Gamification in Education for Phishing Prevention: A Systematic Review

Alexis José Dominguez Aguila[1]; Randdy Samhir Ojeda Marchán[2]; Francisco Alonso Donayre Monteza[3]
[1,2,3]Universidad Tecnológica del Perú, u20216232@utp.edu.pe, u20213568@utp.edu.pe, c29224@utp.edu.pe

Abstract– Digital transformation has increased users' exposure to cyber threats, with phishing being one of the most frequent. Although informational campaigns exist, many users do not adopt effective preventive measures. In this context, gamification has emerged as an innovative educational strategy to enhance awareness of phishing. This systematic review analyzes the use of gamification techniques in preventive education, evaluating their benefits, limitations, and effectiveness compared to traditional methods. The PRISMA methodology was applied using the PICO framework, and the databases EBSCOHOST Xplore, ACM Digital Library, and Scopus were consulted, considering studies published between 2020 and 2025. Out of 246 articles identified, after removing duplicates and applying inclusion and exclusion criteria, 33 were selected for analysis. The most common gamified strategies include interactive simulations, serious games, reward systems, and dynamic feedback. These approaches have proven effective in improving knowledge retention and raising awareness about phishing attacks. However, some limitations were identified, such as limited adaptation to different user profiles, lack of comprehensive conceptual coverage, and insufficiently standardized evaluation mechanisms. It is concluded that gamification represents a promising alternative in cybersecurity education, but its effectiveness depends on instructional design, clear objectives, and the integration of appropriate evaluation systems.

Keywords: Gamification, Phishing prevention, Cybersecurity awareness, Digital education, Interactive learning, Systematic review

Gamificación en la educación para la prevención del phishing: una revisión sistemática

Alexis José Dominguez Aguila[1]; Randdy Samhir Ojeda Marchán[2]; Francisco Alonso Donayre Monteza[c3]
[1,2,3]Universidad Tecnológica del Perú, u20216232@utp.edu.pe, u20213568@utp.edu.pe, c29224@utp.edu.pe

Resumen*– La transformación digital ha incrementado la exposición de los usuarios a amenazas cibernéticas, siendo el phishing una de las más comunes y persistentes. A pesar de existir campañas informativas, muchos usuarios no adoptan medidas preventivas efectivas. En este contexto, la gamificación ha surgido como una estrategia educativa innovadora para mejorar la concienciación y respuesta frente al phishing. El objetivo de esta revisión sistemática es analizar el uso de técnicas de gamificación en la educación para prevenir ataques de phishing, identificando sus beneficios, limitaciones y su efectividad comparada con métodos tradicionales. Se aplicó la metodología PRISMA, guiada por el enfoque PICO, y se consultaron tres bases de datos científicas: EBSCOHOST Xplore, ACM Digital Library y Scopus, considerando publicaciones entre 2020 y 2025. Se identificaron inicialmente 246 artículos, de los cuales se eliminaron 6 duplicados. Tras el proceso de cribado y aplicación de criterios de inclusión y exclusión, se evaluaron 51 estudios, y finalmente se seleccionaron 33 artículos relevantes para el análisis. Los resultados muestran que las estrategias gamificadas más utilizadas incluyen simulaciones interactivas, juegos serios, sistemas de recompensas y retroalimentación dinámica. Estas han demostrado ser efectivas en el aumento de la retención del conocimiento y en la concienciación de los usuarios frente a ataques de phishing. Sin embargo, persisten limitaciones relacionadas con la falta de adaptación a distintos perfiles de usuario, la cobertura conceptual y los mecanismos de evaluación. Se concluye que la gamificación representa una alternativa prometedora para fortalecer la educación en ciberseguridad, pero su efectividad depende del diseño instruccional, la claridad de objetivos y su integración con métodos evaluativos apropiados.

Palabras clave: Gamificación, Prevención del phishing, Concienciación en ciberseguridad, Educación digital, Aprendizaje interactivo, Revisión sistemática.

I. Introducción

En el contexto actual de creciente conectividad digital, los usuarios realizan gran parte de sus actividades cotidianas como estudiar, trabajar, comprar y comunicarse a través de internet. Esta dependencia tecnológica ha incrementado su exposición a diversas amenazas cibernéticas, entre las cuales el phishing destaca por su frecuencia, sofisticación y persistencia. Este tipo de ataque, basado en la ingeniería social, emplea técnicas engañosas como mensajes o interfaces falsas para obtener información personal, credenciales o datos financieros de los usuarios [1]. Según el Anti-Phishing Working Group, en el primer trimestre de 2023 se registraron más de 1.35 millones de ataques mensuales, lo que evidencia la magnitud del problema [2].

A pesar de los esfuerzos por sensibilizar a los usuarios mediante campañas informativas, muchas personas siguen sin adoptar medidas de seguridad adecuadas. Esto demuestra que el conocimiento teórico por sí solo no garantiza comportamientos seguros en el entorno digital. Frente a esta limitación, la gamificación ha emergido como una estrategia educativa innovadora que emplea dinámicas propias de los juegos como recompensas, misiones, niveles o retroalimentación inmediata en contextos no lúdicos para mejorar la motivación, el compromiso y la eficacia del aprendizaje.

Diversos estudios han explorado el uso de la gamificación en la educación en ciberseguridad, reportando resultados prometedores en cuanto a la retención del conocimiento y la concienciación de los usuarios frente al phishing [5]. Sin embargo, muchas de estas iniciativas presentan debilidades, como la falta de adaptación a distintos perfiles de usuario, una cobertura limitada de conceptos clave o la ausencia de mecanismos robustos para evaluar el aprendizaje. Asimismo, aún no se cuenta con una revisión sistemática que integre, compare y analice de manera estructurada las fortalezas y debilidades de estas propuestas gamificadas en educación contra el phishing.

Por ello, esta revisión sistemática tiene como objetivo analizar el uso de técnicas de gamificación en la educación para prevenir ataques de phishing, identificando sus beneficios, limitaciones y su efectividad en comparación con los métodos tradicionales. Con ello se busca sentar las bases para el diseño de futuras estrategias educativas más efectivas, inclusivas y adaptadas a diversos públicos.

Este documento se organiza de la siguiente manera: en la Sección II se describe la metodología empleada, basada en el modelo PRISMA y el enfoque PICO; en la Sección III se presentan los resultados obtenidos, segmentados en análisis bibliométrico y de contenido; la Sección IV discute los hallazgos más relevantes; y finalmente, en la Sección V, se exponen las conclusiones y recomendaciones para futuras investigaciones.

