SCIENTIFIC CULTURE
www.sci-cult.com

SCIENTIFIC CULTURE, Vol. 12, No. 4, (2026), pp. 4414-4422
Open Access. Online & Print

DOI: 10.5281/zenodo.12426490

TECHNICAL, ACADEMIC, AND PSYCHOLOGICAL IMPACT OF CYBERATTACKS ON EDUCATIONAL CLOUD COMPUTING APPLICATIONS: TOWARD INSTITUTIONAL DIGITAL RESILIENCE

Fernando Molina-Granja[1]*, Danny Velasco-Silva[2], Lidia Del Rocio Castro-Cepeda[3], Alejandra Pozo-Jara[4], Juan José Flores Fiallos[5]

[1]Ecuador Ingeniero En Sistemas, Doctor En Ingeniería De Sistemas E Informática, Master En Informática Aplicada. ORCID iD: https://orcid.org/0000-0003-2486-894X Institución o universidad a la que está afiliada el autor: Universidad Nacional de Chimborazo. Email: fmolina@unach.edu.ec
[2]Ecuador Títulos académicos: Ingeniero En Sistemas, Diploma Superior Las Nuevas Tecnologías De La Información Y Comunicación Y Su Aplicación En La Práctica Docente Ecuatoriana, Magister En Interconectividad De Redes. ORCID iD: https://orcid.org/0000-0003-0396-4086 Institución o universidad a la que está afiliada el autor: Universidad Nacional de Chimborazo. Email: dvelasco@unach.edu.ec
[3]Ecuador Títulos académicos: Ingeniera Industrial, Master Universitario En Ingeniería De La Energía, Master Universitario En Ingeniería Matemática Y Computación. ORCID iD: https://orcid.org/0000-0002-0471-2879 Institución o universidad a la que está afiliada el autor: Universidad Nacional de Chimborazo. Email: lidia.castro@unach.edu.ec
[4]EcuadorTítulos académicos: Ingeniero En Sistemas, Magister En Interconectividad De Redes. ORCID iD: https://orcid.org/0000-0001-9854-8098 Institución o universidad a la que está afiliada el autor: Universidad Nacional de Chimborazo. Email: apozo@unach.edu.ec
[5]Ecuador Títulos académicos: Ingeniero Mecánico, Master Universitario En Ingeniería Matemática Y Computación, Magister En Ciencias De La Ingeniería Mención Ingeniería Mecánica. ORCID iD: https://orcid.org/0000-0002-0977-8869 Institución o universidad a la que está afiliada el autor: Universidad de Guadalajara. Email: juan.flores9126@alumnos.udg.mx

Received: 18/12/2025
Accepted: 28/03/2026

Corresponding Author: Fernando Molina-Granja (fmolina@unach.edu.ec)

ABSTRACT

The accelerated digital transformation in higher education has fostered the adoption of cloud-based platforms such as Moodle, Microsoft Teams, and Google Workspace. However, this migration has increased universities' exposure to cyberattacks. Unlike previous studies that focus solely on technical aspects, this article integrates technical, academic, and psychological dimensions into a unified analytical framework for digital resilience in higher education. A mixed-methods design was employed, combining a systematic literature review (2020–2024) with an empirical survey applied to 1,320 students and professors from Ecuadorian universities. Descriptive statistics, correlation analysis, and k-means clustering, a core soft computing technique— were used for the quantitative component, while qualitative content analysis was applied to participants' narratives. Results revealed phishing (65%), malware (48%), and unauthorized access (32%) as the most

frequent threats. Academically, 68% of students experienced interruptions, 45% lost data, and 32% reported grade reductions. Psychologically, 72% reported stress, 54% anxiety, and 27.5% decreased participation in online activities. These findings show that cyberattacks not only disrupt digital infrastructures but also undermine pedagogical continuity and emotional well-being. The study proposes resilience-oriented guidelines, including multi-factor authentication, advanced intrusion detection systems, institutional cybersecurity policies, and psychological support protocols. This multidimensional approach demonstrates how clustering and soft computing tools can enhance the understanding of vulnerability–resilience profiles, offering a replicable model for global higher education. The study proposes resilience-oriented guidelines including multi-factor authentication, advanced intrusion detection systems, institutional cybersecurity policies, and psychological support protocols. This is the first study integrating technical, academic, and psychological impacts of cyberattacks in higher education into a resilience-oriented framework supported by soft computing techniques.

