ESCUELA NAVAL DE CADETES
"ALMIRANTE PADILLA"
Honor y Tradición

Article

Gamification Software to educate against Cyber Addiction and Digital Threats

Software de gamificación para educar contra la ciberadicción y las amenazas digitales

Alexander Rangel [1]* Jose Peña [2] Alejandro Cuello [3] Ana Meza [4] and Julian Castro [5]

[1] Mathematics Program, Universidad del Norte, Barranquilla, 80003, Colombia; alexanderrangel@uninorte.edu.co; mezaana@uninorte.edu.co; cjcalvo@uninorte.edu.co

[2] Faculty of Engineering, Universidad del Norte, Barranquilla, 80003, Colombia; pjosed@uninorte.edu.co; mcalejandro@uninorte.edu.co

* Correspondence: alexanderrangel@uninorte.edu.co

Citation: Rangel, A.; Peña, J.; Cuello, A.; Meza, A.; Castro, J. Gamification Software to educate against Cyber Addiction and Digital Threats. *OnBoard Knowledge Journal* **2025**, *1*, 8. https://doi.org/10.70554/OBJK2025.v01n02.08

Received: 13/08/2025, Accepted: 29/09/2025, Published: 06/11/2025

DOI: https://doi.org/10.70554/OBJK2025.v01n02.08

Abstract: This project addresses the growing need to educate teenagers on digital security practices and emotional well-being through an interactive video game inspired by "My Talking Tom." The game features a cat character who faces daily situations involving phishing, spoofing, and cyber addiction, where players must guide it to make responsible decisions that affect its self-esteem bar. The project followed an agile development approach, including stages of requirements analysis, design, implementation, and testing. The results of the usability evaluation, conducted with 20 teenagers, showed a 91% task success rate and an average satisfaction score of 4.3 out of 5. Participants demonstrated improved understanding of digital risks and reflected positively on how their decisions influenced online safety. The conclusions indicate that the objectives were successfully achieved, as the video game effectively combined entertainment and education, promoting awareness and responsible digital behavior among teenagers. Identified limitations include the variety of scenarios and dependence on access to technological resources. Overall, the game represents an innovative and valuable educational tool for strengthening digital literacy and emotional self-management in youth.

Keywords: Cyber addiction; Cybersecurity education; Educational video games; Emotional well-being; Gamification.

Resumen: Este proyecto aborda la creciente necesidad de educar a los adolescentes en prácticas de seguridad digital y bienestar emocional mediante un videojuego interactivo inspirado en "My Talking Tom". El protagonista es un gato que enfrenta situaciones cotidianas relacionadas con el phishing, el spoofing y la ciberadicción, donde los jugadores deben orientarlo para tomar decisiones responsables que afectan su barra de autoestima. El desarrollo siguió un enfoque ágil, que incluyó las fases de análisis de requerimientos, diseño, implementación y pruebas. Los resultados de la evaluación de usabilidad, realizada con 20 adolescentes, mostraron una tasa de éxito del 91% y un nivel promedio de satisfacción de 4.3 sobre 5. Los participantes demostraron una mejor comprensión de los riesgos digitales y reflexionaron sobre cómo sus decisiones influyen en la seguridad en línea. Las conclusiones indican que los objetivos se cumplieron satisfactoriamente, ya que el videojuego combinó de manera efectiva el entretenimiento y la educación, fomentando la conciencia y el comportamiento responsable en el entorno digital. Se identificaron como limitaciones la cantidad de escenarios disponibles y la dependencia de recursos tecnológicos. En conjunto, el videojuego representa una herramienta educativa innovadora y valiosa para fortalecer la alfabetización digital y la autorregulación emocional en los adolescentes.

Palabras clave: Bienestar emocional; Ciberadicción; Educación en ciberseguridad; Gamificación; Videojuegos educativos.

