VISUAL REVIEW | Vol. 17, No. 8, 2025 | ISSN 2695-9631
International Visual Culture Review / Revista Internacional de Cultura Visual
https://doi.org/10.62161/revvisual.v17.5806

FACTORES DE CIBERSEGURIDAD EN JUEGOS DE METAVERSO EN NIÑOS Y ADOLESCENTES

ZULEMA DARIA LEIVA BAZAN[1]
zleiva@uch.edu.pe
JULIO CÉSAR MENDEZ-NINA[1]
jmendez@uch.edu.pe

[1] University Association of Sciences and Humanities, Peru

PALABRAS CLAVE

Juegos en metaverso
Metaverso
Ciberseguridad
Amenazas
Ciber juegos
Niños
Adolescentes

RESUMEN

Este estudio tuvo como objetivo analizar los factores de ciberseguridad en juegos de metaverso entre niños y adolescentes, basándose en 64 artículos de Scopus. Se concluye que los menores constituyen el mayor número de usuarios que incumplen las normas del mundo real. Los niños son los más vulnerables, siendo los niños más propensos a la adicción y las niñas con mayor riesgo. En el entorno de los videojuegos, la educación preventiva es insuficiente, al igual que la capacidad para detectar ciberamenazas, que se consideran delitos menores. Los juegos en línea aumentan la interacción y la información, fomentan la innovación y mejoran el comportamiento. Las amenazas se clasifican como sexuales, fraudulentas y que atentan contra la dignidad. Se recomienda una regulación adecuada y la participación, así como la comprensión, el análisis y el conocimiento de los peligros, y la provisión de recursos.

Recibido: 23/ 03 / 2025
Aceptado: 17/ 06 / 2025

1. Introducción

Atravesamos una de las mayores crisis en la historia de la humanidad; el cambio de paradigma se intensificó a partir de la pandemia de COVID -19, lo que propició el avance de las tecnologías, entre ellas las inmersivas, modificando los servicios y la comunicación. Este nuevo escenario, lejos de verse como algo negativo, debe entenderse a modo de oportunidad de crecimiento (Winterhalter, 2023). Las tecnologías de la información y comunicación (TIC) de avanzada, han logrado efectos transformadores y constantes en diversos ámbitos de la vida: desde consecuencias éticas y económicas, hasta modificaciones culturales, sostenibles y científicas (Padilla, et al, 2023). El acelerado y constante desarrollo ha cambiado la manera de hacer las cosas, e invita a todos los actores a sumar esfuerzos para potenciar las ventajas del ciberespacio (Cano, 2022).

A la par con el progreso tecnológico, emergió el metaverso, entorno que integra disciplinas como el modelado 3D, la animación, la computación en la nube, la cadena de bloques, la inteligencia artificial (IA) y las aplicaciones de Internet de próxima generación, que se compone de la Realidad Extendida (VR), compuesta por la Realidad Aumentada (AR) y la Realidad Mixta (MR), configurándose como espacios donde se integran los mundos físico, humano y digital, generando ambientes interconectados (Dwivedi et al., 2022). Otra clasificación, nos la brindan Lee & Gu (2022), quienes manifiestan que el metaverso integra cuatro categorías: realidad aumentada, registro de vida, así como de los mundos espejo y virtuales. Este último basado por las realidades virtual, mixta y extendida, y es una realidad alternativa similar, pero con características propias al mundo real. Se trata, entonces, de simulaciones que se conectan para obtener una versión mejorada de la conjunción de lo físico y lo digital. En suma, a partir de esta taxonomía, el metaverso se establece a partir del entorno, la interfaz, interacciones y valor social. Su consolidación ha sido impulsada por los nativos digitales y los usuarios de la generación Z, quienes adoptan el rol de prosumidores en este campo (Barrio, 2023; Crespo-Pereira et al., 2023) y se consolidará con los usuarios alfas.

En este nuevo espacio los usuarios realizan diversas actividades y son representados, de manera general, por avatares, en un proceso denominado personalización, en el cual los individuos interactúan de acuerdo con sus expectativas e intereses. La inmersión se realiza a través de meta-niveles aumentados, basadas en códigos y lenguajes. Se prevé que en el futuro ofrecerá nuevos usos y beneficios, augurando un entorno sin límites, que presente amplias perspectivas de aplicación y desarrollo. El metaverso es un sistema ampliado que agrupa redes sociales, juegos y comunidades; espacios en los cuales se realizan interacciones de avanzada se funden con las experiencias de la vida real, ofreciendo oportunidades de construir nuevas y mejores formas de comunicación (Jim et al., 2023; Wang et al., 2022; Bruni et al., 2023).

Por otro lado, las redes sociales pasaron a formar parte de las actividades cotidianas de millones de usuarios. En el 2023 desempeñó su papel en dos tercios de la población mundial, se han afianzado como uno de los espacios de integración y comunicación más relevantes a escala global. Ello se evidencia entre la niñez y adolescencia, quienes disfrutan videos, comparten imágenes y reaccionan de forma positiva, al contenido difundido y, de manera más activa. La comunicación de avanzada representa espacios de interacción, en los cuáles fomentan el aprendizaje, el conocimiento de culturas y de nuevas formas de vida. También se las considera herramientas de entretenimiento, entre las más populares destacan los videojuegos, que proporcionan esparcimiento, aunque pueden atraer potenciales peligros en la salud mental y física de los usuarios (Cabeza-Ramírez et al., 2022; Ramírez-Plascencia, et al, 2022).

Al respecto, la gamificación se define como el uso de elementos, procedimientos, enfoques o actividades; basados en los principios de los juegos y, aplicados en diversos contextos. Se le considera una estrategia novedosa, especialmente en el área del deporte. Estas ventajas Los videojuegos se han convertido en uno de los medios de entretenimiento más influyentes (Navarro et al., 2021; Rodríguez et al., 2022). De acuerdo con Palma-Ruiz et al. (2022), los videojuegos aparecen a inicios de la década de los 70, a partir de la introducción de las máquinas recreativas y las primeras consolas.

El primer torneo de deportes electrónicos se realizó en el año 1972, en la Universidad de Stanford; después, en los años 80, empresas como Sega, Atari o Nintendo masificaron las consolas domésticas, a través de torneos masivos nacionales e internacionales. En la década de los 90, el internet permitió que los jugadores interactúen con otros, en consecuencia, se impulsan las competencias multijugador. A partir de ello, los videojuegos como Battlefield, Quake, la serie Warcraft, EA Sports FIFA, entre otras, alcanzaron gran popularidad. A fines del siglo XX, con el progreso de las nuevas tecnologías y el respaldo

de los desarrolladores profesionales, los videojuegos ampliaron su base de acción, mejorando la organización de los torneos, estructura y premios. Posteriormente, se multiplicó la venta de dispositivos tecnológicos web, en respuesta al incremento del número de jugadores, debido a las capacidades lúdicas de los videojuegos, atrayendo importantes patrocinios a los torneos, entre ellas de las corporaciones Samsung, Microsoft, ATI, AMD, etc.

Los medios tradicionales se involucraron al transmitir la Serie Mundial, después, la consolidación de los procesos transmedia con las plataformas de *streaming* y el vídeo bajo demanda. Hoy en día, los ciber juegos están a la par de las actividades deportivas y de socialización, también la profesionalización del mundo competitivo de los videojuegos. Existe un creciente interés por los ciber juegos, tanto entre los usuarios como en los espectadores. Se evidencia el incremento exponencial en el uso de videojuego, para el año 2021 el número de jugadores se situó en 3.000 millones, es decir, un 5.3% más que en el 2020. En la actualidad, los videojuegos online compiten con los deportes físicos y otros eventos de socialización. Se han posicionado entre los medios inmersivos de mayor incidencia, debido a su fascinante contenido (Cabeza-Ramírez et al., 2022; Ortega-Jiménez et al., 2023).

Los videojuegos son toda clase de programas electrónicos o digitales, que implica la interacción entre varias plataformas. Para su acceso, se utilizan algún tipo de pantalla, además de equipos y dispositivos portables, entre ellas, consolas y plataformas recreativas (Xbox, PlayStation, Game Boy). También a través desde teléfonos móviles, joysticks, salas, aparatos de visualización de video (por ejemplo, auriculares de realidad virtual (VR) y realidad mixta. Estos últimos los de avanzada y relacionados con la IA Se clasifican en ocho géneros: acción, aventura, lucha, rompecabezas, de rol, simulación, deportes y de estrategia; que a menudo se superponen y/o combinan, siendo favoritos los dos primeros. (Asadzadeh et al., 2024; Palma et al., 2022). La integración de las realidades virtual y aumentada con la gamificación, dan lugar a espacios dirigidos a menores de edad; destacando aplicaciones como Sandbox, Roblox, Minecraft, Illuvium, Axie Infinity, Fortnite y otros. Son notables los atractivos de los juegos inmersivos, pero también brindan oportunidad de acción a los cibercriminales anónimos (Chamorro et al., 2023).

En este contexto, Latinoamérica es la región con mayor desventaja digital, donde en los últimos cinco años la cantidad de los ataques cibernéticos aumentaron en 40%, que equivale a más de 700 millones. Las causas de la falta de protección se originan por la limitada conciencia contra las amenazas, el empleo de aplicativos inactuales, las brechas en infraestructura crítica, el bajo nivel en capacitación, la legislación que no penaliza ciberdelitos (Flor-Unda et al., 2023; Kosevich, 2020; Parra & Concha, 2021). Los aspectos positivos son la implementación en la ciberseguridad en las IA, contra las amenazas maliciosas, las mejoras en la identificación y la resolución de riesgos. En ese sentido, los juegos inmersivos ofrecen recursos que garantizan la privacidad y seguridad de la información, aunque todavía deban configurarse (Martínez et al., 2021; Padilla et al., 2023).

