Transdigital
revista científica

Sociedad de Investigación sobre Estudios Digitales S.C. | ISSN: 2683-328X

Principales riesgos en el uso de tecnologías de la información en adolescentes

Main risks in the use of information technologies in teenagers

Gualberto Aguilar-Torres
Escuela de Ingeniería y Ciencias del Tecnológico de Monterrey, México
gualberto.aguilar@tec.mx
ORCID: 0000-0002-1808-3962

Kevin A. Delgado-Vargas
Centro de Investigación en Computación del Instituto Politécnico Nacional, México
kdelgadov2019@cic.ipn.mx
ORCID: 0000-0002-5053-1796

Alfonso F. De Abiega-L'Eglisse
Escuela Superior de Ingeniería Mecánica y Eléctrica del Instituto Politécnico Nacional, México
adeabiegal1900@alumno.ipn.mx
ORCID: 0009-0006-7287-1966

Lissete López-Hernández
Escuela Superior de Cómputo del Instituto Politécnico Nacional, México
llopezh1600@alumno.ipn.mx
ORCID: 0009-0000-2066-3299

Gina Gallegos-García*
Centro de Investigación en Computación del Instituto Politécnico Nacional, México
ggallegosg@ipn.mx
ORCID: 0000-0002-5212-350X

Autora de conrrespondencia*
Sección: Ensayo científico
Fecha de recepción: 25/05/2023 | Fecha de aceptación: 05/06/2023
Referencia del artículo en estilo APA 7ª. edición:

Aguilar-Torres, G., Delgado-Vargas, K. A., De Abiega-L'Eglisse, A. F., López-Hernández, L. & Gallegos-García, G. (2023). Principales riesgos en el uso de tecnologías de la información en adolescentes. *Transdigital*, *4*(7), 1–14. https://doi.org/10.56162/transdigital218

Transdigital
revista científica

Sociedad de Investigación sobre Estudios Digitales S.C. | ISSN: 2683-328X

Resumen

A principios del año 2020 el mundo se enfrentó a una de las más grandes pandemias en la historia y, con esto, a un cambio en el modo de vida de las personas. Este cambio tuvo como elemento central el uso de las tecnologías de la información. Si bien su uso había evolucionado rápidamente, aún se tenían muchos sectores de la población que no las integraban por completo. Además, con la llegada de la pandemia, el mundo entero tuvo la necesidad de adaptarse a una nueva forma de interactuar, desde la forma de convivir con la familia hasta la forma de impartir y tomar clases, por mencionar algunas actividades. En este sentido, la educación básica fue uno de los sectores más afectados, ya que tuvo que pasar del trabajo presencial a una enseñanza completamente en línea. Sin embargo, gran parte de esta población, integrada por adolescentes, niñas y niños no están familiarizados con los riesgos que conlleva la convivencia diaria con Internet. Esto dejó ver que las instituciones educativas no tuvieron tiempo de educar a sus estudiantes en materia de ciberseguridad. Con base en lo anterior, este artículo muestra algunos de los principales riesgos a los que se enfrentan los adolescentes, derivados principalmente de una cada vez mayor exposición a Internet. Para esto, no se contemplaron medidas mínimas de seguridad y prevención. Finalmente, se presentan algunas estrategias que ayudan a mitigar dichos problemas.

Palabras clave: ataques cibernéticos, cibereducación, ciberseguridad, ciberespacio, tecnologías de información.

Abstract

At the beginning of 2020, the world faced one of the biggest pandemics in history, resulting in a change in people's way of life with the use of information technologies at its center. Although their use had evolved rapidly, there were still many sectors of the population that had not fully integrated them. With the arrival of the pandemic, the entire world had to adapt to a new way of interacting, from the way of living with the family to the way of teaching and taking classes, to name a few activities. Basic education was one of the most affected sectors, as it had to transition from face-to-face work to completely online teaching. However, a large part of this population, made up of adolescents, girls and boys, were not familiar with the risks that daily coexistence with the Internet entailed. This revealed that educational institutions did not have time to educate their students on cybersecurity. This article shows some of the main risks that adolescents face, derived mainly from an increasing exposure to the Internet, and does not contemplate minimum safety and prevention measures. Finally, some strategies are presented that help to mitigate these problems.

Keywords: cyber-attacks, cyber education, cybersecurity, cyberspace, information technologies.

Transdigital
revista científica

Sociedad de Investigación sobre Estudios Digitales S.C. | ISSN: 2683-328X

1. Introducción

La educación es el punto neurálgico del proceso de inserción en la sociedad de las nuevas generaciones. De ahí que el sistema educativo debiera brindar, no solo conocimientos elementales, sino también guiar en el desarrollo de aquellas habilidades que permitían enfrentar la vida tomando en cuenta los retos de cada época (Guiot Limón, 2021).

