Artículo de Investigación

Intervención didáctica para minimizar la ciber victimización de adolescentes

Educational intervention to minimize the cyber victimization of teenager

Haz, Lídice; Dávila, Araceli;
Domínguez, Mariela; Campuzano, María Gabriela

Lídice Haz
lhaz@upse.edu.ec
Universidad Estatal Península de Santa Elena, Ecuador

Araceli Dávila
araceli.davilam@ug.edu.ec
Universidad de Guayaquil, Ecuador

Mariela Domínguez
gdominguezgomez@upse.edu.ec
Universidad Estatal Península de Santa Elena, Ecuador

María Gabriela Campuzano
mcampuzano@upse.edu.ec
Universidad Estatal Península de Santa Elena, Ecuador

Pro Sciences: Revista de Producción, Ciencias e Investigación
CIDEPRO, Ecuador
e-ISSN: 2588-1000
Periodicidad: Trimestral
Vol. 6, No. 45, 2022
editor@journalprosciences.com

Recepción: 17 Junio 2022
Aprobación: 22 Agosto 2022

DOI: https://doi.org/10.29018/issn.2588-1000vol6iss45.2022pp119-135

Resumen: Los avances tecnológicos en los últimos años han contribuido a grandes cambios sociológicos. La globalización y los cambios en los diferentes ámbitos de la comunicación han propiciado una temprana adopción de las tecnologías de la información y la comunicación (TIC). Esta situación, conlleva a que los usuarios especialmente menores de edad se expongan a riesgos y amenazas derivados del mal uso de las TIC y el internet. La victimización en entornos virtuales es más evidente en menores de edad quienes sufren una violencia silenciada pero con consecuencias psicológicas graves. Es importante conocer y hacer visible este fenómeno para saber cómo abordarlo. El objetivo de este trabajo es describir las características y las consecuencias de las diferentes formas de victimización en entornos virtuales, tales como *grooming*, *sexting* y *ciberbullying*. También, se presentan algunos mecanismos de prevención para mitigar estos tipos de acosos; además, se detalla la propuesta de un programa de formación académica en seguridad informática dirigida a menores de edad, con la finalidad de que aprendan a utilizar y convivir de manera adecuada en los entornos virtuales generando mayor interés, conciencia y reflexión sobre los riesgos presentes en estos medios.

Palabras clave: grooming, sexting, ciberbullying, victimización, entornos virtuales.

Abstract: Technological advances in recent years have contributed to major sociological changes. Globalization and changes in the different areas of communication have led to an early adoption of information and communication technologies (ICT). This situation means that users, especially minors, are exposed to risks and threats arising from the misuse of ICTs and the Internet. Victimization in virtual environments is more evident in minors who suffer silenced violence but with serious psychological consequences. It is important to know and make this phenomenon visible in order to know how to deal with it. The objective of this work is to analyze the characteristics and consequences of the different forms of victimization in virtual environments, such as grooming, sexting and cyberbullying. Also, some prevention mechanisms are presented to mitigate these types of harassment; In addition, a proposal is presented for an academic training program in computer

Cómo citar: Haz, L., Dávila, A., Domínguez, M., & Campuzano, María G. (2022). Intervención didáctica para minimizar la ciber victimización de adolescentes. Pro Sciences: Revista De Producción, Ciencias E Investigación, 6(45), 119-135.https://doi.org/10.29018/issn.2588-1000vol6iss45.2022pp119-135

security aimed at minors, in order for them to learn to use and coexist appropriately in virtual environments, generating greater interest, awareness and reflection on the risks present in virtual environments. these means.

Keywords: grooming, sexting, ciberbullying, victimization, virtual environments.

Introducción

El panorama cambiante de la tecnología promueve nuevos mecanismos por los cuales se puede infligir daño. Diversos enfoques investigativos pueden ayudar a profesionales del área académica, político, social o empresarial a intervenir de una manera adecuada y válida respecto a la sobreexposición de información personal de los menores en internet y redes sociales ante una serie de riesgos para su privacidad, integridad, propia imagen y desarrollo de la personalidad.

El acoso en línea se materializa de diferentes maneras tales como, mensajes que generan pánico, amenazantes, emocionalmente dañinos o sexuales que son entregados a través de un medio digital o electrónico generando en las victimas sentimientos de angustia o miedo de forma similar al acoso y acecho del mundo real (Villacampa & Gómez, 2016; Bossler et al., 2012). Uno de los grandes problemas de victimización en línea es el ciberbullying. Esto es, transmitir texto, enviar o publicar imágenes hirientes o crueles a través de internet sea esta por mensajería instantánea, salas de chat, correos electrónicos o por redes sociales (Pittaro, 2009).

Sin embargo, el ciberbullying no es el único tipo de acoso que las personas sufren en un entorno virtual. También existe el grooming donde los acosadores utilizan el anonimato en internet, y se hacen pasar por menores de edad. Esto con el fin de establecer comunicación con otros menores o adolescentes hasta generar un vínculo de confianza y luego obtener control emocional de los mismos para finalmente chantajearlos con fines sexuales (The Children, 2021).

Otra situación problemática en entornos virtuales es el sexting, el cual se refiere explícitamente al intercambio de material altamente sexual o de contenido provocante ya sea por fotos, mensajes de texto o videos a través de internet, un teléfono celular o redes sociales (Morelli et al., 2016).

En este trabajo se analizan las características de las diferentes formas de victimización en entornos virtuales. También, se presentan algunos mecanismos de prevención para mitigar estos tipos de acosos; y se describe la propuesta de un programa de formación académica en seguridad informática dirigida a menores de edad, cuyo fin es el uso seguro y responsable de las TIC, generando mayor interés, conciencia y reflexión sobre los riesgos presentes en el uso de las tecnologías e internet.

Victimización en entornos virtuales

Los patrones de asociación han cambiado a lo largo de las décadas teniendo en cuenta factores psicológicos y sociales como el género y el entorno tecnológico. En este sentido, la proliferación de dispositivos electrónicos como medio de comunicación incansable para crear, descubrir y mantener nuevas amistades es tan beneficioso, ya que la comunicación, a través de la red, promueve estándares de interacción interpersonal similares a los que ocurren en el espacio físico de manera positiva y negativa (Pacheco, 2018).

El uso de dispositivos tecnológicos como videojuegos, tabletas y teléfonos inteligentes conectados a internet forman parte de la cotidianidad infantil, ya sea en el hogar o en las instituciones educativas. Las ventajas que ofrecen las innovaciones de las TIC favorecen las destrezas tecnológicas en los menores de edad; sin embargo, las experiencias negativas también se incrementan como consecuencia del uso inadecuado de las mismas (Rodríguez-Álvarez et al., 2018).

