ANÁLISIS DE LOS RIESGOS DE SEGURIDAD A LOS CUALES ESTÁN EXPUESTOS LOS NIÑOS Y NIÑAS CON EL USO DE LA RED SOCIAL FACEBOOK Y CÓMO ESTOS PODRÍAN REDUCIRSE

JULIÁN ANDRÉS ARANGO NIÑO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2021

ANÁLISIS DE LOS RIESGOS DE SEGURIDAD A LOS CUALES ESTÁN EXPUESTOS LOS NIÑOS Y NIÑAS CON EL USO DE LA RED SOCIAL FACEBOOK Y CÓMO ESTOS PODRÍAN REDUCIRSE

JULIÁN ANDRÉS ARANGO NIÑO

Proyecto de Grado – Monografía presentado para optar por el título de especialista en seguridad informática

Edgar Mauricio López
Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2021

NOTA DE ACEPTACIÒN

Firma del presidente del jurado

Firma del jurado

Firma del jurado

Bogotá., 27 de octubre de 2.021

DEDICATORIA

Este trabajo va dedicado a Dios por todo lo que me ha dado día a día si no, que todo lo que hagamos, lo hagamos con amor y dedicación, con disciplina y constancia, siempre nos ha dicho que realicemos lo que nos hace realmente feliz y que siempre demos lo mejor de sí.

A mi padre que nos ha enseñado que debemos trabajar día a día y luchar siempre por que nada nos lo regalan.

También a mis hermanos y a mi hermana que no solo han sido mi gran compañía si no mi apoyo incondicional, que siempre con ejemplo nos corregimos y nos aconsejamos los unos a los otros.

También a los profesores y a las directrices de la universidad que a lo largo de mi carrera gracias a ellos tengo el conocimiento hoy en día y puedo llevar en el alto el nombre de la universidad.

AGRADECIMIENTOS

Este trabajo monográfico tiene un especial agradecimiento a los tutores y directivas de la Universidad Nacional Abierta y a Distancia UNAD, por habernos guiado en este arduo proceso con gran paciencia, una increíble aptitud, flexibilidad e interés en enseñarnos y ayudarnos a culminar nuestro trabajo.

CONTENIDO

pág.

INTRODUCCIÓN 13
1. DEFINICIÓN DEL PROBLEMA 15
1.1 ANTECEDENTES DEL PROBLEMA 15
1.2 FORMULACIÓN DEL PROBLEMA 17
2 JUSTIFICACIÓN 18
3 OBJETIVOS 20
3.1 OBJETIVO GENERAL 20
3.2 OBJETIVOS ESPECÍFICOS 20
4 MARCO REFERENCIAL 21
4.1 MARCO TEÓRICO 21
4.2 MARCO CONTEXTUAL 24
4.3 MARCO CONCEPTUAL 31
4.4 MARCO LEGAL 33
5 DISEÑO METODOLÓGICO 35
5.1 Unidad de análisis 35
5.1.1 Población y Muestra 35
5.2 Estudio Metodológico 35
5.3 Etapas de la investigación 36
5.4 Línea de investigación 37
5.5 Instrumentos de recolección de datos 38
6 RESULTADOS Y DISCUSIÓN 39
7 BIBLIOGRAFÍA 58

LISTA DE TABLAS

Pág.

Tabla 1. Técnica de ingeniería social: Grooming 39
Tabla 2. Técnica de ingeniería social: Ciber inducción al daño físico y mental 41
Tabla 3. Técnica de ingeniería social: Sextorsión 45
Tabla 4. Técnica de ingeniería social: Cyberbullying/ Ciberacoso.....45

LISTA DE FIGURAS

Pág.

Figura 1. Redes sociales 26
Figura 2. Reto “La ballena azul” 43
Figura 3. Victimas por la ballena azul en Colombia.....44
Figura 4. Edades permitidas para acceder a redes sociales 47
Figura 5. Porcentaje exposición niños y niñas 48

GLOSARIO

BAITING: Colocar memorias externas con malware instalado.

CHAT: Participar con una o más personas, a través de Internet, en una conversación en tiempo real, generalmente como una serie de intercambios breves de texto en una aplicación específica, como mensajería instantánea, o mediante el uso de imágenes, voz, video o alguna combinación de estos.

