
FACULTAD DE CIENCIAS HUMANAS Y SOCIALES

# Amenazas del futuro *metaverso*

Autora: Rebeca Del Castillo Cordero

Director: José María Blanco Navarro

Madrid

2021/2022

**Resumen**

El metaverso está en boca de todos. El fundador de Facebook, Mark Zuckerberg, ha apostado por el metaverso y ha renombrado su compañía con el nombre de *Meta*. No es la única compañía, sino que muchas empresas de auge tecnológico apuestan por el metaverso y trabajan para que esta realidad virtual sea posible. Con ella convergen diversas tecnologías como el Blockchain, la inteligencia artificial o las gafas de realidad virtual que prometen una segunda vida digital, en la se ofrezcan posibilidades de trabajo, arte y entretenimiento, educación y hasta de inversión de dinero. Sin embargo, el metaverso no está exento de amenazas, y expertos ya especulan sobre las dificultades que puede tener para los usuarios a nivel físico, mental y social. Asimismo, debido al registro de información de los usuarios para participar en la plataforma, los ciberataques conforman una amenaza para la privacidad de los mismos y registran un beneficio considerable para los ciberdelincuentes.

*Palabras clave: metaverso, amenazas, ciberataques, Blockchain, inteligencia artificial, Facebook, realidad virtual*

**Abstract**

The metaverse is on everyone's tongue. The founder of Facebook, Mark Zuckerberg, has committed to the metaverse and has renamed his company to Meta. It is not the only company, but many technological leaders are committed to the metaverse and are working to make this virtual reality possible. It involves the convergence of various technologies such as blockchain, artificial intelligence and virtual reality glasses, which promise a second digital life, offering opportunities for work, art and entertainment, education and even money investment. However, the metaverse is not without its threats, and experts are already speculating about the physical, mental and social difficulties it may pose for users. Furthermore, due to the registration of user information to participate in the platform, cyber-attacks pose a threat to users' privacy and are of considerable benefit to cybercriminals.

*Key words: metaverse, threats, cyber-attacks, Blockchain, artificial intelligence, Facebook, virtual reality*

## Índice

1. Introducción ..... 4

Propósito general y contextualización del tema ..... 4

Objetivos del trabajo ..... 5

2. Metodología ..... 6

*Diseño de encuesta* ..... 7

*Muestra* ..... 8

3. Marco teórico ..... 9

3.1. Origen y evolución del metaverso ..... 9

¿Qué es el metaverso? ..... 12

Tipos de metaverso ..... 13

3.2. Convergencia de las diferentes tecnologías en el metaverso ..... 15

Blockchain, criptomonedas y NFT ..... 15

Inteligencia artificial ..... 17

5G ..... 18

Realidad virtual, aumentada y mixta ..... 18

4. Riesgos y amenazas del futuro metaverso ..... 19

Físico, mental y social ..... 19

Fraudes y engaños ..... 22

Ciberataques ..... 24

Privacidad ..... 25

Resultados del análisis ..... 27

5. Conclusiones y propuestas ..... 34

Conclusiones ..... 34

Propuestas de mejora ..... 37

6. Glosario ..... 42

7. Bibliografía ..... 44

# 1. Introducción

## Propósito general y contextualización del tema

El propósito general de este trabajo es investigar sobre el futuro de esta nueva realidad virtual y los riesgos que vendrán ligados a ella.

La incorporación de nuevas tecnologías digitales y la aplicación de Internet han transformado la vida cotidiana de las personas. Internet llegó para cambiarlo todo. Esta infraestructura que se esparció por el mundo ha llegado a modificar la economía, la forma de socializar, la música y las comunicaciones; lo que hoy en día conocemos se ha visto alterado por esta red de conexiones. La evolución de la tecnología es cada vez más rápida, y en este trabajo describiremos lo que podría ser el futuro de Internet, el metaverso.

Precedente de Second Life o Fornite llega de nuevo el concepto del metaverso que comprende la nueva realidad a la que nos enfrentamos y que el inversor de riesgo Piers define como: 'un universo digital en vivo y persistente que permite a los individuos un sentido de agencia, presencia social y conciencia espacial compartida así como la habilidad de participar en una extensiva economía virtual con un profundo impacto social' (Bush, 2021). Es decir, es un mundo virtual en 3D, interactivo, y además multiusuario que te permite relacionarte con otras personas estés donde estés a través de herramientas computacionales en forma de avatares y agentes personificados en simulación.

Por otra parte y debido a las circunstancias de la Covid-19, muchas personas se han visto obligadas a trabajar en remoto, utilizando plataformas de videoconferencias como Zoom, Teams y otras aplicaciones de mensajes de texto. Es por ello que la realidad virtual convertirá estas aplicaciones en remoto en una novedosa forma de trabajar junto a otros, independientemente de la distancia que les separe. La realidad virtual, no solo comprenderá los videojuegos, sino que será parte de aerolíneas, tratamientos de salud, seguridad y de la nueva economía de la que será protagonista el Blockchain. Esto no ha pasado desapercibido, y grandes empresas tecnológicas como Facebook, Apple,

Sony, Alibaba y Tencent están creando fondos centrados en el valor económico de estos mundos que llega a una inversión de 500 millones de euros.

El metaverso está creando un nuevo mundo de infinitas posibilidades y experiencias novedosas y por tanto, de nuevos peligros. La tecnología no está exenta de amenazas y riesgos de modo que se debe trabajar en construir una nueva realidad libre de deepfakes, macrodatos, ciberataques, fraudes y estafas. El uso ético de los datos que se recopilan y la transparencia de las grandes tecnologías es la labor de organizaciones como X Reality que lucha contra los desafíos de seguridad cibernética que vendrán ligadas a estas nuevas tecnologías emergentes. Estos peligros serán estudiados con detenimiento en este trabajo.

## Objetivos del trabajo

El objetivo general será estudiar la nueva realidad virtual del metaverso y los elementos tecnológicos consiguientes a ello. Además, nos centraremos en las amenazas que vendrán de la mano de esta tecnología emergente y las nuevas necesidades que surgirán con ella.

Como objetivos específicos nos centraremos en:

- Estudiar la convergencia de diferentes tecnologías como la Inteligencia Artificial, 5G, la Realidad Virtual, Aumentada y Mixta, el Blockchain y las criptomonedas.

- Exponer los riesgos ligados a la realidad virtual, ya sean fraudes, engaños, ciberataques y amenazas físicas, sociales o psicológicas.

- Estudiar el marco legal en el que confluye la nueva realidad virtual y la protección de dispositivos e información y su relación con la privacidad del usuario

- Conocer el impacto del metaverso en las personas y si existe implicación con el mismo

## 2. Metodología

La metodología del presente trabajo es de naturaleza mixta. Para ello, se realizará una revisión bibliográfica acompañada de unas conclusiones propias de la información recabada. La revisión bibliográfica se ha definido como "la operación documental de recuperar un conjunto de documentos o referencias bibliográficas que se publican en el mundo sobre un tema, un autor, una publicación o un trabajo específico. Es una actividad de carácter retrospectivo que nos aporta información acotada a un periodo determinado de tiempo' (Silamani, 2015). Se recurrirá a fuentes diversas con el objetivo de contextualizar teóricamente el concepto del metaverso y las amenazas surgidas con ella; fuentes primarias, como informes de organismos oficiales- Interpol, Europol, Digital Euro Association- pero sobretodo, y debido a la primicia del asunto, se ha tenido que recurrir a fuentes periodísticas, de prestigio, y a blogs de expertos en el tema. Además, se ha recopilado información de trabajos académicos de universidades de Reino Unido, Estados Unidos, Italia y España.

La extracción de la información de las fuentes ha estado guiada por palabras clave, introducidas de manera progresiva para completar los apartados del trabajo. En su mayoría, los términos utilizados han sido en inglés, siendo los más mencionados: 'metaverse', 'fraud',' cyberattacks', 'cryptocurrency'AND 'metaverse', 'metaverse' AND affairs'.

Tras la obtención de una importante suma de material bibliográfico, se ha procedido a analizar, validar y sintetizar la información para la elaboración del marco teórico.

Así mismo, esta investigación se compondrá de un enfoque de tipo cualitativo, que tiene como instrumento de recolección de datos una encuesta, definida como 'instrumento para recoger información cualitativa y/o cuantitativa de una población estadística. Para ello, se elabora un cuestionario, cuyos datos obtenidos será procesados con métodos estadísticos.' (Westricher, 2020) para recabar datos sobre opiniones del metaverso, su posible uso y su implicación con el mismo.

## *Diseño de encuesta*

Como instrumento de recogida de datos se ha utilizado la plataforma de Google Forms, para darle forma al cuestionario.

Se trata de un cuestionario de naturaleza cualtitativa, destinada a conocer las opiniones y puntos de vista sobre el metaverso. Cuenta con 8 preguntas cerradas y estructuradas de opción múltiple divididas en tres sectores: concepto del metaverso, inclusión en el mundo virtual y amenazas.

Para la elaboración del cuestionario se obtuvieron preguntas del cuestionario de Digital Information World (Ahmed, 2021), que posteriormente han sido modificadas, además de añadir otra serie de preguntas de elaboración propia. En el cuadro mostrado a continuación:

| PREGUNTAS | OBSERVACIÓN | FUENTE |
|---|---|---|
| 1. ¿Conoces el concepto de metaverso? | | Elaboración propia |
| 2. ¿Tienes un concepto positivo o negativo del metaverso? | | Elaboración propia |
| 3. ¿Crees que se podrá implementar el metaverso? ¿De cuánto tiempo crees que se trata? | | Elaboración propia |
| 4. Si se pudiese implementar el metaverso y contaras con las herramientas para formar parte del mismo, ¿te plantearías ser usuario del metaverso? | | Elaboración propia |
| 5. ¿Por qué motivos te unirías al metaverso? Selecciona al menos dos: | Trabajo, juegos, entretenimiento para adultos, educación, inversión de dinero, arte y entretenimiento, citas en línea | Elaboración realizada por Digital Information World |
| 6. ¿Qué amenazas consideras más importantes en el metaverso? Califica siendo 1 poco relevante y 5 muy relevante | Fraudes y engaños, privacidad, mental, ciberataques, físico y | Elaboración realizada por Digital Information World |

| | | |
|---|---|---|
| | social | |
| 7. ¿Qué crees que debería estar censurado en el metaverso? | Sin censura, restringido y completamente censurado | Elaboración propia a partir de Digital Information World |
| 8. ¿Crees que los criminales registrados (como los asesinos en serie y agresores sexuales) deberían vivir sus impulsos en los espacios restringidos del metaverso con la guía de un terapeuta, haciendo que la sociedad sea más segura? | | Elaboración realizada por Digital Information World |

### *Muestra*

El procedimiento de selección de individuos ha sido a través de una encuesta online de muestreo probabilístico, ya que se ha utilizado un método de selección aleatoria. Este cuestionario ha sido cumplimentado por un total de 84 usuarios, sin discriminar por edad, nacionalidad o sexo, por lo que cuenta con opiniones de grupos de individuos de manera genérica. Se ha difundido a través de redes sociales como Whatsapp, Instagram y LinkedIn, solicitando su colaboración en la realización del cuestionario y en su difusión.

Las fechas en las que se realizó la recogida de datos fueron entre el 12 de marzo y el 17 de marzo.

## 3. Marco teórico

### 3.1. Origen y evolución del metaverso

El origen del metaverso no está claro pero sí se puede hablar de las primeras referencias al mismo, en la novela de Neal Stephson, Snow Crash, que dota del año 1992. Lo más característico de este libro es que el autor creó la primera referencia a un mundo virtual mucho antes de que se empezase a hablar del ciberespacio. Neal incluye en su libro la idea de configurar avatares digitales de los usuarios como una forma de escapar de una realidad distópica. Además, ya se hablaban de ciertos accesorios, como gafas de realidad virtual y auriculares que hacían más real esa inmersión y otorgaban la capacidad de poder moverse por ese entorno (Orellana, 2022).

Desde este primer acercamiento al metaverso ha habido otras descripciones y aplicaciones del concepto.

En 2003 se abrió una Comunidad Virtual denominada Second Life a la que se podía acceder de manera gratuita a través de Internet. Sus usuarios podían explorar el mundo virtual a través de su avatar que interactuaba con otros usuarios, establecía relaciones sociales y participar en diversas actividades tanto individuales como en grupo. Su creador, Philip Rosedale, fue pionero de muchos conceptos de los que se están explorando en la actualidad, pese a que en aquel entonces no se les bautizó como metaverso. Con el auge del 'meta' de Facebook, el fundador de Second Life ha vuelto a recobrar el interés en este mundo virtual y se ha reincorporado en la plantilla de su antigua empresa (Orellana, 2022).

Otra de las grandes referencias al concepto del metaverso lo da el visionario director Steven Spielberg en 2018, con su película Ready Player One, adaptación de un libro de Ernest Cline publicado en 2011. Se encuentran muchas similitudes entre el mundo virtual que promete Facebook y el de la película de Spielberg, solo que en vez de llamarse metaverso se denomina Oasis (Orellana, 2022). En ambos se necesitan unas gafas de realidad virtual que te teletransportan a una nueva forma de vida, se crean avatares en los que puedes escoger la apariencia que desees en un escenario o espacio sin límites. Las amenazas que se señalan en la película se pueden asemejar a posibles amenazas que puede suponer este futuro metaverso y que veremos en otro punto del trabajo.