1. Introduction

In today's hyperconnected world, teenagers are immersed in a digital environment that provides unprecedented opportunities for learning, communication, and entertainment, but also exposes them to a wide range of cyber risks. Threats such as phishing, spoofing, identity theft, and cyber addiction not only compromise personal data and online security, but also have a direct impact on adolescents' emotional and psychological well-being. The increasing dependence on digital platforms and social networks has intensified adolescents' vulnerability to manipulation, misinformation, and social pressure. Despite this reality, digital security education and emotional self-regulation are often insufficiently addressed within formal educational curricula, leaving young users without the necessary skills to identify and respond effectively to online threats.

Addressing this gap requires innovative pedagogical approaches that go beyond traditional instructional methods. Gamification, defined as the application of game design elements in non-entertainment contexts, has emerged as an effective educational strategy to enhance motivation, engagement, and learning retention among students. By embedding educational content within interactive and playful environments, gamified systems allow learners to experiment with decision-making processes, observe consequences, and reflect on their actions in a safe and controlled setting. In recent years, serious games focused on cybersecurity education have demonstrated positive outcomes in increasing awareness and encouraging responsible digital behavior.

Within this context, this project proposes the development of an interactive educational video game aimed at raising awareness among teenagers about cyber risks and emotional self-regulation. The game follows the narrative of a cat character inspired by *My Talking Tom*, who encounters everyday digital situations involving threats such as suspicious messages, fraudulent websites, and excessive device usage. Players are required to guide the character's decisions, with each choice dynamically influencing a self-esteem indicator that represents the balance between emotional stability and responsible digital behavior. Rather than presenting binary correct or incorrect responses, the game encourages critical thinking and ethical reflection, allowing players to better understand the real-life implications of their online actions.

The primary objective of this initiative is to create a meaningful learning experience that integrates cybersecurity education with emotional intelligence through an engaging digital platform. By combining contextual learning, adaptive feedback, and decision-based scenarios, the proposed solution seeks to strengthen teenagers' ability to recognize digital threats, regulate their emotions, and adopt safer online habits. In doing so, the project contributes to the promotion of responsible digital citizenship, complementing formal education with a technological tool that is both educational and engaging.

The structure of this paper is as follows. Section 2 describes the main contributions of the proposed work. Section 3 reviews relevant related studies on cybersecurity education, gamification, and digital well-being. Section 4 details the methodological approach and development process of the video game. Section 5 presents and discusses the results obtained from the functionality and usability evaluations. Finally, Section 6 summarizes the main conclusions and outlines future improvements and research directions.

2. Contributions

This research presents the following contributions:

i. This work presents the design and development of an educational gamification-based software application aimed at raising awareness among teenagers about cyber addiction and common digital threats, including phishing and spoofing, by integrating cybersecurity concepts with emotional self-regulation mechanisms.

ii. It proposes an interactive video game model in which user decisions dynamically affect an emotional feedback indicator (self-esteem bar), enabling players to reflect on the consequences of their digital behavior in a safe and engaging learning environment.

iii. It applies an agile software development methodology to combine pedagogical objectives with technical implementation, covering requirements analysis, game design, implementation, and usability evaluation.

iv. It provides empirical evidence of the effectiveness of gamified learning for cybersecurity education through usability testing with adolescents, demonstrating high task success rates, user satisfaction, and improved understanding of digital risks.

3. Related Works

This project explores topics such as cybercrimes and cybersecurity, particularly in the context of an educational video game aimed at raising awareness of online risks, including phishing, identity theft, cyber addiction, and the responsible use of Information, Communication, and Relationship Technologies (ICRT). A relevant study validated a cybercrime awareness scale among university students, highlighting factors like phishing, spamming, antivirus effectiveness, and online bullying [8]. A 20-item questionnaire was applied to 372 students, revealing difficulties in identifying fraudulent sites and a lack of familiarity with data protection practices. Engineering students demonstrated greater awareness compared to other faculties, likely due to their technical training and familiarity with cybersecurity topics. The scale's high reliability (Cronbach's alpha of 0.892) makes it useful for measuring and improving preparedness against cyber threats.