II. METODOLOGIA

Con el objetivo de identificar las metodologías más prometedoras y efectivas para la educación en la prevención del phishing mediante el uso de la gamificación, se llevó a cabo una revisión sistemática de la literatura, aplicando un proceso riguroso de búsqueda y selección de estudios relevantes. Para estructurar la pregunta de investigación y

guiar el proceso de búsqueda, se utilizó la estrategia PICO, un acrónimo que estructura las preguntas de investigación en cuatro componentes clave: Población o problema, Intervención, Comparación y Outcome como resultado esperado [6]. Esta estrategia facilita la formulación precisa de preguntas de investigación y mejora la calidad del proceso de búsqueda y análisis de la evidencia científica.

El proceso para desarrollar la estrategia se realizó de la siguiente manera: en la Tabla I se presenta la formulación de la pregunta de investigación utilizando el modelo PICO, tomando como base el tema central del estudio y desglosándolo según los componentes del acrónimo. En la Tabla II, muestra la selección de las palabras clave más adecuadas, basada en la estructura PICO y en los términos más utilizados en la literatura relevante. Finalmente, en la Tabla III, se detallan las ecuaciones de búsqueda, integrando los términos clave tanto en inglés como en español, adaptadas para su implementación en diferentes bases de datos académicas.

TABLA I – Descripción de la pregunta PICO

Tema de investigación: Gamificación en la educación para la prevención del phishing	
Pregunta general: ¿De qué manera la gamificación contribuye en la educación para la toma de decisiones frente a ataques de phishing?	
Acrónimo y componente	Subpreguntas
P: Limitaciones en la educación para prevenir el phishing.	¿Cuáles son las principales deficiencias o retos en la educación actual respecto a la prevención del phishing?
I: Uso de la gamificación como estrategia educativa	¿Qué técnicas de gamificación se están utilizando para enseñar a prevenir ataques de phishing?
C: Comparación con métodos educativos tradicionales	¿En qué aspectos la gamificación supera a las estrategias tradicionales en la prevención de ataques de phishing?
O: Efectividad de la gamificación en la prevención del phishing	¿Qué nivel de efectividad tiene la gamificación para reducir la vulnerabilidad frente al phishing en comparación con otras estrategias educativas?

TABLA II – Descripción de las palabras clave

Acrónimo y componente	Subpreguntas
P: Limitaciones en la educación para prevenir el phishing.	Phishing, phishing attacks, cybersecurity training, limitations, constraints
I: Uso de la gamificación como estrategia educativa	gamification, game-based learning, serious games, educational strategy
C: Comparación con métodos educativos tradicionales	Education, comparison, benchmarking
O: Efectividad de la gamificación en la prevención del phishing	Effectiveness, phishing prevention, awareness

TABLA III – Descripción de las ecuaciones de búsqueda

Acrónimo	Subpreguntas
P	Phishing, phishing attacks, cybersecurity training, limitations, constraints
I	gamification, game-based learning, serious games, educational strategy
C	Education, comparison, benchmarking
O	Effectiveness, phishing prevention, awareness
EB1 – SCOPUS: ((phishing OR "phishing attacks" OR "cybersecurity training" OR limitations OR constraints) AND (gamification OR "game-based learning" OR "serious games" OR "educational strategy") AND (education OR benchmarking OR comparison) AND (effectiveness OR "phishing prevention" OR awareness))	
EB2 – EBSCO: (gamification OR game-based learning) AND (phishing OR cybersecurity) AND (education OR training)	
EB3 – ACM Digital: ((phishing OR "phishing attacks" OR "cybersecurity training" OR limitations OR constraints) AND (gamification OR "game-based learning" OR "serious games" OR "educational strategy") AND (education OR benchmarking OR comparison) AND (effectiveness OR "phishing prevention" OR awareness))	

La búsqueda bibliográfica se realizó utilizando ecuaciones específicas diseñadas para tres bases de datos académicas: Scopus, EBSCOhost y ACM Digital Library. Para asegurar la pertinencia de los estudios seleccionados, se definieron criterios de elegibilidad que incluyeron tanto criterios de inclusión como de exclusión, con el objetivo de garantizar que los estudios seleccionados fueran relevantes para el tema de prevención de phishing mediante el uso de la gamificación.

TABLA IV – Descripción de los criterios de elegibilidad

N°	CRITERIOS DE INCLUSIÓN	N°	CRITERIOS DE EXCLUCIÓN
CI1	Estudios que aborden el fenómeno del phishing o ataques de ingeniería social.	CE1	Estudios centrados solo en aspectos técnicos de ciberseguridad sin enfoque educativo.
CI2	Estudios que describan o apliquen métodos de enseñanza mediante gamificación.	CE2	Publicaciones en idiomas distintos al inglés o español.
CI3	Estudios que reporten resultados, métricas o evaluaciones del impacto educativo.	CE3	Artículos publicados antes de 2020.
CI4	Estudios realizados en entornos educativos (escolares, universitarios o laborales).	CE4	Publicaciones que no sean investigaciones originales (e.g., editoriales, reseñas, etc.).

Como resultado de la búsqueda inicial, se identificaron 246 artículos: 213 en Scopus, 23 en EBSCOhost y 10 en ACM Digital Library. Tras eliminar 6 duplicados, se procedió al cribado inicial, en el cual fueron excluidos 160 artículos por no alinearse con el enfoque de esta revisión sistemática.

Se seleccionaron 82 artículos como potencialmente relevantes. Sin embargo, 28 de estos no estaban disponibles en texto completo, resultando en un total de 51 artículos para la evaluación de elegibilidad. Durante esta etapa, se aplicaron criterios de exclusión adicionales, lo que llevó a descartar 18 artículos, entre ellos: aquellos que se centraron solo en aspectos técnicos de ciberseguridad sin enfoque educativo, publicaciones con antigüedad superior a 5 años y los publicados en idiomas distintos al inglés o español. Finalmente, se incluyeron 33

artículos en la revisión sistemática, distribuidos de la siguiente manera: 20 provenientes de Scopus, 11 de EBSCOhost y 2 de ACM Digital Library.

El proceso completo de selección se representa en el diagrama PRISMA [7], que se muestra a continuación. Este diagrama permite visualizar de forma clara y transparente las etapas del proceso de búsqueda, selección y exclusión, asegurando la trazabilidad y rigurosidad metodológica de la revisión. Los 33 estudios seleccionados proporcionan una base sólida para el análisis de las metodologías más eficaces en la educación para la prevención del phishing mediante gamificación.

