TÉCNICAS DE INGENIERÍA SOCIAL EMPLEADAS EN COLOMBIA POR LOS CIBERDELINCUENTES A MENORES DE EDAD

LEIDY TATIANA SOLER PÁEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2021

TÉCNICAS DE INGENIERÍA SOCIAL EMPLEADAS EN COLOMBIA POR LOS CIBERDELINCUENTES A MENORES DE EDAD

LEIDY TATIANA SOLER PÁEZ

Proyecto de Grado – Monografía presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Director:
MSC. KATERINE MÁRCELES VILLALBA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2021

NOTA DE ACEPTACIÓN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

DEDICATORIA

Principalmente dedico este trabajo a Dios ya que sin su voluntad y misericordia no hubiese sido posible alcanzar este logro.

A mi hijo y esposo por su comprensión y aliento en todo momento para lograr este objetivo propuesto, también lo dedico a mis padres que gracias a su apoyo y moral me animaron para continuar avanzando hasta el final de este logro.

AGRADECIMIENTOS

Agradezco a las directivas de la Universidad Nacional Abierta y a Distancia UNAD, quienes con su trabajo continuo nos brindan la oportunidad de estudiar y laborar, por otro lado, a cada uno de los tutores y asesores que me acompañaron en el proceso les reconozco que sin su apoyo y colaboración éste logro no hubiera sido posible.

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

AMENAZA: Evento que produce indisponibilidad o mal funcionamiento sobre un activo se genera de forma intencional o accidental.

CIBERACOSO: Es el uso de recursos digitales para fomentar el acoso a un grupo de personas o a una persona puntual.

CIBERCRIMEN: Acto criminal llevado a cabo por internet valiéndose de herramientas tecnológicas, tiene como finalidad conseguir beneficios económicos.

CIBERDELINCUENTE: Individuo que hace uso de internet para cometer actos criminales.

DELITO INFORMÁTICO: Acto criminal realizado a través de herramientas tecnológicas como el internet.

DOXING: Técnica empleada por los ciberdelincuentes para recopilar datos de una persona valiéndose de la información publicada en la red, generalmente con el objetivo de hacer una extorsión.

FUGA DE DATOS: Es la perdida de información sensible puede ser de forma accidental o intencional.

GROOMING: Técnica usada con el fin de engañar a un menor, logrando ganar su confianza y así establecer una amistad, por medio de la cual el delincuente generalmente un adulto consigue material sensible del menor como fotos en ropa interior o de sus genitales, para luego extorsionarlo.

INGENIERÍA SOCIAL: Grupo de técnicas empleadas para engañar o manipular una víctima haciendo que éste suministre información personal involuntariamente poniéndose en peligro.

RESUMEN

Este proyecto de investigación se centra en el análisis de las principales técnicas de ataque de ingeniería social usadas en la población de jóvenes colombianos, para lo cual se recopiló en específico, información de los diferentes métodos de ataque usados en menores de edad. Para abordar el objetivo de la investigación, se revisó el estado del arte relacionado con las tecnologías que usan los jóvenes para su interacción con internet, y se resaltó su predilección en el uso de redes sociales, sitios web de entreteniendo y esparcimiento. Así mismo se revisó la literatura periodística, noticias y titulares informativos de menores víctimas de extorsión por redes sociales, uso inadecuado del internet, y uso no supervisado de las tecnologías de información y comunicación. También se consolidó el estado de los incidentes reseñados anteriormente en el mundo y Colombia, buscando promover en los padres o responsables de los menores, el uso adecuado de las tecnologías.

El desarrollo de la investigación comprendió tres momentos: 1) recopilación de información de los diferentes métodos y técnicas de ataque usadas para hacer ingeniería social en menores de edad, 2) construcción de una taxonomía de los ataques más relevantes de ingeniería social donde se evidencia el impacto en menores de edad, con el fin de determinar cuáles son los vectores de ataque más comunes y, 3) planteamiento de una estrategia para reducir los riesgos de la población juvenil frente al uso de las TIC.

Finalmente, el análisis e interpretación de resultados de la investigación permitieron generar recomendaciones para reducir la exposición de los jóvenes colombianos enfocadas al uso responsable de las TIC, cuando éstos interactúan con Internet.

Palabras clave: Adolescente, ataque, delincuente, delito, extorsión, ingeniería social, internet, Niño, pornografía infantil, red social, seguridad, tecnología, víctima

ABSTRACT

This research project focuses on the analysis of the main social engineering attack techniques used in the Colombian youth population, for which specific information is collected on the different attack methods used on minors. To address the objective of the research, the state of the art related to the technologies that young people use for their interaction with the Internet was reviewed, and their predilection in the use of social networks, entertainment and leisure websites was highlighted. Likewise, the journalistic literature, news and informative headlines of minors who were victims of extortion through social networks, inappropriate use of the Internet, and unsupervised use of information and communication technologies were reviewed. The status of the incidents previously outlined in the world and Colombia was also consolidated, seeking to promote the appropriate use of technologies among parents or those responsible for minors.

The development of the research comprised three moments: 1) compilation of information on the different attack methods and techniques used to carry out social engineering in minors, 2) construction of a taxonomy of the most relevant social engineering attacks where the impact on minors, in order to determine the results are the most common attack vectors and, 3) proposal of a strategy to reduce the risks of the youth population against the use of ICT.

Finally, the analysis and interpretation of the research results made it possible to generate recommendations to reduce the exposure of young Colombians focused on the responsible use of ICT, when they interact with the Internet.

Keywords

Adolescent, attack, offender, crime, extortion, social engineering, internet, child, child pornography, social network, security, technology, victim

INTRODUCCIÓN

El uso extensivo de Internet y las Tecnologías de la Información y Comunicación, se ha intensificado en los menores de edad y adolescentes, consolidándolos en una población de riesgo, debido a que pueden desarrollar comportamientos intransigentes en torno a la Red o ser afectados por su naturaleza emocionalmente vacilante y tendiente a la exploración de vivencias y nuevas experiencias, pues es sin lugar a dudas, una población de seres humanos en proceso de maduración personal y social. En las estadísticas que se abordarán en este documento, se observará que las tecnologías sitúan a los infantes y adolescentes en los primeros lugares de uso de internet, acentuando su predilección en el uso de redes sociales, sitios web de entreteniendo y esparcimiento.

Internet se convirtió para los infantes y adolescentes en un espacio para desarrollar su identidad, potenciar sus relaciones sociales y fortalecer su conocimiento del mundo, pero esta exposición conduce al surgimiento de eventos de riesgo para su seguridad física y mental. Entre estos riesgos que merodean a los menores de edad están aquellos que les posibilitan el acceso a contenidos multimediales no adecuados para su edad como pornografía, xenofobia, drogas, violencia, racismo, entre otros. Existen riesgos de mayor complejidad que a menudo están relacionados con el acoso en Internet, la existencia de redes y comportamientos de terceros que sitúen a los menores de edad en situaciones que pongan en riesgo su integridad mental o física.

Bajo el contexto reseñado anteriormente, este documento pretende identificar las diferentes técnicas de ataque de ingeniería social usadas en la población juvenil colombiana, con el fin de presentar una propuesta documental que brinde al joven recomendaciones para reducir su exposición en redes sociales, para lo cual se recopiló información de los diferentes métodos y técnicas de ataque usadas para

hacer ingeniería social en menores de edad, y se planteó una estrategia que brinde recomendaciones para reducir la exposición de los jóvenes colombianos, cuando hacen uso de redes sociales.

Lo anterior está apalancado en la periodicidad de noticias y titulares de menores víctimas de extorsión por redes sociales, todo por el uso inadecuado y no supervisado del internet y las redes sociales. La mayoría menores no tienen precaución y desconocen de los peligros existentes en internet, algunos menores tienen acceso a internet de forma libre sin un adulto que conozca en realidad los sitios visitados por el menor o sus amigos virtuales en las diferentes redes sociales.

Por esta razón con este trabajo se mostrará el comportamiento de los menores en las redes sociales, buscando que el lector del mismo logre conocer los peligros del uso inadecuado y no supervisado de las redes sociales, y al mismo tiempo conozca las diferentes técnicas que un ciberdelincuente puede usar para llegar a extorsionar a su víctima. Para esto se citarán diferentes artículos e investigaciones, además se presentará el estado actual de los incidentes de este tipo en Colombia, buscando promover en los propios padres o responsables de los menores de edad, el uso adecuado de las redes.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Hoy en día es muy común encontrar casos de ingeniería social en donde el objetivo es obtener información sensible y confidencial usando diferentes prácticas como grooming, doxing, phishing, Vishing. Los delincuentes engañan a sus víctimas aprovechándose de la falta de prevención y el desconocimiento de las personas sobre los riesgos que existen, como: suplantación, pornografía y extorsión, al dar mucha información por redes sociales o vía telefónica. Lo anterior se puede justificar con los resultados obtenidos por ESET en una investigación, donde Colombia ocupa el tercer puesto de países en Latinoamérica más ataques de ingeniería social con un 19% posteriormente de Costa Rica y Uruguay, que obtuvieron un porcentaje de 21% y 24% respectivamente.[1]

Haciendo énfasis en prácticas como doxing y grooming, en donde el objetivo del doxing es recopilar información de la víctima por medio de fotos, información personal publicada en redes sociales, lugares frecuentados recurrentemente, datos familiares, se realiza un análisis de la víctima usando todo lo anterior para realizar, robos, extorsión, bullying y secuestros.

El grooming involucra comúnmente a niños y adolescentes quienes sin conocer mucho de quien está del otro lado dan confianza y comparten información sensible o imágenes personales si saber que esta información compartida puede ser usada en su contra para aplicar temas prostitución, pornografía infantil o extorsión.

[1] MOLANO, Natalia. Colombia es el tercer país con más ataques de ingeniería social en América Latina. [En línea] Colombia: larepublica, 2019. [Citado Abril-2020]. Disponible en internet: https://www.larepublica.co/empresas/colombia-es-el-tercer-pais-con-mas-ataques-de-ingenieria-social-en-america-latina-2928973

En la actualidad la tecnología y el internet son usados para realizar un sin número de actividades en las que se involucran datos sensibles, por ejemplo realizar pagos, contactar a las personas, comprar, a través de estas actividades muchas veces se puede ser víctima de ingeniería social.

La sociedad no es consciente de la existencia de la ingeniería social y sus diferentes técnicas de aplicación, por eso es importante concientizar a las personas, sobre todo a los niños y adolescentes acerca de la ingeniería social, sus técnicas y las consecuencias que puede traer ser víctima de los delincuentes que practican ingeniería social.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo la inclusión de buenas prácticas de seguridad informática puede contribuir a la reducción de casos de ingeniería social de menores de edad en Colombia?

2 JUSTIFICACIÓN

Actualmente la tecnología juega un gran papel en la sociedad, ya que día a día se pueden realizar muchas cosas sin necesidad de salir de casa solo con el hecho tener internet y un dispositivo para realizar compras, pagos, estudiar, asistir a reuniones por videoconferencia, conocer personas, entre otras; por otra parte, puede llegar a ocasionar también el mal uso de la tecnología la falta de prevención en la ingeniería social.

En el 2018 la universidad EAFIT y Tigo realizaron un estudio donde evaluaron el uso de redes sociales y herramientas tecnológicas en un grupo de menores entre los 9 y 16 años de edad, de acuerdo a los resultados obtenidos de este estudio se evidencio: el 84% de los jóvenes en Colombia hacen uso de redes sociales; el 75% de los menores hacen uso de dispositivos móviles para acceder a internet.
Con lo anterior, se confirma que son muchos los menores que se exponen en internet a ser víctimas de grooming o acoso sexual.[2]

Las técnicas de ingeniería social permiten al ciberdelincuente manipular psicológicamente a las víctimas para que compartan información sensible, muchos adultos se hacen pasar por menores de edad para engañar a los menores y obtener contenido de tipo sexual para luego de esto extorsionarlos.

Para prevenir ser víctima de ingeniería social se requiere educar a las personas, dándoles a conocer y brindando herramientas que concienticen a los menores y sus acompañantes en diferentes temas como, el uso del internet supervisado o restringido, o el uso responsable y prevenido de las redes sociales.

[2] TIGO, Une – EAFIT Navegando entre las oportunidades y los riesgos en los escenarios digitales. [En línea] Colombia: Tigo-Une, 2018. [Citado Abril-2020]. Disponible en internet: http://tigo-une.com/contigoconectados/img/press-book-tigo-une.pdf

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Analizar diferentes técnicas de ataque de ingeniería social usadas en la población juvenil colombiana, con el fin de presentar una propuesta documental que brinde al joven recomendaciones para reducir su exposición en redes sociales.

3.2 OBJETIVOS ESPECÍFICOS

Recopilar información de los diferentes métodos y técnicas de ataque usadas para hacer ingeniería social en menores de edad.

Construir taxonomía de los ataques más relevantes de ingeniería social donde se evidencia el impacto en menores de edad, con el fin de determinar cuáles son los vectores de ataque más comunes.

Plantear una estrategia que brinde recomendaciones para reducir la exposición de jóvenes colombianos, cuando hacen uso de redes sociales.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

4.1.1 **¿Qué es la ingeniería social?** Son las diferentes técnicas empleadas por los ciberdelincuentes para acceder de forma no autorizada a información confidencial, ya sea de un sistema o de una persona con el fin de cometer un fraude o delito informático, generalmente lo hacen logrando ganar la confianza de la víctima vía personal o telefónica.

La Ingeniería Social es un arte y no todos los seres humanos tienen habilidades sociales. Existen personas que desde temprana edad demuestran tener la capacidad y algo habilidades para realizar labores maliciosas. Por ejemplo: existen delincuentes que en lugar de perder tiempo intentando descifrar una contraseña empleando fuerza bruta, prefieren obtenerla realizando diferentes preguntas a un empleado, de esta forma con la diferente información obtenida puede llegar a la contraseña de manera más fácil y rápida[3].

Según la opinión de uno de los más importantes hackers de la historia Kvein Mitnick[4] los seres humanos cuentan con cuatro aspectos por medio de los cuales se hace ingeniería social:

- Todos queremos ayudar.

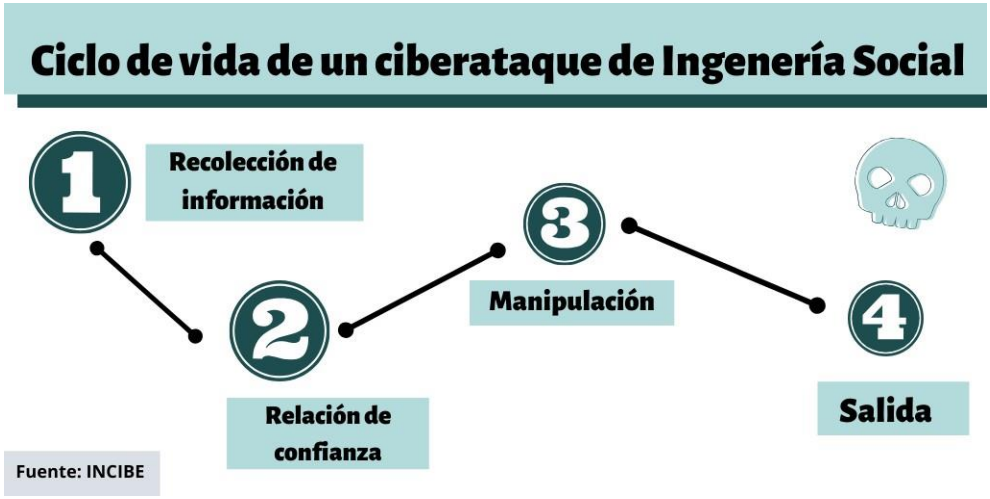
[3] SANDOVAL, Edgar Jair. INGENIERÍA SOCIAL: CORROMPIENDO LA MENTE HUMANA. . [En línea]. México: Revista Seguridad. [Citado Abril-2020]. Disponible en internet: https://revista.seguridad.unam.mx/numero-10/ingenier%C3%AD-social-corrompiendo-la-mente-humana

[4] PASTOR, Javier. Kevin Mitnick, genio o figura de uno de los hackers más famosos de la historia. [En línea] xataka, 2018. [Citado Abril-2020]. Disponible en internet: https://www.xataka.com/seguridad/kevin-mitnick-genio-o-figura-de-uno-de-los-hackers-mas-famosos-de-la-historia

- El primer movimiento es siempre de confianza hacia el otro.
- No nos gusta decir no
- A todos nos gusta que nos alaben.

4.1.2 **Ciclo de un ataque de ingeniería social.** Son las diferentes actividades o pasos que usa un ciberdelincuente para llevar a cabo un ataque de ingeniería social de manera exitosa, en la Figura 1 se observa cada uno de los pasos:

Figura 1. Ciclo de un ataque de ingeniería social



Fuente: Cuadernosdeseguridad. [Sitio web]. El ciclo de vida de un ciberataque basado en ingeniería social. Madrid [Consulta: 20 de abril de 2020]. Disponible en: https://cuadernosdeseguridad.com/2020/02/ingenieria-social-seguridad-incibe/

A continuación, se explican las 4 fases que conforman el ciclo de vida de un Ciberataque de Ingeniería social:

Recolección de la Información: En esta fase el atacante recolecta toda la información de la posible victima con el objetivo de conocer sus datos y relaciones, con alguna de la información que pueda lograr recolectar, sería la siguiente:

- Números de teléfono
- Correo
- Dirección
- Lista de amigos
- Lugares frecuentados recurrentemente

Desarrollo de la relación: Con la información anterior ya recolectada, el atacante iniciará una relación más cercana con la víctima, la relación construida determinará el nivel de contribución de la víctima y por ende ampliará el porcentaje del ataque con éxito.

Manipulación: En esta fase el atacante toma la información recolectada y lograda en las dos fases anteriores y emplea una manipulación psicológica, con el objetivo de tener un acercamiento más a la víctima e indagar y obtener información confidencial aparentemente sin importancia o el acceso concedido y/o transferido al atacante.

Salida: En esta fase el atacante alcanza el objetivo final del ataque, y lo hace sin levantar sospechas de lo acontecido, intentará de poner fin al ataque sin cuestionar lo sucedido, ya que si lo hace posiblemente la victima sospechara. Además, deja la impresión de haber hecho algo bueno por la víctima, dejando la puerta abierta para futuros acercamientos[5].