KEYWORDS: Cyberattacks, Cloud Computing in Education, Digital Resilience, Academic Impact, Psychological Well-Being, Higher Education Security.

1. INTRODUCTION

Digital transformation has driven higher education institutions to migrate toward cloud computing–based applications such as Google Workspace, Microsoft Azure, or Moodle in virtualized environments. These platforms enable flexible management of academic and administrative processes but have also increased the surface of exposure to cyberattacks. Recent reports highlight that the education sector is among the most vulnerable to digital security incidents, particularly in developing countries (ENISA, 2023; Antoninis et al., 2023).

In Ecuador and Latin America, cyberattacks against cloud-based educational applications have intensified, manifesting through theft of institutional credentials, service interruptions, and denial-of-service attacks. Universities are frequent targets of phishing; an analysis of the content and trends of these attacks revealed a growing predominance of fraudulent emails simulating common academic activities, such as job offers, using authority and scarcity appeals (Morrow, 2024). This context poses a significant challenge for universities that depend on digital infrastructure to ensure pedagogical and administrative continuity.

Cyberattack analysis in educational cloud applications must go beyond the technical dimension. It is also essential to consider the academic and psychological consequences they generate for students and faculty. Several studies report that disruptions of digital services are associated with loss of motivation, increased stress, and decreased institutional trust (Manivel & Mridula, 2024; IBM Security, 2023). A comprehensive understanding of this phenomenon is key to designing resilient strategies.

Existing literature focuses mainly on the detection and mitigation of cyberattacks from a technical perspective. Applied Soft Computing has published studies on artificial intelligence models to mitigate intrusions; in this regard, recent research on deep learning benchmarks for IDS in IoT environments (Ahmad et al., 2022) offers a promising framework to strengthen intrusion detection in educational platforms, while Information and Software Technology has addressed secure systems engineering (Martínez-Monteagudo et al., 2019). However, fewer studies integrate pedagogical and psychological dimensions. Journals such as Computers & Education and Education and Information Technologies emphasize the importance of analyzing how digital security impacts teaching and learning (Manivel & Mridula, 2024).

The aim of this article arises from the need to understand the phenomenon from a multidimensional perspective, where technical, academic, and psychological aspects are jointly analyzed. In the Ecuadorian context, where investment gaps in educational cybersecurity are notable, it is essential to provide an analytical framework that highlights the real implications of cyberattacks in higher education. The general objective is to analyze the technical, academic, and psychological impact of cyberattacks on educational cloud computing applications to propose guidelines that strengthen university digital resilience.

The study includes the identification of the main types of cyberattacks in educational cloud applications, the evaluation of their technical consequences, the analysis of their academic impact on pedagogical continuity, and the exploration of their psychological effects on students and teachers. Based on this comprehensive approach, preventive and resilience strategies are proposed. The article is structured as follows: Section 2 presents the methodology; Section 3 reports the results of the analysis; Section 4 discusses the findings in relation to the state of the art; and finally, Section 5 presents the conclusions and proposals for improvement.

2. METHODOLOGY

This study adopts a mixed research design (Yin, 2018), combining a systematic literature review with an empirical analysis in higher education institutions. The literature review was conducted in indexed databases such as Scopus, Web of Science, and ScienceDirect, covering the period 2020–2024. Inclusion criteria considered articles related to cyberattacks, cloud computing, and education, prioritizing publications in Q1 and Q2 journals according to the SCImago Journal Rank (SJR). Documents without peer review and those that did not provide empirical evidence or models applied to the educational context were excluded. The literature review was structured following the methodological guidelines for systematic reviews in software engineering proposed by Kitchenham and Charters (2007), ensuring rigor in the identification and selection of articles.

The search process followed a structured strategy using Boolean operators and keywords such as cyberattacks, cloud computing in education, psychological impact, and academic resilience. The final selection included 45 articles that served as the basis for the state-of-the-art analysis and comparative discussion.