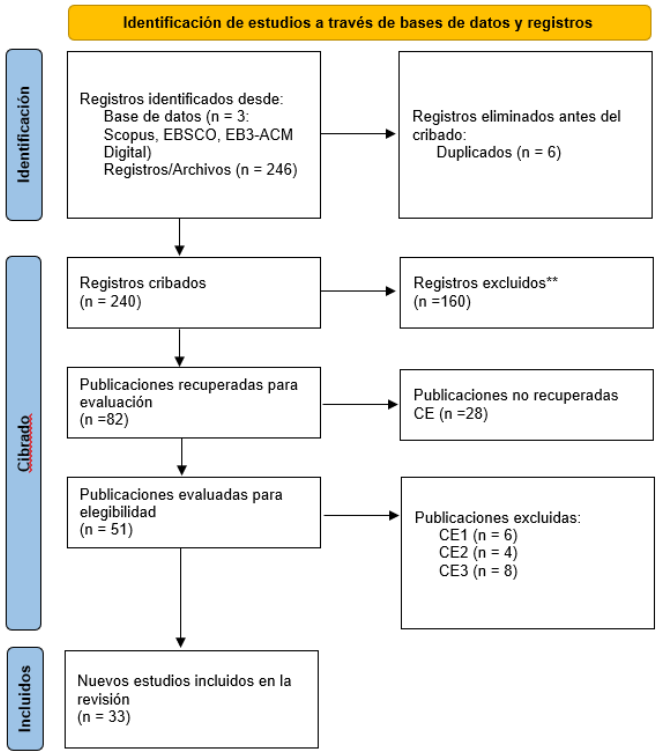

Fig. 1 Diagrama de flujo de selección de artículos [7].

III. RESULTADOS

Para el desarrollo de la fase de resultados, se segmento en dos secciones: datos bibliométricos y datos de contenido. La sección de resultados bibliométricos presenta una tabla con los artículos elegidos, un gráfico que ilustra la cantidad de artículos por año, el tipo de publicación, la metodología utilizada y su ubicación geográfica. En la sección de contenido, se abordan las preguntas formuladas en la metodología PICO [6], haciendo uso de los datos de los artículos seleccionados.

DATOS BIBLIOMÉTRICOS

En base a los criterios utilizados en la metodología respecto al uso de la gamificación como estrategia educativa para la prevención del phishing entre los años 2020 y 2025, se ha notado una tendencia creciente en el número de publicaciones, con 2 artículos en 2020, 3 en 2021, 6 en 2022, y alcanzando un pico de 9 en 2023. Posteriormente, se registra una leve disminución con 8 publicaciones en 2024 y 5 en 2025. Esta evolución se muestra en el siguiente gráfico.

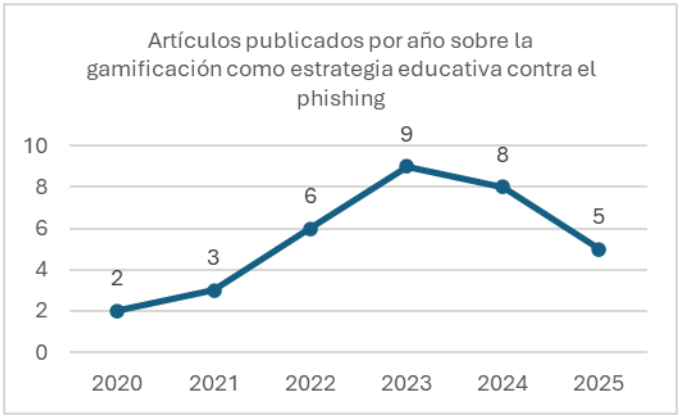

Fig. 2 Número de artículos publicados por año sobre la gamificación como estrategia educativa contra el phishing.

Con la base bibliográfica que contamos para la elaboración de la revisión sistémica muestra que existe una predominancia de publicaciones en el formato de ponencias en congreso 12, seguidas por artículos en revistas académicas 11. En menor medida, se identificaron artículos científicos 6, publicaciones en revistas científicas 3 y capítulos de libro 1 Esta distribución sugiere que gran parte de los estudios vinculados con la gamificación como estrategia educativa para la prevención del phishing han sido difundidos principalmente en congresos y, en menor grado, en publicaciones científicas consolidadas. A continuación, se presenta dicha distribución mediante un gráfico.

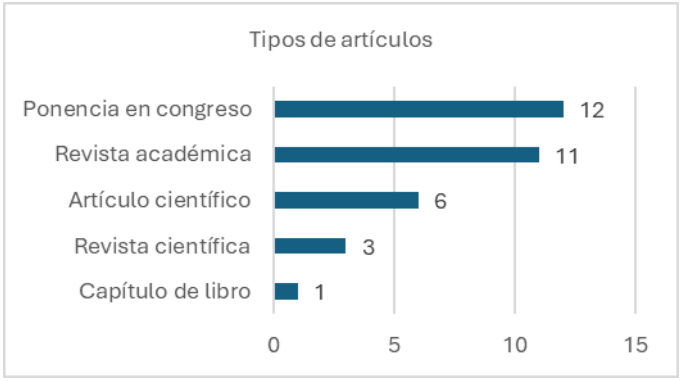

Fig. 3 Tipos de artículos publicados sobre la gamificación como estrategia educativa contra el phishing.

A partir de la base bibliográfica considerada en esta Revisión Sistemática se identifica que la gran parte de los estudios revisados sobre la gamificación como estrategia educativa para prevenir el phishing emplearon metodologías mixtas 43%, seguidos por aquellos que aplicaron un enfoque cuantitativo 36%. En menor proporción, se identificaron estudios con enfoque cualitativo 15% y conceptual 6%. Esta distribución refleja una tendencia hacia la integración de métodos en los trabajos analizados. La siguiente figura muestra gráficamente la proporción de metodologías identificadas en los documentos analizados.

