CIBERSEGURIDAD: EL PELIGRO AL ACECHO DE LOS NIÑOS, NIÑAS Y ADOLESCENTES

Laura Camila Peñuela Jiménez[1]

RESUMEN

Los niños, niñas y adolescentes son sujetos de especial protección en el derecho, es por ello que como sociedad su seguridad y bienestar son uno de los principales objetivos, sin embargo las nuevas generaciones cuentan con acceso directo y fácil a través de las nuevas tecnologías a la espacios como la WEB 3.0 o el Metaverso, espacios nuevos para muchos, inexplorados y blancos para ciberdelitos. Existen testimonios de adultos acerca de sus acciones en la WEB 3.0 o el Metaverso, quienes incluso siendo personas conscientes de las normas y peligros a los que se exponen, han caído en las trampas y engaños de personas inescrupulosas convirtiéndose en víctimas de los diferentes ciberdelitos. Es por ello que es necesario analizar la seguridad y el peligro ante los cuales se encuentran expuestos los niños, niñas y adolescentes quienes navegan a través de la WEB 3.0 o el Metaverso gran parte del tiempo.

PALABRAS CLAVE

Adolescentes, Ciberdelito, Ciberseguridad, Metaverso,Niños, WEB 3.0

ABSTRACT

Children and adolescents are specially protected by law, which is why as a society their safety and welfare are one of the main objectives, however, new generations have direct and easy access through new technologies to spaces such as WEB 3.0 or the Metaverse, new spaces for many, unexplored and targets for cybercrime. There are testimonies of adults about their actions in the WEB 3.0 or the Metaverse, who even being aware of the rules and dangers to

[1] Universidad Santo Tomás sede Villavicencio; Laurapenuelaj@usantotomas.edu.co

which they are exposed, have fallen into the traps and deceptions of unscrupulous people becoming victims of various cybercrimes. That is why it is necessary to analyze the security and danger to which children and adolescents are exposed, who navigate through the WEB 3.0 or Metaverse most of the time.
KEY WORDS
Adolescents, Cybercrime, Cybersecurity, Metaverse, Children, WEB 3.0, Cybercrime, WEB3.0

INTRODUCCIÓN

El internet se encuentra en constante evolución, hoy en día se conoce la WEB 3.0, a través de la cual muchas personas tienen la oportunidad de realizar diferentes actividades, de tal forma que se podría afirmar que es necesario para las actividades diarias, desde el inicio del día con apps que funcionan como despertadores, agendas, cronogramas, relojes los cuales a través de la web se conectan a nivel mundial, incluso algunos usan la WEB 4.0 al contar con sistemas de Google Home o HomeKit de Apple.

Al ser una plataforma con tantos beneficios y a la cual accede muchas personas están expuestos a diferentes peligros en un inicio era común escuchar recomendaciones Cómo aquellas de: 1) No enviar información personal, 2)No registrar nombres reales, 3) No enviar claves, contraseñas, códigos de seguridad a través del mismo, 4)No confiar en cualquier correo o mensaje, esto con el fin de evitar la comisión de diferentes ciberdelitos, aquellos como la infección de un malware, los ataques de phishing y pharming keylogger, botnet y crypto jacking.

Sin embargo, a pesar de existir los diferentes protocolos de seguridad y mecanismos de ciberseguridad establecidos por las diferentes entidades y plataformas muchas personas han sido víctimas de los ciberdelitos mencionados anteriormente.

De esta forma es posible afirmar que aún contando con el conocimiento de los métodos o protocolos y de los diferentes ciberdelitos personas adultas que son conscientes de los diferentes casos de otras víctimas, que conocen y leen cada uno de los términos y condiciones que acepta y aún así son víctimas de ciberdelitos.

Ahora bien, los niños y niñas de las últimas generaciones han tenido un contacto a temprana edad con las diferentes tecnologías y con acceso directo al internet, de esta forma conociendo el uso de las diferentes plataformas desde funciones educativas, plataformas de streaming y videojuegos. Desde una visión cercana se podría pensar que el uso del internet en estas categorías no podría generar un peligro para los niños y niñas que hacen uso de estas plataformas ya sea para educación o entretenimiento. Sin embargo es necesario analizar que

muchos adultos han sido víctimas de ciberdelitos; así como existen muchos niños, niñas y adolescentes que se encuentran en el uso de las mismas plataformas, de esta forma se debe cuestionar ¿Los niños, niñas y adolescentes se encuentran en peligro al hacer uso del internet, de plataformas educativas, entretenimiento e incluso el Metaverso?