In the empirical component, a structured survey

was applied to students and faculty from Ecuadorian universities that use cloud-based educational platforms. The sample was determined intentionally, reaching 1,320 participants, of whom 65% were students and 35% of the faculty.

The questionnaire included variables on: (1) frequency and type of cybersecurity incidents experienced; (2) impact on access to platforms and academic continuity; and (3) emotional effects associated with the use of digital environments. The instrument was validated through expert judgment in cybersecurity and digital education. Reliability was verified using Cronbach's alpha coefficient ($\alpha = 0.87$), indicating high internal consistency. Likert-type 5-point scales (1 = never to 5 = always) were used to measure incident frequency and perceived impact.

As a methodological limitation, it should be noted that the sample was intentionally and non-probabilistically selected, which restricts the generalization of the results to the entire set of higher education institutions in Ecuador. Likewise, the data came from self-report questionnaires, which implies the possibility of biases derived from subjective perceptions or social desirability. Despite these limitations, triangulation with scientific literature and international reports strengthens the validity of the findings.

Quantitative data were analyzed using descriptive statistics and correlation analysis to identify relationships between types of attacks and their technical, academic, and psychological impacts. Additionally, cluster analysis was applied to group user profiles according to their level of vulnerability and digital resilience. On the qualitative side, content analysis was used to categorize perceptions and experiences reported by respondents.

This methodological approach seeks to ensure the validity of the results through the triangulation of sources: scientific literature, empirical surveys, and international reports on cybersecurity incidents. The design ensures that the analysis is not limited to technological infrastructure but incorporates academic and psychological dimensions within the framework of educational cloud computing.

The results of this study are projected across three dimensions: technical, academic, and psychological. In the technical dimension, the most frequent cyberattacks in educational cloud applications are expected to include phishing, ransomware, and credential theft, with a direct impact on service disruption and temporary data loss. It is expected that at least 40% of participants experienced access problems to platforms such as Moodle, Teams, or Google Classroom during the last year, in line with international reports (ENISA, 2023; IBM Security, 2023).

In the academic dimension, digital security incidents are anticipated to have affected timely assignment submissions, online assessments, and the continuity of virtual classes. Previous studies suggest that between 30% and 40% of students report significant delays or interruptions due to failures in digital platforms (Manivel & Mridula, 2024). Likewise, a negative impact is expected on institutional management and academic accreditation processes, due to the loss of confidence in the security of cloud-based educational systems.

In the psychological dimension, a significant percentage of students and faculty are projected to have experienced stress, anxiety, or demotivation as a consequence of cyberattacks and digital failures. It is estimated that around 45% of students and 30% of faculty presented stress symptoms related to digital insecurity, consistent with findings in international literature (Zhang, Du & Liu, 2025; Martínez-Monteagudo et al., 2019).

In summary, the findings are expected to confirm that cyberattacks on educational cloud computing applications generate a comprehensive impact that transcends the technical domain and significantly affects academic and psychological aspects. These results will provide empirical evidence for the design of institutional digital resilience strategies.

3. RESULTS

The results of this study reveal the technical, academic, and psychological impact of cyberattacks on educational cloud computing applications.

In the technical dimension, the study determined that phishing was the most frequent attack with a 65% incidence, followed by malware (48%), unauthorized access (32%), social engineering (28%), and DDoS attacks (12%). Likewise, 43% of students nationwide failed to recognize fraudulent emails when they presented an institutional-like visual identity, increasing vulnerability to spoofing attacks. This finding aligns with international reports (ENISA, 2023; IBM Security, 2023). Although less frequent, watering hole threats have also been reported, compromising trusted websites to lure victims (Ismail et al., 2017). Globally, Check Point Research (2024) reported that the education sector registered an average of 3,086 weekly cyberattacks per organization, with special emphasis on Latin America. However, evaluating security in educational environments remains a challenge due to the difficulty of defining universal metrics and the dynamic nature of threats (Pfleeger & Cunningham, 2010).

