[Cierre de edición el 01 de Setiembre del 2019]

doi: http://dx.doi.org/10.15359/ree.23-3.17
URL: http://www.una.ac.cr/educare
CORREO: educare@una.cr

Peligros de las redes sociales: Cómo educar a nuestros hijos e hijas en ciberseguridad

Social Nerworks Dangers: How to educate our childs in cibersecurity

Perigos das redes sociais: como educar nossas crianças em segurança cibernética

Cristel Astorga-Aguilar
Universidad Nacional
Región Huetar Norte y Caribe
Costa Rica
cristel.astorga.aguilar@una.cr
https://orcid.org/0000-0002-1151-9954

Ileana Schmidt-Fonseca
Universidad Nacional de Costa Rica
Región Huetar Norte y Caribe
Costa Rica
ileana.schmidt.fonseca@una.cr
https://orcid.org/0000-0001-6227-3299

Recibido • Received • Recebido: 22 / 11 / 2017
Corregido • Revised • Revisado: 04 / 02 / 2019
Aceptado • Accepted • Aprovado: 05/ 05 / 2019

Resumen: El objetivo de esta investigación es analizar el estado del arte en el país sobre el conocimiento de los peligros de las redes sociales en línea y cómo protegerse por medio de buenas prácticas de ciberseguridad para las personas menores de edad. Por medio de una revisión bibliográfica se exponen diferentes temáticas relacionadas con manejo de las redes sociales y el peligro al que se exponen niños, niñas y adolescentes en Costa Rica; se evalúan términos de seguridad y privacidad, el rol de los padres y las madres de familia y algunos de los elementos en ciberseguridad de las redes sociales más populares en estas generaciones. Entre los principales hallazgos, se determinó que los mayores peligros de las redes sociales para las personas menores de edad son el *ciberbulling, grooming, sexting* y adicción, los cuales, sin una adecuada educación en seguridad cibernética, les hace más vulnerables. Las redes sociales más populares entre la niñez y la juventud son *Facebook, Instragram, Whatsapp y SnapChat,* y cada una se rige por una serie de condiciones de uso; además cada red social ofrece herramientas para asegurar la privacidad y la seguridad de los datos, pero deben ser configurados, y esto es básicamente lo que conocemos como ciberseguridad. Educar en ciberseguridad a las personas menores de edad es un nuevo reto para los padres y las madres de familia, que deben prepararse y conocer para enseñarles a protegerse de estos nuevos peligros.

Palabras claves: Medios sociales; tecnología de la comunicación; acceso a la información; educación familiar.

doi: http://dx.doi.org/10.15359/ree.23-3.17
URL: http://www.una.ac.cr/educare
CORREO: educare@una.cr

Abstract: This research aims to analyze the state of the art in the country of the knowledge of dangers of online social networks and how to protect minors through good cybersecurity practices.Through a bibliographic review, different topics related to the management of social networks and dangers young people in Costa Rica are exposed to. Security and privacy terms are evaluated, as well as the role of parents, and some elements of Cybersecurity of the most popular Social Networks among underage people. Among the most important findings, it was determined that the greatest dangers of social networks for minors are harassment, cyberbullying, grooming, sexting and addiction, which, without an adequate education in Cybersecurity, make children vulnerable. The most popular social networks online among children and adolescents are *Facebook, Instragram, Whatsapp,* and *SnapChat*, and each one is governed by a series of conditions; these media also offer a series of tools to ensure privacy and data security, but they must be configured and this is basically what we know as Cybersecurity. Educating children in cybersecurity is a new challenge for parents: they must know and be prepared to teach their children on how to protect themselves from these new dangers.

Keywords: Social Media; **communication technology**; access to information; family education.

Resumo: O objetivo desta pesquisa é analisar o estado da questão no país sobre o conhecimento dos perigos das redes sociais em linha e como se proteger através de boas práticas de segurança cibernética para pessoas menores de idade. Por meio de uma revisão bibliográfica, são considerados diferentes temas relacionados à gestão das redes sociais e ao perigo que estão expostas crianças e adolescentes na Costa Rica; os termos de segurança e privacidade são avaliados, o papel dos pais e mães de família e alguns dos elementos da segurança cibernética das redes sociais mais populares dessas gerações. Entre as principais conclusões, determina-se que os maiores perigos das redes sociais para menores são o cyberbulling, grooming, sexting e o vício, que, sem uma educação adequada em segurança cibernética, os torna você mais vulnerável. As redes sociais mais populares entre crianças e jovens são Facebook, Instragram, Whatsapp e SnapChat, e cada uma é administrada por uma série de condições de uso; além disso, cada rede social oferece ferramentas para garantir a privacidade e a segurança dos dados, porém devem ser configuradas, e isso é basicamente o que conhecemos como segurança cibernética. Educar menores em segurança cibernética é um novo desafio para pais e mães, que devem se preparar e conhecer para ensiná-los a se proteger desses novos perigos.

Palavras-chave: Mídia social; tecnologia de comunicação; acesso à informação; educação familiar.

Introducción

En la actualidad, el uso de la tecnología es característico de todas las poblaciones a nivel local, nacional e internacional; específicamente el manejo de las redes sociales en línea son parte del diario vivir de muchas personas y, en especial, de la niñez y la adolescencia costarricense.

No obstante, en muchas ocasiones, la manipulación de la información que se realiza es en contra de las políticas de seguridad y privacidad que deberían imperar en el manejo de datos personales, al considerar la vulnerabilidad de la población a la que hace énfasis este estudio.

doi: http://dx.doi.org/10.15359/ree.23-3.17
URL: http://www.una.ac.cr/educare
CORREO: educare@una.cr

Por lo tanto, el objetivo de esta investigación es analizar el estado del arte en el país sobre el conocimiento de los peligros de las redes sociales en línea y cómo protegerse por medio de buenas prácticas de ciberseguridad para las personas menores de edad.

Contextualizando el origen de las redes sociales y su acelerado avance en la aparición de nuevas tendencias de comunicarse, así como en el uso que se les da, se denota la relevancia de brindar recomendaciones que sirvan de guía de cómo proteger y educar la forma de relacionarse a través de internet. Hütt (2012) menciona que "Internet ha facilitado la creación de espacios de interacción virtual innumerables" (p. 125), lo que implica que las redes sociales, como *Facebook, WhatsApp e Instagram* son de las más comunes entre la juventud, según Chacón (2016); así como la aplicación *Snapchat,* de acuerdo con Herrera (2015).

Por medio de una revisión bibliográfica sobre los principales conceptos relacionados con redes sociales en línea se analizan cuáles son sus implicaciones, peligros e impactos para la niñez y la adolescencia, así como las recomendaciones en seguridad y privacidad que deberían considerar los padres y madres de familia para asegurar que sus hijos e hijas realicen una interacción más responsable.

Contextualizando

Según Shin, Lee y Hall (2014, citados en Sánchez, Schmidt, Zuntini y Obiol, 2017): "La era moderna de las redes sociales comenzó con la mejora de la performance de internet a partir de 1995. En el periodo 2002-2004 aparecieron y se promocionaron Cyworld, Friendster, Plaxo, Reunion.com, Hi5, LinkedIn, MySpace, Orkut, Facebook, y Live Spaces..." (p. 72). En Costa Rica, para el año 2005, surge entre la niñez y la adolescencia la popularidad de la red social Hi5 entre otras, lo cual para los padres y las madres de familia era una experiencia desconocida.

Si bien muchos entendían el concepto de red social, en aquella época nadie vislumbraba su impacto en la niñez y adolescencia, no se alcanzaba a dimensionar la implicaciones tanto positivas como negativas que podrían tener. Y esto no es de extrañar, pues para 1990, Costa Rica apenas iba ingresando a la red de redes con su acceso a BITNET; tal como lo narra Siles (2012), e los primeros pasos de un pequeño grupo de ingeniería y asistentes, dirigido por Teramond, estableció el primer enlace a BITNET en el país. El nodo costarricense en la Universidad de Costa Rica (UCR) conectado a Florida Atlantic University el 8 de noviembre de 1990 fue el primer enlace a BITNET en Centroamérica.

