Centro Sur Vol. 10 No. 2- April - June - Revista Centro Sur - eISSN: 2600-5743

http://centrosureditorial.com/index.php/revista

Cybersecurity And Privacy Of Adolescents On Gaming Platforms In Ecuador: An Evaluation

Ciberseguridad Y Privacidad De Adolescentes En Plataformas De Gaming En Ecuador: Una Evaluación

Jorge Paolo Morales Jaya
Universidad Estatal Península de Santa Elena, Posgrado, Maestría en Ciberseguridad, Ecuador, jorge.moralesjaya0842@upse.edu.ec,
https://orcid.org/0009-0006-3424-8487

Byron Oviedo-Bayas
Universidad Estatal Península de Santa Elena, Facultad de Posgrado, Ecuador
Universidad Técnica Estatal de Quevedo, Facultad de Posgrado, Ecuador
boviedo0373@upse.edu.ec
boviedo@uteq.edu.ec
https://orcid.org/0000-0002-5366-5917

ABSTRACT

Online gaming has become one of the primary social environments for adolescents in Ecuador. For many young people, gaming platforms are not merely entertainment spaces but environments where identity, belonging, and peer relationships are constructed. However, these same platforms incorporate interaction dynamics that may compromise cybersecurity and privacy, especially when digital knowledge does not translate into consistent self-protection practices. This study aimed to analyze the relationship between cybersecurity knowledge and privacy protection practices among Ecuadorian adolescents using gaming platforms, integrating a correlational empirical study with a systematic literature review. A quantitative, non-experimental, cross-sectional study was conducted with 100 adolescents aged 12 to 18. A structured questionnaire validated by

https://doi.org/10.37955/cs.v10i1.407
Received October 04, 2026/ Approved January 09, 2026 Pages: 16-32
eISSN: 2600-5743

expert judgment was applied, achieving adequate reliability levels (α = 0.83 and α = 0.79). In parallel, a systematic review was conducted following PRISMA 2020 guidelines (Page et al., 2021). Results revealed a moderate level of cybersecurity knowledge (M = 3.13), partial implementation of privacy protection measures, and high exposure to contact with strangers (79%). A statistically significant moderate positive correlation was found between cybersecurity knowledge and privacy protection (r = 0.42; p < 0.001). Findings indicate that strengthening cybersecurity knowledge contributes to improved digital protection behaviors, yet it does not fully eliminate vulnerability. Effective adolescent protection in gaming environments requires an integrated approach that combines critical digital education, context-specific regulation, and responsible platform design.

RESUMEN

El gaming en línea se ha convertido en uno de los principales escenarios de socialización adolescente en Ecuador. Para muchos jóvenes, no es únicamente un espacio de entretenimiento, sino un entorno donde construyen identidad, pertenencia y vínculos sociales. Sin embargo, estas mismas plataformas incorporan dinámicas que pueden comprometer su ciberseguridad y privacidad, especialmente cuando el conocimiento digital no se traduce en prácticas efectivas de autoprotección. Este estudio tuvo como propósito analizar la relación entre el conocimiento en ciberseguridad y las prácticas de protección de la privacidad en adolescentes ecuatorianos usuarios de plataformas de gaming, integrando un estudio correlacional con una revisión sistemática de la literatura científica reciente. Se desarrolló una investigación cuantitativa, no experimental y transversal con 100 adolescentes de entre 12 y 18 años. Se aplicó un cuestionario estructurado validado por expertos y con adecuados niveles de confiabilidad (α = 0.83 y α = 0.79). Paralelamente, se realizó una revisión sistemática siguiendo las directrices PRISMA 2020 (Page et al., 2021). Los resultados evidenciaron un nivel moderado de conocimiento en ciberseguridad (M = 3.13), una implementación parcial de medidas de privacidad y una alta exposición a contacto con desconocidos (79%). Se identificó una correlación positiva moderada y significativa entre conocimiento y protección (r = 0.42; p < 0.001). Los hallazgos muestran que el conocimiento contribuye a mejorar la protección digital, pero no elimina completamente la vulnerabilidad. Se concluye que la protección efectiva requiere un enfoque integral que

Received October 04, 2026/ Approved January 09, 2026 Pages: 16-32
eISSN: 2600-5743

combine formación crítica, regulación específica y diseño responsable de plataformas.

