Evaluation of the Impact of Cybersecurity Knowledge on the Prevention of Social Cybercrime Among University Students in Mexico, Colombia, and Peru

Yasmina Riega-Viru[1], Lainiver Mendoza Munar[2], Mario Ninaquispe-Soto[3], Kiara Nilupu-Moreno[4], Juan Luis Salas-Riega[5], Alfonso Renato Vargas-Murillo[6]*, Yolanda Pinto Bouroncle[7]
Universidad Privada del Norte, Lima, Peru[1, 3, 4, 6]
Universidad Cooperativa de Colombia, Cali, Colombia[2]
Pontificia Universidad Católica del Perú, Lima, Peru[5]
Universidad Peruana de Ciencias Aplicadas, Lima, Perú[7]

***Abstract*—Objectives: This study aims to evaluate the degree of cybersecurity knowledge and awareness among university students in Peru, Mexico, and Colombia, and to determine how these factors contribute to protection against social cybercrime. This cross-regional analysis represents a novel contribution by comparing cybersecurity preparedness across three Latin American countries, an underrepresented region in cybersecurity education research. Methods: A cross-sectional study was conducted using a 97-question survey that assessed both cybersecurity knowledge and practices. The study involved 809 university students from Peru, Mexico, and Colombia. Correlation analysis was performed to examine the relationship between cybersecurity knowledge and cybercrime prevention practices. Results: The analysis revealed a positive but low correlation (r=0.252) between cybersecurity knowledge and cybercrime prevention practices. Only 10.71% of preventive practices could be explained by acquired knowledge. Greater efficacy was observed in cyberstalking prevention compared to other forms of cybercrime. A significant gap was found between theoretical knowledge and practical application of cybersecurity, with only 44.6% of students receiving occasional information on the subject. Conclusions: This study highlights the urgent need to improve cybersecurity education in Latin American universities. The findings underscore the importance of integrating applied practices into cybersecurity curricula to strengthen students' ability to effectively counter cyber threats. Future educational initiatives should focus on bridging the gap between theoretical knowledge and practical application to enhance students' resilience against social cybercrime.**

Keywords*—Cybersecurity; social cybercrime; university students

I. Introduction

Technological advancement has transformed the way daily activities are conducted, especially since the Covid-19 pandemic, when dependence on internet access became crucial [1]. Although these advances have proven effective and beneficial in many aspects, it is essential to question whether the associated risks are being adequately considered. International organizations have expressed concern about the increased reliance on applications, online courses, banking services, and other digital resources. They emphasize the need for governments to implement effective strategies to combat cyber threats [2]. Most online vulnerabilities stem from insufficient cybersecurity knowledge among users [3]. For university students, the use of online technology is ubiquitous; however, they often lack awareness about the importance of cybersecurity and risky online behavior due to limited understanding of cyber security. Cybercrime is constantly evolving; for example, an emerging crime is "social cybercrime," which relates to online social interactions and represents the transposition of traditional conflicts to a digital environment [4]. First-world countries have implemented various mechanisms to prevent user vulnerability, such as raising awareness among high school and university students [5]; however, in Latin America, the same attention has not been paid to this problem. This research addresses a critical gap by conducting a comparative analysis across three Latin American countries—Peru, Mexico, and Colombia—to understand regional patterns in cybersecurity awareness and preparedness. Unlike previous single-country studies, this multi-national approach provides insights into shared vulnerabilities and educational needs across the region, contributing to the development of context-specific prevention strategies for social cybercrime in Latin American higher education institutions. Therefore, the question arises: What is the degree of knowledge and awareness about cybersecurity among university students in Peru, Mexico, and Colombia as protective measures against social cybercrime? The remainder of this paper is organized as follows: Section II reviews related work on cybersecurity awareness and social cybercrime; Section III describes the methodology employed in this study; Section IV presents the results of our analysis; Section V discusses the findings and their implications; and Section VI concludes with recommendations for future research and practice.

II. Related Work

A systematic literature review was conducted examining studies published between 2018 and 2023. This review revealed that it is necessary to reinforce the knowledge, attitude, and behavior of university students in cybersecurity, as few countries implement preventive measures in this group [6]. Another descriptive, correlational, and cross-sectional study with 48 female high school students, focused on social

*Corresponding author.

cybercrime, showed that cybersecurity is effective in preventing cyberharassment and cyberbullying [7]. Also, Abdukadir Ahmed and colleagues [8] evaluated cybersecurity awareness in 250 undergraduate and graduate students from five universities. They found that virus and phishing attacks are the most common problems, therefore, they recommended continuous education and supervision in cybersecurity.

The constant evolution of cyber threats, such as ransomware attacks, highlights the growing importance of cybersecurity [9]. This has become essential to prevent data breaches, inactivity, and intellectual property theft [10]. Recent research highlights the growing dependence of individuals, organizations, and countries on digital tools and networks. However, this trend has intensified cybercriminal activities, which in turn highlights the need to continuously improve cybersecurity measures in the face of emerging threats [11]. In a related study, Almansoori and others [12] discovered that the Protection Motivation Theory (PMT) is predominant in most studies on cybersecurity behavior, noting that, of 39 articles analyzed, 56% focused on the organizational level, while research at the individual level is still in an initial stage.

Cybersecurity, crucial for protecting systems, networks, and data against digital attacks and ensuring the confidentiality, integrity, and availability of information, requires a comprehensive understanding of its environment, resources, and guidelines [13, 14, 15]. Currently, organizations must establish adequate levels of access and security gateways to handle information securely. The complexity of cybersecurity suggests a holistic approach, evidenced in the analysis of the legal implications of technologies such as blockchain [16].

