Journal of Cybersecurity and Information Management

♦ ISSN: 2690-6775 Vol: 18, No. 01, 2026 ♦ PP. 14–20

Article DOI: https://doi.org/10.54216/JCIM.180102

FULL LENGTH ARTICLE

Cybercrime and Digital Competence among Students at a Public University in Lima

Belén Vila Osores[1,*]

[1]Universidad Científica del Sur, Perú

Emails: nocturnorosario2015@gmail.com

Received: January 12, 2026 Revised: February 10, 2026 Accepted: March 24, 2026 ⋆ Corresponding author

ABSTRACT

This article is part of an exhaustive study that aspired to determine the relationship between cybercrime and digital competence in sixth-cycle undergraduate students at a public university in Lima. The hypothesis was a sincere relationship between the two variables. The methodology applied is a quantitative, basic, correlational approach with a non-experimental cross-sectional design. The results reflected a medium positive correlation between cybercrime and digital competence, with a Kendall's Tau-b coefficient of 0.585 and a significance level of 0.000 ($p < 0.05$). In conclusion, it was evident that greater digital competence is associated with greater exposure to cybercrime risks, suggesting the need to implement educational strategies aimed at strengthening digital security in the university environment.

Keywords: Cybercrime ▪ Cybersecurity ▪ Digital Competence ▪ University Students ▪ Risk Assessment

1. INTRODUCTION

In Peru, cybercrime has experienced alarming growth, highlighting the increasing vulnerability of users to digital threats [1]. University students are particularly exposed to risks such as phishing, identity theft, online fraud, malware attacks, and privacy breaches on social media platforms. These threats are intensified in a context where rapid digitalization has not been accompanied by a proportional development of cybersecurity awareness and protective practices.

At the same time, studies on digital skills among Peruvian university students reveal worryingly low levels. Cerron et al. [2] found that only 37.92% of social science students achieved an adequate level of digital skills, especially in areas such as security and problem-solving. This gap is especially critical in fields such as Communication Sciences, where the use of digital platforms is inherent to professional training. Digital competence should not be understood solely as the ability to use technological tools, but also as the capacity to identify risks, protect personal data, and engage in safe online behavior.

This research stems from a master's thesis whose main objective was to determine the relationship between cybercrime and digital competence among sixth-semester undergraduate students in the Faculty of Social Sciences at a public university in Lima in 2024. The general hypothesis proposes a significant relationship between these two variables. The concern underlying this study arises from the excessive trust often exhibited by digital natives, who frequently lack a solid culture of digital security. As a result, they are more vulnerable to identity theft, intellectual property violations, online harassment, cyber fraud, and unauthorized access to digital systems. Despite advances in digital security tools, cybercriminals continue to exploit users' weaknesses, adapting their strategies to technological progress [3].

Therefore, this study seeks to contribute to the understanding of how digital competence is associated with exposure to cybercrime risks in the university context. By identifying this

relationship, the research aims to provide evidence to support the development of more effective cybersecurity training strategies tailored to the current digital environment in Peru.

2. RELATED WORK

Soylu et al. [4] identified the level of knowledge about cybercrime among undergraduate and postgraduate students in Kazakhstan. The results showed that participants' knowledge of cybercrime was moderate and required further improvement. In Colombia, Peña [5] analysed cybercrimes related to financial clients and highlighted the need to improve user trust and strengthen digital transaction security.

Al Kurdi et al. [6] examined the effect of digital education on cybersecurity competencies and found a statistically significant relationship between digital education dimensions and cybersecurity skills. Lopez et al. [7] showed that many students were concerned about data protection but lacked the knowledge required to recognize and prevent threats. Flores et al. [8] assessed computer security and problem-solving knowledge among Mexican university students, while Lopez [9] analysed digital competencies and learning strategies during the COVID-19 context.

