Online-Journals.org

iJET International Journal of Emerging Technologies in Learning

iJET | eISSN: 1863-0383 | Vol. 21 No. 3 (2026) | OPEN ACCESS

https://doi.org/10.3991/ijet.v21i03.58977

PAPER

Strategies, Regulations and Mechanisms for Protecting Student Data in University Digital Repositories: A Systematic Review

Marco Yamba-Yugsi[1] (✉), Juan-Carlos Ortega-Castro[1], Jorge Maldonado-Mahauad[2], Cornelio Agustín Borja-Pozo[1]

[1]Universidad Católica de Cuenca, Cuenca, Ecuador

[2]Universidad de Cuenca, Cuenca, Ecuador

marco.yamba@ucacue.edu.ec

ABSTRACT

The digitalization of educational services has increased the exposure of student information to security and privacy risks. This research addresses the need to understand the strategies, regulations, and technologies used to protect data in university digital repositories. A systematic literature review was conducted in recognized databases (WOS, Scopus, and ACM), from which 30 studies meeting the inclusion criteria were selected. The findings showed that higher education institutions face complex challenges in risk management, regulatory compliance (such as GDPR), and the adoption of international standards such as ISO/IEC 27001 and 27002. Additionally, emerging methods such as homomorphic encryption and secure multiparty computation were identified, as well as vulnerability analysis tools that improve system security. Digital curation, awareness programs, and backup policies were also highlighted as essential components. Overall, the results suggest that protecting student data requires a comprehensive approach that combines legal frameworks, technical capabilities, and organizational culture. This review provides a solid conceptual foundation for developing effective strategies for educational data governance and recommends future research in real-world implementation scenarios.

KEYWORDS

data protection, educational cybersecurity, digital repositories, information security, higher education, ISO/IEC 27001, GDPR, homomorphic encryption

1 INTRODUCTION

The digitalization of educational services has changed how higher education institutions manage, store, and share information. This transformation began with the adoption of digital technologies and the growth of virtual learning environments, generating a growing dependence on institutional digital repositories as a means of maintaining academic records, personal data, research papers, and other valuable

Yamba-Yugsi, M., Ortega-Castro, J-C., Maldonado-Mahauad, J., Borja-Pozo, C. A. (2026). Strategies, Regulations and Mechanisms for Protecting Student Data in University Digital Repositories: A Systematic Review. *International Journal of Emerging Technologies in Learning (iJET)*, 21(3), pp. 4–15. https://doi.org/10.3991/ijet.v21i03.58977

Article submitted 2025-10-01. Revision uploaded 2026-03-23. Final acceptance 2026-03-23.

information assets [1]. Under this scenario, student information has been a critical target for different cybersecurity threats, including unauthorized access, accidental data loss, and malicious attacks such as ransomware or data exfiltration [2, 3].

Various studies have highlighted the limited availability of adequate security measures in the education sector, compared to more regulated sectors such as finance and healthcare [4, 5]. Despite the existence of regulatory and technical frameworks focused on these risks—such as the ISO/IEC 27001 standard for information security management or the European Union's General Data Protection Regulation (GDPR)—their adoption in universities remains technically and organizationally challenging [6, 7]. In addition, there are significant gaps in staff and student awareness, increasing institutional exposure to security incidents [3]. On the other hand, novel technological solutions have emerged aimed at enhancing information protection, including homomorphic encryption, which facilitates the processing of encrypted data without decrypting it, and secure multiparty computing (SMPC), which allows for collaborative data analysis without compromising the privacy of the parties involved [8, 9]. These technologies represent an important advance; however, their application in the university environment is still limited. Furthermore, the inclusion of methods such as role-based access control, vulnerability analysis tools, or secure backup and migration systems are relevant technical factors that require systematic evaluation [10, 11].

Although there have been attempts to improve the protection of university digital repositories, the scientific literature on this topic remains dispersed and focused on isolated case studies. To date, there is no systematic review that jointly addresses the different dimensions–regulatory, technological, and organizational–of data security in this area. This lack of integrative evidence limits the ability to plan comprehensive, evidence-based strategies to ensure the effective protection of student information.