Para esos tiempos, en los colegios y escuelas de nuestro país no existían laboratorios de computadoras, y muy poca gente tenía una computadora en su casa. A pesar de que el ingreso a BITNET fue el paso que permitió a Costa Rica ingresar en esta nueva tecnología, su auge duró solo dos años; para 1993, la iniciativa era conectarse a internet. El grupo de Teramond estableció

doi: http://dx.doi.org/10.15359/ree.23-3.17
URL: http://www.una.ac.cr/educare
CORREO: educare@una.cr

el primer acceso a internet en Costa Rica el 26 de enero de 1993, conectando 12 nodos ubicados en diferentes edificios de la UCR. Tres meses después, en abril de 1993, su grupo estableció un enlace a internet en otras universidades públicas, como el Instituto de Tecnología de Costa Rica y la Universidad Nacional Estatal a Distancia, y así creó la primera red de internet en Centroamérica (Siles, 2012).

Diez años después, esto había cambiado radicalmente, tras el impulso dado a internet por la academia, el Estado apuesta a su democratización; según anota Siles (2012), entre 2000 y 2005, cuando el Ministerio de Ciencia y Tecnología (MICITT) e Instituto Costarricense de Electricidad (ICE) implementaron el internet avanzado, el acceso a internet fue entonces posible en universidades y centros de trabajo, y en algunos colegios y escuelas. Además, el teléfono celular se dirigía a dejar de ser solo un aparato para hacer llamadas y convertirse en un centro de comunicación inteligente. Menciona McDuffie (2014) que hace diez años no había *iPhones*, *iPads* y *Facebook* y la mayoría de las otras redes sociales populares no existían. Entonces, aunque muchos desafíos han existido durante más de una década, hay nuevas categorías de amenazas.

De esas primeras cuentas en redes sociales con las que se interrelacionaron la niñez y la adolescencia en nuestro país, han pasado doce años, y parece que sigue siendo un dilema de educación para muchos padres, madres y docentes. Actualmente, existen decenas de redes sociales a lo largo y ancho del planeta, algunas públicas y otras de carácter privado, unas de tema general; otras de temas específicos, pero en cualquier punto del mundo que estemos, nuestros hijos e hijas tienen acceso a ellas todo el tiempo.

En la actualidad, a través de los medios de comunicación se conoce que las personas menores de edad están siendo engañadas, utilizadas en redes de prostitución infantil, secuestradas y violadas por "supuestas" amistades que hicieron en redes sociales y que no son más que perfiles falsos de personas pedófilas y degeneradas. Para el año 2017, señalan las noticias que parece que aún nuestra sociedad no está segura de cómo debe educar a las persons menores de edad. Titulares como "Desmantelan red de pornografía infantil por WhatsApp; caen 2 en México", especifica que 3 sospechosos son de Costa Rica (Associated Press, 2017). "Así fue como un pervertido extorsionó a 4 niñas en Golfito" (Solano, 2017) y "Colegiales de 7° a 9° son más propensos a sufrir 'ciberbullying' " (Recio, 2017), son algunos ejemplos, que narran cómo el exceso de confianza, poco conocimiento de las redes sociales y su uso indebido pone en peligro a niños, niñas y adolescentes en el país.

Y realmente hay consejos que los grupos expertos en ciberseguridad dan, como: no aceptar solicitudes de amistad de sujetos desconocidos, no tener público los contenidos que sube en la red social, no subir a la red información personal como direcciones, no publicar fotografías de niños y niñas que muestren sus centros educativos y ubicación de los hogares, entre otros. Nunca ha existido una receta única de cómo educar a esta población tan vulnerable.

doi: http://dx.doi.org/10.15359/ree.23-3.17
URL: http://www.una.ac.cr/educare
CORREO: educare@una.cr

El tema de investigación es importante a nivel internacional, nacional y aún más a nivel regional, ya que en comunidades rurales en las regiones fuera de la gran área metropolitana, donde la brecha digital es significativa tal como lo muestra el documento *Programa sociedad de la información y el conocimiento. Universidad de Costa Rica* (Amador, 2017): "La literatura internacional señala ampliamente la existencia de una brecha digital generada por la zona geográfica, donde las viviendas ubicadas en regiones urbanas presentan un mayor nivel de tenencia de todo tipo de tecnologías" (p. 197), y además menciona que en el país hay una diferencia en el 2016 de hasta 20 % de tenencia de TIC entre zonas geográficas. Amador (2017) también asocia los niveles de educación con la brecha digital, con lo que tendremos más personas que desconocen el peligro que corren sus hijos e hijas ante el uso de las redes sociales y sobre cómo orientarles en temas de seguridad y privacidad. Por ello es de suma importancia que nos acerquemos a su mundo, les conozcamos y entendamos, así los padres y las madres tendrán mayores herramientas para formarles y educarles en ciberseguridad.

Conociendo el espacio de acción de nuestros hijos e hijas en redes sociales

Las redes sociales son un fenómeno inherente del ser humano, como se desprende del comentario de Hütt (2012): "Las relaciones interpersonales son parte de la esencia natural del hombre, y sin lugar a dudas esta dinámica es trasladada a las organizaciones, las cuales como entes vivos y simbióticos requieren y dependen de una interacción permanente entre sus integrantes" (p. 122). La forma en que nos relacionamos ha sido estudiada junto con la humanidad; actualmente las conocemos ligadas a las plataformas de las tecnologías de información y comunicación (TIC), sin embargo, este es su medio de transmisión más reciente. No obstante, para comprender las redes sociales en línea, debemos primero comprender qué es en sí una red social. En su artículo, Peyró (2015) dice:

> Como mecanismo de adaptación y supervivencia formamos parte de diferentes grupos, desde la familia a los amigos, en todos los ámbitos, académicos, profesionales, culturales, etc. De este modo, los seres humanos estamos inmersos de manera permanente en una red de relaciones, y establecemos conexiones con nuestros iguales pues como seres sociales necesitamos relacionarnos, tomar contacto con el otro. Formamos parte de redes, y en ellas definimos y son definidos nuestros roles, nuestras relaciones, y en base a estas, obtenemos y transmitimos información relevante para diversos ámbitos de nuestra vida. (p. 236)

Es, entonces, la red social un espacio donde los seres humanos interactúan y establecen nexos con otras personas; desde cercanas hasta conocidas de trabajo, amigos, y amigos de amigos y amigas, pero que igualmente integran parte de la red. Este espacio de interacción permite socializar temas con contenidos que favorecen una conexión con los demás sujetos y de

doi: http://dx.doi.org/10.15359/ree.23-3.17
URL: http://www.una.ac.cr/educare
CORREO: educare@una.cr

esta conexión surge un intercambio en donde se envía y se recibe información, principalmente de aquellos temas asociados a nuestro interés, como por ejemplo música, académicos, culturales entre otros. Pero aún más allá de la información compartida, como indica Peyró (2015), en las redes nos definimos y son definidos nuestros comportamientos, que surgen como mecanismos de adaptación y supervivencia. La importancia de ser parte de una red se ve amplificado con el uso de la tecnología, y en la adolescencia, donde aún se están definiendo el rol del individuo en la sociedad, estas cobran mayor relevancia, como indica Pérez (2016), refiriéndose a los grupos adolescentes: "El uso de la tecnología para acceder a redes sociales, pone en evidencia el significado que tiene la integración social en el grupo estudiado" (p. 120).

Las personas menores de edad en Costa Rica, siguiendo con Pérez (2016), utilizan mayoritariamente el teléfono celular (un 97 % de las consultadas) e indica que:

> El hacer llamadas no es la actividad más importante, por el contrario, ocupa una posición intermedia. Las utilizaciones principales son … el envío de mensajes, … acceder a Internet, … escuchar música, ver videos, usar la alarma y tomar fotos". (p. 110)
> Por otra parte:
>
> La necesidad de permanecer conectado, trasciende hasta su tiempo libre.
>
> Escuchar música, entrar a redes sociales y navegar por Internet está en las actividades predilectas de los jóvenes. (Chacón, 2016, Crecer entre 'likes y shares, párr. 9-10)

¿Qué ha cambiado en el acceso a las redes sociales entre la juventud? La respuesta tiene relación con la forma en que acceden a esta, es decir, a través de las tecnologías de información y comunicación (TIC).

