TRABAJO INVIA – GRUPO 1

LA EVOLUCIÓN DE INTERNET
Retos de seguridad en el Metaverso

Irene Alonso Suárez
Carmen Álvarez Utiel
Sergio Arrogante Soria
Diego Bejarano Matías
Antonio Calero Avendaño
Andrea Comesaña Pérez

ÍNDICE

1. Glosario

Blockchain: Cadena de bloques. Es un conjunto de tecnologías que permiten la transferencia de un valor o activo de un lugar a otro sin intervención de terceros, gracias al modelo descentralizado.

Criptomoneda: Es un medio digital de intercambio que cumple la función de una moneda.

DARPA: Agencia de Proyectos de Investigación Avanzados de Defensa (EEUU).

HTML: Lenguaje de Marcas de Hipertexto. Es el lenguaje de programación que define la estructura del contenido de una web.

HTTP: Protocolo de Transferencia de Hipertexto. Es el protocolo de comunicación que posibilita la circulación de información a través de la World Wide Web (WWW) para poder acceder a un navegador web o página web.

NFT: Token no fungible. Es un tipo de token con un certificado digital de autenticidad que mediante la tecnología blockchain se asocia a un solo archivo, lo que lo hace único. Por ello, no se puede modificar ni intercambiar por otro que tenga el mismo valor.

Protocolo TCP/IP: Modelo de comunicación en redes que permite que dos dispositivos se conecten para transferir datos de uno a otro.

RA: Realidad Aumentada. Es un mundo virtual, que permite agregar elementos virtuales sobre el mundo real.

RV: Realidad Virtual. Es un entorno de escenas y objetos de apariencia real, generado mediante tecnología informática, que crea la sensación en el usuario de estar inmerso en él. Para poder visualizar este entorno es necesario un dispositivo llamado casco o gafas de realidad virtual.

MaaS: Metaverse as a Service. Modelo de servicio en el metaverso en el que las marcas podrán definir sus espacios para que sean lo que quieran. Esta plataforma permitirá a otros crear lugares digitales que se ajusten a las necesidades de cada uno de sus usuarios.

Metaverso: Mundo inmersivo 3D donde los ciudadanos pueden interactuar mediante un avatar para llevar a cabo una gran variedad de actividades.

SaaS: Software as a Service. Es un modelo de distribución y de licencias que permite a los usuarios conectarse a aplicaciones almacenadas en la nube a través de Internet y usarlas.

Token: Unidad de valor que una organización crea para gobernar su modelo de negocio y dar más poder a sus usuarios para interactuar con sus productos, al tiempo que facilita la distribución y reparto de beneficios entre todos sus accionistas.

Web Browser: Navegador Web. Software que permite el acceso a la Web.

XR: Realidad Extendida. Es la combinación de las denominadas tecnologías inmersivas: la RV (Realidad Virtual) y la RA (Realidad Aumentada).

2. Introducción

El metaverso, concebido como el sucesor natural del internet tradicional, aún carece de consenso en su definición, pero podría ser descrito como un mundo inmersivo 3D donde los ciudadanos pueden interactuar mediante un avatar para llevar a cabo una gran variedad de actividades. Las actividades abarcan desde el ocio y juegos de azar hasta las interacciones de carácter comercial, económico o sanitario, incluyendo incluso cirugías. La amplitud y el potencial del metaverso todavía se desconoce, así como su posible impacto en la sociedad a medio plazo, sin embargo, su abanico de posibilidades y las oportunidades que nos brindaría ya es perceptible. Por contra, las nuevas oportunidades traerán consigo un nuevo abanico de retos y desafíos en una gran variedad de ámbitos, específicamente en la seguridad.

Se percibe el metaverso como el futuro debido a las grandes inversiones de las potencias tecnológicas, comenzando así el debate legal, financiero y de ciberseguridad sobre cómo se afrontarán los nuevos retos, ya que se abre un nuevo espacio donde se pueden llevar a cabo un gran rango de actividades ilícitas. La responsabilidad y legalidad son conceptos aún por determinar, además sería clave considerar el impacto que podría tener en la salud la excesiva inmersión digital, especialmente en grupos vulnerables, en los que se deberán considerar la igualdad de oportunidades de acceso a él.

3. Evolución de Internet

Network e Interconnect, abreviado como Internet, nace de la necesidad de acelerar la comunicación durante la Guerra Fría. El Departamento de Defensa de Estados Unidos crea en 1958 la Agencia de Proyectos de Investigación Avanzados de Defensa, abreviado como DARPA, con el fin de responder a los desafíos tecnológicos y militares de la URSS. Se considera que esta agencia fue la que asentó los pilares para la creación de Internet tal y como lo conocemos hoy en día. Fue en 1969 cuando Michael Elie consiguió integrar la DARPA y conectar el ordenador de la Universidad de California en Los Ángeles (UCLA) con otro ordenador del Instituto de Investigación de Standford (SRI). En ese mismo año, consiguieron crear una red en la que cuatro universidades estaban interconectadas, denominada Arpanet. El objetivo de la creación de esta red era mantener la capacidad de comunicarse en caso de guerra.

En 1970, Ray Tomlinson asienta los fundamentos de lo que se conocería posteriormente como el correo electrónico. Arpanet fue integrando cada vez más universidades y proyectos de defensa. En 1972, ya estaban integrados en la red 50 universidades y centros de investigación estadounidenses. En 1973, se establecieron conexiones con otros países como Noruega e Inglaterra. El número de ordenadores conectados fue incrementando gracias al auge de su comercialización, a la vez que fueron apareciendo nuevas redes en la década de los 80. Internet nace al unificar todas las redes en 1983. Durante su avance, el Departamento de Defensa de EE. UU. optó por usar el protocolo

TCP/IP en su red Arpanet, dando lugar así a la red Arpa Internet. Posteriormente, quedó únicamente el nombre de «Internet».