Regarding identity theft, another study addressed this issue on social media, where cybercriminals use phishing techniques to steal credentials through fraudulent emails [4;5]. The importance of implementing two-step authentication was emphasized, as studies by Google and Microsoft showed that it can block up to 99% of phishing attacks [3]. Recent studies have also shown that gamified approaches can significantly improve cybersecurity awareness, as they combine active learning and decision-making in realistic virtual scenarios [6]. Additionally, victims of identity theft were encouraged to capture evidence for reporting the crime, underscoring the importance of cybersecurity education and the adoption of authentication tools.

The relationship between identity theft and phishing was investigated in another study, which described how both methods are used together to commit financial fraud or damage victims' reputations [7]. To delve deeper into the issue, laws and jurisprudence on unauthorized system access and disclosure of secrets were reviewed. The study concluded that the lack of security measures, such as two-step authentication, facilitates these crimes and highlighted the need for reforms in the Penal Code to address identity theft in digital environments.

On the other hand, a project related to cyber addiction and other digital risks used the Service-Learning (SL) methodology with secondary school students to raise awareness about cyberbullying, grooming, and sexting aligning with previous studies that have highlighted how excessive internet use can affect students' academic performance and emotional balance [1]. Fourth-year students trained their first-year peers using collaborative materials, increasing awareness of cyber addiction and promoting the responsible use of ICRT. The evaluation phase showed significant improvements in students' perceptions of digital risks and the importance of healthy leisure options. Similarly, gamified learning environments that integrate emotional feedback and decision-based interactions have proven to enhance both digital literacy and emotional awareness among students [9]. These findings are consistent with the conclusions of [2], who identified maladaptive patterns of ICT use among adolescents, emphasizing the importance of digital supervision and stress management strategies in educational contexts.

These studies and projects underscore the importance of addressing cybercrimes and digital security comprehensively, proposing education, security measures, and legislative reforms as pillars for protection in the online environment.

4. Methodology

The development of the video game followed an agile software development approach, specifically inspired by the Scrum framework, due to its iterative structure, adaptability, and emphasis on user feedback. This methodology was chosen instead of the traditional Waterfall model because it allows for continuous evaluation and refinement of the game mechanics and interface design. Given that the project involves both technical and pedagogical dimensions, the agile approach ensured that educational objectives and user experience evolved in parallel throughout the process.

The project was organized into four key phases, each associated with specific goals, activities, and deliverables.

- **Phase 1. Requirements Analysis and Conceptual Design**: This initial phase focused on identifying the educational goals, defining the target audience, and selecting the main topics to be addressed: phishing, spoofing, and cyber addiction. The outcomes of this phase included the functional and non-functional requirements, user stories, and a conceptual model for how digital threats would be represented through gameplay scenarios.
- **Phase 2. Game Design and Prototyping**: In this stage, the project team designed the narrative structure, interface layout, and game mechanics. The team developed mockups and diagrams to define relationships between entities such as the cat, the problems, and the self-esteem bar. A low-fidelity prototype was implemented to test usability and initial gameplay flow with a sample group of users.
- **Phase 3. Implementation and Integration**: The game was developed in Java using the NetBeans IDE, selected for its robustness, portability, and object-oriented programming support. The code implementation included the management of scenarios, player decisions, and adaptive scoring logic. The class diagram illustrating the main entities and their interactions is shown in Figure 1.
- **Phase 4. Testing and Evaluation**: Finally, the system underwent usability and educational impact testing. Twenty teenagers aged 13–18 participated in a usability session following Maze and Nielsen Norman Group guidelines. Metrics such as task success rate, error rate, and satisfaction level were collected to validate the game's effectiveness and user experience. Feedback obtained from these sessions guided refinements in the interface and overall gameplay dynamics.

5. Results

This section presents the results obtained from the implementation and evaluation of the video game, following the stages described in the methodology. The main objective of this phase was to verify the correct functioning of the system, its usability, and its potential educational impact on teenagers.

5.1. Functionality Evidence

Functional tests were conducted to confirm that the game performed as expected according to the defined requirements. These tests verified the proper operation of the character's self-esteem bar, the generation of problems and options in each scenario, and the management of player decisions. The evaluation also included error handling tests, such as name validation and prevention of empty fields, ensuring the game's stability and reliability (Figure 2).

