CENTRO
DE COMPETENCIAS
TECMILENIO

Aspectos generales del metaverso

Tema 7

Protección, validación de identidad y cuestiones legales

Introducción

Sin duda alguna, durante la pandemia por el COVID-19, la masividad por el consumo de datos y las nuevas dinámicas de trabajo y colaboración generaron y concedieron el desplazamiento del ser físico por la representación digital o a través de plataformas digitales.

Debido a la necesidad de socializar y buscar alternativas para hacerlo, aunado a la ubicuidad del Internet, provocan un gran deterioro sobre los conceptos de los espacios íntimos y privados, los cuales se vuelven todo lo contrario; por lo que los espacios de interacción se centran en tener un dispositivo que permita ser el intermediario entre el mundo virtual y la realidad. Con ello se genera una brecha de seguridad entre el ser real y los espacios que no lo son.

Explicación

Protección y validación de identidad

El surgimiento de los diversos mundos virtuales ha aumentando exponencialmente en los últimos dos años, siendo el metaverso uno de los elementos que continuarán evolucionando. Se identifican dos grandes retos: la protección y validación de identidad de los usuarios. Estos conceptos juegan un papel primordial para evitar delitos, proveer y garantizar una óptima experiencia.

De acuerdo con lo que comentan De Asis et al., (2022), la transformación digital de la justicia es un proceso que se ha iniciado, pero queda mucho camino por recorrer. Aunque hoy en día existen normas y leyes sobre la protección de datos que transfieren a los responsables del tratamiento del uso de los datos personales, es indispensable tomar conciencia y no dejar de lado el compromiso que tenemos como personas capacitadas para tomar decisiones, tener la cultura de responsabilidad al hacer transacciones, compras, o adquisición de cualquier tipo en los mundos virtuales.

Es de suma importancia comprender que un entorno que pretende ser una réplica del mundo real, también se repliquen fraudes y todo tipo de robos que existen actualmente en la realidad.

Como indica Orellana (2022), algunos siniestros que pueden ocurrir son los siguientes:

Robo de identidad:

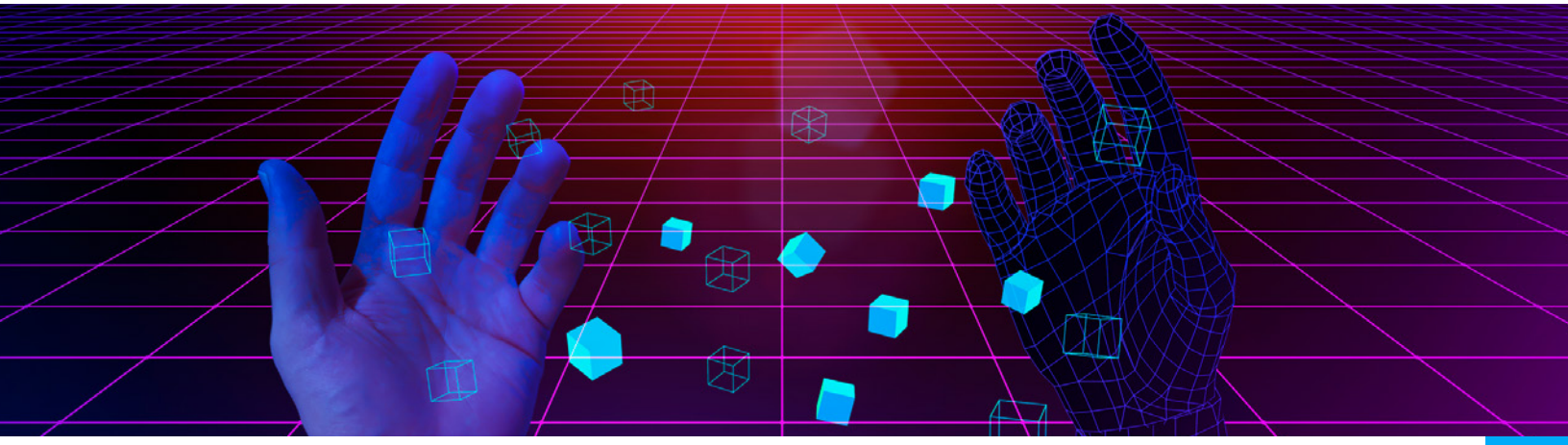
Uso incorrecto de tu información personal.

Ingeniera social:

Acoso o robo de datos a los usuarios más vulnerables originados por las brechas de seguridad.