Fue en 1989 cuando Tim Berners Lee creó por primera vez el protocolo de transferencias de hipertextos, dando lugar a la primera web y utilizó tres nuevos recursos: HTML, HTTP y Web Browser. La World Wide Web creció rápidamente, pasó de 100 World Wide Web Sites en 1993 a más de 200.000 en el 97. En los años posteriores, el número de usuarios de internet fue creciendo exponencialmente a nivel internacional. Dicha tendencia se vio fuertemente incrementada debido al nivel de penetración que han tenido los teléfonos móviles en la sociedad.

A finales de la década de los 80 y principios de los 90, se generó un debate sobre las redes de comunicaciones y su financiación, ya que éstas estaban financiadas con dinero público y eran muy caras de mantener. Por ello, el Gobierno de EEUU decidió llevarlo al sector privado y abrirlo a empresas que aplicaran sus ideas y modelos de negocios. En el año 1994 empezaron a formar parte del proyecto grandes empresas de telecomunicaciones como Sprint, AT&T y UUNET. Posteriormente, empezaron a llevar Internet a los usuarios a través de las líneas telefónicas para conectar en las casas de todo el mundo. A mediados de los años 90 empezaron a desarrollarse las redes sociales. La primera fue la creación de GeoCities, la cual recomendaba al usuario crear su página web y colocarla en "barrios". De esta manera, los usuarios del mismo barrio podían relacionarse. Posteriormente, nació Sixdegrees que permitió enviar mensajes y crear comunidad entre usuarios mediante un sistema de invitaciones. En 2002 apareció Friendster, una red social de videojuegos. En 2004, Mark Zuckerberg creó Facebook y en 2005 llegó Youtube.

Con el paso de los años, las redes sociales fueron evolucionando hasta adquirir importancia no solo en el plano social, sino también en el campo del marketing y los negocios. Así fueron naciendo nuevas figuras en las empresas encargadas de gestionar las redes sociales como los Community y Social Media Manager. La aparición de nuevos dispositivos móviles y tecnologías, que facilitaban el acceso a internet, derivó en la ampliación del negocio de las empresas hacia el comercio digital. En este sentido, se pueden destacar los siguientes eCommerce más importantes del mundo: Amazon (EE. UU.) Alibaba (China), Ebay (EE. UU.), Zalando (Alemania) y JD.com (China).

Actualmente, el número de usuarios de Internet se eleva a 4.950 millones de personas, representando el 62,5% de la población mundial. Entre las webs más visitadas del mundo se encuentran Google, Youtube, Facebook, Twitter e Instagram. Emiratos Árabes Unidos, Dinamarca e Irlanda se encuentran entre los países con mayor penetración de Internet con un 99%, encontrándose España en el puesto 14 con un 94%. Por el contrario, los países con menor penetración de Internet serían Corea del Norte con un 0,1%, República Centroafricana con un 7% y Eritrea con un 8%. La pandemia del Covid-19 en 2020 impulsó fuertemente el uso de las redes sociales y el comercio online, el trabajo en remoto y la dependencia de Internet para realizar tareas diarias. El eCommerce aumentó más de 11 puntos desde el año 2020, ya que el 58% de la población entre 16 y 64 años ha realizado compras semanales por internet en 2021. Sin embargo, la constante innovación de la tecnología y las necesidades

cambiantes de los usuarios han abierto un nuevo plano en el que exploramos Internet: el metaverso.

4. Metaverso

Las nuevas necesidades y avances tecnológicos nos han llevado como sociedad a una evolución de Internet tal y como lo conocemos, en el que los usuarios participarían en un espacio inmersivo y 3D. Si el concepto del metaverso se materializa, podría ser tan revolucionario como el teléfono móvil. Hoy en día, Internet es el punto de referencia para millones de personas que acceden diariamente a información y servicios, sistemas de comunicación o compra y venta de productos. La previsión es que el metaverso será capaz de reproducir esta propuesta de valor de forma inmersiva, en la que será difícil delimitar cuándo estamos fuera de línea y cuándo estamos en línea.

El metaverso se rige y define por siete reglas según el autor Parisi:

Solo hay un metaverso.
El metaverso es abierto.
El metaverso es para todos.
Nadie controla el metaverso.
El metaverso es una red.
El metaverso es independiente del hardware.
El metaverso es Internet.

Por otro lado, los elementos imprescindibles para la materialización y la definición del metaverso incluyen la experiencia inmersiva de la realidad aumentada, la realidad virtual y la realidad mixta, además de la importancia de la interconexión e interoperabilidad entre la red de espacios que lo conforman. Debe facilitarse el movimiento, la creación y la exploración de otros avatares que se encuentren en el mismo espacio digital que el usuario. Hasta ahora, las tecnologías XR, o eXtended Reality se han limitado a una serie de videojuegos y un rango muy escaso de aplicaciones empresariales. Sin embargo, a medida que los videojuegos van evolucionando hacia plataformas sociales, cabe la posibilidad de que sus características transpiren hacia otros contextos, por ejemplo: el ámbito empresarial y económico.

En el ámbito empresarial y económico, se espera que el metaverso se convierta en una extensión del mundo real, proporcionando la posibilidad de construir, comerciar, invertir y proveer bienes y servicios a individuos y empresas que puedan participar de la misma forma en la que lo hacen hoy en día. Tanto la criptomoneda como las Token no Fungibles, abreviado comúnmente como NFT, se consideran parte de la base para la creación de una moneda de cambio en el metaverso. Una NFT es una declaración de propiedad de un activo digital único, y a pesar de su novedad, se ha convertido en tendencia en los últimos meses. Los NFT no son intercambiables y se almacenan en una cadena de bloques, y podrían convertirse en la

herramienta que utilicen los comercios para acelerar la economía digital y alejarse del comercio tradicional.

También alejándose del mercado tradicional se encontrarán las marcas que compran espacios publicitarios en páginas web y actualmente están comprando terrenos digitales en el metaverso, y desde que Facebook anunció sus planes de metaverso y su cambio de nombre de holding a Meta, el precio de los inmuebles se han disparado hasta un 500%. Se prevé que el gran tráfico de personas y transferencias en terrenos del metaverso generen el mismo beneficio que en terrenos del mundo real. Fundamentalmente, el metaverso será una versión 3D de Internet, y ya hay empresas realizando inversiones millonarias en terrenos virtuales. La ubicación donde nos encontremos no importará, ya que en el metaverso se prevé que tanto los individuos como las empresas podrán transportarse a cualquier lugar del mundo, por lo que se generará tráfico comercial con un rango más amplio de posibilidades que en el mundo real.