Por último otro predecesor del metaverso podría ser Fornite, ya hay expertos que señalan que el futuro de Internet podría parecerse a esta plataforma, ya que este se caracteriza por ser un universo tridimensional en el que además de poder jugar, se puede acudir a conciertos de música o a festivales de cortometrajes (Huddleston, 2021). Es más, se han ido produciendo eventos en esta plataforma en los últimos años; en el 2019, más de 7 millones de jugadores asistieron a la transición al Capítulo 2 de Fornite; en abril de 2020 más de 12 millones de usuarios acudieron de manera telemática al concierto en vivo del rapero Travis Scott o el concierto de Ariana Grande que se dio unos meses más tardes durante tres días seguidos, en el cual la cantante se obsequió con más de 20 millones de dólares por su concierto en el Rift Tour en Fornite (Huddleston, 2021). Los jugadores podrían disfrutar del evento independientemente de donde vivan y de manera gratuita, solo necesitaban tener una cuenta de Fornite para poder acceder al evento. El éxito fue rotundo ya que estos renombrados artistas colaboraron con el videojuego para actuar en plena pandemia de COVID-19 donde cada usuario se conectaba desde su ordenador, y fue una opción inteligente en el momento en que los conciertos eran impensables.

El metaverso es aún una idea pero cada vez más palpable con el avance de la tecnología. El que ha revolucionado Internet es Mark Zuckerberg. El empresario y programador informático estadounidense, ya empezó a programar a los 12 años (Millán, 2021).

Bailar en un concierto de forma virtual o reunirse con amigos que viven en la otra punta del mundo son una de las muchas acciones que Zuckerberg promete a sus más de 104 millones de seguidores de Facebook y a lo más de 297 millones de usuarios de Instagram. El 28 de octubre de 2021, un vídeo sobre el futuro metaverso de Facebook inundó Internet, bajo la descripción de: 'Welcome to next chapter of social connection. A place where we'll play and connect in 3D' (Bienvenidos al próximo capítulo de las conexiones sociales. Un lugar donde jugar y conectar en la tercera dimensión) (Pascual, 2021).

La nueva propuesta de Zuckerberg es hacer posible el metaverso, es por ello que han cambiado de nombre a la compañía de Facebook a Meta, para reflejar su compromiso con este futuro. En la presentación del metaverso se pudieron hacer hincapié en diversos puntos que veremos a continuación, pero como síntesis, este nuevo mundo virtual nos permitirá aprender, colaborar y jugar en espacios y de maneras que nunca antes hubiésemos podido imaginar (Millán, 2021).

En el vídeo de presentación se le otorga una gran importancia a que el metaverso será la sucesión a la conexión entre móviles, llegando a poder vivir experiencias con personas que se encuentren lejos de nosotros. Diremos adiós a una pequeña pantalla donde vemos los vídeos y lo cambiaremos por experiencias reales, al igual que jugando a juegos en los que cambiaremos el ordenador por la sensación de estar dentro del juego viviendo las sensaciones y experiencias del mismo avatar. Todo lo que hoy en día conocemos, cambiará, explicaba Mark, cambiará el tiempo que pasamos delante de las pantallas por un tiempo viviendo experiencias, y eso solo lo podremos conseguir con la siguiente generación de Internet (Millán, 2021).

El anuncio de Meta, es una pieza audiovisual que llama la atención de todos, no solo por su contenido sino también por su forma. El creador, sabe que a pesar de que todo el mundo es bienvenido a esta nueva dimensión, se focaliza en un público más joven. Los jóvenes hace ya un tiempo que se desconectaron de Facebook, y que se conectaron a redes como Instagram o Tik tok. Y es que redes sociales como esta última, que hace tres años no existían, han conseguido en una pandemia (en número de usuarios) lo que a Facebook le costó 18 años. Sumida en una colosal crisis de reputación derivada de la publicación de los Facebook Papers (el descrédito de Facebok), fomentado por las críticas de la denunciante francés Haugen de las tropelías cometidas por la empresa, comenzando por fomentar los trastornos alimentarios hasta poner en peligro la democracia, algunos de sus usuarios se preguntaron si no sería mejor un mundo sin estos servicios (Millán, 2021). Pero a pesar de este contexto, Zuckerberg lanzó su apuesta para recuperar la confianza de sus usuarios y captar la atención de los 'nativos digitales' (Ojeda, 2022).

Su contenido, también llama la atención, avatares que interactúan y viven en un mundo que va más allá de la física, y la palabra futuro que se escucha durante todo el anuncio, en el que se nos invita a no tener miedo sino que busquemos con los brazos abiertos a crearlo entre todos.

De hecho, la compañía de Mark Zuckerberg hará una inversión de 10.000 millones de dólares en Facebook Reality. En este metaverso Zuckerberg promete tener una experiencia inmersiva no solo para jugar, sino para asistir a conciertos, viajar online e incluso trabajar y estudiar. Ya explicaba el CEO de Facebook que: 'Buena parte de la experiencia del metaverso va a girar en torno al poder de teletransportarse de una experiencia a otra." (*¿Cómo funcionará el metaverso de Facebook?*, 2022).

No está claro totalmente lo que será el metaverso, pero sí que supondrá una transformación digital en las diversas áreas de nuestra vida.

## ¿Qué es el metaverso?

En una sociedad en continuo cambio no debe sorprendernos los grandes avances tecnológicos a los que la población se ve sometida. Es complicado establecer una definición única para el metaverso cuando acaba de comenzar a emerger.

Snow crash, Ready Player One o Second Life ya nos hablaban de este futuro metaverso e intentaban dibujar lo que Mark Zuckerberg quiere convertir en un proyecto real, en un proyecto que configure la evolución de Internet y que de vida a conceptos que solo podíamos imaginarnos en la ciencia ficción (Bush, 2022).

Lo que hace del metaverso tan significativo es que es un estado sucesor casi de Internet móvil, esto es porque el metaverso no reemplazará al Internet, sino que se basará en él y lo transformará. El metaverso es 'una red interoperable y de escala masiva de mundos virtuales 3D renderizados en tiempo real que pueden ser experimentados de manera sincrónica y persistente por un número efectivamente ilimitado de usuarios con un sentido individual de presencia y con continuidad de datos, como identidad, historia, derechos, objetos, comunicaciones y pagos.' (Ball, 2022). Es importante además, expresar lo que el metaverso no es. No se debe describir como realidad virtual, ya que la realidad virtual es simplemente una forma de experimentar el Metaverso. Tampoco es simplemente un videojuego, ya que estos tienen unos propósitos específicos, no integrados, temporales y limitados en participantes en línea. El metaverso amplificará significativamente el número de experiencias virtuales, y a su vez ampliará el número de personas que participan en ellos (Ball, 2022).

Tres de las reglas que se consideran imprescindibles en el metaverso según Edward Castranova, investigador de videojuegos y mundos virtuales, son la interactividad, la incorporeidad y la persistencia (Silva, 2021). La interactividad permitirá al usuario ser capaz de comunicarse con los demás usuarios, y poder influir sobre objetos, usuarios y el mismo metaverso, así como la incorporeidad dotará al nuevo mundo virtual la posibilidad de eliminar las barreras físicas, incorporando un avatar que representaría nuestra identidad (Silva, 2021). Y por último, la persistencia en la que el metaverso convergerá con diversas tecnologías que hablaremos en otro capítulo

de este trabajo y que permitirá la continuidad de nuestras vidas en este mundo virtual.

No habrá un único metaverso, al igual que no hay un simple sitio web o un país. Podrán existir metaversos interconectados donde se podrá viajar de uno a otro. Existirán metaversos temáticos; una escuela, una universidad podrán ser un metaverso. El metaverso se convertirá en una experiencia virtual en la que sus usuarios no tendrán que salir de casa (Lucatch, 2021). Si de algo se caracteriza el metaverso es de las múltiples actividades que se podrán realizar en el mismo, como jugar de manera totalmente inmersiva, disfrutar de conciertos, trabajar en espacios virtuales de trabajo, comprar en las tiendas del metaverso y por supuesto socializar con otros miembros del metaverso (Silva, 2021).

### Tipos de metaverso

Para comprender mejor este concepto es necesario partir de una diferenciación base. Por un lado, están los metaversos **centralizados**, es decir aquellos que tienen un dueño, y todo lo que existe dentro y lo que puedes consumir en ese entorno no es de tu propiedad sino del dueño del metaverso. En este campo nos encontramos videojuegos como el ya mencionado anteriormente, Fornite, en el que se puede interactuar con gente y comprar hasta productos de marca si estas quisiesen publicitarse y vender en este espacio: «Hay marcas muy potentes que están basando su modelo de negocio en entrar en este videojuego y vender a través de que entren otras marcas en su espacio en el mismo» (*Queen's Printer of Acts of Parliament*, 2018) o la plataforma que surgirá de Facebook. 'En estos metaversos, la organización central, tiene en su poder todos los datos de los usuarios, siendo la única que decide sobre el futuro del metaverso. Además,' se integran micropagos con criptomonedas y los elementos virtuales están representados como NFTs. Por lo tanto, sí tienen una economía virtual propia, pero el control de esta economía recae en manos de unos pocos organizadores' (Callejo, 2021).

En cambio, los metaversos **descentralizados** son aquellos en los que los usuarios pueden comprar una propiedad y pasa a ser suya. Esto da pie a un vacío legal, ya que la persona que ha comprado la propiedad tiene la potestad y el control sobre la misma, y nadie puede hacer nada con ello; es más se podrá poner límites y cobrar entrada por acceder al espacio (Callejo, 2021). Para gestionar un metaverso descentralizado se debe disponer de tokens, y esto da cierto poder de decisión. Estas decisiones se correlacionan

con el porcentaje de tokens que tengas en la comunidad, como un pequeño accionista con votos para determinadas decisiones (Callejo, 2021).

Algunos de los metaversos descentralizados más relevantes son:

1. Decentraland, no cuenta con servidores centrales y nadie controla este mundo virtual, entonces, ¿cómo funciona? Decentraland cuenta con una DAO, Organización Autónoma Descentralizada. Gracias a esto los propietarios de tierra y de MANA (moneda virtual) pueden juntarse, proponer cambios o mejoras y votar por ellas. Esta DAO cuenta con una reserva de MANA para financiar iniciativas y proyectos a futuro. Los usos que se mencionan para esta plataforma, por una parte es utilizarla como infraestructura para diversas aplicaciones ya que es muy fácil crear objetos e integrar sonidos y texturas (Pinto, 2022). Es decir, es posible crear cualquier cosa, galerías de arte, vallas publicitarias, ofrecer conciertos, cursos educativos, casinos. Ya se han dado eventos antes, por ejemplo, en julio de 2021 José Delbo, vendió cientos de NFT por más de 18 millones de dólares en uno de los eventos especiales de Decentraland. Sol Félix la famosa casa de subastas de obras de arte y artículos de lujo, ya abrió una galería virtual en este espacio. Cada vez más y más empresas se suman a este universo. Es por ello que numerosos inversores están comprando propiedades o invirtiendo en la moneda virtual de Decentraland (MANA) (Pinto, 2022).

2. Cryptovoxels: ‘Es un proyecto que nació en 2018 como un mundo virtual similar a Decentraland. Se trata de una plataforma de realidad virtual que se aloja en la Blockchain Ethereum y utiliza el token ERC-721’ (Tech, 2022).
   Cryptovoxels, se formó como un metaverso que como su nombre indica ‘voxels’ (pequeños cubos) trataría de formar un terreno en la web, similar a Minecraft. La gran diferencia es que en esta plataforma se permite hacer vida y socializar con otros usuarios de la aplicación y hasta generar comercios a través de los tokens. Para acceder a Cryptovoxels, no es necesaria ninguna aplicación, sino que lo puedes construir desde tu navegador a través de la página oficial, aunque si necesitarás una parcela y una wallet de navegador. Las acciones principales que puedes realizar en esta plataforma son explorar las parcelas de otros usuarios, participar en eventos, construir tu propia parcela que has adquirido (de

opciones ilimitadas) o comprar y vender en general ya que este metaverso cuenta con su propia economía (Tech, 2022).

3. Sand Box: Sandbox es un juego de Blockchain, con el token SAND, se juega en un mapa de áreas segmentadas. Contiene piezas que son los denominados NFT, que se venden por miles de USD. Se pueden organizar eventos, jugar a juegos, trabajar en diferentes terrenos… Sandbox se dibujar como una gran competencia a meta de Facebook, incorporando la función de poder crear prácticamente cualquier cosa a través de su innovador software de edición 3D (Planteo, 2021).

4. Axie Infinity: terminamos de hablar de tipos de metaverso con uno de los más oídos, Axie Infinity. Con más de 350.000 usuarios activos, este mundo cripto 'combina un modo aventura con misiones diarias, enfrentamientos con otros jugadores y recolección de monedas con la infraestructura subyacente de los NFT y la red Blockchain.' (Pérez, 2021). Como mínimo para acceder al juego se debe comprar tres criaturas asociadas a NFT, y que tienen un valor de 200 dólares, en función al valor actual de Ethereum. Su moneda virtual son los AXS (Axie Infinity Shards) y SLP (Smooth Love Potion) (Pérez, 2021).

