Ciencia Latina Revista Científica Multidisciplinar, Ciudad de México, México.
ISSN 2707-2207 / ISSN 2707-2215 (en línea), mayo-junio 2025,
Volumen 9, Número 3.

https://doi.org/10.37811/cl_rcm.v9i1

ANÁLISIS DE LOS DELITOS CIBERNÉTICOS EN EL ÁMBITO DE LOS VIDEOJUEGOS, METAVERSO Y ESTRATEGIAS PARA MEJORAR LA GESTIÓN DE INCIDENTES CIBERNÉTICOS EN LA POLICÍA NACIONAL

ANALYSIS OF CYBERCRIME IN THE FIELD OF VIDEO GAMES, THE METAVERSE, AND STRATEGIES TO IMPROVE CYBER INCIDENT MANAGEMENT WITHIN THE NATIONAL POLICE

Edilberto Gutiérrez Palacios
Escuela de Tecnologías de la Información y las Comunicaciones

Rut Urueña Sanabria
Escuela de Tecnologías de la Información y las Comunicaciones

Jairo Rojas Ángel
Escuela de Seguridad vial

DOI: https://doi.org/10.37811/cl_rcm.v9i3.18675

Análisis de los Delitos Cibernéticos en el Ámbito de los Videojuegos, Metaverso y Estrategias para Mejorar la Gestión de Incidentes Cibernéticos en la Policía Nacional

Edilberto Gutiérrez Palacios[1]
edilberto.gutierrez1511@gmail.com
https://orcid.org/0009-0002-4264-0252
Escuela de Tecnologías de la Información y las Comunicaciones

Rut Urueña Sanabria
doceducacion2019@gmail.com
https://orcid.org/0009-0000-7960-7902
Escuela de Tecnologías de la Información y las Comunicaciones

Jairo Rojas Ángel
rrangel2024@gmail.com
https://orcid.org/0000-0002-7851-9617
Escuela de Seguridad vial

RESUMEN

Con la innovación tecnológica, las nuevas generaciones están cada vez más inmersas en el mundo digital; esto se debe a la participación de juegos en línea, concibiendo, lamentablemente, un blanco de amenazas y extorsiones por parte de delincuentes cibernéticos. Basado en ello, se planteó el siguiente objetivo de investigación: contribuir al fortalecimiento del manejo de incidentes cibernéticos en la Policía Nacional, a través de la identificación de ciberdelitos en videojuegos y en el metaverso, implementando estrategias específicas que mejoren la capacidad de respuesta ante las amenazas emergentes. El estudio se llevó a cabo mediante una metodología centrada en una investigación no experimental, utilizando criterios sistemáticos para establecer su estructura o comportamiento y proporcionar alternativas de atención a incidentes cibernéticos en la Policía Nacional, mediante un enfoque cualitativo a partir de una revisión documental y la selección de una muestra poblacional de 6577 jugadores de videojuegos y metaverso en la ciudad de Bogotá entre un rango de 18 a 40 años de edad, a partir de una selección muestral de 363 jugadores, con una confianza del 95% y un margen de error del 5%. Los resultados de la revisión documental y el estudio de la población reflejan una alta interacción de los ciberdelincuentes en las plataformas de entretenimiento de videojuegos y el metaverso y, por otro lado, limitaciones estructurales, tecnológicas y operativas de la Policía Nacional para enfrentar este fenómeno delincuencial.

***Palabras claves**:* ciberdelitos, videojuegos, metaverso, tecnología, herramientas tecnológicas

[1] Autor principal
Correspondencia: edilberto.gutierrez1511@gmail.com

Analysis of Cybercrime in the Field of Video Games, the Metaverse, and Strategies to Improve Cyber Incident Management Within the National Police

ABSTRACT

With technological innovation, younger generations are increasingly immersed in the digital world; this is due to their participation in online games, unfortunately creating a target for threats and extortion by cybercriminals. Based on this, the following research objective was proposed: to contribute to strengthening cyber incident management within the National Police by identifying cybercrimes in video games and the metaverse, implementing specific strategies that improve response capacity to emerging threats. The study was carried out using a methodology focused on non-experimental research, using systematic criteria to establish its structure or behavior and provide alternatives for addressing cyber incidents within the National Police, through a qualitative approach based on a documentary review and the selection of a population sample of 6,577 video game and metaverse players in the city of Bogotá between the ages of 18 and 40, from a sample selection of 363 players, with a confidence level of 95% and a margin of error of 5%. The results of the documentary review and the population study reflect a high level of interaction between cybercriminals on video game entertainment platforms and the metaverse, and, on the other hand, structural, technological, and operational limitations of the National Police to confront this criminal phenomenon.

Keywords: cybercrime, video games, metaverse, cybersecurity, national police

Artículo recibido 11 junio 2025
Aceptado para publicación: 30 junio 2025

INTRODUCCIÓN

La acelerada transformación digital ha dado lugar a nuevos espacios de interacción social y económica, donde los videojuegos en línea y el metaverso se han consolidado como entornos virtuales de alta participación, especialmente entre los jóvenes. Los entornos virtuales recorren un doble filo: por un lado, se ofrecen como espacios de ocio y enseñanza; por otro lado, se convierten de inmediato en plazas donde delincuentes ejecutan estafas, chantajes y hurtos de información sensible. El acoso digital se ha normalizado, la extorsión sigue un rumbo al alza y el robo de datos personales, con su rostro infraganti, mantiene ocupadas a las autoridades de seguridad e investigación. Colombia no está exenta de ese problema. La Policía Nacional, ante el asedio de amenazas cibernéticas, recorre el mismo sendero de la innovación tecnológica para reaccionar a la misma velocidad con que emergen los delitos. Cada avance en software o red obliga a una revisión de protocolos, sistemas forenses y cursos de capacitación, porque lo que hoy resulta eficaz mañana puede volverse obsoleto.

La presente investigación emergió de la inquietud por el crimen digital alojado en el mundo de juego y el metaverso, espacios donde los delitos han comenzado a florar cotidianamente. El propósito inicial es desmenuzar esas infracciones, detectar las grietas en el marco normativo vigente y poner al descubierto las debilidades operativas que todavía persisten en las instituciones encargadas de la seguridad, alineadas con los principios de seguridad digital, protección de derechos y eficiencia operativa, basado en los siguientes objetivos: 1) Identificar los tipos de ciberdelitos más frecuentes en los entornos de videojuegos y metaverso, con el fin de establecer un perfil detallado de las amenazas y sus características, facilitando así la comprensión de las dinámicas delictivas para la Policía Nacional. a) Plantear estrategias para el fortalecimiento del proceso y procedimientos de incidentes cibernéticos, permitiendo que la Policía Nacional adopte herramientas con capacidad de respuesta a los ciberdelitos. b) Proponer la actualización del proceso y los procedimientos de gestión de incidentes cibernéticos en la Policía Nacional mediante el desarrollo de protocolos específicos para la identificación, análisis y respuesta a ciberdelitos relacionados con videojuegos y metaverso. c) fortalecer el proceso de respuesta a incidentes cibernéticos en la Policía Nacional a través de la identificación de ciberdelitos en videojuegos y metaverso, mediante la implementación de estrategias específicas que mejoren la capacidad de respuesta frente a las amenazas emergentes.

Aplicando una metodología de diseño no experimental, descriptivo, con un enfoque cualitativo, método deductivo y modalidad documental, buscando identificar las características de los fenómenos existentes sobre los ciberdelitos en videojuegos y metaverso mediante el análisis documental y consulta ciudadana a través de encuesta estructurada, para determinar los diversos factores que inciden en los delitos de videojuegos y metaverso. Para entender el arraigo de este fenómeno se acudió a diferentes conceptos teóricos.

Delitos informáticos en videojuegos y metaverso

La industria de los videojuegos a nivel mundial ha experimentado un crecimiento sorprendente, convirtiéndose en una parte fundamental de la cultura y el entretenimiento de los jóvenes a nivel global (Monzón, 2022). No obstante, esta expansión ha sido acompañada por un incremento en los delitos informáticos vinculados a los videojuegos. Desde estafas y fraudes hasta el lavado de dinero y la explotación de población juvenil, dadas las circunstancias de la innovación tecnológica, puesto que los inducen cada vez más a participar en juegos en línea, siendo en ocasiones objeto de amenazas y extorsión por parte de los ciberdelincuentes (Martínez, 2019). Por otro lado, Chen et al. (2021) basándose en diversos estudios, explican que a medida que el internet se vuelve más potente y alcanza más lugares, tanto la sociedad como su entorno se vuelven cada vez más dependientes del mundo digital. Esta dependencia, sin los debidos controles, convierte al entorno digital en un espacio riesgoso, especialmente por la recolección constante de información personal por parte de múltiples plataformas. Vásquez (2019) señala que los ciberdelincuentes suelen copiar sitios web imitando el diseño de empresas reconocidas, usurpando sus nombres para vender productos falsos en plataformas virtuales atractivas. Utilizan marcas de compañías públicas y privadas con el fin de engañar a los usuarios y estafarlos mediante fraudes en línea.

Valencia et al., (2023) señala que estudios realizados en América Latina sobre delitos informáticos, concluyen que el avance científico ha impulsado un rápido desarrollo de las tecnologías de la información y las comunicaciones (TIC). La falta de regulación y vigilancia ha contribuido al incremento de la ciberdelincuencia, la cual explota vulnerabilidades en los sistemas informáticos para infiltrarse y causar daños. En la misma línea, López (2021), expone en su obra sobre derecho digital una visión innovadora sobre el uso de las herramientas tecnológicas y el rol del Estado y la ciudadanía

en la actual revolución digital. Señala que la ciberdelincuencia se ha venido fortaleciendo en América Latina a medida que surgen nuevos escenarios tecnológicos, lo que exige una evolución permanente de las estrategias de ciberseguridad de los Estados. También resalta la necesidad de cerrar la brecha digital, fortalecer el conocimiento técnico y fomentar un uso responsable de la tecnología, para evitar que actores malintencionados aprovechen indebidamente la información personal."

En Colombia, el gobierno y las autoridades han trabajado en el fortalecimiento tanto de herramientas digitales como del marco normativo para enfrentar los delitos informáticos. Un ejemplo es la Ley 1273 de 2009, que tipifica estas conductas y permite identificar los delitos de mayor incidencia, sus causas y las prioridades de los ciberdelincuentes. Permitiendo a la entidad policial enfrentar las diferentes modalidades de los delincuentes (Rincón, et al., 2023). En otro contexto, Arteaga (2023) desde un análisis conceptual y deductivo, examina los patrones de la ciberdelincuencia en Colombia y los divide en tres aspectos clave. En primer lugar, identifica la trascendencia de las conductas punibles cometidas mediante tecnologías de la información y las comunicaciones. En segundo lugar, analiza las particularidades de los delitos informáticos relacionados con videojuegos. Finalmente, estudia la regulación jurídica nacional y el bien jurídico protegido en estos casos.

Por su parte, Verano (2023) refiere que la expansión del internet como el interés por los videojuegos en Colombia han aumentado significativamente en los últimos años, una tendencia previsible en el contexto de la transformación digital del país. Reportes de instituciones como la Policía Nacional de Colombia y el Centro Cibernético Policial señalan un aumento inquietante en las denuncias de delitos cibernéticos en plataformas de videojuegos (Acosta et al., 2020). La carencia de herramientas especializadas para combatir y prevenir estos crímenes ha dejado expuestos a usuarios y plataformas a diferentes tipos de ataques. Esta situación resalta la importancia de mejorar las habilidades para enfrentar la naturaleza cada vez más compleja de los ataques cibernéticos.

Teoría de la Neutralización

M'Cready Sykes y Matza (2008), en su publicación sobre la teoría de la neutralización de 1957, teoría que fue inicialmente formulada para abordar la delincuencia juvenil, pero también para analizar los ciberdelitos. Propone que los infractores racionalicen sus conductas delictivas mediante técnicas de neutralización, tales como la negación de la responsabilidad ("no es mi culpa") o la minimización del

daño ("no hice nada malo"). En el contexto de los ciberdelitos, se puede observar cómo los perpetradores, hackers o estafadores, justifican sus acciones calculadas en una ética personal que minimiza o desestima las consecuencias de sus delitos. Las teorías del crimen comenzaron a tener un impacto significativo en el estudio científico del delito a finales de los años setenta, siendo uno de sus artículos de Lawrence E. Cohen y Marcus Felson uno de los principales catalizadores de este cambio de enfoque en el análisis y estudio de la delincuencia.

Teoría de metaverso, peligros cibernéticos

Según Peñuela (2023) menciona que la teoría está enfocada a los menores de edad, tanto niños como adolescentes, dado que son considerados sujetos que requieren una protección especial en el ámbito legal. Por esta razón, la seguridad y el bienestar de estos individuos constituyen uno de los principales objetivos de nuestra sociedad. Sin embargo, las nuevas generaciones tienen un acceso directo y sencillo a plataformas como la WEB 3.0 y el Metaverso, entornos que resultan novedosos e inexplorados para muchos, y que se convierten en blancos propicios para la comisión de ciberdelitos. Algunos adultos han compartido experiencias vividas en la Web 3.0 y el Metaverso, en las que, pese a conocer los riesgos y normativas de estos entornos, fueron víctimas de delitos cibernéticos cometidos por actores malintencionados que aprovecharon sus vulnerabilidades. Por ello, resulta fundamental evaluar los riesgos de seguridad que enfrentan los menores de edad que interactúan frecuentemente en entornos digitales como la web 3.0 y el metaverso**.**

Teoría del Control Social

Morillo y Howard (2017) se refieren a la teoría del control social postulada por Travis Hirschi (1969). Quienes sostienen que la ruptura de los vínculos comunitarios puede inclinar a ciertos sectores de la población hacia la delincuencia, incluidos los delitos cometidos en entornos digitales. La pérdida de compromiso, ya sea en la escuela, en el empleo o la disfunción familiar, deja un vacío que algunos llenan con el delito informático. La falta de normativas contundentes y orden legal alimenta el florecimiento de los delitos cibernéticos. Estudios recientes como los de Serna (2024) muestran que, en el ciberespacio, los jóvenes menos integrados socialmente presentan tasas notoriamente más altas de participación en hacking, phishing y fraudes electrónicos. Esta relación coincide con el enfoque del lazo social como factor de protección ante la conducta delictiva.