Keywords / Palabras clave

social engineering, youth digital interaction, risk exposure, privacy settings, digital co-responsibility.

ingeniería social, interacción digital juvenil, exposición a riesgos, configuración de privacidad, corresponsabilidad digital

Introduction

Over the past decade, online gaming platforms have evolved from simple entertainment spaces into true environments for adolescent digital socialization. For many young Ecuadorians, joining games on Roblox, Free Fire, or Minecraft is not just about playing: it means meeting friends, forming teams, competing, chatting via voice chat, sharing achievements, and, in many cases, building part of their social identity. These digital spaces operate as extensions of the offline world, where belonging and reputation are also negotiated and contested.

However, this deep integration of gaming into the daily lives of adolescents is not without risks. The technical architecture of these platforms—based on public profiles, messaging systems, random matchmaking, and virtual economies—significantly increases the surface area of exposure to threats related to cybersecurity and privacy. The issue, therefore, cannot be understood solely as a technical matter related to passwords or security settings, but rather as a socio-technical phenomenon in which psychological, cultural, educational, and regulatory dynamics converge.

Various international studies have documented that online multiplayer environments can facilitate practices such as cyberbullying, grooming, phishing, and identity theft. Hu et al. (2025), in a systematic review of cyberbullying in multiplayer video games, demonstrate that intense competitiveness, combined with anonymity and limited active moderation, fosters the normalization of hostile behaviors. In these spaces, aggressive language can be interpreted as part of the game's culture, making it difficult to distinguish between competitive interaction and digital violence.

At the same time, Gutiérrez et al. (2025) note that chat systems integrated into video games have been used as vectors for social

Received October 04, 2026/ Approved January 09, 2026 Pages: 16-32
eISSN: 2600-5743

engineering attacks. Through seemingly harmless messages—offers of virtual items, promises of account upgrades, or invitations to exclusive events—attackers seek to obtain login credentials or personal information. Phishing on gaming platforms has its own unique characteristics: it relies on the trust generated by repeated interaction and on the symbolic and economic value that adolescents attribute to their digital achievements.

Added to this risk dimension is the issue of massive collection of personal data. Dasgupta and Sarkar (2022) warn that many video game platforms collect sensitive information—such as geographic location, consumption habits, interaction patterns, and financial information associated with microtransactions—without transparency mechanisms that are easily understandable to minors. Privacy policies are often written in complex legal language, and secure settings are not always enabled by default. Consequently, adolescents face technical decisions that exceed their actual level of understanding.

From the perspective of digital literacy promoted by UNESCO (2018), protection in digital environments requires not only instrumental skills but also critical competencies to interpret risks, assess consequences, and make informed decisions. However, acquiring knowledge does not automatically guarantee the adoption of safe behaviors. There is a documented gap between knowing what to do and actually doing it, especially during adolescence, a stage characterized by the search for social acceptance and a perception of invulnerability.

In this context, the use of educational games focused on cybersecurity has been proposed as an effective strategy to strengthen digital competencies among children and adolescents, as it allows for the simulation of risk scenarios in controlled environments (Damenu et al., 2025).

In the Ecuadorian context, this issue takes on particular nuances. Access to mobile devices and connectivity has increased steadily, even in sectors with socioeconomic limitations. However, the systematic incorporation of cybersecurity and privacy content into the school curriculum has been inconsistent. González et al. (2025) found that Ecuadorian adolescents have fragmented and largely self-taught knowledge of digital security. This informal education creates disparities: some young people develop strong skills, while others remain highly vulnerable.

Received October 04, 2026/ Approved January 09, 2026 Pages: 16-32
eISSN: 2600-5743

At the regulatory level, Ecuador has the Organic Law on Personal Data Protection (2021), which establishes principles for the processing of information and the rights of data subjects. However, as Espinosa and Paredes (2025) point out, there are gaps in its specific application to digital platforms used by minors. Effective oversight, the requirement for secure default settings, and the regulation of virtual economies still pose institutional challenges. In this scenario, the responsibility for protection often falls on families, whose digital skills are not always sufficient.