Given this gap, the study presented here aims to conduct a systematic review of the scientific literature on strategies, regulations, and methods for protecting student information in university digital repositories. 30 selected research projects from recognized scientific databases were analyzed, covering topics such as risk management, the adoption of international standards, data governance, and the use of emerging technologies. The article provides an updated framework for scholars, institutional decision-makers, and policymakers and proposes future lines of research to improve cybersecurity in education.

1.1 Related work

The protection of student data in university digital repositories is a multifaceted issue encompassing various strategies, regulations, and mechanisms. A systematic literature review reveals significant insights into current practices and the challenges higher education institutions face in protecting student privacy. The following sections describe key aspects of this topic.

Regulatory frameworks. The GDPR is a cornerstone of data protection in the EU, as it requires educational institutions to identify and mitigate the risks associated with the processing of personal data [12].

The Spanish Law on Data Protection and the Guarantee of Digital Rights complements the GDPR, emphasizing the need for compliance in university settings [13].

Best practices and strategies. Universities are encouraged to adopt comprehensive data protection policies that include regular audits and staff training on data privacy [14, 15].

Implementing privacy-preserving techniques in educational data analysis can help balance data utility and student privacy, ensuring ethical data use.

Challenges and vulnerabilities. The rapid transition to online learning has introduced new vulnerabilities, necessitating robust security measures to protect sensitive student information [3].

Many institutions continue to display weaknesses in their data handling practices, highlighting the need to improve compliance with established regulations.

While significant progress has been made in establishing data protection frameworks, challenges remain, particularly in adapting to evolving technologies and ensuring comprehensive compliance across all university departments.

2 MATERIALS AND METHODS

This study was conducted using a systematic literature review, guided by the recommendations of the 2020 PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) declaration. This approach was chosen due to its structural rigor, transparency in source selection, and ability to synthesize academic data in a reproducible manner. The systematic review allowed us to identify, classify, and critically analyze the main risks, adopted solutions, and emerging trends related to data protection in digital repositories of higher education institutions.

To guide the review, the following question was posed: What strategies, regulatory frameworks, and technical solutions have been reported in the literature to protect student data stored in university digital repositories?

The search strategy was designed to obtain relevant scientific information from the following databases: Web of Science, Scopus, ACM Digital Library, and Consensus (as a complementary database). A combination of controlled and free terms, subject to Boolean operators, was used to expand coverage and precision. The general search string used was: ("student data" OR "student privacy" OR "data protection" OR "information security" OR "data governance" OR "privacy policy") AND ("repository" OR "digital repository" OR "data storage" OR "digital platform" OR "information system") AND ("university" OR "universities" OR "higher education" OR "academic institution"). Searches were conducted between April and May 2025, limiting results to the 2010–2025 period and tailored to the search language of each database.

The study selection process followed the PRISMA framework in three stages:

1. Study identification: records were retrieved through a systematic search of the selected databases.
2. Screening: titles, abstracts, and then full texts were reviewed. The review was conducted independently by two researchers. Discrepancies were resolved by consensus.
3. Inclusion: full-text studies were assessed to verify compliance with the inclusion criteria. Those that did not meet the requirements were excluded.

Inclusion criteria to ensure the relevance, quality, and pertinence of the selected studies:

- Academic publications between 2010 and 2025.
- Articles written in English or Spanish.
- Studies that explicitly address aspects related to data protection or information security in university digital repositories.
- Peer-reviewed articles indexed in recognized scientific databases.

The following exclusion criteria were applied:

- Non-refereed documents (technical reports, theses, and conference proceedings).
- Studies not focused on the university context.
- Publications without full-text access.

Relevant information was extracted using a structured matrix in Microsoft Excel, which included author, year of publication, country, objective, type of study, key findings, and recommendations.

The analysis of the information was carried out at two levels:

1. Qualitative thematic analysis to identify emerging categories and common patterns related to data protection challenges and strategies.
2. Descriptive bibliometric analysis to visualize the evolution of scientific production by year, country, and authorship. Excel and the VOSviewer tool were used for this purpose.

Although this systematic review did not involve primary data collection or direct interaction with human participants, the following ethical considerations were considered: only peer-reviewed studies that adhered to established ethical principles, including approval by ethics committees where applicable, were included; all articles were obtained from legal sources and respected copyright; and the selection and analysis process was objective and unbiased, ensuring integrity in the interpretation of the results.