Moreover, the theory of planned behavior [17] highlights the influence of perceived control and subjective norms on personal actions, relevant to information management and risks in cyberspace. The protection motivation theory [18, 19] complements this approach by predicting the intention to engage in protective practices, integrating risk perception and evaluation of the effectiveness of protective measures.

In the university context, it is vital to develop educational strategies that integrate technical knowledge, understanding of student motivations and behaviors in the face of digital threats, and promote effective security practices. This holistic approach contributes to training professionals capable of navigating cyberspace safely, thus strengthening the digital resilience of society.

There are various models designed to measure and improve cybersecurity knowledge. One of them is the "citizen-centered cybersecurity model" developed by Mahlangu et al. [20]. This model focuses on assessing citizen awareness, threat evaluation, coping mechanisms, attitudes, and behavioral intentions. The purpose is to promote safe behaviors in the digital realm, emphasizing that adequate knowledge is fundamental to understanding and effectively responding to cyber threats. This model integrates concepts from the Protection Motivation Theory (PMT).

On the other hand, the Qualification Level Awareness Measurement Model, proposed by Erol and Sagiroglu [21], offers a framework to direct attention to crucial aspects of a situation, integrate perceived information, and project future system states. This model emphasizes the importance of situational awareness, mental models, and information processing, essential aspects for understanding and improving cybersecurity practices. Applying these principles allows individuals to evaluate cyber threats more effectively, understand system vulnerabilities, and make informed decisions to mitigate risks.

Furthermore, Tirumala et al. [22] propose a tiered structure through the Qualification Level Awareness Measurement Model, arguing that situational awareness or the situation model reflects the current state of the mental model. This model captures not only system parameters but also their interrelationships, facilitating a meaningful understanding of the system's state and its impact on future events. By employing principles of the goal-driven processing model, cybersecurity professionals can make more effective decisions when responding to security incidents or implementing preventive measures, improving cybersecurity posture and risk management.

For the development of social cybercrime, the theory proposed by Miró Linares [4] is taken as a foundation. According to him, the complexity of characterizing the authors of social cybercrimes is due to the diversity of motivations and actions they encompass. This category includes crimes with different purposes, from sexual motivations to verbal aggression on social networks and forums. He points out that minors can not only be victims but also perpetrators of these crimes, actively participating in activities such as sexting, insults, slander, and cyberbullying. It is mentioned that the profiles of social cybercrime perpetrators are as varied as the types of crimes themselves, and that their characteristics may be similar to those who commit similar crimes in physical space. However, cyberspace modifies the risk environment and, therefore, can alter the profile of offenders. As can be noted, there is a need for a deeper analysis of how cyberspace changes the profile of perpetrators of crimes such as cybergrooming, cyberstalking, and cyberbullying.

Cyberbullying is a phenomenon that merges technology and school bullying, using platforms such as social networks and instant messaging to repeatedly harass individuals, causing significant psychological damage to young people and university students [23, 24, 25]. Information and Communication Technologies (ICT) facilitate both communication and amplified forms of bullying [26, 27], also affecting university students, who require adjusted prevention strategies [28]. Cyberbullying is recognized by the European Union as one of the main online risks, driving measures to protect young people [29], while research such as that of Faucher et al. [30] suggests that impacts may vary by gender.

Cyberstalking, an evolution of traditional stalking, involves the use of technology to pursue and threaten, characterized by persistence and methods such as threatening messages and identity theft [31, 32]. This phenomenon is debated among experts on whether it constitutes an extension of conventional harassment or a distinct problem [33]. Research indicates that characteristics such as low self-control and bad social influences predispose to cyberstalking [34], and studies in Italy

reveal that victims can experience severe psychological consequences, especially those exposed to multiple forms of harassment [35].

Sexting, the exchange of erotic images through electronic devices, is common among university students, especially under pandemic circumstances [36, 37]. Although generally consensual, it can lead to risky practices such as non-consensual content publication, highlighting the importance of cybersecurity education to prevent abuse and blackmail [38, 39].

Online grooming is another severe form of online abuse where adults seek to manipulate minors to sexually abuse them, differing from sexting in its intentions and consequences [40, 41]. A study revealed that a significant proportion of Spanish university students has been affected by this phenomenon, with a notable impact on women and non-binary individuals [42]. Research also points to the influence of pornography consumption on vulnerability to grooming [43].

This analysis underscores the urgent need to implement robust educational and protection measures in academic settings to combat cybercrime and ensure a safe environment for students. Therefore, the objective of this study is to evaluate the degree of knowledge and awareness about cybersecurity among university students in Peru, Mexico, and Colombia, and determine how these factors contribute to protection against social cybercrime.

III. Methodology

A basic research of descriptive nature with a quantitative approach was conducted; of non-experimental cross-sectional design and correlational explanatory level, with the purpose of establishing the relationship between variable "X" representing the Level of Knowledge in Cybersecurity and variable "Y", representing the Degree of Prevention in Cybercrime.

For data collection, a questionnaire composed of 66 questions related to variable "X" and 31 questions for variable "Y" was used. The dimensions evaluated for each variable included the Level of Knowledge in aspects such as Online grooming, Cyberstalking, Cyberbullying, and Sexting for variable "X", and for variable "Y", the Degree of Prevention and exposure. To validate and ensure the reliability of the instrument, a pilot test was conducted, and the Cronbach's Alpha coefficient was calculated.