In Peru, Chavarria [10] and Anicama [11] addressed cybercrime from legal and technological perspectives, identifying identity theft and computer fraud as relevant threats. Nuñez et al. [12] reported medium self-perceived digital competence among Peruvian university students, and Huaman et al. [13] studied digital competencies in post-pandemic environments. Together, these studies show that digital skill development does not automatically guarantee safe digital behavior.

The theoretical basis of the study draws on research methodology, general systems theory, and social learning theory [14–19]. Recent work on digital and media competence [20], regional digital competence policies [21], and cybersecurity knowledge in Mexico, Colombia, and Peru [22] supports the need to integrate technical competence with applied cybersecurity awareness.

3. METHOD AND RESULTS

3.1 Design of the Research

The methodology applied followed a quantitative approach, as it focused on studying what undergraduate students reported that they actually do, yielding numerical results that were statistically verified. The research is basic in nature and correlational in level, since it related, linked, and examined the variables that measure the probable relationship between them. The design is non-experimental and cross-sectional because no experiments were conducted; instead, the variables were observed without manipulation.

For this study, the population consisted of 97 students aged between 17 and 26 years enrolled in the sixth academic cycle of the Communications program. The sample was selected through proportional stratified probabilistic sampling to ensure adequate representation of relevant subgroups. Forty-three students were selected, preserving proportional distribution by gender and other program characteristics. The questionnaire was evaluated by three experts in cybercrime and digital competencies. After a pilot test and Cronbach's alpha calculation, the instrument was reduced from 28 to 24 questions, divided into 11 and 13 items.

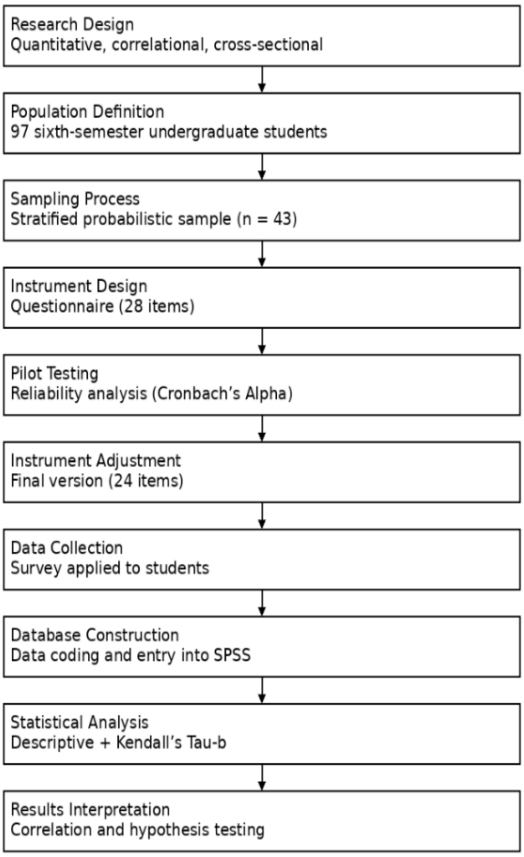


Figure 1. Research Process Flowchart.

3.2 Evidence and Findings

This section presents the results obtained from the administration of questionnaires to the selected sample during the 2024-I semester. The data were analysed using IBM SPSS Statistics 25 for frequency tables, contingency tables, bar charts, and scatter plots. The procedures included database construction, reliability testing, descriptive analysis by dimensions, inferential analysis for each hypothesis, and preparation of tables and figures.

3.2.1 Variable 1: Cybercrime

Table 1. Descriptive Statistics.

	N	Minimum	Maximum	Mean	Std. Deviation
Variable 1: Cybercrime	43	18	28	24.12	2.422
Valid N (listwise)	43				

Table 2. Frequency Table of the Cybercrime Variable by Scale Levels.

	Frequency	Percentage	Valid Percentage	Cumulative Percentage
Valid				
Never	13	30.2	30.2	30.2
Sometimes	23	53.5	53.5	83.7
Always	7	16.3	16.3	100.0
Total	43	100.0	100.0	

The cybercrime variable shows that Never represents 30.2%, Sometimes represents 53.5%, and Always represents 16.3%.