La palabra tecnología "hace referencia al conjunto de conocimientos técnicas, conocimientos y procesos, que sirven para el diseño y construcción de objetos para satisfacer necesidades humanas que permitan satisfacer necesidades humanas" (Alegsa, 2016). Por su parte, Rendón-Rojas (2007), lo explica así: "La tecnología es un conocimiento que produce o transforma objetos individuales para resolver problemas concretos; pero lo hace siguiendo reglas que son producto de una investigación científica, por lo que es posible explicar el por qué esas reglas son eficaces" (p. 4).

Y debemos también entender que existe diferencia entre la tecnología y el objeto tecnológico producido por ella, "esos instrumentos los denominamos **objetos tecnológicos,** y son producto del conocimiento tecnológico, por lo que no se deben confundir con la tecnología" (Rendón, 2007, p. 4).

doi: http://dx.doi.org/10.15359/ree.23-3.17
URL: http://www.una.ac.cr/educare
CORREO: educare@una.cr

Ahora bien, si se analiza la definición y se piensa en ejemplos de tecnología de información y comunicación se puede pensar en internet, bases de datos electrónicas, repositorios, sitios web. Si hablamos de objetos tecnológicos o instrumentos vamos a pensar en la computadora, tabletas y teléfonos inteligentes.

Por lo tanto, las redes sociales en línea definidas por Pérez (2016) son accedidas por la niñez y la adolescencia a través de internet, utilizando teléfonos celulares, computadoras y tablets. Esto aumenta las condiciones de vulnerabilidad, pues el ingreso en línea para menores de edad es asincrónico, es decir, no existe límite de espacio y tiempo.

Las tecnologías de información y comunicación permiten acceso sin límite a las redes sociales, y además estas son de fácil uso para menores de edad, pero no tienen la preparación adecuada para manejar todo lo que esto significa, como lo indica Vanderhoven et al. (2014, citando a Livingstone, 2004): "Se ha constatado que, si bien a los niños les resulta fácil acceder y encontrar cosas en Internet, no tienen tanta habilidad para evitar algunos de los riesgos a los que se ven expuestos por la red" (p. 2). Cabe enfatizar que, en Costa Rica, este fenómeno de fácil a acceso a las redes sociales no es diferente, según indica Chacón (2016) en un artículo "Adolescentes cambian dinámica en el uso de la web", con datos del estudio realizado por RED506 durante el año 2016; donde se consultó "¿cuáles redes sociales utilizó en los últimos 30 días?", se obtuvo que el 90 % utiliza *Facebook*, 58 % *Whatsapp* y el 18 % *Instagram*. En otros estudios, se resalta, además, que la red *Snapchat* es una red que viene emergiendo vertiginosamente.

Peligros en la red

Vanderhoven, Schellens y Valcke (2014) mencionan del estudio de De Moor y colaboradores "Teens and ICT: Risks and Opportunities" (2008), que hay tres tipos de peligros en la red: de contenido, de contacto y comercial.

En síntesis, en las definiciones de Vanderhoven et al. (2014), los peligros de contenido se entienden como aquellos mensajes de odio y mensajes diversos, entre otros que podrían influenciar negativamente a nuestra niñez y juventud. En este rango se incluyen: acceso a pornografía, mensajes racistas, xenofóbicos, sectarios, entre otros. Los de contacto están ligados a todos los medios de comunicación que existen hoy en día a través de las TIC, dígase mensajerías SMS, mensajería instantánea, chats, redes sociales, entre otros, estos están ligados a *ciberbulling,* acoso sexual, riesgos de privacidad, donde los datos y fotos personales puedes ser sustraídos. El último, el comercial, se liga al uso indebido de la información y fotos personales, uso de los datos para hacer seguimiento del comportamiento de la niñez y la adolescencia.

Echeburúa y De Corral (2010) hacen referencia al abuso de las tecnologías de la información y la comunicación. Citan lo siguiente:

doi: http://dx.doi.org/10.15359/ree.23-3.17
URL: http://www.una.ac.cr/educare
CORREO: educare@una.cr

> Los riesgos más importantes del abuso de las TIC son, además de la adicción, el acceso a contenidos inapropiados, el acoso o la pérdida de intimidad. Así, en las redes se puede acceder a contenidos pornográficos o violentos o transmitir mensajes racistas, proclives a la anorexia, incitadores al suicidio o a la comisión de delitos (p. 92).

Además, "existe el riesgo de crear una identidad ficticia, potenciada por un factor de engaño, autoengaño o fantasía … [y se] favorece el mal uso de información privada por parte de personas desconocidas" Echeburúa y De Corral (2010, p. 92). Las personas menores de edad costarricenses, se encuentran expuestas a este tipo de riesgos y, por ende, es responsabilidad de las generaciones adultas, iniciando con los padres y madres de familia, tener un conocimiento general de las principales redes sociales, con el fin de poder brindar recomendaciones de acceso y seguridad en el manejo de la información. Como complemento, Arab y Díaz (2015) hacen la siguiente referencia:

> La masiva popularidad de la comunicación en línea entre los adolescentes ha provocado reacciones encontradas. Las preocupaciones se han focalizado en el desarrollo de relaciones superficiales con extraños, en el riesgo de adicción y en el aumento de la probabilidad de ser víctima de ciberacoso. (p. 8)

Por ello debemos primero conocer bien los peligros a los que está expuesta nuestra niñez y adolescencia y, posteriormente, cómo podemos protegerla. Como menciona García-Maldonado, Joffre-Velázquez, Martínez-Salazar y LLanes Castillo (2011): "La participación de los padres es muy importante, pues muchos imponen reglas a sus hijos acerca del uso que deberían hacer de Internet, y, sin embargo, no son realmente conscientes de las amenazas que se encuentran en la red" (p. 123). Se puede tener leyes y sistemas educativos con mecanismos de vigilancia, pero son los padres y madres la primera barrera de protección de sus hijos e hijas. "Estas acciones deben fortalecerse con la participación de los padres de familia, para que sus hijos hagan un uso adecuado de las redes virtuales y de la tecnología" (Maya-Alvarado, Tapia-Quintana citados por García-Maldonado et al., 2011, p. 124).

El acelerado cambio en la tecnología y sus aplicaciones facilita que la población de interés a la que hace énfasis este estudio se muestre vulnerable y esté expuesta a diferentes riesgos producto del desconocimiento sobre medidas de seguridad. Una persona menor de edad debe acompañarse y educarse sobre los riesgos a los que se expone al acceder a las redes sociales en línea, el entorno familiar es pieza fundamental en este proceso.

doi: http://dx.doi.org/10.15359/ree.23-3.17
URL: http://www.una.ac.cr/educare
CORREO: educare@una.cr

Ciberbullying

Uno de los populares y conocidos peligros es el *ciberbullying*, en gran parte porque su homólogo en los espacios sociales tradicionales, principalmente en ambientes escolares, es el *bullying*. Este fenómeno social, cuyo vocablo inglés significa intimidación, es un fenómeno creciente en nuestra sociedad, el cual ha sido ampliamente estudiado, y con el que se ha estado realizando una lucha mediática por erradicarlo, principalmente por los efectos que ocasiona en quienes lo sufren.

Sin embargo, las nuevas tecnologías de comunicación e información han potenciado este problema, pues ya no solo se circunscribe a un espacio físico y por el tiempo que víctima y victimario coincidieran ahí, sino que han ampliado el ámbito de acción a cualquier momento del día y de forma continua a través de cualquier medio que permita la comunicación, computadoras, teléfonos celulares, por mensajería SMS, chats, redes sociales, etc., y, además, lo ha convertido en una forma asincrónica, es decir, no es necesario que ambos (víctima y victimario) estén al mismo tiempo en el espacio virtual.