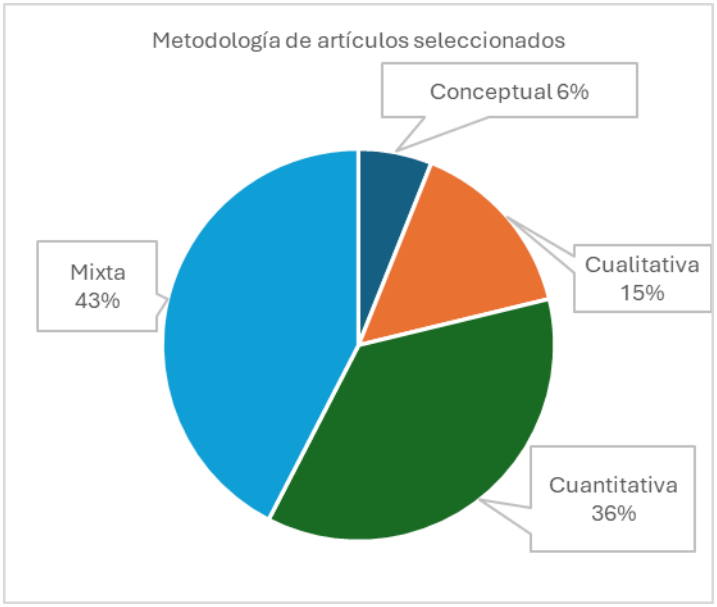

Fig. 4 Tipo de metodología de artículos publicados sobre la gamificación como estrategia educativa contra el phishing.

La distribución geográfica de los artículos incluidos en la revisión revela que la mayoría de las investigaciones se originan en Estados Unidos, con un total de 9 publicaciones. Le siguen países como Reino Unido, Alemania, Suecia, Italia y Singapur, cada uno con 2 estudios. El resto de los países incluidos Suiza, Arabia Saudita, Portugal, Camerún, Países Bajos, Grecia, Malaysia y Pakistán (en coautoría), Colombia, Jordania, Bahréin, Irak, Suecia, e Indonesia están representados con un solo artículo. Esta diversidad evidencia un interés internacional en el estudio de la gamificación como estrategia educativa para prevenir el phishing, con una concentración más significativa en regiones de habla inglesa y países europeos.

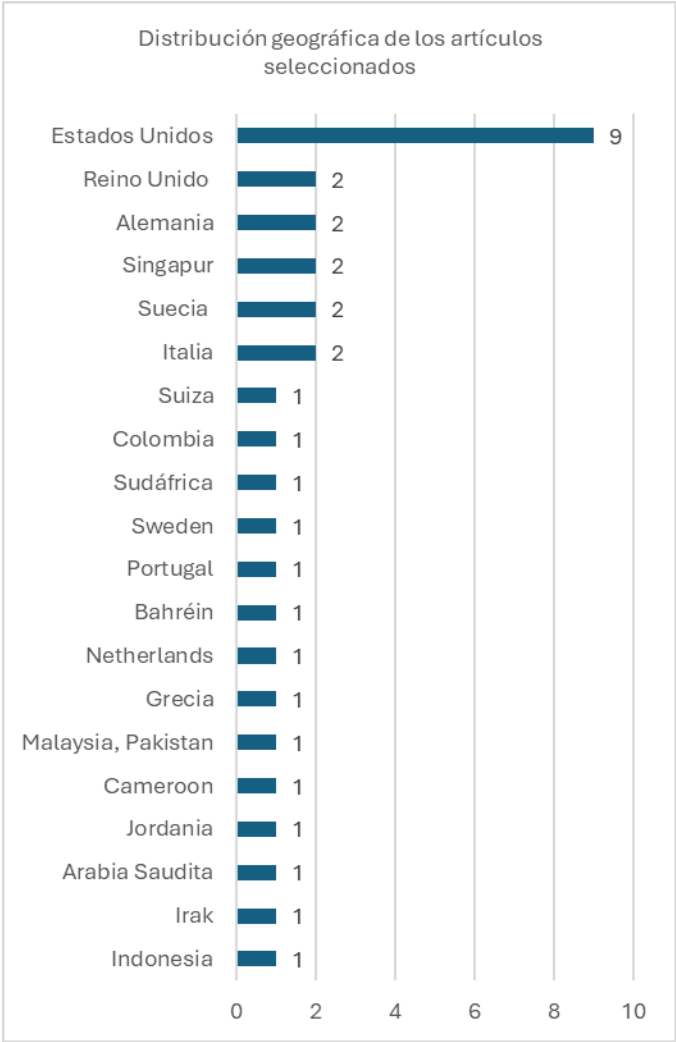

Fig. 5 Distribución geográfica de artículos seleccionados sobre la gamificación como estrategia educativa contra el phishing.

DATOS DE CONTENIDO

A. *¿Cuáles son las principales deficiencias o retos en la educación actual respecto a la prevención del phishing?*

Los resultados de los estudios revisados identifican que existe una serie de deficiencias comunes en los enfoques educativos, especialmente en aquellos cuyo enfoque es la prevención del phishing. Uno de los retos principales es la falta de aplicación del conocimiento teórico en un contexto practico, esto impide que los usuarios actúen eficazmente frente a situaciones reales, pese a haber adquirido información previa. En simulaciones de ataques, más del 50% de los usuarios que participan aun ingresan y hacen clic sobre enlaces maliciosos luego de haber recibido entrenamientos convencionales [1, 8, 14].

Las campañas de concienciación tradicionales presentan resultados con impacto limitado y de corta duración. En algunas situaciones, la merma de errores en simulaciones de ataques apenas alcanza el 10% tras la intervención, y este efecto tiende a reducirse en el mediano plazo si es que no se refuerza con entrenamiento práctico [9, 14]. Otra de las deficiencias es la falta de adaptación a públicos diversos, como adultos mayores, estudiantes sin formación técnica o personas con bajo nivel de alfabetización digital reduciendo significativamente el alcance y la efectividad de los métodos educativos actuales [8, 28]. De igual forma, se indica la existencia de una dependencia muy preocupante a herramientas automatizadas, como los modelos de leguaje (LLMs), que pueden incitar a errores si es que no se aplican bajo un pensamiento crítico [22].

A nivel estructural, varios de los estudios revisados destacan la poca presencia de marcos pedagógicos que sean claros y estandarizados, así como la falta de taxonomías educativas que estén orientadas al diseño de programas formativos en ciberseguridad [23, 36]. Además, la falta de estudios longitudinales que impiden evaluar el impacto real de las intervenciones educativas a largo plazo [23, 36]. Solo un 21% de las intervenciones revisadas aborda tácticas avanzadas de phishing, lo que limita la profundidad del contenido impartido [1].