## 3.2. Convergencia de las diferentes tecnologías en el metaverso

### Blockchain, criptomonedas y NFT

Hasta ahora, nuestra experiencia en el ciberespacio se limitaba al uso del móvil y ordenador, a manejar aplicaciones o a navegar por diversas páginas. Cuando dejábamos de mirar a nuestras pantallas el mundo digital se apagaba. Es por ello que el metaverso llegó para cambiarlo todo, y hacer que vivamos de manera inmersiva estas experiencias. Para comprender el funcionamiento debemos profundizar en las diversas tecnologías que se mueven alrededor del metaverso y que hacen posible su articulación (Escribano, 2021).

Para entender cómo funciona el Blockchain debemos partir de la base es que no existen intermediarios a la hora de realizar transacciones. Esto resulta algo complicado de entender de primeras ya que estamos acostumbrados al sistema usuario-intermediario-usuario; lo podemos ver en un ejemplo sencillo a través de imaginarnos que Juan quiere realizarle una transferencia de 1000 euros a Pedro, y esto lo hace a través del banco, en

el que simplemente esta entidad debe realizar un cambio en los balances de sus cuentas. Ninguno tiene control sobre el proceso, y los bancos contienen toda la información, el banco es el intermediario y están sujetos a sus condiciones. Pero con la llegada de esta nueva tecnología todo cambia. Blockchain o 'cadena de bloques', elimina completamente a los intermediarios, y descentraliza toda su gestión. Esto nos resulta familiar, debido a que ya estuvimos hablando del funcionamiento de los metaversos descentralizados (Escribano, 2021). El control es de los usuarios, y son partes de un banco con millones de nodos, de los cuales se vuelve partícipe. Es además, una base de datos distribuida y segura, gracias al cifrado que tiene, y los usuarios que son parte de ella y que registran todos los movimientos de criptomonedas (Escribano, 2021). Se ha de saber que la tecnología Blockchain permite que existan criptomonedas, como Bitcoin o Ethereum. Pero estas no son solo las que existen. Las criptomonedas son llamadas así gracias a su naturaleza 'encriptada', es decir, protegidas a través de codificación. Esta característica las convierte en un sistema monetario muy atractivo porque es difícil de alterar o hackear y porque no es controlado por un banco o un gobierno, ya lo vimos con el ejemplo anterior de Juan y Pedro. El mercado de las criptomonedas se basa en la especulación. Esto supone que las personas tratan de adivinar lo que sucederá, lo cual crea una gran inestabilidad ya que el valor de algo puede dispararse por los cielos un día, y caer bruscamente al día siguiente (Escribano, 2021).

Y, ¿por qué son las criptomonedas importantes en el Metaverso? En este entorno digital, es necesario realizar transacciones con monedas digitales. Es aquí donde podríamos encontrar el verdadero asentamiento de la economía virtual. A día de hoy, aunque en algunos países y empresas han aceptado la moneda como divisa oficial, es más complicado encontrar la función de las mismas en la sociedad. Es por ello, que en el metaverso, estas podrían identificarse como el sistema económico oficial y único.

'Sea como sea, estos metaversos necesitan de una economía interna, y esta se tiene que dotar de una criptomoneda que permita operar en sus mercados' (Escribano, 2021).

Otra de las tecnologías que ha cobrado una gran repercusión en el presente son los NFT. Pero, ¿qué son los NFT y por qué son tan importantes? En primer lugar, se sabe que normalmente cuando una persona compra un cuadro, compran el objeto físico en sí. Pero en el mundo virtual una sucesión de cambios ha venido ligado a esta nueva era, y es que algunos coleccionistas quieren ser dueños del arte que circula en Internet de manera gratuita. Arte como un GIF, un meme, un tweet, un cuadro que solo existe en Internet, y es aquí donde aparecen los NFT o tokens no fungibles. Que algo sea no

fungible significa que es único e insustituible. Es por ello que los NFT, son tokens o fichas, que forman un título digital que expresa que tienes esa cosa. Los NFT, se pueden tanto comprar como vender y están creados a través de la tecnología Blockchain (Maldonado, 2022). Si por algo tienen importancia los NFT en el metaverso son debido a que los ítems de los juegos pueden ser muy valiosos, ya que suelen otorgar una función concreta o algún tipo de propiedad. Normalmente en los juegos de ordenador, ya se ha implantado una economía en la cual se movilizan millones de euros, pero estos ítems tienen un problema y es que pertenecen a la compañía que las desarrolla. Es decir, si desaparece el juego, desaparecen los ítems y el dinero invertido. Esta es la gran diferencia con los NFT, al ser parte de la tecnología Blockchain se encuentran descentralizados, y 'no solo pueden ser intercambiados a través de un mercado común, sino que pueden representar ítems de cualquier tipo y traspasar esos ítems a distintos espacios donde sean soportados' (Maldonado, 2022).

### Inteligencia artificial

La inteligencia artificial cada vez adquiere mayor importancia en nuestras vidas. Con la mejora e implementación de las nuevas empresas tecnológicas, las máquinas tienen mayor capacidad que los humanos para reconocer patrones y tener todavía un mayor impacto en nuestras vidas. Pero, ¿cuál sería una definición para la Inteligencia Artificial? Utilizaré la propia IA para encontrar una definición, es decir, a través de Google: 'La inteligencia artificial o IA, es la simulación de procesos de inteligencia humana por parte de máquinas especialmente sistemas informáticos. Incluyen el aprendizaje, la adquisición de información y reglas para el uso de la información, el razonamiento, usando las reglas para llegar a conclusiones aproximadas o definitivas, y la autocorrección' (Rouse, 2021). De ese modo podemos llegar a imaginarnos la cantidad de usos que puede tener la Inteligencia Artificial, a la hora de hacer fotografías, conducción autónoma, IA en videojuegos, adelantarse a nuestros gustos, etc. Uno de los usos que más nos interesan es en videojuegos, ya que tiene una gran importancia para su uso y funcionamiento. Meta, la compañía de Zuckerberg ha diseñado y construido el AI Research SuperCluster (RSC), un superordenador que se pronostica como el ordenador más rápido del mundo cuando esté completamente construida a mediados de 2022. Este ordenador ayudará a los investigadores de IA de Meta a construir nuevos y mejores modelos de IA como por ejemplo, impulsar traducciones de voz en tiempo real para

grandes grupos de personas, cada una hablando en un idioma diferente, desarrollar nuevas herramientas de realidad aumentada, y allanará el camino para la creación de tecnologías para el metaverso (Rouse, 2021).

### 5G

Mejoras en la educación, nuevas experiencias inmersivas en espectáculos o videojuegos, mejoras para la salud, la tecnología 5G es una nueva generación de la red móvil y ha llegado para implementar mejoras en nuestro día a día. El 5G, trae nuevas características a diferencia de sus antecesores, mayor ancho de banda, mayor latencia y más seguridad lo que nos permitirá tener una mejor experiencia cuando veamos contenidos de vídeos en Internet, mejor comunicación, e implementaciones en sanidad y educación.

El 5G, según PwC, tendrá un impacto en la economía global de 1.300 millones de dólares en el año 2030. Con el auge del metaverso es inevitable pensar en la conectividad que este debe necesitar. El 4G no es suficiente ni por ancha de banda ni por latencia, necesita una conexión ultrarrápida que se la podrá dar el 5G para que pueda funcionar adecuadamente (*¿Qué es metaverso y cómo se irá desarrollando a medida que avance 5G*, 2021).

### Realidad virtual, aumentada y mixta

Para poder entender el metaverso, es importante definir estos conceptos y hacer énfasis en las similitudes y diferencias de los mismos.

La realidad virtual consiste en un ambiente artificial creada por un ordenador, la realidad aumentada añade a una escena del mundo real información generada de manera tecnológica, y por último, la realidad mixta se sostiene a través de elementos tecnológicos para enriquecer la realidad virtual o aumentada (Milgram y Kishino, 1994).

La realidad virtual está presente en vídeos de Youtube, películas grabadas con una cámara de 360º o simulaciones interactivas en 3D, en la que entran los videojuegos. Para poder reproducir este tipo de contenido son necesarios dispositivos digitales como cascos o gafas de realidad virtual, guantes hápticos y hasta para experiencias olfativas se están programando aromatizadores (Bockholt, 2020).

Por otra parte, nos encontramos con la realidad aumentada que como hemos visto anteriormente nos permite utilizar contenido virtual en el mundo físico. Esto lo vemos

en ejemplos, como el camino más rápido para encontrar un producto de un supermercado, la función en Google Maps para indicarte el camino, y en el sector de entretenimiento vemos como dinosaurios cobran vida en la mesa de tu habitación o coches de juguete que derrapan en el salón. Todo esto depende de la calidad del dispositivo que se utilice (Bockholt, 2020).

Y por último tenemos la realidad mixta, que hace referencia a los vídeos superpuestos que combinan secuencias del mundo real con contenido de la realidad virtual. Encontramos ejemplos, con por ejemplo la tecnología de la pantalla verde (Bockholt, 2020).

## 4. Riesgos y amenazas del futuro metaverso

*'La tecnología inmersiva es como la división de átomos. Puede usarse para ayudar a la humanidad, levantar a la humanidad o puede usarse para destruir a la humanidad. Ahí es donde estamos con la realidad virtual. Estamos a punto de tener herramientas poderosas como el fuego. ¿Qué haremos con esto? ¿Cómo lo vamos a usar? ¿Cómo vamos a poner resguardos para no quemarnos?'* (Heller, 2020).

### Físico, mental y social

La integración del metaverso en nuestras vidas dará lugar a una que se vayan desvaneciendo las líneas entre la realidad y las realidades virtuales alternativas. Esto podría desembocar en nuevas experiencias tanto positivas como negativas ya que las personas podrán explorar puntos de vista alternativos de sí mismos, experimentando con el género, habilidades físicas y poderes que están más allá de los humanos (Magid, 2022).

Y es que si las redes sociales como Instagram conocen con detalle que sus plataformas son tóxicas, sobre todo para los adolescentes, y aun así le han restado importancia, exponiendo que estos efectos negativos no deben de ser generalizables, con el metaverso puede ocurrir lo mismo o puede llegar a tener un mayor alcance (McDougall, 2022).

Ya son algunos autores que consideran que el metaverso puede convertirse en un problema de salud pública en los próximos años. Y es que se predice que le metaverso podría hacernos adictos a la hiperconectividad. Esto lo referencian en que el metaverso

se convertirá en una realidad ideal, y nuestro cerebro pasará a creer que estamos viviendo situaciones reales y muy estimulantes y satisfactorias. ‘Dejaremos de estar pasivos a interactuar con nuestros dispositivos, lo que hace al mundo virtual aún más potencialmente adictivo’. Y es que la psicóloga Gabriela Paoli entrevistada en el artículo en cuestión nos ofrece una visión más negativa sobre el metaverso, expresando que la liberación de dopamina nos hará adictos, y esto podría provocarnos episodios psicóticos constantes y combinados con la falta de sueño puede tener consecuencias negativas en nosotros y nuestras relaciones sociales (González, 2021).

Por otra parte, el contenido que deambula por Internet es en muchos casos abusivo e inicuo; con la llegada del metaverso el contenido no deseado será más gráfico, en 3D y auditivo, por lo que se sentirá de forma más intrusiva (Lalani, 2022). Es importante comprender las características psicológicas de las experiencias inmersivas y hasta qué punto pueden afectar a los usuarios. Las tecnologías inmersivas a diferencia de las redes sociales u otras tecnologías, significa que el usuario se siente como si estuviera en otro entorno. El contenido genera patrones de estimulación, como fotones de luz para los ojos, entrada acústica para los oídos y guantes hápticos para el tacto. Esto hace que el usuario se sienta inmerso y que conduzcan a una sensación de verosimilitud en el entorno.

En segundo lugar, existen aspectos en la tecnología de realidad virtual que da un sentido de presencia, como lo define la directora del Outlaw Lab, Jessica Outlaw: ‘Cuando estoy en un visor de realidad virtual y hablo con personas que conozco, en realidad tengo la sensación de estar allí con ellos y tener una experiencia encarnada… Creo recuerdos con ellos en estos entornos virtuales… No me siento como si hubiera una gran diferencia entre pasar el rato con mis amigos en un espacio virtual y pasar el rato con ellos en el mundo físico real’ (Outlaw, 2022).

Por último nos encontramos con el concepto de encarnación, es decir, experimentar que un cuerpo de un avatar o un cuerpo virtual es tu cuerpo físico.

Es la combinación entre inmersión, presencia y encarnación lo que permite a los usuarios sentir que están en una realidad alternativa, interactuar completamente con las características del entorno y con otras personas del espacio virtual.

