation of more advanced protection strategies is necessary (Sundarrajan et al., 2025; Negi et al., 2026). Thus, it is suggested to adopt security frameworks based on risk management, which include mechanisms for continuous monitoring, threat detection and incident response, in addition to the integration of intelligent technologies to reinforce the protection of the institution's systems.

Third, with regard to data protection, it is recommended that higher education institutions strengthen their information management policies, ensuring compliance with international standards on privacy and data management. The evidence collected shows that the use of generative artificial intelligence entails the processing of large amounts of data, which increases the risk of leaks, misuse, or unauthorized access (Sousa, 2025; Salah et al., 2025). In this sense, it is essential to implement data governance mechanisms that include information classification, access control, data anonymization, and process auditing, in order to guarantee the integrity and confidentiality of institutional information.

At the operations level, it is advised that universities establish clear protocols for the use of generative artificial intelligence tools in their academic and administrative activities. Research on how users perceive this technology indicates that the absence of specific guidelines can lead to inappropriate use of it, which could harm academic integrity and the quality of learning (de los Ángeles Martínez-Mercado et al., 2025; Ratajczak et al., 2025). Therefore, the creation of institutional guides that specify good practices, limits of use and evaluation criteria in educational environments is proposed, as well as monitoring mechanisms that facilitate the supervision of the use of these tools.

In the pedagogical field, the results of the review underline the importance of improving digital skills and the culture of safety within the academic community. Studies by Phakaedam et al. (2026) and Keskin et al. (2025) show that user actions are a key element for information security, suggesting that AI governance should include training and awareness plans. In this context, it is recommended that institutions incorporate digital literacy programs, cybersecurity training, and artificial intelligence ethics education into their curricula, encouraging responsible and conscious use of technology.

From a regional perspective, in the context of Latin America, it is suggested that higher education institutions strengthen the connection between internal policies and national regulatory frameworks, with the aim of reducing the

gaps present in the governance of artificial intelligence. The literature indicates that the region faces structural challenges linked to inequality in access to technology and the limited institutional capacity to manage its implementation (Awashreh, 2025; Afolalu and Tsoeu, 2025). It is therefore essential to foster initiatives of collaboration between institutions, capacity building and knowledge transfer that allow progress towards stronger and more sustainable governance models.

In the specific case of Colombia, it is recommended that higher education institutions align their strategies for the governance of artificial intelligence with national policies on digital transformation and data protection, consolidating the application of current regulatory frameworks. In addition, it is suggested that universities create units specialized in the management of artificial intelligence and digital security, which would facilitate the coordination of technological initiatives and ensure their secure implementation. This approach would help to reduce the institutional fragmentation observed in the studies reviewed and to improve the capacity to respond to emerging risks.

Finally, in the Barranquilla environment, it is suggested that universities adopt a progressive approach in the adoption of artificial intelligence governance, focusing their efforts on improving the capacities of institutions and adjusting international models to local circumstances. The review reveals that although progress has been made in digital transformation, there are still gaps in security and data protection management, implying the need to implement strategies that are adapted to the context. In this framework, the creation of collaborations between universities, the government and the private sector is proposed, with the aim of strengthening technological infrastructure, promoting training in digital skills and stimulating practical research in the governance of artificial intelligence.

Taken together, these suggestions facilitate progress towards a more practical interpretation of how generative AI is managed in university education, underscoring the importance of merging technological innovation with online security, data defense and skills building within institutions. Its implementation would help not only to reduce the dangers linked to the use of artificial intelligence, but also to maximise its potential as a resource to strengthen education systems at both regional and local levels.