Desde los años 50's hasta mediados de los años 80's, la era de las computadoras dio inicio con cursos que se enfocaban en generar especialistas de soporte técnico o para resolver problemas aplicados a la ciencia y la economía. Posteriormente, surgieron las computadoras personales y el impacto del cómputo alrededor del mundo fue notable durante el inicio del siglo XXI. Por último, llegó la implementación mundial del Internet y las tecnologías de la información, lo cual trajo de la mano la exposición del usuario ante una ilimitada cantidad de amenazas informáticas (Coello Coello, 2003; Tesouro Cid & Puiggalí Allepuz, 2004).

Para nadie es extraño que el 2020 quedará marcado como el inicio de una nueva etapa en la forma de trabajar y llevar a cabo ciertos procesos. El sector educativo quedará como uno de los más afectados. Principalmente, porque muy poco trabajo se está realizando desde las instituciones educativas para enfrentar los retos que conlleva una mayor exposición a Internet de las niñas, niños y adolescentes (Alqahtani, 2017; Alqahtani et al., 2017; Ibarrola, 2005). De ahí que es fundamental y urgente que los colegios educativos contemplen a la ciberseguridad como una materia básica en sus programas educativos. Si bien los adultos también pueden ser víctimas de algún delito en Internet, los menores de edad tienen una mayor probabilidad ya que los delincuentes siempre buscarán aprovechar su inocencia.

El artículo está organizado de la siguiente forma: la sección *2. Riesgos en Internet* presenta una revisión de los principales riesgos que los adolescentes tienen por un mayor tiempo y uso de dispositivos conectados a Internet. En la sección *3. Estrategias básicas de seguridad* se presentan estrategias que usuarios menores de edad deben considerar al navegar en Internet; además se enfatiza la importancia de que el usuario sea educado en materia de ciberseguridad para comprender por qué son importantes las medidas de seguridad y en qué momento implementarlas. Por último, se presenta la sección *4. Conclusiones*.

2. Hábitos y riesgos en Internet

De acuerdo con la Asociación de Internet Mx, en su *17° Estudio sobre los Hábitos de los Usuarios de Internet en México 2021* (Asociación de Internet, 2021), México alcanzó 84.1 millones de internautas en 2020, de los cuales una cuarta parte, es decir, alrededor de 21 millones de internautas, son menores de edad.

Transdigital
revista científica

Sociedad de Investigación sobre Estudios Digitales S.C. | ISSN: 2683-328X

Previo a la pandemia, el internauta mexicano pasaba conectado a Internet diariamente nueve horas en promedio. Sin embargo, es un hecho que este tiempo ha sido superado, e incluso algunos países han reportado hasta 12 horas de conexión a Internet en los menores de edad (Sardianos et al., 2018).

Son muchas las razones de este incremento, por ejemplo, cada vez es más común que las escuelas utilicen plataformas digitales para diferentes cursos; es cada vez más frecuente ver que tareas, ejercicios, prácticas o exámenes, se realizan mediante una plataforma digital. Sin duda, esto ha ocasionado que los adolescentes, a una edad cada vez menor, tengan la necesidad de contar con un dispositivo portátil. Las redes sociales también han sido una de las razones de este incremento de tiempo, ya que 7 de cada 10 internautas dedican el 40% de su tiempo conectados a Internet, en alguna red social como *Facebook* y *WhatsApp* (redes sociales preferidas en México). Lo anterior deja ver que el uso de las tecnologías va en aumento, pero no sucede lo mismo con la educación y la formación. Es decir, no se impacta en la enseñanza de las responsabilidades que trae este uso cada vez mayor (Yellowlees & Marks, 2007; Joshi & Rose, 2018). Por eso, es importante identificar los principales riesgos y delitos en Internet (Valencia Ortiz & Castaño Garrido, 2019).

Existen distintos tipos de contenidos que son clasificados como contenido ilícito, nocivo o falso. La noción de saber con qué tipo de contenido se expone a un niño, niña o adolescente muchas veces no es uniforme, puesto que varía dependiendo de los conceptos éticos y jurídicos que tiene cada territorio o bien cada persona (Kahimise & Shava, 2019). Es muy común encontrar material en Internet que puede constituir una ofensa a los valores o sentimientos de algunas personas, donde se pueden expresar opiniones políticas, creencias religiosas o algunas opiniones sobre cuestiones raciales. En este sentido, algunas de las consecuencias de la exposición de este tipo de contenido en adolescentes, van desde daños emocionales y psicológicos, hasta la posibilidad de convertirse en víctimas de algún delito como los que se mencionan a continuación (Binti Mt Tahir & Bin Husin, 2017; Kohli et al, 2015).

2.1 *Cyberbullying*

Este tipo de actividades que puede ser calificado como delito; hace referencia al uso de medios digitales con la intención de acosar psicológicamente a terceras personas. Esta actividad se presenta en niños, adolescentes y jóvenes principalmente. A veces, incluso el agresor como la víctima tienen la misma edad y comparten contextos sociales (Olweus, 2012). Algunos de los métodos que se utilizan para realizar esta actividad son:

- *Creación de perfiles falsos en redes sociales*: Estos perfiles falsos se utilizan, principalmente, para ridiculizar, acosar o confesar experiencias verdaderas o falsas de la víctima.
- *Robo de la contraseña del correo de la víctima*: Este tipo de actividad se utiliza para violar la intimidad de la víctima, utilizando su identidad para suplantarlo digitalmente, o utilizar información confidencial.