Y, ¿qué riesgos psicológicos podemos encontrar tras analizar estas variables? Y es que no es simplemente la calidad inmersiva lo que define estas experiencias sino como nuestra mente las memoriza. Como explicaba el Dr. Thomas Furness, uno de los primeros desarrolladores de tecnologías inmersivas, 'las tecnologías inmersivas

despiertan la memoria espacial como ningún medio lo había hecho' (Heller, 2020). Furness dice que estas experiencias se retienen como si estuvieran 'dibujadas con tinta de manera permanente' Y es que estas afirmaciones las respalda con la neurociencia, ya que la forma en la que nuestros cerebros recuerdan estar en un entorno virtual es similar a una experiencia en la vida real. Los científicos midieron la actividad cerebral en resonancias magnéticas y descubrieron que al experimentar un evento virtual y lo recuerda, la respuesta del hipocampo es parecida a si experimentase un evento real. Y no solo eso, sino que además también se corresponde la respuesta fisiológica que tendría en situaciones reales. El profesor Mark Lemley expresa: 'en una palabra, una experiencia visceral. Las cosas que suceden allí no son físicamente reales: si el malo te dispara en 'Bullet Train', no te mueres en la vida real. Pero se sienten reales. Y estos sentimientos a su vez pueden tener consecuencias físicas reales. Literalmente, podrías morir de miedo (o al menos sufrir un ataque al corazón) por un juego que se sintiera lo suficientemente real. Incluso si no sufre daños físicos, habrá experimentado lo que vio e hizo en la realidad virtual de una manera que no experimenta en Internet o en un videojuego que no es de realidad virtual' (Lemley y Volokh, 2018).

Aprovechando lo que el profesor Lemley indica, procederemos a inducirnos en riesgos más físicos que puede tener esta realidad virtual.

Mirando el contexto digital actual, y revisando el Informe de Evaluación de Amenazas Globales de WEProtect Global Alliance, 1 de cada 3 encuestados, es decir, un 34% de los encuestados de la encuesta global de Economist Impact se les pidió hacer algo sexualmente explícito en línea con lo que se sintieron incómodos durante la infancia (Harrison, 2022). Además, Internet Watch Foundation vio un aumento del 77% en el material sexual infantil en Internet de 2019 a 2020. Por otro lado, se realizó una encuesta mundial por Web Foundation, en 2019 sobre los abusos en línea, y el resultado sorprendió con que más de la mitad de las niñas y mujeres jóvenes habían sufrido abusos por Internet. Esto es destacable ya que los riesgos digitales en el metaverso se sentirán más reales ya que se producen de manera inmersiva. Mary Anne Franks, presidenta de Cyber Civil Rights Initiative, exponía en su artículo que el abuso en realidad virtual es 'mucho más traumático que en otros mundos digitales' (Franks, 2021).

Según la investigación de 'The Extended Mind', en el que se documentaron ataques sexuales, de género, raciales, étnicos, religiosos y homofóbicos, muchos de las víctimas no volvieron a la experiencia virtual. Los resultados de acoso no solo se limitaron a las

mujeres, ya que se detectó contenidos racistas u homófobos para el 30% de los hombres y el 20 % experimentó comentarios violentos o amenazas en la plataforma de Belamire (Franks, 2021).

Los riesgos en el metaverso podrían exacerbarse dependiendo de cómo se gobiernen estos espacios digitales, ya que existen riesgos de contacto no deseado como en redes sociales, como Instagram, Facebook o Whatsapp. Mensajes no deseados, imágenes o emoticonos aunque aún es un desafío que puede desembocar en crímenes denunciables, esto se podrá incrementar si al ingresar al espacio virtual de alguien y 'acercarse' al usuario se siente más real. A través de la tecnología háptica, los riesgos se sentirán más cercanos, ya que como hablamos en el apartado de las tecnologías hápticas, muchas empresas están tratando de implementar el tacto a través de herramientas como los guantes (Franks, 2021).

Concernidos sobre el comportamiento de ciertos usuarios, las empresas están ya implementando funciones de moderación de contenido que tienen en cuenta el control, la voluntad y el consentimiento del usuario. En la conferencia F8, Oculus marca que tiene una gran importancia en el mundo de realidad virtual expresaba que estaba protegiendo el espacio virtual de los usuarios, por ejemplo, existe una burbuja de seguridad en la cual si se sobrepasa por un usuario ajeno a esa burbuja ambos avatares se volverán invisibles entre sí.  Otras configuraciones es a través de silenciar el avatar de otro usuario para que esté desaparezca por completo, moderadores que puedan avisar a la policía, o presionar 'pausa' si el usuario se sintiese incómodo (Franks, 2021).

La prevención será cada vez más importante a medida que los escenarios virtuales evolucionen, más allá de lo ya creado para las actuales redes sociales.

## Fraudes y engaños

Como ya hemos hablado durante este trabajo el auge de las criptomonedas y NFT, que converge bajo la estructura del Blockchain, puede suponer otro desafío en cuanto a la proliferación de contenido y actividades dañinas en Internet.

Y es que  pesar de que la tecnología Blockchain es segura, no es completamente inmune a las vulnerabilidades. Además, al estar descentralizado, no contará con un moderador o administrador para mantener el control. Con esta ausencia de autoridad, los expertos se preocupan por la forma en la que se podrá recuperar los bienes robados u obtenidos de

manera ilegal. Por otra parte, al metaverso trabajar con avatares, no se podrá identificar de manera sencilla a ciberdelincuentes (Wakas, 2022).

El metaverso se centra en gran medida en el uso de criptomonedas y tokens no fungibles (NFTs), que pueden ser objetivos para los ciberdelincuentes. Y es que al igual que en la vida real las piezas de arte se pueden verificar y falsificar, esto también puede ocurrir en el metaverso, engañando a coleccionistas de NFTs. Ya existen maneras de verificar y autentificar las selecciones de NFT, a través de un proceso denominado 'minting' y que da una mayor seguridad al coleccionista (Davies, 2021).

El dinero mueve el mundo, y las criptomonedas lo harán en el mundo digital. El material económico se podrá destinar a buenas acciones e inversiones o podrá dedicarse a actividades corruptas como vemos en el siguiente ejemplo de la revista Rolling Stone:

En Roblox, una plataforma de videojuegos en línea, se han encontrados clubes de striptease, en los que jóvenes, en su mayoría, menores de edad, representan la sexualidad de los adultos. Se conoce de un caso, en que Katie usuaria de 16 años de Roblox, da vida a un personaje 'Valarie' que viste con un top corto y pantalones cortos que se da a conocer en twiter con este mensaje: *"¡HOLA CHICOS! Soy Valarie y soy una stripper de Roblox ", dice el tuit. "Bailaré contigo y tendré sexo contigo gratis, así que envíame un mensaje privado <3"* (Dickson, 2021).

No es la primera usuaria que ofrece estos servicios y en muchos casos son a cambio de la moneda virtual, 'Roblux' que se puede transformar a dinero del mundo real. Las criptomonedas son una opción popular para aquellos que persiguen contenido de abuso sexual infantil, y al ser descentralizadas e independientes de las instituciones financieras, proporciona anonimato (*The Child Explotation Economy*, 2021).

El papel de las monedas digitales en el metaverso será crucial ya que es probable que sea el protagonista del pago y venta en la plataforma. Es por ello que el pago y los incentivos financieros que puedan conducir a la proliferación del contenido dañino puedan aumentar en tamaño y complejidad en esta nueva dimensión (*The Child Explotation Economy*, 2021), además de un mayor riesgo por el seguimiento y la retención de datos biométricos.

Entre 2020 y 2021, el robo de criptomonedas aumentó un 516% correspondiendo a 3200 millones en criptomonedas. (Stroud, 2021) Blockchain sería fundamental para desarrollar el metaverso, pero a pesar de la seguridad económica que anuncia Blockchain, analistas han expresado riesgos como billeteras pirateadas, lavado de dinero y diversas estafas (*The risk of fraud in the metaverse*, 2022).

Cualquier juego con una economía, donde se puedan comprar y vender cosas, estará sujeto a una gama de regulaciones y será necesario la implementación de la ciberseguridad, la privacidad y la protección del consumidor. Así lo exponía Stonehouse, que ve necesario un control para establecer y hacer cumplir las regulaciones (Staff, 2022).

## Ciberataques

Para adentrarnos en el mundo de los ataques cibernéticos es necesario comprender de qué se tratan. Un ataque cibernético es un ataque protagonizado por ciberdelincuentes en el que utilizan uno o varios ordenadores contra otros ordenadores o redes. El ataque tiene como función principal deshabilitar ordenadores de manera malintencionada, robar dato o usar un ordenador como punto para poder lanzar más ataques. Los ciberdelincuentes utilizan diversas técnicas para realizar estas amenazas como puedes ser el malware, phising o ransomware entre otros métodos (*The Global Risks Report 2020*, 2020).

Los ataques cibernéticos se han calificado como el quinto riesgo según World Economic Forum en 'The Global Risks Report 2020' tanto en los sectores públicos como privados. Esto sigue aumentando en 2022, y se espera que los ataques cibernéticos se dupliquen para 2025. Además este informe establece que la tasa de detección o enjuiciamiento de estos ataques es de un 0,05 por ciento en Estados Unidos (*The Global Risks Report 2020*, 2020).

La pandemia amplificó el ciberdelito, y es que el delito dicbernético que incluye desde el robo, malversación, piratería hasta destrucción de datos aumentó un 600% a nivel mundial (*UN Warns Cybercrime on Rise during Pandemic*, 2020). Y es por eso que muchas industrias han tenido que reinventarse y adoptar nuevas soluciones.

Dado que el metaverso traerá consigo muchos desafíos para la ciberseguridad, es necesario implementar estrictas medidas y protocolos de ciberseguridad. El phishing es uno de los problemas a los que se enfrenta la sociedad actual y muy probable se expandirá al metaverso. Los ciberdelincuentes que practican phising priorizan ataques fáciles y rentables y con un alto potencial para atrapar a víctimas. Nos encontramos con el phishing de bajo coste y de una red más amplia, y el sopear phising que tiene un mayor coste pero el objetivo es de un mayor valor (*Email Statistics Report,* 2018).

Muchas de las estafas phising se dan a través del correo electrónico, y es posible que a veces podamos verificar la dirección del correo electrónico pero son muchos casos en los cuales se asume que los emails que recibimos son buenos y correctos. Y esto es debido a que recibimos un promedio de 121 correos diarios solo para el trabajo (*Email Statistics Report,* 2018). Miles de millones de correo electrónicos se envían tratando de robar información, lo que suma que más del 90% de los ataques comienzan con un correo electrónico (Yong, 2020). Con el aumento de ataques de malware o phising es necesario difundir métodos de prevención y concienciar sobre los mismos problemas.

Otro de los problemas del metaverso es su dependencia del hardware para experimentar la realidad virtual. El metaverso se centra en dispositivos externos, como cascos de realidad virtual o guantes hápticos, que pueden caer fácilmente en manos de piratas informáticos si no se protegen.

Los datos que se pueden capturar a través de estos dispositivos pueden ser de naturaleza sensible y pueden convertirse en amenazas o material de chantaje por un ciberdelincuente. La propiedad intelectual será más complicada de proteger si las personas no solo viven en el mundo real sino que también en el metaverso (Davies, 2021).

En definitiva, el metaverso aumenta la superficie de ataque. Al tratarse de una convergencia de diferentes tecnologías obliga a proteger dispositivos físicos, redes y sistemas para la comunicación.

## Privacidad

En un mundo en el que la innovación está a la orden del día, cuando una nueva tecnología invade el mercado, se le puede denominar como perturbadora o disruptiva. Esto lo hemos podido encontrar con tecnologías que superan a las ya establecidas y normalizadas. Suplantar nuestra identidad es un riesgo muy importante y que concierne a la seguridad de cada persona (Sánchez, 2022).

Así como Internet creó desafíos para la seguridad y privacidad, el metaverso agregará mayores y más difíciles desafíos. Los expertos en seguridad se preocupan por el acoso, a intimidación y el comportamiento que personas puede ejercer en los mundos de realidad virtual. El metaverso también podrá impulsar formas para la manipulación (Magid, 2022).

Es importante que los usuarios sean conscientes de que la forma en que se comparten los datos en los mundos digitales deberá considerarse con más cuidado para garantizar así la privacidad de los mismos. Antigone Davis, directora global de seguridad de Meta explicaba: '*Contribuir al metaverso de manera responsable requerirá investigación, colaboración e inversión en seguridad en lo que respecta a XR. Por ejemplo, estamos invirtiendo en controles que permiten a los usuarios administrar y reportar contenido y conducta problemáticos, así como herramientas de seguridad diseñadas para experiencias inmersivas. Pero no podemos hacer esto solos. Para abordar la seguridad de manera integral a medida que emerge el metaverso, necesitamos asociarnos con otros en el gobierno, la industria, la academia y la sociedad civil'* (Lalani, 2022).

*Por otra parte,* el experto en derechos humanos Brittan Heller, en su artículo *'Reimagining Reality: Human Rights and Immersive Technology 'que una nueva calidad de información que se compone de su identidad real combinada con estímulos, lo que indica lo que puede pensar, gustar y desear de manera única* (Siddique et al., 2020)' y habla del concepto de '*psicografía biométrica'* y analiza las implicaciones potenciales de la nueva recopilación de datos con tecnologías para los derechos humanos, la privacidad y la autocensura.

Para empezar, el uso de dispositivos de realidad virtual que recopilan grandes cantidades de datos e información del usuario da lugar a un gran atractivo para ataques de hackers. Es probable que con la llegada del metaverso se necesiten recopilar más datos de los usuarios, lo que puede vulnerar la privacidad de los usuarios (Wakas, 2022).