[5] PISCITELLI, Emiliano. Ingeniería social (Parte 1). [En línea]. Argentina: marketerslatam, 2017. [Citado Mayo-2020]. Disponible en internet: https://www.marketerslatam.com/digital/articulos-marketing-digital/ingenieria-social/

4.1.3 **Técnicas de ingeniería social**. Es la forma en la que un atacante llega a su víctima con el objetivo de obtener información para luego cometer un fraude. Este tipo de técnicas hacen uso de la psicología y habilidades sociales con el fin de obtener información de terceros.

A continuación, en la Tabla 1, se puede observar la clasificación de las técnicas usadas por los atacantes para hacer ingeniería social de acuerdo al artículo publicado por EcuRED[6], y se contrasta con su medio de propagación y tipo de ataque según la Guía Práctica contra la Ingeniería Social referenciada por LISA[7]:

Tabla 1. Clasificación de Técnicas de Ingeniería Social

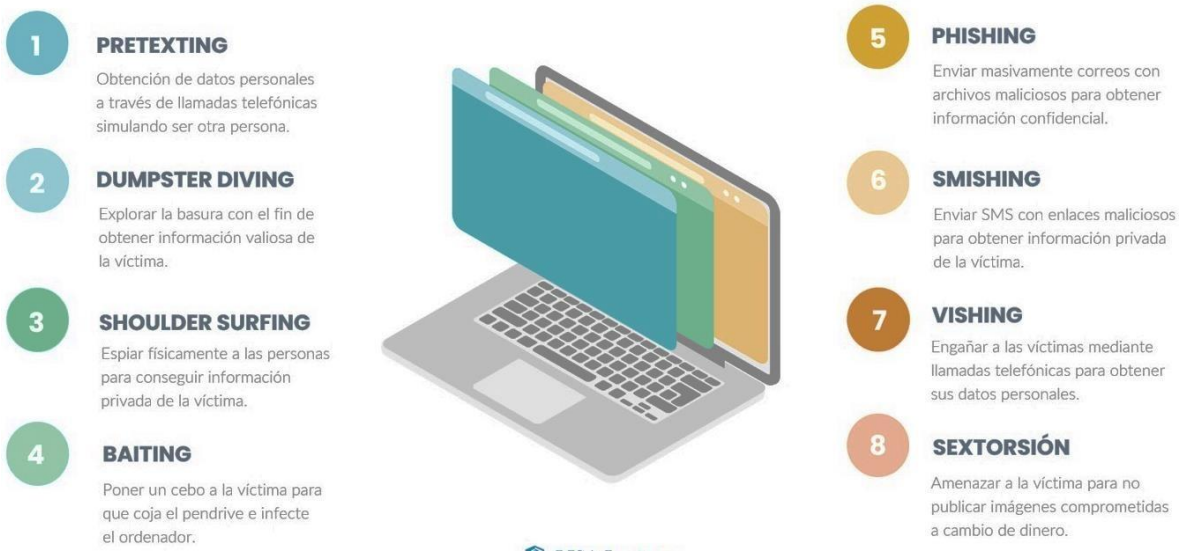
Tipo de Técnica	Medios de Propagación	Medio de Ataque
Pasiva	Observación	Shoulder Surfing, Pretexting
No presencial	Recuperación de contraseña	Baiting, Phishing, Smishing
	Emails	Phishing
	Chats	Smishing
	Teléfono	Pretexting, Vishing
Presencial no agresiva	Búsqueda en la basura	Dumpster Diving
	Persecución a personas	Shoulder Surfing
	Vigilancia de edificios	Shoulder Surfing
	Desinformación	Pretexting

Fuente: Propia del autor

[6] EcuRED. Ingeniería social. [En Línea]. Cuba: EcuRED. [Citado Noviembre -2020]. Disponible en internet: https://www.ecured.cu/Ingenier%C3%ADa_social#T.C3.A9cnicas_pasivas
[7] LISA. [Sitio web]. Guía Práctica contra la Ingeniería Social. Madrid [Consulta: 8 de marzo de 2021]. Disponible en: https://www.lisainstitute.com/blogs/blog/guia-practica-ingenieria-social

Para finalizar, en la Figura 3 se define sucintamente, cada uno de los ataques contrastados en la Tabla 1.

Figura 2. Ataques de ingeniería social



Fuente: LISA. [Sitio web]. Guía Práctica contra la Ingeniería Social. Madrid [Consulta: 8 de marzo de 2021]. Disponible en: https://www.lisainstitute.com/blogs/blog/guia-practica-ingenieria-social

4.1.4 **Medios de propagación de la ingeniería social**. Son los canales más usados por los atacantes para llevar a los métodos de ingeniería social nombrados anteriormente. En la figura 2, se puede observar los distintos medios de propagación de la ingeniería social y el tipo de información que puede ser robada por estos medios:

- Correo electrónico
- Redes sociales
- Llamadas telefónicas
- SMS
- Infección de malware

Figura 3. Medios de propagación de Ingeniería Social

Fuente: INFOSPYWARE. [Sitio web]. ¿QUÉ ES EL PHISHING? Uruguay [Consulta: 11 de noviembre de 2020]. Disponible en: https://www.infospyware.com/articulos/que-es-el-phishing/

4.1.5 **Principales Riesgos en Redes Sociales para los menores**. Internet ha revolucionado el modo en el que las personas interactúan con su entorno porque gracias a él, se accede más fácil a la información, existen mayores oportunidades de aprendizaje y ha potenciado nuevas formas para el esparcimiento y la interacción social. Los menores de edad también son actores principales de esta revolución, pues socializan a través de blogs, redes sociales, salas de chat y sitios web, en efecto según UNICEF, los infantes y adolescentes son la población más activa en Internet, pues uno de cada tres niños en el mundo es menor de 18 años[8].

El hecho de compartir información, realizar publicaciones de comentarios, fotos o videos son peligros inherentes que acarrea socializar en Internet, porque pese a todas sus ventajas, el acceso a las tecnologías sin la formación en su uso responsable o sin el acompañamiento adecuado, está exponiendo a los infantes y adolescentes a diversos riesgos digitales. La solución no es prohibirles navegar en redes sociales, sino enseñarles cómo usarlas, cómo detectar sus peligros y cómo

[8] CODAJIC. [Sitio web]. El Estado Mundial de la Infancia 2017: Niños en un mundo digital. El Bolson, Rio Negro [Consulta: 7 de marzo de 2021]. Disponible en: http://www.codajic.org/node/2861

evitarlos. Por lo anterior es esencial comprender qué riesgos se enfrentan los menores de edad cuando navegan por Internet y la presente sección del documento consignará los principales.

Grooming: Se denomina grooming a la situación en que un adulto logra ganar la confianza de un niño o adolescente valiéndose de engaños, suelen generar un perfil falso en una red social o chat, en donde se hacen pasar por una persona de su edad e inician una relación de amistad y confianza, con el objetivo de que acceda luego a sus peticiones, el delincuente puede ejercer actos criminales como acoso sexual o pornografía infantil[9].

También se puede definir como el conjunto de estrategias que una persona adulta emplea para lograr ganarse la confianza del menor a través de Internet con el fin último de lograr concesiones de índole sexual[10].
De acuerdo con lo publicado en el 2019 por el Canal RCN, el Grooming es una práctica criminal, en la que delincuentes engañan a niños y niñas a través de las redes sociales para extorsionarlos sexualmente[11].

[9] MOLINA, María P. Guía de sensibilización sobre Convivencia Digital. [En línea]. Argentina: Unicef, 2017. [Citado Abril-2020]. Disponible en internet: https://www.unicef.org/argentina/sites/unicef.org.argentina/files/2018-04/COM-Guia_ConvivenciaDigital_ABRIL2017.pdf
[10] FLOREZ, Jorge F. CIBERACOSO SEXUAL DE MENORES, GROOMING Y SEXTORSIÓN. [En línea]. Colombia: dialogando. 2019. Citado Abril-2020]. Disponible en internet: https://dialogando.com.co/ciberacoso-sexual-de-menores-grooming-y-sextorsion/
[11] CANALRCN. Atención padres: el grooming y sus riesgos para los niños en internet. [En línea]. Colombia: Canal RCN. 2019. [Citado Abril-2020]. Disponible en internet: https://noticias.canalrcn.com/tecnologia/atencion-padres-el-grooming-y-sus-riesgos-para-los-ninos-en-internet-347639

Figura 4. El Grooming con niños y adolescentes

Fuente: Carolinamotaymas. [Sitio web]. ¿Qué es el "grooming"?. República Dominicana [Consulta: 11 de noviembre de 2020]. Disponible en: http://carolinamotaymas.blogspot.com/2012/02/que-es-el-grooming.html

Sexting: Es el envío generalmente a través de Smartphones de fotografías y vídeos con contenido sexual, tomadas o grabados por sí mismo. Es una práctica frecuente entre jóvenes, y adolescentes que dejan a un lado su privacidad y no tienen presente los efectos de enviar una imagen íntima para llamar la atención o para generar algún tipo de interés en alguien[12].

Figura 5. El Sexting

Fuente: Diarioportal. [Sitio web] “Sexting”, práctica de riesgo. México [Consulta: 11 de noviembre de 2020]. Disponible en: https://diarioportal.com/2020/05/30/sexting-practica-de-riesgo/

[12] Protecciononline. Los riesgos en Internet: Ciberacoso, grooming, sexting, pornografía. [En línea]. Protecciononline [Citado en Mayo -2020]. Disponible en internet:

Doxing: El doxing es una práctica que usan los delincuentes con el objetivo de recopilar información sobre una persona, valiéndose de bases de datos, redes sociales entre otras, luego de recopilar información de realizar robo de datos personales, extorsión, fraudes[13].

Figura 6. Doxing

Fuente: nacion-hacking. [Sitio web] Doxing. [Consulta: 11 de noviembre de 2020]. Disponible en: https://aminoapps.com/c/nacion-hacking/page/item/doxing/6eGQ_BEUYI6QJdRapkbEEzKKrDbJpv3JZK

Ciberbullying: Es un tipo de bullying que se lleva a cabo por medio de las redes sociales y las nuevas tecnologías. Como en todo tipo de acoso, se basa en la emisión de una conducta de forma intencional con el objetivo de dañar a otra persona, creando una relación de desigualdad.

[13] RIOS, Estefanía C. HUELLA DIGITAL: DOXING. [En Línea]. Crimeandlaw. 2018. [Citado Abril-2020]. Disponible en internet: https://crimeandlawblog.com/2018/05/24/huella-digital-doxing/

Figura 7. Ciberbullying

Fuente: psicologiaymente [Sitio web] Ciberbullying: analizando las características del acoso virtual. [Consulta: 11 de noviembre de 2020]. Disponible en: https://psicologiaymente.com/social/ciberbullying-acoso-virtual

4.2 MARCO CONCEPTUAL

Para la comprensión de esta monografía, a continuación, se realiza la definición de algunos conceptos y procesos:

4.2.1 **Amenaza**. Suceso desfavorable que puede presentarse, generando secuelas negativas sobre los activos estimulando su indisponibilidad, mal funcionamiento o pérdida de valor, puede tener causas naturales, ser accidental o intencionada.

El Instituto Nacional de Tecnologías de la Comunicación (INTECO), órgano promovido por el Ministerio de Industria, Turismo y Comercio de España, define una amenaza como "toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información. Es decir, que podría tener un potencial efecto negativo sobre algún elemento de nuestros sistemas. Las amenazas pueden proceder de ataques (fraude, robo, virus), sucesos físicos (incendios, inundaciones) o negligencia y decisiones institucionales (mal manejo de contraseñas, no usar cifrado)"[14].

Es importante destacar que una amenaza no es equivalente a una vulnerabilidad, puesta ésta última está representada en una debilidad o fallo en un sistema de información que compromete su integridad, disponibilidad o confidencialidad, y generalmente pone en riesgo la seguridad de la información del sistema.

[14] INTECO. [Sitio web]. Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian? León [Consulta: 7 de marzo de 2021]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

4.2.2 **Ciberacoso**. El Instituto Nacional de Tecnologías de la Comunicación (INTECO) en su publicación denominada “Guía de actuación contra el ciberacoso”, define el ciberacoso como “la acción de llevar a cabo amenazas, hostigamiento, humillación u otro tipo de molestias realizadas por un adulto contra otro adulto por medio de tecnologías telemáticas de comunicación, es decir: Internet, telefonía móvil, correo electrónico, mensajería instantánea, videoconsolas online, etc”[15]. De acuerdo a lo anterior, el ciberacoso trasciende en una situación aún más compleja cuando se implica a menores de edad.

En general, el ciberacoso hace uso de medios de comunicación informáticos como correo electrónico, sitios web y redes sociales, con el fin de acosar de forma premeditada a una persona o grupo. Se ha vuelto muy frecuente entre menores que lo utilizan para molestar a sus compañeros de clases.

4.2.3 **Ciberbullying**. En la publicación denominada “Guía de actuación contra el ciberacoso” del Instituto Nacional de Tecnologías de la Comunicación (INTECO), se define el ciberbullying como tipo particular de ciberacoso donde sólo están implicados menores de edad.

INTECO de una forma más amplia indica que “el ciberbullying supone el uso y difusión de información lesiva o difamatoria en formato electrónico a través de los medios de comunicación como el correo electrónico, la mensajería instantánea, las redes sociales, la mensajería de texto a través de dispositivos móviles o la publicación de vídeos o fotografías en plataformas electrónicas de difusión de contenidos”[16]. Algunos ejemplos o actos que materializan el ciberbullying pueden ser: envió de mensajes sea por email o sms amenazando a la víctima, publicación

[15] INTECO. [Sitio web]. Guía de actuación contra el ciberacoso. León [Consulta: 7 de marzo de 2021]. Disponible en: https://www.alcobendas.org/recursos/doc/Educacion/539233046_42201383324.pdf, p. 12

[16] INTECO. [Sitio web]. Guía de actuación contra el ciberacoso. León [Consulta: 7 de marzo de 2021]. Disponible en: https://www.alcobendas.org/recursos/doc/Educacion/539233046_42201383324.pdf, p. 13

de imágenes o archivos multimedia de una persona tratando de avergonzarla en su círculo de amistades, creación de falsos perfiles en nombre de la víctima en un sitio web para escribir en primera persona temas vergonzosas, entre otros.

4.2.4 **Cibercrimen**. Actividad delictiva organizada que implica el uso de herramientas informáticas y se basa en Internet para su ejecución. El objetivo es obtener beneficios, por lo general financieros. Delitos tales como el phishing o robo de identidad son considerados cibercrimen, como así también todos los recursos y actores que forman parte de su circuito criminal.

Adrián Acosta, de la sección Digital CrimeOfficer de la INTERPOL, reseña que el cibercrimen es la "capacidad de acceder sin previo consentimiento a información y datos que son propiedad de gobiernos, personas o empresas. Todo el mundo relaciona al cibercrimen con delitos tecnológicos, o sea, el uso de la tecnología para cometer crímenes. Sin embargo, hoy en día es mucho más amplio que eso, dado que muchos delitos se cometen a través del uso de la tecnología sin distinguir un crimen especifico."[17].

4.2.5 **Delito informático**. Uso de medios electrónicos o comunicaciones basadas en Internet u otras tecnologías para llevar a cabo delitos. Los delitos informáticos son uno de los componentes que conforman el cibercrimen.

[17] MIN. [Sitio web]. Cibercrimen. Buenos Aires [Consulta: 7 de marzo de 2021]. Disponible en: https://www.iri.edu.ar/wp-content/uploads/2016/11/syd15_entrevista_corbino_cibercrimen.pdf

Santiago Acurio del Pino, profesor de Derecho Informático de la Pontificia Universidad Católica de Ecuador (PUCE), elaboró un compendio de definiciones en torno al delito informático. En principio reseña su definición como “aquel que se da con la ayuda de la informática o de técnicas anexas”, no obstante fortalece la definición como “la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software” y, finalmente indica al delito informático como “todas aquellas acciones u omisiones típicas, antijurídicas y dolosas, trátese de hechos aislados o de una serie de ellos, cometidos contra personas naturales o jurídicas, realizadas en uso de un sistema de tratamiento de la información y destinadas a producir un perjuicio en la víctima a través de atentados a la sana técnica informática, lo cual, generalmente, producirá de manera colateral lesiones a distintos valores jurídicos, reportándose, muchas veces, un beneficio ilícito en el agente, sea o no de carácter patrimonial, actúe con o sin ánimo de lucro”[18].

4.2.6 **Doxing**. Es una práctica que usan los delincuentes con el objetivo de recopilar información sobre una persona, valiéndose de bases de datos, redes sociales entre otras, luego de recopilar información se realizar robo de datos personales, extorsión, fraudes.

El CSIRT o Equipo de Respuesta ante Emergencias Informáticas de la Policía Nacional de Colombia, referencia el término como “la técnica de acceso y recopilación de información privada de un usuario, realizada a través de múltiples plataformas en Internet incluyendo las redes sociales, en la mayoría de veces es ejecutada por personas malintencionadas que posteriormente utilizan la información consolidada como una forma de intimidación, lo que contribuye a la extensión del

[18] PUCE. [Sitio web]. Delitos Informáticos: Generalidades. Quito [Consulta: 7 de marzo de 2021]. Disponible en: https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf, p. 10

ciberacoso, realizar estafas con más fundamentos de credibilidad o simplemente para localizar a su víctima y agredirla físicamente”[19].

Doxxing toma como base la consulta y publicación de información de alguna víctima en Internet, y también se prolifera en la revelación de la identidad de una persona identificada con un usuario anónimo. Por lo anterior, los ataques de doxxing generalmente están auspiciados por actos de acoso o venganza, por ejemplo, para identificar a alguien que ha publicado anónimamente, comentarios racistas.

4.2.7 **Fuga de datos**. Sebastián Bortnik, analista de seguridad perteneciente al equipo de investigadores del equipo WeLiveSecurity, creación de la firma eslovaca ESET, reseña que la fuga de datos hace referencia al “incidente que pone en poder de una persona ajena a la organización, información confidencial y que sólo debería estar disponible para integrantes de la misma”[20].