3 RESULTS

After completing the systematic search and the selection process for relevant research, Figure 1 presents the PRISMA flowchart, which illustrates each stage of the review in detail. This diagram visualizes the path taken, starting with the initial identification of articles through their final refinement, culminating in the inclusion of 30 selected studies for analysis.

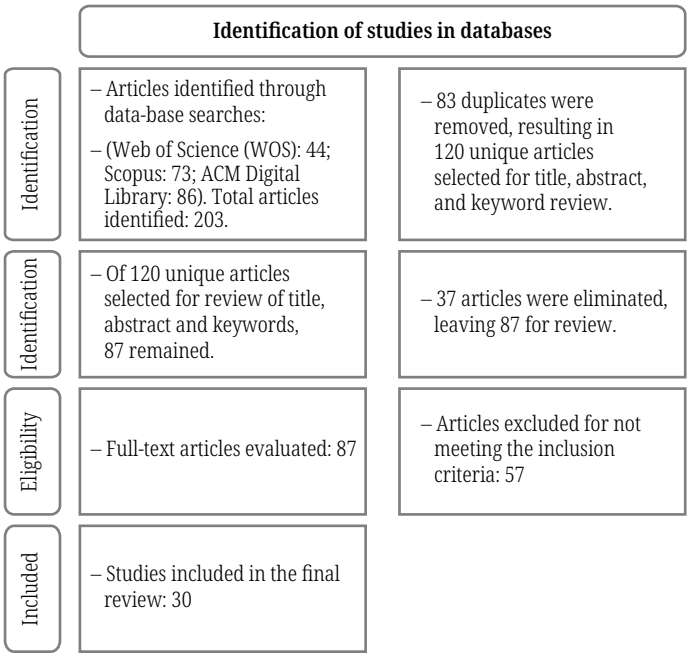

Fig 1. PRISMA flowchart of the study selection process

Protecting student information in university digital repositories is a key challenge that requires comprehensive strategies, robust regulatory frameworks, and advanced technical solutions. A combination of international standards, institutional policies, and encryption technologies is key to ensuring the security and privacy of student data.

3.1 Protection Strategies and Practices

Risk analysis and management. Organizations face challenges in ensuring compliance with information security policies (ISPs), including the need for trained personnel for security training and employee awareness regarding secure information handling practices [1].

The increasing frequency of cyberattacks on educational institutions highlights the importance of comprehensive risk management strategies for the protection of sensitive data. These strategies include continuous monitoring of technological assets, which allows for the timely detection and mitigation of vulnerabilities [1, 2].

Risk analysis allows for the identification of vulnerabilities and threats in digital repositories, generating a matrix that classifies risks based on their location and threat level, according to the probability of occurrence and impact, as well as the assessment of exposure in uncontrolled scenarios [2].

- Risk management strategies require the following:Avoid activities that generate risks.
- Transfer risks to third parties through mechanisms such as insurance or contracts.
- Implement technical and administrative controls to reduce the probability and impact of risks [2].

This systematic approach facilitates proactive threat mitigation and strengthens the security of digital resources.

Digital curation and preservation. Digital curation and preservation, guided by institutional policies, guarantee the long-term authenticity, integrity, and accessibility of student data [3, 16]. Therefore, digital preservation is key to protecting digital assets from disasters and ensuring their continued availability over time [16].

A relevant challenge in this area is digital obsolescence and the lack of trust in established standards, problems that have been critical since 2010 [16]. Therefore, it is important to promote staff awareness regarding compliance with security policies in order to protect information and minimize the risk of breaches or infractions [1].

Institutions must prioritize the protection of strategic assets, including critical systems and data. For this reason, it is important to have a well-structured cybersecurity framework to prevent unauthorized access and disruptions, contributing to institutional operational stability [7].

Education and awareness. Training students and staff in personal data protection and security best practices is essential to strengthening organizations' security posture [4, 5]. In this context, institutions must implement effective and engaging awareness programs that improve employees' ability to identify and assess threats, as well as to adopt appropriate information security behaviors [1].

These awareness programs are designed to actively promote compliance with security policies, encouraging responsible and conscious behaviors regarding the protection of data and technological resources [8]. Similarly, the importance of incorporating participatory methodologies that include feedback, dialogue, and reflection

is highlighted, as these strategies increase security awareness and improve compliance among employees [1].