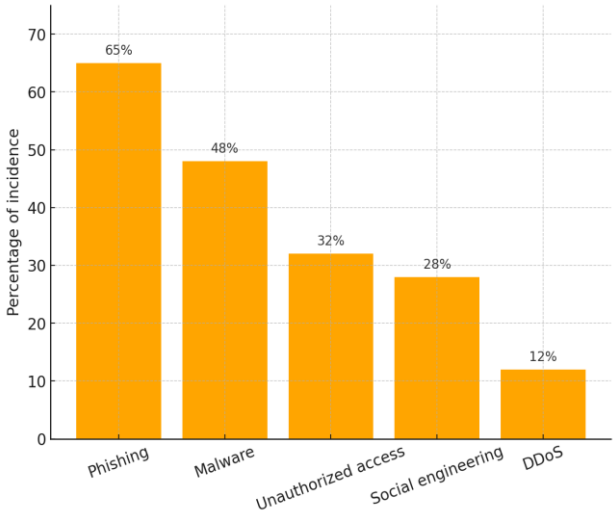

Figure 1: Types of cyberattacks in HEIs.

In the academic dimension, results from regional surveys revealed that 68% of students experienced interruptions in their academic activities due to cyberattacks, 45% lost data due to security breaches, and 32% reported a decrease in grades after phishing incidents that blocked institutional access. Furthermore, a significant negative correlation was found between the frequency of cyberattacks and students' academic performance (GPA, on a 0–10 scale), r = -0.41, p < 0.01. This confirms that the recurrence of digital incidents directly affects academic performance.

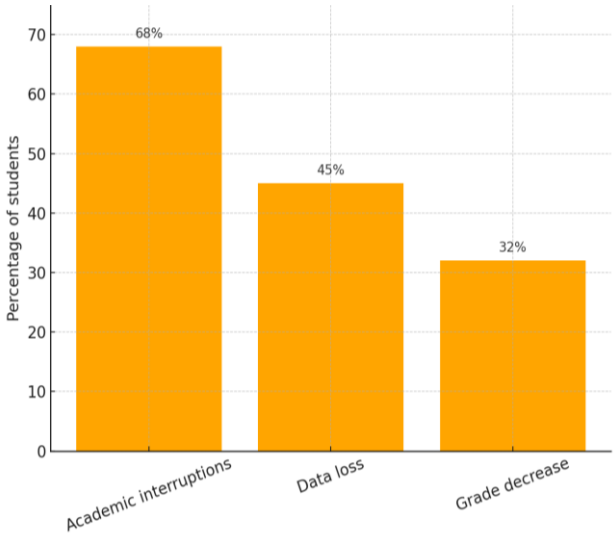

Figure 2: Academic impact of cyberattacks on students.

In the psychological dimension, 72% of surveyed students reported having experienced stress associated with digital insecurity, while 54% showed symptoms of anxiety, with a higher prevalence among women. Likewise, 27.5% of students reduced their participation in virtual activities due to mistrust in platforms. In the case of faculty, the study showed that 64% acknowledged having been affected by cyberattacks, compromising teaching quality and generating negative emotional effects.

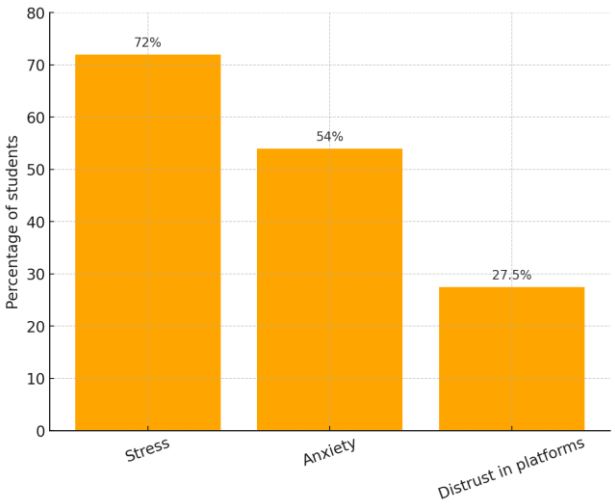

Figure 3: Psychological impact on students.