Este concepto no sólo es de carácter corporativo u organizacional, pues se aplica también a contextos personales cuando existe filtración no controlada de información de naturaleza íntima, por ejemplo, fuga de fotografías, videos u otros medios multimediales bajo custodia y propiedad de una figura pública, una familia, una pareja, entre otros.

[19] CSIRT. [Sitio web]. ¿Qué es Doxxing? Bogotá D.C. [Consulta: 7 de marzo de 2021]. Disponible en: https://cc-csirt.policia.gov.co/noticias/2020/4to-trimestre/que-es-doxxing

[20] WELIVESECURITY. [Sitio web]. ¿Qué es la fuga de información? Buenos Aires. [Consulta: 7 de marzo de 2021]. Disponible en: https://www.welivesecurity.com/la-es/2010/04/13/que-es-la-fuga-de-informacion/

4.2.8 **Eavesdropping**. En este método el atacante espía a la víctima valiéndose de vulnerabilidades de un sistema logrando capturar usuarios o claves de acceso o lo vigila de manera personal con el objetivo de obtener información privilegiada y luego hacer uso de esta para realizar fraudes[21].

4.2.9 **Grooming**. Es la persuasión de un adulto hacia un niño con la finalidad de obtener una conexión emocional y generar un ambiente de confianza para conseguir satisfacción sexual a través de imágenes eróticas o pornográficas del menor. Muchas veces los adultos se hacen pasar por niños de su edad e intentan entablar una relación para luego, buscar realizar encuentros personales -en algunos casos- con fines sexuales.

En la publicación denominada “Guía de actuación contra el ciberacoso” del Instituto Nacional de Tecnologías de la Comunicación (INTECO), se define el grooming como “un acoso ejercido por un adulto y se refiere a acciones realizadas deliberadamente para establecer una relación y un control emocional sobre un niño o niña con el fin de preparar el terreno para el abuso sexual del menor”[22]. Así que se puede inferir que el grooming son situaciones de acoso con un contenido sexual explícito o implícito dirigido a menores de edad.

[21] Deepwebiupsm, Las técnicas de la Ingeniería Social y cómo nos afecta. [En línea]. Deepwebiupsm, 2016. [Citado Mayo-2020]. Disponible en internet: https://deepwebiupsm.wordpress.com/2016/06/23/las-tecnicas-de-la-ingenieria-social-y-como-nos-afecta/

[22] INTECO. [Sitio web]. Guía de actuación contra el ciberacoso. León [Consulta: 7 de marzo de 2021]. Disponible en: https://www.alcobendas.org/recursos/doc/Educacion/539233046_42201383324.pdf, p. 21

4.2.10 **Ingeniería Social**. Conjunto de técnicas utilizadas para engañar a un usuario a través de una acción o conducta social. Consiste en la manipulación psicológica y persuasión para que voluntariamente la víctima brinde información personal o realice algún acto que ponga a su propio sistema en riesgo. Suele utilizarse este método para obtener contraseñas, números de tarjetas de crédito o PIN, entre otros.

Edgar Jair Sandoval Castellanos, pentester en el Departamento de Auditoría y Nuevas Tecnologías de la Universidad Nacional Autónoma de México (UNAM) define la ingeniería social como "el acto de manipular a una persona a través de técnicas psicológicas y habilidades sociales para cumplir metas específicas. Éstas contemplan entre otras cosas: la obtención de información, el acceso a un sistema o la ejecución de una actividad más elaborada (como el robo de un activo), pudiendo ser o no del interés de la persona objetivo"23.

El principio que considera al usuario final de un sistema de información como el eslabón más débil, es el sustento de la Ingeniería Social, puesto que no existe un solo sistema en Internet que no dependa de un ser humano. Adicionalmente se considera la Ingeniería Social como un arte, puesto que personas carismáticas y que han desarrollado grandes "habilidades sociales", se facilitan el sendero ideal para realizar acciones maliciosas respaldadas con tecnología.

[23] UNAM. [Sitio web]. Ingeniería Social: corrompiendo la mente humana. México D.F. [Consulta: 7 de marzo de 2021]. Disponible en: https://revista.seguridad.unam.mx/numero-10/ingenierí-social-corrompiendo-la-mente-humana

4.2.11 **Phishing**. Se basa en un engaño en donde los atacantes hacen que la víctima entregue información privada y confidencial, por ejemplo: contraseñas cuentas, números de tarjeta. Por lo general consiste en enviar un correo electrónico no deseado que aparentemente puede ser legítimo y confiable, tales como: haciendo la suplantación de una entidad financiera, que luego de que la víctima abra el correo lo re direcciona con a un sitio fraudulento que suplanta la identidad de la fuente confiable, una víctima ingresa la información que el atacante desea conseguir, pensando que se encuentra en el sitio auténtico de la entidad financiera[24].

4.2.12 **Tailgating**. Consiste lograr acceso a un lugar restringido, el atacante hace seguimiento del objetivo, analizando factores como: la hora en que sitio es menos concurrido o tal vez el momento en que alguien si autorizado se descuide o intentado mentir suplantando a otra persona y de esta manera obtener el acceso requerido y poder ejecutar la acción propuesta.

4.2.13 **Vishing**. Consiste en que el atacante a través de una llamada telefónica hace una suplantación, logrando envolver a la víctima usando pretextos como qué usted se encuentra participando para ganarse un premio o tal vez que lo llaman de una entidad financiera, con el objetivo que la víctima entregue información sensible generalmente: claves bancarias, números de tarjeta, usuarios de acceso a portales bancarios o hasta consignaciones de sumas de dinero haciendo más fácil que el atacante logre su objetivo.

[24] AMBIT, Spoofing. Qué es y cómo evitarlo. [En línea]. España: Ambit, 2019. [Citado Mayo-2020]. Disponible en internet: https://www.ambit-bst.com/blog/spoofing-que-es-y-c%C3%B3mo-evitarlo

4.3 MARCO LEGAL

En Colombia existen una serie de leyes que protegen a los niños y adolescentes, por medio de las cuales son castigados y condenados aquellos que comentan actos de explotación, pornografía y turismo sexual con menores.

De igual forma existen leyes que castigan y condenan los delitos informáticos en Colombia. A continuación, se describe el marco normativo reseñado:

4.3.1 **Ley 1098 de 2006**. En noviembre de 2006 por medio de esta Ley se expidió el Código de la Infancia y la Adolescencia en Colombia, debido a la condición de vulnerabilidad de los menores de edad que los hace susceptibles a tomar decisiones vertiginosas que pueden impactar su desarrollo y entorno. El Código de la Infancia y la Adolescencia establece los aspectos relacionados con la protección de los menores y describe el procedimiento a seguir cuando sus derechos son vulnerados o amenazados, así mismo contempla las acciones que sancionan a los menores que cometen delitos tan graves como el homicidio[25]. Con esta normativa, la protección de los menores de edad se consolidó como una de las prioridades en Colombia, buscado la protección y atención de los mismos.

4.3.2 **Ley 1878 de 2018**. Transcurrida una década desde la expedición y vigencia del Código de la Infancia y la Adolescencia (L. 1098/06), el órgano legislativo colombiano considero necesario reformar la normativa vigente para los menores de edad y expidió la Ley 1878 de 2018.

[25] OAS. [Sitio web]. Ley 1098 De 2006. Washington. [Consulta: 10 de marzo de 2021]. Disponible en: https://www.oas.org/dil/esp/Codigo_de_la_Infancia_y_la_Adolescencia_Colombia.pdf

Esta ley reformó los trámites administrativos para la conciliación, inobservancia de derechos, proceso administrativo de derechos, los permisos de salida del país, y todo lo referente a las adopciones, La Ley 1878 se convirtió en el desarrollo integral de los menores frente a los programas que maneja cada uno de ellos para mejorar el emprendimiento y también frente a la prevención de hechos que se generan día a día como lo son la violencia intrafamiliar y todo tipo de afectación y vulneración que afecte directamente con sus derechos fundamentales26.

4.3.3 **Ley 679 de 2001**. La ley 679 expedida por el Congreso de la República de Colombia el 3 de agosto de 2001, es una normativa orientada a la prevención y contrarrestar la explotación, la pornografía y el turismo sexual con menores de edad.

Esta ley insta a las personas para que prevengan, bloqueen, combatan y denuncien la explotación, alojamiento, uso, difusión de archivos multimedia o uso indebido de redes sociales relacionadas con actividades sexuales de menores de edad, por cuanto podría generar responsabilidad de tipo penal[27].

4.3.4 **Ley 1336 de 2009**. Por medio de la cual se fortalece la Ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo sexual con menores de edad. La Ley 1336, estipula que las aerolíneas deben adoptar códigos de conducta que prevengan y eviten la utilización y explotación sexual de niños, niñas y adolescentes en su actividad.

Así mismo la normativa solicitó a la Aeronáutica Civil informar a los pasajeros de aerolínea nacional y extranjera, que en Colombia existen disposiciones legales que previenen y castigan penalmente el turismo sexual con infantes28.

[26] ICBF1878. [Sitio web]. Ley 1878 de 2018. Bogotá D.C. [Consulta: 15 de abril de 2020]. Disponible en: https://www.icbf.gov.co/cargues/avance/docs/ley_1878_2018.htm
[27] ICBF679. [Sitio web]. Ley 679 de 2001. Bogotá D.C. [Consulta: 15 de abril de 2020]. Disponible en: https://www.icbf.gov.co/cargues/avance/docs/ley_0679_2001.htm
[28] ICBF1336. [Sitio web]. Ley 1336 de 2009. Bogotá D.C. [Consulta: 15 de abril de 2020]. Disponible en: https://www.icbf.gov.co/cargues/avance/docs/ley_1336_2009.htm

4.3.5 **Ley 1273 De 2009**. La expedición de esta normativa se consolidó como un paso importante en la lucha contra los delitos informáticos en Colombia, pues tuvo como objeto reglamentar todo lo posible sobre los delitos informáticos y salvaguardar el bien jurídico concerniente a la información y a los datos.

La Ley está estructurada en dos capítulos, el primero tipifica “los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos” y el segundo “los atentados informáticos y otras infracciones”. Cabe mencionar del capítulo dos los siguientes artículos: *Artículo 269F* sobre el delito de “violación de datos personales (hacking)” orientado a proteger los derechos fundamentales de la persona cuando un individuo sin estar facultado, sustrae o vende datos personales almacenados en ficheros o medios similares con el fin lucrarse. Y *Artículo 269G* relacionado con la suplantación de sitios web para capturar datos personales, que sucede cuando el delincuente informático hace uso de Phishing para estafar y obtener información confidencial de forma fraudulenta[29].

[29] SECSENADO. [Sitio web]. Ley 1273 de 2009. Bogotá D.C. [Consulta: 15 de abril de 2020]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

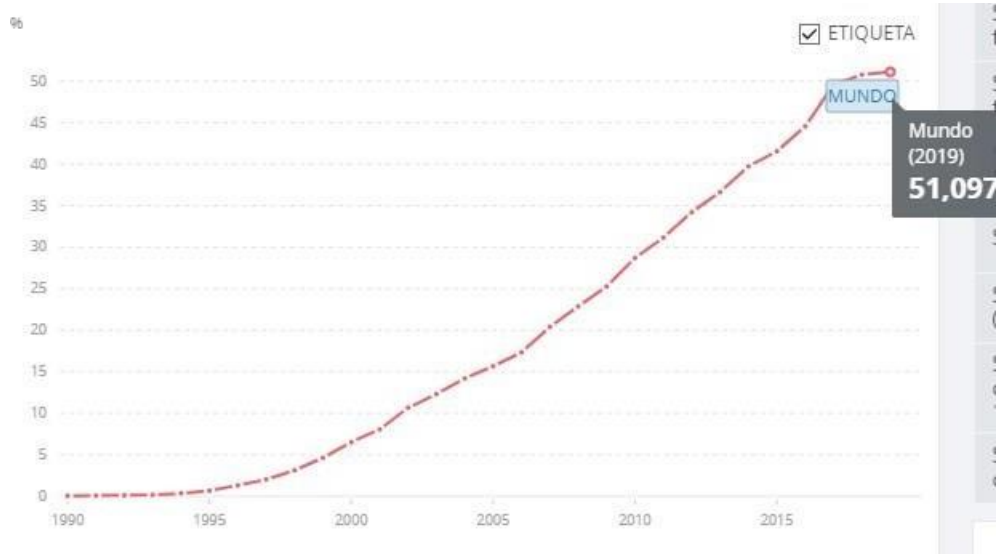
4.4 ANTECEDENTES

Internet potenció las relaciones humanas y acentuó el desarrollo de sus actividades en lo digital, convirtiendo la actual era en un contexto de socialización, y a la vez en un espacio de oportunidad criminal en el que los infantes y adolescentes continúan siendo victimadas. Términos como sexting, grooming o ciberacoso se han constituido en fenómenos que implican a un importante número de menores año tras año, motivo por el cual revisaremos en esta sección estudios de cibervictimización, así como medidas preventivas de ciberdelincuencia relacionada con menores.

En virtud de los datos del Banco Mundial, el crecimiento del uso Internet se ha acelerado durante los últimos años, puesto que el total de usuarios de Internet se ha duplicado en sólo una década, de 25.267 millones en el año 2009 a 51.097 millones a finales del año 2019[30]. En la Figura 8 se puede evidenciar el comportamiento de uso de Internet desde los años 90 hasta el año 2019, percibiéndose un crecimiento exponencial, que continuará manteniéndose por los próximos años de acuerdo a la tendencia mostrada en el gráfico de líneas. Lo anterior fue consolidado por el confinamiento provocado por el COVID-19, puesto que en el 2020 el Internet transcendió y cambio las relaciones humanas, estudios, y trabajos, pues nunca antes había sido tan necesario el uso de la red de redes para dar continuidad a las necesidades globales.

[30] BANCO MUNDIAL. [Sitio web]. Personas que usan Internet (% de la población). Washington [Consulta: 27 de febrero de 2021]. Disponible en: https://datos.bancomundial.org/indicador/IT.NET.USER.ZS

Figura 8. Personas que usan Internet



Fuente: BANCO MUNDIAL. [Sitio web]. Personas que usan Internet (% de la población). Washington [Consulta: 27 de febrero de 2021]. Disponible en: https://datos.bancomundial.org/indicador/IT.NET.USER.ZS

Ahora acentuando el uso de Internet en Colombia, Rosgaby Medina de la Agencia de Marketing Digital Branch, reseñó que el número de teléfonos conectados en el país, el cual es de 60.38 millones, supera en un 119% el número total de la población (50,61 millones)[31]. Lo anterior es explicado puesto que existen personas que tienen varias líneas telefónicas, segregadas teléfonos personales, laborales, teléfonos con multi Sim Card, entre otros.

En la Figura 9 se observa que el número de colombianos conectados a Internet es del 69% de la población total, que corresponde a 35 millones de personas. Esta misma cantidad de personas son usuarios activos en redes sociales.

[31] BRANCH. [Sitio web]. Estadísticas de la situación digital de Colombia en el 2019 y 2020. Bogotá D.C. [Consulta: 03 de marzo de 2021]. Disponible en: https://branch.com.co/marketing-digital/estadisticas-de-la-situacion-digital-de-colombia-en-el-2019-y-2020/

Figura 9. Estado general del uso de móviles, Internet y redes sociales

Fuente: BRANCH. [Sitio web]. Estadísticas de la situación digital de Colombia en el 2019 y 2020. Bogotá D.C. [Consulta: 03 de marzo de 2021]. Disponible en: https://branch.com.co/marketing-digital/estadisticas-de-la-situacion-digital-de-colombia-en-el-2019-y-2020/

Con lo anterior, se deduce que Internet se impregnó en el que hacer de las personas y en el actuar del mundo, pese a no ser un servicio público básico, se convirtió en un servicio necesario para potenciar las relaciones interpersonales y desarrollar actividades humanas. Pero precisamente su constante uso, ha aumentado el cauce de uno de los mayores problemas de la humanidad y mayor amenaza para todas las empresas en el mundo: el cibercrimen.

Robert Herjavec en el Reporte Oficial Anual de Cibercrimen del año 2019 emitido por el Equipo de Ciberseguridad Herjavec Group, indica que el impacto del Cibercrimen en la sociedad se refleja en números[32]. En agosto de 2016, el equipo

[32] HERJAVEC GROUP. [Sitio web]. 2019 Official Annual Cybercrime Report. Los Ángeles. [Consulta: 03 de marzo de 2021]. Disponible en: https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf

de Cybersecurity Ventures de Herjavec Group, predijo que el ciberdelito le costaría al mundo $6 trillones de dólares anuales en 2021, frente a los 3 trillones de dólares de 2015. Esto representa la mayor transferencia de riqueza económica de la historia, convirtiéndose en una actividad más rentable que el comercio mundial de las principales drogas ilegales combinadas. Los costos del delito cibernético incluyen daños y destrucción de datos, dinero robado, pérdida de productividad, robo de propiedad intelectual, robo de bienes personales y financieros datos, malversación de fondos, fraude, interrupción posterior al ataque el curso normal de los negocios, la investigación forense, restauración y eliminación de datos y sistemas pirateados, daño a la reputación, y debemos sumar los cibercrímenes dirigidos a menores de edad.

De acuerdo a Alberto Samuel Yohai, presidente ejecutivo de la CCIT (Cámara Colombiana de Informática y Telecomunicaciones), el uso de las nuevas tecnologías ha crecido durante los últimos años, pero el incremento del cibercrimen también ha sido paralelo, los ciberdelitos se han convertido en una de las principales problemáticas y economías ilegales en Colombia[33].

Por lo anterior, identificar los riesgos relacionados con el cibercrimen y conocer las buenas y mejores prácticas para enfrentarlos, potencia la cultura de la seguridad de la información en la ciudadanía e incrementa la confianza digital de las empresas y personas. Alberto Samuel Yohai reseña que este propósito solicita el compromiso del sector público y privado, los proveedores de tecnología empresarial y ciudadana, y las autoridades responsables de enfrentar las amenazas y mantener el orden público en el País.