Additionally, national studies such as those by Quezada et al. (2025) and Sotomayor et al. (2024) have addressed digital risks among Ecuadorian adolescents, including psychosocial impacts and crimes such as grooming. Along these same lines, national studies have also shown that adolescents' exposure to digital risks extends beyond gaming to social media and other interactive environments, reinforcing the need for comprehensive approaches to digital protection (Martínez & Torres, 2023). However, there remains a gap in studies that specifically integrate the variable of gaming as a distinct socio-technical environment. Video game platforms are not equivalent to traditional social media: they incorporate dynamics of cooperation, competition, reward, and anonymity that alter how risks are perceived and managed.

In this regard, it is important to understand that contact with strangers in video games is not necessarily interpreted by adolescents as a risky situation. In many cases, it constitutes a structural requirement of the game itself. Hu et al. (2025) explain that random matching is a central part of the multiplayer experience. Interaction with strangers is normalized and, at times, incentivized by the platform's design itself. This element creates tension in the relationship between knowledge and preventive behavior.

The systematic review conducted in this study, following the PRISMA 2020 guidelines (Page et al., 2021), revealed that most studies agree on a positive relationship between digital literacy and protective behaviors, albeit with moderate effects. Che Omar et al. (2024) emphasize that the most effective educational strategies are those that combine technical information with ethical reflection and simulation of real-life scenarios.

Based on this theoretical and contextual framework, the present study poses the following question: What is the relationship between the

Received October 04, 2026/ Approved January 09, 2026 Pages: 16-32
eISSN: 2600-5743

level of cybersecurity knowledge and the level of privacy protection among Ecuadorian adolescents who use gaming platforms? The central hypothesis posits that there is a positive and significant relationship between both variables.

This study is significant because it provides empirical evidence specific to the Ecuadorian context, integrating quantitative analysis with a systematic review. Understanding how knowledge, practices, and exposure to risks interact allows us to move beyond simplistic views that place responsibility solely on the individual. Digital protection for adolescents does not depend solely on what the young person knows, but also on how platforms are designed, how regulations are enforced, and how the social environment validates or questions certain behaviors.

Ultimately, analyzing cybersecurity and privacy on gaming platforms involves recognizing that adolescents do not inhabit an isolated digital space, but rather a complex ecosystem where technology, culture, economics, and regulation converge. The evidence generated in this study seeks to contribute to a comprehensive approach to shared responsibility that integrates critical education, effective public policies, and technological design centered on the protection of underage users.

Materials and Methods

This research adopts a quantitative approach, as it focuses on the objective measurement of variables using structured instruments and the statistical analysis of the data obtained. In terms of its purpose, it constitutes applied research, as it seeks to generate empirical evidence useful for educational and regulatory decision-making in the Ecuadorian context.

In terms of scope, the study is descriptive and correlational. It is descriptive because it characterizes the level of cybersecurity knowledge, privacy protection practices, and exposure to digital risks among adolescent users of gaming platforms. It is correlational because it examines the statistical association between cybersecurity knowledge (independent variable) and privacy protection (dependent variable).

The design adopted was non-experimental, as the variables were not deliberately manipulated nor were differentiated treatments assigned

Received October 04, 2026/ Approved January 09, 2026 Pages: 16-32
eISSN: 2600-5743

to the participants. The phenomenon was observed in its natural context.

Furthermore, the study is cross-sectional, as data collection took place at a single point in time (March–May 2025), allowing for the analysis of the relationship between variables at a specific point in time.

The conceptual model guiding the design establishes the independent variable: Cybersecurity knowledge; the dependent variable: Privacy protection on gaming platforms; and complementary descriptive variables: age, gender, frequency of use, primary platform, and experiences of digital risk

The population consisted of Ecuadorian adolescents aged 12 to 18 who use online video game platforms.

Due to the lack of a comprehensive sampling frame, non-probabilistic convenience sampling was used. The sample consisted of 100 adolescents enrolled in three educational institutions in the province of Los Ríos.

Inclusion criteria were established: age between 12 and 18 years, active use of at least one gaming platform, and informed consent signed by legal guardians. Exclusion criteria included: incomplete questionnaires and voluntary withdrawal during the study.

A structured 22-item questionnaire, designed specifically for this study and organized into four sections, was used as the instrument:

1. Sociodemographic data and usage habits (6 items)
2. Cybersecurity knowledge (8 items, 1–5 Likert scale)
3. Privacy protection (5 items, 1–5 Likert scale)
4. Digital risk experiences (3 dichotomous items)

Content validity was determined through expert judgment, yielding an average Content Validity Coefficient (CVC) of 0.89, which is considered adequate.