CIBERINTIMIDACIÓN Actividad relacionada con la utilización de la Internet para hacer daño o asustar a otra persona, especialmente con el envío de mensajes desagradables.

CIBERBULLING: Acoso a través de internet.

CIBERSTALKER: Se da por medio del uso de algunas tecnologías, principalmente Internet. Se caracteriza por el seguimiento e investigación constante de información sobre una persona o empresa. Es un acto premeditado, repetitivo, obsesivo, y, sobre todo, no deseado.

CIBERDELINCUENCIA: Actividades delictivas que se llevan a cabo utilizando Internet.

DELITO: Acción en contra de la ley.

DEEP WEB: Internet profunda es el contenido de la red que no está a la vista de todos los usuarios.

DUMPSTER DIVING: Desechar documentos con información sensible de forma insegura.

GROOMING: Cuando un depredador sexual o de otro tipo prepara el escenario para abusar de otro, como un niño u otra persona (como en el caso del sexo y la teoría de la trata de personas).

INGENIERÍA SOCIAL: Obtener información mediante técnicas de manipulación de las personas.

PHARMING: Suplantación de páginas web, llevando al usuario a páginas falsas.

PHISHING: Estafa a través de correos electrónicos.

PRETEXTING: Es una forma de ingeniería social en la que un individuo obtiene información privilegiada para luego llamar a la persona y robar información.

SEXTING: Comunicación por texto con contenido sexual.

SHOULDER SURFING: Consiste en utilizar técnicas de observación directa, como mirar por encima del hombro de alguien, para obtener información.

SÍNDROME DEL MENSAJE MÚLTIPLE: Impulso por entablar múltiples chats o redes sociales.

SMISHING: Enlaces o correos que envían a páginas falsas.

SUPLANTACIÓN: Quitar a una persona su sitio de manera fraudulenta, ocupando su cargo o posición, o asumiendo sus funciones.

TAILGAITING: Un atacante puede evadir controles de acceso físico como puertas electrónicas e ingresar a una organización sin autorización.

RESUMEN

El objetivo de la investigación, es analizar los riesgos de seguridad a los cuales están expuestos los niños y niñas, a través de los diferentes métodos de ingeniería social con el uso de Facebook y la forma en que estos podrían reducirse. Metodológicamente, se trata de una investigación documental, a través de la cual se busca profundizar respecto a los principales riesgos existentes con el uso frecuente e indiscriminado por parte de los niños y niñas de la red social Facebook, en muchos casos con la inobservancia y falta de guía de un adulto responsable, lo cual es altamente aprovechado por delincuentes informáticos, logrando de esta manera dar a conocer la aplicabilidad de la seguridad informática en estas situaciones, así como de las posibles prácticas de prevención por parte de adultos que pueden ayudar a reducir estos riesgos.

Se obtuvo como resultado que desde la seguridad informática es posible hacer uso de los denominados programas de “Parental control”, a través de ellos es posible limitar el acceso de los niños a todos los contenidos que los padres consideren inapropiados, algunas de las herramientas más completas de este tipo, utilizadas actualmente para controlar y educar los hábitos de los menores de edad en internet son: Qustodio, ESET Parental Control, Web Filter PC, Amigo Control Parental, Kidbox.

Se concluye que es un hecho que la seguridad informática puede aplicarse para intentar reducir los riesgos en el uso de Facebook por parte de los niños y niñas, pero para lograr esto, es esencial que los padres, docentes y adultos responsables de supervisar a los niños, adquieran conocimientos útiles sobre las medidas preventivas que pueden aplicarse para prevenir o minimizar estos riesgos.

Se recomienda que, desde el Ministerio de Tecnologías de la Información y Comunicaciones, es necesario concientizar a los padres a través de la implementación de políticas públicas enfocadas en la educación de la sociedad en general sobre los riesgos de la ingeniería social en niños y niñas.

ABSTRACT

The objective of the research is to analyze the security risks to which children are exposed, through the different methods of social engineering with the use of Facebook and the way in which these could be reduced. Methodologically, this is a documentary research, through which it seeks to deepen the main existing risks with the frequent and indiscriminate use by children of the social network Facebook, in many cases with the non-observance and lack of guidance of a responsible adult, which is highly exploited by computer criminals, thus achieving to make known the applicability of computer security in these situations, as well as possible prevention practices by adults that can help reduce these risks.