El metaverso estará conformado por plataformas finitas dentro de él, por lo que el terreno que se pueda comprar estará limitado al espacio. Al igual que en el mundo real, si la demanda de estos terrenos sube en un espacio finito, el precio subirá. Sin embargo, estos terrenos podrán perder valor si finalmente son infinitas, y no finitas como se espera ahora. Actualmente, existen cuatro plataformas en el metaverso: The Sandbox, Decentraland, Cryptovoxels y Somnium Space. PwC ha adquirido una parcela en The Sandbox, donde tiene como objetivo crear un centro de asesoramiento de la Web 3.0 para "facilitar una nueva generación de servicios profesionales, como la contabilidad y fiscalidad". Multinacionales como Adidas y Warner Music Group también han invertido en terrenos en el metaverso por el amplio abanico de posibilidades que ofrece. Por ejemplo, en el ámbito de la música, la creación de un espacio de conciertos virtual podría ser revolucionario a la hora de incluir a aquellos que, por limitaciones de transporte o ubicación, no pueden acudir a eventos musicales o culturales.

En The Sandbox también ha invertido Republic Realm, uno de los mayores inversores y desarrolladores del modelo de inversiones y compras de terreno en el ecosistema del metaverso. La empresa ha desembolsado más de 4 millones de dólares en terrenos y más de 2 millones de dólares en Tokens en Decentraland, el mayor acuerdo jamás realizado en este ámbito. Las inversiones de Microsoft en el editor de juegos Activision Blizzard son indicadores de la importancia que tendrán los videojuegos en el metaverso.

Aunque nos brindaría un amplio abanico de posibilidades, la lista de desafíos al que se podrían enfrentar es más extensa. La interoperabilidad, el poder moverse fácilmente entre plataformas supondrá un reto para aquellas empresas que no se prestan a renunciar a su propiedad intelectual, además deberán desarrollar normas abiertas que permitan trabajar y asistir a eventos sociales, realizar transacciones económicas y gestiones sin fisuras, lo cual no es tarea fácil debido a las importantes innovaciones que deberán instalar de software y hardware. El objetivo será, al igual que hoy en día existe el SaaS (Software as a Service), convertirlo en MaaS (Metaverse as a Service).

a. Seguridad en el metaverso y sus desafíos

Los desafíos nacen de la velocidad con la que el metaverso ha irrumpido en la sociedad como una posibilidad a corto-medio plazo, en la que muchos lo perciben como un renacimiento de Internet tal y como lo conocemos, una invasión a nuestra vida fuera de lo virtual y una línea borrosa entre el mundo real y el mundo virtual. Es por ello que la línea de investigación girará en torno a estos desafíos de seguridad y el escenario más probable en el que nos veremos inmersos a corto-medio plazo.

Para los gobiernos, los desafíos más importantes incluirán las noticias falsas, espionaje, terrorismo y utilización de la Inteligencia Artificial para la defensa nacional y la guerra. El uso no ético del metaverso está asegurado, al igual que ocurre con Internet, por lo que los gobiernos deberán tomar medidas para proteger a su Estado y sus ciudadanos. Debido a la recopilación de información biométrica tan extensa, la suplantación y el robo de identidad para cometer delitos se podría convertir en una gran amenaza para los gobiernos. En esta línea, la venta de datos biométricos podría convertirse en un mercado negro para así poder imitar la huella de usuarios y suplantar sus identidades para llevar a cabo el robo de propiedades virtuales, además de la venta de propiedades falsas.

En primer lugar, la **gestión de identidades**. En Internet, el uso de perfiles anónimos para llevar a cabo actos de acoso, delitos de odio y difamación ha sido relevante desde el irrumpimiento de las redes sociales en nuestra sociedad. En las aplicaciones actuales, ya es difícil confirmar la identidad del usuario, en el metaverso podría ser peligrosa la desvinculación de individuos con avatares, ya que al ser su uso más amplio, podría convertirse en un espacio de delincuencia sin asunción de responsabilidad. En relación a este tema, el robo de identidad podría llegar a ser uno de los principales problemas que vemos en el mundo virtual. El hecho de interactuar con un avatar requerirá nuevas formas de responsabilizar a empresas e individuos de sus actos, además de la necesidad de instalar nuevos sistemas de detección y verificación de identidad para evitar en la mayor medida posible la ciberdelincuencia a mayor escala. Debido a la mayor implicación e inmersión de los usuarios en el metaverso, será clave que se cree un protocolo robusto para evitar el robo de bienes virtuales o el acceso a datos críticos.

Asimismo, la recopilación tan extensa de datos conforme más usuarios comiencen a usarlo podría suponer una grave amenaza para la **privacidad** de datos de los dispositivos. Las dudas sobre la privacidad, seguridad y protección aumentarán, por ello será vital que se estipulen leyes que fomenten un equilibrio entre la adquisición de datos y el respeto a la privacidad y la propiedad intelectual. Este factor podría ser el que provoque que los usuarios estén más reacios a compartir tantos datos con un sistema aún desconocido para ellos, ya que serán necesarios datos de biometría, movimiento, gestos, ubicación exacta, patrón del habla o voz…entre otros. Debido la delicadeza de estos datos biométricos y de carácter tan personal,

para asegurar la seguridad del metaverso, los operadores de éste deben implementar un sistema en el que sea obligatoria la posesión de un certificado digital de estándar gubernamental.