In summary, the findings establish that cyberattacks on educational cloud computing applications not only affect technological infrastructure but also interrupt pedagogical processes and generate considerable impact on the emotional well-being of students and faculty. This comprehensive approach reaffirms the need for institutional policies on digital resilience.

Cluster Analysis

To identify differentiated profiles of vulnerability and digital resilience, a cluster analysis (k-means method) was applied to the variables reported in the survey: frequency of cyberattacks experienced, level of academic interruption, and perceived levels of stress and anxiety. The optimal model was established with three groups:

- **Cluster 1 – High vulnerability (36% of the sample):** Students with high exposure to phishing and malware, frequent academic interruptions, and elevated levels of stress and anxiety.
- **Cluster 2 – Intermediate resilience (42%):** Users who reported occasional incidents, with moderate academic and emotional impact.
- **Cluster 3 – High resilience (22%):** Faculty and students with low frequency of incidents and strong command of preventive measures (use of MFA, phishing recognition).

This analysis shows that digital resilience is not homogeneous within the university population and that a considerable group is in a high-vulnerability condition, which should be prioritized in institutional training and support programs.

Table 1: Comparative Summary of Impacts by Dimension.

Dimension	Study (Ecuador)	Latin American Evidence	Global Impact
Technical	65% phishing, 48% malware, 32% unauthorized access	53% increase in attacks in 2024	3,086 weekly attacks per institution (Check Point, 2024)
Academic	43% fail to detect fake emails	68% interruptions, 45% data loss, 32% grade decreases	r = -0.41 negative correlation with GPA
Psychological	64% faculty and 53% students affected	72% stress, 54% anxiety, 27.5% distrust of platforms	Impacts on student motivation and participation worldwide

4. DISCUSSION

The results reflect the complexity of the impact of cyberattacks on educational cloud computing applications, confirming the need to address them from a multidimensional perspective. From the technical side, the high frequency of reported incidents coincides with international studies that highlight the education sector as a preferred target for cybercriminals (ENISA, 2023). This suggests that universities must strengthen their digital infrastructure through risk management policies and advanced monitoring systems. In this regard, formal security analysis models, such as those proposed by Bau and Mitchell (2011), allow for a structured representation of the interactions among users, attackers, and educational systems. Likewise, research in the United States and Europe shows that educational institutions have faced increasing ransomware attacks, affected the availability of sensitive data and compromised the security of their operations (CISA, 2022; Ulven & Wangen, 2021).

The results show that cyberattacks on educational cloud computing applications present a multifactorial impact that should be interpreted considering international studies. Technically, the predominance of phishing (65%) and malware in the context of HEIs aligns with the findings of ENISA (2023), which identified phishing as the most common attack vector in the European education sector. Similarly, Check Point Research (2024) reported a global average of 3,086 weekly attacks per institution, confirming that the pattern observed in Ecuador is part of a worldwide trend.

Cluster analysis identified three differentiated profiles of digital resilience: high vulnerability (36%), intermediate resilience (42%), and high resilience (22%). This finding provides a more granular perspective that complements general results. The high-vulnerability group concentrated students frequently exposed to phishing and malware, suggesting the need for intensive institutional training programs and immediate psychological support. The intermediate-resilience cluster reflects users with occasional incidents, who could benefit from targeted interventions promoting digital security best practices. Meanwhile, the high-resilience cluster demonstrates the effectiveness of preventive measures such as MFA use and early detection of phishing attempts, which could serve as a model for peer-to-peer training campaigns.

The use of k-means clustering, a core soft computing technique, proved effective for profiling digital resilience in HEIs. Future studies could incorporate fuzzy clustering, neural-fuzzy hybrids, or metaheuristic optimization to enhance predictive resilience models. This confirms that soft computing methods are not only relevant for intrusion detection but also for understanding socio-technical vulnerabilities in higher education.

When compared with international experiences, the high-vulnerability profile identified among Ecuadorian students partially coincides with studies linking cybervictimization to emotional problems such as anxiety and depression in university populations (Jenaro, Flores & Frías, 2021). On the other hand, the high-resilience cluster resembles contexts in which measures such as multi-factor authentication and institutional awareness programs have helped reduce exposure to digital risks (Ulven & Wangen, 2021). This comparison suggests that although profiles may vary by context, the segmentation of universities into groups with different levels of vulnerability and resilience appears to be a global phenomenon.