3.2.2 Security Dimension: Electronic Fraud

Table 3. Descriptive Statistics.

	N	Minimum	Maximum	Mean	Std. Deviation
Variable 1 - Dimension 1: Security (Electronic Fraud	43	8.00	13.00	9.7907	1.24515
Valid N (listwise)	43				

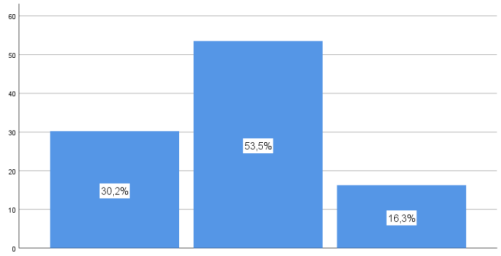


Figure 2. Frequencies of the Cybercrime Variable by Scale Levels.

Table 4. Frequency Table of the Security Dimension (Electronic Fraud) by Scale Levels.

	Frequency	Percentage	Valid Percentage	Cumulative Percentage
Valid				
Never	20	46.5	46.5	46.5
Sometimes	19	44.2	44.2	90.7
Always	4	9.3	9.3	100.0
Total	43	100.0	100.0	

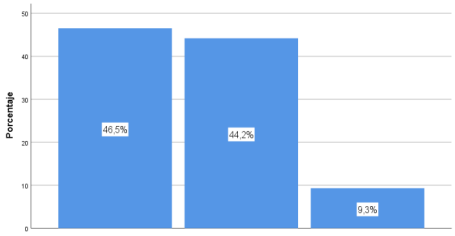


Figure 3. Frequencies of the security dimension (electronic fraud) according to scales.

For the security dimension associated with electronic fraud, Never represents 46.5%, Sometimes represents 44.2%, and Always represents 9.3%.

3.2.3 Technical Problem-Solving Dimension

Table 5. Descriptive Statistics.

	N	Minimum	Maximum	Mean	Std. Deviation
Variable 1 - Dimension 2: SecTechnical Problem Solving	43	4.00	8.00	6.2558	1.19708
Valid N (listwise)	43				

Table 6. Frequency Table of the Technical Problem-Solving Dimension by Scale Levels.

	Frequency	Percentage	Valid Percentage	Cumulative Percentage
Valid				
Never	12	27.9	27.9	27.9
Sometimes	23	53.5	53.5	81.4
Always	8	18.6	18.6	100.0
Total	43	100.0	100.0	

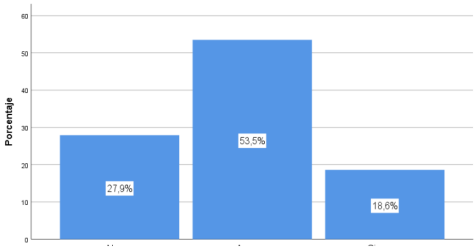


Figure 4. Frequencies of technical problem resolution according to scales.

The technical problem-solving dimension indicates that Never represents 27.9%, Sometimes 53.5%, and Always 18.6%.

3.2.4 Information Dimension

Table 7. Descriptive Statistics.

	N	Minimum	Maximum	Mean	Std. Deviation
Variable 1 - Dimension 3: Information	43	5	11	8.07	1.710
Valid N (listwise)	43				

The information dimension shows Never 27.9%, Sometimes 46.5%, and Always 25.6%.

Table 8. Frequency Table of the Information Dimension by Scale Levels.

	Frequency	Percentage	Valid Percentage	Cumulative Percentage
Valid				
Never	15	34.9	34.9	34.9
Sometimes	17	39.5	39.5	74.4
Always	11	25.6	25.6	100.0
Total	43	100.0	100.0	

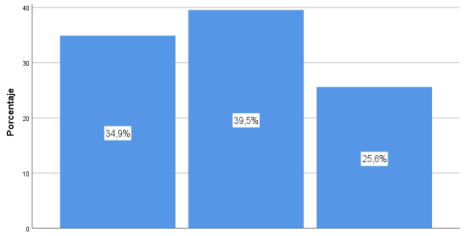


Figure 5. Frequencies of the Information Dimension According to Scales.