TABLE I. Reliability Statistics of the Instrument

Cronbach's Alpha	N of elements
0.962	98

Table I shows the reliability of the applied instrument, amounting to 0.962, which indicates that the applied instrument is highly reliable.

The analysis theory for the cybersecurity variable was based on KAB model [6], for the social cybercrime variable it was based on the typology of cybercrime proposed by Miró Linares.

The population consisted of university students from three Latin American universities (Mexico, Colombia, and Peru). The study was conducted with a sample of 809 students, who voluntarily responded to the questionnaire through a Google form.

The data exported to Excel were processed in the SPSS statistical package version 28. To identify the characteristics of students according to origin, age, study cycle; bivariate statistical analysis of association was applied, data normality analysis was performed, and considering the nature of the variables, Spearman's Rho statistical test was used to measure the correlation between them and their dimensions.

IV. Results

The processed data correspond mostly (57%) to students in cycles II, IV, VI, and VII (Fig. 1)

Fig. 1. Study cycle of students.

Fig. 2 shows that the largest age range of participating students is between 15 and 25 years old with 71%, and only 29% corresponds to students between 26 to 64 years old. Dispersion measures show that the mean age is 25 years with a standard deviation of 8.733 years.

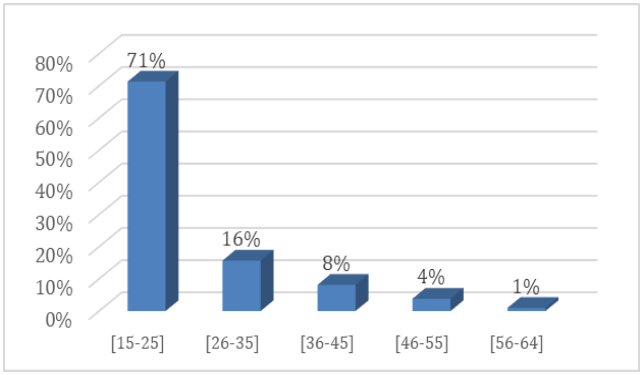

Fig. 2. Age range of participating students.

As shown in Fig. 3, 58% of the surveyed students come from the Universidad Privada del Norte Lima campus, 15% from UAQ Mexico, 13% from the Universidad Tecnológica del Perú, and the remaining 14% from UCC Colombia, UNIFÉ Lima, UPC Lima. This distribution reflects the multi-institutional and cross-national character of the study sample.

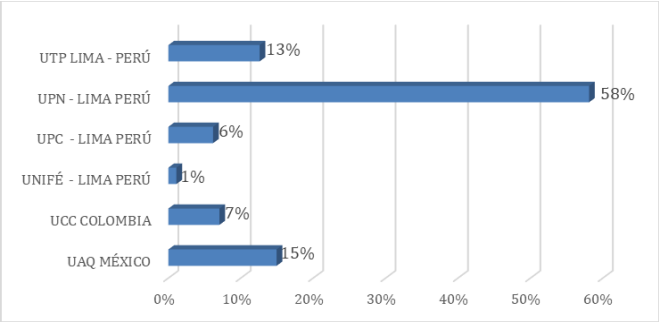

Fig. 3. Universities of origin.

Table II shows that 44.6% of students occasionally receive or have had knowledge about Cybersecurity, with UPN-Lima having the highest level on the subject (27.6%); likewise, 40.3% of students indicate that they have rarely evidenced or put into practice prevention in cybercrime offenses, with UPN-Lima again having the highest percentage with 24.6%.

The data normality analysis for the variables and their dimensions indicates a significance p-value = 0.000 < 0.001, so it is concluded that the behavior of the data does not follow a normal distribution, therefore, it is necessary to apply non-parametric tests for the validation of assumptions (Table III).

TABLE II. CROSS-TABULATION ON LEVEL OF KNOWLEDGE IN CYBERSECURITY AND DEGREE OF PREVENTION IN CYBERCRIME BY UNIVERSITY

		University						Total
		UAQ México	UCC Colombia	UNIFÉ Lima Peru	UPC Lima Peru	UPN Lima Peru	UTP Lima Peru	
X: Level of Knowledge in Cybersecurity	Never	0.5%	0.5%		0.2%	1.7%	1.5%	4.4%
	Rarely	6.8%	2.2%	0.2%	2.8%	20.1%	6.7%	38.9%
	Ocassionally	6.9%	3.3%	0.7%	2.5%	27.6%	3.6%	44.6%
	Frequent	0.7%	0.7%	0.1%	0.6%	7.4%	0.6%	10.3%
	Very Common		0.2%			1.2%	0.2%	1.7%
Y: Degree of prevention in cybercrime	Never	6.7%	2.2%	0.2%	1.6%	19.5%	7.0%	37.3%
	Rarely	5.3%	3.1%	0.2%	3.2%	24.6%	3.8%	40.3%
	Ocassionally	2.3%	1.1%	0.5%	1.0%	10.4%	1.4%	16.7%
	Frequent	0.4%	0.5%	0.1%	0.2%	2.7%	0.4%	4.3%
	Very Common	0.2%	0.1%		0.1%	0.9%		1.4%
Total		15.0%	7.0%	1.1%	6.2%	58.1%	12.6%	100.0%