Transdigital
revista científica

Sociedad de Investigación sobre Estudios Digitales S.C. | ISSN: 2683-328X

- *Propagación de rumores en foros o redes sociales*: Con estas acciones se provoca que la víctima reaccione de forma violenta para denunciar ante responsables de una red social y en distintos casos generar que cierren la cuenta de la víctima.
- *Envío de mensajes amenazantes*: En estos mensajes se aprovecha el anonimato para acosar a las víctimas.
- *Publicación de fotos reales o fotomontajes*: Esta acción normalmente tiene el propósito de avergonzar públicamente a la víctima

Adicional a lo anterior, es importante mencionar que las víctimas de *cyberbullying* tienen una mayor probabilidad de caer en el consumo de drogas, abandonar la escuela, sufrir *bullying* en persona, y tener más problemas de salud que las personas que nunca han sido objetivo de estas prácticas delictivas. Los sobrevivientes de tal agresión en ocasiones se suicidan (Keeley & Little, 2017).

2.2 *Grooming*

Esta acción consiste en la interacción de un adulto con un niño, niña o adolescente. Dicha interacción busca ganarse la confianza de las víctimas para luego involucrarlos en alguna actividad sexual. En este tipo de prácticas se tienen distintos niveles de interacción, que van desde el *sexting* hasta llegar a mantener encuentros sexuales. El *grooming* incluye una serie de fases, donde se encuentran distintos patrones de conducta con los cuales es posible detectar estas prácticas (Bours & Kulsrud, 2019; Craven et al., 2007):

- *Creación de un vínculo de confianza*: Normalmente el agresor establece el vínculo de confianza mediante diferentes técnicas, como fingir una edad diferente, semejante a la víctima, adaptar el lenguaje de la víctima e insistir en mantener su *relación* en secreto.
- *Aislamiento de la víctima*: En esta fase el agresor intenta separar al menor de su familia, amigos y maestros. De esta manera deja desprotegido al menor.
- *Valoración de los riesgos*: En esta fase el agresor asegura su posición averiguando, mediante distintas preguntas que le realiza a la víctima. El objetivo es saber, principalmente, si alguna otra persona tiene acceso al dispositivo que utiliza el menor; busca mantener todo en secreto.
- *Conversaciones sobre sexo*: Una vez que se generó la confianza, el abusador introduce pláticas sexuales de manera paulatina, generando que la víctima se familiarice con la temática, llegando a lo que se le llama *Sexteo*.
- *Peticiones de naturaleza sexual*: Esta fase consiste en utilizar la manipulación, amenazas o chantajes para que la víctima le envíe material sexual, fantasías sexuales o bien hacer que la relación culmine en un encuentro sexual.

Transdigital
revista científica

Sociedad de Investigación sobre Estudios Digitales S.C. | ISSN: 2683-328X

2.3 *Sexting*

Se denomina *sexting* al envío de fotografías o videos con contenido sexual a través de dispositivos electrónicos. Se origina porque el usuario confía plenamente en la discreción. Dado que la víctima desconoce las consecuencias, se deja influenciar por los medios y confía en aplicaciones que garantizan la seguridad de las imágenes enviadas. Todo puede iniciar con el noviazgo, un coqueteo o el lucimiento (Barrense-Dias et al., 2017).

Algunos motivos identificados por los que los adolescentes realizan esta práctica son:

- *Presión social*: Se presenta con las ganas de encajar en un entorno cada vez más sexualizado y llamar la atención del grupo donde se desenvuelve.
- *Confianza con el receptor*: Normalmente se presenta entre parejas donde consideran que la unión será para toda la vida.
- *Desconocimiento técnico*: Se piensa que no hay manera de reproducir el contenido en otros medios. Es decir, no se considera el peligro de robo o pérdida del teléfono del receptor.
- *Incapacidad para percibir el riesgo*: No se consideran las consecuencias futuras que se pueden tener en la vida, lo que puede dar pie a la extorsión, que en este tenor recibe el nombre de *sextorsión*.

Con el propósito de identificar de manera más clara este tipo de acciones, a continuación, se presenta una clasificación de los tipos de *sexting* (Wachs, 2021):

- *Consensuado*: cuando se realiza voluntariamente, sin la ausencia de presión o chantaje y los mensajes no son reenviados sin el consentimiento de la persona que los envía.
- *Agravado*: involucra la presencia de intenciones perjudiciales hacia quien envía los mensajes sugerentes, ya sea obligada o voluntariamente. Dentro del *sexteo* agravado se consideran dos subtipos:
- *No consensuado*: se da cuando los mensajes sugerentes son compartidos sin autorización.
- *Bajo presión*: cuando un individuo es presionado para enviar mensajes sugerentes.