La ciberviolencia o violencia virtual se refiere a la "forma en que los medios de comunicación (internet, telefonía móvil, sitios web y/o videojuegos online) pueden favorecer la violencia e incluso ejercerla sobre distintos grupos de personas" (Arab y Díaz, 2015, p. 10). En el mismo artículo "Impacto de las redes sociales e internet en la adolescencia: Aspectos positivos y negativos", se menciona:

> Se puede manifestar de distintas formas: publicar en internet una imagen, video, "memes", datos privados y cualquier información que pueda perjudicar o avergonzar a alguien o hacerse pasar por otra persona creando un perfil falso, ya sea para exponer aspectos privados de ella o agredir a terceros, entre otros. (Arab y Díaz, 2015, p.10)

Según García-Maldonado et al. (2011) en un estudio realizado sobre el *ciberbullying* y referenciando estudios sobre el tema, "diversos estudios realizados en Canadá (50), España (51) y Estados Unidos (52) estiman que uno de cada cuatro estudiantes está involucrado en este problema como cibervíctima o ciberagresor, o en ambos roles" (p. 121). Explican, más adelante, que además en otros estudios en Suecia y Estados Unidos, al menos un 10 % de la niñez ha sido cibervíctima.

Sin embargo, tal vez el dato más relevante destacado en este estudio de García-Maldonado et al. (2011) es el hecho de que el peligro de sufrir intimidación a través de entornos virtuales (*ciberbullying*), se duplica de su homólogo en entornos tradicionales. Las consecuencias del *ciberbullying*, para aquellos que lo sufren, van desde problemas emocionales, académicos y de comportamiento, hasta baja autoestima, depresión e incluso intentos suicidas u homicidas.

doi: http://dx.doi.org/10.15359/ree.23-3.17
URL: http://www.una.ac.cr/educare
CORREO: educare@una.cr

Pornografía infantil

La difusión de imágenes de menores de edad en la red con fines eróticos es muy demandada, Negredo y Herrero (2016) remarcan: "La descarga, intercambio y producción de pornografía infantil es una conducta delictiva de importancia creciente" (p. 217). Existe incluso mafia organizada que se especializa en este tema, lo mueve en red oscura, es decir, en ambientes de internet de uso restringido y exclusivo para clientes que pagan su acceso a ella, y así tratan de evitar que los controles policiales e INTERPOL afecten sus operaciones.

Este crimen cibernético, contrario a lo que muchos piensan, no se limita solo a niños, niñas, jovencitos y jovencitas en riesgo social que se exponen a secuestros, violaciones o en condición de explotación infantil. Negredo y Herrero (2016) refiere:

> La producción de material pornográfico suelen ser originarias de países donde existe una legislación laxa o inexistente en esta materia. También son países con elevados índices de pobreza, lo que facilita el acceso a las víctimas, en muchas ocasiones, facilitado por los propios padres. Rusia, Ucrania, algunos países de la antigua URSS, el Sudeste Asiático y países de América Central y del Sur suelen ser los objetivos más frecuentes. Sin embargo, la producción doméstica puede producirse en cualquier país (Sotoca, 2010)" (p. 220).

Nuestros hijos e hijas están expuestos también. Aquellas fotografías inocentes donde los menores de edad se lucen en vestido de baño en la playa o la piscina, las fotos de la pijamada donde varias niñas en mudadas cortas juegan, son objeto de esta depravación. Toda imagen de nuestros niños y niñas que está en la red puede ser utilizada por estas redes, si no se tienen los cuidados y los conocimientos para evitarlo.

Grooming

En el *Grooming*, el sujeto abusador accede a la inocencia e ingenuidad de las personas menores de edad para acercárseles y ganarse su confianza utilizando las redes sociales, muchas veces con perfiles falsos, con el único objeto de que, una vez con su confianza, les obligan a conductas de abuso sexual. Para Arab y Díaz (2015), "es un conjunto de estrategias que una persona adulta desarrolla para ganar la confianza del/la [*sic*] joven a través de internet… adquiriendo control y poder sobre él/ella, con el fin último de abusar sexualmente de él/ella" (p. 10).

Los autores mencionan que tiene distintas etapas:

> **1. Amistad.** El abusador se hace pasar por otr@ [*sic*] joven y se gana la confianza de la víctima, seduciéndola y obteniendo así sus datos personales (¿Qué edad tienes?, ¿Con quién vives?, ¿Cuál es tu dirección?, ¿Qué hacen tus padres?, ¿En qué colegio estás?).

doi: http://dx.doi.org/10.15359/ree.23-3.17
URL: http://www.una.ac.cr/educare
CORREO: educare@una.cr

2. Engaño. El abusador finge estar enamorado de la víctima para conseguir que se desnude y realice actos de naturaleza sexual frente a la *webcam,* o le envíe fotografías de igual tipo.
3. Chantaje. El abusador manipula a la víctima amenazándol@ [*sic*] con que va a hacer público el material sexual, si no continúa enviándoselo. Las repercusiones del *grooming* en la víctima están asociadas a depresión, baja autoestima, desconfianza, cambios de humor repentino y bruscos, bajo rendimiento académico, aislamiento, alteraciones del sueño y de la alimentación, ideas e intentos de suicidio. (Bennett, O'Donohue, 2014 y Policy statement sexually, contaception y the media, citados por Arab y Díaz, 2015, p. 10)

Sexting

Este peligro en las redes sociales surge de la necesidad de la persona menor de edad de ser aceptada y avalada por sus pares o por intereses sentimentales. El sexting, por definición, se entiende como:

> Práctica que consiste en compartir imágenes de tipo sexual, personal o de otros, por medio de teléfonos o internet. El riesgo, es que las imágenes sean publicadas y viralizadas sin permiso. Con ello la intimidad queda expuesta a la mirada pública. (Arab y Díaz, 2015, p. 10)

Es una práctica común en la juventud, que da paso a otros peligros, como el acoso o la pornografía infantil.

Ciberadicción o conducta adictiva a internet

Este peligro es definido por Arab y Díaz (2015):

> Patrón de comportamiento caracterizado por la pérdida de control sobre el uso de internet. Esta conducta conduce al aislamiento y al descuido de las relaciones sociales, de las actividades académicas, de las actividades recreativas, de la salud y de la higiene personal. (p. 10)

En este apartado se incluye la adicción a los videojuegos:

> El *gambling disorder* se incluye en el capítulo *Substance-related and addictive disorders* con el argumento de que las conductas de juego activan sistemas de recompensa similares a los que activan las drogas y producen algunos síntomas conductuales comparables a los producidos por sustancias. (Carbonell, 2014, p. 91)

doi: http://dx.doi.org/10.15359/ree.23-3.17
URL: http://www.una.ac.cr/educare
CORREO: educare@una.cr

Es, por lo tanto, una conducta adictiva como cualquier otra, pues provoca un cambio de comportamiento social en los sujetos adolescentes y en los niños o las niñas que los sufren, y conduce a que dejen sus actividades cotidianas y se aíslen, lo cual, a su edad, es aún más peligroso, pues están en formación y pueden perjudicar su desarrollo adulto. Algunos indicadores de ciberadicción son:

- El tiempo de uso ha ido en aumento.
- El rendimiento académico ha disminuido notablemente porque dedica demasiado tiempo a estar conectado.
- Manifiesta una gran irritabilidad cuando alguien l@ interrumpe.
- Se ve ansios@ [*sic*], nervios@, [*sic*] deprimid@ [*sic*] o aburrid@ [*sic*] cuando no está conectad@ [*sic*] a internet.
- Deja de reunirse con sus amig@s [*sic*] por estar frente a la pantalla.
- Se queda hasta muy tarde en la noche navegando, chateando, entre otros.
- Está pendiente a cada momento de sus mensajes y mira en forma obsesiva el doble check del *WhatsApp*.
- Revisa constantemente su teléfono celular para ver si ha llegado un mensaje y presenta vibraciones fantasmas.
- Habitualmente, lo primero y lo último que hace al despertar y al dormir es revisar el teléfono. (Arab y Díaz, 2015, pp. 10-11)

El papel del padre y la madre de familia o la persona adulta responsable de menores de edad es ser constantes en aplicar mecanismos de vigilancia con el fin de detectar este tipo de actos y evaluar la constancia con la que se repiten, se puede iniciar de forma silenciosa e ir en aumento, por lo que el monitoreo es fundamental.