La manipulación que se ha llegado a realizar sobre una imagen o sobre un vídeo alterando tanto lo que las personas vemos como lo que los protagonistas dicen se denomina *deep fake* (*Deepfakes*, 2020). En vista de que el *deep fake* ha supuesto una amenaza para altos cargos o personas conocidas mundialmente, a través de la facilidad de crear videos falsos y difundirlos por redes sociales, no podemos negar que el miedo a que puedan modificar o alterar nuestro avatar exista (Sauliere, 2021). La información que pueda captar el metaverso sobre los usuarios es íntima y permite rastrearles de manera más profunda. Las empresas pueden monitorear respuestas fisiológicas y datos biométricos como expresiones faciales, inflexiones vocales y signos vitales en tiempo real mientras los participantes se encuentren en el metaverso. La publicidad entonces será cada vez más dirigida y personal para el usuario debido a la gran captación de información.

¿Y todo esto cómo quedará regulado?

Podría decirse que el Reglamento General de Protección de Datos de la Unión Europea (GDPR, 2019) puede ofrecer un acercamiento a la forma en que puede estar regulado, pero dada la naturaleza novedosa del metaverso, es probable que muchas de las acciones o actividades que se puedan dar en el metaverso no estén reguladas ni existan los procesos específicos para regir el consentimiento y el procesamiento de datos.

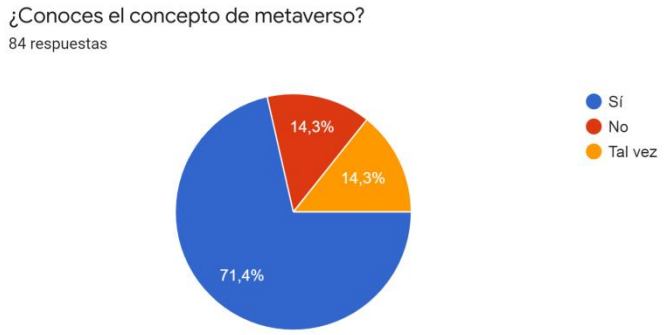
Además, tras la demanda a Facebook por no proteger los datos personales de los usuarios y el mal uso de la información no sitúa en buena posición a la plataforma. (Criddle, 2020). Esto se remonta a 2011, en que Facebook estuvo 4 años usando datos personales de los usuarios para negociar y manipular a competidores. Esto suponía además de engañar a los usuarios sobre su privacidad, también monetizar su información y atentar contra la libre competencia, ya que de esta forma se favorecía a determinadas empresas, como por ejemplo, Amazon. Este fue el famoso caso de Cambridge Anlytuca, el escándalo que involucró datos de casi 1500 millones de usuarios de Facebook en Inglaterra y Gales para publicidad durante las elecciones. Este caso, revelado en 2018, prometió un cambio por parte de Facebook, en el que alegaba que realizaría cambios en el tratamiento de los datos para ofrecer un mayor respeto y seguridad para sus usuarios que se desmienten a través de filtraciones de empleados de Facebook, demuestran que más allá de realizar estos males, eran conocidos por la compañía y realizados con alevosía (McDougall, 2022).

## Resultados del análisis

El cuestionario ha sido respondido por 84 personas por hombres y mujeres para conocer su opinión sobre la realidad virtual del metaverso y sobre asuntos concernientes al mismo.

En primer lugar, analizaremos las 3 primeras figuras del sector de la encuesta, ‘concepto de metaverso’, para analizar los conocimientos y visión de las personas sobre el metaverso, y cómo de lejana ven su implementación en la vida de las personas.

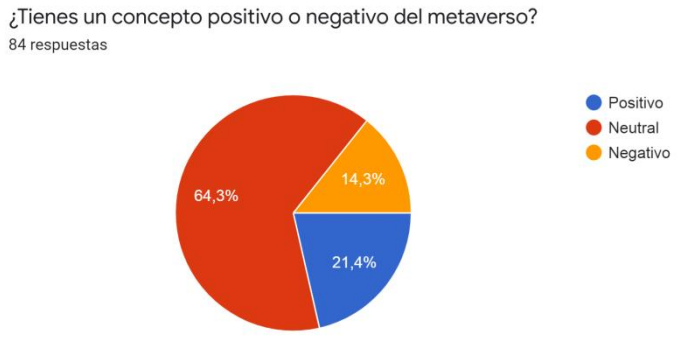
***Figura 1: Concepto de metaverso***




Fuente: Elaboración propia a partir de los datos de la encuesta

El 71,4% de los encuestados conocen el concepto del metaverso, mientras que el 14,3% no habían escuchado el concepto y han tenido que buscarlo para responder a las posteriores preguntas. En consonancia con ambos, y con el mismo porcentaje que la proporción de participantes que no lo habían escuchado, un 14,3 % responde con que tal vez conozcan el concepto.

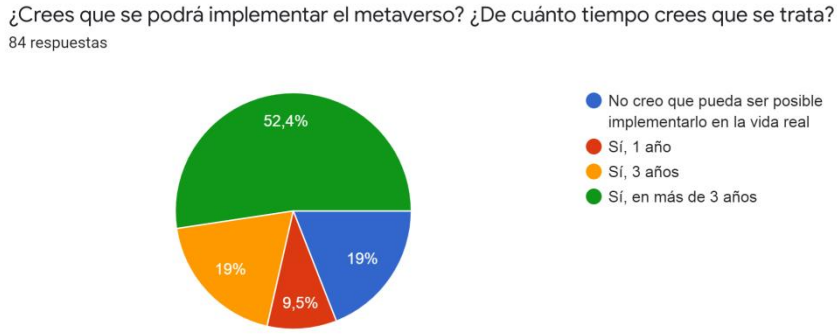
**Figura 2: Valoración del concepto**




Fuente: Elaboración propia a partir de los datos de la encuesta

En el caso de la valoración del concepto que los encuestados tienen del metaverso, un 64.3% se muestra neutral. El concepto positivo del metaverso corresponde a un 21,4%, mientras que el concepto negativo se le otorga un 14,3%.

**Figura 3: Implementación del metaverso**




Fuente: Elaboración propia a partir de los datos de la encuesta

Siguiendo con las opiniones sobre el metaverso, se vio necesario preguntar a los usuarios si pensaban que esto sería una idea realista de implantar en la sociedad, en la que un 19%, considero que esto no sería posible, conformando más de las terceras partes de los encuestados (80,9%) que coinciden en que esto sería posible. Más de la mitad de los encuestados (52,4%) acuerdan que se podrá implantar en más de 3 años, mientras que un 19% opina que en 3 años ya podría ser implementado. Por último, y contando con el porcentaje menor (9,5%), se encuentran aquellos que opinan que el metaverso se podrá implementar en 1 año.

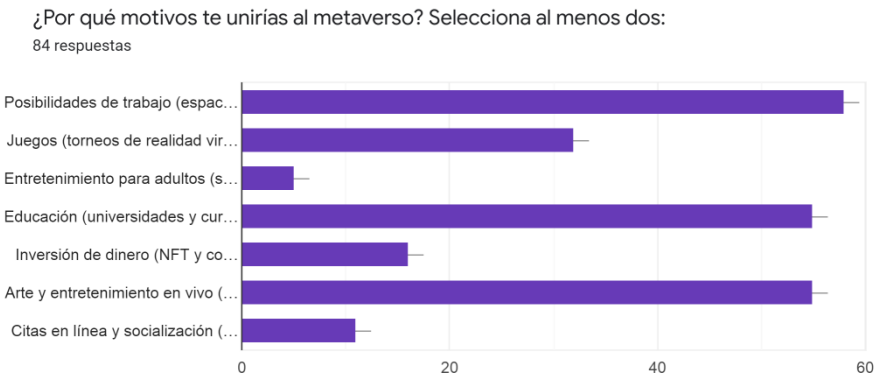
En segundo lugar, nos encontramos en el segundo sector de la encuesta: 'ser parte del metaverso', en que los encuestados nos expondrán si serían usuarios de este mundo virtual y cuáles serían los motivos para ello.

***Figura 4: Formar parte del metaverso***


Fuente: Elaboración propia a partir de los datos de la encuesta

Se observa que casi la mitad de los encuestados responden de manera ambigua a la pregunta, expresando que tal vez serían usuarios del metaverso si contaran con las herramientas para ello. Es interesante, además, analizar que hay un mayor porcentaje, casi el doble que las personas que no formarían parte del metaverso (17,9%), que responden de manera afirmativa a ser parte del mundo virtual, contando con un 34,5% de los encuestados.

***Figura 5: Motivos por el que ser parte del metaverso***

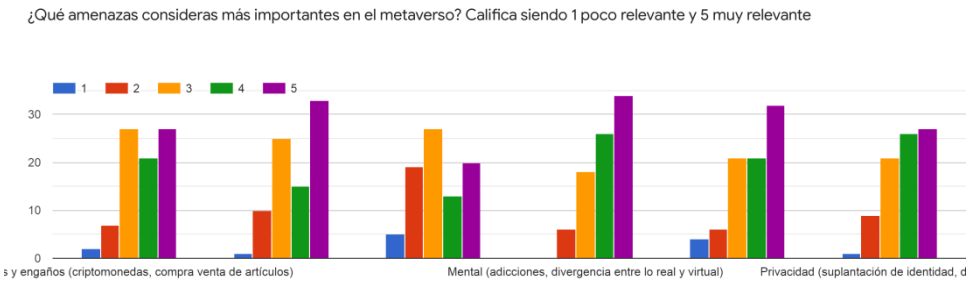



Fuente: Elaboración propia a partir de los datos de la encuesta

En cuanto a los motivos por los que ser parte del metaverso encontramos una variedad de opiniones, siendo el motivo más elegido las posibilidades de trabajo que puede ofrecer, respondido por 58 personas (69%). Le siguen con el mismo porcentaje (65,5%), la posibilidad de implementar herramientas para la educación o disfrutar del arte y entretenimiento en el metaverso. Por otra parte, con casi un 40%, 32 personas han expresado que un buen motivo para unirse al metaverso sería la posibilidad de jugar a juegos de realidad virtual. El 19% corresponde a los encuestados que utilizarían el metaverso para realizar inversiones de dinero, ya sea a través de la compra y venta de NFT o criptomonedas. En el eslabón final nos encontramos con lo relativo al contacto con otros usuarios, con un 13,1% para aquellas personas que encuentran un motivo interesante el hecho de poder tener citas online o socializar con otros usuarios, y un total de 5 personas que respondieron expresando que lo que para ellos sería uno de los motivos para unirse al metaverso sería entretenimiento para adultos, como striptease virtuales o porno en línea.

A continuación, nos encontramos con la tercera fase de la encuesta en la que se pregunta por las posibles amenazas que opinan que pueden encontrar en el metaverso, y la importancia que le adhieren. Además, una pregunta estará dedicada a lo que los encuestados consideran que debe estar censurado o restringido en el mundo virtual.

***Figura 6: Importantes amenazas para el usuario***




Fuente: Elaboración propia a partir de los datos de la encuesta

La importancia de cada amenaza para el encuestado ha sido puntuada del 1 al 5, siendo 1 poco relevante y 5 muy relevante.

La primera variante a analizar son fraudes y engaños, y que cuenta con la mayor puntuación entre el 3 y el 5, siendo considerada una gran amenaza, pero al estar su puntuación repartida entre o últimos números lo calificaremos como una amenaza media-alta.

La segunda variante, ciberataques, conserva su mayor puntuación en el número 5, siendo votado por 33 participantes, a diferencia de las votaciones entre el 1 y 2 que muestran un total de 11 participaciones en total. En el medio encontramos un total de 25 usuarios que puntúan con un 3. La variante se califica como media-alta.

La amenaza física tiene su puntuación más repartida, siendo la votación en el 1, de 5 personas, en el 2 de 19, en el 3 de 27, en el 4 de 13 y en el 5 de 20. Se observa que la amenaza física es media.

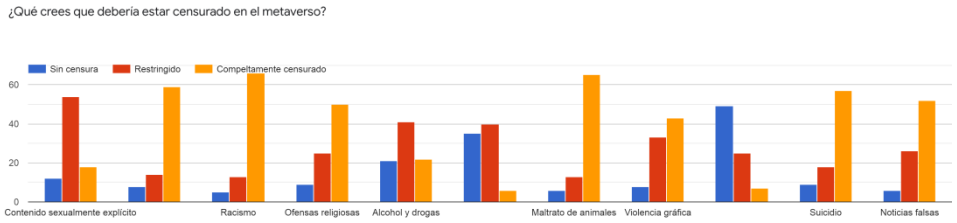
En cuanto a la amenaza mental, es decir, adicciones o divergencia entre lo real y virtual se visualiza que no existe ninguna puntuación en muy poco relevante (1) y que las demás, van incrementándose, siendo la más alta la de muy relevante (5) con 34 votaciones. Se considera esta variable con media-alta.

Asimismo, con la amenaza social ocurre similar, ya que la puntuación dada por los participantes va en aumento, y consigue que entre la puntuación 3 y 5 haya 74 votos lo

que corresponde a más de tres cuartas partes de los votantes. Esta variable se considera alta.

La privacidad encuentra los votos más dispersos en los que se encuentra un gran número de votos entre el 3 y el 5, por lo que obtenemos que se trate de una amenaza media-alta.

***Figura 7: Sin censura, restringido o completamente censurado en el metaverso***




Fuente: Elaboración propia a partir de los datos de la encuesta

1. Contenido sexualmente explícito
2. Hacerse pasar por otra persona
3. Racismo
4. Ofensas religiosas
5. Alcohol y drogas
6. Contacto físico con otro usuario
7. Maltrato de animales
8. Violencia gráfica
9. Tener una relación online
10. Suicidio
11. Noticias falsas

En esta sección dividiremos las amenazas que los usuarios exponen que deben estar permitidos, censurados o restringidos completamente.