Los efectos de estas acciones en la salud psicosocial de la víctima dependen del tipo de *sexting* llevado a cabo. El consensuado no genera consecuencias negativas; contrario al sexting bajo presión, que tiende a causar sentimientos de culpa, humillación y vergüenza. Adolescentes entre 12 y 17 años de edad, a los que se les ha solicitado enviar mensajes sugerentes, tienen una alta probabilidad de reportar síntomas de depresión, ansiedad, impulsividad, hostilidad, desregulación emocional, y temperamento agresivo (Lu et al., 2021).

Transdigital
revista científica

Sociedad de Investigación sobre Estudios Digitales S.C. | ISSN: 2683-328X

2.4 *Sextorsión*

Esta acción muchas veces es consecuencia de las actividades de sexting. Siempre que una persona comparte material de índole sexual, corre el riesgo de ser víctima de amenazas o chantajes, para obtener algún tipo de beneficio. Estos pueden ser económicos o para la obtención de material de las mismas características. Esta práctica no respeta edad, ya que puede dirigerse a menores de edad o incluso a adultos. No distingue género, ya que las imágenes son obtenidas sin conocimiento de la víctima. Se pueden obtener mediante cámaras *web*, correo electrónico, mensajería instantánea o bien pueden ser extraídas desde el teléfono móvil de la víctima, a través de las imágenes provenientes de una relación sentimental.

En resumen, esta práctica se presenta con objeto de un abuso sexual, explotación pornográfica para uso privado o comercial, o una extorsión económica. Puede realizarse por conocidos, ex-amantes, o bien personas desconocidas por la víctima, llegando hasta consecuencias de tipo explotación sexual más graves (Andrade Ureña & Guevara Yáñez, 2019).

2.5 Retos virales

Además de los riesgos que se han mencionado hasta este momento, existen una serie de acciones que se han incrementado en los últimos años: los llamados retos virales. Éstos normalmente consisten en realizar alguna acción frente a la cámara digital para nominar a otras personas, amigos, conocidos o familiares, a través de redes sociales, para que también realicen el reto (Juárez, 2019). Por ejemplo, en 2017 se viralizó por Internet el reto de *La ballena azul*, que consistía en que sus participantes adolescentes realizaran la actividad que se les asignaba cada día; iniciaban con tareas inofensivas hasta llegar al suicidio. La víctima era amenazada si se reusaba a cumplir. Sorpresivamente, el reto está relacionado con cientos de muertes (BBC News Mundo, 2019).

Algunos de los retos son inofensivos como *El baño con la cubeta de hielos*, que fue parte de una campaña publicitaria solidaria con enfermos de esclerosis lateral amiotrófica. Otros, como *La ballena azul*, están elaborados para hacer daño físico o mental a quien lo juegue, lo que puede afectar de manera negativa a la niñez y adolescencia; inclusive puede hacerlos atentar contra su propia vida. Dentro de esta última categoría también existen otros retos, como *Momo*, el reto del *Clonazepam*, o el reto de desaparecer durante 48 horas y reaparecer cuando que se haya difundido una ficha de búsqueda. Todos estos retos se difunden mediante redes sociales y así logran tener un impacto significativo en el número de afectados (BBC News Mundo, 2018; Milenio Digital, 2022; Yedra, 2023).

Transdigital
revista científica

Sociedad de Investigación sobre Estudios Digitales S.C. | ISSN: 2683-328X

3. Estrategias básicas de seguridad

Como se mencionó anteriormente, en México, al igual que en muchos otros países, las instituciones educativas han tenido que usar diferentes plataformas digitales para llevar a cabo su labor cotidiana. Por lo tanto, es muy importante que, con este crecimiento de dispositivos conectados a Internet, también se pueda contar con una cultura de ciberseguridad que sea inherente a la educación desde temprana edad, ya que la mayoría de los adolescentes desconocen los peligros de estar conectados.

Es importante tener consciencia de que, en ocasiones, las interacciones en Internet pueden poner en riesgo todo el entorno. Por ejemplo, hoy en día la gente se puede hacer pasar por alguien más, las fotos o los audios recibidos podrían ser de otras personas que previamente ya fueron víctimas del mismo o de otro agresor, y cada una de las fotos que se comparten en Internet tienen la posibilidad de que ya no se podrán borrar por completo.