1. LOS NIÑOS Y NIÑAS, LA NUEVA GENERACIÓN EN LA WEB 3.0

Las nuevas generaciones nacen teniendo un acceso directo con la tecnología e ingresando a la WEB 3.0, desde el momento en que los padres sustituyen su responsabilidad de prestar atención al menor con una tablet o ipad para distraerlo durante largos periodos de tiempo. Incluso se refiere a la generación Z aquella que nació en el mundo de las tecnologías y generación Alfa aquellos que cuentan con el 100% de tecnología en su entorno desde el momento en que nacen, es por ello que es evidente que se presentarán choques culturales entre las diferentes generaciones.

En la actualidad quienes son adultos han tenido que realizar la transición de aprender y conocer cómo funcionan las nuevas tecnologías; una característica particular de esta generación, es que se pueden identificar aquellos que nacieron sin tecnologia e internet a su alcance por lo cual tienen desconfianza y precaución ante las diferentes acciones que se puedan realizar por medios electrónicos y a pesar de esto no ha sido suficiente para evitar que sean víctimas de situaciones comunes como la estafa, robo de datos o incluso el ataque con algún malware, entre otros.

A diferencia de la generación Z y Alfa se evidencia un aire de superioridad al poder conocer el funcionamiento y manejo de las tecnologías y el internet; de tal forma que se ignora por completo las advertencias y precauciones establecidas por las plataformas, aceptando términos y condiciones sin leerlas previamente. Un punto importante resulta ser la participación de los padres o tutores al tener la responsabilidad de conocer el tipo de contenido o plataformas a las cuales accede el menor.

A medida que los niños y niñas se encuentran creciendo acceden a dos tipos de contenido comúnmente, el primero un contenido audiovisual y el segundo los videojuegos.

El primero se puede evidenciar en plataformas de video, ya sea contenido educativo, de juegos, comida, series o programas; en un inicio puede resultar un espacio con beneficios como los tutoriales para aprender algo nuevo, repasar temáticas o conocer de algo en específico; sin embargo muchas veces los padres o tutores a cargo del menor no tienen las medidas necesarias

como los controles parentales de las apps y dejan al azar la navegación del menor por las diferentes plataformas.

Claramente existen diferentes plataformas que se han establecido parámetros para evitar que los menores estén expuestos a contenido no apto para ellos un ejemplo es YouTube qué ante cualquier infracción de la persona que suba el video bloquea la cuenta y elimina el video para el público.

Por el contrario existen plataformas como tiktok qué no cuentan con tal regulación o no es tan estricta ya que a través de los hashtags los niños, niñas y adolescentes pueden acceder a contenido sexual o pornográfico sin ningún tipo de filtro. Un caso en particular son las plataformas de streaming como lo es Netflix o Disney plus en la cuales se encuentra que para evitar que los menores acceden a contenidos no apto para ellos establecen los límites de edad para cada contenido y permiten el "control parental" una opción aparentemente sencilla pero qué puede contribuir a que los menores no accedan a contenido no apto para su edad.

Por otro lado encontramos niños niñas y adolescentes que disfrutan del contenido de entretenimiento a través de los videojuegos, los cuales se juegan en línea, es decir el menor está teniendo contacto con diferentes personas de manera remota mientras participa en el videojuego.

A través del videojuego el menor está teniendo contacto con una persona a quién no le ve su rostro o su identidad de esta forma el menor se está exponiendo a interactuar con personas desconocidas qué en un buen caso puede ser un niño o niña de su misma edad o en una situación negativa podría ser un adulto con intenciones negativas ya sea de abuso, acoso o situaciones de grooming en la cual está simulando ser un menor de edad para ganar la confianza del menor.