Reliability was assessed using Cronbach's alpha coefficient (Cronbach, 1951), yielding cybersecurity knowledge: $\alpha = 0.83$ and privacy protection: $\alpha = 0.79$. Both values exceed the 0.70 threshold accepted for social research. SPSS version 31 software was used for statistical analysis.

Received October 04, 2026/ Approved January 09, 2026 Pages: 16-32
eISSN: 2600-5743

The study was conducted in five phases:

Phase 1: Conceptual design and systematic review: The theoretical framework was developed, and a systematic review was conducted following the PRISMA 2020 guidelines (Page et al., 2021). Academic databases were analyzed, and 9 relevant studies published between 2020 and 2025 were selected.

Phase 2: Instrument design and validation: The questionnaire was developed, subjected to expert validation, and semantic adjustments were made.

Phase 3: Ethical management and institutional authorizations: Approval was obtained from the Ethics Committee of the Quevedo State Technical University, and informed consent was obtained from parents and guardians.

Phase 4: Data collection: In-person administration of the questionnaire in classrooms, supervised by researchers. Average time: 18 minutes.

Phase 5: Data processing and statistical analysis: Data coding, descriptive analysis, normality tests, and correlational analysis.

Statistical analysis of the data was performed using SPSS version 31 and was conducted sequentially, beginning with rigorous cleaning and coding of the database. First, a descriptive analysis was conducted to characterize the sample and understand the general distribution of the variables studied. For categorical variables such as age, gender, frequency of use, and primary platform, absolute frequencies and percentages were calculated. For variables measured using a Likert scale, measures of central tendency—particularly the arithmetic mean—as well as measures of dispersion—mainly the standard deviation—were estimated. Additionally, overall scores were constructed for the dimensions “Cybersecurity Knowledge” and “Privacy Protection” by averaging the corresponding items, ensuring internal consistency with the reliability values obtained through Cronbach’s alpha coefficient (Cronbach, 1951).

Subsequently, the assumption of normality for the continuous variables was evaluated using the Kolmogorov-Smirnov test. The results indicated significance values greater than 0.05 for both dimensions, allowing us to assume an approximately normal

Received October 04, 2026/ Approved January 09, 2026 Pages: 16-32
eISSN: 2600-5743

distribution and justify the use of parametric techniques for inferential analysis.

In the correlational phase, Pearson's correlation coefficient (r) was applied with a significance level set at $p < 0.05$, in order to determine the direction and magnitude of the relationship between cybersecurity knowledge and privacy protection. To interpret the magnitude of the coefficient, conventional criteria in social research were employed, distinguishing between weak, moderate, strong, and very strong correlations. Additionally, the coefficient of determination (r^2) was calculated to estimate the percentage of variance explained by the independent variable relative to the dependent variable, allowing for a more precise understanding of the actual influence of knowledge on the adoption of digital protection practices.

Results

This result was obtained from the descriptive analysis of the responses corresponding to the sociodemographic and usage habits section of the questionnaire. Absolute frequencies and percentages were calculated for age, gender, frequency of use, and primary platform used.

Table 1. *General characteristics of the participants*

Variable	Category	Frequency (n)	Percentage (%)
Age	12–14 years	14	14%
	15–16 years	35	35
	17–18 years	51	51%
Gender	Male	63	63%
	Female	37	37%
Frequency of use	Daily	54	54%
	Several times a week	27	27%
	Occasionally	19	19%
Primary platform	Roblox	46	46%
	Free Fire	35	35%
	Minecraft	14	14%
	Others	5	5%

Source: Author's own analysis.

Received October 04, 2026/ Approved January 09, 2026 Pages: 16-32
eISSN: 2600-5743

The data shows a higher concentration of participants in the 17–18 age range (51%), with a male predominance (63%). More than half of adolescents (54%) report daily use of gaming platforms, indicating a high level of integration of gaming into their daily routine. The 81% concentration on two platforms (Roblox and Free Fire) suggests massive exposure to multiplayer environments with open interaction and random matchmaking.

The high frequency of daily use exceeds that reported by González et al. (2025) among Ecuadorian adolescents, who identified 42% daily use of digital platforms. This increase can be explained by the sample's specific focus on gamers and the consolidation of digital entertainment post-pandemic. Furthermore, Dasgupta and Sarkar (2022) note that platforms with freemium models and strong social interaction attract a larger youth population, thereby increasing the scope of exposure to risks. From the perspective of Hu et al. (2025), the competitive and social nature of these environments may facilitate normalized risky behaviors.