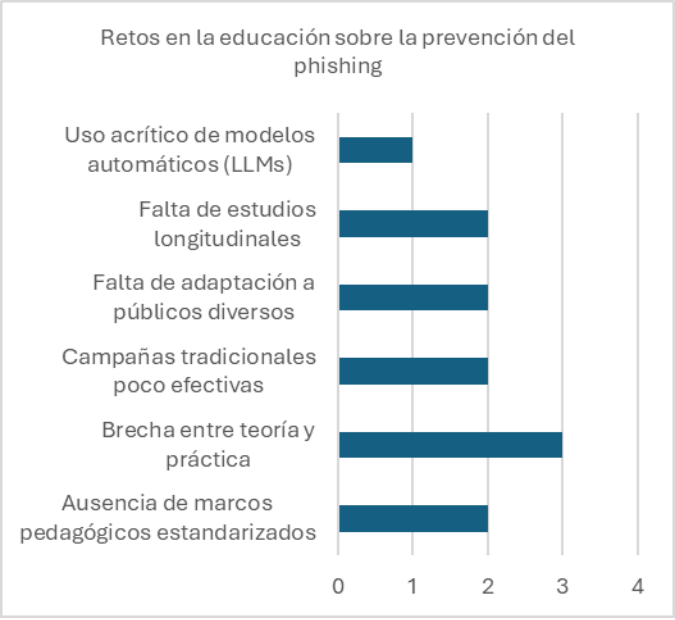

Fig. 6 Frecuencia de retos identificados en la educación para la prevención del phishing.

B. ¿Qué técnicas de gamificación se están utilizando para enseñar a prevenir ataques de phishing?

En los resultados de los estudios que fueron incluidos en la revisión, se identificaron diferentes técnicas de gamificadas diseñadas para prevenir ataques de phishing bajo un contexto educativo.

Una de las técnicas más frecuentes es el uso de sistemas de recompensas, puntos, insignias y niveles de progresión. El modelo Gamified Peer-Reviewed Bug Bounty Programme, emplea recompensas simbólicas, revisión por pares y validación colaborativa para fomentar el descubrimiento de vulnerabilidades, de esta forma logra involucrar de forma sostenible a los estudiantes incluso en contextos con escasos recursos [34]. También existen propuestas basadas en simulación de escenarios reales de ataque, como PeriHack o CyberHero, donde los participantes deben tomar decisiones en tiempo real frente a intentos de phishing en entornos simulados. Estas técnicas, al combinar elementos de rol o narrativa interactiva, promueven la toma de decisiones y el pensamiento estratégico [24, 26]. Otros métodos gamificados adaptan su dificultad de contenido al nivel del usuario. Este enfoque esta adaptado en juegos como CyberHero o sistemas como iCAT, de esta forma se mantiene una curva de aprendizaje adecuada y facilita la autorregulación en los estudiantes [16, 24].

En otros contextos como la educación financiera o informática general, se pueden identificar situaciones similares de técnicas transferibles. El uso de misiones, narrativas y retroalimentación inmediata aseguran el aprendizaje complejo mediante experiencias gamificadas [38]. Por su parte, el modelo RAD-SIM organiza diferentes elementos como la narrativa, la cooperación social y la reflexión metacognitiva, lo que proporciona una guía sistemática para diseñar juegos educativos efectivos [23].

Si bien la mayoría de los autores de los estudios incluidos en la revisión, coinciden en los beneficios de estas técnicas, algunos estudios advierten algunas limitaciones. Se señala que, muchas experiencias gamificadas carecen de una profundidad conceptual y se centran mayormente en mecánicas superficiales, lo que podría reducir el impacto educativo a largo plazo. Además, no todos los juegos gamificados implementan procesos de evaluación que permitan medir su efectividad real [1].

TABLA V – Técnicas de gamificación destacadas en los artículos revisados.

Técnica principal	Métodos
Recompensas y validación	Puntos, logros, revisión por pares, ranking
Adaptación al nivel del usuario	Dificultad dinámica, personalización del aprendizaje
Simulación de ataques	Juegos de rol, escenarios de phishing, decisiones estratégicas

Narrativa y storytelling	Misiones, personajes, entornos narrativos inmersivos
Microlearning y retroalimentación	Contenido breve, feedback inmediato, visualizaciones interactivas
Colaboración y roles	Dinámicas de equipo, roles de atacante y defensor

Complementando la información presentada en la tabla anterior, el siguiente gráfico proporciona una representación visual más clara de las técnicas de gamificación identificadas, clasificadas por tipo. Este permite observar de manera comparativa la frecuencia con la que cada técnica ha sido reportada en los estudios revisados, lo que facilita identificar cuáles enfoques tienen mayor presencia y relevancia en las propuestas educativas orientadas a la prevención del phishing.

Fig. 7 Frecuencia de estudios que respaldan cada técnica gamificadas para la prevención del phishing.

C. *¿En qué aspectos la gamificación supera a las estrategias tradicionales en la prevención de ataques de phishing?*

Para responder esta pregunta se identificaron aspectos clave en los que la gamificación supera a las estrategias educativas tradicionales, especialmente en la prevención del phishing. Dentro de las ventajas más destacadas se encuentran la retención del conocimiento, el desarrollo de habilidades prácticas, el compromiso sostenido, la transferencia del aprendizaje y la personalización del contenido [1, 9, 16, 23, 24, 34, 36].

En cuanto a la retención del conocimiento, se han registrado mejoras significativas. Los participantes que entrenaron mediante simulación gamificada lograron un desempeño 40% superior en la identificación de amenazas frente a aquellos capacitados con métodos tradicionales [9]. El aprendizaje basado en juegos contribuyó a un recuerdo más duradero de los conceptos clave en seguridad digital [36].

Respecto al desarrollo de habilidades prácticas, los entornos gamificados permiten aplicar conocimientos adquiridos en escenarios que simulan situaciones reales. En estos entornos, los usuarios deben tomar decisiones bajo presión y evaluar las consecuencias de sus acciones, lo que fortalece su capacidad de respuesta ante amenazas de phishing [1], [9], [24]. En relación con la motivación y el compromiso, se han reportado incrementos del 50 % en la participación activa cuando se utilizan plataformas gamificadas, en comparación con métodos expositivos tradicionales [16]. Este mayor compromiso se atribuye a elementos como retroalimentación inmediata, recompensas simbólicas, desafíos progresivos y narrativa inmersiva [23], [34]. En cuanto a la transferencia del aprendizaje, se ha observado que los participantes entrenados mediante juegos serios cometen hasta un 30 % menos de errores en pruebas prácticas posteriores al entrenamiento [9]. Este tipo de práctica situacional facilita el reconocimiento de patrones de ataque y promueve una respuesta más consciente frente a amenazas reales.