Ante el anterior escenario pueden surgir diferentes consecuencias una de ellas es que el menor establezca confianza con esta persona y sufre algún tipo de abuso; o por medio de la confianza la persona acceda a datos del grupo familiar o del hogar con el fin de estafar o robar.

Es por ello que en este punto ya podemos evidenciar qué el internet es una herramienta valiosa y que contribuye a en situaciones de tiempo, a las facilidades y a la realización de las diferentes actividades del ser humano. Sin embargo el internet es una plataforma tan amplia a la cual todas las personas tienen acceso y que no todas las apps o plataformas cuentan con ciberseguridad y controles parentales para resguardar la integridad y los derechos de los niños, niñas y adolescentes.

Otro punto evaluar de los videojuegos el tipo de contenido que transmite cada videojuego esto en consecuencia de que muchos de los videojuegos suelen compartir contenido violento o explícito al cual muchos menores tienen acceso, estando expuestos a situaciones explícitas de

violencia, sexuales y de contenido no apto para menores, un ejemplo es un videojuego que se ha hecho viral llamado Huggy Wuggy.

Su misión en el videojuego, que transcurre en una fábrica de juguetes abandonada y donde el participante se tiene que ir escapando de juguetes malvados, es abrazar hasta dejar sin aliento. A pesar de que el videojuego no se recomienda para niños de menos de 12 años, Huggy Wuggy se ha viralizado, gracias sobre todo a YouTube y TikTok, en todo el mundo (solo hay que hacer una búsqueda en cualquier red social) hasta el punto que ha conseguido salir de las pantallas y convertir su formato de peluche en uno de los más reclamados entre los niños de 5 a 12 años. (Escriche, 2022)

Ante esto, es importante aclarar que la violencia no es una actividad cotidiana del ser humano y que solo en casos de supervivencia llegaría aparecer, pero en el caso de los menores que se encuentran en una etapa de crecimiento y desarrollo, quienes copian y adaptan todas las situaciones que observan de su alrededor, por lo cual se podría evidenciar qué los menores adapten rasgos violentos a sus conductas basado en el personaje mencionado anteriormente ya que en el desarrollo del videojuego es través de los abrazos que genera la muerte y dolor a los otros.

Un factor importante en esta situación es que las personas conocen el contenido del videojuego, siendo explícitamente violento e incitador a la violencia, las personas difunden y comparten este videojuego hasta el punto de convertirse en información viral, la cual es una característica atractiva para las nuevas generaciones que viven a través de las tendencias

Otro juego con contenido no apto para menores es Roblox, esto es razón que el contenido explícito y sexual es de categoría adulta y solo esta población debería tener acceso al mismo, por consiguiente ningún menor debe tener acceso a este tipo de contenido por las diferentes consecuencias que establecen en su desarrollo.

El juego ROBLOX que es la novedad entre niños al ser una plataforma para crear juegos y aunque cuenta con estrictos protocolos de seguridad, los jugadores sin importar su edad pueden acceder de forma rápida y sencilla a encuentros de índole sexual.

Está plataforma establece algo particular y es el hecho de que incluso los adultos se han sentido vulnerados al usarla porque en un inicio las personas encontrarán divertido crear salas de juegos el inconveniente surge cuando dichas Salas son invadidas por avatares imitando contenido sexual. (León, 2022)

De esta forma a pesar de que el Internet tiene beneficios es evidente que hace falta regular diferentes plataformas o contar ciberseguridad y controles parentales al momento de ingresar a ellas, ya sea a través de filtros para identificar a los adultos de los niños porque incluso si

existe contenido que resulta incómodo o abusivo para los adultos, las secuelas que puede generar en un niño al tener acceso a ellas pueden llegar a ser irremediables a nivel psicológico y desarrollo.

2. LOS PELIGROS DE LA WEB 3.0 Y EL METAVERSO

Los ciberdelitos dia a dia se convierten en el blanco de muchos delincuentes qué a través de la confianza de las personas las convierten en víctimas de los mismos, es por ello qué es importante exponer diferentes situaciones a las que cualquiera podría estar inmerso. En un inicio contamos con aquella situación en la cual el el adulto responsable cuenta con sus datos bancarios guardados en su laptop a la cual por x motivo el menor tiene acceso, ya sea para jugar algún videojuego o consumir algún tipo de contenido de visual; los menores no cuentan con esta responsabilidad o conciencia económica de identificar cuando realmente se debe efectuar una compra y realizar transacciones.