The game successfully met its functional objectives, allowing the player to interact naturally with the cat and make decisions that affected its emotional state. The responses varied according to the type of situation (phishing, spoofing, or cyber addiction), and each option had a specific effect on the score. These behaviors confirmed that the logic of the program was consistent with the design established during development (Figure 3).

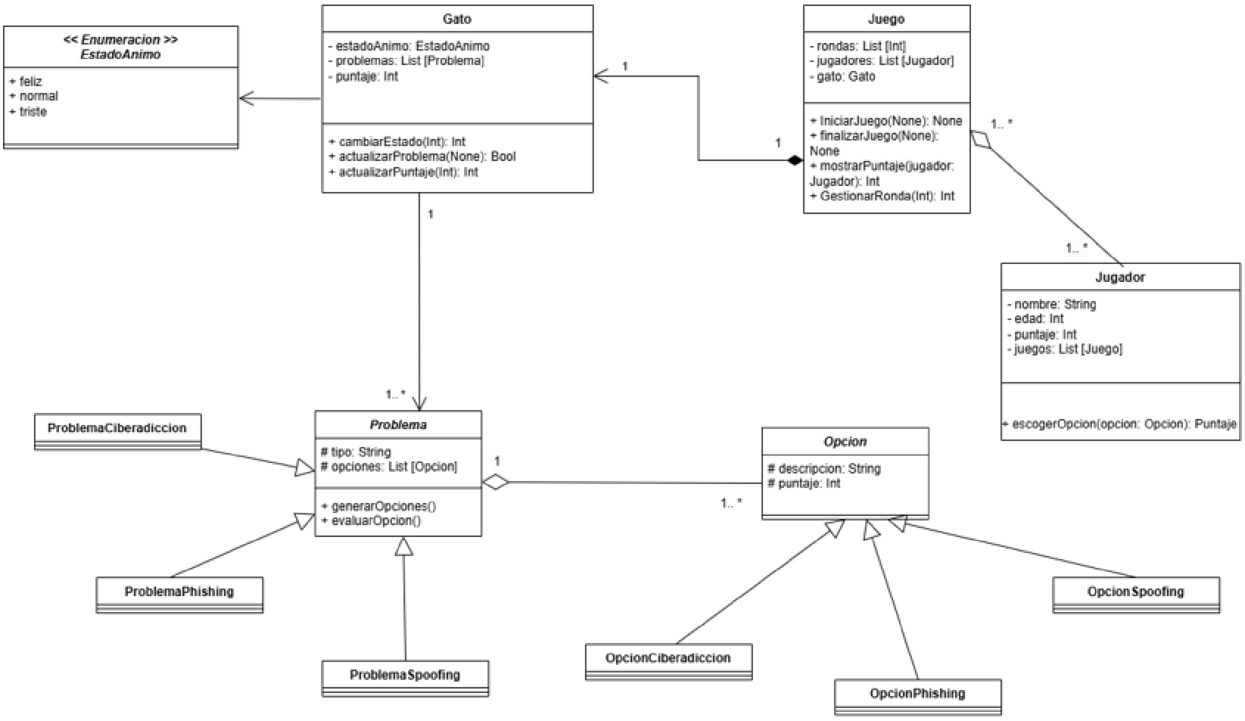


Figure 1. Class Diagram of the video game structure.
Source: The authors.