Teoría de la Gestión del Riesgo Cibernético

La teoría de gestión de riesgos cibernéticos por Gordon, Loeb, & Zhou (2016) publicada en el año 2002 examina la manera en que las organizaciones pueden maximizar la utilización de sus recursos en la gestión de riesgos cibernéticos. Este enfoque sugiere que una inversión estratégica en seguridad, enfocándose en los activos más vulnerables o de mayor importancia, puede fortalecer la capacidad de respuesta ante incidentes cibernéticos. La teoría indica que no todos los activos requieren el mismo nivel de protección, lo que hace que una evaluación de riesgos adecuada sea fundamental para que las organizaciones formulen estrategias más eficaces para reducir el impacto de los ciberdelitos. En la era actual de la interconexión digital, la seguridad cibernética es una preocupación esencial. En realidad, las naciones más desarrolladas de todo el mundo actualmente ven como una prioridad de política nacional el tener una estrategia de ciberseguridad.

Teoría del Enfoque en Defensa

El llamado enfoque en defensa que Barry Boehm separadamente trajo al discurso de la seguridad digital arrastra un legado militar que se remonta a la guerra de trinchera. Presentado en el célebre texto de Sommerville (2011) presenta el modelo originalmente desarrollado en el ámbito militar y posteriormente adaptada a la ciberseguridad por Barry Boehm en 1988, en el que hace hincapié en erigir barreras antes de lanzarse a la detección o la recuperación. La imagen mental es simple: se protege el perímetro, se limita el movimiento del atacante, si toda falla, es necesario pensar en una contramedida útil. Aunque su raíz es táctica, los principios se repiten consecutivamente antes de que este alcance los tesoros de una base de datos central. En los pasillos universitarios y en los cuarteles generales de Silicon Valley (2024), esto se traduce finalmente en la vieja norma de prevenir es mejor que curar, ahora acompañada por mil fórmulas de costes, matrices de riesgo y fórmulas de retorno que acaban en la misma conclusión.

La estrategia de defensa en profundidad sugiere que las instituciones deben instaurar capas superpuestas de protección. Esto abarca desde la formulación de políticas robustas y la instalación de controles técnicos hasta la capacitación continua de todo el personal. El propósito de esa superposición es disminuir la ventana de daño posible una vez que un vector de ataque logra burlar a alguna de las barreras iniciales.

Al consolidar ese entramado, la organización gana agilidad para detectar incidentes y responder a ellos en tiempo real. La eficacia de la configuración se evalúa a través de modelos matemáticos que, incorporados al software de seguridad, permiten calcular con precisión el impacto de parámetros como el tamaño de la red, la variedad de servicios que soporta y los algoritmos que administra.

Teoría de la Resiliencia Organizacional

La noción de resiliencia organizacional, formulada por Según Andrew & Healy (2012), sostiene que las instituciones deben aprender a anticipar, soportar, reaccionar y reponerse ante interrupciones bruscas, delitos cibernéticos incluidos. Este marco teórico va más allá de la mera prevención y centra la atención en fortalecer el tejido adaptativo de la entidad. Desde la óptica de la ciberseguridad, la propuesta exige combinar tácticas proactivas, como la actualización de infraestructuras críticas, con medidas reactivas, entre las que sobresalen los planes de respuesta y las simulaciones recurrentes. La esencia de la resiliencia radica, en extraer lecciones de cada incidente para afinar el dispositivo de defensa y elevar la eficacia frente a las amenazas que seguramente volverán.

Ciberdelitos en videojuegos y metaverso

Las plataformas de videojuego y el metaverso, potencias contemporáneas de la interacción digital, han emergido como nuevos frentes de vulnerabilidad frente al delito cibernético. La violación a la privacidad personal en estos espacios, señala Martínez (2024) que trasciende la simple pérdida de datos y empieza a comprometer ya la estabilidad de sistemas estatales y personales completos. De ese modo, la protección de la soberanía tecnológica se convierte en otro capítulo urgente dentro de la ciberdefensa nacional. El propio diseño interactivo y global del metaverso choca de lleno con el derecho penal tradicional. En su análisis, Carlen (2023), subraya que la fusión de realidades tradicional o el metaverso, aumentada y cadenas de bloques deja obsoletos muchos supuestos previstos en el Convenio de Budapest. Por eso, aparecen en la agenda normativa internacional la creación de instrumentos nuevos que, más que interiorizar, se instauran reglas claras para la defensa de los usuarios que se mueven por fronteras digitales

Tipología de ciberdelitos

Los especialistas coinciden en que los tipos de ciberdelitos se expanden casi tan rápido como avanza la tecnología misma.

Con la llegada del metaverso y plataformas similares, las nociones tradicionales de seguridad ya no encajan del todo, advierte Martínez (2024), que en ese nuevo paisaje digital, las fronteras entre países, delincuentes y delitos se vuelven cada vez más borrosas. Entre las amenazas más inquietantes figuran el hurto de datos personales, las estafas en pagos electrónicos y la suplantación de identidad, situaciones que (Martínez,2024). identifica en sus recientes informes. La creciente dependencia que tienen tanto los ciudadanos como los gobiernos de las redes y aplicaciones diarias significa que un ataque en el metaverso puede golpear con fuerza a las infraestructuras críticas de un Estado. Frente a ese panorama, queda claro que diseñar medidas de ciberseguridad concretas y coordinar la acción entre varias naciones ya no es opcional, sino una necesidad urgente.

Tipos de ciberdelitos más frecuentes

Uno de los delitos cibernéticos que aparece con mayor regularidad es el ciberacoso que circula dentro de los videojuegos competitivos profesionales. Las ligas de esports lo identifican casi a diario como un dolor de cabeza, desde una investigación reciente, Trudgett-Klose et al. (2024) documentaron que las jugadoras son atacadas con más frecuencia que sus pares masculinos, sobre todo en forma de agresiones sexuales explícitas y hostigamiento verbal. Esta dinámica les deja marcas en la salud mental. Los acosadores suelen excluir a la víctima del chat del equipo, difundir rumores malintencionados y, en ocasiones, manipular fotos o vídeos para burlarse abiertamente. Y agrega el autor, que todo esto crea una jerarquía tóxica en la que el agresor siempre parece tener la última palabra; también advierte que la simple decisión de competir en torneos aumenta la probabilidad de ser blanco de ataques, tanto por parte de otros jugadores como de la audiencia que sigue las partidas en línea; por ello, reclaman con urgencia el diseño de protocolos claros que reduzcan el daño psicológico y disciplinen los abusos en el momento en que ocurren. Sin respuestas rápidas, el panorama de los esports seguirá siendo, en muchos sentidos, una arena hostil.

Por su parte, Hu et al. (2024) han observado un auge notable del ciberacoso en los muros de las redes sociales. Este crecimiento, apuntan, al uso de nuevas herramientas tecnológicas que utilizan los agresores, pero también a la mezcla explosiva de rasgos personales en la interacción de ambientes virtuales hostiles. La teoría de acción situacional Wikström y Treiber (2016) sugiere que el delito en línea aparece cuando una predisposición clara se encuentra con un espacio propicio.

En la esfera digital, el anonimato y la desinhibición juegan el papel de esos espacios. Muchos usuarios, al sentirse ocultos detrás de una pantalla, recurren a técnicas de neutralización y convencen a sí mismos de que su daño es insignificante. Según Chen et al. (2021), corroboran este estudio y advierten que las dinámicas sociales dentro de las plataformas moldean fuertemente el acoso en línea, lo que hace urgente pensar en regulaciones que contengan estas manifestaciones de violencia digital.

Modalidad de operar

La capacidad de los ciberdelincuentes ha demostrado una sorprendente capacidad para reinventarse ante cada avance tecnológico. Esta agilidad criminal, según apuntes recientes de Corcoran (2024), afirma las formas de delito que rara vez permanecen estáticas. El ciberacoso, por ejemplo, se ha vuelto casi rutinario en las encuestas de delincuencia juvenil. Su notable recurrencia guarda relación directa con la conectividad y el desplazamiento casi absoluto de las interacciones sociales al espacio digital. Una diferencia clave con el acoso cara a cara es la falta de presencia física del acosador; su anonimato facilita el ataque y dificulta la defensa. En este contexto, el hostigamiento puede reanudar su curso a cualquier hora y en cualquier lugar, dejando a la víctima sin un respiro seguro. A juicio de Alcalá (2024), subraya que los ciberdelitos han ido mutando a la par con las plataformas que aparecen en el mercado, por lo que cada nuevo servicio arrastra consigo nuevos riesgos. El acceso no autorizado a sistemas y el maltrato virtual son dos de esos peligros que, se consolidan en aumento en la arquitectura cotidiana digital.

Impacto de los Ciberdelitos

El impacto de los ciberdelitos sigue ocupando un lugar central en el debate sobre gobernanza digital. Bentaouet (2024) define que el ciberespacio en general y el metaverso en particular han reconfigurado la concepción misma de los derechos humanos. La autora advierte que, aunque esas nuevas plataformas han abierto posibilidades tecnológicas inéditas, también han sido colonizadas por lo que ella denomina meta-delincuentes, individuos que operan al margen de un marco normativo claro. Estas figuras cometen fraudes, hurtos de identidad y otros ataques aprovechando la indefinición legislativa que todavía caracteriza al entorno tridimensional. De manera similar, Mohamed Saad Bentaouet (2024) sostiene que la inteligencia artificial, cuando se combina con prácticas robustas de ciberseguridad, debe erigirse en una primera línea de defensa frente a tales abusos.

De igual manera, subraya la urgencia de que el sector público y el privado coordinen esfuerzos para ahondar en el uso malicioso de las nuevas tecnologías. Ambas investigaciones concluyen que los derechos humanos seguirán en riesgo si no se instauran normas precisas que, además de proteger al ciudadano, actúen como disuasorios frente a los ciberdelincuentes.

Afectación psicológica y emocional en las víctimas

Un incidente delictivo que ocurre dentro de un mundo de juego no siempre se queda ahí; para muchas personas el daño emigra a la vida cotidiana. Psicólogos que han estudiado el fenómeno coinciden en que el trastorno inicial se traduce, con frecuencia, en estados de ansiedad, episodios depresivos y una tendencia creciente al aislamiento (Rubio et al., 2024). Estos síntomas tienden a agravarse por la intensidad inmersiva de las plataformas contemporáneas. Jugadores que han pasado horas forjando una identidad digital a menudo informan que el ataque virtual les parece tan tangible como un asalto en la calle. Por eso el vínculo que establecen con su avatar resulta ser, paradójicamente, un cable que conecta lo virtual con lo real. González (2023) alerta sobre un nuevo umbral de riesgo que trae consigo la realidad virtual inmersiva, especialmente en los espacios que la etiqueta metaverso. Según ella, las emociones que generan esos entornos son tan vibrantes que la propia corteza cerebral las codifica como eventos físicos reales.

En esos escenarios, el perfil del delito también se transforma: surgen agresiones emocionales disfrazadas de bromas inocentes y manipulación muy fina de datos que antes los usuarios consideraban seguros. Frente a ello, la caja de herramientas jurídicas existente muestra, con frecuencia, lo obsolescente que puede llegar a ser. Por su parte, Margaico et al. (2024) y sus colegas sostienen que el uso problemático de los videojuegos se ha convertido en uno de los comportamientos de riesgo más visibles entre los adolescentes de secundaria.

Según su observación, las horas acumuladas frente a la pantalla muestran una correlación directa y estadísticamente significativa con el aumento de la agresividad tanto en el aula como en el hogar. Los mismos investigadores anotan una diferencia notable por género: los varones tienden a superar a las niñas, tanto en el tiempo de juego descontrolado como en la frecuencia de las explosiones de cólera. En otra línea de estudio, Rubio et al. (2024) y sus colaboradores advierten que las violencias de género han encontrado un nuevo auge en espacios digitales como Valorant, donde los insultos y las amenazas

migran con facilidad por sus arquitecturas interactivas, que propician comportamientos misóginos en plataformas multijugador, donde las mujeres suelen ser objeto de trato degradante.

Consecuencias económicas y pérdida de información

El entorno digital contemporáneo ofrece un asombroso grado de anonimato que los delincuentes aprovechan para operar sin ser identificados. Casi siempre el acceso directo a bases de datos personales y la falta de barreras de entrada eficientes dejan a los usuarios en una posición precaria, como observa (Torres, 2024). Desde el hurto de una identidad hasta un simple fraude de compra, la gama de abusos se expande, pero el intruso que logra entrar en una cuenta de correo sigue siendo uno de los clásicos que más daño producen. En plataformas de videojuegos o en mundos emergentes del metaverso, el crecimiento descontrolado de la actividad delictiva exige ahora desmenuzar exactamente qué variables impulsan cada ataque. De acuerdo con Quintero et al. (2024), apuntan que la carencia de normas precisas que definen el delito de manera contemporánea deja a los jueces sin argumentos sólidos y a los delincuentes sin temor, favoreciendo así la suplantación digital o el uso indiscriminado de troyanos. Esa misma indefinición se combina con un arsenal técnico que los cibercriminales actualizan constantemente, lo que coloca a la fuerza publica en la tarea de formar personal que entienda de redes, de criptografía y de software forense antes de que aparezca el siguiente vector de ataque.

Estrategias para el fortalecimiento al proceso de incidentes cibernéticos

Los estudios recientes sugieren que es indispensable mapear la intersección entre rasgos personales de los usuarios y las dinámicas específicas del contexto digital. Esa cartografía sirve de base para construir defensas preventivas que funcionen, por igual, en redes sociales, entornos de tipo metaverso y plataformas de videojuego (Rincón et al.,2023). Tal perspectiva ofrece a la Policía Nacional de Colombia un andamiaje teórico útil en el diseño de políticas de ciberseguridad y en la elaboración de talleres educativos. Las acciones resultantes deben dar igual peso a las disposiciones individuales del sujeto y a las características del ecosistema en red que facilitan la actividad delictiva.