3.2.5 Variable 2: Digital Competence

Table 9. Descriptive Statistics.

	N	Minimum	Maximum	Mean	Std. Deviation
Variable 2: Digital Competence	43	18.00	30.00	23.6744	3.01363
Valid N (listwise)	43				

Table 10. Frequency Table of the Digital Competence Variable by Scale Levels.

	Frequency	Percentage	Valid Percentage	Cumulative Percentage
Valid				
Never	12	27.9	27.9	27.9
Sometimes	22	51.2	51.2	79.1
Always	9	20.9	20.9	100.0
Total	43	100.0	100.0	

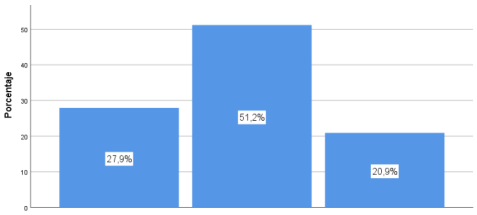


Figure 6. Frequencies of the Digital Competence Variable According to Scales.

The digital competence variable shows 23.3% at the low level, 55.8% at the medium level, and 20.9% at the high level.

3.2.6 Security Dimension: Levels of Knowledge

Table 11. Descriptive Statistics.

	N	Minimum	Maximum	Mean	Std. Deviation
Variable 2 - Dimension 1: Security (Levels of Knowledge)	43	5.00	11.00	8.3023	1.31900
Valid N (listwise)	43				

Table 12. Frequency Table of the Security Dimension (Levels of Knowledge) by Scale Levels.

	Frequency	Percentage	Valid Percentage	Cumulative Percentage
Valid				
Never	10	23.3	23.3	23.3
Sometimes	26	60.5	60.5	83.7
Always	7	16.3	16.3	100.0
Total	43	100.0	100.0	

The security knowledge dimension shows 25.6% at the low level, 58.1% at the medium level, and 16.3% at the high level.

3.2.7 Problem-Solving Dimension: Levels of Knowledge

Table 13. Descriptive Statistics.

	N	Minimum	Maximum	Mean	Std. Deviation
Variable 2 - Dimension 2: Problem Solving (Levels of Knowledge)	43	5.00	12.00	8.19	1.577
Valid N (listwise)	43				

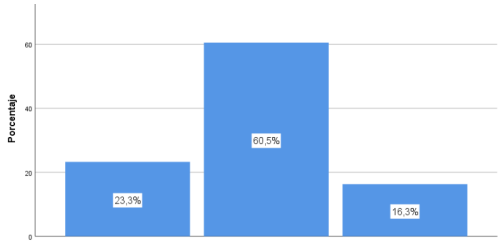


Figure 7. Frequencies of the security dimension (levels of knowledge) according to scales.

Table 14. Frequency Table of the Problem-Solving Dimension (Levels of Knowledge) by Scale Levels.

	Frequency	Percentage	Valid Percentage	Cumulative Percentage
Valid				
Never	16	37.2	37.2	37.2
Sometimes	18	41.9	41.9	79.1
Always	9	20.9	20.9	100.0
Total	43	100.0	100.0	

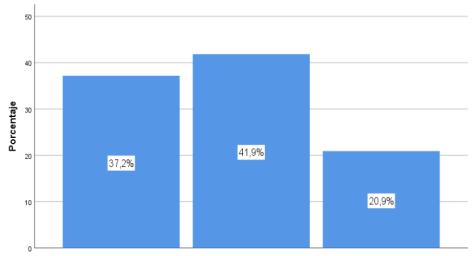


Figure 8. Frequencies of the Problem-Solving Dimension (Levels of Knowledge) by Scale.