3.2 Regulatory Frameworks

ISO/IEC 27001 and 27002. The international standards ISO/IEC 27001 and 27002 are recommended for managing information security in university repositories, facilitating risk identification, establishing controls, and monitoring technological assets [17]. Therefore, implementing a robust information security management system (ISMS), which includes risk treatment plans and periodic updates of security protocols, is key to ensuring compliance with these international standards [18].

The adoption of information security systems in higher education institutions is undergoing a complex evolution, influenced by the development of management information systems (MIS) and the growing need to protect sensitive data [19]. In this context, it is important to enhance employee awareness and encourage rigorous compliance with security policies to reduce breaches and vulnerabilities [20]. Together, ISO/IEC 27001 and ISO/IEC 27002 provide a comprehensive framework for effectively managing information security. While ISO/IEC 27001 focuses on management system requirements, ISO/IEC 27002 provides practical standards for implementing security controls. Adopting these standards protects confidential information and ensures compliance with legal and regulatory requirements, thereby strengthening customer confidence and protecting the institutional reputation [21].

General Data Protection Regulation (GDPR). Compliance with regulations such as the European GDPR requires data audits, the development of privacy policies, and transparency in the processing of personal information [6]. The GDPR, established in 2018, regulates the collection and processing of personal data of individuals in the European Union, including guidelines for the transfer of data outside its jurisdiction [10].

Organizations that handle personal data of European citizens must ensure compliance with the GDPR, which requires clear and accessible privacy statements. However, a study that analyzed 151 privacy statements from 78 higher education institutions found that only 54 of them explicitly mentioned the GDPR [10].

The implementation of data governance policies is critical to ensuring data quality and security, especially in the academic setting [16]. From this perspective, it is important to note that governance frameworks allow for the management of the entire data lifecycle, establishing clear rules and responsibilities for the use and protection of technological resources and sensitive information [8, 11]. Furthermore, student data is subject to multiple regulations, including the GDPR, which protects critical information such as profiles and academic records, ensuring their privacy and security [22]. In this context, it is important to discuss international standards and best practices in information security management to develop effective technical solutions that address the specific challenges of higher education institutions [22].

3.3 Technical Solutions

Homomorphic Encryption and SMPC. Homomorphic encryption (HE) and secure multiparty computation (SMPC) are emerging technologies that enhance data privacy in educational institutions. These techniques enable secure information

sharing and analysis, maintaining the confidentiality of sensitive data such as student records and comments. Their purpose is to process encrypted data and allow collaboration between institutions without exposing confidential information [23].

Regarding homomorphic encryption, its application in education guarantees data security by allowing calculations to be performed directly on encrypted data, preserving privacy throughout the analysis. For example, student comments can be analyzed without revealing individual responses [24]. Furthermore, recent advances have improved the efficiency of these systems, allowing large amounts of data to be processed quickly. Tools such as HomoPai demonstrate the ability to train machine learning models using encrypted data, optimizing the analysis of educational information [25].

On the other hand, SMPC facilitates collaborative analysis between different institutions, allowing aggregate statistics to be calculated without sharing individual data sets, which is particularly useful for managing shared student files [26]. Furthermore, the use of SMPC ensures compliance with data protection regulations, allowing institutions to share and analyze data securely and in compliance with current legislation [27].

Finally, mechanisms for security services based on hybrid cryptosystems that employ lossy crypto-code structures have been proposed, expanding the cryptographic capabilities applicable in this context [28].

Vulnerability analysis tools. The use of specialized vulnerability analysis tools is essential to strengthen the security of web repositories in educational environments. Software such as Acunetix allows for the identification and mitigation of vulnerabilities in institutional web applications [17].

Among the methods used, dynamic analysis stands out for simulating real-life user interactions with web pages, allowing for the detection of vulnerabilities in real time. This approach is more effective than static analysis, which often generates false positives and fails to identify security-critical functional parameters [6].

Another relevant technique is fuzz testing, which involves the automated injection of random or invalid data into applications to identify security flaws. This methodology is widely used due to its efficiency and low cost, without requiring complex reverse engineering [19].