La gestión de incidentes cibernéticos requiere un enfoque integral, adaptable y coordinado que articule elementos técnicos, estructurales y humanos (Mendiola,2022). En este contexto, el uso de tecnologías como los Sistemas de Gestión de Información y Eventos de Seguridad (SIEM) y las plataformas de

Orquestación, Automatización y Respuesta (SOAR) permite detectar y responder de forma más ágil y eficiente a las amenazas digitales (Quintero & Tovar, 2019).

Eficacia de las Estrategias Implementadas

Para evaluar la eficacia de las estrategias de ciberseguridad es indispensable considerar investigaciones como el documento "Libertad vs. Seguridad de Riquert (2024), publicado en la *Revista Amagis Jurídica*. Este trabajo propone mecanismos de formación en ciberpatrullaje y la creación de unidades de inteligencia artificial aplicadas a la seguridad, además de abordar los retos actuales relacionados con el equilibrio entre la protección digital y los derechos individuales (Polícia Nacional, 2018).

Solución de incidentes

El análisis de los delitos cibernéticos en entornos como el metaverso y los videojuegos permite abordar la complejidad de incidentes asociados a actividades ilícitas que explotan vulnerabilidades tecnológicas y se benefician de la naturaleza global del ciberespacio. Según García (2024), subraya que la ciberdelincuencia organizada ha visto un espectacular auge de alcance en el contexto contemporáneo. Marquez et al. (2024) deduce que las regulaciones de los ciberdelitos en transacciones digitales, unido al anonimato en plataformas, contrasta con el escaso conocimiento de prácticas elementales de ciberseguridad entre la población. La suma de estos elementos ha desembocado en una oleada de incidentes que, día tras día, ponen a prueba los recursos de la Policía Nacional.

Para entender la vulnerabilidad actual, es necesario desmenuzar los factores que permiten operar a los grupos criminales a escala global. Su movilidad transnacional, protegida tras una cortina de tecnología, hace que muchas fugas se conviertan en grandes charcos donde la justicia apenas logra pescar algo (López, 2021). Direcciones IP enmascaradas, capas múltiples de cifrado y servidores anclados en jurisdicciones remotas dificultan la recolección de simples evidencias digitales. Ante ese fondo, el cuerpo policial se enfrenta a un doble déficit: técnico y jurídico. Sin herramientas de geo-localización precisas y sin marcos legales que agilicen la cooperación internacional, la persecución tiende a desinflarse antes de empezar (Malo, 2024). De no corregirse esos puntos débiles, el metaverso, los videojuegos y otros espacios digitales seguirán siendo feudos donde los delincuentes se mueven con mayor libertad que los propios investigadores.

El crecimiento desbordante de los delitos cibernéticos en plataformas como el metaverso y los mundos de juego está directamente relacionado con la rápida evolución de las tecnologías digitales (Guerrero, 2022). Esa misma aceleración ha alimentado modalidades delictivas que erosionan los derechos individuales de los usuarios y ponen en riesgo la estabilidad financiera de las empresas. Según Malo et al. (2024), advierten que la ausencia prolongada de marcos jurídicos precisos, así como la falta de tratados internacionales operativos, han generado un ecosistema casi sin consecuencias. Un caso emblemático es el carding, maniobra que implica la utilización no autorizada de números de tarjeta de crédito para concretar compras virtuales (Georgina et al.,2024). La naturaleza anónima de estos entornos facilita a los criminales ocultar sus huellas, lo que convierte dicha práctica en una rutina superficial dentro del comercio online.

Selección de estrategias

La respuesta coordinada contra el ciber delito en plataformas multijugador exige un personal que no solo dominen las herramientas de seguridad, sino que también entiendan las tácticas del crimen virtual. Esto no es un mero adiestramiento técnico, sino un estudio profundo de las rutinas de los agresores y de las intervenciones que se pueden aplicar en tiempo real. Según Chicharro et al.(2024), el videojuego ha pasado de ser simple distractor a actuar como eje de socialización para la adolescencia, por lo que las dinámicas de competencia y colaboración dentro del juego son claves para construir políticas de defensa acertadas. Y agrega que cuando los entornos digitales se integran en los programas académicos el aprendizaje se vuelve más interactivo y crítico. En paralelo, esos mundos virtuales sirven de nicho social, donde se forjan comunidades que refuerzan el sentido de pertenencia juvenil y generan nuevas estructuras de relación en línea.

Valencia et al. (2023) y sus coautores deducen que la cultura gamer agudiza el roce entre miembros de comunidades en línea. Su estudio se centra en los entornos de videojuego convencional y en las ligas de esports. Los foros y las salas de chat que surgen a su alrededor hacen más que entretener; actúan como bancos para identidades colectivas y para tácticas de relación entre pares (Martínez, 2024). Por su parte, la pantalla normal ha dejado atrás su carácter recreativo, por el surgimiento de plataformas y redes sociales en el que expresan conductas y hábitos entre los jugadores atractivos para los jóvenes.

En el ámbito contemporáneo de la ciberseguridad, Campos (2024) alerta sobre la creciente vulnerabilidad que presentan las redes sociales y demanda una campaña de concienciación masiva. Su estudio identifica el robo de identidad y la propagación de rumores falsos como delitos que han encontrado un terreno fértil en estos entornos virtuales, generando daños que trascienden al individuo y afectan al tejido social. El autor insiste en que, además de abrir debate público, es imprescindible educar a los usuarios acerca de las opciones de privacidad disponibles y fomentar rutinas de autoprotección que, aunque simples, pueden mitigar muchos de esos riesgos cotidianos. Hernández (2020), orientado más hacia la política institucional, propone que la evolución de los protocolos de ciberseguridad se centre de manera inequívoca en la confidencialidad y en la integridad de la información, dos pilares que, si flaquean, dejan desprotegidos los datos personales de cualquiera.

Capacitación en temas cibernéticos al Personal del centro cibernético C4 y centro de atención inmediata virtual.

Para los miembros de la Policía Nacional que operan en las unidades de control y prevención de ciberdelitos, el aprendizaje en ciberseguridad ya no es opcional. La escena del crimen ha trasladado su zona de acción al espacio digital y las herramientas tradicionales no bastan. La agenda del curso cubre el análisis forense digital, la recolección ordenada de evidencia electrónica y, por supuesto, el delicado mantenimiento de la cadena de custodia que evita que un dato pierda su valor probatorio.

La tendencia incluye nodos sobre tecnologías emergentes: blockchain, criptomonedas, entornos de metaverso y las rutinas de hacking ético que permiten probar la fortaleza de un sistema antes de que los delincuentes lo hagan. Las sesiones son en su mayoría prácticas, con laboratorios virtuales donde los participantes responden a simulacros que imitan incidentes reales (Guerrero,2022). Las repeticiones de los participantes permiten fortalecer sus conocimientos en sistemas de alertas tecnológicas.

Para que el conocimiento aflore la formación debe ser continua, por lo que es necesario establecer un canal permanente de actualización, con la participación de expertos de la industria privada, universidades públicas, privadas y centros especializados. Acosta et al. (2020) sostiene que la red de colaboradores permite conocer tendencias delictivas recientes y nuevas prácticas de operancia, en

medio de tanto código y protocolos, el oficial también tendrá que navegar el laberinto legal y manejar herramientas digitales de análisis forense que, pese a su poder, no siempre son intuitivas.

Capacitación para enfrentar las amenazas cibernéticas

Los equipos encargados de la ciberprevención benefician de un currículo que incorpora el manejo operativo de la Inteligencia Artificial. Este enfoque práctico responde a la creciente automatización de procesos críticos, como la detección temprana y clasificación de incidentes en tiempo real. Según Legidos (2024), apunta que la IA ha pasado de ser un prototipo en laboratorio a un componente estructural del kit moderno de ciberseguridad. Su utilidad es palpable en delitos recurrentes, desde el ciberacoso hasta el ransomware, cuyos patrones se revisan hoy con algoritmos en vez de solo con informes manuales. A su vez, Legidos y Verely (2024), aclaran que el aprendizaje automático no solo avisa, sino que también ayuda a neutralizar ataques al reconocer huellas digitales de comportamiento malicioso. Por todo ello, los analistas y los operadores del Estado deben practicar el manejo cotidiano de estas herramientas, asegurándose de que su pericia trascienda del ámbito público al privado sin quiebres.

Actualización de formatos del proceso y procedimientos de incidentes cibernéticos

La actualización de los formatos y procedimientos utilizados por la Policía Nacional para tratar incidentes en red, proyecta una remodelación exhaustiva de los procedimientos. Las nuevas modalidades de ataque obligan a replantear no sólo plantillas, sino también protocolos enteros que quedaban bien para el panorama digital de hace un trienio. Al tiempo la Policía Nacional (2018) enfatiza que es necesario implementar protocolos estandarizados que contemplen formularios electrónicos para denuncias en línea, recolección sistemática de evidencia digital y generación automatizada de informes de seguimiento. Arteaga (2023) recomienda que los nuevos formatos deben incluir secciones específicas para clasificar tipos de ciberdelitos, métodos de ataque, vectores de amenaza y consecuencias sobre las víctimas. Esta sistematización facilitará tanto el análisis estadístico como la capacidad de respuesta institucional ante los incidentes.

Tabla 1 Marco Legal

Normas jurídicas para afrontar los ciberdelitos en Colombia	
Política Nacional de Seguridad Digital CONPES 3854, del 2016	Esta norma establece los criterios y objetivos de la estrategia de seguridad cibernética en Colombia, abarcando aspectos como la protección de infraestructuras tecnológicas, el desarrollo de competencias y la cooperación internacional (Política Nacional de Seguridad Digital CONPES 3854, 2016).
Ley 1273 del 2009	Ley que tipifica los delitos informáticos en Colombia, introduciendo modificaciones al Código Penal para salvaguardar la información y los datos como un nuevo bien jurídico, además de proteger los sistemas que utilizan tecnologías de la información y las comunicaciones (Ley 1273, 2009)
Ley 1341 del 2009	Normativa que establece principios y conceptos relacionados con la "sociedad de la información" y la organización de las Tecnologías de la Información y las Comunicaciones (TIC), además de crear la Agencia Nacional de Espectro y emitir regulaciones adicionales en el país (Ley 1341, 2009).
Ley 1581 del 2012	Ley que regula la protección de datos personales, estableciendo directrices para el tratamiento de información personal y definiendo derechos y responsabilidades en su gestión dentro del territorio colombiano (Ley 1581, 2012).
Decreto 2573 del 2014	Reglamento que establece los lineamientos generales para la Estrategia de Gobierno en línea, definiendo directrices para la implementación de la política de Gobierno Digital, incluyendo aspectos relacionados con la seguridad digital (Decreto 2573, 2014). Decreto 1078 del 2015 Normativa que establece medidas de seguridad y privacidad.

Nota. Relación de la normatividad jurídica para afrontar y controlar a los ciberdelincuentes, fuente, páginas de la secretaria del senado http://www.secretariasenado.gov.co/leyes-de-la-republica

Diseño Metodológico

El diseño metodológico representa un eje central para identificar los ciberdelitos en videojuegos y metaverso, ya que define la ruta científica que asegura la validez y confiabilidad de los hallazgos. Según Dalpoas y Shermock (2021), el análisis cualitativo de los patrones delictivos emergentes, acompañado de procedimientos éticos rigurosos que protegen los datos sensibles, es clave para generar conocimiento aplicable. Según Espinoza y Álvarez (2024), subrayan que el uso de herramientas forenses especializadas para el análisis de datos fortalece la capacidad institucional en la formulación de estrategias preventivas y reactivas ante amenazas digitales en constante evolución.

El diseño de la investigación fue descriptivo, como señala Reyes et al (2019). que en el estudio se deben considerar varios aspectos como la información previa, los diseños anteriores, la viabilidad de la investigación.

El enfoque fue mixto puesto que buscó identificar las características del fenómeno (Salazar, 2020), el enfoque cualitativo permite determinar la contextualización de casos de los ciberdelitos (Piña, 2023). Por su parte desde lo cuantitativo Jiménez et al. (2022) refieren que el enfoque cuantitativo establece el número de casos reportados sobre ciberdelitos, identificando plenamente las múltiples acciones presentes en las diferentes plataformas de videojuegos y metaverso ocurridas en los últimos tres años. El método aplicado fue deductivo para comprender los designios del fenómeno respaldados por leyes y teorías científicas (Sánchez, 2019) a través de la lógica pura, la conclusión a partir de ciertas premisas, asegurando así la veracidad de las conclusiones, estableciendo desde lo lógico conceptos apropiados (Reyes y Boente., 2019). La modalidad fue documental y de Campo: puesto que se centró en constatar información relacionada con delitos informáticos relacionados con videojuegos y metaversos (González, 2020) a partir de estudios realizados que pueden llegar a corroborar situaciones y generar nuevos conceptos, de documentos relacionados con investigaciones de ciberdelitos en videojuegos y metaversos, en los que se pudieron concretar datos primarios y secundarios provenientes de investigaciones (Arias, 2023).

La población de estudio se refirió al conjunto de documentos relacionados con ciberdelitos en videojuegos y metaverso de los últimos tres años, de la forma como operan los ciberdelincuentes, la modalidad y los medios electrónicos que utilizan; (Robles, 2019), de otro lado, a una muestra de la población de jugadores de videojuegos y metaverso que han sido objeto o víctimas de delitos cibernéticos y un personal integrantes de la Policía nacional de salas de recepción de denuncias y atención de casos de ciberdelitos. con una totalidad de población de 6577 personas que equivale al 100% de la población de estudio de tipo finito, de los cuales se tomó la muestra.