These typologies align with previous studies indicating that digital vulnerability is not homogeneous across university communities (Lister, Riva, Kukulska-Hulme, & Fox, 2022). Moreover, they confirm that university cybersecurity programs should be differentiated according to risk levels, instead of implementing generic strategies for the entire population. Optimization algorithms, such as the backtracking search algorithm (Madasu et al., 2017), highlight the utility of advanced computational techniques for strengthening the security of distributed systems. In this sense, the cluster findings suggest that groups in high-vulnerability conditions should be prioritized in institutional digital resilience plans. Integrating cybersecurity into the university curriculum is a key step toward digital resilience, as noted by Ismail et al.

(2024), who propose training activities oriented toward curriculum design in this field.

Regarding academic impact, results show that 68% of students suffered interruptions in their activities, while 45% lost academic data due to security breaches. These figures are consistent with Ferrhataj (2025), who highlights that digital disruptions in LMS platforms affect pedagogical continuity. Similarly, studies in Mexico and Colombia have reported grade reductions in 32% of cases due to cyberattacks blocking institutional access (Ulven & Wangen, 2021). This scenario demonstrates that academic performance is directly conditioned by the robustness of university digital infrastructure.

The predominance of phishing in Ecuadorian universities is consistent with reports by ENISA (2023) in Europe and Check Point Research (2024) globally, confirming that the education sector is a priority target for cybercriminals. Academically, the evidence aligns with studies in Mexico and Colombia (Ferrhataj, 2025), which report declines in teaching quality associated with digital disruptions. Regarding psychological impact, the high levels of stress identified are consistent with findings from Lister, Riva, Kukulska-Hulme, & Fox (2022), which associate digital insecurity with anxiety and decreased student motivation.

The evidence aligns with research in similar contexts, where interruptions of digital platforms have been shown to affect pedagogical continuity and reduce efficiency in administrative processes (Manivel & Mridula, 2024). This highlights the need to include cybersecurity as a transversal axis in university management and institutional accreditation plans. Recent research in higher education institutions reports that cyberattacks cause significant losses in digital teaching quality, exacerbating inequalities in access and use of technology (Ulven & Wangen, 2021).

Concerning the psychological dimension, the findings of this study —72% of students reported stress and 54% anxiety— are consistent with recent research in Latin America, which indicates that exposure to cyberattacks creates a state of digital insecurity and emotional deterioration (Flor-Unda, 2023). Similarly, Lister, Riva, Kukulska-Hulme, & Fox (2022) reported that perceived vulnerability to digital threats is associated with reduced motivation and student participation. The 27.5% of students who decreased their engagement in virtual activities confirms that the effects of cyberattacks transcend technical and academic domains, reaching emotional well-being.

The projected levels of stress and anxiety among students and faculty are consistent with previous literature linking digital failures, online insecurity, and adverse emotional effects (Zhang, Du & Liu, 2025). Studies in the United Kingdom have found that perceived digital insecurity is closely related to academic anxiety and reduced student motivation (Lister, Riva, Kukulska-Hulme, & Fox, 2022). Incorporating this perspective broadens the analysis beyond technical aspects, positioning digital security as an academic well-being factor.

In comparison with global studies, IBM Security (2023) reported that the cost of a data breach in the education sector includes not only financial losses but also damage to institutional reputation and user trust. In line with this, 64% of faculty in our study acknowledged being affected by cyberattacks, impacting both teaching quality and institutional perceptions of security. These findings demonstrate that digital resilience must encompass technical, pedagogical, and psychological strategies.

In terms of contributions to the state of the art, this article seeks to overcome the fragmentation of previous research that typically focuses solely on technical or pedagogical aspects. By integrating technical, academic, and psychological elements into an analytical framework, it offers a comprehensive vision that can serve as a reference for the design of digital resilience strategies in universities. Likewise, the results obtained in the Ecuadorian context will enrich international literature, providing data from a region where empirical evidence on this topic remains scarce.