Por ello un menor que tenga acceso a datos bancarios podría realizar compras de de contenido de videojuegos, ya sea equipaje, ropa, modificaciones para su avatar o dado el caso comprar a través de plataformas cosas que resulten interesantes, que a partir de la inocencia de un niño es algo sencillo y lo haría por su bienestar y diversión. Ante esta situación se podría decir que existen soluciones como la devolución y el trámite con el respectivo banco o la plataforma de ventas.

Una situación de peligro en la ciberseguridad ocurre en el momento en que dichos datos son difundidos de manera errónea a través de una plataforma, un juego, un chat o incluso como se mencionó anteriormente al establecer confianza con alguno de los otros jugadores el menor dentro de su ingenuidad compartiría dichos datos confiando en su “Nuevo amigo”. Facilitando situaciones de robos, estafas o incluso fraude de identidad cómo se identifica en Estados Unidos.

Es un delito que provoca escalofríos en padres y abuelos: un delincuente roba la identidad de un niño y utiliza sus datos personales para abrir cuentas de tarjetas de crédito o realizar compras con su celular. Estos delitos pueden pasar desapercibidos durante años porque los niños no declaran impuestos ni solicitan préstamos, lo que normalmente indicaría un fraude de identidad. (Masterson, 2022)

Una situación ejemplo diferente es aquella en la cual por medio de la confianza el menor establecer lazos de amistad con un completo desconocido a través de las diferentes plataformas de videojuegos y a través de esta confianza podría llegar a ser víctima de pornografía infantil.

Un punto importante en la actualidad es la innovación del metaverso, aquella realidad virtual a la que se puede acceder con los dispositivos adecuados a través de un avatar pero en el cual se encuentra un mundo dónde se pueden realizar diferentes actividades. Sin embargo al ser un espacio tan nuevo no cuenta con las regulaciones necesarias para establecer ciberseguridad o en dado caso, los parámetros para el uso del mismo porque existen muchas cuestiones: en un inicio ¿quién sería el encargado de regular el metaverso? ya que alrededor del mundo todas las personas lo usan y de ser así no correspondería a sus inversores y a sus creadores regular pero dicha regulación ¿Cómo podría relacionarse con la regulación interna de cada uno de los países que hacen parte? A partir de esta pregunta se generan muchos más interrogantes pero el principal es ¿el metaverso cuenta con los filtros necesarios para evitar que un menor acceda contenido explícito y no apto para su edad, para poder garantizar una infancia y adolescencia adecuada y sana dentro de los parámetros de la tecnología?

Existe casos de personas adultas sintiéndose violentadas y abusadas dentro del metaverso, de esta forma, si una persona adulta consciente de la realidad, consciente de que se encuentra en una realidad virtual, que se identifica con un avatar y desafortunadamente sintió ser violentada (Frutos, 2022) se siente violentada por actos dentro del metaverso un espacio y que uno es regulado ¿qué se podría esperar para los menores dentro de un espacio con tanto libertinaje?

Por otro lado, un riesgo que no se podría establecer como ciberdelitos pero que se encuentra en el desarrollo de los menores con la tecnología y el internet son las tendencias, hoy en dia existen los influencers que a través de las redes sociales y el internet, difunden mensajes y tendencias entre los jóvenes y lo que se evidencia actualmente entre los menores y los jóvenes es aquella pérdida de identidad por consumir contenido sin creatividad, que mueve masas con ideas vacías, porque al querer ser como un influencer, al querer imitar sus comportamientos su forma de vestir y su forma de actuar se está generando un conflicto en el desarrollo de cada uno de los menores.

3. CIBERSEGURIDAD PARA NIÑOS Y NIÑAS

La ciberseguridad es importante para la protección de datos, el uso correcto de las plataformas, los videojuegos, el internet y todo aquello que lo compone. Es por ello que se han implementado algunas estrategias para proteger a los niños, niñas y adolescentes de las amenazas que se pueden presentar en el internet.