En términos de adaptabilidad, se destacan plataformas que ajustan la dificultad de los desafíos según el nivel del usuario, lo que permite una experiencia personalizada y progresiva [16], [24]. A diferencia de los métodos homogéneos tradicionales, este enfoque permite cubrir mejor las necesidades individuales.

No obstante, algunos estudios advierten limitaciones en ciertas experiencias gamificadas. Se señala que en algunos casos se prioriza el entretenimiento visual sobre la profundidad conceptual, lo que puede reducir la efectividad del aprendizaje si no se vinculan claramente los objetivos educativos [1]. También se indica la necesidad de más estudios longitudinales que evalúen el impacto sostenido de la gamificación en el tiempo [36].

TABLA VI – Ventajas de la gamificación frente a métodos tradicionales en la educación sobre phishing

Aspecto comparado	Ventaja de la gamificación
Retención del conocimiento	Favorece la memorización duradera mediante interacción activa
Desarrollo de habilidades prácticas	Permite aplicar conocimientos en contextos simulados reales
Motivación y compromiso	Uso de recompensas, feedback inmediato y progresión adaptada
Personalización del aprendizaje	Ajuste de dificultad y dinámicas según el perfil del usuario
Transferencia del aprendizaje	Facilita aplicar lo aprendido ante amenazas reales

D. ¿Qué nivel de efectividad tiene la gamificación para reducir la vulnerabilidad frente al phishing en comparación con otras estrategias educativas?

Los estudios revisados coinciden en que la gamificación ha demostrado una alta efectividad para reducir la vulnerabilidad frente a ataques de phishing, superando en múltiples casos los resultados obtenidos mediante estrategias educativas tradicionales.

Uno de los indicadores más consistentes es la disminución de errores durante simulaciones de phishing. En varios estudios, los participantes capacitados mediante métodos gamificados lograron tasas de clics maliciosos entre 30 % y 50 % más bajas que aquellos formados con métodos tradicionales [9, 24, 36]. En términos de retención del conocimiento, se ha reportado que los usuarios entrenados con juegos gamificados recuerdan conceptos clave hasta dos veces más tiempo que quienes reciben charlas expositivas o capacitaciones lineales [36]. Esta mejora en la memoria se refuerza mediante la repetición contextualizada y el feedback inmediato, aspectos centrales en la gamificación [23].

Asimismo, la transferencia del aprendizaje a contextos reales se evidencia en una mayor capacidad para aplicar medidas preventivas, como la verificación de remitentes o el análisis de enlaces sospechosos. En contraste, las intervenciones convencionales suelen tener efectos de corta duración y poca influencia en la conducta real del usuario [1, 23]. Un hallazgo particularmente importante es la sostenibilidad de los efectos a mediano plazo. Algunos programas gamificados mostraron mantener mejoras en la conducta segura incluso semanas después de finalizada la intervención, lo que representa una ventaja frente a métodos informativos cuya efectividad tiende a diluirse rápidamente [24, 36].

Por otro lado, aunque los resultados son prometedores, algunos estudios advierten sobre limitaciones como la superficialidad de algunos contenidos gamificados o la falta de estandarización en la evaluación de resultados, lo que dificulta comparar entre experiencias y contextos diversos [1, 36].

En conjunto, la evidencia recopilada en los artículos revisados muestra que la gamificación no solo es efectiva, sino que representa una estrategia superior en términos de reducción de vulnerabilidad, retención del aprendizaje y generación de comportamientos seguros en entornos digitales. Para complementar los hallazgos descritos, la siguiente tabla presenta los principales indicadores de efectividad identificados en los estudios revisados.

TABLA VII – Indicadores de efectividad de la gamificación en la prevención del phishing

Indicador	**Resultados**	**Referencias**
Disminución de errores en simulaciones de ataque	Hasta 50 % menos errores al identificar correos falsos	[9], [24], [36]
Tasa de clics en enlaces maliciosos	Reducción significativa tras el entrenamiento gamificado	[16], [24], [38]
Retención del conocimiento	Recordación del contenido hasta el doble de tiempo en comparación con métodos expositivos	[36], [23]
Transferencia del aprendizaje	Aplicación efectiva de lo aprendido en escenarios reales	[1], [23], [24]
Sostenibilidad del efecto educativo	Resultados mantenidos semanas después de la intervención	[24], [36]
Participación activa y autoeficacia percibida	Mayor confianza y compromiso respecto a estrategias convencionales	[23], [38], [16]

IV. DISCUSION

Los resultados obtenidos en esta revisión sistemática permiten identificar patrones relevantes respecto al uso de la gamificación como estrategia educativa en la prevención del phishing. Una de las deficiencias más recurrentes en los enfoques tradicionales es la desconexión entre el conocimiento teórico y la aplicación práctica. Si bien muchas iniciativas de concienciación transmiten información básica sobre ciberataques, los usuarios no logran aplicar dichos conocimientos en escenarios reales, lo cual se traduce en bajos niveles de desempeño en simulaciones o ejercicios prácticos [1], [8], [9]. Esta brecha entre teoría y práctica también se ve agravada por la falta de adaptación a públicos diversos, lo cual limita el impacto educativo al ignorar variables como la edad,

el nivel de alfabetización digital o la familiaridad con entornos tecnológicos [8], [14], [28], [33].

Adicionalmente, varios estudios señalan que las estrategias convencionales se centran en enfoques homogéneos, sin considerar la personalización del aprendizaje, lo que reduce el compromiso de los usuarios y la retención del conocimiento a mediano y largo plazo [1], [23], [36]. Incluso en contextos más innovadores, como el uso de tecnologías emergentes (ej. modelos de lenguaje como ChatGPT), se ha evidenciado el riesgo de fomentar errores si no se entrena el pensamiento crítico en paralelo, reforzando la necesidad de marcos pedagógicos sólidos [22].

En contraste, las técnicas gamificadas identificadas muestran mayor efectividad, al integrar mecanismos psicológicos y pedagógicos que favorecen el aprendizaje activo. Las estrategias más comunes, como las simulaciones de ataques, las recompensas simbólicas, la narrativa inmersiva y el microlearning adaptativo, activan la motivación intrínseca de los usuarios y mejoran su disposición a aprender [16], [23], [24], [26], [34], [38]. En particular, entornos como CyberHero o el modelo iCAT han demostrado mejoras significativas en retención y transferencia del aprendizaje, gracias a su enfoque adaptativo, retroalimentación inmediata y progresión por niveles [16], [24], [38].