Educando en ciberseguridad

La ciberseguridad también conocida como seguridad cibernética, abarca algunos campos, como: supervisar y gobernar, investigación, operación y mantenimiento, proteger y defender, entre otros. "Proteger y defender" es el campo que se avoca a la protección a la vida, protección de la propiedad y seguridad de la información. Al respecto, McDuffie y Piotrowsky (2014) dicen que, de hecho, el Marco Nacional de la Fuerza de Trabajo de Ciberseguridad (NCWF) de NICE descompone el campo de seguridad cibernética en 7 categorías y alrededor de 32 conjuntos de habilidades funcionales. Otra categoría del NCWF es "proteger y defender". El foco de las

doi: http://dx.doi.org/10.15359/ree.23-3.17
URL: http://www.una.ac.cr/educare
CORREO: educare@una.cr

actividades en esta área es la preparación, la respuesta y enfoques de recuperación que maximizan la preservación de la vida, la protección de la propiedad y la seguridad de la información.

Prevenir y evitar todos los posibles riesgos que corre nuestra niñez y juventud está en manos de la ciberseguridad que se tenga, y abarcaría conceptos de seguridad y privacidad, para la preservación de su vida, protección de su propiedad y seguridad de su información. En el estudio *Programa sociedad de la información y el conocimiento. Universidad de Costa Rica,* Pérez (2016) remarca en sus conclusiones sobre las prácticas en ciberseguridad de adolescentes en Costa Rica: "En cuanto a la ciber-seguridad, las medidas que toman las y los [*sic*] adolescentes para un uso seguro y confiable de Internet y redes sociales es insuficiente" (p. 118).

La formación en ciberseguridad enfocada en el uso correcto de redes sociales en la niñez y la adolescencia recae en diferentes entes participantes en la acción didáctica: personal docente, estudiantes, padres y madres de familia, comunidad educativa e integrantes del contexto. Tal como se menciona en Pérez (2016): "Es fundamental emprender acciones educativas, familiares y comunitarias que promuevan la concientización y alternativas para el uso seguro" (p. 120). Sin embargo, para efectos de esta investigación, el énfasis es conocer los elementos que fundamenten a futuro la construcción de una metodología de enseñanza y aprendizaje por parte de padres y madres de familia, de manera que desde el hogar se coadyuve a los demás elementos participantes del sistema formal de enseñanza en una temática que es de especial relevancia para la calidad de vida de esta población.

Es importante entender el proceso de aprendizaje como cualquier sistema que permita la construcción de saberes y posterior modificación de las estructuras mentales.

> El aprendizaje es el término que se refiere a los procesos que permiten construir y transformar nuestra experiencia en conocimientos, valores, actitudes, habilidades, creencias, emociones y sensaciones que modifican nuestras estructuras mentales. El aprendizaje ocurre con o sin procesos de enseñanza formales; puede suceder de forma natural y a lo largo de toda la vida, por la experiencia personal individual o por la interacción con otros; en la escuela, pero también en la sociedad en general, puede adquirirse de los docentes, de cualquier otra persona, en forma individual y grupal. Se aprenden contenidos, pero también a pensar, a relacionarse con otros; así como las emociones y los sentimientos, los valores y la identidad cultural. (Seas, 2016, p. 34)

Por su parte, acompañando el aprendizaje se encuentra la enseñanza, proceso sumamente importante para lograr los objetivos y metas planteadas. El proceso de enseñanza se puntualiza en estrategias, técnicas y actividades mediadas, generadoras de experiencias de aprendizaje. La finalidad es que el alumnado logre una formación integral, la cual incluye el desarrollo de conocimientos (conceptuales, procedimentales, actitudinales), y de habilidades sociales y psicomotrices, a partir de un proceso riguroso de planificación y de contextualización (Seas, 2016).

doi: http://dx.doi.org/10.15359/ree.23-3.17
URL: http://www.una.ac.cr/educare
CORREO: educare@una.cr

Echeburúa y De Corral (2010) exponen un argumento importante de analizar en relación con la figura de los padres y madres dentro del proceso educativo en ciberseguridad:

> El uso de las TIC y de las redes sociales impone a los adolescentes y adultos una responsabilidad de doble dirección: los jóvenes pueden adiestrar a los padres en el uso de las nuevas tecnologías, de su lenguaje y sus posibilidades; los padres, a su vez, deben enseñar a los jóvenes a usarlas en su justa medida. (p. 94)

La figura del padre y la madre de familia se convierte en el actor principal del proceso no formal de enseñanza.

> Es un campo de estudio dinámico, que se construye, renueva y contextualiza en cada realidad educativa, tanto en el sistema educativo formal (dirigido a la obtención de grados o títulos propios del sistema educativo) como en el no formal. Asimismo, que la didáctica tiene una dualidad de funciones; por un lado, es un campo de estudio que genera conocimiento; y por otro, una guía práctica para la construcción de los procesos educativos (enseñanza, aprendizaje y evaluación). (Seas, 2016, p.12)

Es responsabilidad de los padres y madres construir el proceso educativo más idóneo y contextualizarlo a las nuevas tendencias en el ámbito de la comunicación, específicamente al uso y manejo de las redes sociales por parte de sus hijos e hijas. Es importante que analicen las características de su entorno y lugar donde se desarrollan, así como las personas con las que interactúan, con el fin de establecer los mejores mecanismos que permitan gestionar ciberseguridad.

Fernández-Montalvo, Peñalva e Irazabal (2015) exponen que, en algunas ocasiones, la preocupación que muestran los padres y madres con el uso de las tecnologías de la información y la comunicación por parte de sus hijos e hijas no está justificada, en razón de que proviene más del desconocimiento sobre las TIC que de una mala utilización de estas mismas. Por lo tanto, se demanda que el proceso de enseñanza y aprendizaje sea constante, dinámico y en permanente construcción, en razón, de los acelerados cambios tecnológicos y la incorporación de nuevas aplicaciones en redes sociales a los que se enfrentan la niñez y la adolescencia actualmente.

Es necesario desarrollar metodologías prácticas y contextualizadas, innovadoras y significativas, que permitan dar solución a problemáticas relacionadas con los peligros en la red a los que se enfrentan; Fernández-Montalvo et al. (2015) afirman que "es fundamental tener criterios claros sobre el uso adecuado del ordenador, [en el internet], así como de los indicadores del mal uso del mismo" (p. 114).

Asimismo, Arab y Díaz (2015) recalcan que "es indispensable por parte de los adultos autoeducarse y aprender todo lo relativo a internet, aplicaciones y redes sociales. Sólo así es

doi: http://dx.doi.org/10.15359/ree.23-3.17
URL: http://www.una.ac.cr/educare
CORREO: educare@una.cr

posible ejercer un adecuado monitoreo, acompañamiento y supervisión (Mosso y Penjerek (2008), especialmente en la etapa adolescente". (p. 8)

El padre y la madre de familia debe estar en la capacidad de facilitar conocimiento en la temática, entendiendo el conocimiento por medio de características citadas por Seas (2016), tales como:

> Es representacional (del mundo de las cosas), es personal (se produce a lo interno), es individual y social a la vez (implica una experiencia personal, así como contextos de interacción), es lingüístico (supone un proceso comunicativo), implica una relación (entre la persona y lo conocido), es emocional (influye en la construcción de significados), es un acto intencional (el acto de aprender y construir lo realiza el ser humano de manera consciente) y es dinámico y estático al mismo tiempo (implica un proceso en el que se pueda de un estado a otro de no saber a saber). (p. 24)