TABLE III. DATA NORMALITY ANALYSIS

	Kolmogorov-Smirnov[a]		
	Statistical	gl	Sig.
D1X: Learning	0.213	809	0.000
D2X: Knowledge	0.223	809	0.000
D3X: Practice	0.242	809	0.000
D4XLearning_ Online Grooming	0.224	809	0.000
D5X: Knowledge_Arrangement Online	0.218	809	0.000
D6X: Practice_Online Arrangement	0.265	809	0.000
D7X: Learning_Cyberstalking	0.204	809	0.000
D8X: Knowledge_Cyberbullying	0.205	809	0.000
D9X: Practice_Cyberstalking	0.228	809	0.000
D10X: Learning_Cyberbullying	0.213	809	0.000
D11X: Knowledge_Cyberbullying	0.223	809	0.000
D12X: Practice_Cyberbullying	0.249	809	0.000
D13X: Learning_Sexting	0.201	809	0.000
D14X: Knowledge_Sexting	0.192	809	0.000
D15X: Practice__Sexting	0.245	809	0.000
D1Y_Victimization	0.224	809	0.000
D2Y_ GROOMING Exhibition	0.360	809	0.000
D3Y_ GROOMING Victimization	0.208	809	0.000
D4Y_CYBERSTALKING Exhibition	0.237	809	0.000
D5Y_Victimization CYBERBULLYING	0.247	809	0.000
D6Y_CYBERBULLYING Victimization	0.203	809	0.000
D7Y_SEXTING Exhibition	0.383	809	0.000
X: Level of cybersecurity knowledge	0.233	809	0.000
Y: Degree of prevention of cybercrime	0.242	809	0.000

TABLE IV. ANALYSIS OF CORRELATIONS BETWEEN THE STUDY VARIABLES

		Y: Degree of prevention of cybercrime
X: Level of cybersecurity knowledge	Spearman's Rho correlation coefficient	,252**
	Sig. (bilateral)	0.000 (p-valor<0.01)

Table IV shows the existing correlation between variable X: Level of knowledge in cybersecurity and variable Y: Degree of prevention in cybercrime, evidencing the existence of a correlation (p-value = 0.000 < 0.01), positive low equal to the Spearman's Rho coefficient 0.252. This statement is corroborated by Fig. 4 where the correlation points between both variables are shown, where the coefficient of determination $R^2 = 0.1071$ indicates that only 10.71% of the degree of prevention in criminality is given by the level of knowledge in cybersecurity.

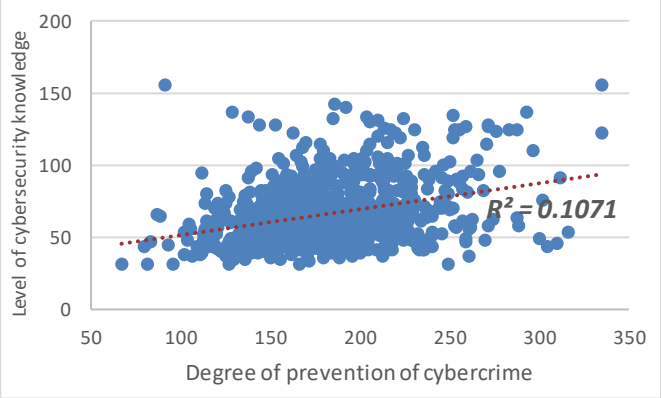

Fig. 4. Scatter plot of correlation between the level of knowledge in cybersecurity and the degree of prevention in cybercrime.

Table V shows the existing correlations between the dimensions of variables X and Y:

- There is a low positive correlation (r=0.134) between Cybersecurity Learning and Victimization in Cybercrime.
- There is a low positive correlation (r=0.239) between Cybersecurity Practice and Victimization in Cybercrime.

Regarding Grooming, it is evident that its Learning has a low positive correlation (r=0.095) with its Victimization; Knowledge and Practice have a low positive correlation with its Exposure (r=0.133, r=0.159) respectively, likewise they have a low positive correlation with its Victimization (r=0.114, r=0.223) respectively.