El internet, además de ofrecer múltiples beneficios también ha promovido el desarrollo de la delincuencia digital (Montenegro et al., 2019). La red encierra riesgos y el uso sin conocimiento ni criterio puede tener como consecuencia situaciones conflictivas y muy peligrosas (C. R. Rodríguez, 2020). Los menores de edad, por su ingenuidad y falta de criterio, carecen de recursos para responder en situaciones que pueden poner en riesgo su imagen, su identidad e incluso su salud. Esto los convierte en usuarios débiles ante los peligros de internet (Cascardo & Veiga, 2018).

Desde una perspectiva psicológica, la victimización infantil incluye cualquier conducta intencional que cause daño a un menor o lo ponga en una situación de alto riesgo, afectando su bienestar psíquico, físico y/o social que interfiere en su óptimo desarrollo (Juan et al., 2014). Existen varias formas de victimización, que en la práctica no son excluyentes, dando lugar a la polivictimización. La Figura 1 muestra diversas formas de victimización sexual online que pueden sufrir los menores de edad; tales como, explotación sexual, solicitudes sexuales online y exposición a contenido sexual de distintas maneras (Villacampa, 2016). Estos tipos de abusos pueden interrelacionarse, dificultando su identificación, diferenciación o aislamiento para su estudio; ya que, muchas veces la misma víctima de una forma de victimización también suele serlo de otra (polivictimización).

Figura 1. Victimización sexual infantil online

Para algunas víctimas el acoso en entornos virtuales es un reflejo del continuo maltrato presencial trasladado a la virtualidad (Hinduja & Patchin 2008; Slojen, Smith & Frisén, 2013). De hecho, es habitual que los adolescentes acosados en el ámbito presencial, también lo sean a través de Internet (Katzer, Ferchenhauer & Belschak, 2009).

Aproximadamente la mitad de las víctimas y de agresores en entornos virtuales también lo son en la vida real (Espelage et al., 2018). Las investigaciones relacionan la cibervictimización a factores como estrés, depresión, conductas suicidas, miedo, baja autoestima, nerviosismo y frustración (Chocarro & Garaigordobil, 2019), además de dificultades académicas y problemas en el entorno escolar.

La victimización verbal es interpretada como un comportamiento intencional, agresivo y en algunos casos repetitivos. A estos factores se suma también la indefensión de la víctima, y se integra el desequilibrio de autoridad y poder entre víctima y agresor; por lo que, el silencio de la víctima refuerza una relación sistemática (Di Napoli, 2018). Por tanto, existe una correspondencia desigual y negativa basada en la soberbia del agresor y la sumisión de la víctima, provocando efectos muy graves, que a menudo resultan en daños físicos (golpizas, robos, etc.), psicológicos (insultos, apodos, amenazas, chismes, aislamiento social, etc.) e incluso muerte (suicidio).

Es necesario profundizar en los factores de riesgo y los factores protectores para los roles de agresor/víctima. Por ello resulta importante tratar de identificar con mayor precisión las características de las formas más comunes de victimización en entornos virtuales como *grooming*, *sexting* y *ciberbullying* para delinear su detección, prevención e intervención.

Víctimas menores de edad en espacios virtuales

Menores de edad de diferentes clases sociales, culturas, religiones y regiones acceden a plataformas de interacción social en los espacios virtuales desde diferentes entornos físicos. El ciberespacio además de sus ventajas también presenta el uso abusivo de la tecnología, facilitando a las personas la oportunidad de contactar a menores de edad que en otras circunstancias no hubiera sido posible.

La violencia silenciada que experimentan las víctimas tiene consecuencias psicológicas graves, que están condicionadas a un proceso dinámico, individual y subjetivo de la víctima de acuerdo con factores personales, sociales y ambientales-criminales. Es decir, cada víctima experimenta y vive su propia realidad de manera particular. Sin embargo, la literatura científica establece ciertos patrones de comportamiento comunes de "las víctimas de violencia ciber-sexual".

La mayoría de los cuales terminaban en delitos sexuales o producción de pornografía infantil (Boldú, 2014). Las víctimas oscilan entre 12 y 17 años, que en su mayoría tienen confusión respecto a su identidad sexual, y en otros casos las víctimas creen estar enamorados o tener un vínculo sentimental muy estrecho con su abusador. La mayoría de las víctimas suelen ser chicas; siendo el abuso más común el "*sexting*" donde las victimas autogeneran imágenes sexuales, convirtiéndose inconscientemente en su propio "verdugo", ya que, estas imágenes las envía a otras personas mediante un dispositivo electrónico a través de internet. Este actuar, representa lo que los expertos llaman "extimidad", esto significa hacer pública la intimidad de cada persona, una mezcla entre narcisismo y exhibicionismo, derivado muchas veces del éxito de los contenidos que se promueven en reality shows tipo Gran Hermano y la Web 4.0 (redes sociales, blogs, etc.), y que hoy forma parte de la identidad y el autoconcepto de los adolescentes (Pineda et al., 2019).

La mayoría de las víctimas de los ciberacosos están conscientes de que se relacionan con un adulto que quiere mantener relaciones sexuales con ellos y muchos de ellos acceden a hacerlo, bien a través de Internet (cibersexo) o en encuentros presenciales. En la Tabla 1, se muestran las víctimas más propensas a involucrarse en relaciones sentimentales con personas que conocen en Internet, y con mayor riesgo de solicitudes cibersexuales (Wolak et al., 2010).

Tabla 1. Características de las víctimas de delitos sexuales iniciados en Internet

Características de las víctimas de delitos sexuales iniciados en Internet que se implican voluntariamente en relaciones online con adultos
• Adolescentes con relaciones conflictivas con sus padres con poca supervisión parental, y con problemas de conducta antisocial.
• Adolescentes mujeres que empiezan a ser sexualmente activas a temprana edad con personas mayores que ellas.
• Adolescentes con problemas de depresión y soledad. Jóvenes tímidos y solitarios que carecen de habilidades sociales, y tienen problemas para establecer relaciones de amistad fuera de Internet.
• Jóvenes con historia de abuso físico o sexual, excesivamente preocupados, que buscan afecto y atención en la Red.
• Jóvenes homosexuales o aquellos que se cuestionan su identidad sexual y buscan respuestas en Internet.
• Jóvenes sumisos y complacientes o "*Statutory victims*", que cooperan activamente con sus abusadores en la creación de fuertes vínculos emocionales y sexuales.

(Wolak et al., 2010)

La edad de mayor riesgo de ser víctima cibersexual, de acuerdo con la literatura científica son los jóvenes entre 13 y 15 años, especialmente cuando el ciberagresor es conocido por la víctima (Mitchell et al., 2007). Este riesgo, se incrementa con la edad de la víctima, pues utilizan con más frecuencia el Internet y asumen más riesgos que los internautas más pequeños; además su curiosidad e interés por la sexualidad predominan en esa etapa de vida en la que se está formando su identidad sexual (Cabrales, 2019).

En estudios basados en las experiencias de ciberagresores, se concluye que existen dos tipos de cibervíctimas, las "arriesgadas" y las "vulnerables" (Whittle et al., 2013).