Las amenazas en las que se comparte una opinión más clara sobre aquellas que deberían estar completamente restringidas son: hacerse pasar por otra persona, el racismo, ofensas religiosas, maltrato animal, suicidio, violencia gráfica y noticias falsas.

Lo que los encuestados consideran que debería estar restringido, sin estar completamente vetado de la plataforma es: contenido sexualmente explícito, alcohol y drogas y contacto físico con otro usuario. Tiene una gran relevancia en cuanto a

puntuación de los usuarios, aun siendo menor que lo completamente restringido en violencia gráfica y noticias falsas.

Por otra parte, la opinión que gana en cuanto a algo sin restricciones en el metaverso es tener una relación online. También comparte una fuerte puntuación aun siendo algo más bajo que lo restringido, en el contacto físico con otro usuario.

En el general de las puntuaciones la que más votaciones ha demostrado ser la que los usuarios vetarían completamente de la plataforma es el racismo con 66 votaciones. Le sigue el maltrato animal con 65, y el suicidio con 57.

La máxima puntuación en aquello restringido pero no censurado completamente es en contenido sexualmente explícito con 54 votos, alcohol y drogas con 41 votos y por último, el contacto físico con otro usuario con 40 votos.

Para finalizar, lo permitido por los usuarios en el metaverso cuenta con una puntuación de 49 votos tener una relación online. Junto a esto también tiene una gran relevancia el contacto físico con otro usuario que cuenta con 35 votos.

***Figura 8: Criminales en el metaverso***


Fuente: Elaboración propia a partir de los datos de la encuesta

En esta pregunta, se da una gran variedad de opiniones dividida muy similarmente. En respuesta a si piensan que los criminales registrados como asesinos en serie o agresores sexuales deberían vivir sus impulsos en lugares restringidos del metaverso para que la sociedad sea más segura un 36.9% no expone ninguno de los dos extremos de respuesta a la pregunta, ya que responde con un 'No estoy seguro'. Por otra parte, se da un mayor porcentaje con un 35,7% de los usuarios en que comparten que puede tratarse de una buena idea, mientras que un 27,4% exponen que esto solo reforzará sus impulsos y empeorará las cosas.

## 5. Conclusiones y propuestas

### Conclusiones

Observando la diversidad de respuestas recibidas, se recogen las siguientes ideas.

En primer lugar, es interesante conocer que a pesar de la repercusión de meta de Facebook u otras plataformas, no todos los encuestados han escuchado sobre ella, por lo que existe una gran desinformación sobre este mundo virtual, y por tanto, no existe realmente una opinión formada sobre el mismo. Es por ello, que más de la mitad de los encuestados expresan que su percepción sobre el metaverso es neutral, y eso puede ser debido a que no existe la información suficiente para que formen una opinión, o que simplemente no le otorgan la importancia necesaria porque no consideran que esto sea posible de implantar

Cuando le pregunto a los encuestados cuáles serían los motivos por los que se unirían al metaverso, son la mayoría los que responden que los mayores motivos son las posibilidades de trabajar, educación y entretenimiento en vivo. Tras los efectos del Covid-19, millones de personas alrededor del mundo ha tenido que rehacer su vida y adaptarse a esta nueva crisis sanitaria mundial. Esto ha afectado a todos los ámbitos de la vida de las personas, comenzando con cómo se relacionan, en qué emplean su tiempo libre, estudios y trabajo entre otras cosas. Las personas han podido darse cuenta de la importancia de la tecnología y las facilidades que en tiempos de crisis pueden facilitar, y se ha visto reflejada en esta votación, ya que el teletrabajo, conciertos o entretenimiento online o la educación a distancia ya forman parte de nuestra vida diaria y es muy probable que esto sea solo el principio. Además, también hay un gran porcentaje de los encuestados que dotan de una gran importancia a los juegos, en cuanto a torneos en realidad virtual y a las inversiones de dinero. Y es que a día de hoy, más de 3 mil millones de personas en todo el mundo juegan a videojuegos en su tiempo libre, lo que hace un total de casi el 40% de la población mundial, según un informe de DFC Intelligence (Mason, 2020), y las criptomonedas cada vez son más populares, con casi 4,4 millones de inversores solo en España (*Casi 4,4 millones de españoles invierten en criptomonedas, pese al desconocimiento general*, 2022*).*

En cuanto a que amenaza del metaverso es considerada como más relevante para los encuestados es la amenaza mental, seguida por los ciberataques y en tercer lugar, las amenazas a nivel social. Las adicciones y la convergencia entre el mundo real y virtual

es una de las preocupaciones de las personas, y esto puede ser debido a que la media global de uso de ordenadores o smartphones es de 6 horas y 54 minutos, con el máximo en Filipinas con 10 y 56 minutos de media al día según el informe Digital 2021 Global Overview Report. (Roa, 2021), esto puede ser más alto si adentramos más aspectos de nuestra vida en un mundo virtual. Asimismo, esto se relaciona mucho con el tercer factor que ha sido protagonista, el aislamiento y la irascibilidad, son consecuencias directas de una adicción a diversas plataformas. Además, no es difícil encontrar los ciberataques como una preocupación o un futuro desafío debido a la multitud de información que el metaverso podrá manejar de los usuarios y esto puede ser un gran aliciente para los ciberdelincuentes.

En cuanto a las amenazas percibidas por los encuestados, la mayoría de las propuestas serían vetadas del mismo, aunque hoy en día muchas de estas están presentes en plataformas de renombre. El maltrato animal, el racismo y el suicidio, son aquellas más votadas por la toxicidad y la negatividad que podrían traer a la plataforma. Es también interesante, recoger que la opinión que muchos de los encuestados comparten en no vetar en absoluto es el contacto con otro usuario, a pesar de lo que se ha estudiado en otro apartado del estudio de las amenazas, en que el contacto físico con otro usuario puede resultar ser uno de los mayores desafíos del metaverso. Alcohol y drogas y contenido sexualmente explícito destacan en cuanto a lo restringido, ya que los encuestados no lo consideran un peligro para los usuarios del metaverso, y puede deberse a la normalización en películas o en plataformas de internet de este contenido.

Por último, analizando la pregunta de: '¿Crees que los criminales registrados (como asesinos en serie y los agresores sexuales) deberían vivir sus impulsos en los espacios restringidos para que la sociedad sea más segura como resultado? se da una diversidad de opiniones. Creo que es significante que sea mayor porcentaje dedicado a que podría ser una buena idea más que a que reforzaría sus impulsos y empeoraría las cosas. No es fácil encontrar la respuesta a esta cuestión, es debido a esto que donde se encuentra el mayor porcentaje de la puntuación es en el 'No estoy seguro'. Ya se conocen de casos en que se dan violaciones y acoso en el metaverso, y no existe una línea segura de como imponer penas a estos ciberdelincuentes.

La presente investigación ha permitido indagar en las amenazas que desafían las nuevas cuestiones que conforman el metaverso. El trabajo evidencia las posibles amenazas del metaverso y su convergencia con las diversas tecnologías emergentes integradoras e igualmente realizar una investigación a través de una encuesta para conocer las

principales opiniones sobre esta realidad virtual y las posibles amenazas que consideran importantes si fuesen usuarios de la plataforma (Stanley, 2021).

El metaverso ofrece una infinidad de posibilidades, y esto debe comprender un espacio seguro para los usuarios de la plataforma, pero para ello debe estar regulado y tener límites establecidos. El metaverso cada vez cobra mayor importancia para las empresas, y las menciones del mismo, tras el cambio de nombre de Facebook a Meta, ha aumentado de manera considerable. Dado que los riesgos digitales ya son altos, los riesgos de seguridad podrían ser más frecuentes y diversos en el metaverso, así como sus posibilidades para las empresas. Pero aun así, existe una gran desinformación sobre las oportunidades y los riesgos de lo que puede suponer esta realidad virtual, y lo hemos visto presente en la encuesta de investigación realizada en la que muchas personas respondían de manera ambigua. Además, hemos analizado que muchas de las personas encuestadas no confían que esto sea algo que pueda ser establecido a corto plazo, pero probablemente sea el futuro de las conexiones móviles.

Todo esto conlleva una gran responsabilidad para los desarrolladores, que deben encargarse de que sus plataformas no supongan un peligro para el usuario. Las herramientas a utilizar proporcionarán una experiencia muy real, y lo que vivan en el mundo virtual debe estar regulado y proporcionar límites. No solo lo que ocurra en el metaverso es asunto de los empresarios, también lo es su repercusión cuando los usuarios salgan de este mundo, sin olvidar que puede tener repercusiones en su vida real. Los escándalos en privacidad de Facebook, o su conocimiento de que las redes que posee son tóxicas y adictivas para los consumidores hace que muchos de los usuarios se planteen realmente si confiar en el metaverso que Facebook promete.

El reto entonces se encuentra en una continua adaptación a los nuevos desafíos que nos propone el mundo virtual, comprendiendo asuntos relativos a la privacidad, en que la lucha por la prevención de ciberataques es cada vez una preocupación considerable y que demandan las empresas. Asimismo, es importante la lucha por la salud mental, física y social y crear planes de prevención para tener en cuenta las repercusiones que pueden tener en los usuarios que comienzan a utilizar el metaverso como otra forma de ocio. El dinero virtual también configura otro desafío, y es que el auge de las criptomonedas también ha conformado otra vía para cometer delitos. Es innegable que el metaverso usará de esta tecnología digital monetaria para sus transacciones, compras y ventas de ítems, por lo que debe estar regulado y dirigido únicamente a lo legalmente aceptado en la plataforma virtual.

Nuevas formas de vivir vendrán de la mano del metaverso, que promete una sociedad en la que hace a todos iguales, permitiéndonos no ser juzgados por nuestra apariencia física o limitaciones, sino por lo que existe dentro de nuestras cabezas, por cómo queremos ser vistos. Vivir en un lugar más emocionante, más gratificante en el que puedes ser quien tú quieras. Sin embargo, bajo mi punto de vista, y tras la investigación en este trabajo, los mundos virtuales no son inherentemente mejores que los reales. Se conoce que la explotación de trabajadores existe en ellos, como venezolanos produciendo criptomonedas para venderlas a jugadores del primer mundo (Parkin, 2022) o en Roblox, en que jóvenes desarrolladores de juegos dedican largas horas a proyectos no regulados por una pequeña recompensa (Parkin, 2022). La misoginia, la homofobia y el racismo también existe en estos juegos, al igual que existe en el mundo real. Es por ello, que problemas del mundo real no desaparecerán si el metaverso está formado por personas. A no ser que las empresas hagan un gran esfuerzo por desmantelar los prejuicios y los sesgos inconscientes, estas actitudes se replicarán en el metaverso y las consecuencias de esto serán trascendentales para los usuarios.

## Propuestas de mejora

Las posibilidades del metaverso son infinitas, y esto es debido a que son plataformas con muchas posibilidades de crear y dirigir hacia realidades todavía desconocidas para el ser humano, pero como todo en la industria tecnológica, es necesario el control para el uso de esta plataforma de manera respetuosa y segura. A través de la búsqueda bibliográfica y la encuesta realizada, encuentro que son necesarias ciertas líneas de actuación para prevenir posibles riesgos que se puedan dar en el futuro en el metaverso:

1. **Reglas y regulación**

Si algo es necesario para el control del metaverso son reglas y regulaciones. El metaverso, tiene infinitas posibilidades y es probable que pueda funcionar de manera similar al mundo real, es decir, se podrá interactuar con otros usuarios de manera virtual, comprar y vender activos, participar en eventos sociales o trabajar y estudiar. A través de equipos tecnológicos como los guantes hápticos o las gafas de realidad virtual, la experiencia cada vez será más real. Es por ello, crucial, que existan parámetros donde los usuarios puedan convivir, ya que a pesar de que se traten de mundos descentralizados y sin una idea de gobierno, pueden existir ciertos usuarios que influyan de manera negativa y perjudicial a otros. Se pueden establecer parámetros en cuanto al

uso de lenguaje o actitudes abusivas (racista, homófobo o con carácter inicuo), el robo, la suplantación de identidad y otros delitos cibernéticos (Rees, 2022). Debe, asimismo, estar regulado aquel contenido para menores de edad, además de contenido restringido para cualquier usuario del metaverso , en la encuesta realizada se compartió la idea de vetar contenidos racistas, maltrato de animales y suicidio, lo que pueden ser ejemplos de contenidos a censurar en la plataforma. Es importante acordar una serie de normas, y sus posibles consecuencias si se incumplieran, que impidan a usuarios beneficiarse de esta tecnología a costa de realizar el mal a otros, como ya se han producido, en la violación en manada en un metaverso (Soria, 2022).

También, debe haber reglas para los anunciantes dentro del metaverso, para que no hagan del mismo un entorno desagradable y manipulador; es por ello, que no solo debe ser tarea de los usuarios obedecer las reglas, sino también de las empresas que formen parte del mundo virtual (Rees, 2022).