In this case, penetration testing allows for the simulation of real attacks to assess the security of computer systems. This practice is common in organizations because it enables the detection and documentation of vulnerabilities before they are exploited by malicious actors [19].

Furthermore, black-box testing offers an external perspective on application security, as it is performed without prior knowledge of the source code, providing a comprehensive view of potential weaknesses [19].

A particularly critical attack vector is SQL injection, as it is considered one of the most common threats in web applications. For this reason, it is essential to have tools that can detect and mitigate these types of vulnerabilities [19].

Additionally, the application of data mining and clustering techniques allows for the identification of vulnerable patterns in user or system behavior, segmenting activities into groups with similar risk profiles and facilitating the implementation of specific security measures [29].

Embargo and selective access policies. These allow access to certain sensitive data or studies to be restricted until it is safe to publish them [5].

In addition, embargo policies restrict access to certain educational materials, such as theses and dissertations, for a specified period. Their objective focuses

on protecting intellectual property and confidential data during the publication process [30].

Institutions vary in their practices regarding the duration and conditions of embargoes, often influenced by institutional needs and legal frameworks. Information security policies are crucial for protecting confidential data, including student records and research results [9].

Data migration and backup. Data migration and backup are essential components of information security in educational institutions, especially to ensure data preservation and recovery in the event of technical failures or cyberattacks [3, 16].

The implementation of data loss prevention (DLP) systems is key in this context, as it allows for the analysis, control, monitoring, and protection of sensitive information. These systems ensure that migration processes do not expose confidential data, thus contributing to secure information management [31].

Likewise, the use of role-based access control (RBAC) is highlighted as an effective mechanism for protecting data during migration and backup tasks. This approach allows for the establishment of access policies tailored to institutional needs, ensuring that only authorized personnel access sensitive information at critical moments in the data lifecycle [10]. Transparency in data management processes also plays a crucial role, as it fosters trust among users and ensures compliance with regulations such as FERPA (Family Educational Rights and Privacy Act), which regulates the management and privacy of students' academic data in the educational field [32].

4 DISCUSSION

The results of this systematic review identify key trends and persistent challenges in information security management and data protection within higher education institutions. Considering previous research, the findings confirm the urgency of designing comprehensive approaches that combine robust regulations, advanced technologies, and an organizational culture focused on awareness and prevention.

Consistent with previous studies [1–4], the findings confirm that risk management remains a central pillar for ensuring the integrity of digital assets. The use of risk matrices, impact analysis, and asset monitoring allows for anticipating threats in an environment where cyberattacks are increasingly frequent. prevent incidents and reinforce regulatory compliance and informed decision-making.

In line with [2, 3, 7], the results highlight that digital curation and preservation must be conceived as an active and strategic process, especially in the face of threats such as technological obsolescence and accidental data loss. In this sense, the adoption of international standards such as ISO/IEC 27001 and 27002 has proven effective in structuring sound institutional policies [11]. However, as explained in previous studies, the effectiveness of these standards depends on their practical implementation and the degree of appropriation by the educational community.

Cybersecurity education and awareness, recognized as a critical factor in previous work [1, 5, 8], continues to be an area for improvement. The results show that traditional programs, focused on the one-way transmission of information, must shift toward participatory and contextual models that promote sustained behavioral transformations. This is especially relevant in academic environments where user autonomy is high.

From a regulatory perspective, the GDPR compliance analysis reveals a worrying gap between the legal framework and its effective implementation. Only a limited proportion of institutions explicitly mention the regulation in their policies [11], which

is consistent with studies that report a lack of alignment between legal obligations and institutional practice [16, 19]. This situation highlights the need to strengthen data governance mechanisms with clearer and more accountable frameworks.

At the technological level, there is growing interest in solutions such as homomorphic encryption and SMPC, which allow the analysis of sensitive data without compromising its confidentiality. Recent studies [18–21] have demonstrated their effectiveness in enabling secure inter-institutional collaborations. However, their widespread adoption remains limited by barriers such as technical complexity, computational costs, and limited specialized training.

Vulnerability analysis tools—such as dynamic analysis, fuzz testing, and penetration testing—confirm their usefulness in identifying weaknesses in institutional systems, in line with [8, 23]. Despite this, there remains a need to develop internal capabilities to interpret the findings and translate them into concrete actions.