Cibervíctimas arriesgadas: presentan una actitud desinhibida y arriesgada cuando interactúan en los entornos virtuales. Demuestran una sensación de control propio de adolescentes extrovertidos y seguros de sí mismos, y guardan el secreto del abuso por su aparente "complicidad" en la dinámica.

Cibervíctimas vulnerables: se caracterizan por necesitar una elevada atención y afecto producto de sus sentimientos de soledad y su baja autoestima. Provienen de hogares disfuncionales y conflictivos con dificultades para relacionarse con sus padres. Buscan el amor en Internet y cuando creen haberlo encontrado conservan la situación de abuso por miedo a perderlo.

Ciberagresores

Los ciberagresores, en general, son personas aparentemente normales, generalmente hombres aunque, también cada vez hay más mujeres, de casi cualquier edad, religión, cultura y ubicación geográfica, con acceso a Internet y que saben cómo interactuar de forma anónima en los entornos virtuales.

Los estudios de Crimes Against Center Research Center (CCRC), exponen que la mayor parte de los ciberagresores son hombres cuya edad promedio es menor a 25 años, y que no mienten sobre sus intereses sexuales ni sobre su edad al conocer a su víctima. En estos estudios, también se observó que la mayoría de los ciberagresores eligen con mayor frecuencia a víctimas que ya conocen en persona, incluso miembros de su propia familia (Wolak, Finkelhor y Mitchell, 2010). Una de las características de los ciberagresores es la tenencia de pornografía infantil, así como cierto comportamiento exhibicionista, ya que envían fotos eróticas o sexualmente explícitas de sí mismos a sus víctimas con la intención de reducir sus inhibiciones (Alonso & Triñanes, 2016).

Hay que señalar que, no es posible establecer el perfil exacto de un ciberagresor sexual infantil (Juan et al., 2014), debido a que, no son un grupo homogéneo en características demográficas o de comportamientos. Sin embargo, se han identificado algunos patrones de comportamiento de tipo "*online groomers*" cuyas estrategias de contacto y acercamiento se marcan de acuerdo con sus necesidades y motivaciones. Existen ciberagresores que buscan relaciones románticas e íntimas a largo plazo con menores ("*intimacy-seeking*" o "*distorted attachment offender*"), otros que necesitan satisfacer impulsos sexuales de manera inmediata ("*hyper-sexualised offender*"), y otro grupo que se adapta a las características del menor y a como éste reaccionara durante la dinámica ("*adaptable offender*") (Machimbarrena & Garaigordobil, 2018).

En este contexto, también se suman las discretas redes sociales que se pueden crear en el internet profundo donde personas interesadas en sexo con menores pueden acceder de manera anónima. Estos espacios virtuales promueven el acceso a contenido pornográfico infantil como legítimo mediante el intercambio de monedas; además de otorgar a sus miembros un estatus dentro de su grupo social; incluso competir entre ellos por obtener nuevas y mejores imágenes pornográficas infantiles (Posada, 2021; Norberto, 2019).

Por último, hay que considerar que si el ciberagresor no logra conseguir su objetivo con la víctima, simplemente puede desaparecer por un tiempo y volver a intentarlo con una nueva identidad, o simplemente, atacar al mismo tiempo a varias víctimas potenciales; ya que, una de las mayores ventajas que presenta el ciberespacio es el anonimato, situación que en el mundo real es difícil de conseguir.

Tipos de acosos en entornos virtuales

Grooming

El vocablo groom se usa para indicar voluntad para algo. El termino pederasta, se usa para referirse a cualquier persona que quiera dañar psicológicamente a un niño, es decir usarlo y controlarlo emocionalmente mediante un acoso progresivo, para luego someterlo a cualquier tipo de abuso sexual (Carrizo, 2017). Entonces, grooming se refiere a la situación donde un adulto acosa sexualmente a un menor de edad mediante el uso de internet en plataformas de interacción social.

Los ciberagresores de este delito suelen utilizar un perfil falso en una plataforma de interacción social como, sala de chat, foro, videojuego u otro, en donde se hacen pasar por un chico o una chica e inician una relación de amistad y confianza con el niño o niña que quieren acosar.

El grooming tiene varias fases o etapas, inicia con un pedido de foto o video de índole sexual o erótica (pedido por el adulto, utilizando el perfil falso) a su víctima. Luego de obtener ese material, el ciberagresor puede o bien desaparecer o iniciar un chantaje a la víctima amenazando en hacer pública esa información si no entrega nuevos videos o fotos, o si no accede a un encuentro personal.

Sexting

La expresión anglosajona sexting, indica el envío de mensajes con contenido de tipo pornográfico y/o erótico a través de los teléfonos móviles. Es decir, la transmisión de mensajes sumamente explícitos que incluyen un contenido lascivo o libertino a través de un teléfono móvil. Sin embargo, desde hace cierto tiempo también incluye el envío y recepción de videos e imágenes fotográficas, a las que también se les denomina como "*selfies*", donde las personas generalmente intercambian mensajes y contenido de tipo erótico con otra persona mediante un teléfono inteligente, pudiendo mostrar las partes íntimas a través de una fotografía o un video realizando alguna actividad de tipo sexual (Narváez, 2022).

Ciberbullying

El ciberbullying es el término usado para describir cuando un menor de edad es fastidiado, amenazado, acosado, humillado, avergonzado o abusado por otro menor, a través de Internet o cualquier medio de interacción virtual como teléfonos móviles o tablets. Esta ciberamenaza se caracteriza porque se da entre dos iguales, es decir, entre menores de edad (Macaulay et al., 2022). Es importante distinguirlo ya que existen otras prácticas donde intervienen adultos con lo cual, se estaría ante otro ilícito de ciberacoso. A continuación, se describen las características del ciberbullying:

- Anonimato: el ciberagresor puede esconderse detrás de un apodo o un seudónimo.
- Eliminación de la ética: el ciberagresor dice o hace acciones que no se pueden hacer en la vida real.
- No hay lugar seguro: las víctimas no se sienten seguras en ningún lugar, las agresiones pueden ocurrir en cualquier momento y en cualquier lugar.
- Agresiones repetidas: las agresiones se repiten una y otra vez, publicando la información en la Web, por lo que, el daño es exponencial por el número de espectadores.
- Violación de la privacidad: el acosador puede publicar información de la víctima en la red sin que esta lo conozca.
- Escasa visibilidad parental: los padres no conocen del daño que su hijo está recibiendo debido a una falta de comunicación entre ellos.

Metodología

Ubicación del estudio

Dado que se trata de describir las características y las consecuencias de las diferentes formas de victimización en entornos virtuales, tales como *grooming*, *sexting* y *ciberbullying*, se recurrió a una investigación documental-explicativa. Este trabajo se realiza bajo el planteamiento del enfoque cualitativo, el cual se ajusta a las características y necesidades de la presente investigación, permitiendo recopilar información cualitativa y fiable para realizar el análisis de la información obtenida.