For the problem-solving knowledge dimension, 27.9% are at the low level, 51.2% at the medium level, and 20.9% at the high level.

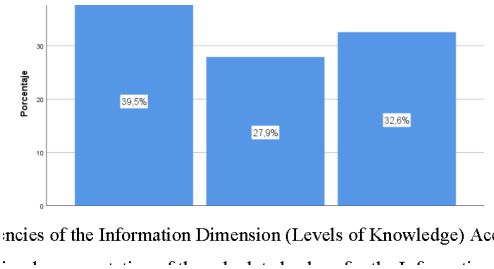
3.2.8 Information Dimension: Levels of Knowledge

Table 15. Descriptive Statistics.

	N	Minimum	Maximum	Mean	Std. Deviation
Variable 2 - Dimension 3: Information (Levels of Knowledge)	43	3.00	9.00	7.1860	1.63672
Valid N (listwise)	43				

Table 16. Frequency Table of the Information Dimension (Levels of Knowledge) by Scale Levels.

	Frequency	Percentage	Valid Percentage	Cumulative Percentage
Valid				
Never	17	39.5	39.5	39.5
Sometimes	12	27.9	27.9	67.4
Always	14	32.6	32.6	100.0
Total	43	100.0	100.0	



ncies of the Information Dimension (Levels of Knowledge) Acc

Figure 9. Frequencies of the Information Dimension (Levels of Knowledge) According to Scales.

The information knowledge dimension shows 14.0% at the low level, 53.5% at the medium level, and 32.6% at the high level.

3.3 Hypothesis Testing

Hypotheses were tested using Kendall's Tau-b correlation, a non-parametric statistic appropriate for ordinal variables. The study examined the relationship between cybercrime and digital competence and its dimensions.

Table 17. Summary of Hypothesis Testing Results.

Hypothesis	p-value or Significance Level	Coefficient	Decision
General	0.000	0.585	Accept
Derived 1	0.220	0.173	Do not accept
Derived 2	0.001	0.477	Accept
Derived 3	0.041	0.285	Accept

Table 18. Interpretation of the Correlation Coefficient.

Coefficient	Interpretation
0.00	No correlation
0.10	Very weak positive correlation
0.25	Weak positive correlation
0.50	Moderate positive correlation
0.75	Considerable positive correlation
0.90	Very strong positive correlation
1.00	Perfect positive correlation

3.3.1 General Hypothesis

The general hypothesis states that there is a significant relationship between cybercrime and digital competence among sixth-semester undergraduate students at a public university in Lima, 2024. The significance value of 0.000 is lower than 0.05; therefore, the null hypothesis is rejected and the alternative hypothesis is accepted. The Kendall's Tau-b coefficient of 0.585 indicates a moderate positive correlation.

Table 19. Contingency Table Corresponding to the General Hypothesis Test.

			Variable 1: Cybercrime (Scales)	Variable 2: Digital Competence (Grouped)
Kendall's Tau-b	Variable 1: Cybercrime (Scales)	Correlation coefficient	1.000	,585
		Sig. (two-tailed)		0.000
		N	43	43
	Variable 2: Digital Competence (Grouped)	Correlation coefficient	0.585**	1.000
		Sig. (two-tailed)	0.000	
		N	43	43

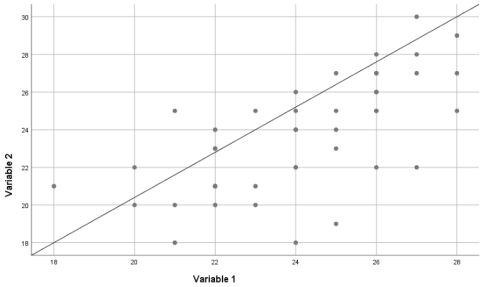


Figure 10. Scatter Plot Corresponding to the General Hypothesis Test.