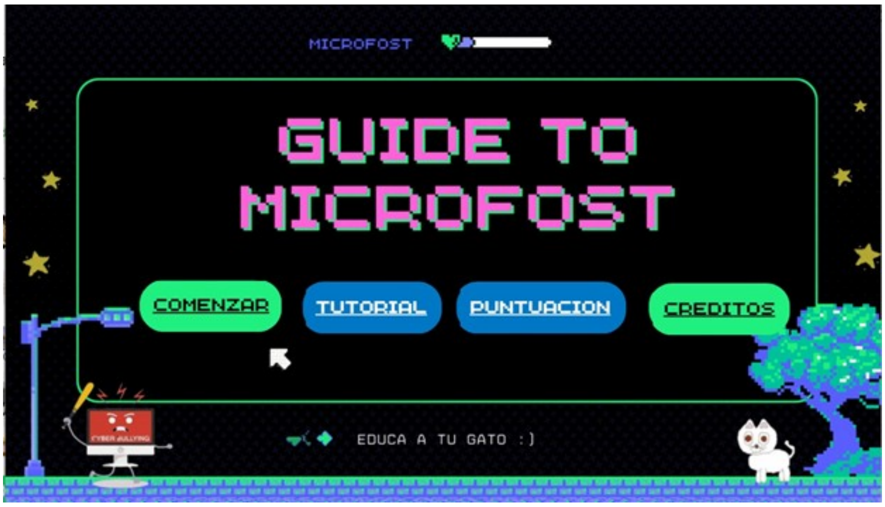
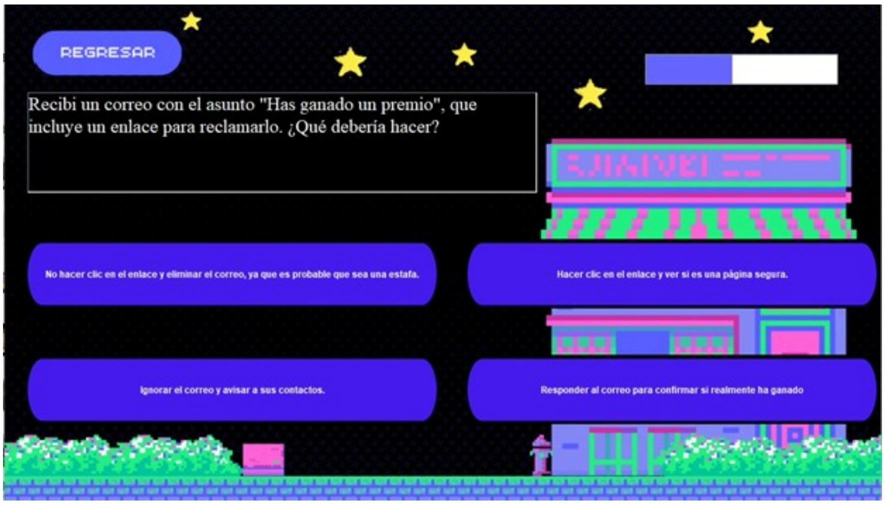


Figure 2. Main screen of the video game showing the start menu.
Source: The authors.

5.2. *Usability Test*

To evaluate the user experience, a usability test was carried out following the guidelines proposed by Maze and the Nielsen Norman Group. A group of 20 teenagers between 13 and 18 years old participated in the activity. Each participant played five complete rounds of the game and answered a short questionnaire about their experience.

The following aspects were measured during the test:



Recibi un correo con el asunto "Has ganado un premio", que incluye un enlace para reclamarlo. ¿Qué debería hacer?

No hacer clic en el enlace y eliminar el correo, ya que es probable que sea una estafa.

Hacer clic en el enlace y ver si es una página segura.

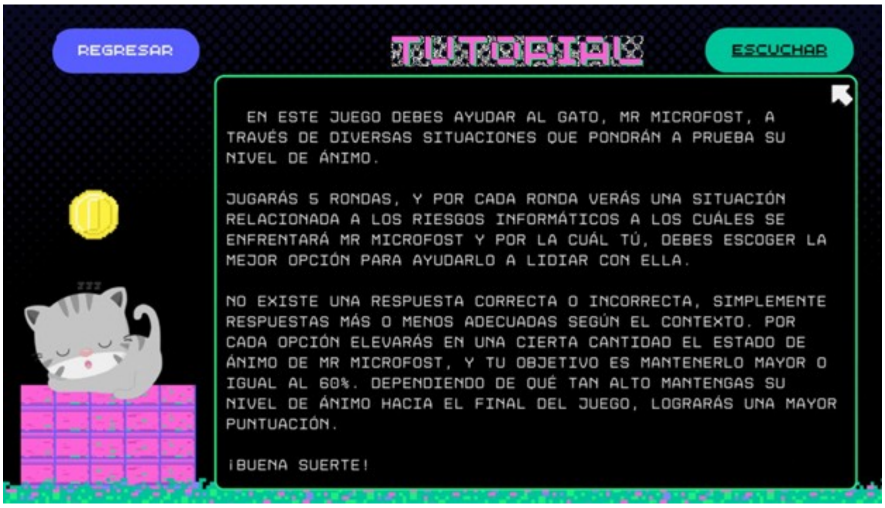
Ignorar el correo y avisar a sus contactos.