Los ambientes futuristas implican desafíos por la preservación de la seguridad; aunque la tecnología 5G es una opción eficaz, también presenta riesgos relacionados con la vulneración de la intimidad de los usuarios. Es por ello por lo que las realidades virtual y aumentada requieren de una red confiable que permita la interacción en tiempo real; también una eficiente generación de identidad a través de la autenticación que responde a la fusión sensorial de señales, recogidas por los dispositivos portátiles y la comprobación de estos datos. Se necesita, además, del trabajo de los desarrolladores y especialistas para difundir con mayor precisión las bondades de estas nuevas tecnologías biométricos (Cervel, 2023; Jim et al., 2023; Al-Sharafi et al., 2023).

Objetivo general

El objetivo principal del presente estudio es analizar los factores de ciberseguridad en los juegos del metaverso en niños y adolescentes.

Objetivos específicos:

- Identificar la situación actual de los ciber juegos inmersivos entre los menores de edad.
- Reconocer las ventajas de los juegos en metaverso entre los niños y adolescentes.
- Identificar las principales amenazas para los menores de edad en este tipo de juegos.
- Evidenciar las soluciones contra los riesgos en los juegos inmersivos.

2. Metodología

En el contexto actual de la importancia de la seguridad cibernética, aparece la necesidad de analizar sus factores en los videojuegos inmersivos. Este estudio se enmarca en un enfoque cualitativo, basado en una revisión sistemática de la literatura (SRL). Se implementó un proceso de cuatro fases (identificación, selección, elección y análisis de la literatura), dado su carácter estructurado y claro, que favorece la reproducibilidad y minimiza el sesgo.

Manterola et al. (2013) indican que la revisión sistemática tiene como objetivo la indagación exhaustiva y detallada de las evidencias existentes sobre un tema específico. Se realiza mediante un protocolo estandarizado, que permite identificar datos confiables y verídicos, con los cuales se evalúa la calidad y la sensibilidad del conocimiento científico. Reduce el sesgo debido a su carácter sistemático, que contribuyen en la estructuración de la información (Samnanni et al., 2017).

Este análisis siguió las pautas PRISMA, que, de acuerdo con Moher et al. (2009), se manifiesta en un diagrama que muestra el proceso de inclusión y exclusión del análisis de estudios previos (Page et al., 2021). La fuente científica utilizada fue Scopus, de donde se seleccionaron 64 publicaciones, priorizando los trabajos de la última década, con el fin de asegurar que se incluyeran los enfoques más recientes (Figura 1).

A. Búsqueda bibliográfica e identificación de estudios

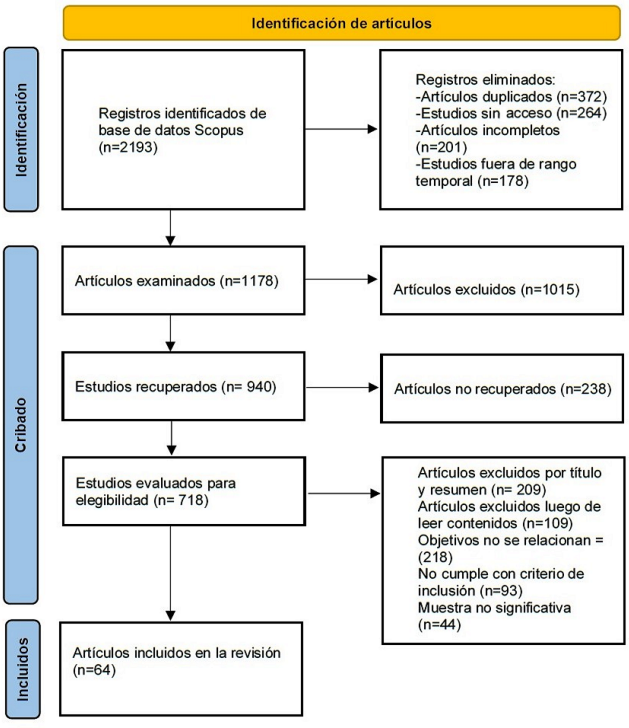
Se seleccionaron y analizaron temáticamente los estudios sobre la ciberseguridad en videojuegos de metaverso entre el 2014 y el 2025. Se excluyeron las investigaciones incompletas, originando diferentes factores y subtemas desde la SLR, considerando la importancia de la información respecto a los factores que repercuten en la seguridad en los videojuegos online. Este artículo sirve como antecedente para académicos y profesionales de la seguridad en el tema, arribando a la comprensión de los artículos de los años 2014 a 2025, para establecer lo investigado y lo que necesita mayor abordaje.

B. Selección de artículos

Inicialmente, se revisaron 2193 artículos, de los cuales se excluyeron aquellos no vinculados con la ciberseguridad. Se culmina el proceso con la selección de 64 fuentes para la revisión sistemática. Se identificaron 2193 estudios, de los cuales 1015 registros se eliminaron; 372 por ser duplicados; 264, sin acceso (no disponibles); 201 incompletos; y 178, muy antiguos. Después, se excluyeron 1015 investigaciones; asimismo, 238 estudios no recuperados; 209, separados por el título y resumen; 109 y 218, por contenido y objetivo no relacionado; 93, que no cumplen con criterio de inclusión; y 44, por muestra no significativa.

C. Elección

Figura 1. Artículos seleccionados

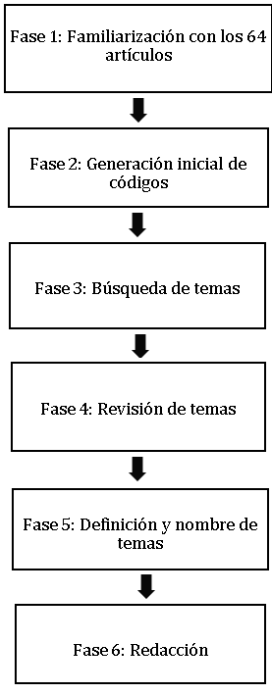


Fuente: Base de datos Scopus, 2014 – 2025.

D. Análisis

Luego se identificaron los factores y subtemas, empleando el modelo de Braun y Clarke (2006), que implica una serie de etapas expresadas en la figura 2. Se analizó la literatura seleccionada con el propósito de reconocer a los agentes de la ciberseguridad en los aplicativos de juegos. Finalmente, se obtuvieron subcategorías. Se suprimieron las subcategorías y códigos duplicados, con el apoyo de expertos en el tema.

Figura 2. Etapas del análisis de información



Fuente: Base de datos Scopus, 2014 -2025.

A continuación, se aprecia el listado de los 64 estudios provenientes de la base de datos de Scopus, detallados de acuerdo con el país, año de publicación y área de enfoque.

Tabla 1. Temas abordados en artículos seleccionados

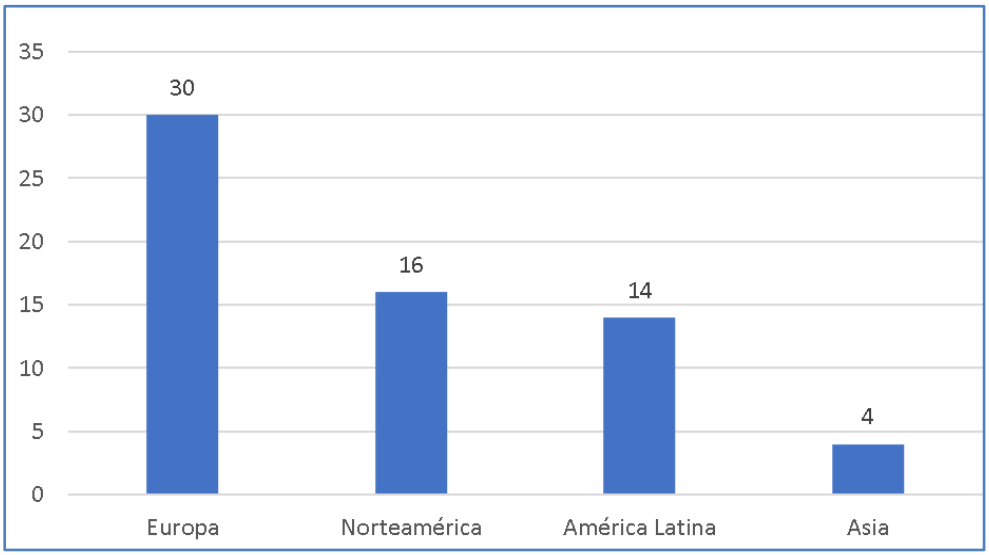
Autores	Tema	Cantidad
Cano (2022), Cervel (2023), Criollo-C et al. (2024), Falchuk et al. (2021), Faraz et al. (2022), Flor-Unda et al (2023), Kang et al. (2023), Kim et al. (2023), Kosevich (20222), Lena-Acebo et al. (2022), Lopez et al. (2020),), Martinez et al. 2024), Padilla (2023), Quayyum et al. (2021), Riega et al. (2023), Rodríguez y Palomo (2023), Sommer et al. (2023), Wang et al. (2022).	Ciberseguridad	18
Asadzadeh et al. (2024), Calli & Ediz (2023), Camacho (2023), Da Silva et al. (2019), Del Moral (2016), Guerra – Antequera (2024), Hou et al. (2023), King (2023), Lluch et al. (2022), López et al. (2022), Martin (2023), Navarro et al. (2021), Palma (2022), Rodrigues et al. (2019), Rodríguez et al. (2022), Ruiz-Bañuls (2021), Valencia (2022).	Gamificación	17
Al-Sharafi et al. (2023), Bruni et al (2023), Chamorro-Atalaya et al. (2023), Crespo-Pereira et al. (2023), Dwivedi et al. (2022), Jim et al. (2024), Kshetri (2022), Lee y Gu (2023), Lee & Kim (2022), Patan y Parizi (2023), Oz (2023), Rangel (2022), Winterhalter (2023).	Metaverso	13
Astorga-Aguilar & Schmidt-Fonseca (2019), Cabeza-Ramírez et al. (2022), Dzomira (2023), França et al. (2022), Gómez-Quintero et al. (2022), López-Belmonte (2020), Martínez et al. (2021), Ortega et al. (2023), Qamar y Afzal (2023), Talapuru et al. (2023), Trejos y Peláez (2023).	Amenazas en videojuegos	11
Barrio (2023), Ester (2018), Klein et al. (2019), Parra & Concha (2020), Ramirez-Plascencia et al. (2022),	Legislación en ciberseguridad	5

Fuente: Artículos seleccionados de base de datos Scopus, 2014 - 2025.