Los juegos serios que emulan escenarios de phishing permiten a los usuarios tomar decisiones bajo presión, evaluar riesgos y recibir consecuencias simuladas por sus acciones. Estas dinámicas fomentan habilidades prácticas que son difíciles de adquirir mediante métodos expositivos tradicionales [9], [13], [23], [24]. Por ejemplo, se reporta que los usuarios capacitados mediante simulaciones gamificadas cometieron hasta 50 % menos errores en la identificación de amenazas, y lograron una retención del conocimiento más duradera que los formados con charlas o materiales teóricos [9], [36].

Otro punto destacable es la motivación sostenida y el nivel de participación activa generado por los entornos gamificados. Estudios indican que los participantes muestran hasta un 50 % más de compromiso en comparación con cursos tradicionales, lo cual se asocia con la incorporación de feedback instantáneo, metas alcanzables y progresión visible [16], [23], [34]. Esta mayor implicación no solo mejora los resultados inmediatos, sino también la disposición a aplicar los conocimientos adquiridos en contextos reales, lo cual reduce la vulnerabilidad ante ataques.

Sin embargo, también se identifican limitaciones en los enfoques gamificados. Algunos estudios critican que ciertas experiencias priorizan el entretenimiento visual o la interactividad superficial, descuidando la cobertura de conceptos técnicos fundamentales. Solo un porcentaje limitado de propuestas aborda tácticas avanzadas o variantes sofisticadas de ataques de phishing [1], [36]. Además, la falta de marcos pedagógicos estandarizados dificulta la replicación de los resultados, y la escasez de estudios longitudinales impide evaluar la sostenibilidad del aprendizaje en el tiempo [23], [36].

En conjunto, los hallazgos sugieren que la gamificación, si se implementa con una base educativa bien diseñada, tiene el potencial de superar los métodos tradicionales en la formación en ciberseguridad, especialmente en lo referente a phishing. No obstante, su eficacia depende de la alineación entre mecánicas lúdicas, objetivos de aprendizaje y evaluación continua del impacto, evitando caer en soluciones estéticamente atractivas, pero pedagógicamente débiles.

V. CONCLUSIÓN

Esta revisión sistemática permitió analizar el estado actual de la gamificación aplicada a la educación en ciberseguridad, específicamente en la prevención del phishing. Los hallazgos muestran que, aunque existen esfuerzos formativos tradicionales, estos presentan deficiencias significativas, como la escasa transferencia del conocimiento a contextos reales, la limitada adaptación a distintos perfiles de usuarios y la baja efectividad en la modificación de conductas inseguras.

La gamificación se posiciona como una alternativa prometedora frente a estos retos. Los artículos revisados evidencian que las técnicas gamificadas como simulaciones, sistemas de recompensas, progresión adaptativa y narración de historias fomentan la motivación, incrementan la participación y mejoran tanto la retención del conocimiento como la capacidad de los usuarios para identificar y responder ante amenazas reales. Además, se ha documentado una reducción tangible en la vulnerabilidad frente al phishing en poblaciones entrenadas mediante juegos serios o plataformas lúdicas.

No obstante, la efectividad de la gamificación no es automática ni homogénea. Su éxito depende de una adecuada integración pedagógica, del equilibrio entre entretenimiento y contenido formativo, así como de una evaluación continua de resultados. A pesar de sus ventajas, aún se evidencian limitaciones como la falta de estandarización en marcos instruccionales, la escasa cobertura de conceptos avanzados y la ausencia de estudios longitudinales que midan el impacto sostenido en el tiempo.

En conclusión, la gamificación representa una estrategia educativa eficaz para reducir la vulnerabilidad frente al phishing, especialmente cuando se diseña con criterios pedagógicos sólidos y se adapta a las características del público objetivo. Futuras investigaciones deberían enfocarse en estandarizar las prácticas de diseño instruccional, evaluar el impacto a largo plazo y explorar el uso responsable de tecnologías emergentes que complementen la experiencia de aprendizaje sin reemplazar el pensamiento crítico.

REFERENCIAS

[1] Yasin, A., Fatima, R., JiangBin, Z., Afzal, W., & Raza, S. (2024). Can serious gaming tactics bolster spear-phishing and phishing resilience?: Securing the human hacking in information security. *Information and Software Technology, 170*, Article 107426.

[2] Anti-Phishing Working Group (APWG), Phishing Activity Trends Report – Q1 2023.

[3] Choudhary, A. S., Desai, R., Gupta, L., & Gedam, M. (2021). Detection and prevention of Phishing Attacks. Asian Journal of Convergence in Technology, 7(1), 193–196.

[4] Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2020). Cyber security awareness, knowledge and behavior: A comparative study. Journal of Computer Information Systems, 62(1), 82–97.

[5] Rodríguez León, D. M., Guerra Rodríguez, S., & Morillo Heredia, P. (2023). *Educación en ciberseguridad mediante estrategias de gamificación*.

[6] A. Nishikawa-Pacher, "Research Questions with PICO: A Universal Mnemonic," Publications, vol. 10, no. 3, p. 21, 2022.

[7] D. Moher, A. Liberati, J. Tetzlaff, D. G. Altman, y The PRISMA Group, "Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement," PLoS Med, vol. 6, no. 7, e1000097, 2009.

[8] S. Kazamia, C. Culnane, D. Gardham, S. Prior, and H. Treharne, "Phish and Tips: Phishing Awareness and Education for Older Adults," in Proceedings of the 17th International Conference on Availability, Reliability and Security (ARES '22), New York, NY, USA: ACM, 2022, pp. 1–10.

[9] C. Scherb, L. B. Heitz, F. Grimberg, H. Grieder, and M. Maurer, "A Cyberattack Simulation for Teaching Cybersecurity," EPiC Series in Computing, vol. 93, pp. 129–140, 2023.

[10] DeCusatis, C., Alvarico, E., & Dirahoui, O. (2022). Gamification of cybersecurity training. *Proceedings of the 1st International Workshop on Gamification of Software Development, Verification, and Validation*.

[11] Tareque, M. H., Deutekom, S., Anvik, J., & Bashir, M. (2024). You hacked my program! Teaching cybersecurity using game-based learning. *The 26th Western Canadian Conference on Computing Education*.

[12] J. B. Kim, C. Zhong, and H. Liu, "Teaching Tip: What You Need to Know about Gamification Process of Cybersecurity Hands-on Lab Exercises: Lessons and Challenges," *Journal of Information Systems Education*, vol. 34, no. 4, pp. 387-405, 2023.