Es necesario que en los programas de educación básica se integren materias relacionadas con la ciberseguridad para adquirir paulatinamente una cultura de prevención desde temprana edad, minimizando riesgos y conociendo las buenas prácticas que deben implementarse al navegar por Internet (Demirol et al., 2017; Fauzi & Bours, 2020; Garriga Domínguez, 2016; Martínez-de-Morentin et al., 2021; Matković et al., 2021; Naylor et al., 2014; Shalini & Shankaraiah, 2019). Con base en lo anterior, algunas de las estrategias básicas que se deben tener en cuenta son las siguientes:

- *Concientización en ciberseguridad*: Esta estrategia es crucial en menores de edad y extremadamente útil durante la adolescencia. Consiste en informar sobre los riesgos y buenas prácticas de ciberseguridad que los ayudará a regular su comportamiento en línea y de esta forma disminuir su exposición al riesgo.
- *Instalación de antivirus para proteger los dispositivos conectados a Internet*: Una medida básica de seguridad son los antivirus, que se encargan de buscar en los archivos de las computadoras o teléfonos celulares software malicioso. En caso de hallarlo, lo eliminan.
- *Generación de contraseñas que incluyan números, letras y símbolos.* Es muy común el uso de contraseñas como técnica para mantener la confidencialidad en las herramientas o dispositivos utilizados. Sin embargo, hoy en día con el incremento de dispositivos y herramientas, sería muy complicado tener contraseñas distintas para cada caso. Esta es la razón por la cual muchas personas generan sus contraseñas con información personal, lo que las convierte automáticamente en un blanco fácil para el robo de contraseñas. Por lo tanto, las mejores prácticas para generar tu contraseña es que incluyan letras mayúsculas, minúsculas, números y algún símbolo o carácter especial.
- *Almacenamiento de la información en lugares seguros.* Se debe procurar no subir documentación personal a la nube (*Dropbox*, *iClould*, *Google Drive*, etc.), como copias de credencial de elector, acta de nacimiento, comprobantes de domicilio, etc. Al momento de compartir esa información, se abre un

Transdigital
revista científica

Sociedad de Investigación sobre Estudios Digitales S.C. | ISSN: 2683-328X

flanco de vulnerabilidad. Si realmente existe la necesidad de realizar esta actividad, la recomendación es cifrar la información antes de subirla.

- *Revisar y analizar la información recibida.* Descargar o abrir archivos de remitentes desconocidos puede ocasionar la instalación de uno o varios virus. Por esta razón, es importante analizar la información recibida y, en la medida de lo posible, no abrir información de emisores desconocidos.
- *Navegar en sitios seguros.* Se debe evitar la navegación en sitios que no cuenten con conexiones "https" para realizar operaciones financieras, bajar información y comprar productos, por citar algunos. Sin embargo, aunque los sitios que se visitan actualmente cuenten con el acrónimo "https", esto no significa que son 100% seguros.
- *Cifrar información.* Una de las técnicas más seguras, hoy en día, para la confidencialidad de la información es el cifrado. Esto garantiza que la información transmitida sea vista por las personas correctas, es decir, solamente emisor y receptor podrán transformar y hacer ilegible dicha información. También es posible utilizar estas técnicas para almacenar información de manera segura.
- *Actualiza el navegador*. Es muy importante, además de contar con antivirus, actualizar de manera constante los navegadores del equipo, así como los respectivos parches de seguridad.
- *Descargar aplicaciones en sitios oficiales*. Además de todo lo mencionado hasta el momento, la descarga de aplicaciones en sitios no oficiales puede ocasionar que estas descargas contengan software malicioso y, con esto, la instalación de algún *malware* que pueda robar información o, peor aún, que ocasione que el equipo pueda ser manipulado de forma remota.
- *Doble factor de autenticación.* En la medida de lo posible, y siempre que el sistema o las aplicaciones lo permitan, se debe ocupar el doble factor de autenticación. Esto se basa en validar la identidad de un usuario mediante una segunda capa de protección a la contraseña original.

Es necesario, en la medida de lo posible, implementar buenas prácticas al navegar por Internet para evitar riesgos. Sin embargo, hacerlo requiere comprensión por parte del usuario, tanto de las posibles amenazas como de las medidas de seguridad que debe tomar. Es por ello que la educación y concientización en ciberseguridad son necesarias desde la educación temprana.

Es importante destacar que, no por contar con un antivirus, el usuario puede dejar de lado las buenas prácticas, ya que factores como la complejidad o el surgimiento de nuevas amenazas cada día, algunas de ellas llamadas de día cero, provocan que ningún sistema sea completamente seguro. A pesar de esto, se recomienda tener instalado siempre un antivirus, y mantenerlo actualizado, pues solamente así se puede asegurar que el software cuente con la información más reciente sobre las nuevas amenazas, además de tener la versión con menos vulnerabilidades.

Hablando en términos de las contraseñas, si bien existen muchas recomendaciones para crearlas de manera segura, como son cambiarlas periódicamente, usar números, letras y símbolos especiales, que su longitud

Transdigital
revista científica

Sociedad de Investigación sobre Estudios Digitales S.C. | ISSN: 2683-328X

sea larga, debe ser restrictivo usar información personal en ellas. También, es primordial que sean difícil de adivinar, lo que implica que el uso de palabras existentes en un diccionario no es opción. Si se quiere aumentar la seguridad en ese sentido, recibir mensajes de correo electrónico, mensajes SMS, o el uso de *tokens* al momento, después de haber ingresado la contraseña de la cuenta a la que se desea acceder, es conocido como *doble factor de autenticación*. El beneficio que otorga es que, si los atacantes obtienen la contraseña del usuario, no podrán acceder a la cuenta, a menos que cuenten con el segundo método de autenticación.