En la época donde vivimos, la niñez y la adolescencia se enfrentan a la tecnología y a las redes sociales, por ello el conocimiento no parte de cero; por el contrario, se deben aprovechar esas nociones previas y, con base en las experiencias, apoyar aprendizajes significativos aplicados al contexto donde se desarrollan. Los actores del proceso pueden trabajar con distintos tipos de conocimiento, tanto los teóricos, científicos y tecnológicos, así como los que aportan los grupos participantes del proceso y la sociedad misma. En relación con la didáctica y el conocimiento, se requiere que la niñez y la adolescencia obtengan conocimiento sobre ciberseguridad aplicada a redes sociales, pero que principalmente se apropien e interioricen con el aprendizaje, de manera que dicha información pase a sus estructuras cognitivas con el fin de identificar peligros en la red. Adicionalmente, Seas (2016), menciona:

> El conocimiento y la cognición involucran el uso de los sentidos, las emociones y la sensibilidad, que le permiten al individuo percibir: situaciones, elementos o circunstancias que le genera incertidumbre y la necesidad o el deseo de aprender o resolver un problema. (p. 29)

Para ello el padre y la madre de familia debe estar en constante actualización; formándose e investigando acerca de los cambios que se realizan en las redes sociales, con el fin de brindar las recomendaciones preventivas necesarias a nivel familiar, principalmente con niños, niñas y jóvenes. Debe tener en cuenta que su papel debe ser como mediador del proceso, facilitándoles la construcción de significados, de manera integrada para ser asimilados con sus conocimientos previos; por medio de la comprensión y utilización de esos aprendizajes para resolver problemas y transferirlos a nuevos contextos.

doi: http://dx.doi.org/10.15359/ree.23-3.17
URL: http://www.una.ac.cr/educare
CORREO: educare@una.cr

El uso de redes sociales y la seguridad informática son temáticas que constantemente tienen discusión a nivel local, nacional e internacional; sin embargo, con frecuencia se brindan datos relacionados con delitos, muertes, fraudes que sufre la niñez y la adolescencia, muchas veces por desconocimiento. Se requiere de una mayor presencia y supervisión por parte de las partes adultas y, en este caso en particular, de los padres y las madres de familia. Arab y Díaz (2015) ofrecen una amplia gama de recomendaciones e intervenciones:

- Bajar el tiempo de uso de redes sociales y de objetos tecnológicos al mínimo (una o dos horas por día) (Strasburger, 2010)
- Ser modelos de un adecuado uso de las herramientas que proporciona internet
- Definir en familia espacios libres de aparatos electrónicos
- Educar en mecanismos de autorregulación, ayudando a equilibrar las actividades *online* con las actividades *offline*. Es importante estimular actividades que no involucren pantallas y que fomenten la comunicación directa y sin mediatizadores electrónicos
- Hablar con el/la adolescente sobre el uso de internet, mostrándole que se confía en sus criterios y en su "no ingenuidad"; que se tiene interés por lo que hace; y que se respeta su conocimiento sobre la tecnología. No hay que olvidar los dos puntos fundamentales en la relación: el diálogo y la negociación, evitando acceder con una actitud desconfiada y controladora para llegar a un acuerdo de uso seguro
- Trabajar en la comprensión de las consecuencias de lo que se hace y/o se dice en la web
- Instruirse en el uso de internet en general y en el de todas las redes sociales en particular, conociendo la jerga que se utiliza en ellas, como requisito de la parentalidad moderna
- Recibir y pagar las cuentas de los celulares de los hijos, con el objetivo de tener la información de uso …
- Crear una lista de reglas (sitios a los que puede acceder, tiempos de uso, horarios, contenidos). Los celulares en la noche se deben cargar fuera de la pieza
- Ubicar los computadores en lugares comunes (salas de estar)
- Instalar herramientas de filtros de contenido (programas diseñados para controlar qué contenidos se permiten mostrar en la web), actualizándolos periódicamente …
- Controlar el historial de las páginas que se han usado en el computador (si se ha vaciado el fichero, probablemente es por alguna razón) … Asegurarse de que no haya contactos desconocidos en el *email* y en la mensajería instantánea
- Desconectar *wifi* en la noche

doi: http://dx.doi.org/10.15359/ree.23-3.17
URL: http://www.una.ac.cr/educare
CORREO: educare@una.cr

- Averiguar si en el colegio existe supervisión y programas de filtro de internet
- Explicar a los hijos que la información contenida en celulares y computadores y otros dispositivos puede ser vista y mal usada si son robados o perdidos. Es importante transmitirles que es mejor no guardar imágenes o información comprometedora
- Si un adolescente tiene acceso a una página que no es aceptable, es importante que los padres y madres no reaccionen de forma exagerada …
- Educar respecto a los riesgos asociados al uso de las redes sociales
- Ser consistentes con las consecuencias de un mal uso de las redes sociales …
- Estar alertas a cualquier variación significativa en el comportamiento físico, cognitivo, emocional y social del adolescente. (pp. 11-12)

Adicionalmente, en cada red social se pueden configurar opciones de seguridad y privacidad, por lo que es importante realizarlo en conjunto con los niños, las niñas, los adolescentes y las adolescentes, así como verificar y dialogar acerca de las condiciones de uso de cada una de ellas. Los padres y las madres deben tener claro que la formación inicia en casa y que, además, en la actualidad, la temática debe ser analizada constantemente, producto de la incorporación de nuevas tecnologías.

Ciberseguridad en las redes sociales

Tal vez lo más importante de repasar antes de conocer algunas de las herramientas de seguridad y privacidad que dan las redes sociales es que todas tienen condiciones de uso (en su mayoría con restricción de edad): el uso que se le da a la red social, contenidos que se pueden poner en la red, entre otros. Por ejemplo, tanto *Facebook, Snapchat y Whatsapp* tiene como restricción de edad mayor de 13 años e Instagram es de 14 años. Esto significa que si algo le ocurre a un niño o niña menor de esta edad la empresa no tiene responsabilidad alguna, pues su servicio advierte que no es permitido para esta población.

Por ello resulta muy importante conocer cada servicio al que acceden los menores de edad, así como el ordenamiento jurídico. Aún más grave, todas las políticas de seguridad y privacidad están definidas en el entendido de que ninguna persona menor utilizará su servicio. Por lo tanto, es sumamente necesario que padres y madres busquen esas condiciones de uso y las lean, para tener seguridad de que sus hijos e hijas utilicen adecuadamente la red social y ser responsables de que se configuren los servicios de seguridad y privacidad adecuadamente, si es que van a permitirles su uso.

doi: http://dx.doi.org/10.15359/ree.23-3.17
URL: http://www.una.ac.cr/educare
CORREO: educare@una.cr

Al respecto Martínez-Villalba (2014, citando a Pérez Luño) señala:

> Paradójicamente, los grandes beneficiarios de la anarquía de Internet no son los cibernautas particulares, sino las grandes multinacionales e, incluso, los aparatos de control social de los gobiernos. Los peligros de una utilización abusiva, incontrolada o criminal de ese espacio, plantean ahora, de forma apremiante, la necesidad de su ordenación jurídica. (p.19)

Las condiciones de uso son tan importantes, por lo cual existen incluso cláusulas donde el público usuario da acceso abiertamente a su información personal, información del dispositivo que utiliza (teléfono celular), los contenidos que accede, información sobre ubicación, libreta de contactos, control sobre la cámara, e incluso algunas redes declaran derecho sobre las fotografías que suba a la red, como en el caso de Snapchat.

En cuanto a las normas de privacidad y seguridad, la mayoría de las redes sociales permiten, de forma predeterminada, que cualquiera pueda ver el perfil y las publicaciones, cualquier persona puede ser buscada y encontrada, cualquier persona que siga a otra puede ver su historia, cualquier persona puede enviarle un mensaje privado y cualquier persona pueda ver la información personal.

Por ello es muy importante conocer las opciones que ofrece cada red social para administrar la privacidad, pero en general la mayoría permite controlar aspectos tales como: quién puede ver sus publicaciones y lista de amigos, quién puede enviarle solicitudes de amistad, quién puede buscarle por correo electrónico, quién puede buscarle por el número de teléfono y que los motores de búsqueda enlacen el perfil. Con las políticas de seguridad podemos controlar: amigos o amigas para contactar en caso de problemas para iniciar sesión, histórico donde se inició sesión y alertas sobre inicios de sesión no reconocidos.