Finally, the study reaffirms the importance of having effective data migration and backup policies, as argued in previous work [3, 25, 26]. The implementation of role-based access control (RBAC) mechanisms and transparency in data management contribute to strengthening institutional trust and regulatory compliance (FERPA, GDPR).

5 CONCLUSIONS

This systematic review provides a comprehensive perspective on the strategies, standards, and technologies used to protect data and ensure cybersecurity in higher education institutions. The results showed that data security cannot be addressed solely from a technical perspective but rather requires the integration of robust regulatory frameworks, emerging technologies, and an institutional culture focused on risk management, awareness, and data governance.

International standards such as ISO/IEC 27001 and 27002, when aligned with regulatory frameworks such as the GDPR, were found to provide a structured basis for determining data protection policies, despite the persistence of challenges in their effective implementation. Technologies such as homomorphic encryption and secure multiparty computation represent promising opportunities for protecting sensitive information, especially in inter-institutional collaboration scenarios. Likewise, the use of vulnerability analysis tools and secure backup and migration systems are key to maintaining the integrity and availability of digital assets.

However, the review revealed significant barriers to adopting these solutions, as well as a significant gap in awareness programs for staff and students.

Overall, the findings underscore the need to adopt a holistic and dynamic approach to information security management in the academic field, recognizing its fundamental role in protecting personal data, institutional reputation, and educational continuity.

5.1 Implications and future lines of research

These results imply important aspects for formulating institutional policies, designing curricular cybersecurity training programs, and developing technological systems tailored to the educational setting. In an environment of rapidly advancing digital transformation, schools must take a proactive and strategic approach to data protection.

Future research can study the practical application of technologies such as SMPC and homomorphic encryption in real-life university contexts, examining their technical feasibility, organizational impact, and cost-benefit ratio. It is also relevant to delve into empirical research related to the degree of regulatory compliance (e.g., GDPR, FERPA) in different regions and institutional levels. Furthermore, it was identified that it is urgent to analyze how organizational cultures influence the effectiveness of data security awareness programs.

6 ACKNOWLEDGMENT

The authors thank the Universidad Católica de Cuenca and the Universidad de Cuenca for their institutional support and for providing the necessary resources to conduct this systematic literature review. Special thanks to the Academic Postgraduate Unit for its commitment to research in educational cybersecurity.

7 REFERENCES

[1] A. Almuqrin, I. Mutambik, A. Alomran, and J. Z. Zhang, "Enforcing information system security: Policies and procedures for employee compliance," *International Journal on Semantic Web and Information Systems (IJSWIS)*, vol. 19, no. 1, pp. 1–17, 2023. https://doi.org/10.4018/ijswis.331396

[2] A. Khan, M. Ibrahim, and A. Hussain, "An exploratory prioritization of factors affecting current state of information security in Pakistani university libraries," *International Journal of Information Management Data Insights*, vol. 1, no. 2, p. 100015, 2021. https://doi.org/10.1016/j.jjimei.2021.100015

[3] E. N. Anyaoku, A. U. N. Echedom, and E. E. Baro, "Digital preservation practices in university libraries: An investigation of institutional repositories in Africa," *Digital Library Perspectives*, vol. 35, no. 1, pp. 41–64, 2019. https://doi.org/10.1108/dlp-10-2017-0041

[4] Y. N. Kuligin, "Data protection in the digital age: Ensuring the security of students' personal data," *Ekonomika I Upravlenie: Problemy, Resheniya*, vol. 10/3, no. 151, pp. 72–80, 2024. https://doi.org/10.36871/ek.up.p.r.2024.10.03.009

[5] D. Stern, "Student embargoes within institutional repositories: Faculty early transparency concerns," *Journal of Librarianship and Scholarly Communication*, vol. 2, no. 2, pp. 1–9, 2014. https://doi.org/10.7710/2162-3309.1080

[6] J. Cox, "Understanding GDPR: Libraries, repositories, & privacy policies," in *Proceedings of the 2018 DC-HUG Conference*, Fort Hays State University, 2018. https://doi.org/10.58809/ngrw4078

[7] J. S. Suroso and C. P. Prastya, "Cyber security system with SIEM and honeypot in higher education," *IOP Conference Series: Materials Science and Engineering*, IOP Publishing, vol. 874, no. 1, 2020, p. 012008. https://doi.org/10.1088/1757-899x/874/1/012008