TABLE V. ANALYSIS OF CORRELATIONS BETWEEN THE STUDY VARIABLES

			Y						
			D1Y Victimization	**D2Y Groomin Exhibition**	**D3Y Victimization Grooming**	**D4Y Cyberstalking Exhibition**	**D5Y Cyberstalking Victimization**	**D6Y Cyberbulluing Victimization**	**D7Y Sexting Exhibition**
X	D1X: Learning	Correlation coefficient	,134**	,069*	,111**	,194**	,143**	,132**	0.059
		Sig. (bilateral)	0.000	0.050	0.002	0.000	0.000	0.000	0.096
	D2X: Knowledge	Correlation coefficient	0.065	,071*	0.044	,173**	,080*	0.053	0.017
		Sig. (bilateral)	0.063	0.042	0.215	0.000	0.024	0.135	0.627
	D3X: Practice	Correlation coefficient	,239**	,155**	,165**	,233**	,210**	,156**	,158**
		Sig. (bilateral)	0.000	0.000	0.000	0.000	0.000	0.000	0.000
	D4X: Online Grooming Learning	Correlation coefficient	,184**	0.024	,095**	,193**	,131**	,123**	0.060
		Sig. (bilateral)	0.000	0.489	0.007	0.000	0.000	0.000	0.088
	D5X: Online Grooming Knowledge	Correlation coefficient	,157**	,133**	,114**	,190**	,157**	,120**	,084*
		Sig. (bilateral)	0.000	0.000	0.001	0.000	0.000	0.001	0.017
	D6X: Online Grooming Practice	Correlation coefficient	,344**	,159**	,223**	,277**	,280**	,207**	,178**
		Sig. (bilateral)	0.000	0.000	0.000	0.000	0.000	0.000	0.000
	D7X: Cyberstalking Learning	Correlation coefficient	,118**	,074*	,082*	,220**	,103**	,108**	0.040
		Sig. (bilateral)	0.001	0.036	0.019	0.000	0.003	0.002	0.251
	D8X: Cyberstalking Knowledge	Correlation coefficient	,111**	0.038	,076*	,173**	,097**	,095**	0.005
		Sig. (bilateral)	0.002	0.278	0.030	0.000	0.006	0.007	0.896
	D9X: Cyberstalking Practice	Correlation coefficient	,424**	,166**	,263**	,287**	,345**	,252**	,202**
		Sig. (bilateral)	0.000	0.000	0.000	0.000	0.000	0.000	0.000
	D10X: Learning Cyberbullying	Correlation coefficient	,134**	,069*	,111**	,194**	,143**	,132**	0.059
		Sig. (bilateral)	0.000	0.050	0.002	0.000	0.000	0.000	0.096
	D11X: Cyberbullying Knowledge	Correlation coefficient	0.065	,071*	0.044	,173**	,080*	0.053	0.017
		Sig. (bilateral)	0.063	0.042	0.215	0.000	0.024	0.135	0.627
	D12X: Cyberbullying Practice	Correlation coefficient	,344**	,167**	,220**	,235**	,283**	,213**	,175**
		Sig. (bilateral)	0.000	0.000	0.000	0.000	0.000	0.000	0.000
	D13X: Learning Sexting	Correlation coefficient	,305**	,171**	,216**	,312**	,305**	,232**	,161**
		Sig. (bilateral)	0.000	0.000	0.000	0.000	0.000	0.000	0.000
	D14X: Sexting Knowledge	Correlation coefficient	,154**	,090*	,088*	,212**	,148**	,113**	0.050
		Sig. (bilateral)	0.000	0.011	0.013	0.000	0.000	0.001	0.156
	D15X: Sexting Practice	Correlation coefficient	,422**	,198**	,301**	,301**	,337**	,262**	,221**
		Sig. (bilateral)	0.000	0.000	0.000	0.000	0.000	0.000	0.000
	X	Correlation coefficient	,285**	,148**	,174**	,267**	,249**	,189**	,141**
		Sig. (bilateral)	0.000	0.000	0.000	0.000	0.000	0.000	0.000

Regarding Cyberstalking, it is evident that its Learning has a low positive correlation with its Exposure and Victimization (r=0.220, r=0.103) respectively; Knowledge about this crime has a low positive correlation with Exposure and Victimization (r=1.73, r=0.097) respectively, finally its Practice has a low positive correlation with Exposure and Victimization (r=0.287, r=0.345) respectively. Regarding Cyberbullying, it is evident that Practice in its knowledge has a low positive correlation (r=0.213) with the Victimization of this crime.

Regarding Sexting, it is evident that Learning and Practice in the recognition of this crime have a low positive correlation (r=0.161, r=0.221) with its Exposure, respectively.

Finally, variable X (Level of knowledge in cybersecurity) has a low positive correlation with Exposure and Victimization of the crimes: Grooming, Cyberstalking, Cyberbullying, and Sexting, which leads to the need to improve the mechanisms and procedures of knowledge about cybersecurity, which improve this correlation and thus avoid exposure and victimization of these crimes.

V. Discussions

This study on the knowledge and awareness of cybersecurity of social cybercrime among university students from Mexico, Colombia, and Peru reveals significant findings that indicate the need to improve cybersecurity education for this demographic group.

It is observed that the studied university population presents a diversity in terms of experience and exposure to knowledge about cybersecurity. Although the average age is 25 years, with a standard deviation of 8.733 years, it is important to note that 71% of the participants are in the range of 15 to 25 years, while only 29% corresponds to students between 26 to 64 years. This distribution suggests that a significant proportion of students are younger than average.

Although it could be expected that this population has had time to be exposed to knowledge about cybersecurity, the data indicates that only 44.6% of students occasionally receive or have had knowledge on the subject. Furthermore, the low elevation (r=0.252) between the level of knowledge in cybersecurity and the degree of prevention of cybercrime suggests that age and exposure time do not necessarily translate into greater awareness or effective practice in relation to social cybercrime in its various manifestations.

A. Gap Between Theoretical Knowledge and Practical Application of Cybersecurity

The data obtained in this study reveal a concerning gap between theoretical knowledge of cybersecurity and its practical application by university students. Despite having a relatively high level of theoretical awareness about cyber threats, many students do not effectively apply this knowledge to protect themselves. This is reflected in the modest correlations between the level of knowledge and the degree of prevention of cybercrime, indicating that knowledge alone is not sufficient to guarantee safe online behaviors [44, 45]. The KAB model [6] suggest that cybersecurity education must go beyond the simple transfer of information and focus on the formation of practical skills and motivation to effectively apply this knowledge.

B. Variability in Awareness and Prevention of Different Types of Cybercrime

The study also shows significant variability in awareness and prevention among different types of cybercrimes. For example, awareness about cyberbullying seems to be higher than about online grooming, which may be influenced by the frequency and visibility of prevention campaigns focused on school bullying. However, the lack of awareness and effective prevention in less discussed crimes, such as cyberstalking and sexting, suggests the need for more inclusive and diversified educational approaches that address all forms of cybercrime [4, 42], ensuring that students are equipped to recognize and respond to a wider range of threats.