It was obtained as a result that from the computer security it is possible to make use of the denominated programs of "Parental control", through them it is possible to limit the access of the children to all the contents that the parents consider inappropriate, some of the most complete tools of this type, used at the moment to control and to educate the habits of the minors in Internet are: Qustodio, ESET Parental Control, Web Filter PC, Amigo Parental Control, Kidbox.

It is concluded that it is a fact that computer security can be applied to try to reduce risks in the use of Facebook by children, but to achieve this, it is essential that parents, teachers and adults responsible for supervising children, acquire useful knowledge about preventive measures that can be applied to prevent or minimize these risks.

It is recommended that, from the Ministry of Information and Communication Technologies, it is necessary to raise awareness among parents through the implementation of public policies focused on educating society in general about the risks of social engineering in children.

INTRODUCCIÓN

Actualmente, la tecnología está inmersa en la vida de la mayoría de las personas facilitando la comunicación entre sí, con el simple hecho de tener acceso a un dispositivo tecnológico, para nadie es un secreto que el internet es la red más grande del mundo, la cual permite que sea mucho más fácil y amigable interactuar con otros usuarios. Indiscutiblemente la tecnología llegó y no se irá, así facilitando las actividades diarias relacionadas con el trabajo, de índole recreativo, educativo, u otros.

Diversas herramientas informáticas vienen de la mano con el internet, permitiendo la comunicación e interacción entre los individuos que usan la web, las mismas han tenido gran acogida, siendo las redes sociales (RR. SS.), tales como Twitter, TikTok, Instagram y Facebook algunas de las más utilizadas, contando con millones de usuarios en el mundo. En el mes de enero del 2.019 3.26 mil millones de usuarios se registraron en alguna de las diferentes redes existentes[1] esta cifra se estima que aumenta anualmente en un 15% siendo así Facebook la red social con más popularidad en el planeta y por ende la más utilizada.

En este contexto, es importante señalar que Facebook está presente a nivel mundial y en el año 2.019 recolectó datos de 187.000 usuarios, de los cuales 34.000 fueron menores de edad[2], así sea para trabajo o diversión, sin duda esta herramienta facilita la interacción entre usuarios.

Facebook, como red social, trae consigo diversos beneficios, sin embargo, también tiene sus riesgos si se hace un uso indebido de la misma, siendo tan significativos los riesgos que pueden llevar a perder la vida de una persona que resulte afectada por las interacciones que se desarrollen en dicha plataforma. Se debe tener muy presente que los niños y niñas como menores de edad, están más propensos a los riesgos de Facebook, puesto que los delincuentes que operan bajo esta red, los ven

[1] MARTÍN, Ana. Las Redes Sociales Más Utilizadas: Cifras y Estadísticas." *Thinking for Innovation.* 2020. [En línea]. Recuperado en: 2020-08-05. Disponible en: https://www.iebschool.com/blog/medios-sociales-mas-utilizadas-redes-sociales/.

[2] PORTALTIC/EP. Facebook Reconoce Que Recopiló Datos de 187.000 Usuarios, 34.000 de Ellos Menores de Edad." [En línea]. Recuperado en 2019-06-14. Disponible en: https://www.abc.es/tecnologia/redes/abci-facebook-reconoce-recopilo-datos-187000-usuarios-34000-ellos-menores-edad-201906141756_noticia.html?ref=https:%2F%2Fwww.google.com%2F.

con inexperiencia e inocencia, lo que los hace víctimas fáciles. La llegada de la tecnología trae una cantidad de delitos conectados con las diversas redes sociales, cabe resaltar que está, la suplantación de identidad el *cyberbullying,* el *grooming,* el *sexting*, y la pornografía infantil, entre otros.