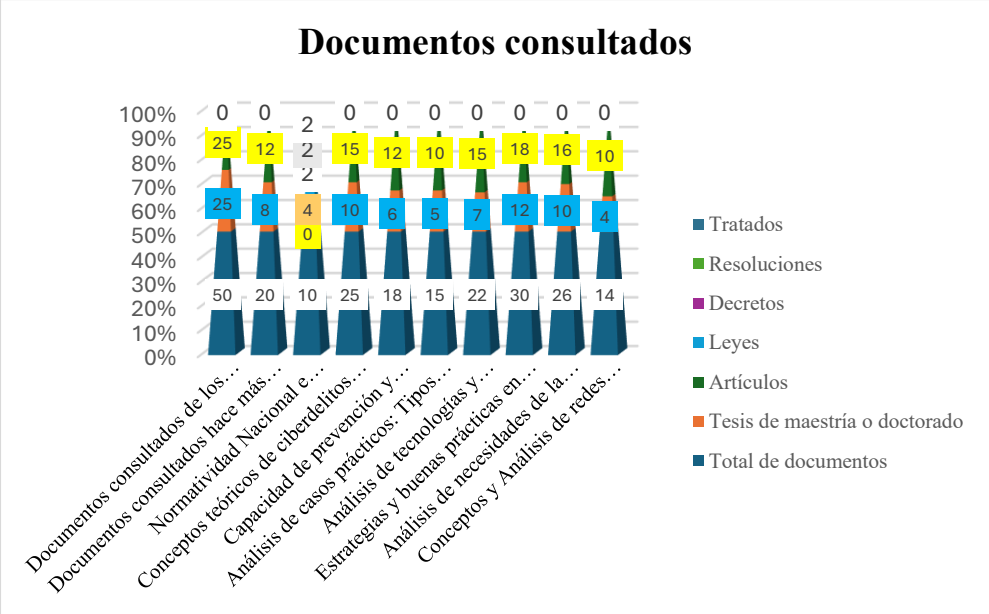
En esta investigación, se llevó a cabo un estudio con una muestra de 363 jugadores de videojuegos y de metaverso, residentes en Bogotá y con edades que oscilan entre los 18 y 40 años. Para calcular la muestra, se tuvo en cuenta un nivel de confianza del 95% y un margen de error del 5%, lo que permitió realizar un análisis adecuado de los datos obtenidos a través del instrumento seleccionado para el estudio. La fase de reclutamiento se ejecutó de acuerdo con las pautas de ética en pesquisa, lo que implicó que se recibiera una exposición clara al propósito del trabajo y formalizara su aprobación mediante un consentimiento informado.

Para el segmento compuesto por gamers y usuarios de entornos metaverso, se consideraron predominantemente la franja etaria, la identidad de género y el trasfondo personal frente a conductas delictivas en el ámbito digital.

RESULTADOS

En el contexto moderno y altamente digitalizado que hoy vivimos, arenas como los videojuegos y el metaverso han empezado a funcionar como verdaderos salones de crimen cibernético. Esa transformación obliga a las instituciones, y particularmente a la Policía Nacional encargada de la ciberseguridad, a actualizarse con rapidez y a pulir sus protocolos de respuesta (Policía Nacional, 2018). Para abordar el reto, esta investigación se cimentó en un repaso exhaustivo de artículos revisados por pares, normas vigentes y tesis de posgrado, esfuerzo que pretendió compilar un corpus teórico ajustado a los incidentes que brotan en esos mundos virtuales (Arias, 2023). La velocidad con que emergen tecnologías nuevas y variantes delictivas pide que los investigadores policiales piensen en soluciones frescas, de modo que puedan prevenir y controlar los delitos que surgen en fronteras digitales tan volátiles (Bentaouet, 2024). Solo así se protegerá a los ciudadanos en espacios que, día tras día, ganan protagonismo en nuestra vida cotidiana.

Figura 1 Documentos Consultados en la Investigación



Nota. Relación de los documentos consultados, concernientes con el estudio, artículos, normas, tesis de maestría y doctorado, fuente bases de datos

Análisis

Para llevar a cabo esta indagación se fundamentó en una exploración exhaustiva de literatura previa, marcos teóricos y disposiciones normativas relacionadas con los ciberdelitos que surgen en entornos de videojuegos y en el metaverso. Se recopilaron algo más de 200 referencias, entre las cuales figuran 93 tesis de posgrado, 107 artículos revisados por pares y un conjunto de diez textos normativos, dentro de ellos, leyes, decretos y resoluciones tanto nacionales como internacionales. La pesquisa examinó conceptos definitorios, clasificaciones de ilícitos digitales, herramientas de detección y prevención, casos emblemáticos, tecnologías emergentes, respuestas institucionales y el papel mediador de las plataformas sociales, en un esfuerzo por construir una base documental contemporánea y rigurosa que sostenga el estudio.

Una revisión minuciosa de la normativa vigente muestra que la respuesta institucional al cibercrimen ha estado prácticamente encerrada en un laberinto de sanciones y decretos. En su pesquisa más reciente, Khan (2024) observa que se suele promulgar legislación nueva sin siquiera asomarse a los fundamentos de la ciberseguridad. Ese apresuramiento legislativo refleja una mirada simplista, pues omite la prevención, ignora la alfabetización digital y pasa por alto la defensa de los derechos humanos en el espacio virtual.

Dicha perspectiva reaccional resulta endeble ante las dinámicas complejas que emergen en entornos como los videojuegos o el metaverso, donde el delito no es solo una infracción, sino también una manifestación de redes sociales, culturas y tecnologías entrelazadas, coincidiendo con el estudio de Mendiola (2022), en su investigación sobre el metaverso, apuntó precisamente a ese fenómeno al describirlo como una nueva puerta hacia la educación digital, Serna (2024) sobre los retos jurídicos del metaverso y Monzón (2022) acerca de narrativas que buscan fomentar comportamientos sostenibles dentro de la industria de los videojuegos. Así mismo se logró identificar confusión entre ciberseguridad y ciberdelitos, además una débil interacción entre normativas internacionales como el Convenio de Budapest y las leyes nacionales, estas debilidades limitan la capacidad del Estado para responder de manera efectiva y garantista a estas amenazas emergentes como menciona Mohamed (2024) en su investigación en ciberespacio, metaverso y nuevos delitos que gravitan sobre los derechos humanos y Martínez (2024) metaverso, amenazas internacionales y cooperación en la digitalización

Así pues, las investigaciones y los modelos de gestión que se ha revisado revelan serias limitaciones en las capacidades de las instituciones, tanto del sector público como del privado, para enfrentar los riesgos digitales cómo lo menciona estudios de Carlen (2023) derecho penal y metaverso en Argentina, Alcalá (2024) desafíos en México sobre la regulación de los ciberdelitos. De otro lado, en áreas como la educación en línea y el trabajo remoto, las instituciones han mostrado una notable vulnerabilidad ante las amenazas cibernéticas, principalmente por la falta de políticas robustas, protocolos de respuesta y formación en habilidades digitales como refiere Margaico et al. (2024) problemática de videojuegos y agresividad en estudiantes de secundaria de instituciones educativas del distrito de Puente Piedra y Marquez et al. (2024) regulación de los ciberdelitos en el Convenio de Budapest, aspectos normativos y desafíos a partir de la Comparación entre Colombia y Alemania.

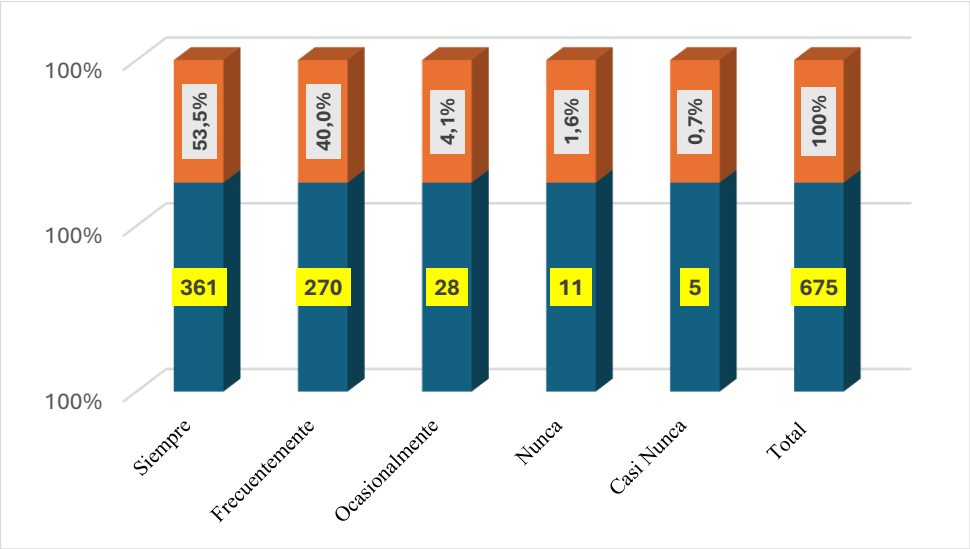
Aunque ha habido algunos avances en los marcos de gestión propuestos por el CSIRT y los Gobiernos, la inversión en infraestructura tecnológica sigue siendo baja, la cultura de reporte de incidentes es limitada y los líderes institucionales aún no asumen plenamente el riesgo digital. Esta situación resalta la necesidad urgente de un enfoque integral y conectado que reconozca la complejidad, la naturaleza de cambio y las relaciones de los ciberdelitos, especialmente en plataformas inmersivas como los videojuegos y el metaverso, tal como insinúa Malo et al.(2024) en la regulación jurídica del ciberdelito del carding a través del derecho, y Siqi et al. (2024) en su investigación, perpetración de ciberacoso en las redes sociales, demostrando los estudios que la ciudadanía aún carece de mecanismos claros para la protección, orientación y denuncia de los ciberdelincuentes

Resultados de la encuesta

Los hallazgos de la encuesta sobre ciberdelitos en videojuegos y metaverso. Percepciones, impacto y vulnerabilidades revelan una creciente preocupación entre los usuarios acerca de la seguridad en los espacios virtuales. Un porcentaje considerable de los participantes indicó haber sido testigo o víctima de delitos como el robo de identidad, el acoso en línea y fraudes vinculados a criptomonedas. Asimismo, se detectó un limitado conocimiento sobre las medidas de ciberseguridad y los protocolos de protección en las plataformas de videojuegos y metaverso, lo que incrementa la exposición a estos riesgos. Estos hallazgos enfatizan la necesidad de mejorar la formación en temas digitales, implementar mecanismos de prevención más efectivos y promover la responsabilidad compartida entre desarrolladores,

autoridades y usuarios para enfrentar las amenazas que cada día aumentan considerablemente. Para ser más explícita la información, se consolidó el análisis de cada una de las preguntas, a partir de gráficas y análisis de cada ítem.

Figura 2 ¿Es Frecuente que los Ciberdelincuentes Utilicen Mensajes Engañosos para Obtener Información Personal a los Usuarios de Plataformas de Videojuegos y Metaverso?

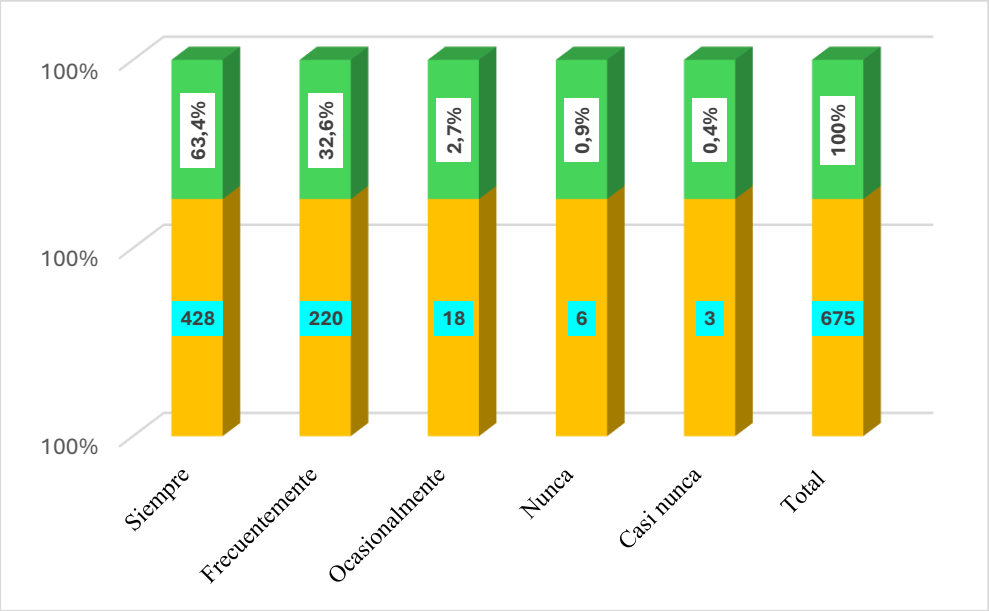


Nota. Descripción porcentual de las respuestas por los participantes, sobre la frecuencia que utilizan ciberdelincuentes para obtener información personal, análisis de datos SPSS.

Análisis

Del total de la población encuestada, relativo a la utilización de mensajes engañosos a los usuarios de videojuegos y metaverso para tener acceso a información personal. Se pudo determinar que, de acuerdo a las categorías de respuesta, el más alto fue en categoría Siempre con un 53,5%, Frecuentemente: 40,00%, Ocasionalmente: 41%, Nunca: 1,6% y Casi nunca: 0,7%. Es decir que la mayoría de los encuestados, el 93,48%, perciben que los ciberdelitos en videojuegos y metaverso ocurren siempre o frecuentemente y un 6,52% muy pocos creen que ocurren ocasionalmente o nunca, lo que significa que la mayoría de las veces los ciberdelincuentes están maquinando cómo crear mensajes para que las personas suministren información de sus actividades personales y laborales.

Figura 3 ¿Los Delincuentes Utilizan Medios como chat, Enlaces y Correos Engañosos entre Grupos en las Plataformas de Videojuego para Atraer a sus Víctimas?