En la tabla 1 se aprecia que el tema más analizado en la selección de artículos es el de "ciberseguridad", con 18 estudios; seguido de la "gamificación", con 17; después destacan las

investigaciones acerca de “metaverso”; mientras que las “amenazas en videojuegos” se abordan en 11; finalmente el tema de “lesgislación en ciberseguridad”, con 5 artículos.

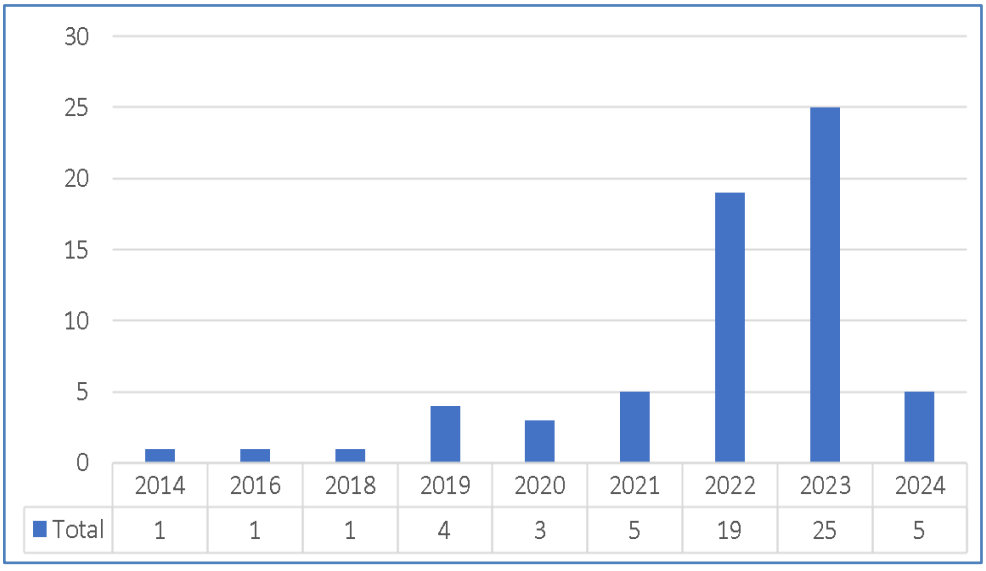
Figura 3. Publicación de artículos por regiones



Fuente: Artículos seleccionados de base de datos Scopus, 2014 - 2025.

La figura 3 muestra que el continente del cual proviene la mayor cantidad de publicaciones sobre ciberseguridad en videojuegos para menores es Europa con 30 artículos; seguido de Norteamérica (Estados Unidos), con 16 publicaciones; en tercer lugar, América Latina con 14 y, finalmente Asia, que cuenta con 4 investigaciones.

Figura 4. Publicación de artículos por años



Fuente: Artículos seleccionados de base de datos Scopus, 2014 - 2025.

Respecto a los años en los cuáles se publicaron estudios respecto a la seguridad en videojuegos online, el 2023 cuenta con más artículos, asciende a 25; seguido del 2022, con 19; después, el 2024 y el 2021, con 5 investigaciones cada uno; finalmente, los años 2024, con 4; 2020, 3; 2018, 2016 y 2014, con 1 artículo respectivamente.

3. Resultados

El propósito principal del presente estudio es analizar los factores de ciberseguridad en juegos del metaverso en menores, a continuación, se detallan los resultados obtenidos, a partir del análisis.

3.1 Situación de la ciberseguridad en los juegos de metaverso entre los menores

En la actualidad, coexisten dos visiones irreconciliables sobre los juegos en el metaverso. Una que los considera una herramienta valiosa y socialmente útil y; otra, que son un vano entretenimiento, además de presentar potenciales riesgos. Respecto a esta última postura, es crucial evaluar la confiabilidad de los aplicativos inmersivos, debido a los desbalances entre la realidad y el entorno virtual; así como, diseñar las mejoras que requieren. Al respecto, las quejas más comunes sobre las aplicaciones lúdicas de avanzada incluyen la escasa confiabilidad, la persistencia de amenazas, la falta de credibilidad y el mayor alcance de los peligros; generando inseguridad y rechazo (Calli & Ediz, 2023; Jim et al., 2023; Winterhalter, 2023).

Los niños y adolescentes representan el mayor número de participantes en los ciber juegos, debido a que prefieren la diversión y las libertades que la virtualidad ofrece, por encima de su bienestar, ignorando, muchas veces, las reglas del mundo real. Por otra parte, los adolescentes son más susceptibles a desarrollar problemas de adicción, sobre todo en juegos de disparos y de rol, donde la interacción con otros jugadores puede intensificarlos, a través de mecanismos como niveles, puntos e insignias, que mantienen la atención de los usuarios, incrementando el tiempo de juego (França et al., 2023; Hou et al., 2022; Ruiz-Bañuls et al., 2021; Wang et al., 2022).

Esta realidad demuestra que, de acuerdo con la edad y género de los usuarios, existen diferencias en la conducta digital. Respecto al primer criterio, la desprotección de la privacidad en los niños es más alta en comparación con los adolescentes, quienes son más conscientes de la información que difunden. Porque comenzar a jugar a edades tempranas incrementa los problemas, entre ellos la adicción y la exposición futura a contenido inadecuado. A medida que la edad avanza, se incrementa la asiduidad a estos entornos lúdicos, por consiguiente, los peligros también. En un gran porcentaje, los infantes usan las plataformas digitales para informar y compartir contenido propio, mientras que los adolescentes se enfocan en alcanzar mayor reconocimiento, con el fin de obtener auto representatividad y facilitar la conexión social (Hou et al., 2022; Lena et al., 2022).

Respecto al género, los hombres interactúan de manera más frecuente, con los videojuegos, debido a las recompensas y satisfacción que obtienen, lo que repercute en la falta de control, síntoma asociado a la tendencia de adicción. Asimismo, los varones suelen involucrarse más intensamente en los programas de tipo multijugador. Por otra parte, son las mujeres quienes se implican más en acciones contra la normatividad, porque presentan un mayor grado de inconsciencia sobre sus actos (Cabeza-Ramírez et al., 2022; Riega-Viru et al., 2023; Ortega-Jiménez et al., 2023).

Las plataformas de juegos más populares destacan Twitch y YouTube Gaming, donde la interacción social es un elemento clave, lo que contribuye a que los usuarios prolonguen su permanencia. En cuanto a los dispositivos preferidos, los smartphones, las PC y el PlayStation, facilitan el acceso a una amplia variedad, incluyendo los encuentros de acción y aventura, que atraen a un gran número de participantes. Los usuarios enfrentan peligros, entre ellas la adicción, el ciberacoso y la exposición a contenido violento o pornográfico; que traen consecuencias negativas, como el descuido de sus responsabilidades, la incapacidad de controlar el tiempo y la aparición de conflictos familiares y sociales (Cabeza-Ramírez et al., 2022; Hou et al., 2022).

En la actualidad, la gobernanza mundial se construye en Internet, escenario en el cual las principales amenazas se originan en las potencias del hemisferio norte, específicamente en desde los Estados Unidos (EE. UU.) y la Unión Europea (UE). El enfoque hacia la ciberseguridad varía en estas dos regiones. Por un lado, en EE. UU. se prioriza la vigilancia y el control global, otorgándole la mayor capacidad en espionaje y ataques en línea. Mientras que en la UE se estructuran las legislaciones de forma supranacional, enfocándose en la prevención, sanción y persecución de los crímenes en internet. Para ello, que requiere una evaluación y adaptación constante de las respuestas. Destacan las jurisdicciones de España y Alemania (Hurel, 2022; Mejía-Lobo et al., 2023; Perafán Del Campo et al., 2021; Seoane, 2022;).

En América Latina, el nivel de seguridad cibernética es inferior en comparación con otras regiones, se evidencia una preparación insuficiente para enfrentar los ciber riesgos, aunque se observa un avance gradual (Kosevich, 2020). Existen esfuerzos, entre los que se encuentra la legislación peruana, en la cual se anticipa y contrarresta la ciberdelincuencia. En Chile, tanto las leyes como la infraestructura crítica digital no ofrecen protección contra las agresiones. Del mismo modo, la normativa en Colombia presenta

serias deficiencias para tipificar estos atentados (López et al., 2021; Mejía-Lobo et al., 2023; Queirolo et al., 2021).

En cuanto a la comprensión de las amenazas en juegos inmersivos, la mayoría de los usuarios poseen habilidades técnicas, pero no la madurez para reflexionar sobre los riesgos. La cultura de prevención se adquiere en edades tempranas, ello demuestra por qué muchos menores configuran de manera incorrecta sus perfiles o comparten información (França et al., 2023; Lena et al., 2022; Quayyum et al., 2021). Otras preocupaciones es que las empresas carecen de recursos destinados a la seguridad; la ausencia de prevención en el personal y la falta de herramientas para detectar peligros (Dzomira, 2014).