Evaluación del nivel de uso de internet y sus amenazas

Para plantear los componentes de la propuesta se elaboró un pre-test dirigido a estudiantes. El objetivo de este test fue identificar el nivel de conocimiento y uso del internet; así como sus amenazas.

En la investigación participaron 4 Unidades Educativas de la provincia de Santa Elena, Ecuador. La cantidad de estudiantes fueron 922 de los cuales 434 son hombres y 488 son mujeres; en edades entre 9 y 17 años, siendo el rango entre 15 y 17 años el porcentaje más alto (63%).

Los datos obtenidos en el cuestionario realizado ponen de manifiesto que el uso de las TIC es una actividad habitual para la totalidad de los estudiantes. La gran mayoría (72%) reconoce tener un nivel de dominio suficiente en el uso y aplicación de las TIC (Figura 2). Respecto a la cantidad de horas diarias que se conectan a internet, se obtuvo que el 55.1% pasa conectado en internet más de 8 horas diarias, seguido del 28.6% que se conecta más de 12 horas diarias, y el 29.1% menos de 4 horas diarias. También expresaron que mayormente usan el internet para buscar información, acceder a las redes sociales y realizar actividades de educación virtual.

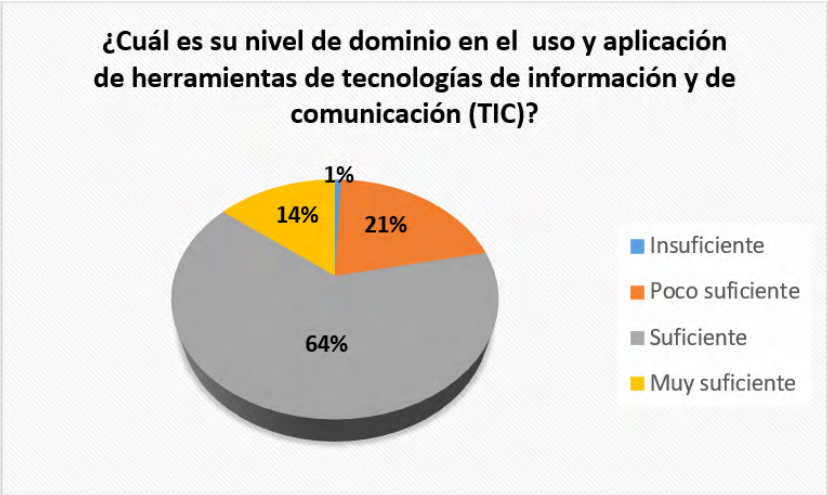

Figura 2. Nivel de dominio en el uso de las TIC
Elaborado por: los autores

Las herramientas más utilizadas son el teléfono móvil personal y el ordenador personal con acceso a internet. Es decir, predomina el uso de dispositivos personales en relación con los dispositivos compartidos por el resto de los integrantes de la misma familia.

En cuanto al uso de las redes sociales, el 64.5% indicó que utilizan las redes sociales, de ese grupo, la gran mayoría tiene al menos dos cuentas activas en Facebook, Instagram y/o Twitter; además, el 18.5% utiliza un perfil público y desconoce el nivel de privacidad de su perfil. Respecto a la frecuencia con la que utilizan las redes sociales para conocer nuevas personas y hacer amigos, el 33.2% indicó que casi siempre lo utiliza, seguido del 53% que lo hace ocasionalmente (Figura 3).

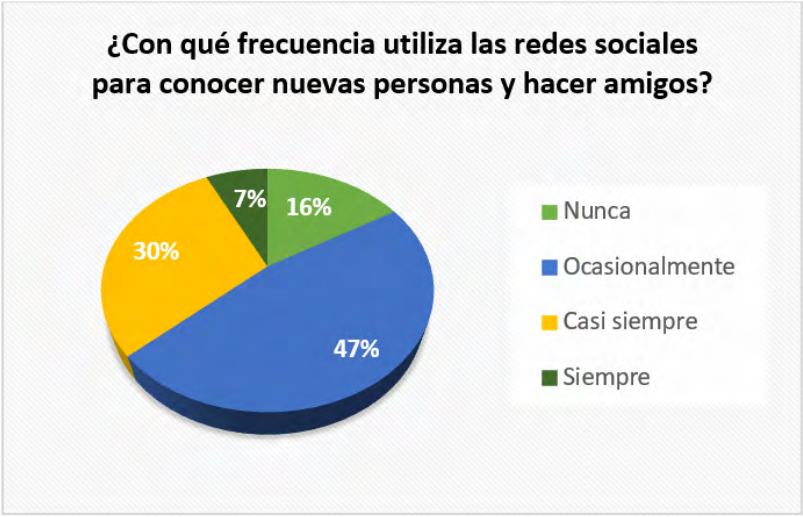

Figura 3. Frecuencia de uso de redes sociales para conocer nuevas personas
Elaborado por: los autores

En cuanto al conocimiento de riesgos y amenazas en internet los estudiantes dijeron conocer el ciberbullying, propagación de *malware, sexting* y *phishing*. Respecto al manejo de la privacidad de sus datos la mayoría indicó que ocasionalmente facilitan información personal.

En cuanto a las experiencias negativas durante el uso de Internet, el 58% de los estudiantes reconoce haber vivido, en algún momento, alguna situación desfavorable (Figura 4).

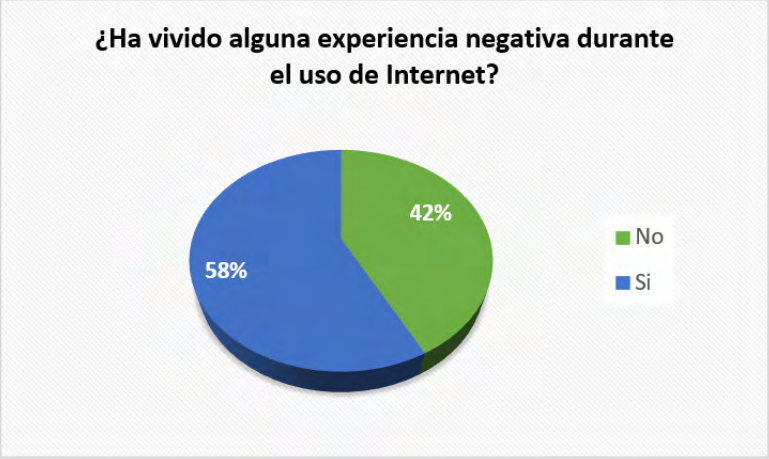

Figura 4. Estudiantes que han vivido experiencias negativas durante el uso de Internet
Elaborado por: los autores

Del 58% que indicó haber vivido una experiencia negativa, destacan con mayor frecuencia los insultos y comentarios inapropiados, seguidos de los chantajes con fotografías (Figura 5).