Level of Cybersecurity Knowledge and Privacy Protection Practices

Means and standard deviations were calculated for each item in the "Cybersecurity Knowledge" and "Privacy Protection" dimensions. Subsequently, an overall average score was obtained for each dimension.

Table 2. *Level of cybersecurity knowledge*

Item	Mean	SD
I recognize phishing attempts	2.8	1.2
I use strong passwords	3.5	0.9
I identify suspicious profiles	3.1	1.4
I am familiar with two-step verification	2.9	1.3
I understand the privacy policy	2.7	1.1
I can identify malicious links	3.2	1.2
Overall score	**3.13**	**0.78**

Received October 04, 2026/ Approved January 09, 2026 Pages: 16-32
eISSN: 2600-5743

Table 3. *Privacy protection practices*

Item	Average	SD
Set profile to private	3.7	1.3
Review privacy settings	3.2	1.4
I limit who can contact me	2.6	1.5
I manage friend requests	3.4	1.2
I review default settings	2.8	1.3
Overall score	**3.14**	**0.81**

Source: Author's own work.

The overall level of knowledge (M = 3.13; SD = 0.78) falls within a moderate range. Heterogeneity is observed in specific competencies, especially in phishing identification (M = 2.8). In privacy protection (M = 3.14; SD = 0.81), the least adopted practice is limiting contacts (M = 2.6), with the greatest dispersion (SD = 1.5), indicating significant behavioral variability.

The results align with those of González et al. (2025), who identified fragmented knowledge among Ecuadorian adolescents. The weakness in phishing recognition aligns with the findings of Gutiérrez et al. (2025), who note that attacks in video games exploit trust dynamics. Hu et al. (2025) explain that restricting contacts can be perceived as a social barrier in multiplayer environments, creating tension between security and belonging. Che Omar et al. (2024) argue that education must incorporate socio-emotional components, not just technical ones.

Digital Risk Experiences

We analyzed the frequencies and percentages of dichotomous responses regarding risk experiences.

Table 4. *Digital risk experiences*

Situation	Yes (n)	No (n)	% Yes
Cyberbullying	23	77	23%
Contact with strangers	79	21	79%
Phishing attempt	13	87	13%

Source: Author's own analysis.

Received October 04, 2026/ Approved January 09, 2026 Pages: 16-32
eISSN: 2600-5743

79% report contact with strangers, constituting the most frequent risk experience. Cyberbullying accounts for 23% and phishing for 13%. These figures reflect significant exposure to structural risks in multiplayer environments.

Hu et al. (2025) reported international rates of contact ranging from 45% to 60%, so the observed 79% indicates greater local normalization. Dasgupta and Sarkar (2022) note that default open settings facilitate this phenomenon. Sotomayor et al. (2024) note that cyberbullying in gaming is rendered invisible by the competitive culture.

Relationship between cybersecurity knowledge and privacy protection

The Pearson correlation coefficient was calculated between the overall scores of both dimensions.

Table 5. *Correlation between knowledge and protection*

Variables	r	p	n
Knowledge – Privacy	0.42	<0.001	100

Source: Author's own work.

A moderate positive correlation ($r = 0.42$) was identified, and it was statistically significant ($p < 0.001$). The coefficient of determination ($r^2 = 0.176$) indicates that 17.6% of the variance in privacy protection is explained by knowledge.

This finding is consistent with González et al. (2025), who reported correlations between 0.35 and 0.48. However, 82.4% of the variance depends on other factors. According to UNESCO (2018), critical digital literacy requires reflective skills beyond technical knowledge. Dasgupta and Sarkar (2022) emphasize that platform design structurally influences behavior. This confirms that knowledge is necessary but insufficient.

The results obtained provide a deeper understanding of the complexity of cybersecurity and adolescent privacy on gaming platforms within the Ecuadorian context. While the study confirmed the existence of a positive and statistically significant relationship between cybersecurity knowledge and privacy protection ($r = 0.42$; $p < 0.001$), the moderate magnitude of this association reveals that the phenomenon cannot be explained exclusively through cognitive or

Received October 04, 2026/ Approved January 09, 2026 Pages: 16-32
eISSN: 2600-5743

informational logic. Knowing does not always imply acting accordingly.