Con base en lo expuesto, la presente investigación tiene por objetivo analizar los riesgos de seguridad a los cuales están expuestos a través de los diferentes métodos de ingeniería social los niños y niñas, con el uso de Facebook, de igual manera la forma en que estos podrían reducirse. Para ello, la misma se encuentra estructurada de la siguiente manera:

En primer lugar, se presenta la definición del problema que comprende la presentación de antecedentes del mismo y la formulación. Seguidamente se expone la justificación de la investigación y los objetivos tanto general como específicos. Posteriormente, se desglosa el marco referencial, el cual se encuentra comprendido por: marco referencial, contextual, conceptual y legal. Subsiguientemente, se presenta el diseño metodológico, donde se explica la unidad de análisis, población muestra, estudio metodológico, etapas de la investigación, línea de investigación e instrumentos de recolección de datos. Luego, se presenta el desarrollo de los objetivos, explicando los principales hallazgos alcanzados, finalmente se narran las principales conclusiones y recomendaciones a las que hubo lugar.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

El uso incremental de las tecnologías de la información y comunicación es sin duda un hecho contundente, el cual ha llevado a vivir hoy una era digital. Y por supuesto, dentro de este contexto los niños y niñas, quienes no son ajenos a esta realidad, han hecho que el uso desmesurado de las redes sociales sea una práctica casi espontánea de su cotidianidad, la cual incluso puede pasar por ser algo muy natural o normal. Por lo cual a pesar de las desigualdades económicas y de acceso a la tecnología existentes en Colombia todos sin distinción las usan, "los niños y adolescentes de América Latina se están integrando al mundo digital de modo masivo".[3]

Ahora bien, dentro de esta incertidumbre también surge una nueva relacionada con el uso continuo de las redes sociales tales como Facebook, el cual es uno de los más populares, ya que el 95% de internautas colombianos la utilizó en enero del año 2020.[4] Puesto que, aunque puede existir una percepción generalizada satisfactoria respecto al nivel de seguridad que ofrece esta plataforma e incluso de privacidad, por ser un medio masivo de comunicación de fácil acceso, puede ser utilizado como posible fuente de delitos informáticos e incluso de violencias, que comúnmente son desconocidas, y mucho más, cuando se trata de un niño o niña quien sin el debido acompañamiento o guía de los adultos accede a esta red social.

Sin embargo, aunque podría pensarse que la posible alternativa o solución frente a estas y otras problemáticas relacionadas con el uso de redes sociales por parte de la población infantil, sería la prohibición o limitación de su acceso, ésta dista de la realidad y sería casi imposible de realizar a cabalidad, por lo que sería más apropiado partir por conocer los riesgos para de esta manera abordarlos de una forma efectiva. En este contexto, de acuerdo a cifras del Ministerio de Tecnologías de la Información y Comunicaciones:

Facebook, constituye la red social más popular actualmente con más de 2.167 millones de personas registrados, en Colombia según MINTIC esta red social posee

[3]SÁNCHEZ, David y ROBLES, María, Riesgos y potencialidades de la era digital para la infancia y la adolescencia 2018, p. 187.

[4]HOOTSITE, *Digital 2020: Colombia*. [En línea]. Recuperado en: 25-06-2020. Disponible en https://datareportal.com/reports/digital-2020-colombia

más de 20 millones de usuarios registrado, siendo Bogotá la novena ciudad del mundo con usuarios que hacen uso de esta red social con 6,5 millones de usuarios registrados.[5]

En una investigación realizada en Colombia, en el año 2.018, se determinó que “los jóvenes se ven afectados por el uso de las redes sociales en especial Facebook, pues entre ellos es la más popular, haciendo de ella un lugar donde se realiza discriminación, amenazas, burla, intimidación y otros males que son altamente nocivos para los adolescentes que los llevan al aislamiento y a las relaciones interpersonales con sus familias y el entorno en general, con el agravante que estos en su mayoría son anónimos lo que hace que sea difícil la detección temprana de ellos”[6]

En otro estudio realizado en Colombia en el año 2.019, se realizó un análisis de riesgo por el uso de la red social Facebook en la población juvenil colombiana, determinando que “la ingeniería social es uno de los delitos informáticos más usados por los delincuentes”[7], dentro de los principales hallazgos encontrados se tuvo que el crecimiento de Facebook le ha facilitado a los criminales virtuales como pedófilos y violadores vías alternativas y herramientas para cometer sus crímenes, puesto que en este espacio es posible para ellos generar las estrategias de ingeniería social para atacar a las víctimas; destacando que cada vez son más la cantidad de encuentros con desconocidos que se pactan en esta red social, algunos con fines de amistad, sin embargo, otros tienen el fin de cometer actos ilegales, en donde en la mayoría de las ocasiones los más perjudicados son los menores de edad: niños y jóvenes.[8]

[5] Facebook ya tiene más de 20 millones de usuarios en Colombia. [En línea]. Recuperado en 20-04-2021. Disponible en: https://www.elespectador.com/tecnologia/facebook-ya-tiene-mas-de-20-millones-de-usuarios-en-colombia-article-492061/

[6] MONTES, Carolina y VARGAS, Viviana. Problemas de ingeniería social y su impacto en la adolescencia colombiana. Universidad Nacional Abierta y a Distancia – UNAD. 2018. Bogotá.