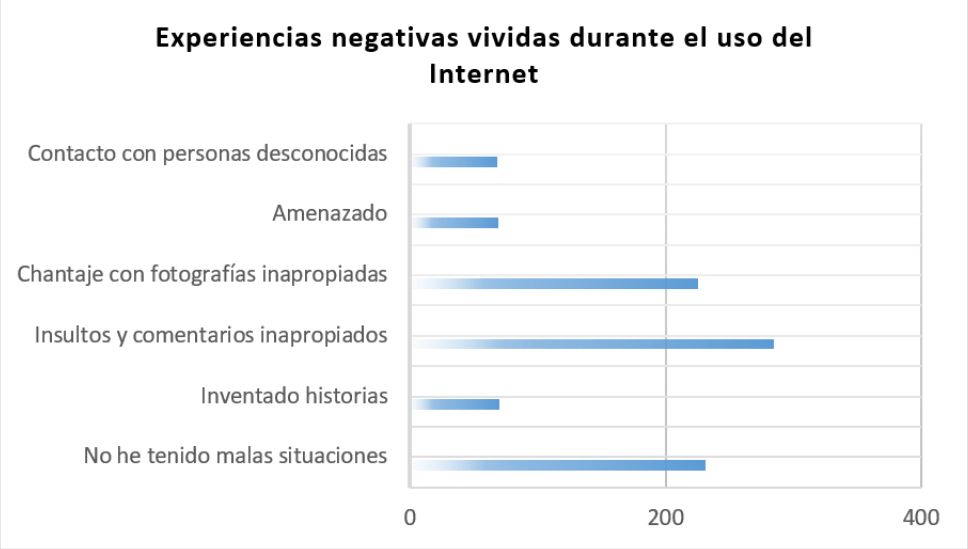

Figura 5. Tipos de experiencias negativas durante el uso de internet
Elaborado por: los autores

Resultados

Formación y reflexión sobre los riesgos de internet

De acuerdo con el panorama antes descrito, son diversos los riesgos a los que se exponen los niños y jóvenes en la red, situación que se ha evidenciado con mayor fuerza en los últimos años. Sin embargo, esta población confía en su conocimiento y experiencia en el uso de las TIC que creen estar aptos para sobrellevar cualquier situación en la web (Ramos-Soler et al., 2018; Soriano-Ayala et al., 2018).

Es necesario crear consciencia en la juventud respecto a los riesgos en internet (Gamito et al., 2017). Por ejemplo, gran parte de los adolescentes no considera peligrosa la acción de mantener una conversación con desconocidos o publicar información privada (Cucalón Estrada & Oliván Blázquez, 2015; McCarty Cheryl y Prawitz, 2011).

El uso de dispositivos móviles con acceso a internet cada vez está en aumento, se afirma que más del 50 % de los niños y jóvenes acceden a internet por este medio (Quimbayo et al., 2018; Ruiz et al., 2019). Esta situación complica el control y vigilancia de sus acciones; ya que, limita las posibilidades de mediación y seguimiento por parte de los adultos (Vázquez Gavilanes, 2021); además, los niños y los jóvenes consideran que pueden publicar cualquier foto en la red, sin que esto represente ningún riesgo (Álvarez-de-Sotomayor & Carril, 2021).

El acceso a la comunicación y a la información a través de los medios virtuales es cada vez más generalizado. Las diversas formas que dispone esta población para acceder a internet han aumentado considerablemente como consecuencia de la normalización de las tecnologías móviles. Esto se debe a la rápida e imparable expansión de las TIC; por lo que, a los adultos cada vez les resulta más difícil controlar las conexiones realizadas por los menores de edad (Carrasco Rivas et al., 2017), para quienes cada vez resulta más fácil utilizar internet de manera privada (de la Hoz, 2018a; Díaz-Vicario et al., 2019).

En este contexto, diversas investigaciones coinciden que la mejor herramienta de seguridad y prevención se basa en la comunicación y el diálogo, con relación a implantar medidas de restricción tales como limitar el uso de dispositivos móviles e internet, o controlar su uso mediante software de control parental (Giménez Gualdo et al., 2017; Unicef & others, 2014; Vázquez Gavilanes, 2021). Desde luego, el uso de las TIC para los menores de edad es necesario para su desarrollo socio-tecnológico(M. D. Rodríguez et al., 2018). Sin embargo; su uso debe estar fundamentado en el conocimiento adecuado de los riesgos, implementar mecanismos y herramientas de seguridad informática, así como mantener una actitud responsable, crítica y reflexiva sobre el uso seguro de la tecnología (de la Hoz, 2018b).

El desarrollo de habilidades digitales permite el uso adecuado, seguro y crítico de las TIC en diversos ámbitos. Estas capacidades se definen como un conjunto de actitudes, estrategias y habilidades que se exigen para el uso de las TIC (Berrocoso, 2012; Collantes-Inga, 2019). Para las instituciones educativas es esencial, ya que, el adquirir y repetir los conocimientos no significa que un estudiante pueda construirlos; es decir, una persona competente digitalmente debería ser capaz de resolver problemas cotidianos de forma eficiente (Rodríguez-Álvarez et al., 2018).

Al respecto, el Parlamento Europeo (2006/962/CE) menciona que la competencia digital es una habilidad clave para el aprendizaje permanente, definiendo que el manejo seguro y adecuado de las TIC es necesario en el trabajo, el ocio y la comunicación como competencias básicas. Además; se incluye la necesidad de gestionar la identidad digital, el uso seguro de internet y la protección de los datos personales en estas competencias (Ferrari & DIGCOMP, 2013).

Por lo expuesto, es recomendable reservar espacios para trabajar la gestión de la privacidad, los riesgos de internet, el uso de herramienta de seguridad informática y, la importancia de ser consciente de la identidad digital y, con ello obtener un adecuado desarrollo de la autonomía digital segura (Arango Niño & others, 2021; Dans, 2015; González Porras, 2016; Rial et al., 2014).

Mecanismos de prevención para mitigar ciberacosos

A continuación, algunas sugerencias para prevenir los ciberacosos revisados en este trabajo.

Prevención de ciberbullying

Es importante utilizar la configuración de privacidad disponible en las plataformas de interacción social como Facebook, twitter, Instagram, etc.; además de verificar el uso de datos mínimos necesarios al momento de crear un perfil en una red social, y que esta permita utilizar herramientas como *privacy shield*.

Otro aspecto importante, es tener cuidado con las personas que se agregan a la red social personal para evitar el acceso y contacto de personas desconocidas; además ante una situación intimidante es importante informar a un adulto, y proceder a bloquear o denunciar al ciberagresor en la misma red social mediante las opciones de seguridad (Oliva-Sequeda & Triana-Pereira, 2022).

Como parte del cuidado de la imagen digital, antes de subir a internet una fotografía o video grupal es necesario solicitar autorización de las personas que se encuentran en la misma; ya que muchas veces estas pueden contener imágenes que podrían avergonzar a sus compañeros, y no ser de su agrado.