### 2. Protección del usuario

La protección de los usuarios, al igual que en el mundo real debe ser primordial en el mundo virtual. Dicha protección podemos encontrarla en diversas formas pero debe ser muy importante mantener la privacidad y seguridad como elemento fundamental. Además, es fundamental que los usuarios puedan informar si alguna persona parte del metaverso ha actuado de manera inapropiada, por lo que encuentro adecuado que exista la posibilidad de que los usuarios puedan presentar quejas y que sean consideradas para la protección del espacio. Esto ya se está instaurando con la función Límite personal de Meta (Meta's Personal Boundary feature), ‘que establece un radio invisible de dos pies alrededor del avatar en el que los extraños no pueden ingresar. Por lo tanto, todos tendrán una distancia de cuatro pies entre ellos y otros usuarios’ (Kaleem, 2022) y ayudará a prevenir intentos de abuso físico. Es necesario darle la importancia necesaria a este asunto ya que puede ser el objetivo de delincuentes que quieren aprovecharse de las vulnerabilidades de otros usuarios, y es por ello que los desarrolladores deben primar su seguridad.

### 3. Sanciones necesarias

Es complicado regular lo que sucede en el mundo virtual, y es más, la idea del crimen en el metaverso no es fácilmente determinable en cuanto a si se debe o se puede considerar de la misma manera que uno realizado en el mundo real. Es necesario

legislar y reglar las consecuencias de los actos que se puedan dar en el usuario para dar el control y seguridad al usuario que decida formar parte del metaverso.

### 4. Identificación del usuario

Hoy en día es fácil realizar actividades poco éticas en línea y que luego sea difícil para las autoridades localizar al autor de las mismas. Además, con la utilización de una VPN, es aún más complicado identificar al autor, e imponerle su sanción. Es por ello que considero necesario una identificación previa a acceder al metaverso, ya sea una foto del pasaporte, certificado de nacimiento o licencia de conducir para que el usuario no pueda ocultar su identidad y que evite que menores de edad entren a espacios inseguros del metaverso (Rees, 2022). Esto también puede ayudar a la preocupación creciente del robo de identidad, ya que a través de una identificación previa será más complicado que esto llegue a suceder. En el metaverso, se creará una versión digital de ti mismo, que vive por ti, lo que pone a la identidad digital en primer plano. La identidad digital, a diferencia de la del mundo real, utiliza una raíz de confianza criptográfica, en lugar de una raíz de tipo humanista. Cuando operamos en el mundo real, conoces a la persona y por tanto confías en ella. En cambio, en línea esos componentes esenciales no existen, lo que conducen a un posible fraude. La posible solución es mejorar la confianza humana con credenciales criptográficas digitales fiables. El metaverso necesita un respaldo de autenticidad, pero eso no significa que la anonimidad deba de ser restringida, sino que cada personaje del metaverso debe estar respaldada por la identidad de una persona real, es decir, solo se le podrá dar acceso a la plataforma si está autenticado como un individuo real. La identidad digital autenticada asegura que los usuarios tratan con personas reales en un mundo virtual. Verificar que las personas son reales reduce el fraude y los problemas de identidad que surgen con cada interacción en línea (Lucatch, 2021).

### 5. Restricción del uso

La divergencia entre lo real y lo virtual es una de las preocupaciones de los encuestados de la investigación analizada previamente. Si contamos con que la realidad a la que el usuario se inmersa es más agradable que su propia vida puede generar que la persona quiera dar vida únicamente a su avatar y olvidarse de su vida real. La adicción puede ser un problema, y existe el peligro de un uso excesivo si no se establecen limitaciones. Encuentro difícil poder impedir completamente que una persona no pueda utilizar el

metaverso si sus niveles de actividad son demasiado altos, pero se pueden establecer advertencias y sugerencias sobre su uso, y establecer límites, como ya hacen otras aplicaciones como Instagram o Youtube (Rees, 2022).

## 6. Concienciación en ciberseguridad

La ciberdelincuencia es una amenaza que cada vez preocupa más a las empresas. El coste medio de la ciberdelincuencia para una organización ha aumentado en 1,4 millones de dólares en el último año, hasta llegar a 13 millones de dólares, siendo el número medio de infracciones de seguridad de un 11%. Cada vez surgen nuevas amenazas y formas de atacar a las grandes compañías para su filtración de datos a través de herramientas sofisticadas de ingeniería social, y todo lo que se necesita es que un empleado pulse en un enlace malicioso. Los empleados de la compañía deben ser la primera línea de defensa contra los ciberataques, por lo que es necesario una formación para capacitar a los usuarios sobre posibles amenazas y que eviten situaciones que puedan poner en riesgo la organización (*Plan de concienciación de seguridad informática*, 2019). Para luchar contra los ciberataques se debe concienciar sobre estas amenazas para que los trabajadores sean capaces de discernir entre un correo bueno o malo o ficheros perjudiciales y que favorecen al robo de información.

## 7. Alfabetización mediática y digital

La nueva sociedad digital requiere de crear una cultura de ciberseguridad, para alertar a los ciudadanos de las posibles amenazas que se ejecutan en la red, así como las nuevas posibilidades tecnológicas, las redes sociales, aplicaciones o asistentes de voz. La alfabetización mediática es la posible solución que encuentro para subsanar estas amenazas, que se define como 'la capacidad de acceder, analizar, crear y actuar utilizando todas las formas de comunicación. Desde interpretar emojis, hasta comprender los mensajes subliminales en anuncios, producir vídeos virales o reconocer la publicidad nativa.' (Álvarez, 2021). Los usuarios de Internet no son consciente del impacto de sus acciones, ni de la susceptibilidad a la que nos vemos sometidos de ser sometidos por parte de los medios digitales. Por eso es necesario enseñar una cultura de ciberseguridad que enseñe desde edades tempranas, a través de la incorporación en los colegios, del uso seguro y saludable de la tecnología, ya sea para aprender a buscar información de manera fluida, crear y compartir contenido y diferenciar la información verdadera de la falsa. Esto último es necesario debido a la cantidad de información que

está a nuestra disposición, y que en muchas ocasiones pueden tratarse de ‘fake news’ que buscan la manipulación de pensamiento con el objetivo de confundir o alterar la opinión de las personas (Álvarez, 2021).

En conclusión, el metaverso ofrece la oportunidad de explorar mundos que solo hemos imaginado, pero esto no se podrá dar de manera segura si no se establecen ciertos límites conjugados con reglas y regulaciones. Se debe hacer del metaverso un lugar seguro en el que se proteja al usuario de amenazas y riesgos generados de la misma plataforma.

## 6. Glosario

**Blockchain**: ‘Blockchain, o cadena de bloques, es un libro de contabilidad digital distribuido que almacena datos de cualquier tipo. Una cadena de bloques puede registrar información sobre transacciones de criptomonedas, propiedad de NFT o contratos inteligentes DeFi. Si bien cualquier base de datos convencional puede almacenar este tipo de información, *Blockchain* es única, al estar totalmente descentralizada y no depender de ningún organismo’ (*Qué es el blockchain: definición, tipos, ejemplos, ventajas y utilidades*, 2021).

**Ciberataque:** ‘Un ciberataque es un conjunto de acciones dirigidas contra sistemas de información, como pueden ser bases de datos o redes computacionales, con el objetivo de perjudicar a personas, instituciones o empresas’ (*Ataques cibernéticos,* 2021).

**Criptomonedas**: ‘La criptomoneda o criptodivisa es un tipo de moneda digital que utiliza la criptografía para proporcionar un sistema de pagos seguro. Estas técnicas de cifrado sirven para regular la generación de unidades monetarias y verificar la transferencia de fondos. No necesitan de un banco central u otra institución que las controle’ *(*Ferre, 2022*).*

**(Metaverso) Descentralizado**: ‘Se considera como una propiedad colectiva respaldada por la comunidad y usuarios independientes de manera descentralizada ni control corporativo’ (Bastón, 2021).

**Inteligencia artificial: ‘**La inteligencia artificial (IA) se refiere en términos generales a cualquier conducta humana que desarrolle una máquina o sistema. En la forma más básica de inteligencia artificial, los PC están programados para «imitar» la conducta humana utilizando amplios datos de ejemplos previos de conductas similares. Este enfoque puede englobar desde reconocer diferencias entre un automóvil y un ave hasta realizar actividades complejas en una fábrica’ (*¿Qué es la inteligencia artificial?*, 2019).

**Malware**: ‘Hace alusión al software malicioso que incluye virus y gusanos. Básicamente, lo que hace es aprovechar las vulnerabilidades para infringir las

redes y suele atacar cuando un usuario hace clic en un enlace o en un archivo adjunto a un email' (*Ataques cibernéticos*, 2021).

**Metaverso**: 'El metaverso es una red de entornos virtuales siempre activos en los que muchas personas pueden interactuar entre sí y con objetos digitales mientras operan representaciones virtuales, o avatares, de sí mismos' (Ratan y Lei, 2021).

**Phising**: 'El phishing consiste en el envío de mensajes fraudulentos, usualmente a través de correo electrónico, que aparentemente proceden de fuentes fiables y seguras. El principal objetivo de este tipo de ciberataque es robar datos personales muy sensibles, como información sobre inicios de sesión o datos de tarjetas de crédito, entre otros' (*Ataques cibernéticos*, 2021).

**NFT**: '*Non Fungible Token* o Tokens no fungibles, en castellano, que viene a ser un certificado digital de autenticidad que mediante la tecnología blockchain, la misma que se emplea en las criptomonedas (los tokens), se asocia a un único archivo digital' (*Qué es un NFT y cómo funciona*, 2022).

**Realidad virtual:** 'La tecnología de Realidad Virtual consiste en la inmersión del usuario en un mundo completamente sintético generado por ordenador, en el que sus sentidos dejan de percibir el mundo real, sumergiendo al usuario en un entorno alternativo con la ayuda de gafas de realidad virtual o guantes hápticos' (*Realidad virtual*, 2022).

## 7. Bibliografía


Silamani, J. (2015). *Utilidad y tipos de revisión de literatura*. Utilidad y tipos de revisión de literatura. https://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1988-348X2015000200002#:%7E:text=La%20revisi%C3%B3n%20bibliogr%C3%A1fica%20se%20ha,publicaci%C3%B3n%20o%20un%20trabajo%20espec%C3%ADfico.

Westreicher, G. (2020, 7 mayo). *Encuesta*. Economipedia. https://economipedia.com/definiciones/encuesta.html

Ahmed, A. (2021, 15 diciembre). *A Recent Survey Reveals Consumers Thoughts On The Metaverse And Its Potential Future*. Digital Information World. https://www.digitalinformationworld.com/2021/12/a-recent-survey-reveals-consumers.html

Orellana, R. (2022, 12 febrero). *Qué es el metaverso y quiénes lo impulsan*. Digital Trends Español. https://es.digitaltrends.com/realidad-virtual/que-es-metaverso/

Huddleston, T. (2021, 3 noviembre). *This 29-year-old book predicted the «metaverse» — and some of Facebook's plans are eerily similar*. CNBC. https://www.cnbc.com/2021/11/03/how-the-1992-sci-fi-novel-snow-crash-predicted-facebooks-metaverse.html

Millán, V. (2021, 7 noviembre). *Breve historia del metaverso antes de Meta: de 'Snow Crash' a 'Second Life'*. Hipertextual. https://hipertextual.com/2021/11/historia-metaverso

Pascual, M. G. (2021, 30 octubre). *Metaverso: el mundo virtual donde Zuckerberg quiere que compres, te diviertas y trabajes*. El País. https://elpais.com/tecnologia/2021-10-30/metaverso-el-mundo-virtual-donde-zuckerberg-quiere-que-compres-te-diviertas-y-trabajes.html

Ojeda, P. (2022, 8 marzo). *Guía práctica para no perderse de la transformación digital al Metaverso*. Inese. https://www.inese.es/guia-practica-para-no-perderse-de-la-transformacion-digital-al-metaverso/

*¿Cómo funcionará el metaverso de Facebook?* (2022, 2 enero). Forbes México. https://www.forbes.com.mx/forbes-life/tecnologia-como-funcionara-el-metaverso-de-facebook/

Bush, A. (2021a, enero 24). *Into The Void: Where Crypto Meets the Metaverse*. Naavik. https://naavik.co/business-breakdowns/into-the-void

Ball, M. (2022, 9 marzo). *Framework for the Metaverse*. MatthewBall.Vc. https://www.matthewball.vc/all/forwardtothemetaverseprimer

Silva, M. (2021, 30 octubre). *«Ready player one»: Similitudes de la cinta con Metaverso, la nueva versión de Facebook*. SensaCine.com.mx. https://www.sensacine.com.mx/album/album-18571404/

Lucatch, D. (2021, 29 diciembre). *Digital Identity In The Metaverse*. Forbes. https://www.forbes.com/sites/forbesbusinesscouncil/2021/12/28/digital-identity-in-the-metaverse/?sh=cf7da4d1fb6b

Queen's Printer of Acts of Parliament. (2018). *Data Protection Act 2018*. Data Protection Act 2018. https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Callejo, G. (2021, noviembre 30). *Te contamos las diferencias entre los distintos tipos de metaversos*. Noticias Blockchain | Observatorio Blockchain. https://observatorioblockchain.com/metaverso/te-contamos-las-diferencias-entre-los-distintos-tipos-de-metaversos/

Pinto, H. (2022, 19 febrero). *Decentraland: qué es, cómo entrar, comprar y más*. El Grupo Informático. https://www.elgrupoinformatico.com/tutoriales/decentraland-que-como-entrar-comprar-mas-t82865.html