La iniciativa se desarrolla dentro del convenio firmado entre el Ayuntamiento de Cuenca y el Incibe, entidad cuya misión es reforzar la ciberseguridad, la confianza y la protección de la información y la protección de la información y privacidad en los servicios de la Sociedad de

la Información, aportando valor a ciudadanía, empresas, administraciones, red académica y de investigación española, sector de las tecnologías de la información y las comunicaciones, y sectores estratégicos en general. (VocesdeCuenca, 2022).

Esta iniciativa de España podría ser una estrategia didáctica que otros países podrían adaptar a su cultura, en razón que el internet y la ciberseguridad no son temáticas exclusivamente de España, sino que nos competen a todos alrededor del mundo, los niños, niñas y adolescentes deben ser instruidos sobre los peligros a los cuales se encuentran expuestos y cómo evitarlos, los ciberdelitos se enfrentan teniendo conocimiento de ellos y de las formas para evadirlos y no ser una víctima más.

Otro ejemplo lo ha tomado Chile y Colombia, quienes a través de su gobierno han difundido una serie de consejos para evitar que los niños, niñas y adolescentes estén expuestos a los peligros de las plataformas.

Entel, en conjunto con el Equipo de Respuesta ante Incidentes de Seguridad Informática Entel, (CSIRT) de Gobierno, dependiente del Ministerio del Interior, han elaborado una serie de consejos para navegar de manera segura. En esa línea, existen softwares o aplicaciones para dispositivos móviles que permiten realizar un control del uso y así aportar al cuidado responsable para una navegación más segura. (Televisión Regional, 2022).

De esta forma se puede concluir que los gobiernos deberán a través de la didáctica y la academia instruir a las personas, en especial a los niños, niñas y adolescentes de los diferentes ciberdelitos a los cuales se encuentran expuestos al hacer uso del internet o la WEb 3.0 e incluso del Metaverso, pues con un solo click cualquier persona puede llegar a robar información extremadamente importante y confidencial para cualquier persona. Por ello, las campañas de socialización y concientización resultan ser un mecanismo clásico pero en muchas ocasiones efectivo. Así como invertir en la ciberseguridad de las diferentes plataformas es otra de las posibles soluciones o prevenciones ante los ciberdelitos, estableciendo un espacio seguro para todos los niños, niñas y adolescentes.

Bibliografía

Escriche, E. (2022). *Huggy Wuggy, el peluche que tus hijos quieren pero no deberían tener.* ara. Recuperado de: https://es.ara.cat/sociedad/huggy-wuggy-muneco-peluche-no-deberia-recomendado-ninos_1_4432784.html

Frutos, A. (2022). *Escándalo en el metaverso: una mujer declara ser víctima de una violación virtual.* La vanguardia. Recuperado de: https://www.lavanguardia.com/tecnologia/20220203/8032429/escandalo-metaverso-mujer-violacion-virtual-nbs.html

León, C. (2022). *Roblox, un juego "inofensivo" que expone a niños a contenido no apto.* Posta. Recuperado de: https://www.posta.com.mx/nuevo-leon/roblox-un-juego-inofensivo-que-expone-a-ninos-a-contenido-no-apto/579176

Masterson, K. (2022). *Los niños se convierten en blanco para el robo de identidad y el fraude.* AARP. Recuperado de: https://www.aarp.org/espanol/dinero/estafas-y-fraudes/info-2022/robo-de-identidad-infantil.html

Televisión Regional. (2022). *Ciberseguridad: consejos para resguardar a los niños en estas vacaciones de invierno.* Televisión Regional. Recuperado de: https://www.itvpatagonia.com/cultura/ciberseguridad-consejos-para-resguardar-a-los-ninos-en-estas-vacaciones-de-invierno/2022/07/06/62c5bca051144200092ea6e1

Voces de Cuenca. (2022). 'Cuenca Game' conciencia a niños y jóvenes sobre ciberseguridad para un uso seguro de internet. Voces de Cuenca. Recuperado de: https://www.vocesdecuenca.com/cuenca/cuenca-game-conciencia-a-ninos-y-jovenes-sobre-ciberseguridad-para-un-uso-seguro-de-internet/