3.3.2 Derived Hypothesis 1

The first derived hypothesis examined the relationship between cybercrime and digital security competence. The significance value of 0.220 is greater than 0.05; therefore, the null hypothesis is accepted. The coefficient of 0.173 indicates a very weak positive correlation without statistical significance.

Table 20. Contingency Table Corresponding to Derived Hypothesis 1.

			Variable 1: Cybercrime (Scales)	Variable 2: Dimension 1 - Security (Levels of Knowledge) (Scales)
Kendall's Tau-b	Variable 1: Cybercrime (Scales)	Correlation coefficient	1.000	0.173
		Sig. (two-tailed)		0.220**
		N	43	43
	Variable 2: Dimension 1 - Security (Levels of Knowledge) (Scales)	Correlation coefficient	0.173	1.000
		Sig. (two-tailed)	0.220	
		N	43	43

The correlation is not significant.

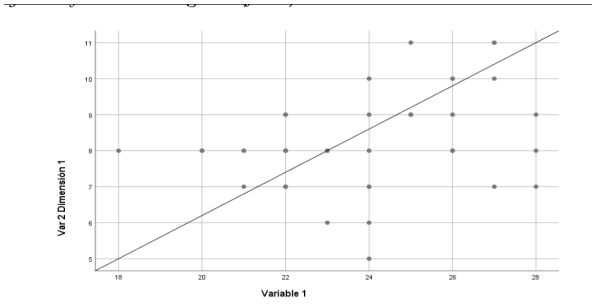


Figure 11. Scatter Plot Corresponding to Derived Hypothesis 1.

3.3.3 Derived Hypothesis 2

The second derived hypothesis examined the relationship between cybercrime and the problem-solving dimension of digital competence. The significance value of 0.001 is lower than 0.05; therefore, the null hypothesis is rejected and the alternative hypothesis is accepted. The coefficient of 0.477 indicates a weak positive correlation.

Table 21. Contingency Table Corresponding to the Derived Hypothesis 2 Test.

Table 21: Contingency Table Corresponding to the Derived Hypothesis 2 Test

			Variable 1: Cybercrime (Scales)	Variable 2: Dimension 2 - Problem Solving (Levels of Knowledge) (Scales)
Kendall's Tau-b	Variable 1: Cybercrime (Scales)	Correlation coefficient	1.000	,477**
		Sig. (two-tailed)		0.001
		N	43	43
	Variable 2: Dimension 2 - Problem Solving (Levels of Knowledge) (Scales)	Correlation coefficient	,477	1.000
		Sig. (two-tailed)	0.001	
		N	43	43

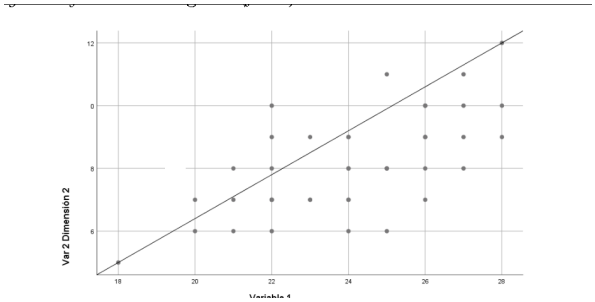


Figure 12. Scatter plot corresponding to the derived hypothesis test 2.

3.3.4 Derived Hypothesis 3

The third derived hypothesis examined the relationship between cybercrime and the information dimension of digital competence. The significance value of 0.041 is lower than 0.05; therefore, the null hypothesis is rejected and the alternative hypothesis is accepted. The coefficient of 0.285 indicates a weak positive correlation.

Table 22. Contingency Table Corresponding to the Derived Hypothesis 3 Test.