En una situación de intimidación es importante guardar las pruebas del ciberacoso, tales como mensajes, conversaciones y archivos compartidos, ya que pueden servir como medios de prueba en la investigación.

Prevención de Grooming

Es importante que un menor diferencie un acto sano y un acto irrespetuoso que lleve a algún tipo de abuso sexual. A continuación, algunos mecanismos de prevención de grooming (Sinchiguano, 2020).

- Nunca publicar información personal en internet, ya sea en redes sociales, foros o juegos online. Si es posible, utilizar nicks o sobrenombres en lugar de tu nombre real.
- Usar contraseñas seguras, que combinen letras, números, caracteres especiales y con una longitud mínima entre 8 y 12 caracteres.
- Desconfiar de todas las personas desconocidos que le hablen por Internet, y ante cualquier sospecha, bloquearlos.
- Nunca acceder a cualquier tipo de peticiones que le hagan por Internet, y menos tener un contacto en persona con alguien que no se conoce. En caso de que sea totalmente necesario, acudir con una persona adulta que pueda supervisar y controlar que no suceda nada.
- Nunca enviar información personal o cualquier tipo de contenido a personas desconocidas a través de Internet.
- Asegurar la privacidad de sus redes sociales. Restrinja el acceso de sus publicaciones.
- No proporcionar públicamente sus localizaciones a través de internet.

Prevención de Sexting

Como ya se ha mencionado, es necesario enseñar la importancia de la privacidad a los menores, los consejos más relevantes para evitarlo son:

- Bloquear el teléfono móvil con seguridad para impedir que cualquiera acceda a su dispositivo.
- Nunca enviar imágenes comprometedoras a personas que no conoce o que no tiene confianza.

- Si decide enviar material con contenido erótico y/o sexual, asegúrese que el receptor lo borre de su dispositivo una vez visualizado; además cerciórese que lo envíe al contacto que desea y no cometer el error de enviárselo a otra persona.
- Si recibe imágenes comprometedoras de alguien que conoce, notifique al afectado por si este no supiera que su fotografía está difundiéndose públicamente.
- Si recibe material en el que aparecen menores, bórrelo inmediatamente e informe a las autoridades. Es posible que el emisor original del contenido esté detrás de un delito de pornografía infantil.
- Instale un antivirus que avise de cualquier malware que pueda dañar su sistema informático.

Propuesta de formación académica en seguridad informática

La propuesta de este trabajo tiene como objetivo principal desarrollar un programa de formación académica en seguridad informática dirigida a menores de edad. Los resultados que se esperan con la implementación del programa es mejorar la convivencia en los entornos virtuales. Los contenidos educativos deben promover el uso de herramientas de seguridad informática básica.

El proyecto consiste en desarrollar un sitio web que integre los contenidos de una guía multimedia relacionada con el uso responsable y seguro de las TIC. El objetivo de la propuesta didáctica denominada "Tecnología Segura" es promover e integrar una cultura informática responsable mediante la sensibilización de los estudiantes respecto al uso de las TIC; y, con ello desarrollar y fortalecer una actitud crítica, reflexiva y responsable ante el uso de las mismas.

La estructura didáctica de la guía multimedia "Tecnología Segura" incluye el desarrollo de cinco unidades temáticas: (1) Internet y las plataformas digitales, (2) Riesgos del internet para menores de edad, (3) Delincuentes y pederastas en las redes sociales, (4) Respondiendo a amenazas no deseadas en internet, y (5) Técnicas y herramientas para proteger la privacidad. Estos contenidos serán integrados y publicados en el sitio web del proyecto, la Figura 6, muestra el diseño de la página de inicio.

Figura 6. Diseño de la página de inicio de sitio web
Elaborado por: los autores

Proceso de diseño técnico de la propuesta

El diseño técnico de la guía multimedia se realiza en cuatro fases: planificación, preproducción, producción y postproducción. En la fase de planificación se analiza el material a publicar en la guía y las herramientas a utilizar, de acuerdo con las siguientes actividades:

- Selección de los contenidos.
- Selección de las herramientas para edición y producción del video, y del ambiente gráfico del sitio web.
- Edición de las unidades temáticas en el sitio web.
- Pruebas de integración de videos y ambiente gráfico en el sitio web.

En la fase de preproducción se seleccionan los diseños de la maquetación del sitio web, y también se eligen las herramientas de conversión a formatos de video:

- Powerpoint, para la presentación textual.
- Camptasia Studio para conversión a formatos de video.
- Lenguaje HTML, CSS y Javascript para el ambiente gráfico de interacción con el usuario.

La fase de producción se realiza de acuerdo con el formato seleccionado para el ambiente textual de la guía multimedia. La duración de todo el contenido del sitio web tiene un tiempo aproximado de 3 meses previo al inicio de la capacitación.

Por último, en la fase de postproducción se realizan los siguientes pasos:

- Revisión y edición de los contenidos del sitio web.
- Mejoramiento de resolución de videos e imágenes.
- Integración de videos y ambiente gráfico.

Finalmente, este proyecto servirá para desarrollar y mejorar las competencias digitales en los estudiantes; además de fomentar una cultura sociotecnológica responsable y segura respecto al uso de las TIC.

Los resultados que se esperan alcanzar luego de su implementación son:

- Adquirir una formación sobre las plataformas digitales y la seguridad informática.
- Desarrollar en los alumnos habilidades que permitan identificar situaciones de riesgo en internet.
- Reforzar valores actitudinales en grupo, convivencia y respeto en el uso de medio digitales.
- Conocer los riesgos a los cuales se exponen en internet y cómo actuar para su minimización.
- Fomentar el uso responsable de las tecnologías de información y comunicación.
- Valorar el uso y divulgación de la información en la web.

Conclusiones

El internet y las redes sociales fomentan el desarrollo tecnológico de las personas. Las plataformas digitales promueven nuevos espacios virtuales donde la interacción entre las personas sobrepasa el tiempo, la distancia, el idioma y cualquier otra variable que pudiera limitar la comunicación. En este sentido, las conductas delictivas también se trasladan a estos medios adquiriendo nuevas dimensiones y características con consecuencias específicas, entre ellas la victimización sexual infantil y el acoso.

Por lo cual, es necesario evaluar este fenómeno para poder entender su accionar y proponer una adecuada intervención, desde diferentes aspectos como psicológico (prevención, detección, intervención y tratamiento, tanto de víctimas como de agresores), académico (formar respecto al uso

seguro de internet y concientizar en relación a sus riesgos), legal (adaptación de los tipos delictivos a la realidad social, mayor protección de las víctimas), psicojurídico (valoración pericial de víctimas y victimarios) o de política criminal (anticipación de la barrera de protección penal en casos de menores, edad de consentimiento sexual, etc.).