Responder al correo para confirmar si realmente ha ganado

Figure 3. Example of an interactive scenario where the player must choose among different options after receiving a suspicious email.
Source: The authors.

- **Task success rate:** 91% of participants completed all five rounds without major difficulties.
- **Error rate:** Less than 30% of users reported minor navigation issues.
- **Satisfaction level:** On a scale from 1 to 5, the game achieved an average satisfaction score of 4.3.

The participants expressed that the interface was clear, the controls were easy to use, and the topics were realistic and relevant to their daily lives. Some users suggested adding more scenarios and customization options for the main character to make the experience more engaging (Figure 4).



EN ESTE JUEGO DEBES AYUDAR AL GATO, MR MICROFOST, A TRAVÉS DE DIVERSAS SITUACIONES QUE PONDRÁN A PRUEBA SU NIVEL DE ÁNIMO.

JUGARÁS 5 RONDAS, Y POR CADA RONDA VERÁS UNA SITUACIÓN RELACIONADA A LOS RIESGOS INFORMÁTICOS A LOS CUÁLES SE ENFRENTARÁ MR MICROFOST Y POR LA CUÁL TÚ, DEBES ESCOGER LA MEJOR OPCIÓN PARA AYUDARLO A LIDIAR CON ELLA.

NO EXISTE UNA RESPUESTA CORRECTA O INCORRECTA, SIMPLEMENTE RESPUESTAS MÁS O MENOS ADECUADAS SEGÚN EL CONTEXTO. POR CADA OPCIÓN ELEVARÁS EN UNA CIERTA CANTIDAD EL ESTADO DE ÁNIMO DE MR MICROFOST, Y TU OBJETIVO ES MANTENERLO MAYOR O IGUAL AL 60%. DEPENDIENDO DE QUÉ TAN ALTO MANTENGAS SU NIVEL DE ÁNIMO HACIA EL FINAL DEL JUEGO, LOGRARÁS UNA MAYOR PUNTUACIÓN.

¡BUENA SUERTE!

Figure 4. This screen presents the tutorial that introduces the player to the purpose and mechanics of the game.
Source: The authors.

5.3. Evaluation Procedure

Functional tests were conducted to confirm that the game performed as expected according to the defined requirements. These tests verified the proper operation of the character's self-esteem bar, the generation of problems and options in each scenario, and the management of player decisions. The evaluation also included error handling tests, such as name validation and prevention of empty fields, ensuring the game's stability and reliability.

The game successfully met its functional objectives, allowing the player to interact naturally with the cat and make decisions that affected its emotional state. The responses varied according to the type of situation (phishing, spoofing, or cyber addiction), and each option had a specific effect on the score. These behaviors confirmed that the logic of the program was consistent with the design established during development.

5.4. Summary of Results

The results demonstrate that the video game fulfills its functional and educational purposes, successfully capturing user attention and promoting awareness of digital risks and emotional well-being. The usability test confirmed that the interface is intuitive and the game mechanics are engaging. Moreover, the responses from participants indicated a better understanding of cybersecurity practices and responsible technology use. Future versions are expected to include new scenarios and additional features to enhance the educational experience.