[8] A. R. Ahlan, M. Lubis, and A. R. Lubis, "Information security awareness at the Knowledge-Based institution: Its antecedents and measures," *Procedia Computer Science*, vol. 72, pp. 361–373, 2015. https://doi.org/10.1016/j.procs.2015.12.151

[9] A. A. Ahmed and H. Abas, "Factors influencing information security policy compliance behavior in high education institutions: Systematic literature review," *Advances in Social Sciences Research Journal*, vol. 11, no. 7, pp. 260–273, 2024. https://doi.org/10.14738/assrj.117.17308

[10] M. Francis, M. Avoseh, K. Card, L. Newland, and K. Streff, "Student privacy and learning analytics: Investigating the application of privacy within a student success information system in higher education," *Journal of Learning Analytics*, vol. 10, no. 3, pp. 102–114, 2023. https://doi.org/10.18608/jla.2023.7975

[11] M. Bylina, E. Podwysocki, and M. Michajłowicz, "Data Governance at the National Information Processing Institute in Poland," *EPiC Series in Computing*, vol. 25, pp. 79–88, 2023.

[12] A. Cerrillo i Martínez, "The protection of personal data at the University from the perspective of a university ombudsman," *Rev. Univ. Ética Derechos*, nos. 4–5, pp. 58–74, 2019. Available: https://revistas.uca.es/index.php/Rueda/article/view/5425

[13] E. Nikolova, M. M. Zheleva, and Y. Zhelev, "Personal data processing in a digital educational environment," *Math. and Comp. Sc.*, vol. LXV, no. 4, pp. 365–378, 2022. http://dx.doi.org/10.53656/math2022-4-4-per

[14] C. Varela-Orol and R. Ameneiros Rodríguez, "Personal data protection in Spanish university libraries in the digital environment," *Rev. Gen. Inf. Docum.*, vol. 28, no. 2, pp. 685–702, 2018. https://doi.org/10.5209/RGID.62844

[15] M. M. Ncube and P. Ngulube, "A systematic review of postgraduate programmes concerning ethical imperatives of data privacy in sustainable educational data analytics," *Sustainability*, vol. 16, no. 15, p. 6377, 2024. https://doi.org/10.3390/su16156377

[16] J. S. Lima, F. Molina-Granja, R. Lozada-Yanez, D. Velasco, G. A. Peñafiel, and L. P. Castelo, "The importance of the digital preservation of data and its application in universities," in *Knowledge Management in Organizations: 15th International Conference*, Kaohsiung, 2021.

[17] A. F. Setyowardhani, I. Nurlela, J. Primaranti, V. Ghrandiaz, and Y. Yulhendri, "Analisis Resiko Keamanan Informasi Website Repository Digital Library Menggunakan Framework ISO/IEC 27001 & 27002: Studi Kasus Perguruan tinggi X," *Jurnal Riset Multidisiplin dan Inovasi Teknologi*, vol. 2, no. 1, pp. 327–373, 2023.

[18] L. Hernandez Collante, A. Pranolo, and A. Prasetya Wibawa, "Implementation plan of the information security management system based on the NTC-ISO-IEC 27001:2013 standard and security risk analysis. Case study: Higher education institution," *Transactions on Energy Systems and Engineering Applications*, vol. 5, no. 2, pp. 1–20, 2024. https://doi.org/10.32397/tesea.vol5.n2.635

[19] Y. C. Cho, "Implementation and analysis of website security mining system, applied to universities academic networks," *Tehnički vjesnik*, vol. 22, no. 2, pp. 279–287, 2015.

[20] R. Gött *et al.*, "3LGM2IHE: Requirements for data-protection-compliant research infrastructures—A systematic comparison of theory and practice-oriented implementation," *Methods of Information in Medicine*, vol. 61, no. S 02, pp. e134–e148, 2022. https://doi.org/10.1055/a-1950-2791

[21] N. Nurbojatmiko *et al.*, "Risk assessment maturity level of academic information system using ISO 27001 system security engineering-capability maturity model," *Journal of Applied Engineering and Technological Science (JAETS)*, vol. 5, no. 2, pp. 941–954, 2024. https://doi.org/10.37385/jaets.v5i2.2971

[22] G. Melançon, N. Pinède, and U. Verdi, "Redefining data Governance: Insights from the French University System," in 26*th International Conference on Enterprise Information Systems (ICEIS)*, Angers, 2024.