La mayor incidencia de abusos en línea es el ciberacoso sexual y el ciberbullying. La victimización sexual infantil comprende acciones ofensivas contra la sexualidad de un menor afectando su desarrollo psicosocial. En este contexto, las TIC ofrecen nuevas herramientas y entornos virtuales como una vía de captación de víctimas y difusión de imágenes abusivas en contextos agresivos y pornográficos en los últimos años.

Este fenómeno nos ubica en un escenario incierto donde cada vez se generan más abusos online. Las consecuencias psicológicas para los menores pueden ser devastadoras, y aunque estas víctimas no pudieran manifestar secuelas psíquicas clínicamente relevantes, es necesario evitar estas situaciones, especialmente la difusión de pornografía infantil.

La temática descrita en este trabajo evidencia la necesidad de promover e integrar una cultura informática responsable en la comunidad académica. En la práctica diaria del uso de las TIC por parte de los menores se observan deficiencias respecto al uso seguro de la tecnología y el poco conocimiento sobre los riesgos de internet y como evitarlos. Esta situación está en aumento debido al amplio intervalo de tiempo que dedican a conectarse a Internet y el acceso a diferentes redes sociales para publicar y consumir información. Así como, la cantidad de datos personales que comparten en la red sin ser conscientes de los graves peligros a los que se exponen. Además; a esto se suma, el uso inadecuado de las herramientas de seguridad informática, muchos desconocen las posibilidades de gestionar la privacidad de los datos en las aplicaciones que utilizan. También el desconocimiento del concepto de identidad digital, y su importancia.

Evidentemente, la responsabilidad de evitar estos abusos contra la libertad e integridad sexual de los menores recae sobre los gobiernos, las academias, las empresas privadas y públicas, el núcleo familiar, y en general la sociedad civil. El desafío será incorporar nuevas medidas y estrategias dirigidas a la prevención de la victimización online y, aunque no pudiera parecer que no son totalmente efectivas, se ha contribuido a generar conciencia, interés y sensibilización en estas nuevas formas delictivas.

Referencias Bibliográficas

- Arango Niño, J. A., & others. (2021). Análisis de los riesgos de seguridad a los cuales están expuestos los niños y niñas con el uso de la red social facebook y cómo estos podrían reducirse.
- Alonso, C., & Triñanes, E. R. (2016). Ciberacoso: Características de personalidad y psicopatológicas del ciberagresor y de la cibervíctima. Anuario Psicoloxía e Saúde: Revista Oficial da Sección de Psicoloxía e Saúde do COPG, (9), 164-175.
- Álvarez-de-Sotomayor, I. D., & Carril, P. C. M. (2021). Internet y redes sociales: un desafío a la convivencia familiar. Educatio Siglo XXI, 39(2), 123–142.
- Balakrishnan, V., Khan, S., Fernandez, T., & Arabnia, H. R. (2019). Cyberbullying detection on twitter using Big Five and Dark Triad features. Personality and individual differences, 141, 252-257.
- Berrocoso, J. V. (2012). Estrategias educativas para el desarrollo de la competencia digital. Las Tecnologías de La Información En Contextos Educativos: Nuevos Escenarios de Aprendizaje, 55–68.

- Boldú Pedro, A. (2014). El ciberacoso: una aproximación criminológica.
- Bossler, A. M., Holt, T. J., & May, D. C. (2012). Predicting online harassment victimization among a juvenile population. Youth & Society, 44(4), 500-523.
- Cabrales Pinto, G. (2019). El cibersexo, fenómeno contemporáneo de la cibercultura en jóvenes universitarios (Doctoral dissertation, Universidad de la Costa).
- Carrasco Rivas, F., Droguett Vocar, R., Huaiquil Cantergiani, D., Navarrete Turrieta, A., Quiroz Silva, M. J., & Binimelis Espinoza, H. (2017). El uso de dispositivos móviles por niños: Entre el consumo y el cuidado familiar. Cultura-Hombre-Sociedad, 27(1), 108–137.
- Carrizo, S. A. (2017). Delitos informáticos que atentan contra la indemnidad sexual de los menores de edad–grooming (Bachelor's thesis).
- Cascardo, E., & Veiga, M. C. (2018). Tecnoadictos: Los peligros de la vida online. EDICIONES B.
- Chocarro, E. y Garaigordobil, M. (2019). Bullying y cyberbullying: diferencias de sexo en víctimas, agresores y observador. Pensamiento Psicológico, 17 (2), 57-71.
- Collantes-Inga, Z. (2019). Competencias digitales y educación. Propósitos y Representaciones, 7(2), 569–588.
- Cucalón Estrada, L., & Oliván Blázquez, B. (2015). Análisis sobre la utilización de redes sociales en jóvenes y adolescentes de Aragón.
- Dans, I. (2015). Identidad digital de los adolescentes: la narrativa del yo. Revista de Estudios e Investigación En Psicología y Educación, 1–4.
- De la Hoz, J. P. (2018a). Ventajas y desventajas del uso adolescente de las TIC: visión de los estudiantes. Revista Complutense de Educación, 29(2), 491.
- De la Hoz, J. P. (2018b). Riesgos percibidos por estudiantes adolescentes en el uso de las nuevas tecnologías y cómo reaccionan ante ellos. Bordón. Revista de Pedagogía, 70(2), 105–120.
- Díaz-Vicario, A., Mercader Juan, C., & Gairín Sallán, J. (2019). Uso problemático de las TIC en adolescentes. Revista Electrónica de Investigación Educativa, 21.
- Di Napoli, P. (2018). Reflexiones críticas sobre la noción de bullying desde un caso de estudio. Un análisis de las luchas simbólicas por el poder de nominación en el ámbito escolar. Espacios en blanco. Serie indagaciones, 28(2), 33-48.
- Espelage, DL, Hong, JS y Valido, A. (2018). El ciberacoso en los Estados Unidos. En Perspectivas internacionales sobre el ciberacoso (págs. 65-99). Palgrave Macmillan, Cham.
- Ferrari, A., & DIGCOMP, B. B. (2013). A framework for developing and understanding digital competence in Europe. IPTS Reports. Luxembourg: European Commission. https://doi.org/http://dx. doi. org/10.2788/52966.
- Gamito, R., Aristizabal, P., & Olasolo, M. (2017). La necesidad de trabajar los riesgos de internet en el aula. Profesorado. Revista de Curr{\'\i}culum y Formación de Profesorado, 21(3), 409–426.
- Giménez Gualdo, A. M., Luengo Latorre, J. A., Bartrina, M. J., & others. (2017). ?` Qué hacen los menores en Internet? Usos de las TIC, estrategias de supervisión parental y exposición a riesgos. Electronic Journal of Research in Educational Psychology, 15(3).
- González Porras, A. J. (2016). Privacidad en internet: los derechos fundamentales de privacidad e intimidad en internet y su regulación jurídica. La vigilancia masiva.
- Hinduja, S. y Patchin, JW (2019). Conexión del suicidio adolescente con la gravedad del acoso y el ciberacoso. Revista de violencia escolar, 18 (3), 333-346.
- Juan, I. M., Vayá, E. J. C., & García, M. S. (2014). Victimización infantil sexual online: online grooming, ciberabuso y ciberacoso sexual. Delitos sexuales contra menores: abordaje psicológico, jurídico y policial, 203-224.