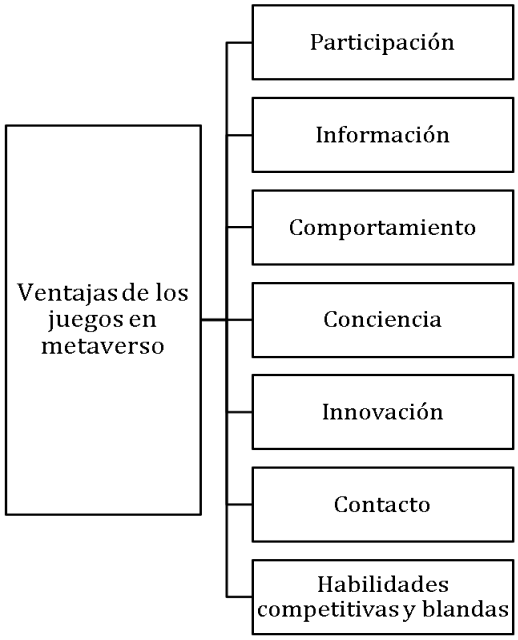
La adicción a los videojuegos puede vincularse a la falta de atención y con una relación distante de padres e hijos. Entre otras causas destacan la falta de conciencia de los menores sobre los peligros, así como de una baja percepción de riesgo, incrementa la vulnerabilidad durante situaciones de acoso y otros riesgos en línea Ello representa un reto en términos legales, ya que las regulaciones del uso de la IA varían de acuerdo con la región, generando inconsistencias en la aplicación de medidas de protección (Hou et al., 2022; Ramírez-Plascencia et al., 2022).

La convergencia de la inteligencia artificial con la delincuencia ha modificado la forma de los ataques, explotando debilidades sin ser identificados. Existen usuarios quienes en la vida real se conducen de manera correcta; sin embargo, en el entorno virtual hacen lo contrario, debido a la falta de una regulación estricta. Por otro lado, las víctimas de ciberacoso no poseen un perfil único, incluyen personas intimidadas de forma presencial. También, usuarios populares, vulnerables al encontrarse en contextos sociales frágiles. Asimismo, las dinámicas de los roles son complejas, donde las víctimas pueden convertirse en agresores y viceversa. El impacto de los espectadores es relevante, algunos permanecen indiferentes, otros defienden a la víctima, incluso respaldan al agresor, legitimando su comportamiento y estatus. Por estas razones, se considera un desafío para la prevención y regulación (Flor-Unda et al., 2023; Martín, 2022).

3.2 Ventajas de los juegos de metaverso

La consolidación del metaverso en las diferentes plataformas digitales implica una serie de cambios y desafíos. No obstante, también genera diversos beneficios, de manera especial en el ámbito de los juegos, como se detalla a continuación.

Figura 5. Ventajas de los juegos en metaverso



Fuente: Artículos seleccionados de base de datos Scopus, 2014 – 2025.

A. Participación

La gamificación, a través de los avatares y otros elementos, promueve el intercambio e interacción positiva entre usuarios; además, gracias a la inmersión los jugadores pueden socializar y participar en actividades lúdicas. En ese contexto, las aplicaciones en redes sociales se afianzan como espacios de interacción e integración, facilitando la conexión entre usuarios y actuando como agentes de cohesión en las comunidades digitales (Bruni et al., 2023; Kim et al., 2023; Ramírez-Plascencia et al., 2022).

Asimismo, los videojuegos se destacan como entornos de socialización, gracias a la organización de eventos populares, que fomentan las relaciones, a través de las redes de amistad y contactos. No obstante, esta dinámica requiere de los usuarios una inversión significativa de tiempo (Palma et al., 2022; Ruiz-Bañuls et al., 2021).

B. Información

Los juegos en el metaverso se consideran instrumentos de divulgación de información, porque facilitan la transferencia de conocimientos, captando el interés mediante su contenido novedoso, entre ellas las experiencias en 3D (Valencia, 2022). Esta transmisión de datos fortalece los conocimientos y la capacidad de comunicarse, e incentiva la cooperación (Silva et al., 2019). Es así como el metaverso, en los últimos diez años, se ha constituido como un agente de comunicación global cada vez más relevante y uno de los efectos de la masificación de las redes sociales es que los niños y adolescentes se han convertido en consumidores de información más activos. Además, esta información puede integrarse al contenido curricular, promoviendo el aprendizaje cooperativo y el descubrimiento de otras culturas y modos de vida (Asadzadeh et al, 2024).

C. Comportamiento

La gamificación en el metaverso traslada elementos de la virtualidad al mundo real, influyendo en el comportamiento, de manera especial de los niños, al remplazar conductas indeseadas como la negligencia o despreocupación ante las potenciales amenazas, por una mayor conciencia y preocupación hacia estos riesgos. Los juegos en metaverso orientan la mejora de la conducta de los estudiantes porque las actitudes son relevantes para comprender y prever el comportamiento social (Crespo et al., 2023; Quayyum et al., 2021).

Una actitud es un patrón de comportamiento que obedece a una respuesta condicionada a estímulos a partir de experiencias sociales. En el caso de los menores a través de los contenidos de los juegos en metaverso. Además, estos juegos fomentan actitudes y comportamientos colaborativos mediante el desarrollo de dinámicas enfocadas a modificar determinadas conductas negativas (Da Silva, et al, 2019; López-Belmonte et al., 2020; Ruiz-Bañuls et al., 2021).

D. Conciencia

La motivación a partir de las experiencias inmersivas incrementa la conciencia sobre ciberseguridad, contribuyendo a la sensibilización de los peligros existentes y, lograr cambios en el comportamiento de los menores. Es un beneficio destacado de los aplicativos de entretenimiento. Su éxito radica en la diversión asociada a los juegos, ya que la gamificación aumenta el esfuerzo de los menores (Kim et al., 2023; Oz, 2023; Ramírez-Plascencia et al., 2022). Fomentan a la ejecución de tareas, en busca de reconocimiento con el que reflexionen y se interesen por aprender. Introducir el videojuego temprano impulsa alcanzar los objetivos, logrando capturar la atención, creando un entorno propicio para el desarrollo de habilidades y competencias (Asadzadeh et al., 2024; Guerra-Antequera et al., 2022).

E. Innovación

Las aplicaciones de gamificación basadas en inteligencia artificial desarrollan habilidades para el diseño y la mímesis, al estimular la innovación y la creatividad, cuando los jugadores buscan alternativas para navegar en estos entornos relaciona conocimientos y habilidades para brindar soluciones. La creatividad se desarrolla de manera lúdica, especialmente durante la niñez y la adolescencia, etapas en las que el entretenimiento ocupa un lugar central. Ver videos, compartir imágenes y reaccionar al contenido, se han convertido en una de las principales formas de esparcimiento (Del Moral & Guzmán, 2016; Lluch-Molins et al., 2022; Valencia, 2022; Oz, 2023).

F. Contacto

El metaverso, a través de sus avatares personalizados, ofrece una serie de ventajas para el contacto con otros usuarios, brinda cercanía con los seres queridos, así como la conservación de recuerdos, incluso después de fallecer. Además, se pueden desarrollar actividades laborales a distancia y, se reduce el contacto personal para la protección de la salud.

G. Habilidades competitivas

Los videojuegos se han caracterizado por incentivar el espíritu competitivo. Su propia elección supone la auto imposición de retos La confrontación en línea permite a los jugadores medir y comparar sus habilidades, lo cual es característico en los deportes electrónicos (Guerra-Antequera et al., 2022; Palma et al., 2022; Ruiz-Bañuls et al., 2021). Estos retos desarrollan el aprendizaje colaborativo, porque la tecnología de avanzada relaciona los conocimientos y habilidades, con el fin de brindar soluciones. Es

indispensable, también, adoptar retos de mayor atractivo, que permitan equivocarse, mientras se realiza seguimiento y, actualizar las estrategias de recompensa (Lluch-Molins et al., 2022; López-Belmonte et al., 2020).

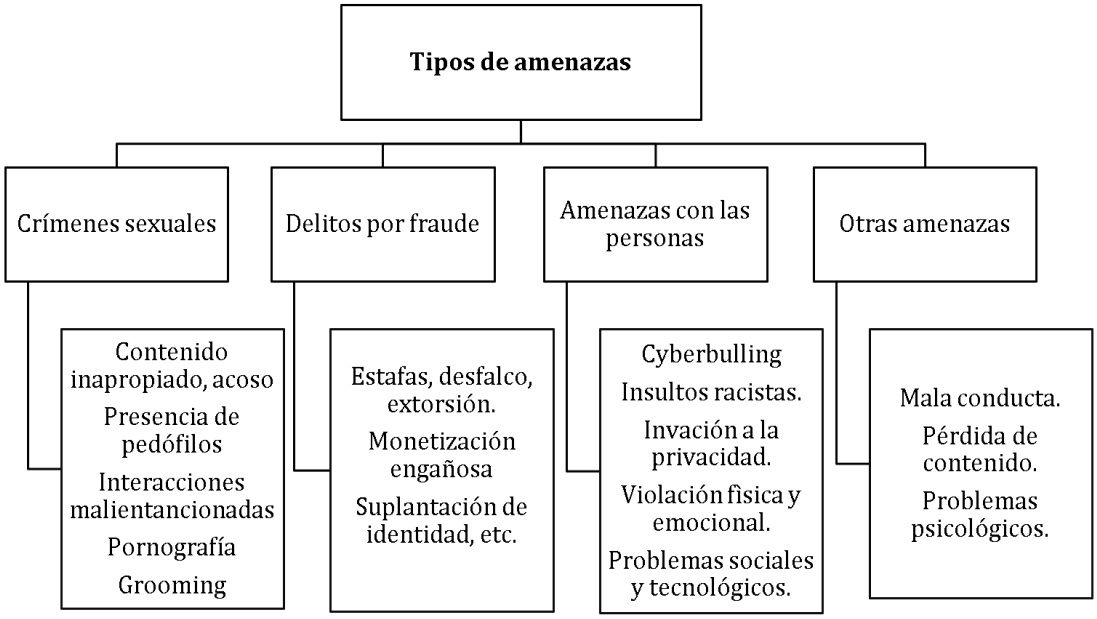
H. Habilidades blandas

Los videojuegos fomentan competencias blandas esenciales para el desempeño exitoso en la vida y el trabajo. Entre ellas destacan el compromiso, el trabajo en equipo, la toma de decisiones individuales y colectivas, el aprendizaje cooperativo y, la resolución de problemas (Palma et al., 2022; Ruiz-Bañuls et al., 2021). Asimismo, los videojuegos promueven el desarrollo de capacidades motoras finas, porque el éxito en los deportes electrónicos requiere óptima coordinación. Compitiendo con los deportes físicos, fomentando hábitos saludables y fortalecen habilidades mentales. Por otro lado, el avance de las plataformas de *streaming* permite a los jugadores mejorar su práctica, porque apreciar a otros, enriquece la experiencia, ayudando a perfeccionar destrezas (Asadzadeh et al.,2024; Cabeza-Ramírez et al., 2022; Guerra-Antequera et al., 2022).