En esta misma línea se consideran los **servicios financieros** en el metaverso, el uso de la criptomoneda aún no está regulado, por lo que convertirlo en un sistema de pago en el metaverso sólo añadiría más complicaciones a las transacciones diarias de los usuarios. Una fisura en este sistema podría suponer un desastre para grandes empresas o incluso a nivel individual. La solución que podría evitar este problema sería una moneda digital, blockchain para asegurar las transacciones económicas y la conversión de criptomonedas con interoperabilidad de plataformas para que los usuarios puedan transitar de unas a otras. La mayoría de estos factores los desconocemos a día de hoy ya que dependen de la gobernanza del metaverso: si finalmente constituye un sistema de sistemas abiertos o queda bajo el control de un número reducido de empresas, como sucede hoy con el monopolio de Google, Facebook e Instagram.

En relación a los **problemas económicos** se podría incluir la criptomoneda como una forma empleada con fines de blanqueo de dinero y facilitar transferencias de dinero entre delincuentes que no desean dejar huella en el mundo real. La falta de regulación de la criptomoneda y la desinformación que la rodea, además de su volatilidad y vulnerabilidad, podría suponer una desventaja del metaverso. Además, un desarrollo ilegal de las criptomonedas y la posibilidad de su uso anónimo o mediante un avatar falso podría incrementar el número de usuarios anónimos con el fin de delinquir, dificultando así la detención de los responsables de la ciberdelincuencia. Debido a la novedad y desinformación que existe acerca de las NFTs, los fraudes son extremadamente comunes, así como la apropiación indebida de éstos, ya que la verificación de la propiedad es fácil en la teoría, en la práctica no es posible debido al gran número de NFTs que se han generado en los últimos meses. Se estima que hasta el 80% de los NFTs creados con OpenSea, el mayor punto de venta de NFTs, son ilegítimos.

Con respecto a las comunidades vulnerables de exclusión social, se tendría que tener en consideración las implicaciones de la estandarización del metaverso. Al igual que la estandarización del uso de ordenadores y dispositivos móviles para recibir la educación obligatoria durante la pandemia del Covid-19 supuso un problema para millones de familias, la estandarización del metaverso podría excluir aún más a personas ya en riesgo de exclusión. Al no tener acceso a los medios necesarios, de convertirse el metaverso en el estándar, sería problemático a la hora de asegurar igualdad de condiciones para toda la población. Asimismo, el hardware, software, protocolos, procesos e interoperabilidad deben estar estandarizados para poder ser accesibles a toda la población. Las herramientas de creación y economías digitales, la realidad virtual, los NFTs, ciberseguridad, deberán estar a alcance de todos para poder convertirlo en un bloque estándar de nuestro futuro.

El metaverso es un desafío en sí, especialmente considerando el contexto actual en el que nos encontramos a nivel económico y energético. La implementación del metaverso como estándar en nuestro día a día supondría un desafío a nivel energético debido al aumento

del uso de la electricidad y su consecuente consumo de energía que es necesario para desarrollar un sistema como el metaverso.

El precio actual de la energía y la crisis económica convertirá en un bien exclusivo el acceso al metaverso, por lo que su implementación como estándar en la vida diaria será prácticamente imposible a no ser que se pueda asegurar la igualdad de condiciones de acceso para toda la población. Además, cabe esperar que este aumento en la consumición de energía dejará una **huella de carbono** desorbitada en un contexto histórico delicado a nivel de medio ambiente, pudiendo traer consecuencias ambientales devastadoras, por lo que hay que tener en cuenta las consecuencias del metaverso a todos los niveles.

En lo que respecta al aspecto social del metaverso, los gobiernos no solo deben imponer sistemas de control a nivel económico o legal, sino ser capaces de controlar la **desinformación o mensajes radicales**, **fake news**, **deep fakes** o **manipulación**. En el uso que realizamos actualmente de Internet, las noticias falsas ya se encuentran entre las mayores amenazas para la credibilidad y soberanía de los gobiernos, por lo que una mayor inmersión en el uso de Internet supone más riesgo de radicalización o difusión de noticias falsas que pueden dañar a propósito la reputación de empresas o Estados. Los sistemas digitales y redes sociales ya cuentan con métodos para recopilar información destinada a dirigir mensajes específicos a grupos designados para influir en su pensamiento y comportamiento, con el fin de obtener algún beneficio económico, comercial o político. Con el almacenamiento de una mayor cantidad de datos biométricos y un mayor conocimiento del comportamiento individual, aumentará la capacidad de los sistemas de conocer a su objetivo y por ende su capacidad de manipularlo, ya que tendrán una mayor comprensión de su comportamiento y podrán predecirlo con mayor exactitud.

Sin embargo, lo más preocupante es ciertamente la suplantación de identidad mediante el uso de vídeos falsos generados con Inteligencia Artificial. Mediante una recopilación de los movimientos, datos biométricos, tono de voz y demás detalles específicos individuales, los sistemas tendrían la capacidad de aprender a imitar exactamente a personajes públicos o políticos, generando vídeos falsos creando noticias falsas a partir de palabras clave que no han sido dichas pero pueden ser añadidas falsamente. Finalmente, al igual que hoy en día el algoritmo nos muestra información con la que nos sentiremos identificados o estaremos de acuerdo, en el metaverso el riesgo se amplifica debido a los factores anteriormente mencionados. La experiencia inmersiva y la cantidad de datos específicos recopilados harían más difícil distinguir la realidad del contenido falso. Además, la difusión de noticias falsas y deep fakes de forma viral podrían llegar a millones de usuarios dependiendo de sus gustos o creencias, difundiendose así a millones de personas.

A su vez, estos algoritmos crean burbujas en las que los usuarios solo reciben contenido afín a sus intereses, opiniones, creencias, orientación política, por lo que se crean núcleos en los que los usuarios sólo consumen información que refuerza sus propias opiniones. Esta ocurrencia es peligrosa, ya que evita que se consuma información alternativa y crea una cámara de eco en la cual el usuario puede llegar a radicalizarse en su propia opinión. Esto es especialmente importante de cara a las elecciones políticas, ya que, como se

observó en las elecciones de Estados Unidos en 2016, fue gracias a la manipulación en redes por parte de bots rusos lo que impulsó la victoria de Donald Trump.