[33] CCIT. [Sitio web]. Tendencias, Cibercrimen en Colombia 2019 - 2020. Bogotá D.C. [Consulta: 04 de marzo de 2021]. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

Teniendo en cuenta que los menores de edad también interactúan en la Era Digital, éstos no son ajenos a las problemáticas del cibercrimen, motivo por el cual también se han instaurado medidas para su protección. Para efectos Juan Manuel Ávila Silva, profesor investigador de tiempo completo de la Universidad Autónoma de Baja California, identificó las medidas preventivas adoptadas en el ámbito internacional para la protección de los menores de edad víctimas de ciberdelitos[34]. El académico indica que en cuanto a la protección de los menores en el ámbito internacional encontramos que los instrumentos internacionales de la Tabla 2, los cuales se centran en los abusos sexuales y la explotación sexual, como una violación de los derechos humanos del niño, y se centran en respuestas de carácter judicial.

Tabla 2. Instrumentos internacionales para protección de menores

No.	Instrumento
1	Convención sobre los Derechos del Niño (1989)
2	Protocolo Facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía (PFVN, 2000)
3	Protocolo para prevenir, reprimir y sancionar la trata de personas, especialmente mujeres y niños, que complementa la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional (“Protocolo de Palermo”, 2000)
4	Convenio del Consejo de Europa sobre la Ciberdelincuencia (2001)
5	Convenio del Consejo de Europa sobre la protección de los niños contra la explotación y el abuso sexual (2007) (Centro de Investigaciones Innocenti, UNICEF, 2012)

Fuente: Ávila Silva, J. (2018). Los menores víctimas de la ciberdelincuencia. Medidas preventivas en el ámbito internacional. Advocatus, 15(31), 79-84. https://doi.org/10.18041/0124-0102/a.31.5223

[34] ÁVILA SILVA, J. (2018). Los menores víctimas de la ciberdelincuencia. Medidas preventivas en el ámbito internacional. Advocatus, 15(31), 79-90. https://doi.org/10.18041/0124-0102/a.31.5223

Durante el Tercer Congreso Mundial de 2008 relacionado con la explotación sexual comercial de los niños, La Organización de las Naciones Unidas dió lugar a la Declaración de Río, que exhorta a cada Soberanía y País a llevar a cabo acciones para prevenir y evitar abusos sexuales de niños, y la utilización de Internet y de las nuevas tecnologías para la captación y manipulación de los niños con fines de abusos sexuales en línea y fuera de línea[35].

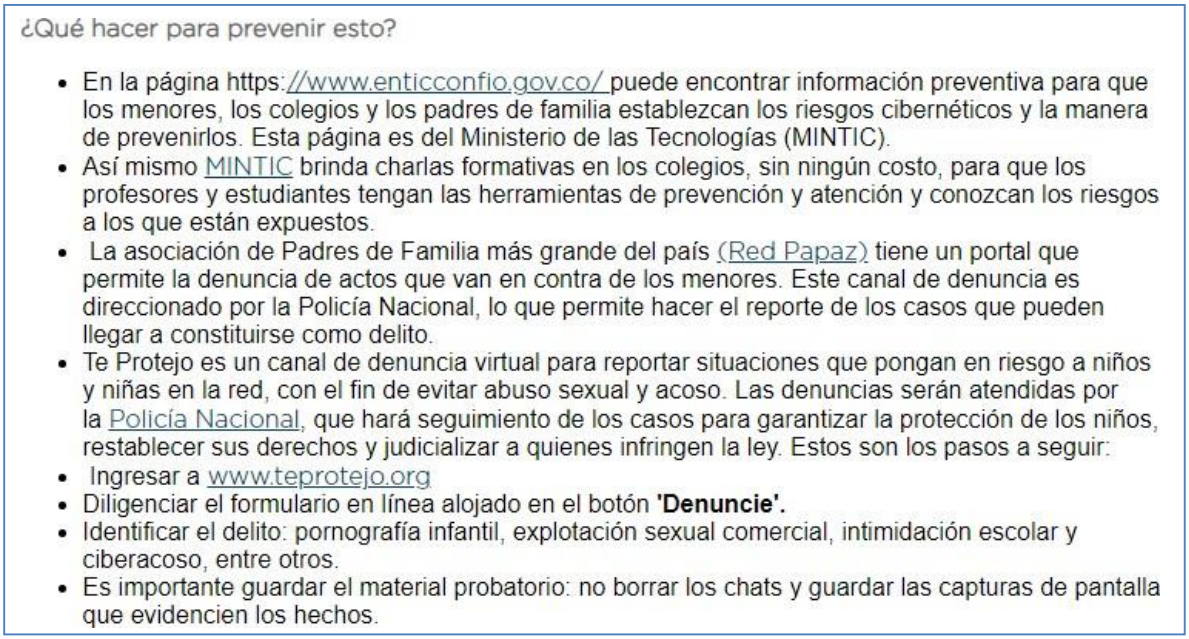
Producto de lo anterior y en relación con Colombia, la Alta Consejería Distrital TIC reseña que los niños son los más vulnerables en las redes sociales en esta época en la que el Internet está al alcance de todos. Por tal motivo en la Figura 10, la Alta Consejería Distrital TIC indica las medidas preventivas para prevenir y proteger a los infantes y adolescentes de cibercrímenes relacionados con abuso.

Así mismo el alto consejero TIC, Sergio Martínez con respecto al cibercrimen que pueden sufrir los niños colombianos, expresó que “los niños y adolescentes no se pueden dejar solos y sin ninguna supervisión en Internet; además los padres deben revisar el historial de internet frecuentemente y monitorear las redes sociales que utilizan sus menores a cargo, porque el margen de ganancia de los delincuentes está en que los niños se asustan con facilidad y no dicen lo malo que les ocurre”[36].

[35] Ibid., p. 85

[36] TIC BOGOTA. [Sitio web]. ¡Ojo con sus niños! Cuídelos de los crímenes cibernéticos. Bogotá D.C. [Consulta: 05 de marzo de 2021]. Disponible en: https://tic.bogota.gov.co/noticias/¡ojo-sus-niños-cuídelos-los-crímenes-cibernéticos

Figura 10. Estrategias de Prevención abuso en menores colombianos



¿Qué hacer para prevenir esto?

- En la página https://www.enticconfio.gov.co/ puede encontrar información preventiva para que los menores, los colegios y los padres de familia establezcan los riesgos cibernéticos y la manera de prevenirlos. Esta página es del Ministerio de las Tecnologías (MINTIC).
- Así mismo MINTIC brinda charlas formativas en los colegios, sin ningún costo, para que los profesores y estudiantes tengan las herramientas de prevención y atención y conozcan los riesgos a los que están expuestos.
- La asociación de Padres de Familia más grande del país (Red Papaz) tiene un portal que permite la denuncia de actos que van en contra de los menores. Este canal de denuncia es direccionado por la Policía Nacional, lo que permite hacer el reporte de los casos que pueden llegar a constituirse como delito.
- Te Protejo es un canal de denuncia virtual para reportar situaciones que pongan en riesgo a niños y niñas en la red, con el fin de evitar abuso sexual y acoso. Las denuncias serán atendidas por la Policía Nacional, que hará seguimiento de los casos para garantizar la protección de los niños, restablecer sus derechos y judicializar a quienes infringen la ley. Estos son los pasos a seguir:
- Ingresar a www.teprotejo.org
- Diligenciar el formulario en línea alojado en el botón **'Denuncie'.**
- Identificar el delito: pornografía infantil, explotación sexual comercial, intimidación escolar y ciberacoso, entre otros.
- Es importante guardar el material probatorio: no borrar los chats y guardar las capturas de pantalla que evidencien los hechos.

Fuente: TIC BOGOTA. [Sitio web]. ¡Ojo con sus niños! Cuídelos de los crímenes cibernéticos. Bogotá D.C. [Consulta: 05 de marzo de 2021]. Disponible en: https://tic.bogota.gov.co/noticias/¡ojo-sus-niños-cuídelos-los-crímenes-cibernéticos

5 DESARROLLO DE LOS OBJETIVOS

5.1 RECOPILAR INFORMACIÓN DE LOS DIFERENTES MÉTODOS Y TÉCNICAS USADAS PARA HACER INGENIERÍA SOCIAL EN MENORES DE EDAD

La ingeniería social emplea un conjunto de métodos para influenciar sobre las personas, y éstos han sido potenciados con el uso de Internet, porque ha permitido reducir el distanciamiento geográfico y ha facilitado las actividades de compartir información de forma masiva, así como de permitir la interacción con un amplio colectivo de modo simultáneo. Es importante resaltar que estos métodos y técnicas que usa la ingeniera social están orientadas a disuadir la forma de pensar de los individuos y se convierten en operaciones psicológicas orientadas a una población objetivo.

De acuerdo a lo anterior y teniendo en cuenta que en la sección 4.1.3 del documento, se generó un acercamiento de las modalidades usadas por la ingeniería social, durante el desarrollo del siguiente capítulo se acentuará y detallará en aquellos métodos y técnicas que afectan llanamente a los menores de edad, que bajo un uso malintencionado se aprovechan de la inestabilidad emocional de los infantes y adolescentes, y de su característica innata de explorar y generar nuevas experiencias.

Finalmente se reseñarán estadísticas de las modalidades de la ingeniería social que impactan más a los menores de edad, contrastando fuentes informativas de intuiciones de orden civil y policivo.

5.1.1 **Técnicas usadas para hacer ingeniería social en menores de edad**. De acuerdo la investigación realizada por Ellien Yulieth Rodríguez Rincón[37], los ciberdelincuentes se valen de diferentes técnicas o estrategias para lograr acercarse a sus víctimas y lograr su objetivo, entre ellas:

5.1.1.1 Pasivas. Consisten realizar un análisis e investigación de los comportamientos de la víctima con el fin de identificar y crear un perfil característico con sus diferentes hábitos, gustos y tendencias.

Frente a este tipo de técnicas, Javier Ponferrada López, técnico informático de la firma ticARTE, indica que son usadas de modo inicial para acopiar información sobre la víctima[38], convirtiéndolas en procedimientos de exploración que generalmente usan las redes sociales, puesto que la mayoría de las personas tienen la tendencia de publicar su información en línea, y esta situación no exceptúa a los menores de edad, quienes también usan el ciberespacio para compartir sus gustos.

De acuerdo a lo anterior, los ciberdelincuentes tienen a su disposición la red de Internet para copiar información confidencial de su objetivo y generalmente pueden crear una cuenta falsa en redes sociales para que la víctima los agregue como amigo o para seguir la cuenta de alguien y así obtener su información.

[37] (RODRIGUEZ RINCON, Ellien Yulieth. Op. Cit., P. 17 Metodologías de Ingeniería Social.[En línea].Madrid - España Universidad Oberta de Cataluña. Junio. [Citado Octubre-2020]. Disponible en internet: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/81255)

[38] TICARTE. [Sitio web]. ¿Qué es footprinting y fingerprinting?. Vancouver, Canadá. [Consulta: 12 de abril de 2021]. Disponible en: https://www.ticarte.com/contenido/que-es-footprinting-y-fingerprinting

5.1.1.2 No presenciales. Logran obtener información de la víctima por medio de llamadas telefónicas, correos electrónicos con solicitudes de información haciendo suplantación de identidad.

Ampliando lo último, el Programa educativo Foro Nativos Digitales de Junta de Extremadura en España, referencia la suplantación de identidad como la acción por la que una persona se hace pasar por otra[39]; este comportamiento, que es bastante usual entre los adultos para realizar acciones ilícitas o ilegales, a veces se da también entre los menores, ya sea por broma o con finalidad de acoso. La Junta de Extremadura también indica que los siguientes ejemplos, son las estrategias más frecuentes de suplantación de identidad entre menores:

- Crear un perfil falso, utilizando datos personales de la víctima.
- Entrar sin consentimiento en la cuenta de un servicio de Internet de otro menor para hacerse pasar por él.
- Publicación de anuncios o comentarios en páginas web de contactos o mediante mensajería instantánea (por ejemplo, WhatsApp).

5.1.1.3 Presenciales no agresivas. Se realiza por medio de seguimiento a la víctima y su entorno, buscando obtener información personal como lugar de residencia, oficina, amigos y familiares haciendo de manera presencial pero aún sin atacar.

Generalmente este tipo de técnicas están asociadas a espionaje físico, con el fin de materializar acciones sobre las víctimas orientadas a obtener información mediante

[39] EDUCAREX. [Sitio web]. Suplantación de identidad. Extremadura, España. [Consulta: 12 de abril de 2021]. Disponible en: https://emtic.educarex.es/nativosdigitales_materiales/pildoras_familias/rrssyadolescentes/suplantacin_de_identidad.html

persecuciones o ataques tipo Shoulder Surfing, éste último al cual referenciaremos con detalle en la sección 5.2 de este documento.

5.1.1.4 Agresivas. Consiste en lograr obtener la confianza de la víctima, para luego influir en el mismo y así manipularlo haciendo que realice cosas indebidas para luego poder chantajear o extorsionar amenazando con divulgar lo realizado por la víctima.

Jorge Flores, editor de Xataka, reseña que con las técnicas agresivas generalmente el delincuente emplea el material íntimo para ganar dinero[40], y también advierte que los chantajes, en estos casos, suelen ser orquestarlos por bandas organizadas que buscan enriquecerse con sus víctimas. Flores indica que con la proliferación de las redes sociales, se reduce la edad de la víctima potencial para los chantajes, pues si antes era un hombre de 40 años al que engañaban, ahora puede ser un adolescente o infante.

5.1.2 **Grooming**. Una modalidad de la ingeniería social que se convirtió en un problema de la sociedad y que afecta gravemente el actuar de los menores de edad, es el grooming, método en el cual un adulto gana la confianza de un infante con el fin de realizar contacto sexual.

De acuerdo a Patricia de Santisteban y Manuel Gámez, investigadores de la Universidad Autónoma de Madrid, actualmente se sabe poco sobre las tácticas que los adultos usan para manipular a los menores e interactuar sexualmente con

[40] XATAKA. [Sitio web]. Qué hacer si alguien te chantajea a ti o a tus hijos con la publicación de fotos y material íntimo. Madrid. [Consulta: 12 de abril de 2021]. Disponible en: https://www.xataka.com/legislacion-y-derechos/que-hacer-alguien-te-chantajea-a-ti-a-tus-hijos-publicacion-material-intimo

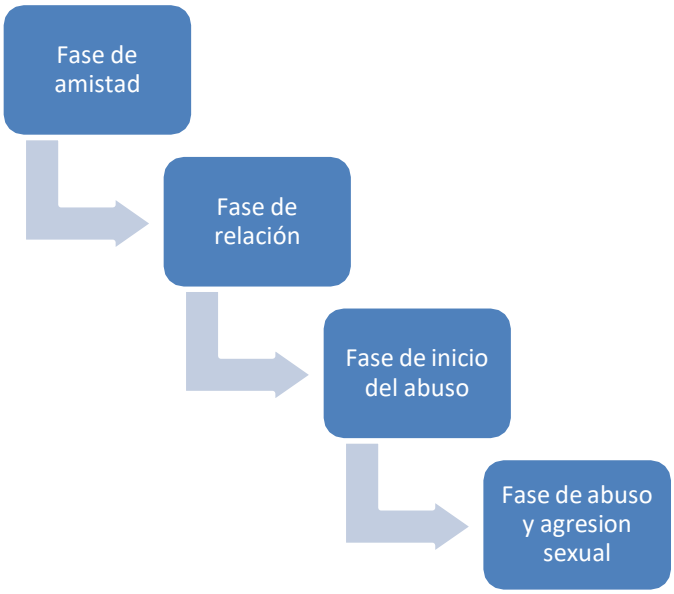
ellos[41], pero indican que el modus operandi del atacante representado por un adulto, conduce a hacerse pasar por un menor con el fin de construir una relación de confianza con su víctima, y así lograr obtener información usando artimañas de engaño y persuasión para que finalmente consiga que la víctima acceda a sus peticiones, que generalmente concluyen con prácticas criminales como acoso sexual o pornografía infantil.

Las acciones ejecutadas por el adulto malintencionado para establecer control emocional y una relación sobre los menores de edad, generalmente cuentan con un conjunto de actividades encadenadas, para efectos en la Figura 11 Fases del grooming, se observa las etapas de acoso por las que el adulto atacante logra hacerse con la confianza del infante y consume el abuso. Posteriormente se amplía el detalle de cada una de las fases del grooming de acuerdo a lo reseñado por el CEFIRE - Centro de Formación Innovación y Recursos Educativos de la ciudad de Valencia en España[42].

[41] COPMADRID. [Sitio web]. Estrategias de persuasión en grooming online de menores: un análisis cualitativo con agresores en prisión. Madrid. [Consulta: 19 de marzo de 2021]. Disponible en: https://journals.copmadrid.org/pi/art/j.psi.2017.02.001

[42] CEFIRE. [Sitio web]. Fases del grooming. Valencia, España. [Consulta: 19 de marzo de 2021]. Disponible en: http://cefire.edu.gva.es/pluginfile.php/1364209/mod_resource/content/10/51_fases_del_grooming.html

Figura 11. Fases del grooming



Fuente: Propia del autor

5.1.2.1 Fase de amistad. En esta fase inicial el atacante realiza contacto con la victima logrando entablar relación de amistad, haciendo creer que comparten gustos y vivencias, aparentando ser una persona de la misma edad de la víctima.

5.1.2.2 Fase de relación. Aprovechándose del acercamiento logrado en la etapa anterior el atacante logra obtener información y datos personales de la víctima, en ocasiones la victima siente tanta confianza en su nuevo amigo que realiza confesiones y accede a peticiones de índole sexual (intercambio de imágenes o videos) hechas por el atacante.

5.1.2.3 Fase de inicio del abuso. Valiéndose de tácticas aplicadas a la personalidad de la víctima (como la seducción o el mostrar imágenes de contenido pornográfico) el atacante consigue que la víctima le comparta imágenes de su cuerpo desnudo, se masturbe frente a la webcam o realice expresiones de insinuación sexual.

En ocasiones la victima sede las peticiones realizadas por el atacante ayudándole a conseguir el contenido con el que más adelante lo chantajeara para obtener más contenido o hasta un encuentro personal.