The most revealing finding of the study is the coexistence of a moderate level of knowledge (M = 3.13) with high exposure to contact with strangers (79%) and a low tendency to limit interactions (M = 2.6). This apparent contradiction confirms the gap between knowledge and preventive behavior described in the international literature. From the perspective of the socioecological model proposed by Hu et al. (2025), adolescent digital behavior is shaped at the intersection of individual, relational, and structural factors. Knowledge constitutes a relevant individual component, but its impact is mediated by group dynamics and the technical design of the platforms.

In the case of platforms such as Roblox and Free Fire, which were predominant in the sample, interaction with strangers is not an exception but a structural feature of the environment. Random matchmaking, open chat systems, and rewards tied to cooperation or competition mean that restricting contacts may be perceived as a social constraint rather than a safety measure. In this sense, adolescents face a constant tension between protection and the sense of belonging. As Che Omar et al. (2024) point out, preventive strategies must take these social pressures into account and not limit themselves to conveying technical information.

Likewise, the relatively low ability to identify phishing attempts (M = 2.8) aligns with the findings of Gutiérrez et al. (2025), who highlight that attacks in video games exploit the trust built within the gaming community. The symbolic and economic value of virtual objects increases vulnerability, especially when adolescents do not clearly perceive the economic dimension of digital assets. In the Ecuadorian context, recent research has indicated that adolescents' exposure to digital risks is associated with psychosocial impacts and challenges in managing privacy, highlighting the need for context-specific preventive strategies (Quezada et al., 2025). In this regard, from a structural perspective, Dasgupta and Sarkar (2022) warn that permissive default settings and the complexity of privacy menus shift the burden of protection onto the user.

Therefore, the results of this research support a shared responsibility approach. Adolescent protection in gaming environments cannot depend solely on individual knowledge but requires comprehensive interventions that combine critical education, specific regulation, and

Received October 04, 2026/ Approved January 09, 2026 Pages: 16-32
eISSN: 2600-5743

platform redesign with privacy-by-default principles. Within the digital literacy framework proposed by UNESCO (2018), the challenge is not only to teach how to configure security settings but also to strengthen adolescents' ability to assess risks in complex and dynamic social contexts.

In summary, empirical evidence shows that knowledge is a partial protective factor, but its effectiveness depends on the digital ecosystem in which it operates. Understanding this interaction is essential for designing contextualized and sustainable educational policies and strategies.

Conclusions

The objective of this study was to analyze the relationship between cybersecurity knowledge and privacy protection among Ecuadorian adolescents who use gaming platforms, integrating empirical evidence with a systematic review of recent scientific literature. The results allow us to draw conclusions that are directly linked to the subject of study and the identified contextual issues.

First, it is confirmed that the participating adolescents demonstrate a moderate level of cybersecurity knowledge, indicating the existence of basic notions regarding secure passwords, the identification of suspicious profiles, and privacy settings. However, this knowledge is heterogeneous and exhibits specific weaknesses, particularly in recognizing phishing attempts and understanding privacy policies. This demonstrates that digital literacy in the Ecuadorian context is still developing in a fragmented and predominantly self-taught manner, without systematic integration into structured educational processes.

Second, it was found that privacy protection practices also fall at an intermediate level. Although a significant proportion of adolescents set their profiles to private, there is a low tendency to restrict who can contact them and to review default settings. This finding reveals a tension between the need for self-protection and the pursuit of social interaction within gaming environments, where open communication is perceived as a natural part of the experience.

Third, the high prevalence of contact with strangers (79%) confirms that gaming platforms constitute spaces of structural exposure to digital risks. This phenomenon cannot be interpreted solely as risky

Received October 04, 2026/ Approved January 09, 2026 Pages: 16-32
eISSN: 2600-5743

individual behavior, but rather as an inherent characteristic of the design of multiplayer environments such as Roblox and Free Fire, where open interaction is a central element of operation.

Fourth, the identification of a moderate positive correlation between knowledge and privacy protection ($r = 0.42$; $p < 0.001$) confirms that knowledge acts as a relevant protective factor, but not a determining one. The coefficient of determination ($r^2 = 0.176$) demonstrates that most of the variability in protection practices depends on other factors, such as social pressure, platform design, gaming culture, risk perception, and the regulatory environment. Consequently, knowledge is a necessary but insufficient condition for ensuring effective digital protection.