Tech, E. (2022, enero 14). *Cryptovoxels: Qué es, cómo funciona y qué podemos hacer en este metaverso*. GizTab. https://www.giztab.com/cryptovoxels-metaverso-tokens/

Planteo, E. (2021, 16 noviembre). *¿Es la Criptomoneda The Sandbox (SAND) una Buena Inversión?* El Planteo. https://elplanteo.com/criptomoneda-sandbox-sand-inversion/

Pérez, E. (2021, julio 20). *'Axie Infinity' es de los juegos con mayor crecimiento de ingresos de la historia: el "Pokémon de los. . .* Xataka. https://www.xataka.com/videojuegos/axie-infinity-juegos-mayor-crecimiento-ingresos-historia-pokemon-nft-que-vende-que-podemos-ganar-dinero-jugando

Escribano, M. (2021, diciembre 26). *Por qué la clave del futuro del metaverso no será Facebook, sino las criptomonedas*. elconfidencial.com.

https://www.elconfidencial.com/tecnologia/2021-12-26/metaverso-facebook-criptomonedas-realidad-virtual_3348873/

Maldonado, J. (2022, enero 25). *Te contamos el papel que desempeñan los NFT en la construcción de los metaversos*. Noticias Blockchain | Observatorio Blockchain. https://observatorioblockchain.com/metaverso/te-contamos-el-papel-que-desempenan-los-nft-en-la-construccion-de-los-metaversos/

Rouse, M. (2021, 7 abril). *Inteligencia artificial o IA*. ComputerWeekly.es. https://www.computerweekly.com/es/definicion/Inteligencia-artificial-o-IA

*¿Qué es metaverso y cuál es su relación con 5G?* (2021, 2 septiembre). iProfesional. https://www.iprofesional.com/tecnologia/346896-que-es-metaverso-y-cual-es-su-relacion-con-5g

Milgram, P., & Kishino, F. (1994). *A taxonomy of mixed reality visual displays* (N.º 12). Ieice Transactions. https://search.ieice.org/bin/summary.php?id=e77-d_12_1321

Bockholt, N. (2020, 3 septiembre). *Realidad virtual, realidad aumentada, realidad mixta. y ¿qué significa «inmersión» realmente?* Think with Google. https://www.thinkwithgoogle.com/intl/es-es/futuro-del-marketing/tecnologia-emergente/realidad-virtual-aumentada-mixta-que-significa-inmersion-realmente/

Heller, B. (2020). *Reimagining Reality: Human Rights and Immersive Technology*. Carr center for human rights policy. https://carrcenter.hks.harvard.edu/files/cchr/files/ccdp_2020-008_brittanheller.pdf

Magid, L. (2022, marzo 4). *Metaverse: What's the Risk?* ConnectSafely. https://www.connectsafely.org/metaverse-what-it-is-and-what-are-its-risks/

McDougall, F. (2022, 21 enero). *Metaverso: qué es y cómo cambiará Internet para siempre*. https://www.iproup.com/innovacion/28915-metaverso-que-es-y-como-cambiara-internet-para-siempre. https://www.iproup.com/innovacion/28915-metaverso-que-es-y-como-cambiara-internet-para-siempre

González, A. (2021, noviembre 17). *El metaverso podría afectar a la salud mental de millones de personas*. Vandal Random. https://vandal.elespanol.com/noticia/r13511/el-metaverso-podria-afectar-a-la-salud-mental-de-millones-de-personas

Lalani, F. (2022, 24 febrero). *Safety in the metaverse: what are the risks and challenges?* World Economic Forum.

https://www.weforum.org/agenda/2022/01/metaverse-risks-challenges-digital-safety/

Outlaw, J. (2022, 15 enero). *In the metaverse, how do you manage your data? - Jessica Outlaw*. Medium. https://jessica-outlaw.medium.com/in-the-metaverse-how-do-you-manage-your-data-170a90338637

Lemley, M., & Volokh, L. (2018). Law, virtual reality and augmented reality. *University of Pennynsilvania Review*, *166*(5), 1051–1138. https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=9622&context=penn_law_review

Harrison, M. (2022, 22 marzo). *WeProtect Global Alliance - against child sexual exploitation and abuse online*. WeProtect Global Alliance. https://www.weprotect.org/

Franks, M. A. (2021). *The Desert of the Unreal: Inequality in Virtual and Augmented Reality*. University of Miami School of Law Institutional Repository. https://repository.law.miami.edu/fac_articles/539/

Wakas, W. (2022, 11 febrero). *How the metaverse could shape cybersecurity in 2022*. VentureBeat. https://venturebeat.com/2022/02/12/how-the-metaverse-could-shape-cybersecurity-in-2022/

Davies, N. (2021, 10 diciembre). *Cybersecurity and the Metaverse: Pioneering Safely into a New Digital World - Blog | GlobalSign*. GlobalSign GMO Internet, Inc. https://www.globalsign.com/en/blog/cybersecurity-and-metaverse-pioneering-safely-new-digital-world

Dickson, E. J. (2021, 12 septiembre). *Inside the Underground Strip-Club Scene on Kid-Friendly Gaming Site Roblox*. Rolling Stone. https://www.rollingstone.com/culture/culture-features/roblox-virtual-strip-clubs-condo-games-sex-1197237/

*The Child Exploitation Economy*. (2021, noviembre 23). ActiveFence. https://www.activefence.com/research/the-child-exploitation-economy/

Stroud, F. (2021, 28 octubre). *Cryptocurrency*. Webopedia. https://www.webopedia.com/definitions/cryptocurrency/

*The Risk of Fraud in the Metaverse*. (2022, 25 febrero). eWEEK. https://www.eweek.com/security/fraud-in-the-metaverse/

Staff, V. B. (2022, 4 febrero). *How the metaverse will impact governance, privacy, fraud, identity, and more*. VentureBeat.

https://venturebeat.com/2022/01/26/how-the-metaverse-will-impact-governance-privacy-fraud-identity-and-more/

*The Global Risks Report 2020*. (2020). WEF. https://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf

*UN warns cybercrime on rise during pandemic*. (2020, 25 mayo). ABC News. https://abcnews.go.com/Health/wireStory/latest-india-reports-largest-single-day-virus-spike-70826542

Staff, V. B. (2021, septiembre 21). *2 million malicious emails bypassed secure email defenses over 12 months*. VentureBeat. https://venturebeat.com/2021/09/21/2-million-malicious-emails-bypassed-secure-email-defenses-over-12-months/

*Email Statistics Report*. (2018, 8 diciembre). Campaign Monitor. https://www.campaignmonitor.com/resources/knowledge-base/how-many-emails-does-the-average-person-receive-per-day/

Yong, S. (2020, 9 enero). *91% of all cyber attacks begin with a phishing email to an unexpected victim*. Deloitte Malaysia. https://www2.deloitte.com/my/en/pages/risk/articles/91-percent-of-all-cyber-attacks-begin-with-a-phishing-email-to-an-unexpected-victim.html

Davies, N. (2021, 10 diciembre). *Cybersecurity and the Metaverse: Pioneering Safely into a New Digital World - Blog | GlobalSign*. GlobalSign GMO Internet, Inc. https://www.globalsign.com/en/blog/cybersecurity-and-metaverse-pioneering-safely-new-digital-world

Sánchez, I. N. (2022, 4 febrero). *Ciberseguridad en el Metaverso: 3 ciberataques que deben preocuparnos*. Empresa de Ciberseguridad. https://ciberseguridad.oesia.com/ciberseguridad-en-el-metaverso/

Magid, L. (2022, marzo 4). *Metaverse: What's the Risk?* ConnectSafely. https://www.connectsafely.org/metaverse-what-it-is-and-what-are-its-risks/

Siddique, M., Shoaib, S., & Jan, Z. (2020). https://imsciences.edu.pk/files/journals/vol12_2/New%201%20MA.864.pdf. *Business & Economic Review*, *12*(2), 19–50. https://doi.org/10.22547/ber/12.2.2

*Deepfakes*. (2022). INCIBE. https://www.incibe.es/aprendeciberseguridad/deepfakes

Sauliere, S. (2021, 27 abril). *Blurring the lines between real and virtual: Deepfake Geography & Nvidia Metaverse*. Blurring the Lines between Real and Virtual. https://www.linkedin.com/pulse/blurring-lines-between-real-virtual-deepfake-nvidia-severin-sauliere

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. *Diario Oficial de la Unión Europea, L119,* de 4 de mayo de 2016. https://www.boe.es/doue/2016/119/L00001-00088.pdf

Criddle, B. C. (2020, 28 octubre). *Facebook sued over Cambridge Analytica data scandal*. BBC News. https://www.bbc.com/news/technology-54722362#:%7E:text=Facebook%20is%20being%20sued%20for,used%20for%20advertising%20during%20elections.

Mason, E. (2020, 15 agosto). *El informe muestra cuántas personas juegan juegos en todo el mundo. Spoiler: hay muchos*. Últimas noticias de juegos, guía y consejos. https://dlprivateserver.com/el-informe-muestra-cuantas-personas-juegan-juegos-en-todo-el-mundo-spoiler-hay-muchos/#:%7E:text=Seg%C3%BAn%20el%20informe%20de%20DFC,m%C3%B3viles%20en%20paralelo%2C%20por%20ejemplo.

*Casi 4,4 millones de españoles invierten en criptomonedas, pese al desconocimiento general*. (2022, 8 marzo). El Independiente. https://www.elindependiente.com/economia/2021/11/25/casi-44-millones-de-espanoles-invierten-en-criptomonedas-pese-al-desconocimiento-general/

Roa, M. M. (2021, 28 enero). *¿Cuántas horas al día pasamos conectados a Internet?* Statista Infografías. https://es.statista.com/grafico/22701/tiempo-medio-de-uso-diario-de-internet/

Parkin, S. (2022, 20 enero). *The trouble with Roblox, the video game empire built on child labour*. The Guardian. https://www.theguardian.com/games/2022/jan/09/the-trouble-with-roblox-the-video-game-empire-built-on-child-labour

Stanley, M. (2021). *Should Investors Take the Metaverse Seriously?* Morgan Stanley. https://www.morganstanley.com/ideas/metaverse-investing

Rees, K. (2022, 28 febrero). *5 Vital Safety Features the Metaverse Needs*. makeusof. https://www.makeuseof.com/metaverse-safety-features/

Soria, M. C. L. S. (2022, 7 febrero). *El peligro del Metaverso: violan en manada al avatar de una mujer*. COPE. https://www.cope.es/programas/fin-de-semana/noticias/metaverso-aun-tiene-mucho-que-mejorar-para-evitar-comportamientos-inadecuados-dentro-20220206_1771241

Kaleem, K. (2022, 11 febrero). *How Meta Is Dealing With Sexual Harassment in VR*. Makeusof. https://www.makeuseof.com/meta-sexual-harassment-vr-personal-boundary/

Lucatch, D. (2021, 29 diciembre). *Digital Identity In The Metaverse*. Forbes. https://www.forbes.com/sites/forbesbusinesscouncil/2021/12/28/digital-identity-in-the-metaverse/?sh=cf7da4d1fb6b

*Plan de concienciación de seguridad informática*. (2019, 28 noviembre). Ciberseguridad. https://ciberseguridad.com/normativa/espana/medidas/plan-concienciacion/#:%7E:text=las%20redes%20sociales-,%C2%BFQu%C3%A9%20es%20un%20Plan%20de%20Concienciaci%C3%B3n%20de%20Seguridad%20inform%C3%A1tica%3F,los%20datos%20de%20la%20organizaci%C3%B3n.

Álvarez, R. (2021, 8 diciembre). *Cultura de ciberseguridad y alfabetización digital para la ciudadanía*. Blog Educación y Bienestar digital. https://gaptain.com/blog/alfabetizacion-mediatica-que-es-y-porque-introducirla-en-el-aula/

*Qué es el blockchain: definición, tipos, ejemplos, ventajas y utilidades*. (2021, 8 septiembre). LISA Institute. https://www.lisainstitute.com/blogs/blog/que-es-blockchain-tipos-ejemplos-ventajas

*Ataques cibernéticos: ¿Cuáles son los principales y cómo protegerse de ellos?* (2021, 30 junio). Iberdrola. https://www.iberdrola.com/innovacion/ciberataques

Ferre, I. B. (2022, 2 marzo). *Criptomoneda*. Economipedia. https://economipedia.com/definiciones/criptomoneda.html

Bastón, R. (2021, 20 septiembre). *Metaversos descentralizados: los 6 principales (y ninguno es Facebook), con Sergio García (Floc)*. Marketing 4 Ecommerce. https://marketing4ecommerce.net/metaversos-descentralizados-los-6-principales-y-ninguno-es-facebook-con-sergio-garcia-floc/

*¿Qué es la inteligencia artificial?* (2019). Hewlett Packard. https://www.hpe.com/es/es/what-is/artificial-intelligence.html#:~:text=La%20inteligencia%20artificial%20(IA)%20se,ejemplos%20previos%20de%20conductas%20similares.

Ratan, R., y Lei, Y. (2021, 10 noviembre). *¿Qué es el metaverso, futuro de la convivencia humana?* The Conversation. https://theconversation.com/que-es-el-metaverso-futuro-de-la-convivencia-humana-166481

*Qué es un NFT y cómo funciona*. (2022, 10 marzo). ELMUNDO. https://www.elmundo.es/como/2022/03/10/6229eb5c21efa072618b4578.html