C. International Collaboration and Multidisciplinary Approach

International collaboration and a multidisciplinary approach are crucial aspects for effectively combating cybercrime. This study, which encompasses universities from Peru, Mexico, and Colombia, underscores the importance of this perspective. The variability in legislation and security practices between different countries demands greater cooperation and coordination between governmental entities, educational institutions, and private sectors at a global level. Furthermore, integrating approaches from multiple disciplines, such as psychology, law, and information technology, can offer more comprehensive perspectives and more effective solutions to cybersecurity challenges, especially in academic and youth environments [17, 18].

VI. Conclusion

This study provides empirical evidence of the cybersecurity knowledge and preventive practices among 809 university students across Peru, Mexico, and Colombia. The findings reveal a positive but weak correlation ($r=0.252$, $p<0.01$) between cybersecurity knowledge and cybercrime prevention practices, with only 10.71% of variance in preventive behaviors explained by knowledge levels ($R^2=0.1071$). These quantitative results indicate that 44.6% of students receive only occasional cybersecurity training, and 40.3% rarely implement preventive measures against social cybercrime. Among the four types of social cybercrime examined, cyberstalking prevention demonstrated the highest correlation with knowledge (r=0.287 for practice-exposure and r=0.345 for practice-victimization), while grooming showed the weakest associations.

A. Theoretical and Practical Implications

This research contributes to cybersecurity education theory by empirically validating the gap between theoretical knowledge and behavioral application in the Latin American context, extending the Protection Motivation Theory (PMT) and the Knowledge-Attitude-Behavior (KAB) model to the domain of social cybercrime prevention. The multi-national comparative approach reveals that cybersecurity challenges are regionally consistent across Mexico, Colombia, and Peru, suggesting that coordinated educational interventions could be effective across Latin America.

From a practical standpoint, these findings have direct implications for higher education institutions. Universities should redesign cybersecurity curricula to emphasize hands-on training, simulation-based learning, and real-world case studies rather than solely theoretical instruction. Educational programs must specifically address the four dimensions of social cybercrime—grooming, cyberstalking, cyberbullying, and sexting—with particular attention to grooming prevention, which showed the weakest knowledge-practice correlation. Furthermore, institutions should implement mandatory, continuous cybersecurity awareness programs integrated throughout the academic curriculum rather than optional or occasional workshops. Policymakers in Latin American countries should consider establishing regional cybersecurity education standards and sharing best practices to strengthen collective digital resilience.

B. Research Limitations

This study presents several limitations that should be acknowledged. First, the cross-sectional design captures only a snapshot of cybersecurity knowledge and practices, preventing causal inferences or the examination of temporal changes in behavior. Second, the convenience sampling method, while yielding a substantial sample size (n=809), may not fully represent the diversity of university students across all Latin American countries, as the study focused on three specific nations. Third, self-reported measures are susceptible to social desirability bias, potentially leading participants to overestimate their cybersecurity knowledge or underreport risky online behaviors. Fourth, the study did not account for potential confounding variables such as socioeconomic status, prior technology education, or individual differences in digital literacy that may moderate the knowledge-practice relationship. Finally, the instrument, while demonstrating high reliability (α=0.962), was not validated across different cultural contexts, which may affect its applicability to other regions or populations.

C. Future Research Directions

Based on these findings and limitations, we propose three specific directions for future research. First, longitudinal studies should be conducted to track changes in cybersecurity knowledge and preventive behaviors over time, particularly following targeted educational interventions. Such studies could employ pre-test/post-test experimental designs to establish causal relationships between specific teaching methodologies and behavioral outcomes. Second, future research should expand geographically to include other Latin American countries and develop cross-cultural comparisons with other global regions to identify universal versus culture-specific factors influencing cybersecurity behaviors. This expansion would enable the development of globally informed yet locally adapted prevention strategies. Third, researchers should investigate the psychological and social factors that mediate or moderate the knowledge-practice gap, such as risk perception, self-efficacy, peer influence, and institutional support. Mixed-methods approaches combining quantitative surveys with qualitative interviews could provide deeper insights into the barriers preventing students from translating knowledge into protective action. Additionally, future studies should explore the effectiveness of innovative pedagogical approaches, such as gamification, virtual reality simulations, and peer-to-peer learning, in enhancing practical cybersecurity skills among university students.

REFERENCES

[1] C. Cardona-Londoño, M. Ramirez-Sanchez, and E. Rivas-Trujillo, "Educación Superior en un mundo virtual, forzado por la pandemia del Covid 19," Revista Espacios, vol. 41, no. 35, pp. 1–14, 2020.

[2] Organizaction of American States, "Ciberseguridad Marco NIST," 2019. [Online]. Available: https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf

[3] Organization of American States, "Cybersecurity Education Future Planning through Workforce Development," 2020. [Online]. Available: https://www.oas.org/es/sms/cicte/docs/White-Paper-Cybersecurity-Education.pdf

[4] F. Miró Linares, Cibercrimen Fenomenología y criminología de la delincuencia en el ciberespacio. Marcial Pons Ediciones Jurídicas y Sociales, 2012.

[5] M. A. Alqahtani, "Factors Affecting Cybersecurity Awareness among University Students," Applied Sciences, vol. 12, no. 5, p. 2589, 2022, doi: 10.3390/app12052589.

[6] K. Nilupú-Moreno, J. L. Salas-Riega, M. Ninaquispe-Soto, and Y. Riega-Virú, "Cybersecurity in University Students: A Systematic Review of the Literature," in Lecture Notes in Networks and Systems, 2024, pp. 315–332. doi: 10.1007/978-981-99-7886-1_27.