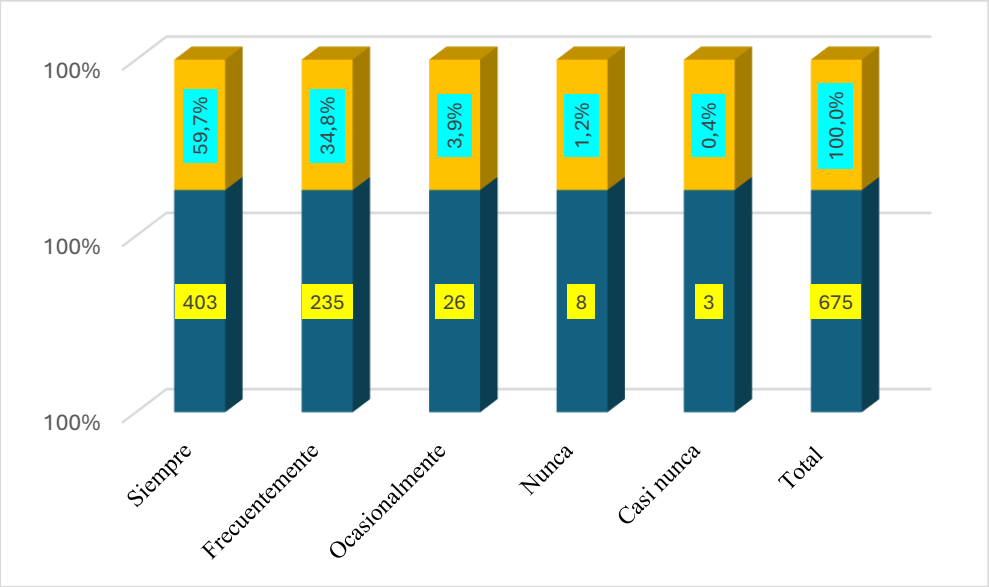


Nota. Descripción porcentual de las respuestas por los participantes, sobre los medios que utilizan los ciberdelincuentes como chat y enlaces de correos para obtener información personal, análisis de datos SPSS.

Análisis

En la segunda pregunta, se habla sobre la utilización de medios como chat, enlaces y correos engañosos entre grupos en las plataformas de videojuego como una forma de atracción a sus víctimas. Los encuestados respondieron con un número porcentual alto en la respuesta siempre con un 63,4%, frecuentemente: 32,6%, ocasionalmente: 2,7%, nunca: 0,9% y casi nunca: 0,4%. Esto quiere decir que hay un aumento en la percepción de siempre, frecuentemente y ocasionalmente con un 98,7% frente a la respuesta de nunca y casi nunca con un 2,3%. Es significativo que los ciberdelincuentes simples estén buscando la forma de interactuar con los usuarios para engañarlos de diversas formas y obtener información, llegando al punto de extorsionarlos.

Figura 4 ¿Cree que los Ciberdelincuentes Aprovechan Herramientas Tecnológicas Fraudulentas para Interactuar con Víctimas dentro de Plataformas de Videojuegos para Hurtar Información Personal?

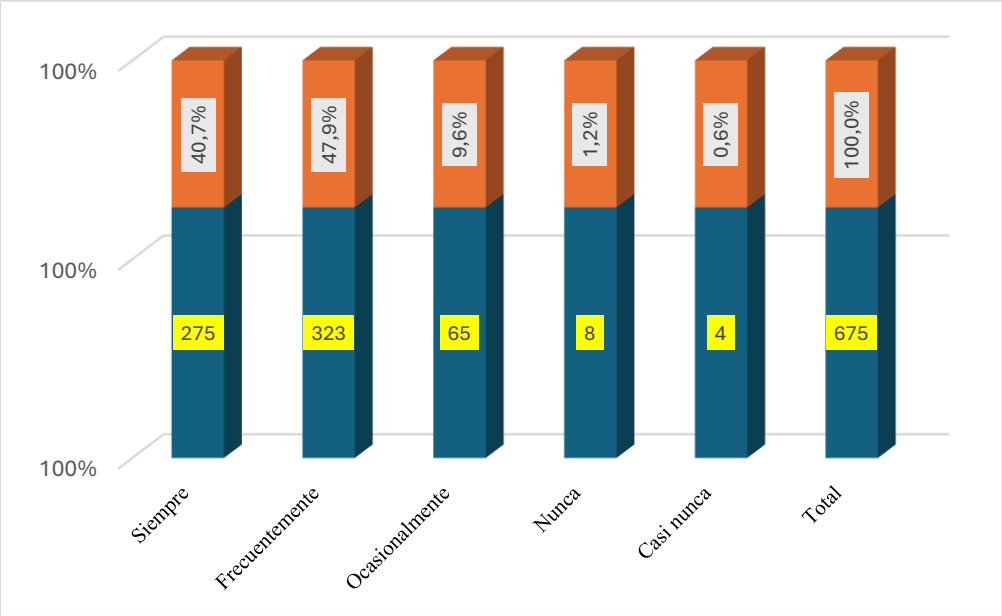


Nota. Descripción porcentual de las respuestas por los participantes, sobre el uso de herramientas tecnológicas fraudulentas que utilizan los ciberdelincuentes para interactuar con sus víctimas en videojuegos y metaverso, análisis de datos SPSS.

Análisis

La tercera pregunta está relacionada con el uso de herramientas tecnológicas fraudulentas para interactuar con víctimas dentro de las plataformas de videojuegos por los ciberdelincuentes para hurtarles su información personal. Se encontró resultados significativos como en la respuesta: Siempre: un 59,7%, Frecuentemente: 34,8%, Ocasionalmente: 3,9%, Nunca: 1,2%, Casi nunca: 0,4%. En esta pregunta se pudo analizar que en los primeros tres ítems de respuesta se describe un alto grado de opinión por los usuarios, puesto que se consolidó el 97.5%, de los cuales han conocido casos de ser víctimas de información fraudulenta por los ciberdelincuentes teniendo una relevancia mayor, respecto a las dos últimas respuestas, que tienen una representación del 3.5%, siendo una distribución muy baja. Es decir que, en las plataformas de videojuego y metaverso, los delincuentes han venido aumentando su accionar a través de datos fraudulentos para tener acceso a información de las diferentes actividades que los usuarios realizan, hurtándoles información personal, datos de actividades laborales y personales.

Figura 5 ¿El ciberacoso es uno de los delitos más recurrentes en las plataformas de videojuegos y metaverso?

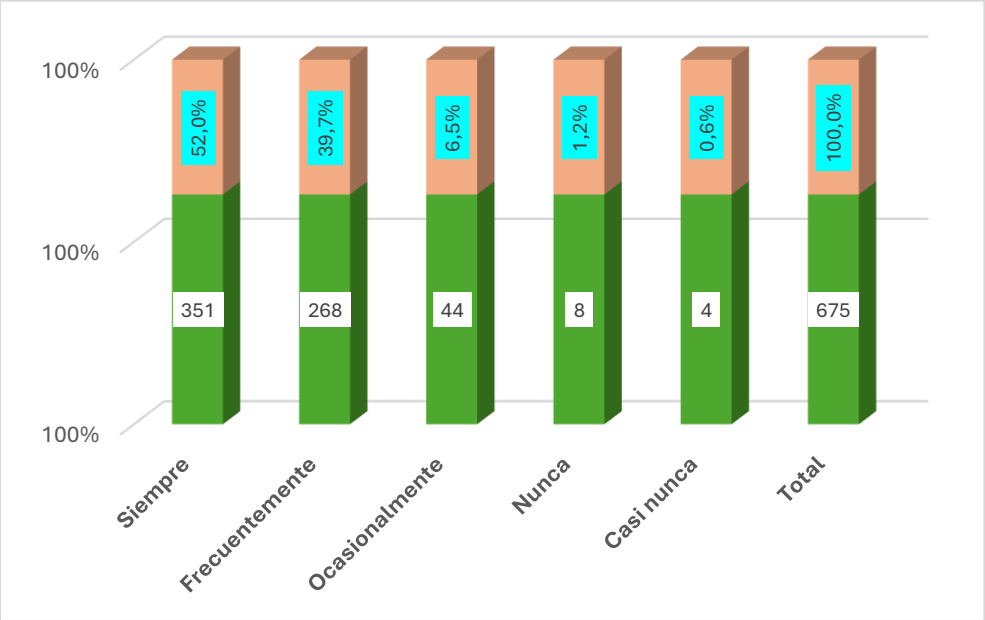


Nota. Descripción porcentual de las respuestas por los participantes, si el ciberacoso es uno de las modalidades más utilizados por los ciberdelincuentes a los usuarios de videojuegos y metaverso, análisis de datos SPSS.

Análisis

En relación a la pregunta si los usuarios de videojuegos y del metaverso han experimentado ciberacoso, los encuestados respondieron según el margen de respuesta, indicando que efectivamente han sido víctimas de ciberacoso en las siguientes proporciones: Frecuentemente 49,9%, Siempre 40,7%, Ocasionalmente 9,6%, Nunca 1,2%, Casi Nunca 0,6%. Con una significancia del 98,2%, se concluye que los usuarios de videojuegos y del metaverso han sufrido ciberacoso, lo que sugiere la necesidad de implementar medidas para combatir este delito, especialmente considerando que las respuestas de nunca y casi nunca son muy bajas, alcanzando solo un 1,8%. Desde esta perspectiva, es pertinente que las autoridades establezcan estrategias de control, en particular los equipos de respuesta a incidentes cibernéticos de la Policía Nacional.

Figura 6 ¿Cree que la Población Menor son las Principales Víctimas de Ciberacoso en estos Entornos de Videojuegos y Metaverso?

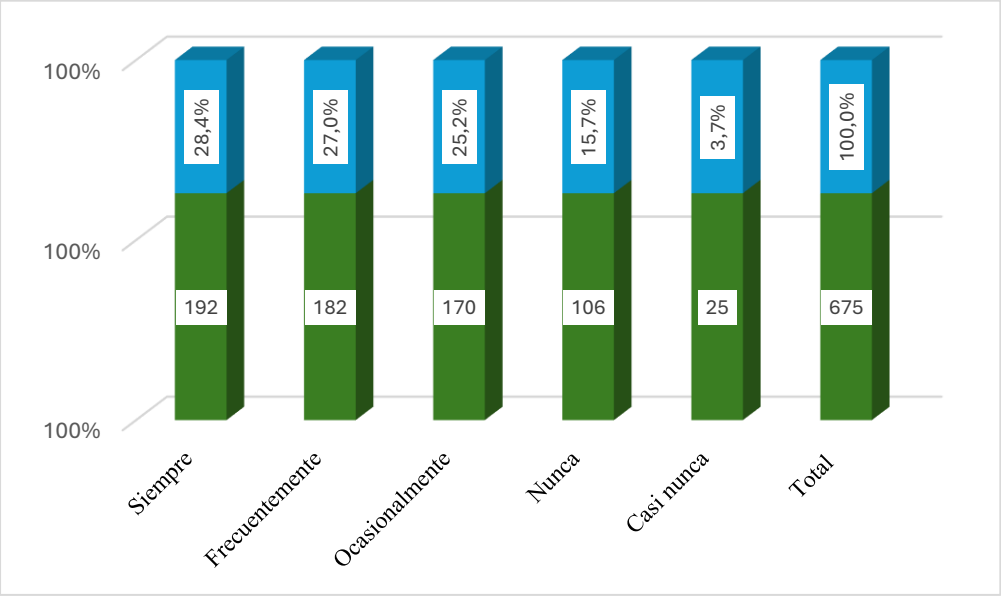


Nota. Descripción porcentual de las respuestas por los participantes, si la población menor asido víctimas del ciberacoso en los diferentes entornos de videojuegos y metaverso, análisis de datos SPSS.

Análisis

La mayoría de los encuestados (98,2%) afirmó que los menores han sido víctimas de acoso por ciberdelincuentes en videojuegos y el metaverso, con un 52% señalando que ocurre siempre y un 39,7% frecuentemente. Estos resultados evidencian una alta exposición de los menores al ciberacoso, lo que exige acciones urgentes por parte de autoridades, padres de familia y la Policía Nacional, incluyendo la creación de protocolos específicos para atender estos casos.

Figura 7 ¿Conoces o ha Identificado Escenarios de Fraude Relacionados con la Compra y Venta de Artículos o Monedas Virtuales Dentro de las Plataformas de Videojuegos y el Metaverso?



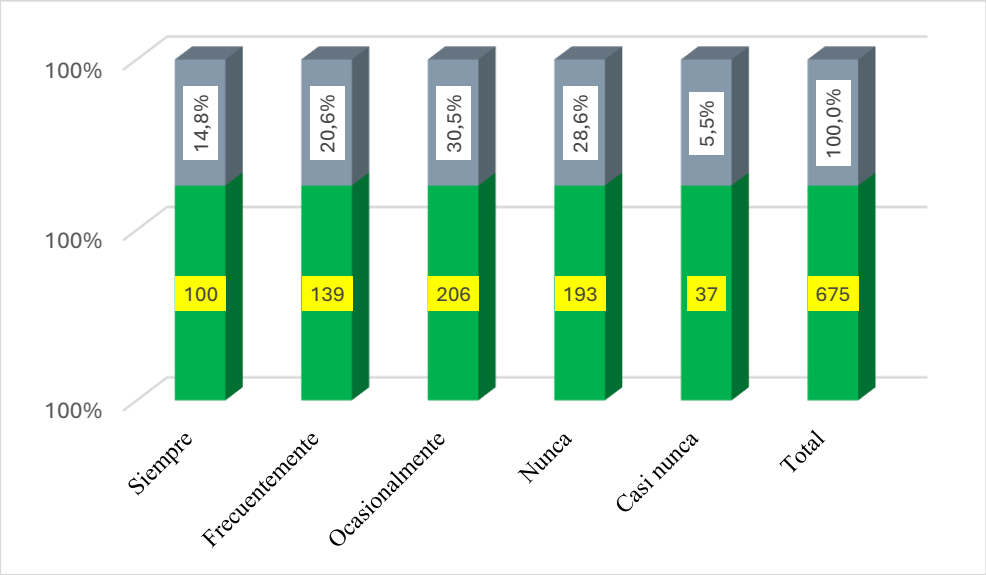
Nota. Descripción porcentual de las respuestas por los participantes, sobre escenarios fraudulentos en la utilización de monedas ofertadas en las plataformas de videojuegos y metaverso, análisis de datos SPSS.