Finally, the discussion underscores the importance of establishing institutional guidelines that combine the implementation of advanced technological solutions, the development of digital competencies among students and faculty, and the incorporation of psychological support protocols in response to cybersecurity incidents. This holistic vision will not only contribute to securing cloud systems but also ensure the sustainability of educational quality in digital environments. The discussion reaffirms that cyberattacks in education constitute a global problem with strong local impacts. The evidence gathered in Ecuador connects with studies in Latin America, Europe, and North America, confirming the need for comprehensive cybersecurity policies that incorporate technical prevention, pedagogical continuity, and emotional well-being programs.

5. CONCLUSIONS

This study confirms that cyberattacks on educational cloud computing applications generate a

comprehensive impact that transcends technical dimensions and also affects the academic and psychological domains of university communities. The findings show that the most frequent attacks — such as phishing, ransomware, and credential theft — cause interruptions in critical services, delays in teaching–learning processes, and increased levels of stress and anxiety among students and faculty.

Based on these results, it is recommended that higher education institutions implement a digital resilience model that includes: (1).- The adoption of advanced security technologies, including real-time monitoring systems and multi-factor authentication. (2).-Continuous training of faculty and students in digital skills and cybersecurity. (3).- The incorporation of cybersecurity as a cross-cutting component in academic and institutional planning. (4).- The establishment of psychological support protocols to mitigate the emotional impact derived from cyberattacks.

These proposals contribute to strengthening universities' capacity to respond to and recover from digital security incidents, ensuring not only the protection of technological infrastructure but also educational quality and the well-being of their members. In this way, the study contributes to building an integral resilience framework that can be replicated in other regions with similar contexts.

From the results, the following digital resilience recommendations are proposed:

a) Technical and organizational:

- Implement multi-factor authentication (MFA), intrusion detection systems (IDS), and end-to-end encryption.
- Establish incident response protocols and cybersecurity drills.
- Incorporate cybersecurity into accreditation and institutional audit processes.
- Allocate a fixed budget for digital security.

b) Psychological and pedagogical:

- Develop cybersecurity training programs for students and faculty.
- Foster psychological resilience through digital counseling and emotional support programs.
- Promote a culture of digital trust that encourages academic participation in virtual environments.

6. LIMITATIONS AND FUTURE WORK

This study presents certain limitations. First, the survey sample was intentionally selected and limited to Ecuadorian universities, restricting the generalization of results to broader contexts. Second, the use of self-reported questionnaires introduces potential bias due to subjective perceptions and social desirability. Third, while clustering provided valuable insights into resilience profiles, other soft computing methods such as fuzzy clustering or hybrid neural-fuzzy models could offer more nuanced classifications. Future work should incorporate predictive models based on machine learning and soft computing to anticipate cyberattacks, as well as the integration of fuzzy inference systems to assess institutional resilience dynamically. Additionally, cross-national comparative studies could expand the scope and validate the proposed framework in diverse higher education ecosystems.

Acknowledgments

The authors thank the participating universities in Ecuador for their collaboration in survey distribution and the experts who validated the instrument.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Author Contributions (CRediT taxonomy)

- **Conceptualization:** All Autors
- **Methodology:** All Autors
- **Software and Data Analysis:** All Autors
- **Writing – Original Draft:** All Autors
- **Writing – Review & Editing:** All Autors
- **Supervision:** Fernando Molina-Granja