Por otro lado, en cuanto al almacenamiento de la información, cabe destacar que los servicios en la nube cuentan con sus propios mecanismos de seguridad. Sin embargo, en cuestiones de ciberseguridad, el usuario siempre debe considerar el peor caso, como un ciberataque a las compañías que proporcionan los servicios o que el atacante obtenga las credenciales de la cuenta en *la nube* del usuario. En ambos casos, los datos sensibles del usuario (en caso de haberlos), serán expuestos. En la medida de lo posible se debe tratar de almacenar la información cifrada. Es destacable recordar que el cifrado de la información consiste en transformar la información y protegerla bajo un elemento secreto mejor conocido como llave de cifrado. De tal forma que solamente los usuarios que cuenten con dicho elemento podrán eliminar la transformación previamente hecha a la información.

En cuanto a la comunicación, además de verificar el certificado de seguridad con el que cuentan las páginas *web*, es posible recurrir al uso de servicios como *Norton Safe Web* y *Google Safe Browsing*, que analizan la reputación de los sitios web para indicar si son peligrosos o no, así como bloquear las conexiones en caso de ser de alto riesgo (Google, s.f.; Norton, 2021) (de hecho, no todos los *emails*, archivos, programas o recursos digitales existentes en Internet son legítimos; algunos han sido alterados con el objetivo de distribuir *software* malicioso. Para ello, se debe buscar directamente en sitios de páginas oficiales, frecuentemente con extensiones como: *.org*, *.com*, *.gob*, donde los nombres de dominio corresponden al nombre de la compañía o propietario de dicho *software*.

Posteriormente, se debe verificar que la información descargada se mantuvo de manera integra. Para tal fin se puede recurrir a las funciones *hash*, las cuales son mapeos informáticos que generan cadenas de caracteres únicas, como una huella dactilar. De ahí que, si se compara la cadena *hash* de un archivo legitimo con la del mismo archivo modificado, se observará que ambas cadenas son diferentes, lo que indica que el archivo ha sido alterado; en caso de que no encontrar ninguna diferencia entre las cadenas, el archivo es legítimo. Los valores *hash* pueden generarse por aplicaciones, o mediante consolas de los sistemas operativos de las computadoras.

En las redes sociales no se debe compartir datos personales, se debe pensar antes de publicar, utilizar contraseñas fuertes, elegir un sobrenombre o apodo (nickname) en lugar de mostrar tu nombre real, restringir el acceso a los perfiles y, de ser posible, monitorear la actividad de menores de edad. Todo esto define una estrategia a seguir cuando se usan las redes sociales. La configuración de privacidad depende del usuario, así como la responsabilidad de su interacción en la red social. En este último punto recae la decisión sobre qué usuarios aceptar

Transdigital
revista científica

Sociedad de Investigación sobre Estudios Digitales S.C. | ISSN: 2683-328X

como amigos, ya que generalmente son ellos los que tienen más facilidad de acceso a la información en los perfiles de los usuarios.

Las actualizaciones en el software poseen parches de seguridad creados como defensa de las nuevas vulnerabilidades encontradas y de las amenazas recientemente descubiertas. No se debe olvidar que muchos de los ciberataques que han tenido éxito recientemente se deben a la falta de actualización en el software del equipo.

4. Conclusiones

Hoy en día, la sociedad tiene una fuerte dependencia a la interacción con las redes sociales. Con el trabajo virtual, la interacción personal se ha ido alejando más y más. Esto ha marcado una brecha de seguridad que los atacantes aprovechan y seguirán aprovechando para conseguir su objetivo. Un ejemplo muy claro es el delito de pornografía infantil. Desafortunadamente, México ha ocupado en los últimos años los primeros lugares en la difusión de pornografía infantil y, sin lugar a duda, muchas de las actividades mencionadas en este artículo con anterioridad han colaborado para tener este lamentable lugar. Es fundamental darles la importancia necesaria a todas las actividades que han coadyuvado para llegar a estos problemas.

Muchas de las acciones revisadas en este artículo han crecido de forma exponencial por el simple hecho de que no se ha logrado generar una guía responsable para navegar en Internet. Esto no significa que se desconozca cómo tomar una foto con los dispositivos móviles, cómo responder un mensaje o realizar llamadas. Más bien se refiere al enfoque de que cada dispositivo se puede convertir en una copia fiel de la vida diaria, de los gustos, vivencias o incluso de la estabilidad económica, misma que por mucho tiempo se justifica diciendo “A mí no me va a pasar”.

Desafortunadamente, son muchos los riesgos en Internet, así como las formas en que se podrían presentar. Por esta razón, es fundamental que existan mayores esfuerzos y técnicas para prevenir los riesgos a los que se expone un menor de edad en Internet. El objetivo es que estos usuarios puedan disfrutar de un Internet seguro. No olvidemos que una parte muy importante para la protección en menores de edad, también se encuentra en manos de los padres. Su tarea es muy importante para lograr que los menores de edad utilicen las tecnologías de una forma consciente, responsable y segura.