From a comprehensive perspective, the study concludes that adolescent cybersecurity on gaming platforms must be addressed through a shared responsibility approach. The education system must strengthen critical digital literacy aimed not only at acquiring technical information but also at developing reflective decision-making skills in highly socially interactive environments. The government must advance the effective enforcement of data protection regulations in digital contexts used by minors. Platforms, for their part, must incorporate privacy-by-default and secure-by-design principles, reducing exclusive reliance on individual user action.

Finally, this research provides contextualized empirical evidence for Ecuador and opens future lines of study aimed at analyzing additional moderating variables, comparing differences between specific platforms, and evaluating educational interventions that integrate technical, ethical, and socio-emotional components. The protection of adolescent privacy in gaming environments is not merely a technological challenge, but an educational, cultural, and regulatory challenge that demands coordinated and sustainable responses.

References

National Assembly of Ecuador. (2021). *Organic Law on the Protection of Personal Data*. Official Register Supplement No. 459. https://files.cdn-files-a.com/uploads/7721063/normal_690a6d8a4f243.pdf

Che Omar, M. F. R., Abdullah, N. A., & Saad, M. N. (2024). Prevention of cyberbullying in online games: Intervention of cybersecurity

Received October 04, 2026/ Approved January 09, 2026 Pages: 16-32
eISSN: 2600-5743

strategies. *Pakistan Journal of Life and Social Sciences, 22*(1), 5450–5464. https://doi.org/10.57239/PJLSS-2024-22.1.00402

Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika, 16*(3), 297–334. https://doi.org/10.1007/BF02310555

Damenu, T. K., Gökbay, İ. Z., Covaci, A., & Li, S. (2025). Cyber security educational games for children: A systematic literature review. *ACM Computing Surveys.*

Dasgupta, D., & Sarkar, S. (2022). Privacy: A myth in online gaming? *International Journal of Advanced Mass Communication and Journalism, 3*(2), 38–47. https://doi.org/10.22271/27084450.2022.v3.i2a.49

Espinosa Carvajal, G. G., & Paredes Fuentes, F. E. (2025). Cybercrimes and the protection of personal data in the Ecuadorian criminal justice system. *Revista Lex, 8*(29), 559–572.

González, M. Y., Salto, R. E., Zapata, A. M., & Cadme, M. D. (2025). Cybersecurity and digital citizenship: Challenges in the education of adolescents in Ecuador. *Pentaciencias, 7*(5), 354–363.

Gutiérrez Palacios, E., Urueña Sanabria, R., & Rojas Ángel, J. (2025). Analysis of cybercrimes in the context of video games and the metaverse. *Ciencia Latina Revista Científica Multidisciplinar, 9*(3). https://doi.org/10.37811/cl_rcm.v9i3.18675

Hu, Y., Sophie, E., Clancy, E. M., & Klettke, B. (2025). Player versus player: A systematic review of cyberbullying in multiplayer online games. *Computers in Human Behavior Reports, 18*, 100675. https://doi.org/10.1016/j.chbr.2025.100675

Martínez, A., & Torres, D. (2023). Social media use among students in Loja and its relationship to exposure to digital risks. *Pentaciencias, 5*(4), 75–90.

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., & Moher, D. (2021). The PRISMA 2020

Received October 04, 2026/ Approved January 09, 2026 Pages: 16-32
eISSN: 2600-5743

statement: An updated guideline for reporting systematic reviews. *BMJ, 372*, n71. https://doi.org/10.1136/bmj.n71

Quezada, R., Mendoza, L., & Castillo, P. (2025). Social media use among adolescents: Psychosocial impact and exposure to digital risks. *Ciencia Latina Revista Científica Multidisciplinar, 9*(2).

Sotomayor, J., Alarcón, M., & Vega, R. (2024). Grooming in online games in Ecuador: Prevention strategies from a legal-technological perspective. *Revista UNEMI, 17*(45), 88–102.

UNESCO. (2018). *A global framework of reference on digital literacy skills for indicator 4.4.2*. UNESCO Institute for Statistics.

Received October 04, 2026/ Approved January 09, 2026 Pages: 16-32
eISSN: 2600-5743