Análisis

Cuando se les preguntó a los encuestados si en las plataformas de videojuegos y metaverso los ciberdelincuentes les han ofrecido artículos, elementos, negocios atractivos y la utilización de monedas con facilidad para obtener beneficios personales y económicos, de acuerdo al rango se logró obtener los siguientes resultados en la respuesta: Siempre se obtuvo un 28,4 %, Frecuentemente 27 %, Ocasionalmente 25,2 %, Nunca 15,7 % y Casi Nunca 3,7 %. Los resultados muestran que el 55,4% de los encuestados ha experimentado de manera constante o frecuente acercamientos sospechosos por parte de posibles ciberdelincuentes. Si se incluyen a quienes respondieron "ocasionalmente", el porcentaje asciende al 80,6%.

Esto pone de manifiesto una alta incidencia de exposición a actividades potencialmente delictivas en entornos digitales recreativos. En comparación, el 19,4% de los participantes indicó no haber tenido contacto o haberlo tenido en muy pocas ocasiones. Los hallazgos permiten determinar que las plataformas de videojuegos y metaverso constituyen entornos de riesgo considerable por los ciberdelincuentes, dado el contexto de atracción y oportunidades para atraer a sus víctimas, especialmente a través de ofertas que parecen inofensivas o atractivas para los usuarios.

Figura 8 ¿Ha sido Testigo o Conoce Casos de Afectaciones Psicológicas y Emocionales como Consecuencia del Ciberacoso en Videojuegos o Redes Sociales Dentro del Metaverso?

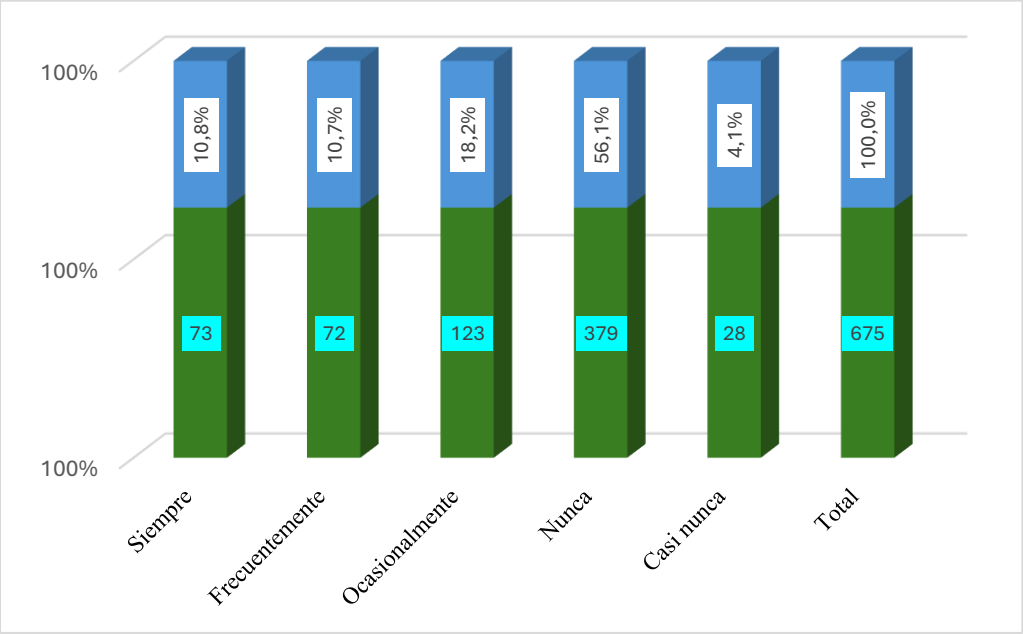


Nota. Descripción porcentual de las respuestas por los participantes, sobre testigo o si ha conocido casos de afectaciones psicológicas y emocionales por ciberacoso en las plataformas de videojuegos y metaverso, análisis de datos SPSS.

En el análisis frente a la pregunta sobre si han sido testigos o conocen casos de afectaciones psicológicas y emocionales derivadas del ciberacoso en videojuegos o redes sociales dentro del metaverso revela una tendencia significativa de exposición y conocimiento de ese tipo de situaciones. El grupo más numeroso fue el de quienes respondieron Ocasionalmente, representado en un 30,5% seguido por Nunca con un 28,6%, Frecuentemente con 20,6% y un 14,8% indicó que Siempre ha conocido o presenciado estos casos mientras que solo un 5,5% señaló Casi nunca.

Los resultados muestran que un 66% del total ha tenido contacto; ocasional, frecuente y constantemente en situaciones de ciberacoso en entornos digitales, lo cual pone de manifiesto que esta problemática genera problemas Psicológicos, comportamientos sociales y de salud significativos a los usuarios. Por otro lado, solo el 34,1% de las respuestas Nunca y Casi Nunca, no han tenido experiencia directa o indirecta con estos casos, lo que indica que un numero representativo de la población tiene percepción o conocimiento del daño emocional que este fenómeno puede causar. Los hallazgos representan la urgencia de establecer medidas preventivas más efectivas, tales como programas de concienciación sobre los efectos del ciberacoso por la Policía Nacional, protocolos de respuesta en las plataformas digitales y atención especializada en salud mental para las víctimas. Por otro lado, los resultados pueden ser utilizados como fundamento para crear campañas educativas en entornos escolares y familiares.

Figura 9 ¿Ha Sufrido Consecuencias Económicas, como la Pérdida de Información Personal o Dinero, Debido a Ciberdelitos Cometidos en Plataformas de Videojuegos o el Metaverso?

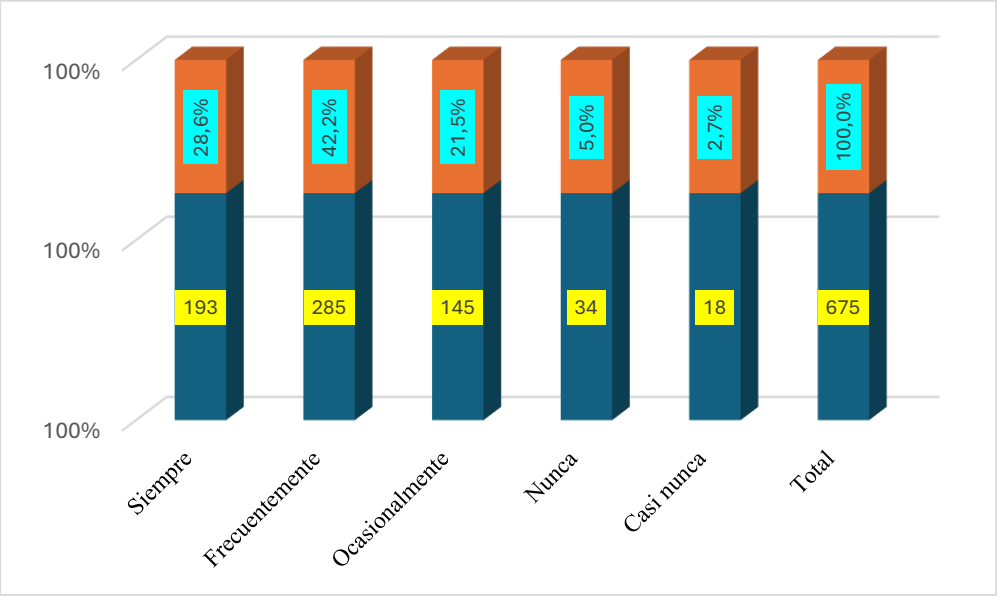


Nota. Descripción porcentual de las respuestas por los participantes, sobre consecuencias económicas, hurto de información y dinero a los usuarios de las plataformas de videojuegos y metaverso, análisis de datos SPSS.

Análisis

El 60,2% de los encuestados indicó no haber sufrido consecuencias económicas por ciberdelitos en videojuegos o el metaverso. No obstante, el 39,8% sí reportó haber sido víctima de pérdidas económicas o robo de datos personales. Estos resultados evidencian que los ciberdelincuentes están utilizando activamente estas plataformas para cometer fraudes, estafas y robos de identidad relacionados con monedas virtuales y datos sensibles.

Figura 10 ¿Percibe que las Plataformas de Videojuegos y Metaverso son más Vulnerables a Ataques Cibernéticos en comparación con otras Plataformas Digitales*?*

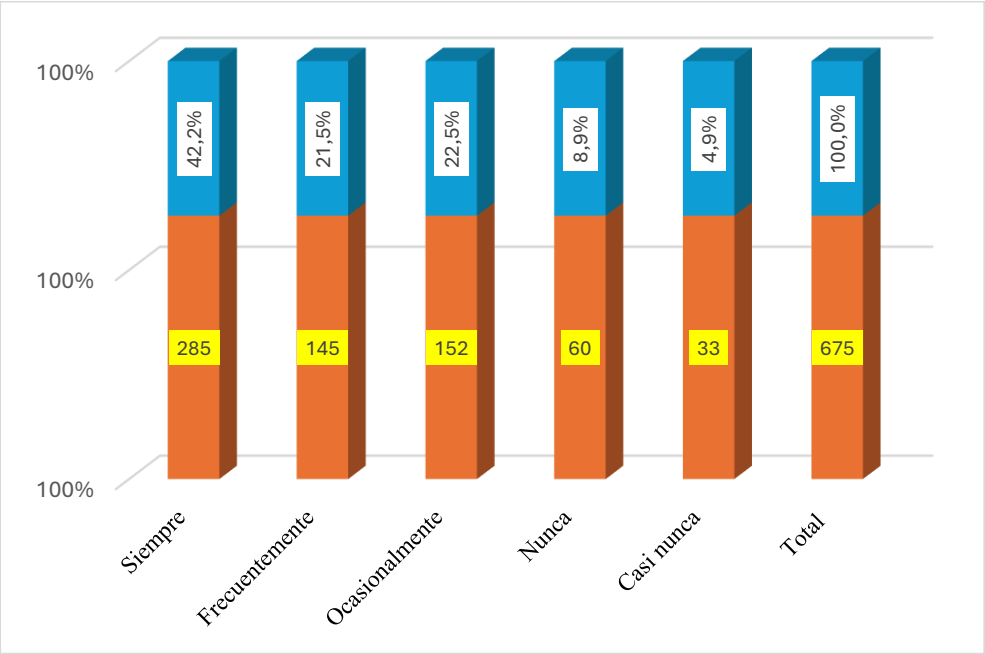


Nota. Descripción porcentual de las respuestas por los participantes, sobre la percepción de vulnerabilidad de los usuarios de las plataformas de videojuegos y metaverso frente a otras plataformas digitales, análisis de datos SPSS.

Análisis

Del total de las personas encuestadas, una clara mayoría manifestó percibir un mayor nivel de vulnerabilidad en las plataformas de videojuegos y metaverso frente a los ataques cibernéticos. De acuerdo a los resultados de las respuestas, el 42,2% respondió que frecuentemente perciben vulnerabilidad, seguido de un 28,6%, obteniendo un total de 70,8% de respuestas afirmativas de percepción constante o frecuente de riesgo, lo que evidencia un alto nivel de alerta o desconfianza por parte de los usuarios frente a estos entornos digitales. De otro lado, un 21,5% de los encuestados manifestó que ocasionalmente han detectado fallos de seguridad, lo que indica que, aunque no lo hagan de manera constante, han reconocido vulnerabilidades en algún momento. Solo el 7,7% en las respuestas Nunca o Casi Nunca consideraron que las plataformas son menos propensas a riesgos, es decir, que no han sido víctimas de los ciberdelincuentes. Sin embargo, los hallazgos reflejan una inquietud generalizada entre los usuarios sobre la seguridad en los entornos virtuales inmersivos. Dado que el metaverso y los videojuegos en línea manejan información delicada, como datos personales, interacciones en tiempo real, contenido generado por los usuarios y transacciones económicas que incluyen el uso de monedas virtuales, es comprensible que sean víctimas potenciales por parte de los ciberdelincuentes.

Figura 11 ¿Considera que los Miembros de la Policía Nacional Están Adecuadamente Capacitados y Cuentan con las Herramientas Necesarias para Enfrentar los Ciberdelitos en Plataformas de Videojuegos y el Metaverso?



Nota. Descripción porcentual de las respuestas por los participantes, sobre la percepción de los usuarios frente a la capacitación y uso de herramientas de los integrantes de la Policía Nacional para la prevención de ciberdelitos en las plataformas de videojuegos y metaverso, análisis de datos SPSS.

Análisis

De acuerdo a los resultados obtenidos de la encuesta, más del 63% de los encuestados en las respuestas, siempre y frecuentemente, consideran que los miembros de la Policía Nacional están capacitados y cuentan con herramientas y medios necesarios para enfrentar incidentes en ciberdelitos en entornos virtuales de videojuegos y el metaverso. Esto evidencia una percepción mayormente positiva de la preparación institucional frente a este tipo de fenómenos. Sin embargo, un 22,5% considera que ocasionalmente se cuenta con dicha preparación, lo que demuestra un bajo conocimiento y elementos para enfrentar la problemática al surgimiento de incidentes cibernéticos: nacional, departamental y localmente. No obstante, el 13,8% del total de respuestas Nunca y Casi Nunca expresaron desconfianza y escepticismo hacia la capacidad de respuesta de los investigadores de la Policía Nacional frente a los nuevos tipos de delito.