3.3 Tipos de amenazas

La convergencia de las tecnologías de avanzada en áreas como la social, político, económico, militar y de entretenimiento, las han hecho vulnerables a los ataques cibernéticos (Flor-Unda et al., 2023; Kosevich, 2020). En consecuencia, los peligros asociados a los juegos en línea del metaverso se clasifican de la siguiente manera: crímenes sexuales, delitos por fraude, amenazas contra la persona y otras (Qamar & Afzal, 2023).

Figura 6. Tipos de amenazas en juegos en metaverso



Fuente: Artículos seleccionados de base de datos Scopus, 2014 - 2025.

A. Crímenes sexuales

Entre estos delitos, prevalecen el contenido inapropiado para menores, la presencia de pedófilos, las interacciones malintencionadas entre niños y adultos, la pornografía, el acoso sexual y las citas en línea. En el juego 'Roblox', destacan el grooming de menores, la difusión de material sexual, las amenazas de violación, entre otros (Calli & Ediz, 2023; França et al., 2023).

B. Delitos por fraude

En cuanto a los fraudes, los más frecuentes son el robo de identidad, las estafas con bitcoins, el desfalco financiero, la monetización engañosa en *freemium*, las farsas en los juegos de azar, la suplantación de identidad, los espacios económicos no regulados, la extorsión, entre otros (King, 2023; Qamar & Afzal, 2023).

C. Amenazas contra la persona

Respecto a las amenazas contra la persona, los usuarios están expuestos al ciberbullying, insultos racistas, invasión de la privacidad, captación y radicalización de ideas y, desde luego, a la violencia verbal y/o física. Asimismo, se presentan problemas sociales y tecnológicos como la desigualdad digital, la

exclusión, exposición a virus informáticos, detección de la ubicación física, la adicción, la dependencia tecnológica, el aislamiento, etc. (França et al., 2023; Quayyum et al, 2021).

D. Otras amenazas

También se consideran como amenazas frecuentes a la manipulación emocional y la obligación narrativa. Asimismo, la mala conducta social, la pérdida de contenido propio y, otros problemas psicológicos dentro del metaverso. Existe un incremento de los delitos en torno a los juegos inmersivos, en especial los de naturaleza sexual y los fraudes, los que vulneran la dignidad y derechos de las personas (Calli & Ediz, 2023; Ester, 2023; King, 2023). El peligro más frecuente para los menores de edad es el ciberbullying, el cual se inicia como un juego. La actitud de poder y el anonimato que brinda el mundo online, potencia la criminalidad.

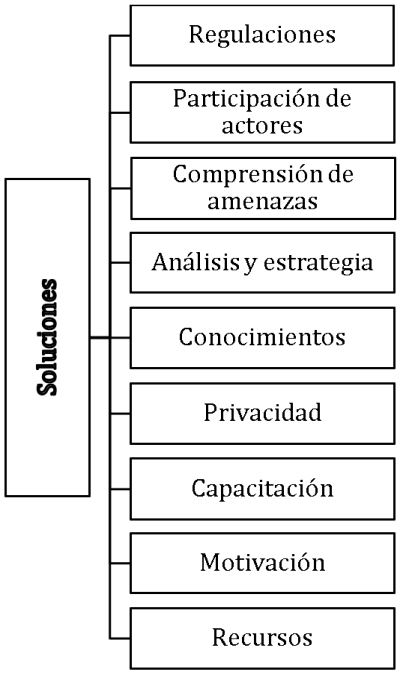
Estos actos delictivos muestran mayores riesgos y se abordan con mayor complejidad. Ante este panorama, los desarrolladores se enfrentan a una excesiva cantidad de solicitudes en tiempo real (Talapuru et al, 2023; Trejos & Peláez, 2023). El exceso de permanencia en los juegos en línea ocasiona dificultades en la adaptación social, que derivan en problemas de conducta, como la agresividad o realizar comentarios hirientes. Actitudes que perturban el ambiente digital, incluso llegando a la agresión física. Asimismo, el exceso de interacción con los videojuegos genera mayor probabilidad de problemas de salud mental, como la depresión y la ansiedad social.

Otras amenazas son las de tipo fisiológicas, entre ellas, la peor calidad de vida y sueño y, los trastornos somáticos (Cabeza-Ramírez et al., 2022; Hou et al., 2022). Asimismo, se presentan dificultades académicas, entre ellos el menor rendimiento escolar, el descuido de tareas importantes, etc. En cuanto a los riesgos tecnológicos, destacan la adicción a los juegos, la pornografía móvil, la agresión cibernética, la violencia web, el acoso, la victimización, la difusión de contenido inapropiado, la brecha generacional socio tecnológica, que se amplía rápidamente (Palma et al., 2022; Ramírez-Plascencia, et al., 2022).

3.4. Soluciones contra las amenazas en metaverso

La ciberseguridad en el metaverso debe priorizar un enfoque integral, que contemple regulaciones, colaboración entre actores, y educación continua. Por ello, se plantean las siguientes soluciones desde diversos puntos clave:

Figure 7. Soluciones contra las amenazas en metaverso



Fuente: Artículos seleccionados de base de datos Scopus, 2014 - 2025.

A. Regulaciones

Los avances tecnológicos exigen la adaptabilidad de los sistemas normativos, respecto a los riesgos. Deben ser reglados de manera jurídica, a través de normas estandarizadas, certificadas y aplicadas de manera transparente, sobre todo en el servicio de las empresas privadas. Asimismo, se requiere la

supervisión y monitoreo por parte de organismos reguladores, para garantizar la confiabilidad y seguridad en el metaverso; en línea con los desafíos de la economía 4.0, las necesidades de las empresas y las expectativas de la sociedad (Bruni et al., 2023; França et al., 2023; Ilárraz & Palomo, 2023; Klein et al., 2022; Parra & Concha, 2021; Sommer et al., 2023; Wang et al., 2022).

En la legislación europea, la ciberseguridad se aborda con la no intervención y se prioriza la soberanía en el ciberespacio. En Latinoamérica, resulta imprescindible que los ciberdelitos sean juzgados con un enfoque especializado. Lo anterior requiere la implementación de un marco jurídico, que permita el desarrollo de la prevención, persecución y sanción de estas infracciones (Hortal, 2023; Trejos & Peláez, 2023).

La aplicación de las sanciones debe considerar la edad de los infractores, fomentando la disposición a no reincidir y, el aprendizaje sobre la falta cometida, evitando penas extremas y optando por mecanismos de mediación. Los gobiernos deben políticas de restricción de edad, que protejan a los niños (Hou et al., 2022; Martín, 2022;). Asimismo, se exige un enfoque jurídico internacional unificado, que faculten a los organismos competentes a ejercer su función (Payá-Santos & Luque Juárez, 2021).

B. Participación de actores

La ciberseguridad no es solo responsabilidad del gobierno y las empresas tecnológicas; se requiere participación de organismos públicos y privados, de las familias, la comunidad, los medios de comunicación e instituciones académicas. La colaboración entre los actores es fundamental para establecer estándares y protocolos. A partir de ellos, se obtiene confianza en el metaverso (Crespo et al., 2023; Falchuk et al., 2018; Jim et al., 2023).

En consecuencia, involucrar a los agentes es imperioso, urge la colaboración entre las organizaciones de ingeniería, de seguridad y protección profesional. A partir del cual se involucren la tecnología, personas y cambios, en los procesos. Convocar analistas mejor capacitados y dotarlos de herramientas tecnológicas de vanguardia, para enfrentar el elevado número de ciberamenazas que no solo afecta la seguridad, sino también los derechos de los ciudadanos (Payá-Santos & Luque Juárez, 2021).

Respecto a los agentes cercanos, como padres, familiares y amigos, su apoyo se constituye útil para prevenir posibles trastornos del uso de videojuegos. En especial, se recomienda que los padres se involucren activamente en el uso que sus hijos hacen de la web, fomentando buenas relaciones y comprendiendo sus comportamientos en los juegos, para mediar de manera efectiva (Cabeza-Ramírez et al., 2022; Dzomira, 2014; Martínez et al., 2024).

C. Comprensión de las amenazas

Es indispensable comprender la naturaleza delictiva de los peligros en los juegos online y tomar acciones que los contrarresten; estableciendo límites y responsabilidades con el propósito de prevenirlos. Los adolescentes entienden como percepción del riesgo, al reconocer y reaccionar ante situaciones conflictivas, derivadas de la interacción en internet. Es necesario que los menores comprendan los peligros a los que se encuentran expuestos (Gómez et al., 2024; Martín, 2022).