Transdigital
revista científica

Sociedad de Investigación sobre Estudios Digitales S.C. | ISSN: 2683-328X

Referencias

Alqahtani, N. (2017). A state-of-the-art review of Internet risks on children. *2017 2nd International Conference on Anti-Cyber Crimes* (ICACC), 108-112. https://doi.org/10.1109/Anti-Cybercrime.2017.7905273

Alqahtani, N., Furnell, S., Atkinson, S. & Stengel, I. (2017). Internet risks for children: Parents' perceptions and attitudes: An investigative study of the Saudi Context. *2017 Internet Technologies and Applications* (ITA), 98-103. https://doi.org/10.1109/ITECHA.2017.8101918

Andrade Ureña, R. F. & Guevara Yánez, R. E. (2019). *El acto de sextorsión y su necesaria tipificación en el código orgánico integral penal ecuatoriano*. Proyecto de Investigación de Abogado(a) de los Tribunales de la República [Tesis de licenciatura de Universidad Regional Autónoma de los Andes "Uniandes"]. https://dspace.uniandes.edu.ec/bitstream/123456789/10098/1/PIUSDAB049-2019.pdf

Asociación de Internet. (2021). *17º Estudio de Hábitos de Internet en México*. https://www.asociaciondeinternet.mx/estudios/habitos-de-internet

Barrense-Dias, Y., Berchtold, A., Surís, J. C. & Akre, C. (2017). Sexting and the definition issue. *Journal of Adolescent Health*, (61), 544-554. https://doi.org/10.1016/j.jadohealth.2017.05.009

BBC News Mundo. (2018, 25 julio). Qué es «Momo», el juego viral por WhatsApp que preocupa a autoridades en América Latina. *BBC News Mundo*. https://www.bbc.com/mundo/noticias-44952770

BBC News Mundo. (2019, 27 enero). La verdadera historia del reto suicida de la «Ballena Azul» que se hizo viral en internet. *BBC News Mundo*. https://www.bbc.com/mundo/noticias-46974250

Binti Mt Tahir, T. & Bin Husin, M. H. (2017). Online social media and risks: An exploration into existing children practice. *2017 International Conference on Electrical Engineering and Informatics* (ICELTICs), 195-200. https://doi.org/10.1109/ICELTICS.2017.8253250

Borj, P. R. & Bours, P. (2019). Predatory Conversation Detection. *2019 International Conference on Cyber Security for Emerging Technologies* (CSET), Doha, Qatar, 1-6. https://doi.org/10.1109/CSET.2019.8904885

Bours, P., & Kulsrud, H. (2019). Detection of Cyber Grooming in Online Conversation. *2019 IEEE International Workshop on Information Forensics and Security* (WIFS), 1-6. https://doi.org/10.1109/WIFS47025.2019.9035090

Craven, S., Brown, S., & Gilchrist, E. (2007). Sexual grooming of children: Review of literature and theoretical considerations. *Journal of Sexual Aggression*, *12*(3), 287-299. https://doi.org/10.1080/13552600601069414

Coello Coello, C. A. (2003). *Breve Historia de la Computación y sus Pioneros*. Fondo de Cultura Económica.

Demirol, D., Tuna, G., & Das, R. (2017). A simple logging system for safe internet use. *2017 International Artificial Intelligence and Data Processing Symposium* (IDAP), 1-5. https://doi.org/10.1109/IDAP.2017.8090252

Transdigital
revista científica

Sociedad de Investigación sobre Estudios Digitales S.C. | ISSN: 2683-328X

Milenio Digital. (2022, 11 noviembre). ¿De qué trata el reto viral con clonazepam? Estos son los riesgos y casos en México. *Grupo Milenio*. https://www.milenio.com/virales/el-reto-del-clonazepam-que-esta-alertando-a-los-padres.

Fauzi, M. A., & Bours, P. (2020). Ensemble Method for Sexual Predators Identification in Online Chats. *2020 8th International Workshop on Biometrics and Forensics* (IWBF), 1-6. https://doi.org/10.1109/IWBF49977.2020.9107945

Garriga Domínguez, A. (2016). *Nuevos retos para la protección de datos personales. En la Era del Big Data y de la computación ubicua*. Dykinson.