DISCUSIÓN DE RESULTADOS

Los hallazgos obtenidos en esta investigación permiten ser testigos de una realidad preocupante respecto a la escalada de los ciberdelitos en relación con los videojuegos y el metaverso, así como los límites estructurales, operacionales de la Policía Nacional frente al fenómeno. La revisión de documentos revela que la respuesta institucional a los ciberdelitos ha estado marcada por un enfoque que se centra principalmente en la penalización y la regulación. A menudo, se tiende a crear nuevas leyes sin tener una comprensión completa de la ciberseguridad como lo menciona Khan (2024) en su estudio reconceptualización de la actuación policial frente a la ciberdelincuencia. Esto refleja una visión simple del fenómeno, que pasa por alto aspectos cruciales como la prevención, la educación digital y la defensa de los derechos humanos en el entorno virtual.

Este enfoque es inadecuado frente a dinámicas más complejas, como las que se observan en los videojuegos y el metaverso, donde los delitos informáticos no son solo actos ilegales, sino también expresiones de relaciones sociales, culturales y tecnológicas que se desarrollan en el entorno digital, coincidiendo con el estudio de Mendiola (2022), el metaverso como una nueva puerta hacia la educación digital, Serna (2024) sobre los retos jurídicos del metaverso y Monzón (2022) acerca de narrativas que buscan fomentar comportamientos sostenibles dentro de la industria de los videojuegos. Así mismo se logró identificar confusión entre ciberseguridad y ciberdelitos, además una débil interacción entre normativas internacionales como el Convenio de Budapest y las leyes nacionales, estas debilidades limitan la capacidad del Estado para responder de manera efectiva a estas amenazas emergentes como menciona Mohamed (2024) en su investigación en ciberespacio, metaverso y nuevos delitos que gravitan sobre los derechos humanos y Martínez (2024) metaverso, amenazas internacionales y cooperación en la digitalización.

Así pues, las investigaciones y los modelos de gestión que se ha revisado revelan serias limitaciones en las capacidades de las instituciones, tanto del sector público como del privado, para enfrentar los riesgos digitales cómo lo menciona estudios de Carlen (2023) derecho penal y metaverso en Argentina, Alcalá (2024) desafíos en México sobre la regulación de los ciberdelitos. De otro lado, en áreas como la educación en línea y el trabajo remoto, las instituciones han mostrado una notable vulnerabilidad ante las amenazas cibernéticas, principalmente por la falta de políticas robustas, protocolos de respuesta y

formación en habilidades digitales como refiere Margaico et al. (2024) problemática de videojuegos y agresividad en estudiantes de secundaria de instituciones educativas del distrito de Puente Piedra, y Marquez et al. (2024) regulación de los ciberdelitos en el Convenio de Budapest, aspectos normativos y desafíos a partir de la Comparación entre Colombia y Alemania.

Cabe mencionar que ha habido algunos avances en los marcos de gestión propuestos por el CSIRT, pero la inversión en infraestructura tecnológica sigue siendo baja, la cultura de reporte de incidentes es limitada y los líderes institucionales aún no asumen plenamente el riesgo digital. Esta situación resalta la necesidad urgente de un enfoque integral y conectado que reconozca la complejidad, la naturaleza de cambio y las relaciones de los ciberdelitos, especialmente en plataformas inmersivas como los videojuegos y el metaverso, tal como insinúa Malo et al.(2024) en la regulación jurídica del ciberdelito del carding a través del derecho, y Siqi et al. (2024) en su investigación perpetración de ciberacoso en las redes sociales, demostrando los estudios que la ciudadanía aún carece de mecanismos claros para la protección, orientación y denuncia a los ciberdelincuentes.

En particular, la percepción del problema reportada por los encuestados muestra la alta exposición a riesgos digitales como la mensajería engañosa, el phishing, los protocolos de robo de información tecnológica y el ciberacoso desenfrenado, particularmente a los usuarios y menores de edad en contraste con el estudio de Mayorga y Holguín (2024). Esta tendencia es consistente con estudios previos y teorías contemporáneas sobre la evolución del cibercrimen que indican técnicas sofisticadas empleadas por los criminales y la facilidad con la que operan en el espacio virtual.

De otro lado, más del 90% de los encuestados cree que los delitos cibernéticos ocurren con mucha frecuencia, lo que muestra una preocupación colectiva a los usuarios con respecto a ese tipo de amenazas, como lo describe en su estudio (Acevedo, 2023). Esto se vuelve más grave al considerar que cerca del 98% de los participantes identifican el ciberacoso como una experiencia común y normal de la cotidianidad, pero lo más preocupantes es un alto porcentaje en el que demuestra que la mayoría de los jóvenes menores de edad frecuentemente se convierten en víctimas, lo que presenta un desafío urgente en términos de protección de derechos y prevención del ciberdelito. Esto no solo confirma la existencia de tales problemas, sino que también nos permite vislumbrar el impacto psicológico, social

y económico que estos crímenes tienen en casos donde se reportan pérdidas financieras o se sufren emocionalmente como lo determina en estudios realizados por (Khan, 2024 y Guerrero, 2022)

En esta línea, la interpretación de los datos de información sugiere que, aunque los ciudadanos reconocen la existencia de amenazas latentes en estos entornos virtuales, todavía hay una mezcla de confianza y desconfianza sobre las capacidades institucionales de la Policía Nacional. Sin embargo, el 63% de los encuestados cree que hay una preparación adecuada para enfrentar estos desafíos, pero también preocupa dado que el 36% profesa desconocimiento o escepticismo, ilustrando las brechas en el conocimiento y la necesidad de fortalecer las competencias mediante capacitaciones en torno al fenómeno delincuencial digital y la comunicación institucional como marcos de respuesta a la gestión de incidentes cibernéticos.

Así mismo, los hallazgos coinciden con lo planteado por estudios analizados durante el proceso investigativo de (González 2023) en el que aborda estrategia para contrarrestar figuras delictivas de tipo digital. Lo que demuestra el estudio como una urgencia de una transformación institucional orientada hacia la ciberseguridad especializada. A pesar de los esfuerzos existentes, aún es limitada la integración de protocolos de atención específicos para el metaverso y los videojuegos en los procedimientos, lo cual reduce la eficacia de la acción policial y la confianza ciudadana.

Desde otra óptica, el enfoque teórico basado en los resultados, valida la necesidad de aplicar enfoques multidisciplinarios e innovadores, que contemplen no solo la actualización tecnológica, sino también el desarrollo de habilidades investigativas adaptadas a los nuevos escenarios digitales como menciona Khan (2024) en su estudio sobre analizar los desafíos que enfrentan las agencias policiales para abordar los crecientes ciberdelitos. Del mismo modo, se ratifica la conveniencia y el papel activo que deben tener los usuarios, desarrolladores y reguladores en la configuración de un ecosistema de medios tecnológicos con estrategias de socialización y comprensión por las comunidades para contribuir a la prevención de los delitos cibernéticos lo cual contrasta con la investigación realizada por Bautista (2022) en su trabajo titulado Incidencia de un ambiente de aprendizaje basado en la metodología del ABP y apoyado en TIC en el desarrollo de la competencia matemática de resolución de problemas.

Finalmente, la evidencia recopilada respalda que el fenómeno de los ciberdelitos en ambientes de videojuegos y metaverso constituyen un desafío para la institución, en prevención y demanda a respuestas sólidas con la colaboración internacional, a través de estrategias en prevención y disuasión de los delitos cibernéticos. La Policía Nacional tiene que fortalecer su rol como actor fundamental en la protección de los derechos fundamentales, no solo mediante su capacidad de acción, sino también a través de la actualización de sus procesos y procedimientos específicamente en términos de ciberdelitos en videojuegos y metaverso para corresponder a la edificación de confianza y legitimidad de los ciudadanos cada vez más vulnerables por los ciberdelincuentes.

La triangulación entre el análisis de documentos y los resultados de la encuesta nos permite identificar un desfase crítico entre las normativas institucionales y la realidad operativa frente a los ciberdelitos en entornos digitales, como los videojuegos y el metaverso. Los estudios revisados, como los de Khan (2024), Mohamed (2024) y Martínez (2024), indican que la respuesta del estado sigue centrada en un enfoque penal y normativo que no se ha línea con las complejidades tecnológicas actuales. Los datos muestran que los ciudadanos, especialmente los menores, están muy expuestos a amenazas como el ciberacoso, el phishing y el robo de datos, a menudo sin una protección efectiva por parte de las autoridades (Acevedo, 2023; Mayorga y Holguín, 2024).

Esta brecha se agrava aún más por la escasa inversión institucional en formación, infraestructura y herramientas tecnológicas de ultima generación, como menciona Malo et al. (2024) y Siqi et al. (2024) reflejándose en la percepción del ciudadano, determinando que el 63% confía en la preparación policial, un 36% expresa desconfianza o falta de conocimiento, lo que pone de manifiesto fallos en la comunicación y en la capacidad operativa. Autores como Mendiola (2022), Serna (2024) y Monzón (2022) destacan que estos delitos surgen en contextos culturales y relacionales del entorno virtual, y no pueden abordarse con enfoques tradicionales.

Por lo tanto, la convergencia de fuentes confirma que tanto la acción estatal como la institucionalidad policial necesitan una transformación urgente hacia un enfoque integral, preventivo y multidisciplinario, que articule cooperación internacional, tecnología actualizada y participación activa de la ciudadanía, tal como exige la complejidad de los delitos en el ciberespacio.

Con base en los resultados obtenidos, se prevé la elaboración de la propuesta para la actualización e inmersión de la guía de procedimientos de investigación judicial, con el objetivo de controlar y prevenir la proliferación de delitos cibernéticos en las plataformas de videojuegos y en el metaverso.

CONCLUSIONES

A través de un análisis exhaustivo de fuentes académicas, normativas y los resultados obtenidos de encuestas, se ha identificado la necesidad urgente de reforzar el proceso de gestión de incidentes cibernéticos mediante la implementación de protocolos específicos, herramientas tecnológicas avanzadas y estrategias de prevención adaptadas a las dinámicas particulares de estos entornos virtuales.

Se determinó que los delitos más comunes en los videojuegos y el metaverso abarcan el robo de identidad, el ciberacoso particularmente hacia los menores de edad, la extorsión y los fraudes relacionados con criptomonedas. Estas formas delictivas se distinguen por su habilidad para adaptarse a las interacciones digitales y por el uso de métodos engañosos como chats, enlaces y plataformas inmersivas, lo que resalta la necesidad de que las autoridades actúen más a fondo estos fenómenos.

Los datos recopilados señalaron que, a pesar de que hay una percepción en parte favorable sobre la capacidad de la Policía Nacional para enfrentar los ciberdelitos, continúa existiendo una considerable deficiencia en herramientas tecnológicas, formación especializada y protocolos definidos para intervenir en espacios como videojuegos y el metaverso

La ausencia de protocolos concretos para la gestión de incidentes en entornos virtuales inmersivos restringe la eficacia de la respuesta institucional. La investigación respaldó la propuesta de modernizar los procedimientos vigentes, integrando modelos de análisis de riesgos, metodologías forenses digitales, sistemas de alerta temprana y rutas de atención diferenciadas, especialmente para situaciones que involucren a menores o delitos con un impacto emocional considerable.

REFERENCIAS BIBLIOGRAFICAS

Acevedo Alemán, J. (2023). El metaverso: Los nuevos entendimientos del Trabajo Social en una era transhumanista. Margen: *revista de trabajo social y ciencias sociales,* 110, 3.

Acosta, M. G., Benavides, M. M., & García, N. P. (2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. *Revista Venezolana de Gerencia*, vol. 25, núm. 89. https://www.redalyc.org/journal/290/29062641023/html/

Andrew, Z., & Healy, A. M. (2012). Libros de Gerencia Resumidos Resiliencia. *Libros de gerencia*. https://www.amazon.com/-/es/Andrew-Zolli-Ann-Marie-Healy/dp/0755360338

Arias, F. G. (2023). Investigación documental, investigación bibliométrica y revisiones sistemáticas. *Revista deposito legal IPP* vol. 31, nim 32, 1-20. file:///C:/Users/LENOVO/Downloads/Dialnet-InvestigacionDocumentalInvestigacionBibliometricaY-9489470%20(1).pdf

Arteaga, C. D. (2023). Ciberdelincuencia, a propósito del derecho penal informático en Colombia. *Revista de Estudios Socio-territoriales, 13(1), 38-47*. doi: https://doi.org/10.15332/27113833.8322

Bautista Triana, D. J., & Sandoval Silva, R. A. (2022). *Incidencia de un ambiente de aprendizaje basado en la metodología del ABP y apoyado en TIC en el desarrollo de la competencia matemática de resolución de problema*s. http://hdl.handle.net/1992/59003.

Bentaouet, Mohamed Saad. 2024. "VERDUGO GUZMÁN, Silvia Irene: Ciberespacio, metaverso y nuevos delitos que gravitan sobre los derechos humanos. *Tirant lo Blanch, Valencia, 2023,* 200 pp. 978-84-1169-779-8". IUS ET SCIENTIA 10(1):182–85.

Bentaouet, Mohamed Saad. (2024). "VERDUGO GUZMÁN, Silvia Irene: Ciberespacio, metaverso y nuevos delitos que gravitan sobre los derechos humanos. *Tirant lo Blanch, Valencia,* 2023, 200 pp. ISBN: 978-84-1169-779-8". IUS ET SCIENTIA 10(1):182–85.

Campos Varela, Estefanía. 2024. "*Análisis de la Privacidad y Seguridad en las Redes Sociales en un Mundo de Ciberdelitos"*.

Campos Varela, Estefanía. 2024. "*Análisis de la Privacidad y Seguridad en las Redes Sociales en un Mundo de Ciberdelito*s".

Carlen, Santiago. 2023. "Derecho penal y metaverso en Argentina: propuestas para abordar posibles conflictos". Ratio Iuris. *Revista de Derecho Privado,* 11(1), 209-301 (2023).

Carlen, Santiago. 2023. "Derecho penal y metaverso en Argentina: propuestas para abordar posibles conflictos". Ratio Iuris. *Revista de Derecho Privado*, 11(1), 209-301 (2023).

Castillo Torres, María Carolina. 2024. "*Investigación de ciberdelitos como medio de tutela judicial efectiva"*.