Los algoritmos de la Inteligencia Artificial pueden marcar la diferencia a la hora de difundir información manipulada orientada hacia un partido político u otro. Esto también será especialmente relevante a nivel empresarial, a la hora de hundir la reputación de la competencia, las grandes empresas tendrían la posibilidad de manipular la información, generar vídeos o noticias falsas y hacerlas llegar a millones de personas para conseguir una ventaja frente a la competencia. Una vez más, dada la extensa recopilación de datos y la experiencia inmersiva, cada vez será más difícil distinguir qué es verdad y qué no.

A nivel de seguridad, se tendrá que tener en cuenta la **integridad física** de aquellos que entren en el metaverso. Recientemente, han existido casos de violaciones en el metaverso que han planteado una nueva problemática a la legislación actual, ya que la línea que separa el mundo real y el ficticio cada vez se vuelve más borrosa e indefinida. Un avatar es virtual, y sin embargo una agresión sexual requiere contacto físico, por lo que la aplicabilidad de la legislación en cuanto a la violencia en el metaverso se pone seriamente en tela de juicio. Los avances tecnológicos han conseguido que las experiencias cada vez se vuelvan más realistas, por lo que se deberá decidir hasta dónde llega lo ficticio y empieza lo real. En esta línea, supondría un reto para grupos vulnerables, especialmente menores, ya que su protección deberá ser tomada más en serio conforme más realista sea el metaverso en el que se mueven. El contenido explícito, no deseado, el acoso o cualquier tipo de abuso será difícilmente controlable debido a la posibilidad de hacerlo mediante usuarios anónimos, además de que serán completamente necesario la implementación de sistemas que puedan proteger eficazmente a los menores de contenido violento o perjudicial para su seguridad. La experiencia inmersiva, podría suponer un riesgo en el ámbito del ciberacoso, ya que éste podría ser más pronunciado, más realista, y más difícil de escapar de él, por lo que los menores podrían percibirlo como una realidad, agravando así problemas subyacentes.

Las redes sociales ya presentes como Instagram o TikTok podrían ser consideradas como las grandes responsables de una gran mayoría de trastornos mentales con alta incidencia hoy en día, debido a una suma entre la presión social que ejercen y la forma en la que distorsionan la realidad. La experiencia inmersiva combinada con horas de exposición pondrá en riesgo la salud mental de aquellos ya vulnerables. Trastornos alimenticios como anorexia, vigorexia o bulimia podrían ver un aumento debido a la disociación del mundo real y la asociación propia a un avatar falso, generado por una dismorfia corporal debida a no ser capaces de distinguir con criterio el contenido real del contenido falso. El algoritmo, una vez más, podría ser responsable de difundir información dañina que pueda poner en peligro la integridad física o mental de los jóvenes, si un sistema deseara, de forma maliciosa, atacar a los más vulnerables en el metaverso. Si el algoritmo consigue atrapar al usuario en contenido que se alinee con sus intereses, los usuarios podrían comenzar a consumir contenido en el metaverso de forma obsesiva con el fin de escapar de su realidad. La información dañina, campañas de desinformación manipuladas deliberadamente o propaganda terrorista podrían agravar seriamente la salud mental de los usuarios, consiguiendo así condicionar y controlar. Se teme que estas campañas lleguen a poder desestabilizar a la gente con el fin de hacerles

luchar por distinguir lo que es real de lo que no mediante una manipulación del entorno virtual.

Esta manipulación del entorno podría engañar a los usuarios para que golpeen objetos o se trasladen a otro lugar físico, poniendo en riesgo así su integridad física si desea hacerlo de forma maliciosa, con el fin de forzarlos a ver contenido no deseado o desorientar al usuario. Además, el **terrorismo** se nutre del terror causado en la población, por lo que sería posible que diferentes grupos terroristas pudieran llevar a cabo campañas de desinformación para promover la radicalización y el reclutamiento. La falta de responsabilidad real en el metaverso podría promover actos ilegales, entrenamientos, planeamiento de ataques terroristas y los reclutas tendrán acceso a personas vulnerables e influenciables más allá de las fronteras de su país, ya que gracias al algoritmo tendrán acceso a millones de personas que cumplan las características necesarias. Podrán, así, orientar su propaganda hacia los reclutas y sembrar el terror en la población con más eficacia. Mientras que ahora dependen de su repercusión en medios de comunicación, en el metaverso, ellos mismos podrían hacerse pasar por medios de comunicación y difundir información falsa con el fin de conseguir manipular y controlar a sus objetivos. La radicalización podría ser más rápida y profunda debido a la inmersión en el metaverso y la manipulación del entorno podría generar que el usuario no sea capaz de distinguir qué es real y qué no, por ejemplo, creando un califato o un entorno en el que exista el supremacismo blanco.

Un tipo diferente de ataque pero con consecuencias graves para los gobiernos o empresas multinacionales podrían ser las escuchas malintencionadas, el **espionaje** o la capacidad de entrar en una sala virtual sin consentimiento ni conocimiento del resto de sus participantes con el fin de obtener información que comprometa a los usuarios.

b. Escenarios

Una vez expuestos los desafíos de seguridad a los que nos podríamos enfrentar con la llegada del metaverso como evolución natural de Internet, es clave poner en valor cuál es la posibilidad real de un metaverso como parte de nuestra vida cotidiana. Para ello, se establecen diversos impulsores en los que se basaría el escenario posteriormente propuesto.

En **materia económica**, en el actual mercado internacional se encuentran en auge las aplicaciones de blockchain, las finanzas descentralizadas basadas en cripto bienes adquiridos a través de criptomonedas, tokens o NFT y los servicios o comercio entre pares, siendo un modelo de intercambio a través de monedas virtuales que permite su comercialización sin un tercero que facilite transacciones. Esta descentralización de la economía podría atraer a usuarios, marcas y retailers hacia el metaverso.

También la expansión de la **vida social digital** con la puesta en valor del metaverso, su creciente aceptación social y la evolución de los comportamientos, intereses y hábitos de los usuarios, favorece el traslado de usuarios de la actual web 3.0 a una experiencia más sensorial, inmersiva y directa como la que presenta el metaverso. Impulsando así su

crecimiento y desarrollo para satisfacer las demandas por parte de los usuarios de experiencias y comunicaciones más directas y reales.