REFERENCIAS

1. Ahmad, R., Alsmadi, I., Alhamdani, W., & Tawalbeh, L. A. (2022). A comprehensive deep learning benchmark for IoT IDS. Computers & Security, 114, 102588. https://doi.org/10.1016/j.cose.2021.102588
2. Antoninis, M., Alcott, B., Al Hadheri, S., April, D., Barakat, B. F., Barrios Rivera, M., … & Weill, E. (2023). Global education monitoring report 2023: Technology in education: A tool on whose terms? UNESCO. https://discovery.ucl.ac.uk/id/eprint/10195257/
3. Bau, J., & Mitchell, J. C. (2011). Security modeling and analysis. IEEE Security & Privacy, 9(3), 18–25. https://doi.org/10.1109/MSP.2011.2
4. CISA. (2022). Protecting our future: Cybersecurity in K-12 schools. Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov
5. ENISA. (2023). Threat landscape report. European Union Agency for Cybersecurity. https://www.enisa.europa.eu
6. Ferhataj, A., Memaj, F., Sahatcija, R., & Ora, A. (2025). Strengthening cybersecurity education for university students: bridging vulnerabilities and promoting proactive digital safety practices. *Millenium – Journal of Education, Technologies, and Health, 2*(27), Article e41111. https://doi.org/10.29352/mill0227.41111
7. Flor-Unda, O., Simbaña, F., Larriva-Novo, X., Acuña, Á., Tipán, R., & Acosta-Vargas, P. (2023). A comprehensive analysis of the worst cybersecurity vulnerabilities in Latin America. *Informatics, 10*(3), 71. https://doi.org/10.3390/informatics10030071
8. IBM Security. (2023). Cost of a data breach report. IBM Security. https://www.ibm.com/reports/data-breach
9. Ismail, K. A., Singh, M. M., Mustaffa, N., Keikhosrokiani, P., & Zulkefli, Z. (2017). Security strategies for hindering watering hole cyber crime attack. Procedia Computer Science, 124, 656–663. https://doi.org/10.1016/j.procs.2017.12.202
10. Ismail, M., Madathil, N. T., Alalawi, M., Alrabaee, S., Al Bataineh, M., Melhem, S., & Mouheb, D. (2024). Cybersecurity activities for education and curriculum design: A survey. Computers in Human Behavior Reports, 16, 100501. https://doi.org/10.1016/j.chbr.2024.100501
11. Kitchenham, B., & Charters, S. (2007). Guidelines for performing systematic literature reviews in software engineering (EBSE Technical Report EBSE-2007-01). Keele University & Durham University. https://www.cs.auckland.ac.nz/~norsaremah/2007%20Guidelines%20for%20performing%20SLR%20in%20SE%20v2.3.pdf
12. Lister, K., Riva, E., Kukulska-Hulme, A., & Fox, C. (2022). Participatory digital approaches to embedding student wellbeing in higher education. Frontiers in Education, 7, Article 924868. https://doi.org/10.3389/feduc.2022.924868
13. Madasu, S. D., Kumar, M. S., & Singh, A. K. (2017). Comparable investigation of backtracking search algorithm in automatic generation control for two area reheat interconnected thermal power system. Applied Soft Computing, 55, 197–210. https://doi.org/10.1016/j.asoc.2017.01.018
14. Manivel, R., & Mridula, K. (2024). Review article on challenges and opportunities for higher education in India. *SSRN.* https://doi.org/10.2139/ssrn.4886898
15. Martínez-Monteagudo, M. C., Delgado, B., García-Fernández, J. M., & Ruíz-Esteban, C. (2019). Cyberbullying in the university setting: Relationship with emotional problems and adaptation to the university. Frontiers in Psychology, 10, 3074. https://doi.org/10.3389/fpsyg.2019.03074
16. Morrow, E. (2024). Scamming higher ed: An analysis of phishing content and trends. Computers in Human Behavior, 158, 108274. https://doi.org/10.1016/j.chb.2024.108274
17. Pfleeger, S. L., & Cunningham, R. K. (2010). Why measuring security is hard. IEEE Security & Privacy, 8(4), 46–54. https://doi.org/10.1109/MSP.2010.60
18. Jenaro, C., Flores, N., & Frías, C. P. (2021). Anxiety and depression in cyberbullied college students: A retrospective study. *Journal of interpersonal violence*, *36*(1-2), 579-602. https://doi.org/10.1177/0886260517730030
19. Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. Future Internet, 13(2), 39. https://doi.org/10.3390/fi13020039
20. Yin, R. K. (2018). Case study research and applications: Design and methods (6th ed.). SAGE Publications.
21. Zhang, Y., Du, Y., & Liu, C. (2025). Enhancing cybersecurity awareness among university students: A strategic approach. *Learning & Education, 14*(1). Retrieved from https://ojs.piscomed.com/index.php/L-E/article/view/4275