- Katzer, C., Fetchenauer,D.,& Belschack,F. (2009). Cyberbullying: Who are the victims? A comparison of victimizacion in Internet chatrooms and victimizacion in school. Journal of media Psychology, 21(1), 25-36.
- Macaulay, P. J., Betts, L. R., Stiller, J., & Kellezi, B. (2022). An introduction to cyberbullying. In Cybersecurity and Cognitive Science (pp. 197-213). Academic Press.
- Machimbarrena, J. M., & Garaigordobil, M. (2018). Bullying y cyberbullying: diferencias en función del sexo en estudiantes de quinto y sexto curso de educación primaria. Suma Psicológica, 25(2), 102-112.
- Mitchell, K. J., Ybarra, M., & Finkelhor, D. (2007). The relative importance of online victimization in understanding depression, delinquency, and substance use. Child maltreatment, 12(4), 314-324.
- McCarty Cheryl y Prawitz, A. D. y D. L. E. y M. B. (2011). Seguridad percibida y riesgos que corren los adolescentes en los sitios de chat en línea. In 3.er piso New Rochelle N Y 10801 E E U U Mary Ann Liebert Inc. 140 Huguenot Street (Ed.), Cyberpsychology, Behavior, and Social Networking.
- Montenegro, M. A. S., Miranda, Á. S. B., & de Vinces, P. J. G. (2019). El hacking como comportamiento típico en las nuevas formas de delincuencia organizada. Espirales Revista Multidisciplinaria de Investigación, 3(26), 60–70.
- Morelli, M., Bianchi, D., Baiocco, R., Pezzuti, L., & Chirumbolo, A. (2016). Sexting, psychological distress and dating violence among adolescents and young adults. Psicothema.
- Norberto, H. J. (2019). Cybersex and crime. Comments on the sentence by the Supreme Court of Justice (SP4573-2019). Nuevo Foro Penal, 15(93), 255-262.
- Narváez Peralta, J. S. (2022). El sexting como conducta sexual de riesgo en adolescentes.
- Oliva-Sequeda, E. A., & Triana-Pereira, C. J. (2022). Esquema para la prevención del grooming en niños, niñas y adolescentes desde los 7 a 14 años en Bogotá a través de un análisis de riesgos basados en la norma ISO 27005.
- Pacheco, B., Gutiérrez, J. L. L., & Ríos, N. G. (2018). Diagnóstico de utilización de Redes sociales: factor de riesgo para el adolescente. Revista Iberoamericana para la Investigación y el Desarrollo Educativo: RIDE, 8(16), 53-72.
- Pineda, C. O., Torres, C. A., Carreño, T. P., & Rodríguez, R. A. (2019). El sexting y su relación con los esquemas tempranos de inadaptación en adolescentes. Revista Argentina de Clínica Psicológica.
- Pittaro, M. (2020). Cyberbullying in adolescence: Victimization and adolescence. In Developing Safer Online Environments for Children: Tools and Policies for Combatting Cyber Aggression (pp. 131-154). IGI Global.
- Posada Maya, R. (2021). ¿ Delincuencia sexual virtual? Una aproximación desde la revolución tecnológica. Estudios críticos 8: jurisprudencia de la Corte Suprema de Justicia.
- Quimbayo, A. R., Campiño, C. A. F., Patarroyo, N. V. H., & Osorio, G. O. A. (2018). Adicción y abuso a dispositivos móviles en estudiantes universitarios, Pereira. Cuaderno de Investigaciones: Semilleros Andina, 11.
- Ramos-Soler, I., López-Sánchez, C., & Torrecillas-Lacave, T. (2018). Percepción de riesgo online en jóvenes y su efecto en el comportamiento digital. Comunicar, 26(56), 71–79.
- Rial, A., Gómez, P., Varela, J., & Braña, T. (2014). Actitudes, percpeciones y uso de internet y las redes sociales entre los adolescentes de la comunidad gallega. Anales De Psicología/Annals of Psychology, 30(2), 642–655.
- Rodríguez-Álvarez, J. M., del Carmen Cabrera-Herrera, M., & Jiménez, S. Y. (2018). Los riesgos de las TIC en las relaciones entre iguales. Cyberbullying en Educación Primaria y Secundaria. Innoeduca. International Journal of Technology and Educational Innovation, 4(2), 185–192.

- Rodríguez, C. R. (2020). Los menores ante los peligros digitales en México y su protección legal. Universos Jurídicos, 1(15), 236–259.
- Rodríguez, M. D., Moreno, Méndez, V. G., & Martín, A. M. R. (2018). Alfabetización informacional y competencia digital en estudiantes de magisterio. Profesorado, Revista de Currículum y Formación Del Profesorado, 22(3), 253–270.
- Ruiz, Y. P., Nieto, R. M., & Vozmediano, M. M. (2019). Patrones de uso, control parental y acceso a la información de los adolescentes en la red. Estudios Sobre El Mensaje Periodístico, 25(2), 995.
- Save The Children, «Grooming: ¿Qué es? ¿Cómo detectarlo? Y como prevenirlo,» 1 Julio 2019. [En línea]. Available: https://www.savethechildren.es/actualidad/grooming-que-es-como-detectarlo-y-prevenirlo.
- Sinchiguano Allán, D. E. (2020). Descripción del fenómeno del grooming y su prevención (Bachelor's thesis, Quito).
- Soriano-Ayala, E., Hermosilla-Rivera, A., Cala, V. C., & Dalouh, R. (2018). Riesgos en Internet: el mal uso de las Tecnologías de la Información y la Comunicación. EDUTECH REVIEW. International Education Technologies Review, 5(1), 43–50.
- Unicef, & others. (2014). Grooming. Guía práctica para adultos: Información y consejos para entender y prevenir el acoso a través de Internet. Buenos Aires: Fondo de las Naciones Unidas para la Infancia (UNICEF).
- Vázquez Gavilanes, M. P. (2021). Factores protectores y de riesgo en el uso de redes sociales en adolescentes. Universidad del Azuay.
- Villacampa Estiarte, C., & Gómez Adillón, M. (2016). Nuevas tecnologías y victimización sexual de menores por online grooming. Revista Electrónica de Ciencia Penal y Criminología, 2016, vol. 18, núm. 2, p. 1-27.
- Whittle, H., Hamilton-Giachritsis, C., Beech, A., & Collings, G. (2013). A review of online grooming: Characteristics and concerns. Aggression and violent behavior, 18(1), 62-70.
- Wolak, J., Finkelhor, D., Mitchell, K. J., & Ybarra, M. L. (2010). Online “predators” and their victims: Myths, realities, and implications for prevention and treatment.