Protección a la propiedad:

Existencia de reglas sobre derechos de autor y protección legal de los activos virtuales adquiridos.



Riesgos en el metaverso
Por ser una nueva tecnología, el metaverso recibe sus primeras preocupaciones sobre la privacidad y la seguridad. El uso de esta herramienta no es una situación tranquila y segura, ya que como todas las nuevas tecnologías tienen su lado negativo. La Realidad Aumentada (AR) y la Realidad Virtual (VR), que proporcionan la interfaz del metaverso, son las mismas que lo impulsan y que también afectan con sus propios problemas de seguridad y privacidad.

Riesgos de seguridad en la realidad aumentada
La realidad aumentada (AR), se considera un fundamento básico del metaverso. Abre una serie de nuevas posibilidades para cambiar los vínculos entre el mundo virtual y físico. No obstante, también es la culpable de una serie de importantes problemas de seguridad, principalmente en la privacidad del usuario. Los siguientes puntos muestran las vulnerabilidades a considerar de seguridad como resultado de la realidad aumentada y la inteligencia artificial en la red.

- *¿Cómo utilizan y protegen las empresas de AR la información obtenida de los usuarios?*

- *¿Dónde guardan las empresas los datos de AR y qué mecanismos de cifrado utilizan?*

- *¿Comparten las empresas de AR los datos con terceros? Y si es así, ¿por qué razón y cómo se utilizan estos datos?*

Todas estas preocupaciones ponen de manifiesto las vulnerabilidades de la seguridad en el metaverso, incluyendo robo de credenciales, ingeniería social y denegación de servicios (DOS).

Ataques de ingeniería social
Hoy en día cualquiera podría utilizar la documentación adecuada para confirmar su identificación en el mundo real, pero los usuarios en el metaverso deben emplearse con avatares digitales para verificar la voz, registros de video y rasgos faciales. Los aparatos de realidad aumentada y realidad virtual permiten a los usuarios relacionarse entre sí, utilizando técnicas de ingeniería social o estrategias de robo de identidad. Los *hackers* pueden persuadir a los usuarios para dar información personal y que permitan deducir contraseñas importantes.

Robo de credenciales
Se considera que la dificultad mayor en el metaverso para los usuarios es detectar el robo de credenciales. Esto podría poner en peligro la información personal y datos financieros de los usuarios que están guardados en sus cuentas.

Riesgos de seguridad en la Realidad Virtual (VR)
La tecnología de realidad virtual cuenta con una serie de notables problemas de privacidad; muchos de estos surgen de los datos recogidos por la misma tecnología como los escaneos de retina, el uso de datos biométricos, las huellas dactilares o patrones de voz, por mencionar algunos.

Reducción de la percepción del espacio físico
Perder la conexión natural con el mundo real es uno de los mayores desafíos entre los problemas existentes en el metaverso, más allá de los límites de seguridad y privacidad. La VR aísla a la persona de su mundo real durante un tiempo determinado, estando dentro de la VR se pierde noción del espacio tiempo en su mundo real, llevando al usuario a tener accidentes físicos por perder la noción de que la VR y su mundo real no son de las mismas dimensiones.

Conclusión

El metaverso no consiste únicamente en crear aplicaciones basadas en la tecnología *blockchain*. Las tecnologías de realidad aumentada y virtual en el mundo del metaverso pueden dar lugar a una serie de vulnerabilidades de seguridad y privacidad, como ataques de ingeniería social, *ransomware*, robo de credenciales en la red y robo de identidad. Los hackers pueden ser capaces de secuestrar la identidad de un usuario dentro del mundo metaverso, explotando las debilidades de los dispositivos de AR y VR. Además, la falta de una conexión visual y sonora con el mundo físico (mundo real) hace que el metaverso sea un riesgo para la seguridad física. Lo más significativo es que la polarización y la radicalización en el metaverso son un enorme problema de seguridad y privacidad.

Referencias bibliográficas

- De Asis, R., Belloso, N., Bini, S., Campione, R., Casadei, T., De Asis, M., y García, D. (2022). *Inteligencia artificial y filosofía del derecho*. Recuperado de https://idus.us.es/bitstream/handle/11441/137250/Inteligencia%20artificial_Llano%20Alonso.pdf?sequence=1&isAllowed=y

- Orellana, R. (2022). ¿Es seguro el metaverso? Los 5 riesgos asociados a esta tecnología. *Digital Trends Español*. Recuperado de https://es.digitaltrends.com/sociales/es-seguro-el-metaverso-cinco-riesgos/