Otro impulsor clave es el **desarrollo de las capacidades técnicas**, imprescindible para el establecimiento del metaverso, algunas tecnologías actuales favorecen su implementación o están siendo desarrolladas con el objetivo de impulsarlo. Entre ellas destacan las innovaciones en hardware como las mejoras en infraestructura de red, el despliegue de fibra o las pantallas holográficas, así como en software con el desarrollo de la inteligencia artificial, el internet de las cosas, el 5G y el blockchain.
En relación a estas capacidades, cabe mencionar la **compatibilidad de software** entre plataformas y sistemas como impulsor de fricción, requisito técnico que podría conllevar un freno para la implementación del metaverso al ser necesario una capacidad de ejecución homogénea en los diferentes dispositivos. Pudiendo conllevar un mínimo de 15 años para su establecimiento en la sociedad.

Además, las **grandes inversiones** que se están realizando con adquisiciones masivas de compañías de videojuegos y plataformas virtuales, registran nuevos récords de inversión en nuevas tecnologías, enmarcándose como movimientos estratégicos con el futuro objetivo de fomentar el desarrollo y posicionamiento dentro del metaverso.

Tal y como indicaba Mark Zuckerberg, CEO de Meta, que ha apostado por el metaverso a pesar de asegurar que perderá cantidades importantes de dinero en los próximos años, ya que el proyecto del metaverso no será viable hasta, por lo menos, dentro de 10 años.

Meta ha destinado más de 10.000 millones de dólares al diseño del metaverso, sin embargo, ya ha perdido aproximadamente la mitad de la inversión económica. Al igual que otros gigantes tecnológicos como Google o Microsoft que también han hecho inversiones billonarias en el metaverso, previendo que al menos un cuarto de la población mundial pase mínimo una hora diaria en él. Además, el aumento de valor del mercado de la Realidad Virtual y la Realidad Aumentada hasta llegar a 4.000 millones de dólares, y la previsión de que esta cifra alcanzará los 36.000 millones, garantiza que, aunque no llegue a convertirse un imprescindible en nuestras vidas, existirá la adopción generalizada de algunos aspectos de nuestra vida diaria.

A nivel internacional, se ha de considerar que el metaverso es percibido por las potencias mundiales como el próximo escenario de confrontación de internet. En este sentido, las empresas chinas y estadounidenses son las que se encuentran más a la vanguardia del metaverso. Sin haberse conseguido un concepto global de este, las empresas norteamericanas están tratando de crear la infraestructura que sirva de base, mientras que China lo considera como una oportunidad para consolidar su hegemonía tecnológica, así como para impulsar su industria digital.

En el caso de la Unión Europea, destaca la puesta en marcha de algunas iniciativas legislativas, que puedan indicar la dirección que los reguladores pueden tomar con relación al

metaverso, enfocada en su supervisión y reglas, con el objetivo de ser pionera en dicho ámbito. No obstante, sin una sólida infraestructura, las industrias europeas del metaverso podrían verse abocadas únicamente a la prestación de servicios al consumidor.

En este contexto, cabe la posibilidad de que se genere una lucha entre tres enfoques distintos:

- Un enfoque normativo apoyado por los Estados;
- Un enfoque orientado a lograr una web libre, descentralizada y abierta para todo el mundo, así como el dinero digital y los derechos de propiedad integrados en protocolos automatizados. Por otra parte, la web seguiría controlada por grandes compañías y vigilada por el Estado. Este perspectiva sería impulsada por activistas tecnológicos;
- Una perspectiva dirigida a los negocios respaldado por el sector tecnológico, cuyo objetivo se basa en reclamar la propiedad del Metaverso a través del control de sus componentes.

En referencia al ámbito geopolítico del metaverso, es probable que se genere una lucha por la orientación y el dominio tecnológico entre el modelo occidental y el chino. Al respecto, ya existe en la actualidad una confrontación en el ámbito de la Inteligencia Artificial. Por su parte, Shanghái ha impulsado la utilización del Metaverso en los servicios públicos y las oficinas comerciales. Cabría mencionar que la falta de fronteras y reglas en el Metaverso podría desafiar la noción de soberanía territorial.

Implicaciones para la seguridad nacional

A **nivel tecnológico**, el Metaverso ocasionará una brecha digital entre los países. En el **ámbito político**, representará un escenario más para la propagación de la ideología política y la cultura de un país. En **materia laboral**, podría generar cambios en la estructura social mediante nuevos trabajos digitales, así como el desarrollo de pequeñas y microempresas en la economía digital. Finalmente, en cuanto a la **seguridad técnica**, es probable que se produzcan ataques a la red. Asimismo, los defectos técnicos de seguridad pueden ser aprovechados por atacantes cibernéticos. Por otro lado, también existirán vulnerabilidades en la creación de nuevas infraestructuras críticas (por ejemplo, si el sistema de almacenamiento funciona mal o es atacado podría conllevar pérdidas económicas considerables). Por último, también podrá existir manipulación, robo y fugas a gran escala en la tecnología de cadena de bloques (blockchain).

Implicaciones para el usuario

Las implicaciones que puede tener este escenario a nivel de los usuarios son diversas. En primer lugar, referidas a la **gestión de identidades**, que supondrán un aumento de los problemas de autenticación y de la suplantación de identidades. Asimismo, requerirá también de la digitalización de los gobiernos para la oferta a los nuevos ciudadanos digitales de nuevos servicios de gestión de pagos o formularios. En cuanto a la **seguridad y privacidad**

de los datos, existirá un aumento de las amenazas ya existentes (phishing, suplantación) y también una necesidad **normativa** de responsabilizar a los usuarios de sus actos, así como de proteger la propiedad intelectual. En términos **económicos y financieros**, existirán complicaciones asociadas al uso de criptomonedas con nuevos desafíos y vulneraciones a los usuarios y un aumento del fraude, especialmente en relación a los NFTs. En relación a la **seguridad física**, será necesario resolver los problemas asociados a los posibles abusos sexuales y también a los ataques infligidos para desorientar y dañar al usuario (p. ej. joystick humano). En cuanto a los problemas de **desinformación**, los usuarios tenderán a estar más polarizados y a ser más susceptibles de ser radicalizados y manipulados debido a los algoritmos de recomendación basados en los intereses, los sesgos del usuario y sus datos biométricos. También se producirá un aumento de la **incidencia de trastornos mentales**, emocionales y de adicción debido a esta nueva dimensión más inmersiva y reforzante de las redes sociales y el uso inapropiado de internet para evadirse de la realidad. Finalmente, también se producirá un aumento considerable de las **oportunidades** para los usuarios en el ocio (conciertos, cine, salas de reunión), la formación (simulaciones, clases digitales) o el desempeño en sus profesiones (reuniones).