5.1.2.4 Fase de abuso y agresión sexual. En esta fase el atacante logra extorsionar a la víctima, logrando obtener más material o lograr un encuentro personal con el fin abusar sexualmente de él.

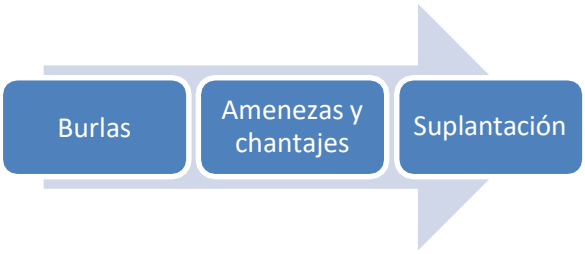
Lo logra por medio del chantaje, muchas veces manifestado a la víctima que si no accede a sus peticiones compartirá o enviará sus contactos las imágenes o video realizados o se contactará con los padres de la víctima y les mostrará las fotos de la víctima. [43]

5.1.3 **Ciberbullying**. Es un tipo de bullying que se lleva a cabo por medio de las redes sociales y las nuevas tecnologías.

Como en todo tipo de acoso, se basa en la emisión de una conducta de forma intencional con el objetivo de dañar a otra persona, creando una relación de desigualdad. Ahora bien, equivalente a la técnica de grooming, el ciberbullying también cuenta con un conjunto de etapas que se observan en la Figura 12.

[43] (DEFO, Julio, Grooming. [En línea]. Seguridad TIC y menores de edad para educadores. Octubre 2015. [Citado Octubre-2020]. Disponible en internet: https://seguridadticymenoresdeedad.wordpress.com/2015/10/12/grooming/)

Figura 12 Fases del ciberbullying



Fuente: Propia del autor

A continuación, se detalla cada una de las fases del ciberbullying:

5.1.3.1 Burlas. Tiene como fundamento la ridiculización de la víctima dentro de un grupo o en el aula de clase por alguna característica de su aspecto físico o social, los cuales influyen en la autoestima y la moral de la víctima, la mayoría de las veces pasa del entorno escolar a las redes sociales.

5.1.3.2 Amenazas y chantajes. El entorno y las situaciones que ha sufrido la victima lo hacen vulnerable lo que permite a sus atacantes aprovechase de esto y hacen la víctima no sea capaz de manifestar los problemas.

En esta fase es habitual que el atacante amenace a la víctima con situaciones que podrían presentarse en la vida real e incluso les obliguen con fotografías u objetos personales con los que consigan hacerles daño.

5.1.3.3 Suplantación. En esta fase el atacante ya tiene el control psicológico de la víctima, tanto así que ya se tiene control hasta de las redes sociales por medio de las cuales lo deja en ridículo haciendo viral el acoso, acabando por completo con su autoestima. [44]

5.1.4 **Sexting y Sextorsión**. Sexting es una práctica malintencionada que consiste en la difusión de contenidos infantiles eróticos o pornográficos a través de redes sociales y teléfonos móviles[45].

Existen dos tipos: sexting activo que consiste en la distribución de imágenes comprometidas, y sexting pasivo que está constituido por la recepción de contenidos sexuales. Por otra parte, sextorsión corresponde a una extorsión sexual, lo cual se materializa cuando una persona es amedrentada con una imagen íntima, en la mayoría de los casos la víctima es obligada para tener relaciones sexuales con alguien, entregar dinero o más imágenes pornográficas, o algún otro beneficio.

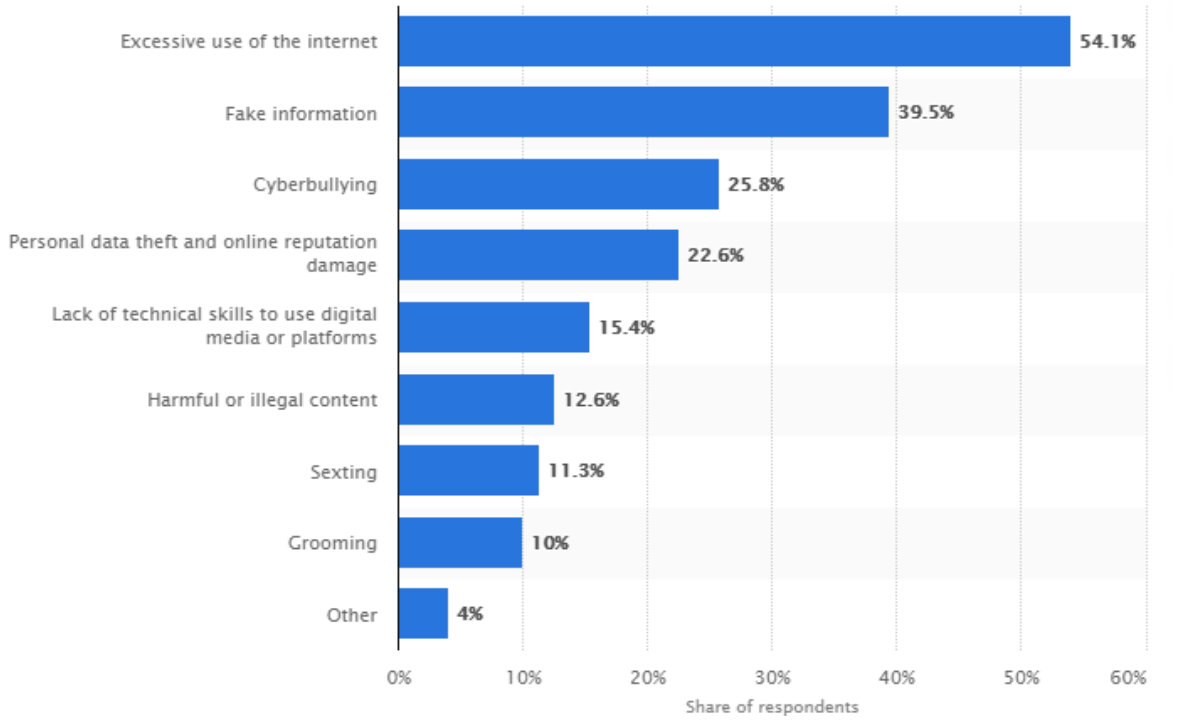
Entre las principales intenciones que los acosadores encuentran para chantajear a sus víctimas mediante la sextorsión, se encuentran recibir más contenidos similares de las víctimas, acordar una cita con objetivos sexuales o, abusar sexualmente de la víctima.

[44] (EXTRA Tecnología, Las etapas del ciberbullying. [En línea]. Agenda de la empresa. Abril 2016. [Citado Octubre-2020]. Disponible en internet: https://www.agendaempresa.com/71839/las-etapas-del-ciberbullying/)

[45] GOBIERNO DE CANARIAS. [Sitio web]. Sexting. Canarias. [Consulta: 19 de marzo de 2021]. Disponible en: https://www3.gobiernodecanarias.org/medusa/ecoescuela/seguridad/riesgos-asociados-al-uso-de-las-tecnologias/sexting/

5.1.5 **Estadísticas relacionadas con los métodos y técnicas de ingeniería social que afectan a menores de edad**. La economista e investigadora rumana Justina Alexandra Sava en la Figura 13, indica que a nivel mundial el riesgo más grande para los menores de edad en el ciberespacio corresponde al excesivo uso de internet sin supervisión de un adulto, seguido de la información falsa que se publica en la web pues no tiene control, y en pocos minutos está viralizada a nivel global. También destaca en tercer lugar el Cyberbulling, y hace mención a la participación del Sexting y Grooming como riesgos inherentes de la Internet que hoy por hoy impactan a los infantes y adolescentes[46].

Figura 13. Riesgos en línea más comunes sobre los niños

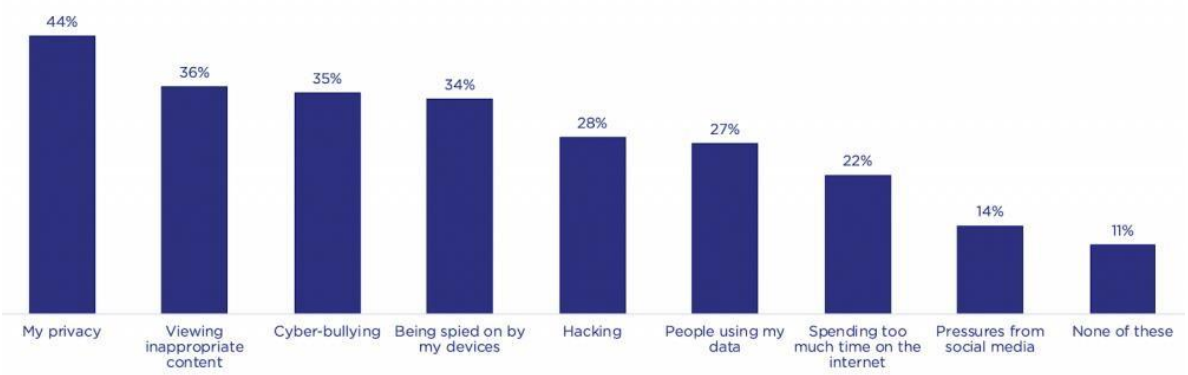


Fuente: STATISTA. [Sitio web]. What do you think are the most common online risks that you and other children your age had been exposed to?. [Consulta: 19 de marzo de 2021]. Disponible en: https://www.statista.com/statistics/1167050/romania-online-risks-that-children-had-been-exposed-to/

[46] STATISTA. [Sitio web]. What do you think are the most common online risks that you and other children your age had been exposed to?. [Consulta: 19 de marzo de 2021]. Disponible en: https://www.statista.com/statistics/1167050/romania-online-risks-that-children-had-been-exposed-to/

Frente a lo anterior el CEO de Kids Corp, Demian Falestchi, reseña que los adolescentes son más conscientes de los riesgos que podrían atentar con ellos cuando realizan actividades en Internet[47]. En la Figura 14 se observa que la privacidad es un tema de interés para los adolescentes y menores de edad, así como les preocupa el cyberbullying, el ser espiados y el cómo se utilizan sus datos personales por otros individuos o compañías.

Figura 14. Los niños en América Latina son conscientes de los peligros de Internet



Fuente: IABCOLOMBIA. [Sitio web]. El desconocimiento, la silenciosa complicidad y el avance del grooming en América Latina. Bogotá, Colombia. [Consulta: 19 de marzo de 2021]. Disponible en: https://www.iabcolombia.com/el-desconocimiento-la-silenciosa-complicidad-y-el-avance-del-grooming-en-america-latina/

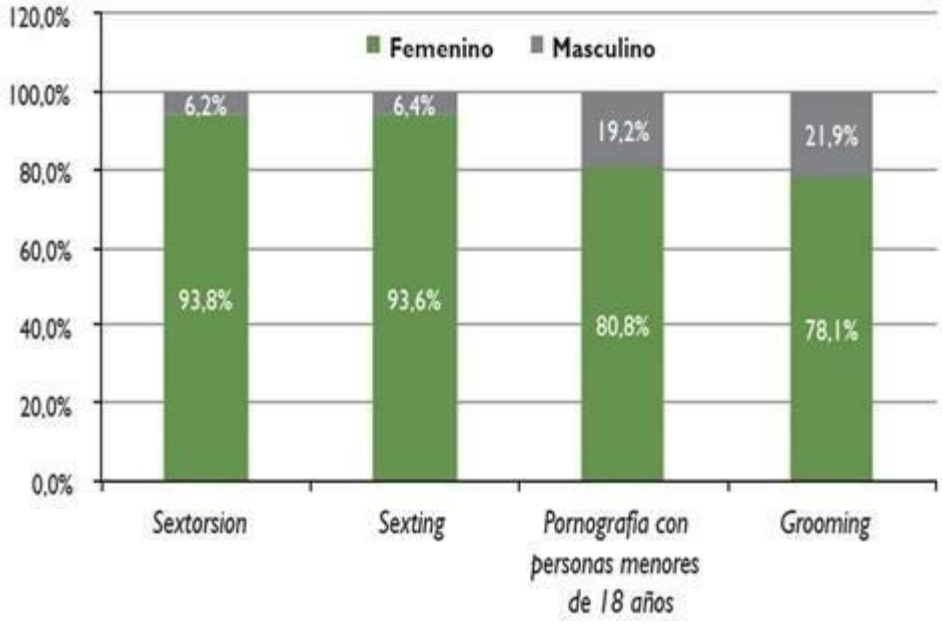
Focalizando cifras en Colombia, el Magister en Victimología y Criminología de la Policía Nacional de Colombia, Mauricio Romero Hernández, realizó una investigación constituida por 1.705 denuncias del Sistema Penal Oral Acusatorio durante los años 2006 a 2015, de las cuales 1.510 corresponden a los artículos 218 y 195 al 219A de la Ley 599 de 2000[48], porque son los numerales que más usados

[47] IABCOLOMBIA. [Sitio web]. El desconocimiento, la silenciosa complicidad y el avance del grooming en América Latina. Bogotá, Colombia. [Consulta: 19 de marzo de 2021]. Disponible en: https://www.iabcolombia.com/el-desconocimiento-la-silenciosa-complicidad-y-el-avance-del-grooming-en-america-latina/

[48] SCIELO HERNÁNDEZ. [Sitio web]. Tecnología y pornografía infantil en Colombia, 2013-2015: interpretación desde un enfoque victimológico. Bogotá, Colombia. [Consulta: 19 de marzo de 2021].

por los organismos judiciales y víctimas para relacionar las actividades relacionadas con delitos de abuso y pornografía infantil mediante el uso de las Tecnologías de la Información y Comunicación. En la Figura 15, se observa la participación de las técnicas de sextorsion, sexting y gromming distribuidas por genero sexual de los menores de edad victimizados, donde se evidencia que los delitos en su mayoría están orientados a infantes y adolescentes de género femenino.

Figura 15. Agrupación de denuncias del Sistema Penal Oral Acusatorio durante los años 2006 a 2015



Fuente: SCIELO HERNÁNDEZ. [Sitio web]. Tecnología y pornografía infantil en Colombia, 2013-2015: interpretación desde un enfoque victimológico. Bogotá, Colombia. [Consulta: 19 de marzo de 2021]. Disponible en: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1794-31082017000100027#aff1/

Por otro lado, en el proyecto de acuerdo 470 de 2017 del Consejo de Bogotá D.C., mediante el cual se adoptarían lineamientos y estrategias de prevención frente a crímenes cibernéticos que amenazan a menores de edad del Distrito Capital, se

Disponible en: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1794-31082017000100027#aff1/

informa que el Centro Cibernético Policial reportó entre los años 2014 y 2017, la existencia de 2.969 denuncias de delitos de abuso sexual a menores[49].

En la Figura 16, de acuerdo al informe de las tendencias del cibercrimen en Colombia (2019-2020) del CCIT y la Policía Nacional de Colombia[50], fueron registrados 28.827 casos de cibercrimen durante el 2019, de los cuales 15.948 fueron denunciados como conductas de Delitos Informáticos. Así mismo y de acuerdo a Adriana Magali Matiz Vargas, miembro de la Cámara de Representantes de Colombia, desde 2019 a la fecha se han registrado más de 4.000 denuncias por pornografía infantil, 19 bloqueos de URL con contenidos de material de abuso infantil, 930 casos de facilitación de medios de comunicación para ofrecer actividades sexuales con menores de edad, y más de 2.000 denuncias por sextorsión, ciberbullying virtual y delitos similares[51].

Figura 16. Estadística pornografía infantil de la Policía Nacional

Fuente: CCIT. [Sitio web]. Tendencias, Cibercrimen en Colombia 2019 - 2020. Bogotá D.C. [Consulta: 04 de marzo de 2021]. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf. (s.f.).

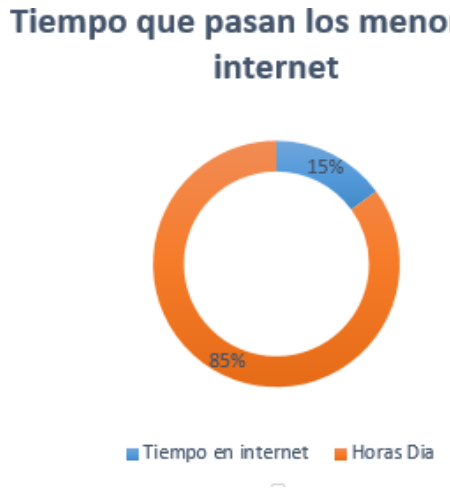
[49] ALCALDÍA BOGOTÁ. [Sitio web]. Proyecto de Acuerdo 470 de 2017. Bogotá, Colombia. [Consulta: 19 de marzo de 2021]. Disponible en: https://www.alcaldiabogota.gov.co/sisjur/adminverblobawa?tabla=T_NORMA_ARCHIVO&p_NORMFIL_ID=9369&f_NORMFIL_FILE=X&inputfileext=NORMFIL_FILENAME

[50] CCIT. [Sitio web]. Tendencias, Cibercrimen en Colombia 2019 - 2020. Bogotá D.C. [Consulta: 04 de marzo de 2021]. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf. (s.f.).

[51] BLURADIO. [Sitio web]. Desde 2019 a la fecha van más de 4.000 denuncias por pornografía infantil en Colombia. Bogotá D.C. [Consulta: 04 de marzo de 2021]. Disponible en: https://www.bluradio.com/politica/desde-2019-a-la-fecha-van-mas-de-4-000-denuncias-por-pornografia-infantil-en-colombia.

También existen estudios de instituciones y organismos independientes que muestran la interacción de los menores de edad con las tecnologías de Internet. Uno de éstos fue el realizado por Tigo, Une y la Universidad EAFIT de Medellín a 485 menores, con edades entre los 9 y 16 años de las principales ciudades del país, en el que se indicó que el 32% de éstos ha conociendo personas por medio de las redes sociales[52]. En el mismo estudio, se referencia en la Figura 17 que el tiempo promedio que los menores se conectan a internet es de 3,5 horas al día, y la cifra tiende a aumentar con la edad de la persona.

Figura 17. Tiempo en internet.