Resulta fundamental fortalecer las políticas informativas para comprender de forma eficiente las comunicaciones aumentadas, reconociendo sus riesgos. Asimismo, crear mecanismos de denuncia y seguimiento para gestionar apropiadamente los peligros. La convivencia en el ciberespacio debe enfocarse en participación ciudadana, para reducir la desinformación, la manipulación y otras amenazas (Cano, 2022; Falchuk et al., 2018).

D. Análisis y estrategia

Como en todo proceso estratégico, la seguridad en los juegos del metaverso requiere de una auditoría rigurosa (Wang et al., 2022). A partir de esta exploración, se diseña una arquitectura de protección, que se ajuste a los principales desafíos y a las características de cada aplicación. Basadas en el intercambio seguro de datos, la autenticación, la proximidad, el cifrado y el uso de *blockchain* (Kang et al., 2024; Patan & Parizi, 2023).

En los últimos años, el uso de la IA ha cobrado una relevancia creciente en seguridad, debido a su capacidad de contrarrestar potenciales amenazas, identificando y mitigando los riesgos. Por su rapidez, esta tecnología acelera la exploración de grandes volúmenes de datos, en busca de cualquier posible amenaza, además de identificar imperfecciones en los sistemas. Con ello se automatizan los mecanismos de defensa reduciendo la intervención humana; sin embargo, debe abordarse por diversos agentes que interactúen de manera coordinada (Padilla et al., 2023; Rafael, 2023).

E. Conocimientos

El nivel de conocimiento respecto al ciberacoso en línea se relaciona con el grado de prevención. Por ello, es necesario buscar, contrastar o reconocer información falsa, sobre un estado crítico, para anticiparse (Riega-Viru et al., 2023). La protección y seguridad en línea dependen de la consciencia de los riesgos por parte de los usuarios, en especial al compartir información, configurar privacidad o eliminar contenido. Es esencial una adquisición de conocimientos preventivos de forma temprana y continua. Además, el papel de los padres es crucial para un desarrollo seguro en el entorno digital (Astorga & Schmidt, 2019; Lena et al., 2022).

G. Privacidad

Ante los peligros latentes, la mejor forma de prevención es anticiparse a cualquier situación de vulnerabilidad. Las acciones orientadas deben ser capaces de iniciar, controlar, monitorear, persistir y determinar su efectividad; mientras se codifican al juego y, son compatibles con los avatares. En ese sentido, la privacidad en estos espacios digitales de ser gestionada por especialistas que garanticen el correcto funcionamiento de las plataformas (Falchuk et al., 2018; Gómez et al., 2024).

H. Capacitación

La capacitación es el enfoque más utilizado para la protección, se recomienda realizarlas a través de contenidos adaptados al público juvenil, como cómics, animaciones, historietas y experiencias en redes sociales. Así, es vital promover entre los menores una educación crítica digital, desde edades tempranas. A partir de la formación, los menores desarrollen habilidades de protección y juicio frente a peligros, como la suplantación de identidad y el ciberacoso. Este último es el riesgo de mayor frecuencia en los últimos años (Martín, 2022; Quayyum et al., 2021).

Otra sugerencia valiosa es el uso de la gamificación en los contenidos de seguridad. No obstante, esta información significa un reto para los padres, quienes deben adaptarse a las innovaciones en comunicación digital, para encaminar a los menores (Criollo et al., 2024; Martínez, 2021). Si las organizaciones deciden apostar por el metaverso, deben gestionar, entre otros, la formación de recursos humanos. Este proceso se complementa con apoyo externo especializado. Entre ellos, la adopción de una propuesta de valor, el establecimiento de objetivos viables y la evaluación de los riesgos tecnológicos (Bruni et al., 2023).

I. Motivación

La motivación es un aspecto clave para incrementar el conocimiento sobre las ciber amenazas entre los menores. El metaverso ofrece experiencias realistas, porque desarrolla la conciencia; modificando la actitud preventiva frente a los peligros. Por tanto, es necesario diseñar y gestionar soluciones eficientes, para los espacios inmersivos. Ello incentiva la participación de los menores, lo que lo convierte en una estrategia efectiva, disminuyendo las amenazas, como el ciberacoso y la victimización (Hou et al., 2022; Quayyum et al., 2021).

J. Recursos

Actualmente, la inversión destinada a la seguridad en el metaverso es considerable, por ello, es importante que las empresas, los negocios y los usuarios finales, gestionen estos recursos, con el fin de lograr un entorno inmersivo confiable y sostenible; reconociendo el valor social de la tecnología ética y, la preocupación por el medio ambiente digital. Con ello se garantiza la ciberseguridad óptima que permita a todos el disfrute seguro en este entorno (Bruni et al., 2023; Crespo et al., 2023; França et al., 2023).

4. Conclusiones

El objetivo principal del presente estudio fue analizar los factores de ciberseguridad en los juegos del metaverso, en niños y adolescentes. Respecto a la situación de riesgo en estos aplicativos, los menores constituyen el mayor número de participantes, quienes contravienen las reglas del mundo real. El metaverso es una herramienta valiosa, pero presenta amenazas. Se incrementaron los delitos, la desprotección es más alta en los niños. En la adolescencia se intensifican los peligros, porque se busca reconocimiento. Los varones son propensos a la adicción, las mujeres se implican más en acciones de riesgo. Los participantes poseen habilidades técnicas, pero carecen de formación preventiva y reflexiva. Las plataformas más populares son Twitch y YouTube Gaming; se prefiere los smartphones, las PC y el PlayStation.

En América Latina, la ciberseguridad es inferior a otras regiones. Existe falta de recursos y herramientas de detección. Los ciberdelitos son considerados como faltas administrativas. Las

regulaciones de la IA varían de acuerdo con la región. El anonimato da ventajas a los delincuentes. La adicción se relaciona con los problemas de atención y mala relación con los padres. Las víctimas pueden convertirse en agresores. Las amenazas en metaverso para menores están tipificadas en: crímenes sexuales, como el contenido inapropiado, la presencia de pedófilos, la pornografía, etc. En Roblox prolifera el grooming y los delitos por fraude; amenazas contra la persona, entre ellas el ciberbullying, que es el peligro más concurrente; las denominadas otras amenazas, invasión de la privacidad y, la manipulación emocional.

Entre las ventajas de los juegos en metaverso: fomentan la participación al ser de naturaleza interactiva, se constituye un excelente canal de divulgativo, por el interés que despierta el contenido inmersivo; a partir de ello, se generan conductas más responsables frente a las amenazas. Se motiva fomentando la innovación y creatividad, facilita el contacto interactivo, ganando tiempo y protegiendo la salud. Incentivar un espíritu competitivo, comparando sus habilidades, soluciones a los problemas, las recompensas. Fomentan habilidades blandas, el desarrollo motor fino, habilidades mentales y mejoras en su práctica. Las soluciones consideradas que se proponen: la supervisión de los reguladores, los ciberdelitos deben ser juzgados con normas estandarizadas.

Los agentes deben ser actores activos. La capacitación necesaria para generar conciencia y prevención, así como el monitoreo de peligros, diseño de protección, según cada aplicativo. Se requiere una inversión significativa para un entorno confiable, sostenible y ético; políticas informativas y canales de denuncia eficiente.

La muestra de 64 reveló que la selección, no puede ser generalizable. Se podría crear un sesgo, por lo que se recomienda realizar estudios acerca de los factores abordados. Asimismo, sobre la ciberseguridad en los diferentes medios de entretenimiento online. Finalmente, se sugiere realizar comparaciones de las variables, por regiones o continentes. Incluir investigaciones que analicen la percepción de la protección digital, entre usuarios que de otras generaciones.

Referencias

Al-Sharafi, M.A., Al-Emran, M., Al-Qaysi, N., Iranmanesh, M., & Ibrahim, N. (2023). Drivers and Barriers Affecting Metaverse Adoption: A Systematic Review, Theoretical Framework, and Avenues for Future Research. *International Journal of Human–Computer Interaction*, 1–22. https://doi.org/10.1080/10447318.2023.2260984

Asadzadeh, A., Shahrokhi, H., Shalchi, B., Khamnian, Z., & Rezaei-Hachesu, P. (2024). Serious educational games for children: A comprehensive framework. *Heliyon,* 10(6), e28108. https://doi.org/10.1016/j.heliyon.2024.e28108

Astorga-Aguilar C., & Schmidt-Fonseca, I. (2019). Peligros de las redes sociales: Cómo educar a nuestros hijos e hijas en ciberseguridad. *Revista Electrónica Educare, 23(*3), 339-362. https://dx.doi.org/10.15359/ree.23-3.17

Barrio, M. (2023). El Metaverso y su impacto en el Estado y la soberanía. *Revista de Derecho Político*, (117), 197–220. https://doi.org/10.5944/rdp.117.2023.37925

Braun, V., y Clarke, V. (2006). Uso del análisis temático en psicología. *Investigación cualitativa en psicología*, 3 (1), 12-23.