Implicaciones para las empresas

La empresa es el aspecto más incierto del metaverso, debido a que todavía no está claro cómo se desarrollará la creación de este. Actualmente, existen dos versiones sobre la tendencia que adquirirá este universo digital próximamente. La primera de ellas se basa en arquitectura tecnológica descentralizada, como la infraestructura del blockchain, en la que diferentes comunidades pueden construir sus propios mundos. El objetivo de esto es un metaverso libre que no sea controlado por nadie. La otra, es un metaverso privatizado y centralizado creado por las grandes empresas como Meta, Microsoft y Apple. Habrá una rivalidad entre ambos modelos, pero lo más probable es que el metaverso empiece siendo centralizado y luego se vaya descentralizando según vaya aumentando la participación de las empresas, al igual que pasó en la evolución de internet. Por ello, la idea clave no es cuántas empresas van a participar en el metaverso, sino cuáles van a perdurar. Habrá competencia entre empresas por ganar terreno en el metaverso, con la incertidumbre de cómo será esta, ya que en principio la posición en el metaverso será aleatoria. La competencia entre empresas no solo será por el metaverso, sino también por los dispositivos físicos necesarios para acceder e interactuar con él.

Aparte de esto, habrá varios retos de seguridad que las empresas deberán superar. El primero de ellos es la **privacidad**, ya que al aumentar la experiencia del usuario aumentarán también el conjunto de datos que se tratan. Por ello, cualquier brecha de seguridad podría producir daños de gran alcance. El segundo aspecto es el **alcance de la seguridad**. En el metaverso podrían existir riesgos tales como la manipulación de este, contenidos ilícitos y nocivos en línea, posible expansión de ideologías extremistas unidos a la captación de individuos. Por ello será importante que exista una vigilancia del metaverso, el reto conseguir una seguridad eficiente que no menoscabe la privacidad del usuario. También será importante la **seguridad**

de los dispositivos del metaverso ya que, por ejemplo, la tecnología RV permite alterar las emociones y la conciencia del usuario. Una violación de la seguridad de esta daría la oportunidad de manipular al consumidor. Además, los hackers que accedieran a un dispositivo de este tipo podrían controlar lo que la víctima ve y oye, y podrían ver el interior de su lugar de trabajo o vivienda, lo que tendría importantes consecuencias para la seguridad física de esta. Por último, es importante la **integridad de los avatares**. Aunque a priori el metaverso será más seguro que internet, existe el riesgo del robo de identidad y la duplicación de avatares, con su consiguiente uso indebido, pueden vulnerar el derecho a la propiedad. La mejora de la autentificación de identidad será crucial para evitarlo.

5. Orientaciones

- Ante la realidad del metaverso, será fundamental la **adaptación** estatal, empresarial e individual a este entorno, venciendo esa resistencia al cambio para no quedarse atrás y perder proyección o desarrollo de los intereses particulares o como empresa.

- **Legislar** para proteger a los usuarios, empresas y gobiernos en términos de privacidad, gestión de identidades, seguridad física, terrorismo y desinformación en el metaverso.

- Aumentar la **inversión** en terrenos en el metaverso de Meta como en el caso de las empresas estadounidenses; Tencent, de otras empresas chinas, Dyson de Reino Unido, Aldin de Islandia y Sensorium de Rusia.

- Dentro del marco europeo, sería interesante **impulsar las empresas europeas** Dyson y Aldin, como elemento clave para la adaptación al metaverso.

- Para **reducir la brecha digital** que se produzca cuando el metaverso se convierta en una realidad, es importante aumentar la inversión en tecnologías asociadas al metaverso de aquellos países menos digitalizados.

- El metaverso supondrá un desafío para la seguridad en muchos ámbitos, aumentando la necesidad de crear capacidades efectivas de **ciber resistencia** y ciberseguridad de la UE, así como fomentar capacidades de ciber inteligencia de acuerdo al avance del metaverso, con protocolos y estrategias robustas y sofisticadas.

- Fomentar la **educación** de los usuarios para proteger sus identidades y activos con un objetivo de prevención de futuros problemas de salud mental asociados.

- La representación de espacios dentro del metaverso, supondrá la **alteración** de las experiencias de **lugares físicos**, afectando especialmente al sector turístico como en conciertos o eventos, implicando un cambio progresivo en el sector y sus costumbres.

- Considerar la **formación en trabajos que aún no existen**, orientando al trabajador a saber anteponerse y adaptarse a esta nueva realidad, invirtiendo en educación especialmente técnica, como las matemáticas e informática.

- Los Gobiernos necesitan coordinar el desarrollo y la seguridad en el proceso regulatorio, así como **implementar reglas técnicas y estándares éticos** de manera anticipada.

- Concebir el metaverso como una evolución más de internet, que aunque de carácter disruptivo e innovador, su desconocimiento no suponga rechazo, concienciar de que no abarcará al completo la realidad, sino que será un **binomio** con el que se convivirá al igual que en la actualidad con internet.

- Las características transnacionales del Metaverso implicarán una **cooperación** exploratoria y constructiva en el marco de la comunidad internacional, que aunque asumiendo cierta competitividad, se focalice en la colaboración para evitar los desafíos de seguridad.