Chen, C., Peersman, C., Edwards, M., Ursani, Z., & Rashid, A. (2021). A Framework for Understanding Cybercriminal Roles in Darknet Markets. *Magazine, PWG Symposium on Electronic Crime Research* (eCrime), 1-12. https://ieeexplore.ieee.org/document/9671906/citations#citations

Chen, C., Peersman, C., Edwards, M., Ursani, Z., & Rashid, A. (2021). A Framework for Understanding Cybercriminal Roles in Darknet Markets. *Magazine, PWG Symposium on Electronic Crime Research* (eCrime), 1-12. Obtenido de https://ieeexplore.ieee.org/document/9671906/citations#citations

Chicharro, Mar, Fátima Gil-Gascón, Salvador Gómez-García, Mar Chicharro, Fátima Gil-Gascón, y Salvador Gómez-García. 2024. "*Jóvenes, videojuegos y ocio digital. Consumos, usos y significados". Comunicación y medios* 33(49):15–25. doi: 10.5354/0719-1529.2024.74945.

Corcoran, Lucie. 2024. "Cyberbullying: A New Dimension to an Old Problem". thesis, Institute of Art, Design + Technology.

Cuellar Quintero, Valeria, y Paula Andrea Astaiza Morales. 2024. "*Análisis dogmático de los delitos informáticos o ciberdelitos en Colombia"*.

Dalpoas, S. E., & Sherlock, K. (2021). *American Journal of Health-System Pharmacy,* Volume 78, Number 22, 233-239. doi:10.1093/ajhp/zxab232

Espinoza, E. A., & Álvarez, M. S. (2024). Análisis de técnicas y herramientas forenses para la investigación de delitos informáticos y su perspectiva legal en Ecuador. *Revista digital Publisher* Vol 9-Num 6, 644-652. doi: doi.org/10.33386/593dp.2024.6.2775

García T, M. 2024. "Ciberseguridad vs ciberdelincuencia: obstáculos procesales en la persecución de la ciberdelincuencia organizada. *Propuestas para una más eficaz represión de los ciberdelitos". Ciencia Policial* 182:15–69. doi: 10.14201/cp.31962.

Georgina Alcalá Casillas, Miryam. (2024). "Desafíos en México sobre la regulación de los ciberdelitos". Derecom: *Revista Internacional de Derecho de la Comunicación y las Nuevas Tecnologías* (35):4.

González, G. (2022). Gerencia de la investigación y del conocimiento en las universidades colombianas: Algunas reflexiones. *Revista de Ciencias Sociales (Ve), vol. XXVIII*, núm. 1, 2022, 187-193. https://www.redalyc.org/journal/280/28069961014/28069961014.pdf

González, L. M., & Gómez, C. (2024). Investigación mixta: ¿qué es y qué no? Metodología Mixta de Investigación: ¿Qué es y qué no es? *Revista Colombiana de Psiquiatría.* https://www.sciencedirect.com/science/article/abs/pii/S0034745024000362

González-Tapia, María Isabel. 2023. "Virtual Emotions and Criminal Law". *Frontiers in Psychology* 14. doi: 10.3389/fpsyg.2023.1260425.

Gordon, L., Loeb, M., & Zhou, L. (2016). Teoría de la Gestión del Riesgo Cibernético. *Revista de Seguridad de la Información*, Vol.07 No.02, 1-11. Obtenido de https://www.scirp.org/html/3-7800345_64892.htm

Guerrero Herrera, L. H. (2022). Los criptoactivos y su influencia en el metaverso. *Informática y Derecho: Revista Iberoamericana de Derecho Informático* (segunda época), 12, 55–64.

Herhuay Margaico, Alexander Emanuel, y Daniela Alejandra Salazar Gongora. 2024. "*Uso problemático de videojuegos y agresividad en estudiantes de secundaria de instituciones educativas del distrito de Puente Piedra, 2024*". Repositorio Institucional - UCV.

Hernández, O. (2020). *Seguirdad Digital Conceptos y Herramientas Basicas. Datos Bajo Llave*. https://conexo.org/wp-content/uploads/2020/06/Seguridad-Digital-Conceptos-y-Herramientas-B%C3%A1sicas-Mayo-2020.pdf

Hernández, O. (2021). Aproximación a los distintos tipos de muestra no probabilístico. *Revista Cubana de Medicina General Integral*. 2021;37(3), 1-7. http://scielo.sld.cu/pdf/mgi/v37n3/1561-3038-mgi-37-03-e1442.pdf

Hernández, S. L., & Ávila, D. D. (2020). Hipótesis de Investigación. *Revista Boletín Científico de las Ciencias Económico Administrativas del ICEA*, Vol. 8, No. 16, 42-43. O https://repository.uaeh.edu.mx/revistas/index.php/icea/issue/archive

Hu, Siqi, Wenjing Lei, Hong Zhu, y Carol Hsu. 2024. "Cyberbullying perpetration on social media: A situational action perspective". *Information & Management* 61(6):104013. doi: 10.1016/j.im.2024.104013.

Jiménez, J. A., Contreras, I., & López, M. (2022). Lo cuantitativo y cualitativo como sustento metodológico en la investigación educativa: un análisis epistemológico. *Revista*

Humanidades, vol. 12, núm. 2, 1.15. Obtenido de https://www.redalyc.org/journal/4980/498070446014/498070446014.pdf

Khan, A. A. (2024). Reconceptualizing Policing for Cybercrime: *Perspectives from Singapore. Laws, 13(4),* Article 4. https://doi.org/10.3390/laws13040044

Legidos Masi, Valery. (2024). "*El papel de la Inteligencia Artificial en la prevención y lucha contra los ciberdelitos*".

López, J. A. (2021). Libro de la soberania digital. *Libros.uua.max, catalogo editorial*. O https://libros.uaa.mx/index.php/uaa/catalog/book/92

M'Cready Sykes, G., & Matza, D. (2008). Técnicas de neutralización, *una teoría de la delincuencia*. Caderno CRH, vol. 21, núm. 52, 163-171. https://www.redalyc.org/pdf/3476/347632174012.pdf

Malo Amancha, Ronald Joshua, y Cristhian Alexander Robalino Pailiacho. 2024. "*La regulación jurídica del ciberdelito del carding a través del derecho comparado"*. bachelorThesis, Universidad Nacional de Chimborazo, Riobamba, Ecuador.

Manterola, C., Quiroz, G., Salazar, P., & García, N. (2019). Metodología de los tipos ydiseños de estudio más frecuentemente utilizados en investigación clínica. *Revista Médica Clínica Las Condes Volumen 30, número* 1, 36-49. Obtenido de https://www.sciencedirect.com/science/article/pii/S0716864019300057

Marquez Guerra, José Francisco, y G. Barrios. 2024. "Regulación de los Ciberdelitos en El Convenio de Budapest: *Aspectos Normativos y Desafíos de Cooperación Internacional a partir de la Comparación entre Colombia Y Alemania*". 978-3-945294-56-7.

Martínez, D. (2019). Expertos en engañar a los ciberdelincuentes. *revista emprendedores: las claves de la economía y el éxito profesional,* Nº. 266, 40- 47. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=7133032

Martínez, José Antonio Moya. 2024. "Metaverso: amenazas internacionales y cooperación en la digitalización". Barataria. *Revista Castellano-Manchega de Ciencias Sociales* (35):15–27. doi: 10.20932/Barataria. v0i35.687.

Mayorga-Sandoval, J., & Holguín-Ordoñez, R. (2024). las redes sociales como instrumento del terrorismo en el Ecuador. *Revista de la Academia del Guerra del Ejército Ecuatoriano*, 17(01), Article 01. https://doi.org/10.24133/AGE.VOL17.N01.2024.0

Mendiola, M. S. (2022). El metaverso: ¿la puerta a una nueva era de educación digital? *Investigación en Educación Médica*, 11(42), Article 42. https://doi.org/10.22201/fm.20075057e.2022.42.22436

Mohamed Saad. 2024. "Verdugo Guzmán, Silvia Irene: Ciberespacio, metaverso y nuevos delitos que gravitan sobre los derechos humanos. *Tirant lo Blanch, Valencia*, 2023, 200 pp. ISBN: 978-84-1169-779-8". IUS ET SCIENTIA 10(1):182–85.

Monzón, E. (2022). Las narrativas orientadas a generar comportamientos sostenibles dentro de la industria de los videojuegos y su incidencia en el activismo social. *Revista Cuadernos Del Centro De Estudios De Diseño Y Comunicación*, (158), 13-22. doi: https://doi.org/10.18682/cdc.vi158.6962

Morillo, S., & Howard, C. (2017). Conducta antisocial adolescente bajo un enfoque integrador de tres teorías criminológicas. *Revista de Ciencias Sociales (Ve), vol*. XXIII, núm. 3, 77-88. https://www.redalyc.org/pdf/280/28056735007.pdf

Peñuela, L. C. (2023). Ciberseguridad: el peligro al acecho de los niños, niñas y adolescentes. *Revista Iberoamericana de Derecho Informático vol ,13, 15-27*. https://revistas.fcu.edu.uy/index.php/informaticayderecho/article/view/3995

Piña, L. S. (2023). El enfoque cualitativo: Una alternativa compleja dentro del mundo de la investigación. *Revista Arbitrada Interdisciplinaria Koinonia* Vol VIII. N°15., 1-7. https://fundacionkoinonia.com.ve/ojs/index.php/revistakoinonia/article/view/2440

Polícia Nacional. (2018). *Proceso de reporte de atención de Incidentes cibernéticos. Policía Nacional.*

Reyes, L. N., & Boente, A. (2019). Metodología de la investigación compilacion total. *Unisoft- alebo bussines.* https://www.academia.edu/40436132/METODOLOGIA_DE_LA_INVESTIGACION_2019

Rincón, J. A., Castiblanco, S. A., Quijano, A., Urquijo, J. D., & Pregonero, Y. K. (2023). Ciberdelincuencia en Colombia: ¿qué tan eficiente ha sido la Ley de Delitos Informáticos? *Revista criminalidad vol 64*, num 3, 95-116. doi: https://doi.org/10.47741/17943108.368

Riquert, Marcelo Alfredo. 2024. "Libertad vs. Seguridad". *Revista Amagis Jurídica 16* (2):253–313.

Robles, B. F. (2019). Población y muestra. *Revista Pueblo continente, vol. núm*. (1), 245-247. https://journal.upao.edu.pe/PuebloContinente/article/view/1269

Rubio-Martín, María José, y Ángel Gordo. 2024. "Violencias de género digitales. Una propuesta desde la arquitectura de los entornos digitales y la lingüística forense". *Revista Española de Investigaciones Sociológicas* (187):129–46. doi: 10.5477/cis/reis.187.129-146.

Salazar, L. S. (2020). Investigación Cualitativa: Una respuesta a las Investigaciones Sociales. *Revista Interdisciplinaria de Humanidades, Educación, Ciencia y Tecnología* Vol. VI. N°11, 101-110. doi: DOI 10.35381/cm. v6i11.327

Sánchez, F. A. (2019). Fundamentos Epistémicos de la Investigación Cualitativa y Cuantitativa: Consensos y Disensos. R*evista digital de la investigación en docencia universitaria vol 13 num*1, 104-122. Obtenido de http://www.scielo.org.pe/pdf/ridu/v13n1/a08v13n1.pdf

Sánchez, Sergio Gabriel Vázquez. 2024. "Las TIC, ciberdelitos, *ciberdelincuencia y su impacto jurídico-social". Voces Y Saberes* (11):37–53. doi: 10.22201/fesa.vocesysaberes.2024.11.86.Solano, Alejandro Castro. S/F. "La Psicología De Internet".

Silicon Valley (2024). Los retos jurídicos del metaverso: Aproximación a los riesgos y desafíos que plantea para la identidad digital. European Public & Social Innovation Review, 9, 1–19. https://doi.org/10.31637/epsir-2024-627.

Siqi, Wenjing Lei, Hong Zhu, y Carol Hsu. 2024. "Cyberbullying perpetration on social media: A situational action perspective". *Information & Management* 61(6):104013. doi: 10.1016/j.im.2024.104013.

Sommerville, I. (2011). Ingeniería de Software. *Cámara Nacional de la Industria Editorial Mexicana.* Reg. núm. 1031. https://gc.scalahed.com/recursos/files/r161r/w25469w/ingdelsoftwarelibro9_compressed.pdf

Trudgett-Klose, Louise H., y Sarven S. McLinton. 2024. "'*Pro Gamers' & Cyberbullying: Workplace bullying & sexual harassment in professional video gaming"*. Entertainment Computing 50:100702. doi: 10.1016/j.entcom.2024.100702.

Valencia, N. A., Yulán Valencia, C. M., & Chipe, B. D. (2023). *Resiliencia en la informática. Revista Recimundo*, 7(1), 79-86. doi: https://doi.org/10.26820/recimundo/7.(1).enero.2023.79-86

Vargas, J. D., Peñalver, C. G., & Genes, J. J. (2020). Estadística descriptiva: *con aplicaciones en Excel y SPSS. Universidad de la Guajira.* https://repositoryinst.uniguajira.edu.co/entities/publication/06036085-aac3-4471-ad34-6afd7d31c323

Vásquez, A. L. (2019). *Falsos portales que conectan a México con el cibercrimen transnacional: ciberdelincuentes ya no asaltan bancos ni casas; con internet y un click atacan a sus víctimas, esta amenaza por los cibernautas apenas empieza* [Tesis de Maestría]. Repositorio de la Universidad. Obtenido de https://repositorio-digital.cide.edu/handle/11651/3561.

Verano, C. A. (2023). *La inserción de las empresas de videojuegos en Colombia en los teléfonos del mundo* [Tesis de maestría, Universidad Militar Nueva Granada]. Repositorio de la universidad. Obtenido de https://repository.unimilitar.edu.co/items/330b36d0-1009-45a7-9a5e-5826394a66bd.

Wikström, P.-O. H., & Treiber, K. (2016). *Individual crime: A situational action theory*. Cambridge University Press. https://doi.org/10.1093/acrefore/9780190264079.013.456