References

1. Afolalu, O., & Tsoeu, M. S. (2025). Cybersecurity in higher education institutions: A systematic review of emerging trends, challenges and solutions.
2. Aguerre, C., & Galperin, H. (2021). Artificial intelligence in Latin America: Challenges and opportunities. Information Technologies & International Development, 17, 1–8.
3. AlKalbani, H. R., & Al-Busaidi, K. A. (2025). An integrated framework for the security of e-learning systems in higher education institutions.
4. Awashreh, R. (2025). Be aware: Navigating challenges in AI-driven higher education.
5. Bommasani, R., Hudson, D. A., Adeli, E., Altman, R., Arora, S., von Arx, S., … Liang, P. (2021). On the opportunities and risks of foundation models. arXiv preprint arXiv:2108.07258.
6. Bwiino, K., Mayoka, G. K., Nkamwesiga, L., & Nyamadi, M. (2026). A systematic literature review of information security practices in higher education contexts.
7. Cobo, C. (2016). Pending innovation: Reflections (and provocations) on education, technology and knowledge. Ceibal Foundation.
8. Cozmescu, A. F., Cernega, A., Mincă, D. G., Didilescu, A. C., Imre, M. M., Totan, A. R., & Pițuru, S. M. (2025). Embracing artificial intelligence in dental practice: An exploratory study of Romanian clinicians' perspectives and experiences.
9. de los Ángeles Martínez-Mercado, M., López-Bustamante, G. E., García-León, A. M., Puente-Aguilar, E. P., & del Carmen Bacre-Guzmán, D. (2025). Artificial intelligence learning: Perceptions and challenges in the profile of industrial engineering students.
10. Dwivedi, Y. K., Kshetri, N., Hughes, L., Slade, E. L., Jeyaraj, A., Kar, A. K., … Wright, R. (2023). “So what if ChatGPT wrote it?” Multidisciplinary perspectives on opportunities, challenges and implications of generative conversational AI. International Journal of Information Management, 71, 102642.
11. Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., … Vayena, E. (2018). AI4People—An ethical framework for a good AI society. Minds and Machines, 28(4), 689–707.
12. González, J., & Gómez, L. (2022). Artificial Intelligence and Education in Colombia: Challenges and Opportunities. Revista Colombiana de Educación, 83, 45–62.
13. Hidayatulloh, S. (2025). Comparative analysis of cybersecurity frameworks in educational institutions: Towards a tailored security model.
14. Junghare, S., & Dube, M. (2026). Design and implementation of information security system for e-learning platform.
15. Karlsson, F., Rostami, E., Gao, S., & Hanif, M. (2026). Artificial intelligence in information security policy management research: A scoping review.

16. Kazakova, M. (2025). Introducing artificial intelligence in education threats and challenges (following the example of Bulgaria).
17. Keskin, H. K., Arıcı, E. Y., Papadakis, S., Kalogiannakis, M., & Baydar, I. Y. (2025). The position of technical competence in establishing digital data security awareness.
18. Kshetri, N. (2021). Cybersecurity management in the era of artificial intelligence. IEEE IT Professional, 23(4), 30–37.
19. Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. Big Data & Society, 3(2), 1–21.
20. Negi, L., Ragiri, P. R., Bhatt, S., Garg, G., Sharma, K., & Bhatt, N. (2026). Integration of artificial intelligence with information security: A systematic literature review.
21. OECD. (2019). OECD principles on artificial intelligence. OECD Publishing.
22. Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., … Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. BMJ, 372, n71.
23. Pérez, J., & Rodríguez, M. (2021). Digital transformation in higher education institutions in the Colombian Caribbean. Revista Educación y Desarrollo, 58, 23–35.
24. Phakaedam, C., Savithi, C., & Suttidee, A. (2026). Behavioral and cognitive pathways to information security outcomes in smart universities.
25. Radwan, A. G., Abd-El-Hafiz, S. K., Abdel Halim, I. T., Liu, Y., & Qiu, M. (2025). Advanced research trends in sustainable solutions, data analytics, and security.
26. Ratajczak, P., Słowik, O., Cynar, J., Kopciuch, D., Paczkowska, A., Zaprutko, T., & Kus, K. (2025). Perceptions of AI-based tools among Polish medical university students.
27. Salah, A. A., Jamil, N., Sulaiman, H., Cangelosi, A., Alyasseri, Z. A. A., & Hosseini, E. (2025). Security, privacy, and AI integration in educational metaverse: A comprehensive review and framework.
28. Selwyn, N. (2019). Should robots replace teachers? AI and the future of education. Polity Press.
29. Sousa, N. M. T. (2025). Integration of artificial intelligence in the digital preservation of academic repositories and scientific data in higher education libraries.
30. Sundarrajan, M., Choudhry, M. D., Jothi, A., & Biju, J. (2025). Securing data of real-world applications in society 5.0: Research challenges and directions.
31. Tian, J. (2025). Integrating artificial intelligence into the cybersecurity curriculum in higher education: A systematic literature review.
32. UNESCO. (2021). Recommendation on the ethics of artificial intelligence. UNESCO Publishing.
33. Voigt, P., & Von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR): A practical guide. Springer.
34. Williamson, B., & Eynon, R. (2020). Historical threads, missing links, and future directions in AI in education. Learning, Media and Technology, 45(3), 223–235.
35. Zawacki-Richter, O., Marín, V. I., Bond, M., & Gouverneur, F. (2019). Systematic review of research on artificial intelligence applications in higher education. International Journal of Educational Technology in Higher Education, 16(1), 39.