6. Bibliografía

Evolución de internet

Santos González, Manuel. *Historia de Internet – nacimiento y evolución*. Redes telemáticas. Recuperado de https://redestelematicas.com/historia-de-internet-nacimiento-y-evolucion/

Metaverso

M. Ball (2022). *The Coming Worlds*. Recuperado de https://time.com/6197849/metaverse-future-matthew-ball/

T. Madiega,, P. Car, y M. Niestadt (2022). *Metaverse: Oportunities, risks and policy implications*. European Parliament. Recuperado de https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733557/EPRS_BRI(2022)733557_EN.pdf

Industry-Academia Summit (2019). *Mixed reality security, privacy, and safety summit report*. University of Washington. Recuperado de https://ar-sec.cs.washington.edu/files/MixedReality_SecurityPrivacySafety_Summit2019.pdf

F. Roesner, y T. Kohno (2021). *Security and Privacy for Augmented Reality: Our 10-Year Retrospective*. University of Washington. Recuperado de https://www.franziroesner.com/pdf/ARSec-10YearRetrospective.pdf

J. M. López (2022). *Cómo garantizar la seguridad de los datos en el metaverso*. Recuperado de https://blogthinkbig.com/seguridad-informacion-metaverso

T. Basu (2022). *El reto casi imposible de ofrecer seguridad y privacidad en el metaverso.* MIT Technology Review. Recuperado de https://www.technologyreview.es//s/13950/el-reto-casi-imposible-de-ofrecer-seguridad-y-privacidad-en-el-metaverso

Europol (2022). *Policing in the Metaverse: What law enforcement needs to know*. Recuperado de https://www.europol.europa.eu/cms/sites/default/files/documents/Metaverse_Report.pdf

P. Casey, I. Baggili y A. Yarramreddy (2021). *Immersive Virtual Reality Attacks and the Human Joystick*. Recuperado de https://dl.acm.org/doi/10.1109/TDSC.2019.2907942

T. Parisi (2021). *The Seven Rules of the Metaverse.* Recuperado de https://medium.com/meta-verses/the-seven-rules-of-the-metaverse-7d4e06fa864c

L. Christensen y A. Robinson (2022). *The Potential Global Economic Impact of the Metaverse*. Recuperado de https://www.analysisgroup.com/globalassets/insights/publishing/2022-the-potential-global-economic-impact-of-the-metaverse.pdf

Telefónica (2022). *Retos sociales y éticos del metaverso*. Recuperado de https://www.telefonica.com/es/wp-content/uploads/sites/4/2022/05/Social-and-ethical-challenges-metaverse-ES.pdf

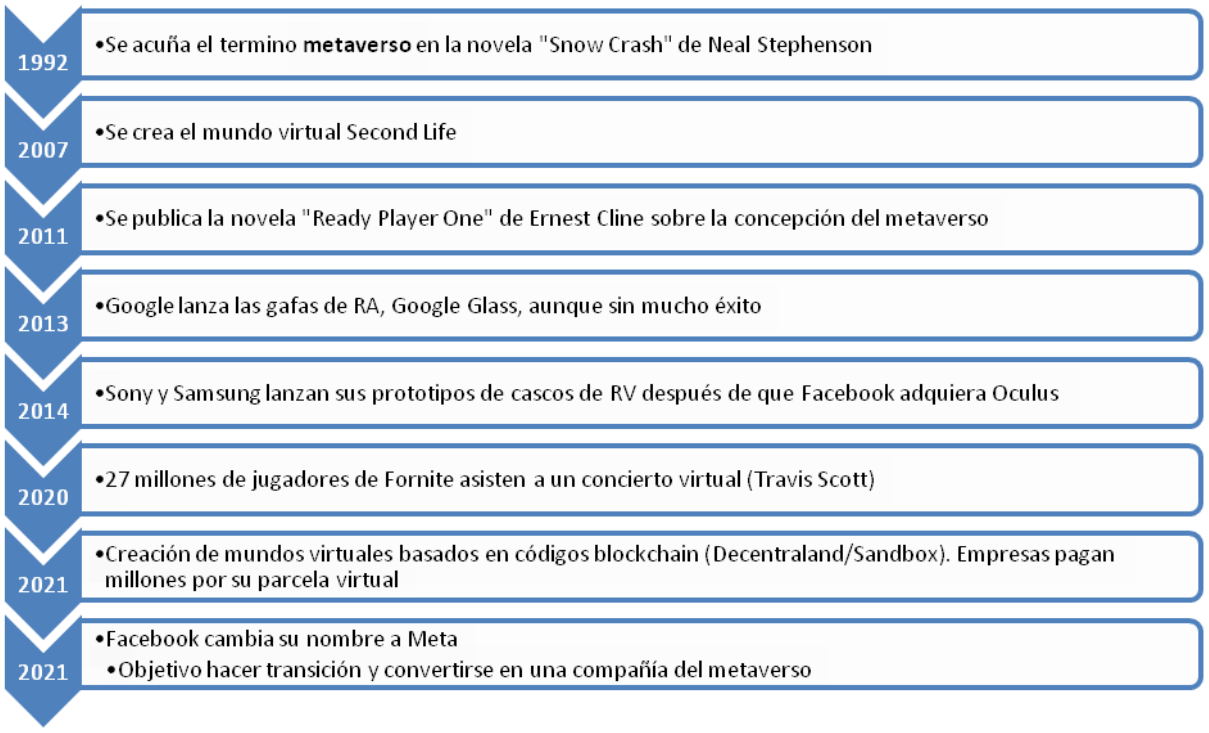
Janet Abbate Universidad Politécnica de Virginia, Abbate, J. and Virginia, U.P.de (no date) *Internet: Su Evolución y Sus Desafíos*, *OpenMind*. Available at: https://www.bbvaopenmind.com/articulos/internet-su-evolucion-y-sus-desafios/

Ruiz, A. *et al.* (2022) *Marketing 4 ecommerce - tu revista de marketing online para E, commerce*. Available at: https://marketing4ecommerce.net/

7. Anexos

Anexo 1

Evolución del metaverso



Fuente de elaboración propia