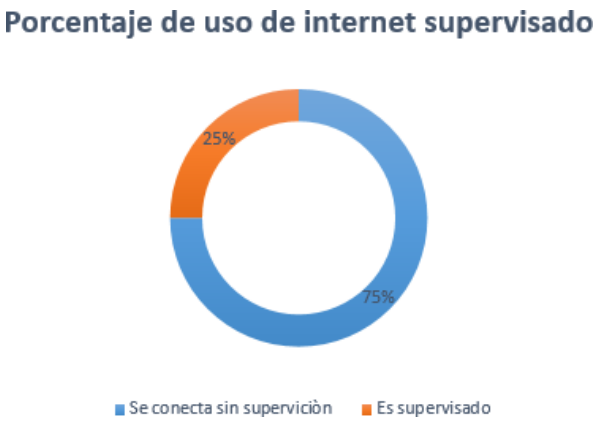


Fuente: Propia del autor

También se observa en el estudio que sólo una cuarta parte de los menores de edad son supervisados por adultos en el uso de Internet. El 75 % de los menores utiliza el celular como el medio favorito para conectarse y lo hace desde su propio cuarto sin supervisión alguna, lo que limita las restricciones.

[52] El Tiempo. El 32% de los niños y adolescentes conocen personas por internet. [En línea]. Colombia: El tiempo. 2018. [Citado Mayo -2020]. Disponible en internet: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/principales-riesgos-para-los-menores-de-edad-en-internet-290684

Figura 18. Porcentaje de uso de internet supervisado



Fuente: Propia del autor

En la Figura 19 se observa que el 35 % de los menores reveló haber visualizado imágenes sexuales en internet, principalmente por medio de las redes sociales. También el estudio determinó que el 55% de los jóvenes entre 15 y 16 años ha conocido extraños por internet y 34% de estos se han encontrado con ellos.

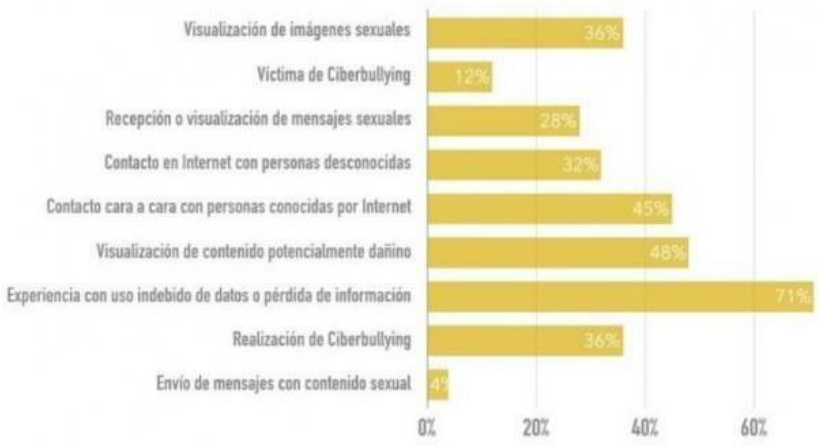
Figura 19. Visualización de contenidos no aptos para menores

Fuente: Propia del autor

Otro estudio independiente liderado por EL TIEMPO reseña que el mayor riesgo que enfrentan los menores de edad en Internet corresponde a la pérdida de

información con una participación del 71%[53]. En la Figura 20 y como segundo factor de riesgo sobre los infantes y adolescentes, se destaca la visualización de contenido inapropiado que prolifera en Internet y que es complejo controlar debido a la facilidad de viralización de la información. Finalmente, el estudio pondera el cyberbulling y el contacto físico con personas que se conocen en Internet, también como riesgos que impactan a los menores de edad.

Figura 20. Los principales riesgos a los que se enfrentan los menores en internet.



Fuente: ELTIEMPO. [Sitio web]. Casi 4 denuncias al día se reciben por casos de explotación de menores. Bogotá, Colombia. [Consulta: 19 de marzo de 2021]. Disponible en: https://www.eltiempo.com/justicia/delitos/claves-que-pedofilos-usan-para-ocultar-pornografia-infantil-en-internet-414560

El estudio de ELTIEMPO informa que las ciudades desde donde más se reportan este tipo de casos relacionados con materializaciones de los riesgos de la Figura 20 son Bogotá, Medellín, Cali, Bucaramanga e Ibagué. En los últimos nueve años, en Colombia se han presentado 5.583 acusaciones de casos por delitos como pornografía y delitos sexuales con menores de edad relacionados con el acceso de

[53] ELTIEMPO. [Sitio web]. Casi 4 denuncias al día se reciben por casos de explotación de menores. Bogotá, Colombia. [Consulta: 19 de marzo de 2021]. Disponible en: https://www.eltiempo.com/justicia/delitos/claves-que-pedofilos-usan-para-ocultar-pornografia-infantil-en-internet-414560

internet. Así mismo se indica que este tipo de delitos por internet año a año se incrementa:

- En el 2018 fueron 1.445 reportes
- En el 2017 se recibieron 1.323
- En el 2016 fueron 866
- En el 2015 llegaron 518 reportes.

De acuerdo a lo expuesto en el presente capítulo, cabe acentuar la adolescencia como un período de riesgo en los menores de edad que paralelo a las alteraciones de la personalidad comunes y presentes en los individuos próximos a la adultez, suelen hacerlos sentir insatisfechos frente a las necesidades psicológicas básicas, como la independencia, generación de relaciones sociales e íntimas, necesidad de explorar nuevas vivencias, entre otros. Ahora bien, los menores de edad ven en la Internet y en las Tecnologías de la Información y Comunicación, un medio para potenciar sus expresiones y sentimientos, y por tal motivo se observa la alta participación de los infantes en el uso de dispositivos móviles y equipos de cómputo para frecuentar sitios web, redes sociales, salas de chat y ocio, esparcimiento y videojuegos.

Se detalló los principales métodos, modalidades y técnicas de ingeniería social usadas malintencionadamente para vulnerar a los menores de edad, entre las que destacan el grooming, cyberbullying, sexting, sextorsion. Finalmente se revisaron cifras a nivel mundial y nacional de las modalidades de ingeniería social que vulneran a los infantes y adolescentes que a la larga evidencian que la mejor forma de mitigar los riesgos es la generación de confianza con los menores a través de la comunicación, respetando el espacio personal y permitiendo la interacción y supervisión de los padres sobre el uso que dan sus hijos a las tecnologías,

enséñales a ser conscientes de su seguridad en la Internet, identificar riesgos, prevenirlos y comunicarlos cuando se sientan amenazados o vulnerados.

5.2 CONSTRUIR TAXONOMÍA DE LOS ATAQUES MÁS RELEVANTES DE INGENIERÍA SOCIAL DONDE SE EVIDENCIA EL IMPACTO EN MENORES DE EDAD, CON EL FIN DE DETERMINAR CUÁLES SON LOS VECTORES DE ATAQUE MÁS COMUNES.

En el sub capítulo 5.1 se reseñaron las modalidades usadas por la ingeniería social para generar aceptación y ganar confianza sobre las personas, y se hizo hincapié en aquellos métodos y técnicas que afectan principalmente a los menores de edad. Ahora bien, estas modalidades de ingeniería social son materializadas a través del uso de un conjunto de ataques que serán detallados en la sección sucesiva.

Así mismo, se reseñarán cifras y estadísticas contrastadas de fuentes informativas de instituciones de orden civil y estudios independientes, con el fin de generar un panorama de los ataques de la ingeniería social que impactan más a los menores de edad.

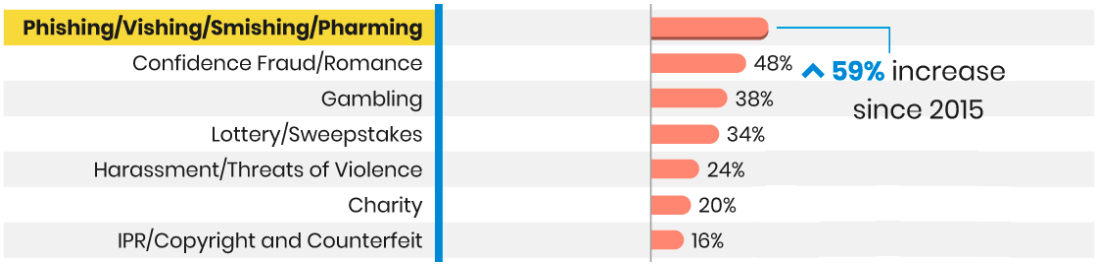
5.2.1 **Ataques más comunes de ingeniería social sobre menores de edad: phishing, vishing, smishing y pharming**. El gusto inherente que genera el uso de la Internet sobre las personas se ha convertido en un modo de vida, en el que actividades laborales, académicas y de esparcimiento interactúan ineludiblemente con las tecnologías de la información y comunicación.

En la Tabla 1 de la sección 4.1.3 - Técnicas de ingeniería social -, se contrastaban las modalidades de ingeniería social vs los ataques usados sobre las personas, que aprovechaban la masificación de la Internet y que día a día incrementarán su participación en las redes de comunicaciones.

Eric Griffith, exfundador de Windows Sources, indica que entre 2015 y 2018 existió un aumento del 59 por ciento en los ataques de ingeniería social relacionados con phishing, vishing, smishing y pharming, de acuerdo a las estadísticas del Informe de

delitos en Internet del FBI del año 2018[54]. En la Figura 21, puede observarse que estos ataques pasaron de un 48% en el año 2015, a tener una participación del 59% tres años después. Ahora bien, extrayendo algunos conceptos del Marco Conceptual y Glosario del documento, y lo referenciado por Griffith, en la Tabla 3 se explican cada uno de los ataques reseñados.

Figura 21. Incremento de víctimas de cibercrimen por ataque



Fuente: PCMAG. [Sitio web]. As Phishing and Similar CyberCrimes Increase, Are Victims Better at Threat Assessment?. New York, USA. [Consulta: 26 de marzo de 2021]. Disponible en: https://www.pcmag.com/news/as-phishing-and-similar-cybercrimes-increase-are-victims-better-at-threat

Tabla 3. Phishing, Vishing, Smishing y Pharming

Amenaza	Descripción
Phishing	Se basa en un engaño en donde los atacantes hacen que la víctima entregue información privada y confidencial, por ejemplo: contraseñas cuentas, números de tarjeta. Por lo general consiste en enviar un correo electrónico no deseado que aparentemente puede ser legítimo y confiable, tales como: haciendo la suplantación de una entidad financiera, que luego de que la víctima abra el correo lo re direcciona con a un sitio fraudulento que suplanta la identidad de la fuente confiable, una víctima ingresa la información que el atacante desea

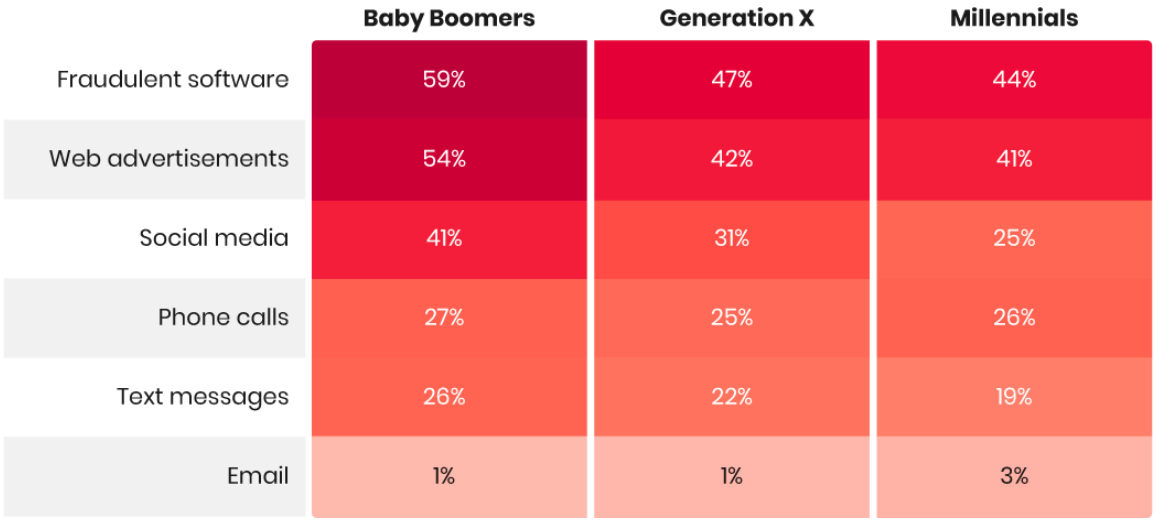
[54] Fuente especificada no válida

	conseguir, pensando que se encuentra en el sitio auténtico de la entidad financiera.
Vishing	Consiste en que el atacante a través de una llamada telefónica hace una suplantación, logrando envolver a la víctima usando pretextos como qué usted se encuentra participando para ganarse un premio o tal vez que lo llaman de una entidad financiera, con el objetivo que la víctima entregue información sensible generalmente: claves bancarias, números de tarjeta, usuarios de acceso a portales bancarios o hasta consignaciones de sumas de dinero haciendo más fácil que el atacante logre su objetivo.
Smishing	Smishing es una forma de phishing en la que un atacante utiliza un mensaje de texto convincente para engañar a los destinatarios específicos para que hagan clic en un enlace y envíen información privada al atacante o descarguen programas maliciosos en un teléfono móvil.
Pharming	El pharming es otra forma en que los piratas informáticos intentan manipular a los usuarios en Internet. Mientras que el phishing intenta capturar información personal haciendo que los usuarios visiten un sitio web falso, el pharming redirige a los usuarios a sitios web falsos sin que ellos lo sepan.

Fuente: Propia del autor

Griffith en la Figura 22 indica que, como parte del Informe de delitos en Internet del FBI del año 2018, Security.org encuestó a 933 personas y se logró identificar que los ataques de ingeniería social en los menores de edad más usados corresponden a Pharming (fraudulent software con una participación del 59% y web advertisements con un 54%), Phishing (social media con un 41% y email con un 1%), Vishing (Phone calls con un 27%) y Smishing (text messages con un 26%).

Figura 22. Ataques de ingeniería social dirigidos menores de edad



Fuente: PCMAG. [Sitio web]. As Phishing and Similar CyberCrimes Increase, Are Victims Better at Threat Assessment?. New York, USA. [Consulta: 26 de marzo de 2021]. Disponible en: https://www.pcmag.com/news/as-phishing-and-similar-cybercrimes-increase-are-victims-better-at-threat

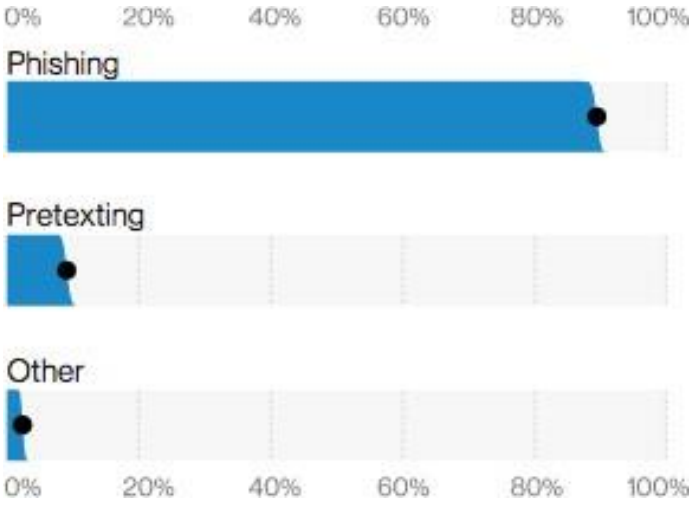
5.2.2 **Ataques atípicos de ingeniería social: baiting, dumpster diving, pretexting y shoulder surfing**. Un paradigma de la gente, es pensar que los ciberdelincuentes realizan sus actividades malintencionadas sólo a través del phishing, sea éste por correo electrónico o vía telefónica. No obstante, existen ataques de ingeniería social particulares que aprovechan la curiosidad o despreocupación de las víctimas.

En este sentido, en la Figura 23 Amanda Marchuk, investigadora de Security Boulevard (división de la compañía MediaOps, Inc), reseña que en el Informe de Investigaciones sobre Violaciones de Datos de Verizon 2020 (DBIR) se presentó la ingeniería social como un actor que representa más de dos tercios de los ataques de ciberseguridad mundiales[55]. De esos ataques, el 96% de ellos llegan a través de

[55] SECURITYBOULEVARD. [Sitio web]. The Rise of Phishing Attacks: P.S. ILoveYou. New York, USA. [Consulta: 26 de marzo de 2021]. Disponible en: https://securityboulevard.com/2020/06/the-rise-of-phishing-attacks-p-s-iloveyou/

phishing, pero la población restante está liderada por ataques pocos comunes: baiting, dumpster diving, pretexting y shoulder surfing

Figura 23. Top de incidentes de ingeniería social



Fuente: SECURITYBOULEVARD. [Sitio web]. The Rise of Phishing Attacks: P.S. ILoveYou. New York, USA. [Consulta: 26 de marzo de 2021]. Disponible en: https://securityboulevard.com/2020/06/the-rise-of-phishing-attacks-p-s-iloveyou/

Extrayendo algunos conceptos del Marco Conceptual y Glosario del documento, y lo referenciado por Marchuk, en la Tabla 4 se explican cada uno de los ataques reseñados.

Tabla 3. Baiting, Dumpster Diving, Pretexting y Shoulder Surfing

Amenaza	Descripción
Baiting	Es un ataque de ingeniería social en la que un atacante atrae a una víctima con una falsa promesa que apela a la codicia o la curiosidad. Generalmente este tipo de ataque emplea una unidad USB que lleva una carga útil maliciosa, y se deja en un vestíbulo, en un estacionamiento, o en el caso de los menores de edad, en

	establecimiento de video juegos. El fin de este ataque es esperar que la curiosidad de alguien lo lleve a conectar la unidad USB a un equipo de cómputo, momento en el que se puede instalar el malware que lleva.
Dumpster Diving	Es el proceso de buscar elementos desechados en la basura, para obtener información útil sobre una persona o empresa que luego se puede utilizar con el propósito de delinquir o extorsionar. Este ataque se dirige para llevar a cabo suplantación de identidad.
Pretexting	Es un ataque de ingeniería social en la que un agresor intenta convencer a una víctima para que ceda información valiosa o acceda a un servicio o sistema. La característica distintiva de este tipo de ataque es que los estafadores inventan una historia, o un pretexto, para engañar a la víctima. El pretexto generalmente coloca al atacante en el papel de alguien con autoridad que tiene derecho a acceder a la información que se busca, o que puede usar la información para ayudar a la víctima.
Shoulder Surfing	Acto de obtener información personal o privada a través de la observación directa. Esta actividad implica mirar por encima del hombro de una persona para recopilar información pertinente mientras la víctima no se da cuenta. Esto es especialmente efectivo en lugares concurridos donde una persona usa una computadora, teléfono inteligente o cajero automático. Si este ataque ocurre cuando hay pocas personas, el acto se vuelve sospechoso rápidamente, motivo por el cual también se utilizan binoculares, cámaras de video y dispositivos para mejorar la visión, según la ubicación y la situación.