6. Conclusions

The development of the video game provided an interactive and educational approach to addressing issues related to cybersecurity and emotional well-being in teenagers. The main objective of the project, to create a learning tool that promotes awareness and responsible behavior in the digital environment, was successfully achieved. The results obtained during the testing phase demonstrated that the game effectively captured users' attention and encouraged reflection on the consequences of their online decisions. The functionality tests confirmed that the system operates correctly according to the defined requirements, while the usability evaluation indicated a high level of satisfaction among participants. However, some limitations were identified, particularly regarding the variety of scenarios available in the current version and the dependence on access to technological resources, which could restrict its use in certain educational environments. Based on these findings, future improvements are expected to focus on expanding the range of scenarios related to cybersecurity and emotional health, incorporating customization features for the main character and environment to enhance player engagement, integrating analytical tools to measure educational impact, and developing multiplatform versions to reach a broader audience. In conclusion, the video game represents a valuable and innovative educational resource that combines entertainment and learning, contributing to the promotion of digital literacy and emotional self-management among teenagers.

Author Contributions: **Alexander Rangel:** Supervision, Project administration, Funding acquisition. **Jose Peña:** Software, Visualization, Data curation. **Alejandro Cuello:** Investigation, Resources, Data curation. **Ana Meza:** Conceptualization, Methodology, Writing – original draft. **Julian Castro:** Validation, Formal analysis, Writing – review & editing.
All authors have read and agreed to the published version of the manuscript. Please refer to the CRediT taxonomy for the definitions of the terms. Authorship is limited to those who have made substantial contributions to the reported work.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable, since the present study does not involvehuman personnel or animals.

Informed Consent Statement: This study is limited to the use of technological resources, so nohuman personnel or animals are involved.

Conflicts of Interest: Under the authorship of this research, it is declared that there is no conflict of interest with the present research.

References

1. Cobacango, M. J., Cedeño, V. P., and Tinoco, M. G. (2019). La ciberadicción en la conducta de los estudiantes. *Revista Atlante: Cuadernos de Educación y Desarrollo*, 11763:1–13.

2. Díaz-López, A., Maquilón, J. J., and Mirete, A. B. (2020). Uso desadaptativo de las tic en adolescentes: Perfiles, supervisión y estrés tecnológico. *Revista Científica de Educomunicación*, (64):29–38.
3. Harán, J. M. (2019). Doble factor de autenticación: la solución más efectiva para prevenir el secuestro de cuentas.
4. Harán, J. M. (2020). El 99,9% de las cuentas vulneradas no utilizan doble factor de autenticación.
5. INCIBE (2023). Suplantación y robo de identidad en las redes sociales, un riesgo para las empresas.
6. Katsantonis, I., Karagiannopoulos, V., Tzafilkou, K., and Protogeros, N. (2022). Gamification in cybersecurity education: A systematic literature review. *Computers & Education*, 191:104642.
7. Pedrero Zornoza, J. (2020). Suplantación de identidad.
8. Ramírez Asís, E. H., Norabuena Figueroa, R. P., Toledo Quiñones, R. E., and Henostroza Márquez Mázmela, P. R. (2022). Validación de una escala de conciencia sobre ciberdelito en estudiantes universitarios de perú. *Revista Científica General José María Córdova*, 20(37):209–224.
9. Villagrasa, S., Fonseca, D., Redondo, E., and Duran, J. (2018). Teaching case of gamification and visual technologies for education. *Journal of Cases on Information Technology*, 20(2):38–55.

Authors’ Biography

Alexander Rangel V. Mathematics student at the Universidad del Norte.

Jose Peña C. Systems Engineering student at the Universidad del Norte.

Alejandro Cuello N. Systems Engineering student at the Universidad del Norte.

Ana Meza G. Mathematics student at the Universidad del Norte

Julian Castro C. Mathematics student at the Universidad del Norte

Disclaimer/Editor's Note: Statements, opinions, and data contained in all publications are solely those of the individual authors and contributors and not of the OnBoard Knowledge Journal and/or the editor(s), disclaiming any responsibility for any injury to persons or property resulting from any ideas, methods, instructions, or products referred to in the content.