[13] G. Tempestini, S. Merà, M. P. Palange, A. Bucciarelli, and F. Di Nocera, "Improving the Cybersecurity Awareness of Young Adults through a Game-Based Informal Learning Strategy," *Information*, vol. 15, no. 10, Oct. 2024. DOI: 10.3390/info15100607

[14] H. F. Vargas Montoya y F. A. Usma Guzmán, "Gamificación: Estrategia preventiva de ciberseguridad para sexting y grooming", *Rev. Logos Cienc. Tecnol.*, vol. 16, núm. 2, pp. 95–117, 2024.

[15] J. Kävrestad, A. Hagberg, M. Nohlberg, J. Rambusch, R. Roos, and S. Furnell, "Evaluation of Contextual and Game-Based Training for Phishing Detection," *Future Internet*, vol. 14, no. 104, Mar. 2022. DOI: 10.3390/fi14040104

[16] H. Taherdoost, "Towards an innovative model for cybersecurity awareness training", *Information (Basel)*, vol. 15, núm. 9, p. 512, 2024.

[17] Y. A. Younis and M. Y. Alghamdi, "The use of computer games for teaching and learning cybersecurity in higher education institutions," *Journal of Education and Research*, vol. 9, no. 3A, Sep. 2021. DOI: 10.36909/jer.v9i3A.10943

[18] N. Veerasamy, T. Mkhwanazi, y Z. Khan, "Digital innovation through cybersecurity learning factories", *Proc. Eur. Conf. Knowl. Manag.*, vol. 24, núm. 2, pp. 1383–1390, 2023.

[19] A. Tay, S. M Hayes, D. Wilson, E. Hall, y D. Kaufman, "Gamified cybersecurity education through the lens of the Information Search Process: An exploratory study of capture-the-Flag competitions [research-in-progress]", *Issues Informing Sci. Inf. Technol.*, vol. 21, p. 001, 2024.

[20] J. J Meadows y S. Sambasivam, "Mandatory gamified security awareness training impacts on Texas public middle school students: A qualitative study", en *InSITE Conference*, 2023, p. 024.

[21] H. M. Jawad y S. Tout, "Gamifying computer science education for Z generation", *Information (Basel)*, vol. 12, núm. 11, p. 453, 2021.

[22] T. Espinha Gasiba, A.-C. Iosif, I. Kessba, S. Amburi, U. Lechner, y M. Pinto-Albuquerque, "May the source be with you: On ChatGPT, cybersecurity, and secure coding", *Information (Basel)*, vol. 15, núm. 9, p. 572, 2024.

[23] L. Thompson, N. Melendez, J. Hempson-Jones, y F. Salvi, "Gamification in cybersecurity education: The RAD-SIM framework for effective learn", *Proc. Eur. Conf. Games-based Learn.*, vol. 16, núm. 1, pp. 562–569, 2022

[24] R. Hodhod, H. Hardage, S. Abbas, y E. A. Aldakheel, "CyberHero: An adaptive serious game to promote cybersecurity awareness", *Electronics (Basel)*, vol. 12, núm. 17, p. 3544, 2023.

[25] K. H. Sharif and S. Y. Ameen, "A Intelligent Security Power Lab (SPL): The Ultimate Serious Game Training in Cybersecurity," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 11, no. 11s, pp. 245–259, Aug. 2023.

[26] R. Dillon y Arushi, "'PeriHack': Designing a serious game for cybersecurity awareness", *arXiv [cs.CR]*, 2022.

[27] M. Silic y P. B. Lowry, "Using design-science based gamification to improve organizational security training and compliance", *J. Manag. Inf. Syst.*, vol. 37, núm. 1, pp. 129–161, 2020.

[28] S. Karagiannis y E. Magkos, "Engaging students in basic cybersecurity concepts using digital game-based learning: Computer games as virtual learning environments", en *Learning and Analytics in Intelligent Systems*, Cham: Springer International Publishing, 2021, pp. 55–81.

[29] P. A. Godejord y B. J. Godejord, "Computer games as a pedagogical tool for creating cyber security awareness", *Proc. Eur. Conf. Games-based Learn.*, vol. 17, núm. 1, pp. 220–224, 2023.

[30] T. Espinha Gasiba, U. Lechner, y M. Pinto-Albuquerque, "Cybersecurity Challenges in industry: Measuring the challenge solve time to inform future challenges", *Information (Basel)*, vol. 11, núm. 11, p. 533, 2020.

[31] F. Vapiwala y D. Pandita, "Leveraging gamified learning management systems to enhance E-learning outcomes", en *2024 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*, 2024, pp. 535–540.

[32] J. E. Ntsama, C. Fachkha, P. B. Owomo, y A. C. Focho, "A gamification architecture to enhance phishing awareness", en *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, Cham: Springer Nature Switzerland, 2024, pp. 37–57.

[33] E. T. Al-Shammari, "Integrating Protection Motivation Theory With Cultural Context: A Framework for Cybersecurity Education," *Journal of Cases on Information Technology*, vol. 27, no. 1

[34] J. O'Hare y L. A. Shepherd, "Developing a gamified peer-reviewed bug bounty programme", en *Communications in Computer and Information Science*, Cham: Springer International Publishing, 2022, pp. 514–522.

[35] L. Hafner, F. Wutz, D. Pöhn, y W. Hommel, "TASEP: A collaborative social engineering tabletop role-playing game to prevent successful social engineering attacks", en *Proceedings of the 18th International Conference on Availability, Reliability and Security*, 2023, pp. 1–10.

[36] K. Amjad, K. Ishaq, N. A. Nawaz, F. Rosdi, A. B. Dogar, y F. A. Khan, "Unlocking cybersecurity: A game-changing framework for training and awareness—A systematic review", *Hum. Behav. Emerg. Technol.*, vol. 2025, núm. 1, 2025.

[37] M. Al-Hammouri y J. A. Rababah, "The effectiveness of the Good Behavior Game on students' academic engagement in online-based learning: Good Behavior Game effectiveness on students engagement in online learning", *Online Learn.*, vol. 29, núm. 1, 2025.

[38] L. Lisana, H. Dinata, y G. Valencia Tanudjaja, "Playing to learn: Game-based approach to financial literacy for generation Z", *Entertain. Comput.*, vol. 52, núm. 100896, p. 100896, 2025.

[39] R. Roepke, V. Drury, U. Meyer, y U. Schroeder, "Better the phish you know: Evaluating personalization in anti-phishing learning games", en *Proceedings of the 14th International Conference on Computer Supported Education*, 2022.