Seguridad y privacidad en Facebook

Para acceder a las opciones de seguridad, privacidad y condiciones de uso, según Facebook (2015), debemos: acceder a configuración en Facebook y posteriormente configurar la privacidad y la seguridad. En este apartado podrá configurar: amigos o amigas para contactar en caso de problemas para iniciar sesión, histórico donde se inició sesión y alertas sobre inicios de sesión no reconocidos.

En privacidad se podrá elegir alguna de las siguientes opciones: quién puede ver los datos (publicaciones y lista de amigos y amigas), quién puede enviarle solicitudes de amistad, quién puede buscarle por correo electrónico, quién puede buscarle por el número de teléfono y que los motores de búsqueda enlacen el perfil.

doi: http://dx.doi.org/10.15359/ree.23-3.17
URL: http://www.una.ac.cr/educare
CORREO: educare@una.cr

Seguridad y privacidad en Instagram

Con la configuración de privacidad, de acuerdo con Instagram (2017), se puede: hacer las publicaciones privadas, definir quién puede buscarle y quién no, definir quiénes pueden ver las historias que se publican, definir quién puede enviarle mensajes privados y bloquear a una persona. Para ello se debe: acceder en el área del perfil, tocar los tres puntos ordenados de manera vertical y desplegar un menú de opciones, donde se debe seleccionar la opción llamada *cuenta privada* y, de esta forma, el perfil quedará privado.

Si lo que se ocupa es bloquear una persona, se debe ir al perfil de la persona que se desea bloquear, tocar los tres puntos y desplegar un menú de opciones, donde se debe seleccionar la opción que dice bloquear.

Seguridad y privacidad en WhatsApp

Según WhatsApp Inc. (2016), permite controlar: quién puede ver su foto de perfil, quién ve la última vez que se conectó o si está en línea, quién puede ver su información, quién puede ver su estado y quién puede ver su ubicación en tiempo real. Para ello debe: desplazarse a la parte superior de la ventana y seleccionar los tres puntos verticales, en la ventana que se despliega debe seleccionar Ajustes, se despliega una ventana en cual deben seleccionar *cuenta* donde se accede a *privacidad* para configurar las opciones que desea.

Seguridad y privacidad en Snapchat

Snap Inc. (2017) menciona que Snapchat ofrece algunos métodos de configuración de privacidad para evitar compartir todo el contenido. Entre ellos están: quién puede contactarle (todas las personas, cualquier persona, mis amigos y amigas, solo personas agregadas), quién puede ver la historia: (todas las personas, cualquier persona, mis amigos y amigas, solo personas agregadas, personalizado con solo los sujetos contactos que especifiquemos) y también existe la opción de bloquear a algún usuario o usuaria que no se quiere en nuestro grupo de amigos o amigas.

Para ello debe entrar en ajustes del perfil y configurar las condiciones de privacidad, según Snap Inc. (2017), primero nos encontraremos en la interfaz principal del sistema: se da un toque a la cara del emoji, para poder ingresar al menú de la aplicación; una vez en el menú principal, se selecciona la configuración, la cual es el ícono del engranaje, en ajustes encontraremos donde configurar la privacidad.

La seguridad en Snapchat "es responsabilidad de todos" (Snap Inc., 2017), en ese sentido, como seguridad esta red social da una serie de lineamientos de comportamiento y sugiere al

doi: http://dx.doi.org/10.15359/ree.23-3.17
URL: http://www.una.ac.cr/educare
CORREO: educare@una.cr

público usuario ir a ajustes de privacidad y configurar a quién se le da acceso a sus historias. Sugiere mantener segura la contraseña, y otras sugerencias; sin embargo, no dan ningún elemento de seguridad.

Esta red social en particular tiene, en sus condiciones de uso, acceso a toda la información e incluso derecho sobre las imágenes que se suben en ella, y es muy popular entre las personas menores de edad, por lo tanto resulta de suma importancia tomar en cuenta una serie de lineamientos para mantenerlas seguras:

1. **Advierta a su hijo o hija sobre qué contenido puede enviar**

A pesar de que su hijo o hija podría pensar que están enviando la **imagen o el vídeo a sus amistades,** hay que recordar que **esta aplicación fue hackeada** en el pasado y que, si ocurre de nuevo, sus imágenes podrían hacerse públicas. Se requiere conversar sobre el tema y aconsejarles que no envíen algo que no quisieran que todo el mundo viera.

2. **Recordarles que las imágenes se pueden guardar**

A pesar de que las imágenes enviadas a los contactos caducan automáticamente después de un período determinado de tiempo, hay varias maneras de evitar esto y es importante informarles que es posible hacer **capturas de pantalla** de las fotos y vídeos que se reciben en el móvil.

3. No permita que personas extrañas contacten [a personas menores de edad]

Después de seguir los pasos anteriores, lo siguiente es asegurarse de que ninguna persona desconocida pueda enviar a su hijo o hija imágenes inapropiadas o contactarles. Para cambiar la configuración y asegurarse de que solo sus amistades pueden enviarles mensajes:

- pulse el **icono de fantasma** en la parte superior de la pantalla para acceder al perfil de su hijo.
- pulse el icono del **engranaje** en la esquina superior derecha y en el menú *ajustes* vaya a "Recibir Snaps de…"
- Seleccione "Mis Amigos" en lugar de "Todo el mundo".

Por último, si alguien ha estado acosando a su hijo puede eliminar y bloquear de la misma sección del menú como el paso anterior. También puede escribir a **safety@snapchat.com.** Si todavía no se siente cómodo o cómoda dejando que personas menores de edad utilicen la aplicación, se puede eliminar la cuenta introduciendo el nombre de usuario o usuaria y la contraseña. (Panda Security, Cómo mantener seguros a tus hijos en Snapchat, 2015, párr. 1-5)

doi: http://dx.doi.org/10.15359/ree.23-3.17
URL: http://www.una.ac.cr/educare
CORREO: educare@una.cr

Conclusiones

Educar a nuestros hijos e hijas, para que puedan protegerse de los peligros en el mundo real, ha sido siempre una preocupación para padres y madres responsables; igualmente debemos educarles para que se puedan proteger en el ciberespacio.

Las redes sociales han difundido males sociales al que las personas menores de edad solo estaban expuestas en cierto momento y lugar, convirtiéndolas en blancos fáciles sin barrera de tiempo ni de espacio, pues están expuestas en todo momento.

Pornografía infantil, acoso y bullying son solo algunos de los peligros sociales que tienen en el ciberespacio, y hacen que los cuidados y protección de nuestras personas menores de edad requieran del conocimiento de estos entornos en que se desenvuelven para poder orientarles en cómo evitar ser víctimas.

Educar en ciberseguridad en el uso de la redes sociales en línea es responsabilidad, en primera instancia, del padre y la madre de familia, por ende, es necesario que se establezca una metodología de enseñanza y aprendizaje bilateral; de manera que el sujeto adulto se autoeduque y actualice constantemente en normas de seguridad y manejo de las redes sociales, con el fin de facilitarles las herramientas necesarias y, a partir de ahí, favorecer espacios de construcción de conocimiento significativo.

El establecimiento de buenas prácticas se puede resumir en: conocer las políticas de uso de las redes sociales a que accedan sus hijos e hijas, investigar y configurar la seguridad y privacidad de la cuenta o perfil y delimitar quiénes pueden acceder a los contenidos y publicaciones que hacen, así como a la información que dejan abierta.

La temática de ciberseguridad, actualmente, en razón del uso de las redes sociales por parte de la niñez y la adolescencia, debe ser un tema de discusión y análisis familiar, mediante el empleo de metodologías prácticas y contextualizadas, innovadoras y significativas, que permitan dar solución a problemáticas relacionadas con los peligros en la red a los que se enfrenta la población de interés.