[7] Y. Riega-Virú, K. Nilupu-Moreno, J. L. Salas-Riega, and M. Ninaquispe-Soto, "Knowledge of cybersecurity against social cybercrime of female high school students," in Proceedings of the 2023 IEEE 3rd International Conference on Advanced Learning Technologies on Education and Research, ICALTER 2023, 2023. doi: 10.1109/ICALTER61411.2023.10372927.

[8] A. Abdukadir Ahmed, A. Hussein Elmi, A. Abdullahi, and A. Yahye Ahmed, "Cybersecurity awareness among university students in Mogadishu: a comparative study," Indonesian Journal of Electrical Engineering and Computer Science, vol. 32, no. 3, p. 1580, 2023, doi: 10.11591/ijeecs.v32.i3.pp1580-1588.

[9] H. Almonajid, "Fundamentals of Cyber Security," International Journal of Emerging Multidisciplinaries: Security, vol. 1, no. 1, 2023, doi: 10.54938/ijemds.2023.01.1.232.

[10] M. Mijwil, "The Significance of Machine Learning and Deep Learning Techniques in Cybersecurity: A Comprehensive Review," Iraqi Journal for Computer Science and Mathematics, pp. 87–101, 2023, doi: 10.52866/ijcsm.2023.01.01.008.

[11] A. Loishyn, S. Hohoniants, M. Tkach, M. Tyshchenko, N. Tarasenko, and V. Kyvliuk, "Development of the Concept of Cybersecurity of the Organization," TEM Journal, pp. 1447–1453, 2021, doi: 10.18421/TEM103-57.

[12] A. Almansoori, M. Al-Emran, and K. Shaalan, "Exploring the Frontiers of Cybersecurity Behavior: A Systematic Review of Studies and Theories," Applied Sciences, vol. 13, no. 9, p. 5700, 2023, doi: 10.3390/app13095700.

[13] B. Yadav, "Overview of Cyber Security," International Journal of Advanced Research in Science, Communication and Technology, pp. 489–492, 2022, doi: 10.48175/IJARSCT-3959.

[14] S. Chopra, H. Marwaha, and A. Sharma, "Cyber-Attacks Identification and Measures for Prevention," in Proceedings of the International Conference on Cybersecurity and Cybercrime (IC3), 2022, pp. 83–90. doi: 10.19107/CYBERCON.2022.11.

[15] M. Haripriya, "Cyber Security Unveiled: Trends and Protections in the Digital World," International Journal Of Scientific Research In Engineering And Management, vol. 07, no. 07, 2023, doi: 10.55041/IJSREM24720.

[16] L. Mendoza Munar, and A. Riascos Diaz, "Aspectos jurídicos de la tecnología Blockchain". Law, State & Telecommunications Review/Revista de Direito, Estado e Telecomunicações, vol. 13, no. 1

[17] I. Ajzen, "The theory of planned behavior," Organizational Behavior and Human Decision Processes, vol. 50, no. 2, pp. 179–211, 1991, doi: 10.1016/0749-5978(91)90020-T.

[18] R. W. Rogers, "Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation," in Social psychophysiology: A sourcebook, 1983, pp. 153–176.

[19] I. Woon, G.-W. Tan, and R. Low, "A Protection Motivation Theory Approach to Home Wireless Security," in ICIS 2005 Proceedings, 2005.

[20] G. Mahlangu, C. Chipfumbu Kangara, and F. Masunda, "Citizen-centric cybersecurity model for promoting good cybersecurity behaviour," Journal of Cyber Security Technology, vol. 7, no. 3, pp. 154–180, 2023, doi: 10.1080/23742917.2023.2217535.

[21] S. E. Erol and S. Sagiroglu, "Awareness Qualification Level Measurement Model," in 2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT), 2018, pp. 107–112. doi: 10.1109/IBIGDELFT.2018.8625305.

[22] S. S. Tirumala, M. R. Valluri, and G. Babu, "A survey on cybersecurity awareness concerns, practices and conceptual measures," in 2019 International Conference on Computer Communication and Informatics (ICCCI), 2019, pp. 1–6. doi: 10.1109/ICCCI.2019.8821951.

[23] W. Lim, B. T. Lau, and F. M. A. Islam, "Cyberbullying Awareness Intervention in Digital and Non-digital Environment for Youth: Current Knowledge," Education and Information Technologies, vol. 28, no. 6, pp. 6869–6925, 2023, doi: 10.1007/s10639-022-11472-z.

[24] A. C. Beluce, K. L. de Oliveira, A. S. Ferraz, and L. da S. Almeida, "Cyberbullying and Motivation to Learn with Digital Technologies: Identification and Correlation," Psicologia: Teoria e Pesquisa, vol. 39, no. spe, 2023, doi: 10.1590/0102.3772e39nspe07.en.

[25] A. Bussu, M. Pulina, S.-A. Ashton, and M. Mangiarulo, "Exploring the impact of cyberbullying and cyberstalking on victims' behavioural changes in higher education during COVID-19: A case study," International Journal of Law, Crime and Justice, vol. 75, p. 100628, 2023, doi: 10.1016/j.ijlcj.2023.100628.

[26] L. Fernández, "Formación TIC (redes sociales, internet, ciberseguridad, big data, etc.) en casa, en el colegio, en la universidad y en la empresa: características, razón de ser y contenido," Revista Tecnología, Ciencia y Educación, vol. 12, no. 12, pp. 89–110, 2019.