Guiot Limón, I. (2021). Uso de las TICS en la educación superior durante la Pandemia COVID-19: Ventajas y desventajas. *Interconectando Saberes*, *6*(12), 223–227. https://doi.org/10.25009/is.v0i12.2724

Google. (s. f.). *Google Safe Browsing*. https://safebrowsing.google.com/

Ibarrola, M. (2005). Educación y trabajo. *Revista Mexicana de Investigación Educativa*, *10*(25), 303-313. https://comie.org.mx/revista/v2018/rmie/index.php/nrmie/article/view/767/767

Joshi, S. C., & Rose, G. (2018). Information Technology, Internet Use, and Adolescent Cognitive Development. *2018 3rd International Conference on Computational Systems and Information Technology for Sustainable Solutions* (CSITSS), 22-28. https://doi.org/10.1109/CSITSS.2018.8768780

Juárez, M. B., (2019). La necesidad de clasificar los retos virales para establecer un sistema de prevención eficaz. En A. M. de Vicente Domínguez & J. Sierra Sánchez (Eds.), *Aproximación periodística y educomunicativa al fenómeno de las redes sociales* (pp. 907-920). Mc. Graw Hill.

Kahimise, J., & Shava, F. B. (2019). An analysis of children's online activities and behaviors that expose them to cybercrimes. *2019 27th Telecommunications Forum* (TELFOR), 1-4. https://doi.org/10.1109/TELFOR48224.2019.8971089

Keeley, B., & Little, C. (2017). *The State of the Worlds Children 2017: Children in a Digital World*. UNICEF. https://files.eric.ed.gov/fulltext/ED590013.pdf

Kohli, V., Saxena, S., & Patni, J. (2015). A SURVEY- Academic demolition via internet addiction. *2015 2nd International Conference on Computing for Sustainable Global Development* (INDIACom), 1769-1774.

Lu, Y., Baumler, E., & Temple, J. R. (2021). Multiple Forms of Sexting and Associations with Psychosocial Health in Early Adolescents. *International Journal of Environmental Research and Public Health*, *18*(5), 2760. https://doi.org/10.3390/ijerph18052760

Martínez-de-Morentin, J. I., Lareki, A., & Altuna, J. (2021). Risks Associated with Posting Content on the Social Media. *IEEE Revista Iberoamericana de Tecnologías del Aprendizaje*, *16*(1), 77-83. https://doi.org/10.1109/RITA.2021.3052655

Matković, R., Vejmelka, L., & Ključević, Ž. (2021). Use of security settings on social networks of elementary and high school students in the Split-Dalmatia County. *2020 43rd International Convention on Information, Communication and Electronic Technology* (MIPRO), 1476-1481. https://doi.org/10.23919/MIPRO48935.2020.9245249

Transdigital
revista científica

Sociedad de Investigación sobre Estudios Digitales S.C. | ISSN: 2683-328X

Naylor, D., Finamore, A., Leontiadis, I., Grunenberger, Y., Mellia, M., Munafò M., & Steenkiste, P. (2014). The cost of the "s" in https. *Proceedings of the 10th ACM International on Conference on emerging Networking Experiments and Technologie*, 133-140. https://doi.org/10.1145/2674005.2674991

Norton. (2021). How to know if a website is safe: 10 steps to verify secure sites. *Norton*. https://us.norton.com/blog/how-to/how-to-know-if-a-website-is-safe#safe

Olweus, D. (2012). Cyberbullying: An overrated phenomenon. *European Journal of Developmental Psychology*, *9*(5), 520-538. https://doi.org/10.1080/17405629.2012.682358

Sardianos, C., Varlamis, I., & Bouras, G. (2018). Extracting User Habits from Google Maps History Logs. *2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining* (ASONAM), 690-697. https://doi.org/10.1109/ASONAM.2018.8508442

Shalini, P., & Shankaraiah (2019). A Novel Technique to regulate access to immoral content for Minors. *2019 7th International Conference on Smart Computing & Communications* (ICSCC), 1-5. https://doi.org/10.1109/ICSCC.2019.8843593

Tesouro Cid, M., & Puiggalí Allepuz, J. (2004). Evolución y utilización de internet en la educación. *Pixel-Bit. Revista de Medios y Educación*, 24, 59-67. https://recyt.fecyt.es/index.php/pixel/article/view/61231

Valencia Ortiz, R & Castaño Garrido, C. M. (2019). Use and abuse of social media by adolescents: a study in Mexico. *Pixel-Bit*. *Revista de Medios y Educación*, (54), 7-28. https://doi.org/10.12795/pixelbit.2019.i54.01

Wachs, S. (2021) How Are Consensual, Non-Consensual, and Pressured Sexting Linked to Depression and Self-Harm? The Moderating Effects of Demographic Variables. *International Journal of Environmental Research and Public Health*, *18*(5) 2597. https://doi.org/10.3390/ijerph18052597

Yedra, S. (2023, 1 abril). En Guanajuato, alertan autoridades por reto viral de TikTok para "desaparecer por 48 horas". *Microsoft Start*. https://www.msn.com/es-mx/noticias/other/en-guanajuato-alertan-autoridades-por-reto-viral-de-tiktok-para-desaparecer-por-48-horas/ar-AA19mvtt

Yellowlees, P. M., & Marks, S. (2007). Problematic Internet use or Internet addiction? *Computers in Human Behavior*, *23*(3), 1447-1453. https://doi.org/10.1016/j.chb.2005.05.004