Bruni, R., Piccarozzi, M., & Caboni, F. (2023). Defining Metaverse with challenges and opportunities in the business environment. *Journal of Marketing Theory and Practice*, 33 (1), 1–18. https://doi.org/10.1080/10696679.2023.2273555

Cabeza-Ramírez, L.J., Rey-Carmona, F.J., del Carmen Cano-Vicente, M. (2022). Analysis of the coexistence of gaming and viewing activities in Twitch users and their relationship with pathological gaming: a multilayer perceptron approach. *Sci Rep 12*, 7904 https://doi.org/10.1038/s41598-022-11985-0

Calli, B., & Ediz. C. (2023). Top concerns of user experiences in Metaverse games: A text-mining based approach*. Entertainment Computing, 46*, 1-17. https://doi.org/10.1016/j.entcom.2023.100576

Camacho-Sánchez, R., Serna, J., Rillo-Albert, A., & Lavega-Burgués, P. (2023). Enhancing motivation and academic performance through gamified digital game-based learning methodology using the ARCS model. *Interactive Learning Environments*, 1–18. https://doi.org/10.1080/10494820.2023.2294762

Cano, J. (2022). Prospectiva de ciberseguridad nacional para Colombia a 2030. *Revista Científica General José María Córdova*, 20(40), 815-832. https://dx.doi.org/10.21830/19006586.866

Chamorro-Atalaya, O., Durán-Herrera, V., Suarez-Bazalar, R., Nieves-Barreto, C., Tarazona-Padilla, J., Rojas-Carbajal, M., Cruz-Telada, Y., Caller-Luna, J., Alarcón-Anco, R., & Arévalo-Tuesta, J. (2023). Inclusion of Metaverses in the Development of the Flipped Classroom in the University environment: Bibliometric Analysis of Indexed Scientific Production in SCOPUS. *International Journal of Learning, Teaching and Educational Research, 22*(10). https://doi.org/10.26803/ijlter.22.10.14

Crespo-Pereira, V., Sánchez-Amboage, E., & Membiela-Pollán, M. (2023). Facing the challenges of metaverse: a systematic literature review from social sciences and marketing and communication. *Profesional de la Información*, *32*(1), 1-21. https://doi.org/10.3145/epi.2023.ene.02

Criollo-C., S., Guerrero-Arias, A., Buenaño, D., & Luján-Mora, S. (2024). Usability and Workload Evaluation of a Cybersecurity Educational Game Application: A Case Study. *IEEE Access, 12,* 12771-12784. https://doi.org/10.1109/ACCESS.2024.3352589

Da Silva, J. (2023). Protection, expertise and domination: Cyber masculinity in practice. Computers & Security, 133, 103408. https://doi.org/10.1016/j.cose.2023.103408

Del Moral, E., & Guzmán, A. (2016). Jugar en red social: ¿Adicción digital versus comunicación e interacción en CityVille? *Cuadernos.info*, (38), 217-231. http://dx.doi.org/10.7764/cdi.38.810

Dwivedi, Y., Hughes, L., Baabdullah, A., Ribeiro, S., Giannakis, M., Al-Debei, M., Dennehy, D., Metri, B., Buhalis, D., Cheung, C., Conboy, K., Doyle, R., Dubey, R., Dutot, V., Felix, R., Goyal, D., Gustafsson, A., Hinsch, C., Jebabli, I., . . . Wamba, S. (2022). Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*, 66, 1–55. https://doi.org/10.1016/j.ijinfomgt.2022.102542

Dzomira, S. (2014). Electronic fraud (cyber fraud) risk in the banking industry Zimbabwe. *Risk governance & control financial markets & institutions, 4*(2), 17-27. https://doi.org/10.22495/rgcv4i2art2

Ester, A. (2023). El desafío de la Inteligencia Artificial a la vigencia de los derechos fundamentales. *Cuadernos Electrónicos de Filosofía del Derecho, 48*, 111-139. http://dx.doi.org/10.7203/CEFD.48.25863

Falchuk, B., Loeb, S., & Neff, R. (2018). The Social Metaverse: Battle for Privacy. *IEEE Technology and Society Magazine*, 37, (2), 52-61. https://doi.org/10.1109/MTS.2018.2826060

Faraz, A., Montsef, J., Raza, A., & Willis, S. (2022). Child Safety and Protection in the Online Gaming Ecosystem. *IEEE Access, 10*, 115895-115913. https://doi.org/10.1109/ACCESS.2022.3218415

Flor-Unda, O., Simbaña, F., Larriva-Novo, X., Acuña, Á., Tipán, R. y Acosta-Vargas, P. (2023). Comprehensive Analysis of the Worst Cybersecurity Vulnerabilities in Latin America. *Informatics, 10*(3). https://doi.org/10.3390/informatics10030071

França, F., Leitão, B., Santos, J., & Oliveira, M. (2023). O abuso sexual contra crianças e adolescentes no ambientes virtual: o caso do abuso de avatar e os riscos na expansão do metaverso. *Relacoes Internacionais no Mundo Atual, 4*(42), 102–129. https://revista.unicuritiba.edu.br/index.php/RIMA/article/view/e-5953/371374555

Gómez-Quintero, J., Johnson, S., Borrion, H., & Lundrigan, S. (2024). A scoping study of crime facilitated by the metaverse. *Futuros, 157*, 1-22. https://doi.org/10.1016/j.futures.2024.103338

Guerra-Antequera, J., Antequera-Barroso, J. A., & Revuelta-Domínguez, F. I. (2022). Degree of motivation and acquisition of visuospatial perception after the incorporation of a video game in the learning of mathematical knowledge. *Heliyon,* 8(8), e10316. https://doi.org/10.1016/j.heliyon.2022.e10316

Cervel, M. (2023). Ciberinjerencias en los procesos electorales y el principio de no intervención (una perspectiva internacional y europea). *Revista Electrónica de Estudios Internacionales*, (45). https://dialnet.unirioja.es/servlet/articulo?codigo=9033002

Hou, C. Y., Rutherford, R., Chang, H., Chang, F. C., Shumei, L., Chiu, C. H., Chen, P. H., Chiang, J. T., Miao, N. F., Chuang, H. Y., & Tseng, C. C. (2022). Children's mobile-gaming preferences, online risks, and mental health. *PloS one,* 17(12), e0278290. https://doi.org/10.1371/journal.pone.0278290

Hurel, LM (2022). Interrogando la agenda de desarrollo de la ciberseguridad: Una reflexión crítica. *The International Spectator*, 57 (3), 66–84. https://doi.org/10.1080/03932729.2022.2095824

Ilárraz, C. R., & Zurdo, R. J. P. (2023). Transparencia, ciberseguridad e identidad digital en el entorno 5G. *Revista española de la transparencia,* (18), 359-380. DOI: https://doi.org/10.51915/ret.298

Jim, J., Hosain, M., Mridha, M., Kabir, M., & Shin, J. (2023). Toward Trustworthy Metaverse: Advancements and Challenges. *IEEE Access, 11*, 118318–118347. https://doi.org//10.1109/ACCESS.2023.3326258.

Kang, G., Koo, J., & Kim, Y. G. (2024). Requisitos de seguridad y privacidad para el metaverso: una perspectiva de las aplicaciones del metaverso. *Revista IEEE Communications, 62* (1), 148-154. https://doi.org/10.1109/MCOM.014.2200620

Kim, J.B., Zhong, C., & Liu, H. (2023). Teaching Tip: What You Need to Know about Gamification Process of Cybersecurity Hands-on Lab Exercises: Lessons and Challenges. *Journal of Information Systems Education, 34*(4), 387-405. https://jise.org/Volume34/n4/JISE2023v34n4pp387-405.html

King, J., Fitton, D., & Cassidy, B. (2023). Investigating Players Perceptions of Deceptive Design Practices within a 3D Gameplay Context. *Proceedings of the ACM on Human-Computer Interaction, 7*(407), 876–892. https://doi.org/10.1145/3611053

Klein, V., Domingues, J., & Tajra, G. (2023). Antitruste no metaverso: economia comportamental e o bem-estar do consumidor. *Revista de Defesa da Concorrência, 11*(2). https://doi.org/10.52896/rdc.v11i2.1052.

Kosevich, E. (2020). Cyber Security Strategies of Latin America Countries. *Iberoamericana*, (1) 137-159. https://doi.org/10.37656/s20768400-2020-1-07

Kshetri, N., (2022). Metaverse technologies in product management, branding and communications: virtual and augmented reality, artificial intelligence, non-fungible tokens and brain-computer interface. *Central European Management Journal*. *(31)*4, 511-521. https://www.emerald.com/insight/2658-0845.htm

Lee, H., & Gu, H. (2022). Empirical Research on the Metaverse User Experience of Digital Natives. *Sustainability, 14*(22). https://doi.org/10.3390/su142214747.

Lee, U.K., & Kim, H. (2022). UTAUT in Metaverse: An "Ifland" Case. *Journal of Theoretical and Applied Electronic Commerce Research, 17*(2), 613–635. https://doi.org/10.3390/jtaer17020032

Lena-Acebo, F.J., Renés-Arellano, P., Hernández-Serrano, M.J., & Caldeiro-Pedreira, M.C. (2022). Knowing how to share and to protect oneself: key factors on digital cybercritical education for children. *Profesional de la información*, *31*(6). https://doi.org/10.3145/epi.2022.nov.09

Lluch, L., Balbontin, F., & Sullivan, N. (2022). Enhancing cooperative learning and student motivation with gamification strategies: A case study in industrial engineering. *Journal of Technology and Science Education, 12*(3), 611-627. https://doi.org/10.3926/jotse.1693

López-Belmonte, J., Segura, A., Fuentes, A., & Parra, M. (2020). Evaluating Activation and Absence of Negative Effect: Gamification and Escape Rooms for Learning. *International Journal of Environmental Research and Public Health, 17*(7). https://doi.org/10.3390/ijerph17072224

López-Noguero, F., Gallardo-López, J., & Muñoz-Villaraviz, D. (2022). Videojuegos y preadolescencia. Uso, hábitos e implicaciones socioeducativas en función del género. *Revista Colombiana de Educación, 1*(84), 1-25. https://doi.org/10.17227/rce.num84-12701

López, FA, Ruete, D., Gatica, G. (2021). Infraestructura crítica y ciberseguridad en Chile: Lineamientos para el consenso. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, (E43), 41–55. https://www.risti.xyz/issues/ristie43.pdf

Manterola, C.; Astudillo, P.; Arias, E. & Claros, N. (2013). Systematic reviews of the literature: what should be known about them. *Cir. Española Journal,* 91(3):149-55. DOI: 10.1016/j.cireng.2013.07.003