[23] W. Chen, J. Zuo, S. Su, and C. Chen, "A privacy-preserving across-institution archives utilization framework and implementation," in *2024 IEEE Cyber Science and Technology Congress (CyberSciTech)*, IEEE, 2024, pp. 138–145. https://doi.org/10.1109/cyberscitech64112.2024.00031

[24] S. A. Hegde, N. N. Shetty, P. N. Soma, N. N. Naik, H. N. Ramachandra, and K. S. Shivaprakasha, "Privacy preserving student feedback system using homomorphic encryption," in *2024 Second International Conference on Networks, Multimedia and Information Technology (NMITCON)*, IEEE, 2024, pp. 1–5. https://doi.org/10.1109/nmitcon62075.2024.10699172

[25] Q. Li *et al.*, "Homopai: A secure collaborative machine learning platform based on homomorphic encryption," in *2020 IEEE 36th International Conference on Data Engineering (ICDE)*, IEEE, 2020, pp. 1713–1717. https://doi.org/10.1109/icde48307.2020.00152

[26] J. Li, L. Yao, T. Zhou, and R. Li, "Homomorphic encryption-based privacy-protecting multi-institution data classification method," 2020.

[27] S. Pandey, H. Azath, R. U. Rahman, and H. Lamkuche, "Homomorphic encryption and secure multi-party computation: Mathematical tools for privacy-preserving data analysis in the cloud," in *14th International Conference on Communication Systems and Network Technologies*, Bhopal: IEEE, 2025, pp. 437–442.

[28] S. Yevseiev *et al.*, "Development of a methodology for building an information security system in the corporate research and education system in the context of university autonomy," *Eastern-European Journal of Enterprise Technologies*, vol. 3, no. 9 (99), pp. 49–63, 2019. https://doi.org/10.15587/1729-4061.2019.169527

[29] V. Lakhno *et al.*, "Analysis of digital footprints associated with cybersecurity behavior patterns of users of university information and education systems," *International Journal of Electronics and Telecommunications*, vol. 70, no. 3, pp. 673-682, 2024. https://doi.org/10.24425/ijet.2024.149596

[30] S. Miskam, N. Sholehuddin, F. Mohd Shahwahid, T. N. Raja Abdul Aziz, and N. Mansor, "Data privacy practices of private higher education institutions in Malaysia: A preliminary study," *Malaysian Journal of Information and Communication Technology (MyJICT)*, vol. 8, no. 2, pp. 88-99, 2023. https://doi.org/10.53840/myjict8-2-99

[31] A. Boranbayev, M. Mazhitov, and Z. Kakhanov, "Implementation of security systems for prevention of loss of information at organizations of higher education," in *2015 12th International Conference on Information Technology – New Generations*, IEEE, 2015, pp. 802–804. https://doi.org/10.1109/itng.2015.147

[32] J. I. Galchynskyi and M. Sturchak, "Data protection in the information model of the 'Department' module of the university automated information system," *Information Technologies and Learning Tools*, vol. 1, no. 99, pp. 95–117, 2024.

8 AUTHORS

Marco Yamba-Yugsi is the technical coordinator at the Academic Postgraduate Unit of the Universidad Católica de Cuenca, Cuenca, Ecuador (E-mail: marco.yamba@ucacue.edu.ec).

Juan-Carlos Ortega-Castro is the Coordinator of the Master's program in Cybersecurity at the Academic Postgraduate Unit of the Universidad Católica de Cuenca, Cuenca, Ecuador (E-mail: jcortegac@ucacue.edu.ec).

Jorge Maldonado-Mahauad holds a PhD in Engineering Sciences and is the Director of Educational Innovation at the Universidad de Cuenca, Cuenca, Ecuador (E-mail: jorge.maldonado@ucuenca.edu.ec).

Cornelio Agustín Borja-Pozo holds a PhD in law and is the rector of the Universidad Católica de Cuenca, Cuenca, Ecuador (E-mail: cborjap@ucacue.edu.ec).