Table 22: Contingency Table Corresponding to the Derived Hypothesis 3 Test

			Variable 1: Cybercrime (Scales)	Variable 2: Dimension 3 - Information (Levels of Knowledge) (Scales)
Kendall's Tau-b	Variable 1: Cybercrime (Scales)	Correlation coefficient	1.000	,285*
		Sig. (two-tailed)		0.041
		N	43	43
	Variable 2: Dimension 3 - Information (Levels of Knowledge) (Scales)	Correlation coefficient	,285*	1.000
		Sig. (two-tailed)	0.041	
		N	43	43

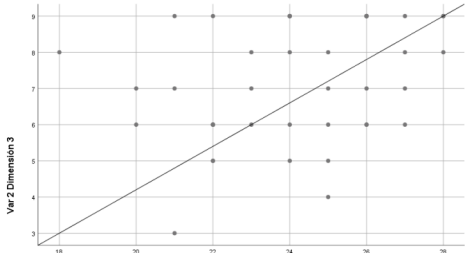


Figure 13. Scatter plot corresponding to the derived hypothesis test 3.

4. INFORMATION MANAGEMENT AND CYBERSECURITY MODEL

Based on the findings, a practical information management and cybersecurity protocol is proposed for universities. The model responds to the paradox that higher digital competence may coexist with higher exposure to cybercrime because students with stronger digital skills often spend more time online and may develop overconfidence in their abilities.

The first component is risk awareness and behavioural training. Universities should implement continuous cybersecurity education that addresses phishing, identity theft, privacy risks, safe authentication, and responsible use of social media. The second component is data protection and secure digital practices, including password management, multi-factor authentication, secure storage of personal information, and critical evaluation of digital content. The third component is institutional cybersecurity protocols and monitoring, including reporting channels, preventive campaigns, incident response, and coordination among academic and technical units.

5. DISCUSSION

The results confirm the general hypothesis and show a statistically significant positive relationship between cybercrime and digital competence. This finding should not be interpreted as evidence that digital competence directly causes cybercrime risk. Rather, it suggests that students with higher digital engagement may face more opportunities for exposure and may underestimate risks because of overconfidence in their technological ability.

The non-significant result for the security dimension suggests that knowledge about security alone is insufficient to reduce vulnerability. By contrast, the weak positive correlations observed for problem solving and information dimensions indicate that interaction with digital tools and information environments may increase exposure if not accompanied by risk awareness and responsible online behaviour.

These findings align with regional evidence showing that Latin American students often show moderate digital competence while remaining vulnerable to cybercrime. The expansion of digital access has not always been accompanied by proportional development of cybersecurity competencies. Therefore, universities should redesign digital education policies so that technological proficiency is integrated with prevention, ethics, critical thinking, and practical cybersecurity management.

The study has limitations. The data were collected through

self-reported questionnaires, which may introduce response bias. The sample was relatively small and limited to sixth-semester students from a single public university in Lima. The cross-sectional design does not allow causal relationships to be established. Future research should use larger and more diverse samples, comparative regional designs, longitudinal approaches, and objective measures of cybersecurity behaviour.

6. CONCLUSION

When addressing the general research objective, the results showed a statistically significant relationship between cybercrime and digital competence, with a Kendall's Tau-b coefficient of 0.585 and a significance level of 0.000 ($p < 0.05$), indicating a moderate positive correlation. This finding suggests that higher levels of digital competence are associated with greater exposure to cybercrime among university students.

However, this relationship should be interpreted with caution. The results do not necessarily imply that digital competence directly causes higher risk; rather, they may reflect two complementary factors. Students with higher digital competence tend to spend more time in online environments, increasing exposure to potential threats, while overconfidence in technological skills may lead them to underestimate risks and adopt less cautious behaviours.

Overall, these findings reinforce the idea that digital competence must be understood as a multidimensional construct that goes beyond technical skills, incorporating risk awareness, critical thinking, and responsible online behavior. Universities should not only promote digital skills but also implement structured training programs and institutional protocols aimed at reducing risky behaviours and strengthening safe navigation of digital environments.

FUNDING

This research received no external funding.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

REFERENCES

[1] C. Cabeza, "Cybercrime reports increase by 150% in 2023: The majority are fraud cases," Infobae, 2023.