Fuente: Propia del autor

De acuerdo a lo expuesto en la presente sección del documento, y teniendo en cuenta las modalidades de ingeniería social vistas en el sub capítulo anterior, las personas más sensibles de sufrir ataques de ingeniería social son aquellas que no

están familiarizadas con las tecnologías, esencialmente infantes y adultos mayores. Estos ataques encabezados por el phishing suelen ser difíciles de captar, por tal motivo es importante recordar que se debe desconfiar de toda llamada telefónica o mensaje que pida datos confidenciales (contraseñas, datos de tarjetas de crédito, etc.).

Se especificaron los principales ataques de ingeniería social usados para vulnerar a los menores de edad, entre los que destacan el vishing, smishing, pharming, baiting, dumpster diving, pretexting y shoulder surfing, que proliferan con el frecuente uso de videojuegos en los móviles y tabletas que los padres permiten a sus hijos, por tal motivo es recomendable enseñar a los infantes el correcto uso de las tecnologías virtuales y de información y comunicación, incluso desde la más temprana infancia.

5.3 PLANTEAR UNA ESTRATEGIA QUE BRINDE RECOMENDACIONES PARA REDUCIR LA EXPOSICIÓN DE JÓVENES COLOMBIANOS, CUANDO HACEN USO DE REDES SOCIALES.

El dialogo con los menores puede llegar a ser la forma adecuada para que el menor haga uso responsable y adecuado de las redes sociales, por ello se proponen las siguientes recomendaciones, las cuales pueden minimizar los riesgos a los que se ven expuestos los menores de edad en las redes sociales:

Dialogue con sus hijos acerca de las vivencias que experimentan día a día en las redes sociales, acérquese a ellos e indíqueles que si algo les molesta o los incomoda puede confiar en usted para que juntos puedan aclarar la duda o el inconveniente.

Asegúrese de respetar siempre los límites mínimos de edad para que el menor tenga un perfil en una red social. Cada red social elabora y solicita la aceptación de unas condiciones para poder crear una cuenta en ellas, y una de estas condiciones corresponde a tener una edad mínima. En la Tabla 4, se observan límites de edad para algunas redes sociales y cabe destacar que difieren según la red social, por ejemplo, en Twitter se puede registrar una cuenta con 13 años mientras que en LinkedIn se requiere 16 años.

Tabla 4. Límites mínimos de edad para registrar cuentas en redes sociales

13 años	13 años (con permiso paterno)	14 años	16 años	17 años	18 años
Twitter	WeChat	Facebook	LinkedIn	Vine	Path
Tumblr	Youtube	Instagram			
Pinterest	Flickr				
Snapchat	Foursquare				
WhatsApp					

Fuente: TILOMOTION. [Sitio web]. ¿Cuál es la edad mínima para abrirte una cuenta en una Red Social? Madrid [Consulta: 7 de marzo de 2021]. Disponible en: https://www.tilomotion.com/blog/cual-es-la-edad-minima-para-abrirte-una-cuenta-en-una-red-social/

Haga uso de herramientas de control parental pues apoyarán en el aprendizaje de los menores, limitando las funciones y el alcance de sus dispositivos cuando se conectan a Internet. En la Tabla 5 y de acuerdo al Instituto Nacional de Ciberseguridad de España, se observan las principales herramientas de control parental clasificadas según su función:

Tabla 5: Herramientas de control parental

Función	Descripción	Algunas Herramientas
Filtrado de contenidos	Mediante diferentes sistemas, bloquea el acceso del menor a ciertos contenidos inapropiados (habitualmente de connotación sexual o violenta).	Norton Family Screen Time Family Link Family Time Securekids Qustodio
Control de tiempo	Emite alertas o interrumpe la navegación al alcanzar determinada hora o límite de tiempo.	
Supervisión de actividad	Genera informes con el historial de navegación, búsquedas o reproducción multimedia.	
Geolocalización	Sigue la posición actual y el recorrido anterior del dispositivo.	Family Link Family Time Securekids Qustodio
Protección de la configuración	Evita modificaciones no deseadas de los ajustes de control parental.	Family Link

Fuente: INCIBEGUIACP. [Sitio web]. Guía de herramientas de control parental. Madrid [Consulta: 24 de agosto de 2021]. Disponible en: https://files.incibe.es/is4k/is4k_guia_controles_parentales.pdf

Explíquele al menor a qué se puede exponer si acepta solicitudes de amistad de personas desconocidas, infórmese e infórmelo de qué puede ser víctima de grooming, sexting, pornografía infantil, o ciberacoso.

Adviértale que, si comparte fotos personales o inapropiadas por redes sociales, existen ciberdelincuentes que atacan y extorsionan niños llevándolos a realizar cosas inapropiadas.

Asegúrese de que el menor cuando esté usando redes sociales no lo haga en lugares encerrados como: su habitación. Es importante que lo haga donde pueda ser supervisado por alguien.

No le dé vía libre al menor con el uso de redes sociales, procure tener control por medio de reglas y horarios establecidos como familia.

Ayude al menor a establecer las opciones de privacidad de las redes sociales de forma correcta, con el objetivo que las publicaciones realizas por el menor no queden públicas a todo el mundo, sino solo puedan ser vistas por las personas que él decida.

El uso responsable y supervisado de redes sociales en menores permite tener un control de protección sobre los menores, a continuación, algunos puntos adicionales a tener en cuenta:

- No aceptar solicitudes de amistad de personas desconocidas.
- No publicar información personal o sensible en redes, los atacantes se valen de todo lo que se publica.
- Desconfíe de contactos que soliciten imágenes sexuales o comprometedoras por la red.
- Monitoree el uso de internet de sus hijos.

- Las video llamadas pueden ser peligrosas procure realizarlas solo con contactos conocidos y confiables.
- No programe citas personales con contactos que solo conoce por la red, puede ser muy peligroso.
- Tenga en cuenta que no todo lo que se encuentra en internet es cierto.

El uso de Internet y las nuevas tecnologías ha tomado un papel importante en las actividades cotidianas que realizan las personas, en especial en los menores de edad, puesto que éstos cuentan con las tecnologías desde el principio de sus vidas. Como reflexión final, la solución no es prohibirles a los menores de edad el uso de las tecnologías, sino enseñarles cómo usarlas, cómo detectar sus peligros y cómo evitarlos. La responsabilidad se acentúa en educar el uso razonable, responsable y saludable de las tecnologías, previniendo las consecuencias de un mal uso, y los protagonistas de esta tarea educativa son los padres y educadores. Esta tarea educativa sólo se podrá lograr si se mantiene un diálogo permanente, claro, sensato y preciso con los menores de edad, se les debe poner al tanto de las bondades de las tecnologías, así como de las intenciones ocultas y maliciosas de personas que la usan.

En la sección 9.1, se comparte un plan de sensibilización que busca que docentes, familias, menores y adolescentes promuevan una convivencia digital respetuosa y comprendan la importancia de estar construyendo la identidad de los niños y niñas en un espacio público, así como la concientización y lograr un uso responsable de las tecnologías de información y comunicación

6 CONCLUSIONES

Internet y las Tecnologías de la Información y Comunicación han presentado las redes sociales como mecanismos de interrelación con muchos beneficios, entre los que destacan la capacidad de interactuar en tiempo real, compartir archivos multimedia (vídeos, mensajes o fotos) de forma sencilla, reducir el distanciamiento geográfico, entre otros. No obstante, también han conllevado riesgos y amenazas, pues el acceso a la información personal es más fácil.

Las redes sociales atraen la atención de los menores de edad, sumado a que al ser éstos, nativos digitales, desde el principio de su vida ya interactúan con tecnologías. Muchos infantes navegan en Internet y redes sociales como fuente de esparcimiento o búsqueda de conocimiento, sin embargo, también se pueden convertir en orígenes de riesgo, pues la pornografía infantil, acoso y bullying son una pequeña muestra de los peligros que oculta el ciberespacio.

Es muy importante que los padres y acudientes de los menores tengan claro los riesgos a los que se ven expuestos los menores cuando acceden a internet sin acompañamiento y sin ningún tipo de supervisión. La respuesta no es prohibirle el uso de redes sociales o impedir el uso de las tecnologías a los menores de edad, sino en enseñarles cómo usarlas y cómo detectar y evitar los peligros.

Es función primordial de los padres y educadores enseñar a los infantes y adolescentes el uso responsable de Internet, las redes sociales y las tecnologías, concientizar de los contenidos multimedia compartidos y de la información publicada. Una metodología de enseñanza y aprendizaje bidireccional permitirá al menor de edad auto educarse y manejar con responsabilidad las tecnologías generando conocimiento significativo.

El uso de redes sociales en menores de edad debe ser supervisado y controlado por un adulto, el cual se encuentre informado y pueda hacer un seguimiento adecuado de lo que realiza el menor en la red. Este monitoreo sobre el uso saludable de las redes sociales debe ser periódico debido a los acelerados cambios tecnológicos diarios, con el propósito que a nivel familiar se brinden recomendaciones preventivas.

Aceptar solicitudes de amistad de personas desconocidas es uno de los riesgos más relevantes a los que se ven expuestos los menores en las redes sociales. Así que los perfiles en redes sociales son configurables con el objetivo que sólo personas conocidas puedan acceder a la información e imágenes que son publicadas.

Se determina que las técnicas más usadas por los delincuentes por medio de internet y las redes sociales son: el grooming, la pornografía y delitos sexuales, esto teniendo en cuenta los diferentes artículos investigados y los diferentes titulares de noticias que día a día se ven.

7 RECOMENDACIONES

Para evitar que los menores sean víctimas de ingeniería social por redes sociales en indispensable que tanto los menores como los padres o acudientes, sean conscientes de que existen riesgos de los cuales pueden llegar a ser víctimas, como lo son: el grooming, ciberacoso o delitos sexuales.

Seguir las recomendaciones y los términos y condiciones que tiene las redes sociales al momento de crear una red social es importante para el uso adecuado de las mismas.

Evite compartir información personal como lo es: dirección de residencia, teléfono, lugares frecuentados, imágenes con el uniforme del colegio, imágenes intimas, ya un ciberdelincuente puede usar esta información de manera delictiva.

Si alguien establece contacto por medio de una red social con el menor haciendo propuestas indebidas o solicitando información privada, bloquee la persona y denuncie la cuenta.

8 BIBLIOGRAFÍA

ALCALDÍA BOGOTÁ. [Sitio web]. Proyecto de Acuerdo 470 DE 2017. Bogotá, Colombia. [Consulta: 19 de marzo de 2021]. Disponible en: https://www.alcaldiabogota.gov.co/sisjur/adminverblobawa?tabla=T_NORMA_ARCHIVO&p_NORMFIL_ID=9369&f_NORMFIL_FILE=X&inputfileex. (s.f.).

AMBIT, Spoofing. Qué es y cómo evitarlo. [En línea]. España: Ambit, 2019. [Citado Mayo-2020]. Disponible en internet: https://www.ambit-bst.com/blog/spoofing-que-es-y-c%C3%B3mo-evitarlo. (s.f.).

ANDALUCÍA ES DIGITAL. Seguridad qué es la ingeniería social y cómo protegerse de sus ataques. [En línea] 2018. [Citado Abril-2020]. Disponible en internet: https://www.blog.andaluciaesdigital.es/que-es-la-ingenieria-social-y-como-protegerse/. (s.f.).

ÁVILA SILVA, J. (2018). Los menores víctimas de la ciberdelincuencia. Medidas preventivas en el ámbito internacional. Advocatus, 15(31), 79-90. https://doi.org/10.18041/0124-0102/a.31.5223. (s.f.).

BANCO MUNDIAL. [Sitio web]. Personas que usan Internet (% de la población). Washington [Consulta: 27 de febrero de 2021]. Disponible en: https://datos.bancomundial.org/indicador/IT.NET.USER.ZS. (s.f.).

BRANCH. [Sitio web]. Estadísticas de la situación digital de Colombia en el 2019 y 2020. Bogotá D.C. [Consulta: 03 de marzo de 2021]. Disponible en: https://branch.com.co/marketing-digital/estadisticas-de-la-situacion-digital-de-colombia-en-el-2019-y-2020. (s.f.).

BLURADIO. [Sitio web]. Desde 2019 a la fecha van más de 4.000 denuncias por pornografía infantil en Colombia. Bogotá D.C. [Consulta: 04 de marzo de 2021]. Disponible en: https://www.bluradio.com/politica/desde-2019-a-la-fecha-van-mas-de-4-000-denuncias-por-pornografia-infantil-en-colombia.

CANALRCN. Atención padres: el grooming y sus riesgos para los niños en internet. [En línea]. Colombia: Canal RCN. 2019. [Citado Abril-2020]. Disponible en internet: https://noticias.canalrcn.com/tecnologia/atencion-padres-el-grooming-y-sus-riesgos-para-lo. (s.f.).

CCIT. [Sitio web]. Tendencias, Cibercrimen en Colombia 2019 - 2020. Bogotá D.C. [Consulta: 04 de marzo de 2021]. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf. (s.f.).

CEFIRE. [Sitio web]. Fases del grooming. Valencia, España. [Consulta: 19 de marzo de 2021]. Disponible en: http://cefire.edu.gva.es/pluginfile.php/1364209/mod_resource/content/10/51_fases_del_grooming.html. (s.f.).

CODAJIC. [Sitio web]. El Estado Mundial de la Infancia 2017: Niños en un mundo digital. El Bolson, Rio Negro [Consulta: 7 de marzo de 2021]. Disponible en: http://www.codajic.org/node/2861. (s.f.).

CONFIRMA SISTEMAS, Vishing: el peligroso método de fraude bancario que no todos conocen. [En línea]. España: Confirma Sistemas, 2018. [Citado Mayo-2020]. Disponible en internet: https://www.confirmasistemas.es/es/contenidos/canal-basics/vishing-el-peligro. (s.f.).

COPMADRID. [Sitio web]. Estrategias de persuasión en grooming online de menores: un análisis cualitativo con agresores en prisión. Madrid. [Consulta: 19 de marzo de 2021]. Disponible en: https://journals.copmadrid.org/pi/art/j.psi.2017.02.001. (s.f.).

CSIRT. [Sitio web]. ¿Qué es Doxxing? Bogotá D.C. [Consulta: 7 de marzo de 2021]. Disponible en: https://cc-csirt.policia.gov.co/noticias/2020/4to-trimestre/que-es-doxxing. (s.f.).

DEEPWEBIUPSM, Las técnicas de la Ingeniería Social y cómo nos afecta. [En línea]. Deepwebiupsm, 2016. [Citado Mayo-2020]. Disponible en internet: https://deepwebiupsm.wordpress.com/2016/06/23/las-tecnicas-de-la-ingenieria-social-y-como-nos-afecta/. (s.f.).

DEFO, Julio, Grooming. [En línea]. Seguridad TIC y menores de edad para educadores. Octubre 2015. [Citado Octubre-2020]. Disponible en internet: https://seguridadticymenoresdeedad.wordpress.com/2015/10/12/grooming/. (s.f.).
EcuRED. Ingeniería social. [En Linea]. Cuba: EcuRED. [Citado Noviembre -2020]. Disponible en internet: https://www.ecured.cu/Ingenier%C3%ADa_social#T.C3.A9cnicas_pasivas. (s.f.).

EDUCAREX. [Sitio web]. Suplantación de identidad. Extremadura, España. [Consulta: 12 de abril de 2021]. Disponible en: https://emtic.educarex.es/nativosdigitales_materiales/pildoras_familias/rrssyadolescentes/suplantacin_de_identidad.html. (s.f.).

EL CONGRESO DE COLOMBIA. LEY 1098 DE 2006. [En línea]. Colombia: oas.org. 2006. [Citado Abril-2020]. Disponible en internet: https://www.oas.org/dil/esp/Codigo_de_la_Infancia_y_la_Adolescencia_Colombia.pdf. (s.f.).

EL CONGRESO DE COLOMBIA. Ley 1273 De 2009. [En línea]. Colombia: secretariasenado. 2009. [Citado Abril-2020]. Disponible en internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html. (s.f.).

EL CONGRESO DE COLOMBIA. Ley 1336 de 2009. [En línea]. Colombia: icbf. 2009. [Citado Abril-2020]. Disponible en internet: https://www.icbf.gov.co/cargues/avance/docs/ley_1336_2009.htm. (s.f.).

EL CONGRESO DE COLOMBIA. Ley 1878 de 2018. [En línea]. Colombia: icbf. 2018. [Citado Abril-2020]. Disponible en internet: https://www.icbf.gov.co/cargues/avance/docs/ley_1878_2018.htm. (s.f.).

EL CONGRESO DE COLOMBIA. Ley 679 de 2001. [En línea]. Colombia: icbf. 2001. [Citado Abril-2020]. Disponible en internet: https://www.icbf.gov.co/cargues/avance/docs/ley_0679_2001.htm. (s.f.).

EL TIEMPO. Casi 4 denuncias al día se reciben por casos de explotación de menores. [En línea]. Colombia: El tiempo. 2019. [Citado Mayo -2020]. Disponible en internet: https://www.eltiempo.com/justicia/delitos/claves-que-pedofilos-usan-para-ocultar-pornog. (s.f.).

EL TIEMPO. El 32% de los niños y adolescentes conocen personas por internet. [En línea]. Colombia: El tiempo. 2018. [Citado Mayo -2020]. Disponible en internet: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/principales-riesgos-para-los-menores. (s.f.).