[27] J. Kim, H. Song, and W. G. Jennings, "A Distinct Form of Deviance or a Variation of Bullying? Examining the Developmental Pathways and Motives of Cyberbullying Compared With Traditional Bullying in South Korea," Crime & Delinquency, vol. 63, no. 12, pp. 1600–1625, 2017, doi: 10.1177/0011128716675358.

[28] R. Ortega-Ruiz, R. Del Rey, and J. A. Casas, "Evaluar el bullying y el cyberbullying validación española del EBIP-Q y del ECIP-Q," Psicología Educativa, vol. 22, no. 1, pp. 71–79, 2016, doi: 10.1016/j.pse.2016.01.004.

[29] Euronews, "Lucha contra el ciberacoso: la UE estudia medidas para castigarlo por ley," Euronews, Jun. 17, 2023. [Online]. Available: https://es.euronews.com/2023/06/17/lucha-contra-el-ciberacoso-la-ue-estudia-medidas-para-castigarlo-por-ley

[30] C. Faucher, M. Jackson, and W. Cassidy, "Cyberbullying among University Students: Gendered Experiences, Impacts, and Perspectives," Education Research International, vol. 2014, pp. 1–10, 2014, doi: 10.1155/2014/698545.

[31] R. T. Gopalan, "Offending, victimization, forensic investigation, and prevention of cyberstalking," in Developing Safer Online Environments for Children: Tools and Policies for Combatting Cyber Aggression, 2019. doi: 10.4018/978-1-7998-1684-3.ch001.

[32] T. Begotti, M. A. Ghigo, and D. Acquadro Maran, "Victims of Known and Unknown Cyberstalkers: A Questionnaire Survey in an Italian Sample," International Journal of Environmental Research and Public Health, vol. 19, no. 8, p. 4883, 2022, doi: 10.3390/ijerph19084883.

[33] A. K. Gautam and A. Bansal, "Email-Based Cyberstalking Detection On Textual Data Using Multi-Model Soft Voting Technique Of Machine Learning Approach," Journal of Computer Information Systems, vol. 63, no. 6, pp. 1362–1381, 2023, doi: 10.1080/08874417.2022.2155267.

[34] C. D. Marcum, G. E. Higgins, and J. Nicholson, "I'm Watching You: Cyberstalking Behaviors of University Students in Romantic Relationships," American Journal of Criminal Justice, vol. 42, no. 2, pp. 373–388, 2017, doi: 10.1007/s12103-016-9358-2.

[35] T. Begotti and D. Acquadro Maran, "Characteristics of Cyberstalking Behavior, Consequences, and Coping Strategies: A Cross-Sectional Study in a Sample of Italian University Students," Future Internet, vol. 11, no. 5, p. 120, 2019, doi: 10.3390/fi11050120.

[36] L. A. Reed, M. P. Boyer, H. Meskunas, R. M. Tolman, and L. M. Ward, "How do adolescents experience sexting in dating relationships? Motivations to sext and responses to sexting requests from dating partners," Children and Youth Services Review, vol. 109, p. 104696, 2020, doi: 10.1016/j.childyouth.2019.104696.

[37] J. Mikova, "University Students' Risky Behavior In Online Environment During The Covid-19 Pandemic," in 6th EPIDAPO, International Conference on Applied Psychology and Educational Sciences, 2021, pp. 63–73. doi: 10.15405/epiceepsy.21101.5.

[38] A. Dodaj et al., "Through the Eyes of Young People: A Qualitative Study of Sexting Among Croatian and Bosnian and Herzegovinian College Students," Sexuality & Culture, vol. 26, no. 5, pp. 1885–1918, 2022, doi: 10.1007/s12119-022-09976-4.

[39] A. O. Dunmade, A. Tella, and U. D. Onuoha, "Awareness of Cyberethical Behavior Among Female Postgraduate Students in North Central Nigeria," Journal of Information Ethics, vol. 32, no. 2, pp. 122–136, 2023, doi: 10.2307/JIE.32.2.122.

[40] P. Rezaee Borj, K. Raja, and P. Bours, "Detecting Online Grooming By Simple Contrastive Chat Embeddings," in Proceedings of the 9th ACM International Workshop on Security and Privacy Analytics, 2023, pp. 57–65. doi: 10.1145/3579987.3586564.

[41] S. Craven, S. Brown, and E. Gilchrist, "Sexual grooming of children: Review of literature and theoretical considerations," Journal of Sexual Aggression, vol. 12, no. 3, pp. 287–299, 2006, doi: 10.1080/13552600601069414.

[42] P. Alonso-Ruido, I. Estévez, B. Regueiro, and C. Varela-Portela, "Victims of Child Grooming: An Evaluation in University Students," Societies, vol. 14, no. 1, p. 7, 2024, doi: 10.3390/soc14010007.

[43] A. Bull and T. Page, "Students' Accounts of Grooming and Boundary-Blurring Behaviours by Academic Staff in UK Higher Education," Gender and Education, vol. 33, no. 8, pp. 1057–1072, 2021, doi: 10.1080/09540253.2021.1884199.

[44] M. D. Cavelty, Cyber-security and threat politics: US efforts to secure the information age. Routledge, 2007.

[45] H. A. Kruger and W. D. Kearney, "A prototype for assessing information security awareness," Computers & Security, vol. 25, no. 4, pp. 289–296, 2006, doi: 10.1016/j.cose.2006.02.008.