El monitoreo, el acompañamiento y la supervisión sobre el uso correcto de las redes sociales en línea debe ser constante, en razón de los acelerados cambios tecnológicos que surgen día tras día, con el fin de brindar las recomendaciones preventivas necesarias a nivel familiar.

El desconocimiento sobre el uso correcto de redes sociales y la seguridad informática, lastimosamente, según medios de comunicación como *La Nación, el Diario Mx y el Financiero,* con frecuencia son asociados a delitos, muertes y fraudes, a pesar de que son temáticas que constantemente tienen discusión a nivel local, nacional e internacional.

doi: http://dx.doi.org/10.15359/ree.23-3.17
URL: http://www.una.ac.cr/educare
CORREO: educare@una.cr

Referencias

Alegsa. (2016). *Diccionario de informática y tecnología.* Recuperado de http://www.alegsa.com.ar/Dic/tecnologia.php

Amador, A. (2017). Acceso y uso de las TIC en los hogares costarricenses. En A. Salas y M. Guzmán (Coords.), *Programa sociedad de la información y el conocimiento. Universidad de Costa Rica* (pp. 173-210). San José, Costa Rica: Prosic, UCR. Recuperado de http://www.prosic.ucr.ac.cr/sites/default/files/recursos/informe_2017.pdf

Arab, L. E. y Díaz, A. (2015). Impacto de las redes sociales e internet en la adolescencia: Aspectos positivos y negativos. *Revista Médica Clínica Las Condes, 26*(1), 7-13. doi: https://doi.org/10.1016/j.rmclc.2014.12.001

Associated Press. (12 de julio, 2017). Desmantelan red de pornografía infantil por WhatsApp; caen 2 en México. *El Diario MX*. Recuperado de http://diario.mx/Internacional/2017-07-12_29cde2c2/desmantelan-red-de-pornografia-infantil-por-whatsapp-caen-2-en-mexico/

Carbonell, X. (2014). La adicción a los videojuegos en el DSM-5. *Revista Adicciones, 26*(2), 91-95. doi: https://doi.org/10.20882/adicciones.10

Chacón, K. (4 de setiembre de 2016). Adolescentes cambian dinámica en el uso de la web. Tecnología. *El Financiero*. Recuperado de https://www.elfinancierocr.com/tecnologia/adolescentes-cambian-dinamica-en-el-uso-de-la-web/KDQHCKIHSFERVCHMESV7CWNY4E/story/

Echeburúa, E. y De Corral, P. (2010). Adicción a las nuevas tecnologías y a las redes sociales en jóvenes: Un nuevo reto. *Adicciones, 22*(2), 91-96. doi: https://doi.org/10.20882/adicciones.196

Facebook. (2015). *Condiciones y políticas.* Recuperado de https://www.facebook.com/policies?ref=pf

Fernández-Montalvo, J., Peñalva, A. e Irazabal, I. (2015). Hábitos de uso y conductas de riesgo en internet en la preadolescencia. *Comunicar, 22*(44), 113-120. doi: https://doi.org/10.3916/C44-2015-12

García-Maldonado, G., Joffre-Velázquez, V. M., Martínez-Salazar, G. J. y Llanes-Castillo, A. (2011). Ciberbullying: Forma virtual de intimidación escolar. *Revista Colombiana de Psiquiatría*, *40(1)*, 115-130. doi: https://doi.org/10.1016/S0034-7450(14)60108-6

Herrera, K. (28 de octubre de 2015). Las 5 redes sociales favoritas de los jóvenes ticos. *La Prensa Libre.cr.* Recuperado de http://www.laprensalibre.cr/Noticias/detalle/45125/431/las-5-redes-sociales-favoritas-de-los-jovenes-ticos

doi: http://dx.doi.org/10.15359/ree.23-3.17
URL: http://www.una.ac.cr/educare
CORREO: educare@una.cr

Hütt, H. (2012). Las redes sociales: Una nueva herramienta de difusión. *Reflexiones, 91*(2), 121-128. Recuperado de https://www.redalyc.org/articulo.oa?id=72923962008

Instagram. (2017). *Servicio de ayuda*. Recuperado de https://es-la.facebook.com/help/instagram/478745558852511/?helpref=hc_fnav

Martínez-Villalba, J. (2014). La cuarta ola de derechos humanos: Los derechos digitales. *Revista Latinoamericana de Derechos Humanos*, *25*(1), 15-45. Recuperado de http://www.revistas.una.ac.cr/index.php/derechoshumanos/article/view/6117

McDuffie, E. L. y Piotrowski, V. P. (2014). The future of cybersecurity education. *Computer, 47*(8), 67-69. doi: https://doi.org/10.1109/MC.2014.224

Negredo, L. y Herrero; Ó. (2016). Pornografía infantil en internet. *Papeles del Psicólogo, 37*(3), 217-223. Recuperado de http://www.papelesdelpsicologo.es/pdf/2778.pdf

Panda Security. (2015). *Cómo mantener seguros a tus hijos en Snapchat* [Sitio web]. Recuperado de https://www.pandasecurity.com/spain/mediacenter/consejos/como-mantener-seguros-a-tus-hijos-en-snapchat/

Pérez, R. (2016). Adolescencia, socialización y TIC. En R. Pérez y M. Guzmán (Coords.), *Programa sociedad de la información y el conocimiento Universidad de Costa Rica* (pp. 103-122). San José, Costa Rica: Prosic, UCR. Recuperado de http://www.prosic.ucr.ac.cr/sites/default/files/recursos/informe_2016.pdf

Peyró, B. (2015). [Reseña del libro Conectados por redes sociales: Introducción al análisis de redes sociales y casos prácticos, por M. Del Fresco, P. Marqués y D. S. Paunero (Eds.)]. *REDES- Revista hispana para el análisis de redes sociales, 26*(2), 236-241. doi: https://doi.org/10.5565/rev/redes.548

Recio, P. (14 de marzo, 2017). Colegiales de 7° a 9° son más propensos a sufrir 'ciberbullying'. *La Nación*. Recuperado de https://www.nacion.com/ciencia/salud/colegiales-de-7deg-a-9deg-son-mas-propensos-a-sufrir-ciberbullying/YS6VHAAN7RDQNEVWAANFETHFN4/story/

Rendón-Rojas, M. Á. (2007). Relación de las tecnologías de la información y comunicación con la axiología. *Revista Ciencias de la Información*, *38*(3), 3-12. Recuperado de http://cinfo.idict.cu/index.php/cinfo/article/view/109

Sánchez, M. A., Schmidt, M. A., Zuntini, J. I. y Obiol, L. (2017). La Influencia de las redes sociales virtuales en la difusión de información y conocimiento: Estudio de PyMES. *Revista Ibero-Americana de Estrategia, 16*(4), 69-90. doi: https://doi.org/10.5585/riae.v16i4.2522

Seas, J. (2016). *Didáctica general I*. San José, Costa Rica: EUNED.

doi: http://dx.doi.org/10.15359/ree.23-3.17
URL: http://www.una.ac.cr/educare
CORREO: educare@una.cr

Siles, I. (2012). Establishing the internet in Costa Rica: Co-optation and the closure of technological Controversies. *The Information Society, 28*(1), 13-23. doi: https://doi.org/10.1080/01972243.2012.632257

Snap Inc. (2017). *Condiciones de servicio de Snap Inc.* Recuperado de https://www.snap.com/es/terms/

Solano, J. (11 de abril, 2017). Así fue como un pervertido extorsionó a 4 niñas en Golfito. Crhoy.com. Recuperado de https://www.crhoy.com/nacionales/asi-fue-como-un-pervertido-extorsiono-a-4-ninas-en-golfito/

Vanderhoven, E., Schellens, T. y Valcke, M. (2014). Enseñar a los adolescentes los riesgos de las redes sociales: Una propuesta de intervención en secundaria. *Comunicar,* 22*(43)*, 123-132. doi: https://doi.org/10.3916/C43-2014-12

WhatsApp Inc. (2016). *Información legal de WhatsApp.* Recuperado de www.whatsapp.com/legal/