EL TIEMPO. ¿Hay delitos en el 'sexting'? Estas son las aclaraciones de la Corte. [En línea] 2019. [Citado Abril-2020]. Disponible en internet: https://www.eltiempo.com/justicia/cortes/cuales-son-los-delitos-sexuales-en-internet-segun-la-corte-suprema-4299. (s.f.).

EL TIEMPO. [Sitio web]. Casi 4 denuncias al día se reciben por casos de explotación de menores. Bogotá, Colombia. [Consulta: 19 de marzo de 2021]. Disponible en: https://www.eltiempo.com/justicia/delitos/claves-que-pedofilos-usan-para-ocultar-pornografia-i. (s.f.).

ELAINE, ¿Qué es doxing? [En línea]. onretrieval, 2017. [Citado Mayo-2020]. Disponible en internet: https://onretrieval.com/que-es-doxing/. (s.f.).

EXTRA Tecnología, Las etapas del ciberbullying. [En línea]. Agenda de la empresa. Abril 2016. [Citado Octubre-2020]. Disponible en internet: https://www.agendaempresa.com/71839/las-etapas-del-ciberbullying/. (s.f.).

FLOREZ, Jorge F. Ciberacoso sexual de menores, grooming y sextorsión. [En línea]. Colombia: dialogando. 2019. Citado Abril-2020]. Disponible en internet:

https://dialogando.com.co/ciberacoso-sexual-de-menores-grooming-y-sextorsion/. (s.f.).

GOBIERNO DE CANARIAS. [Sitio web]. Sexting. Canarias. [Consulta: 19 de marzo de 2021]. Disponible en: https://www3.gobiernodecanarias.org/medusa/ecoescuela/seguridad/riesgos-asociados-al-uso-de-las-tecnologias/sexting/. (s.f.).

HERJAVEC GROUP. [Sitio web]. 2019 Official Annual Cybercrime Report. Los Ángeles. [Consulta: 03 de marzo de 2021]. Disponible en: https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf. (s.f.).

IABCOLOMBIA. [Sitio web]. El desconocimiento, la silenciosa complicidad y el avance del grooming en América Latina. Bogotá, Colombia. [Consulta: 19 de marzo de 2021]. Disponible en: https://www.iabcolombia.com/el-desconocimiento-la-silenciosa-complicidad-. (s.f.).

IGLESIAS, Pablo F. MUNDOHACKER: LOS 6 PRINCIPIOS BÁSICOS DE LA INGENIERÍA SOCIAL. . [En línea]. Pabloyglesias. . [Citado Abril-2020]. Disponible en internet: https://www.pabloyglesias.com/mundohacker-ingenieria-social. (s.f.).

INCIBE, Instituto Nacional de Ciberseguridad, Glosario de términos de ciberseguridad. [En línea]. España: Incibe, 2017. [Citado Mayo-2020]. Disponible en internet: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad. (s.f.).

INCIBEGUIACP. [Sitio web]. Guía de herramientas de control parental. Madrid [Consulta: 24 de agosto de 2021]. Disponible en: https://files.incibe.es/is4k/is4k_guia_controles_parentales.pdf

INTECO. [Sitio web]. Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian? León [Consulta: 7 de marzo de 2021]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian. (s.f.).

KASPERSKY. Ingeniería social: definición. [En línea] Colombia: latam.kaspersky. [Citado Abril-2020]. Disponible en internet: https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering. (s.f.).

LISA. [Sitio web]. Guía Práctica contra la Ingeniería Social. Madrid [Consulta: 8 de marzo de 2021]. Disponible en: https://www.lisainstitute.com/blogs/blog/guia-practica-ingenieria-social. (s.f.).

MIN. [Sitio web]. Cibercrimen. Buenos Aires [Consulta: 7 de marzo de 2021]. Disponible en: https://www.iri.edu.ar/wp-content/uploads/2016/11/syd15_entrevista_corbino_cibercrimen.pdf. (s.f.).

MOLANO, Natalia. Colombia es el tercer país con más ataques de ingeniería social en América Latina. [En línea] Colombia: larepublica, 2019. [Citado Abril-2020]. Disponible en internet: https://www.larepublica.co/empresas/colombia-es-el-tercer-pais-con-mas. (s.f.).

MOLINA, María P. Guía de sensibilización sobre Convivencia Digital. [En línea]. Argentina: Unicef, 2017. [Citado Abril-2020]. Disponible en internet: https://www.unicef.org/argentina/sites/unicef.org.argentina/files/2018-04/COM-Guia_ConvivenciaDigital_ABR. (s.f.).

NORTONLIFELOCK. ¿Qué es la ingeniería social? [En línea]. Norton. [Citado Abril-2020]. Disponible en internet: https://co.norton.com/internetsecurity-emerging-threats-what-is-social-engineering.html. (s.f.).

OAS. [Sitio web]. Ley 1098 De 2006. Washington. [Consulta: 10 de marzo de 2021]. Disponible en: https://www.oas.org/dil/esp/Codigo_de_la_Infancia_y_la_Adolescencia_Colombia.pdf. (s.f.).

PASTOR, Javier. Kevin Mitnick, genio o figura de uno de los hackers más famosos de la historia. [En línea] xataka, 2018. [Citado Abril-2020]. Disponible en internet: https://www.xataka.com/seguridad/kevin-mitnick-genio-o-figura-de-uno-de-los-hackers-mas-f. (s.f.).

PCMAG. [Sitio web]. As Phishing and Similar CyberCrimes Increase, Are Victims Better at Threat Assessment?. New York, USA. [Consulta: 26 de marzo de 2021]. Disponible en: https://www.pcmag.com/news/as-phishing-and-similar-cybercrimes-increase-are-victims-. (s.f.).

PISCITELLI, Emiliano. Ingeniería social (Parte 1). [En línea]. Argentina: marketerslatam, 2017. [Citado Mayo-2020]. Disponible en internet: https://www.marketerslatam.com/digital/articulos-marketing-digital/ingenieria-social/. (s.f.).

PROTECCIONONLINE. Los riesgos en Internet: Ciberacoso, grooming, sexting, pornografía. [En línea]. Protecciononline [Citado en Mayo -2020]. Disponible en internet: . (s.f.).

PUCE. [Sitio web]. Delitos Informáticos: Generalidades. Quito [Consulta: 7 de marzo de 2021]. Disponible en: https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf, p. 10. (s.f.).

RIOS, Estefanía C. HUELLA DIGITAL: DOXING. [En Línea]. Crimeandlaw. 2018. [Citado Abril-2020]. Disponible en internet: https://crimeandlawblog.com/2018/05/24/huella-digital-doxing/. (s.f.).

RODRIGUEZ RINCON, Ellien Yulieth, Metodologías de Ingeniería Social. [En línea]. Madrid - España Universidad Oberta de Cataluña. Junio. [Citado Octubre-2020]. Disponible en internet: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/81255/6/jrodriguezr. (s.f.).
SANDOVAL, Edgar Jair. INGENIERÍA SOCIAL: CORROMPIENDO LA MENTE HUMANA. . [En línea]. Mexico: Revista Seguridad. [Citado Abril-2020]. Disponible en internet: https://revista.seguridad.unam.mx/numero-10/ingenier%C3%AD-social-corrompiendo-la-mente-humana. (s.f.).

SCIELO HERNÁNDEZ. [Sitio web]. Tecnología y pornografía infantil en Colombia, 2013-2015: interpretación desde un enfoque victimológico. Bogotá, Colombia. [Consulta: 19 de marzo de 2021]. Disponible en: http://www.scielo.org.co/scielo.php?script=sci_arttex. (s.f.).

SECSENADO. [Sitio web]. Ley 1273 de 2009. Bogotá D.C. [Consulta: 15 de abril de 2020]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html. (s.f.).

SECURITYBOULEVARD. [Sitio web]. The Rise of Phishing Attacks: P.S. ILoveYou. New York, USA. [Consulta: 26 de marzo de 2021]. Disponible en: https://securityboulevard.com/2020/06/the-rise-of-phishing-attacks-p-s-iloveyou/. (s.f.).

STATISTA. [Sitio web]. What do you think are the most common online risks that you and other children your age had been exposed to?. [Consulta: 19 de marzo de 2021]. Disponible en: https://www.statista.com/statistics/1167050/romania-online-risks-that-chil. (s.f.).

TIC BOGOTA. [Sitio web]. ¡Ojo con sus niños! Cuídelos de los crímenes cibernéticos. Bogotá D.C. [Consulta: 05 de marzo de 2021]. Disponible en: https://tic.bogota.gov.co/noticias/¡ojo-sus-niños-cuídelos-los-crímenes-cibernéticos. (s.f.).

TICARTE. [Sitio web]. ¿Qué es footprinting y fingerprinting?. Vancouver, Canadá. [Consulta: 12 de abril de 2021]. Disponible en: https://www.ticarte.com/contenido/que-es-footprinting-y-fingerprinting. (s.f.).

TIGO, Une – EAFIT Navegando entre las oportunidades y los riesgos en los escenarios digitales. [En línea] Colombia: Tigo-Une, 2018. [Citado Abril-2020]. Disponible en internet: http://tigo-une.com/contigoconectados/img/press-book-tigo-une.pdf. (s.f.).

TILOMOTION. [Sitio web]. ¿Cuál es la edad mínima para abrirte una cuenta en una Red Social? Madrid [Consulta: 7 de marzo de 2021]. Disponible en: https://www.tilomotion.com/blog/cual-es-la-edad-minima-para-abrirte-una-cuenta-en-una-red-social/. (s.f.).
UNAM. [Sitio web]. Ingeniería Social: corrompiendo la mente humana. México D.F. [Consulta: 7 de marzo de 2021]. Disponible en: https://revista.seguridad.unam.mx/numero-10/ingenierí-social-corrompiendo-la-mente-humana. (s.f.).

WELIVESECURITY. Glosario. [En Línea]. Welivesecurity. [Citado Abril-2020]. Disponible en internet: https://www.welivesecurity.com/la-es/glosario. (s.f.).

XATAKA. [Sitio web]. Qué hacer si alguien te chantajea a ti o a tus hijos con la publicación de fotos y material íntimo. Madrid. [Consulta: 12 de abril de 2021]. Disponible en: https://www.xataka.com/legislacion-y-derechos/que-hacer-alguien-te-chantajea-a. (s.f.).

9 ANEXOS

9.1 PLAN DE SENSIBILIZACIÓN

ID	Sensibilizaciones	Temática	Mins	Grados
1	Internet con los menores riesgos. Guía para madres y padres	Prevención de riesgos, Internet para menores, riesgos en redes sociales, grooming, ciberacoso, ciberbullying, privacidad	60	Escolar Bachillerato
2	Ciberbullying	Prevención de riesgos en Internet y telefonía móvil o celular en menores, uso seguro y responsable, ciudadanía digital, ciberbullying, privacidad	60	Escolar Bachillerato
3	Sexting, Grooming	Viralización de imágenes y contenidos inadecuados, recomendaciones, cuidados y recursos para la denuncia y asesoramiento.	60	Escolar Bachillerato
4	Diálogo y concientización	Configurar la privacidad en las redes sociales, pensar antes de publicar, colocar contraseña en los celulares u otros dispositivos, controlar qué información personal circula en internet.	60	Escolar Bachillerato
5	Herramientas de control parental	Apoyarán en el aprendizaje de los menores, limitando las funciones y el alcance de sus dispositivos cuando se conectan a Internet.	120	Escolar Bachillerato

6	Protocolo de actuación escolar ante el ciberbullying	Ciberbullying, ciberacoso, privacidad, protección de datos personales, uso de la imagen, webcam o cámara web, usos positivos de la red, grooming, sexting, sextorsion	120	Escolar Bachillerato

Fecha de Realización:	01/10/2021
Programa:	Especialización en seguridad informática
Línea de Investigación:	Infraestructura tecnológica y seguridad en redes
Título:	Técnicas de ingeniería social empleadas en Colombia por los ciberdelincuentes a menores de edad
Autor(es):	Soler Páez Leidy Tatiana
Palabras Claves:	Adolescente, ataque, delincuente, delito, extorsión, ingeniería social, internet, niño, pornografía infantil, red social, seguridad, tecnología, víctima
Descripción:	Hoy en día es común ver noticias y encontrarse con titulares de menores víctimas de extorsión por redes sociales, todo por el uso inadecuado y no supervisado del internet y las redes sociales. La mayoría menores no tienen precaución y desconocen de los peligros existentes en internet, algunos menores tienen acceso a internet de forma libre sin un adulto que conozca en realidad los sitios visitados por el menor o sus amigos virtuales en las diferentes redes sociales. Por esta razón con este trabajo se mostrara el comportamiento de los menores en las redes sociales, buscando que el lector del mismo logre saber los peligros del uso inadecuado y no supervisado de las redes sociales y al mismo tiempo conozca las diferentes técnicas que un ciberdelincuente puede usar para llegar a extorsionar a su víctima.

Fuentes bibliográficas destacadas:

IGLESIAS, Pablo F. MUNDOHACKER: LOS 6 PRINCIPIOS BÁSICOS DE LA INGENIERÍA SOCIAL. Disponible en internet: https://www.pabloyglesias.com/mundohacker-ingenieria-social

MOLANO, Natalia. Colombia es el tercer país con más ataques de ingeniería social en América Latina. Disponible en internet:

<table>
<tr><td colspan="2">https://www.larepublica.co/empresas/colombia-es-el-tercer-pais-con-mas-ataques-de-ingenieria-social-en-america-latina-2928973

ANDALUCÍA ES DIGITAL. SEGURIDAD QUÉ ES LA INGENIERÍA SOCIAL Y CÓMO PROTEGERSE DE SUS ATAQUES. Disponible en internet: https://www.blog.andaluciaesdigital.es/que-es-la-ingenieria-social-y-como-protegerse

Deepwebiupsm, Las técnicas de la Ingeniería Social y cómo nos afecta. Disponible en internet: https://deepwebiupsm.wordpress.com/2016/06/23/las-tecnicas-de-la-ingenieria-social-y-como-nos-afecta

DEFO, Julio .Seguridad TIC y menores de edad para educadores. Octubre Disponible en internet: https://seguridadticymenoresdeedad.wordpress.com/2015/10/12/grooming

FLOREZ, Jorge F. CIBERACOSO SEXUAL DE MENORES, GROOMING Y SEXTORSIÓN. Disponible en internet: https://dialogando.com.co/ciberacoso-sexual-de-menores-grooming-y-sextorsion</td></tr>
<tr><td>Contenido del documento:</td><td>En la actualidad existen diferentes técnicas para hacer ingeniería social, algunas técnicas son: redes sociales, abuso de confianza, phishing, llamadas telefónicas, Vishing. “El uso de estas técnicas tiene como finalidad obtener información confidencial y buscar beneficios propios. Los delincuentes logran su objetivo aprovechándose del desconocimiento y la falta de prevención de la sociedad al momento de compartir información personal de forma física o hacer publicaciones en internet”.
Es muy común ver noticias y encontrarse con titulares, como un adolecente o niño ha sido víctima de extorsión por redes sociales, todo por la falta de precaución y desconocimiento de los peligros existentes en internet. Muchos menores tienen acceso a internet sin la supervisión de un adulto que conozca en realidad los sitios visitados por el menor o sus amigos virtuales en las diferentes redes.</td></tr>
</table>

	Por esta razón con este trabajo se mostrará el comportamiento de los delincuentes frente a los menores en las redes sociales; buscando que el lector del mismo logre saber los peligros del uso inadecuado y no supervisado de las redes sociales y al mismo tiempo conozca las diferentes técnicas que un ciberdelicuente puede usar para llegar a extorsionar a su víctima.
Marco Metodológico:	Se citaran diferentes artículos e investigaciones, además se evidenciará el estado actual de los incidentes de este tipo en Colombia, buscando promover en los menores, en sus propios padres o responsables el uso adecuado de las redes.
Conceptos adquiridos :	Se logró conocer y profundizar en las diferentes técnicas de ingeniería social a las que se puede ver expuesto un menor en redes sociales. Se determina que las técnicas más usadas por los delincuentes por medio de internet y las redes sociales son el grooming, la pornografía y delitos sexuales, esto teniendo en cuenta los diferentes artículos investigados y los diferentes titulares de noticias que día a día se ven. Se conocieron las diferentes leyes que protegen a los niños y adolescentes, por medio de las cuales son castigados y condenados aquellos que comentan actos de explotación, pornografía y turismo sexual con menores. Además de las leyes que castigan y condenan los delitos informáticos en Colombia.
Conclusiones:	Internet y las Tecnologías de la Información y Comunicación han presentado las redes sociales como mecanismos de interrelación con muchos beneficios, entre los que destacan la capacidad de interactuar en tiempo real, compartir archivos multimedia (vídeos, mensajes o fotos) de forma sencilla, reducir el distanciamiento geográfico, entre otros. No obstante, también han conllevado riesgos y

	amenazas, pues el acceso a la información personal es más fácil. Las redes sociales atraen la atención de los menores de edad, sumado a que al ser éstos, nativos digitales, desde el principio de su vida ya interactúan con tecnologías. Muchos infantes navegan en Internet y redes sociales como fuente de esparcimiento o búsqueda de conocimiento, sin embargo, también se pueden convertir en orígenes de riesgo, pues la pornografía infantil, acoso y bullying son una pequeña muestra de los peligros que oculta el ciberespacio. Es muy importante que los padres y acudientes de los menores tengan claro los riesgos a los que se ven expuestos los menores cuando acceden a internet sin acompañamiento y sin ningún tipo de supervisión. La respuesta no es prohibirle el uso de redes sociales o impedir el uso de las tecnologías a los menores de edad, sino en enseñarles cómo usarlas y cómo detectar y evitar los peligros. Es función primordial de los padres y educadores enseñar a los infantes y adolescentes el uso responsable de Internet, las redes sociales y las tecnologías, concientizar de los contenidos multimedia compartidos y de la información publicada. Una metodología de enseñanza y aprendizaje bidireccional permitirá al menor de edad auto educarse y manejar con responsabilidad las tecnologías generando conocimiento significativo.