[2] L. K. Cerron, E. V. Ramirez, K. N. Santos, and L. T. Javier, "Digital competencies in engineering and social sciences students of a university in Peru," *Quintaesencia*, vol. 14, no. 1, pp. 15–21, 2023.

[3] J. González, *Computer crime: Damages under article 264 of the Penal Code and proposal for reform*, Ph.D. dissertation, Universidad Complutense de Madrid, 2013.

[4] D. Soylu, T. D. Medeni, R. Andekina, R. Rakhmetova, and R. Ismailova, "Identifying the cybercrime awareness of undergraduate and postgraduate students: Example of Kazakhstan," IEEE, 2021.

[5] M. Peña, *Cybercrimes*, Master's thesis, Universidad Libre, 2023.

[6] B. Al Kurdi et al., "The impact of digital education on acquiring cybersecurity skills among the students of the Faculty of Medicine at Al-Balqa Applied University," *Migration Letters*, vol. 20, no. 6, pp. 1111–1128, 2023.

[7] H. L. Lopez, L. G. Quirino, and A. C. Carrasco, "Perception of cybersecurity among university students in digital environments," *TIES*, no. 11, pp. 72–95, 2024.

[8] E. Flores, A. Malacara, S. Cano, and V. Palacios, "Competencies in computer security and resolution of technological problems in higher education students," *Journal of Computer and Communications*, vol. 12, pp. 171–185, 2024.

[9] G. Lopez, *Relationship between digital competencies and learning strategies considering study conditions during the COVID-19 pandemic in university students from the Huancavelica region*, Master's thesis, Pontificia Universidad Católica del Perú, 2022.

[10] G. Chavarria, *Cybercrime and the implementation of the Special Cybercrime Prosecutor's Office in Peru*, Master's thesis, Universidad César Vallejo, 2023.

[11] Y. Anicama, *Cybercrime and cybercriminal activities with the use of new technologies in downtown Lima 2022*, Master's thesis, Universidad César Vallejo, 2023.

[12] N. Nuñez, A. Matas, J. Ríos, and L. Llatas, "Digital competencies in university students," *Revista de Ciencias Sociales*, vol. 30, no. 10, pp. 243–256, 2024.

[13] K. M. Huaman et al., "Digital competencies in post-pandemic environments," *Maestro y Sociedad*, vol. 21, no. 1, pp. 100–108, 2024.

[14] R. Hernández and C. Mendoza, *Research methodology: Quantitative, qualitative, and mixed routes*. McGraw-Hill Interamericana, 2018.

[15] L. von Bertalanffy, *General system theory*. Fondo de Cultura Económica, 1986.

[16] A. Bandura and R. H. Walters, *Social learning and personality development*. Alianza, 1974.

[17] S. Pihal, S. Jasmin, and S. Singh, "Commingling conceptual framework to Ludwig von Bertalanffy's general system theory in evidence-based research," *Bulletin of Environment, Pharmacology and Life Sciences*, vol. 4, pp. 539–541, 2022.

[18] E. D. Vázquez, "Systems theory: From Ludwig von Bertalanffy to Niklas Luhmann," *Miradas*, vol. 18, no. 1, pp. 195–206, 2023.

[19] S. Li, Y. C. Hong, and S. D. Craig, "A systematic literature review of social learning theory in online learning environments," *Educational Psychology Review*, vol. 35, p. 108, 2023.

[20] F. Miranda, *Improvement of a project through the development of digital and media competencies*, Master's thesis, Universidad Antonio de Nebrija, 2022.

[21] P. Herrera, M. Huepe, and D. Trucco, "Education and the development of digital competences in Latin America and the Caribbean," ECLAC Project Documents, 2025.

[22] Y. Riega-Viru et al., "Evaluation of the impact of cybersecurity knowledge on the prevention of social cybercrime among university students in Mexico, Colombia, and Peru," *International Journal of Advanced Computer Science and Applications*, vol. 16, no. 10, 2025.