Martín, N. (2022). Estudio del conocimiento de los menores sobre las consecuencias de sus actuaciones en las Redes Sociales. *Doxa Comunicación. Revista Interdisciplinar de Estudios de Comunicación y Ciencias Sociales*, 35, 419. http://hdl.handle.net/10637/13798

Martínez, F., Sánchez, L., Santos-Olmo, A., Rosado, D., & Fernández, E. (2024). Maritime cybersecurity: protecting digital seas. *Revista Internacional de Seguridad de la Información, 23*(2), 1429–1457. https://doi.org/10.1007/s10207-023-00800-0

Martínez, J., Lareki, A., & Altuna, J. (2021). Risks Associated with Posting Content on the Social Media. *Revista Iberoamericana de Tecnologías del Aprendizaje, 16*(1) 77-83. https://doi.org/10.1109/RITA.2021.3052655

Mejía-Lobo, M., Hurtado-Gil, S. V., y Grisales-Aguirre, A. M. (2023). Ley de delitos informáticos colombiana, el convenio de Budapest y otras legislaciones: Estudio comparativo. *Revista de Ciencias Sociales*, XXIX (2), 356-372. https://doi.org/10.31876/rcs.v29i2.39981

Moher, D., Liberati, A., Tetzlaff, J., Altman, DG y PRISMA Group. (2009). Elementos de informe preferidos para revisiones sistemáticas y metanálisis: la declaración PRISMA*. Annals of Internal Medicine*, 151(4), 264-269. DOI: 10.1016/j.jclinepi.2009.06.005

Navarro, C., Pérez, I., & Marzo, P. (2021). La gamificación en el ámbito educativo español: revisión sistemática (Gamification in the Spanish educational field: a systematic review). *Retos, 42*, 507–516. https://doi.org/10.47197/retos.v42i0.87384

Padilla, R., Ojeda, A. y Sanchez, C. (2023). Issues in Information Systems Navigating the business landscape: challenges and opportunities of implementing artificial intelligence in cybersecurity governance. *Issues in Information Systems,* 24(4), 328-338. https://doi.org/10.48009/4_iis_2023_125

Page, M., McKenzie, J., Bossuyt, P., Boutron, I., Hoffmann, T., Mulrow, C., Shamseer, L., Tetzlaff, J., Akl, E., Brennan, S., Chou, R., Glanville, J., Grimshaw, J., Hróbjartsson, A., Lalu, M., Li, T., Loder, E., Mayo-Wilson, E., McDonald, S., …Moher, D. (2021). Declaración PRISMA 2020: una guía actualizada para la presentación de informes de revisiones sistemáticas. *PLOS Medicine*, 18(3), e1003583. https://doi.org/gjpmcj

Palma-Ruiz, J. M., Torres-Toukoumidis, A., González-Moreno, S. E., & Valles-Baca, H. G. (2022). An overview of the gaming industry across nations: using analytics with power BI to forecast and identify key influences. *Heliyon,* 8(2), Artículo e08959. https://doi.org/10.1016/j.heliyon.2022.e08959

Parra, D., y Concha, R. (2021). Inteligencia artificial y derecho. Problemas, desafíos y oportunidades. *Vniversitas*, 70, 1–25. https://doi.org/10.11144/Javeriana.vj70.iadp

Payá-Santos, C., & Luque Juárez, J. M. (2021). El sistema de inteligencia criminal ante las nuevas amenazas y oportunidades del ciberespacio. *Revista Científica General José María Córdova*, 19(36), 1121-1136. https://dx.doi.org/10.21830/19006586.855

Ortega-Jiménez, D., Cedeño-González, G., & Ramírez, M. (2023). Uso problemático de videojuegos y flexibilidad de afrontamiento en adolescentes ecuatorianos. *Health and Addictions/ Salud y Drogas, 23*(1), 289-301. https://doi.org/10.21134/haaj.v23i1.748

Perafán Del Campo, E.A., Polo Alvis, S., Sánchez Acevedo, M.E., & Miranda Aguirre, C. (2021). Estado y soberanía en el ciberespacio. *Via Inveniendi Et Iudicandi,* 16(1). https://doi.org/10.15332/19090528.6480

Oz, B. (2023). A new perspective in construction management; the metaverse*. Revista De La Construcción. Journal of Construction, 22*(2), 321-336. https://doi.org/10.7764/RDLC.22.2.321.

Patán, R., & Parizi, R. (2023). Securing Data Exchange in the Convergence of Metaverse and IoT Applications. *ACM International Conference Proceeding Series,* (129), 1-8*.* https://doi.org/10.1145/3600160.3605019

Qamar, S., Anwar, Z., & Afzal, M. (2023). A systematic threat analysis and defense strategies for the metaverse and extended reality systems. *Comput. Secur. 128*, 1-22. https://doi.org/10.1016/j.cose.2023.103127

Quayyum, F., Cruzes, D., & Jaccheri, M. (2021). Cybersecurity awareness for children: A systematic literature review*. International Journal of Child-Computer Interaction, 30*, 1-25. https://doi.org/10.1016/j.ijcci.2021.100343

Queirolo, F., Matheu, A., Ruff, C., Juica, P., Ruiz, M. (2021). El 5G como vector de soberanía nacional: oportunidades y desafíos. *Revista Ibérica de Sistemas e Tecnologias de Informação*; Lousada. (E46), 28-43.

Ramírez-Plascencia, D., Alonzo-González, R. y Marín-Tapiero, J. (2022). Youtubers menores de edad y sus riesgos frente a los vacíos legales en México. *Revista Mediterránea de Comunicación,* 13(1), 65-77. https://www.doi.org/10.14198/MEDCOM.20781

Rangel, C. (2022). Inteligencia Artificial como aliada en la supervisión de contenidos comerciales perjudiciales para menores en Internet. *Revista Mediterránea de Comunicación, 13*(1), 17-30. https://www.doi.org/10.14198/MEDCOM.20749

Riega-Virú, Y., Nilupu-Moreno, K., Salas-Riega, J., & Ninaquispe, M. (2023). Knowledge of cybersecurity against social cybercrime of female high school students. *Education and Research*. 1-4 https://doi.org/10.1109/ICALTER61411.2023.10372927

Rodrigues, R., Gouveia, R., & Pereira, C. (2019). Gamification in Management Education: A Systematic Literature Review. *BAR - Revista de la Administración Brasileña, 16*(2). https://doi.org/10.1590/1807-7692bar2019180103

Rodríguez, A., Vicente, E., De Mena, J., & Pérez, S. (2022). Efecto de la práctica de actividad física gamificada en el estado de ánimo de jugadoras de baloncesto en etapa de confinamiento (Effect of gamified physical activity practice on the mood of female basketball players in confinement stage). *Retos, 43*, 10–16. https://doi.org/10.47197/retos.v43i0.87177

Rodríguez, C., & Palomo, R. (2023). Transparencia, Ciberseguridad e Identidad Digital en el Contexto 5G | Transparencia, ciberseguridad e identidad digital en el entorno 5G. *Revista Española de la Transparencia*, (18), págs. 359–380. https://doi.org/10.51915/ret.298

Ruiz-Bañuls, M., Gómez-Trigueros, I.M., Rovira-Collado, J., Rico-Gómez, M.L. (2021). Gamification and Transmedia in Interdisciplinary Contexts: A Didactic Intervention for the PrimarySchool Classroom, *Heliyon,* 7 (6), https://doi.org/10.1016/j.heliyon.2021.e07374.

Samnani, S., Vaska, M., Ahmed, S. & Turin, T. C. (2017). Review typology: the basic types of reviews for synthesizing evidence for the purpose of knowledge translation. *J. Coll. Physicians Surg. Pak*., 27(10):635-41. https://www.jcpsp.pk/archive/2017/Oct2017/10.pdf

Silva, R. J. R. da, Rodrigues, R. G., & Leal, C. T. P. (2019). Gamification in management education: A systematic literature review. *Brazilian Administration Review*, 16(2), e180103. https://doi.org/10.1590/1807-7692bar2019180103

Seoane, M. V. (2023). La ciberhegemonía de EE. UU. en la OEA. Estudos Internacionais. *Revista De relações Internacionais da PUC Minas*, 10(4), 91–112. https://doi.org/10.5752/P.2317-773X.2022v10n4p91-112

Sommer, U., Matania, E., & Hassid, N. (2023). The rise of companies in the cyber era and the pursuant shift in national security. *Political Science, 75*(2), 140-164. https://doi.org/10.1080/00323187.2023.2278499

Talapuru, S., Dantu, R., Upadhyay, K., Badruddoja, S., & Zaman, S. (2023). The Dark Side of the Metaverse: Why is it Falling Short of Expectations? *2023 5th IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA),* 287-296. https://doi.org/10.1109/TPS-ISA58951.2023.00043

Trejos-Gil, C., & Peláez-Vélez, Y. (2023). Ciberdelitos en menores de edad en la red social Facebook: revisión sistemática de literatura. *Nuevo Derecho, 19*(32), 1–18. https://doi.org/10.25057/2500672X.1493

Valencia, L. (2022). Implementación de estrategias gamificadas en el marco de la comunicación organizacional. *Revista Internacional de Cultura Visual, 7*(10), 1-11. https://doi.org/10.37467/revvisual.v9.3623

Wang, Y., Su, Z., Zhang, N., Liu, D., Xing, R., Luan, T., & Shen, X. (2022). A Survey on Metaverse: Fundamentals, Security, and Privacy. *IEEE Communications Surveys & Tutorials, 25*(1), 319-352. https://doi.org/10.1109/COMST.2022.3202047

Winterhalter, C. (2023). Metaverse and Its Communication. The Future is Here. True or False? en: Sabatini, N., Sádaba, T., Tosi, A., Neri, V., Cantoni, L. (eds.), Fashion Communication in the Digital Age. FACTUM 2023. *Proceedings in Business and Economics* (37-48). https://doi.org/10.1007/978-3-031-38541-4_4