[7] ILES, Marío. Análisis de riesgo por el uso de la red social Facebook en la población juvenil colombiana. Universidad Nacional Abierta y a Distancia. 2019. Bogotá.

[8] ILES, Marío. Análisis de riesgo por el uso de la red social Facebook en la población juvenil colombiana. Universidad Nacional Abierta y a Distancia. 2019. Bogotá.

1.2 FORMULACIÓN DEL PROBLEMA

Tal como se expuso previamente, a través de la ingeniería social actualmente se cometen muchos delitos en las redes sociales, principalmente en Facebook, por ser una de las más utilizadas, siendo los niños los más afectados por ser considerados víctimas de fácil acceso, debido a su tendencia a ser influenciados con mayor facilidad por los criminales virtuales.

En este sentido, con el propósito de indagar sobre cómo se pueden reducir los riesgos de seguridad a los cuales están expuestos los niños y niñas con el uso de Facebook como red social, y su vez permitir que los padres, educadores, e incluso los mismos niños y niñas puedan prevenir y hacer un uso adecuado, seguro y responsable de las redes sociales, se plantea este estudio, el cual pueda servir como un referente para afrontar dicha. problemática.

Conjuntamente a esta situación, algunos padres o adultos en general permiten el acceso a dispositivos electrónicos de forma indiscriminada, tales como: el celular, tableta o computador sin supervisión o acompañamiento a la población infantil, presumiblemente con la finalidad de mantenerlos entretenidos u ocupados, no obstante, surgen diversas interrogantes: ¿Están haciendo lo correcto? ¿Qué consecuencias o efectos pueden traer para los niños(as)? ¿Realmente saben a qué contenidos están accediendo ellos?

Con relación a lo expuesto, se plantea la siguiente interrogante principal, la cual será objeto de estudio:

¿Cuáles son los riesgos de seguridad a los cuales están expuestos los niños y niñas con el uso de la red social Facebook y cómo estos podrían reducirse?

2 JUSTIFICACIÓN

Con la expansión que han tenido las tecnologías en referencia a la información y comunicación, así como la llegada de la Internet a los hogares, los niños y niñas en su proceso de aprendizaje y curiosidad innata, tienden a conectarse al dispositivo electrónico más disponible para acceder a sus videos preferidos o chatear con sus amigos en redes sociales, chats y demás plataformas, lo cual conlleva a su exposición ingenua a delincuentes con grandes habilidades en la red, quienes están listos para asechar y atacar a sus víctimas.

Por esta razón se hace necesario abordar los riesgos de seguridad más comunes, especialmente con la implementación de Facebook, debido a su gran popularidad, e identificando la aplicabilidad de la seguridad informática en este contexto, ya que pilares tales como la confidencialidad son altamente vulnerados, a través por ejemplo del uso de ingeniería social, logrando de esta manera obtener los datos de la población infantil, así como la integridad, porque la delincuencia puede aprovecharse y modificar a su antojo la información.

Puesto que, "Quizás los más desfavorecidos sean los niños y niñas por no tener claro los conceptos de privacidad y seguridad, y considerar estos temas más ligados al mundo adulto. Así, no prestan atención a acciones tan sencillas como publicar o etiquetar una foto o compartir claves de acceso a una red social. Es preciso que dediquemos tiempo y espacio en las aulas para educar en la ciudadanía digital, de manera que lo mismo que usamos las redes sociales para trabajar de manera didáctica, sirvan para que nuestro alumnado comprenda la mejor manera de utilizarlas en su tiempo de ocio"[9]

En este contexto, desde el punto de vista teórico, la investigación se justifica pues esta sustentada por las teorías y conceptualización de autores reconocidos en materia de ingeniería social y los riesgos a los cuales se encuentran expuestos los niños en las redes sociales, especialmente Facebook lo cual le da carácter científico al estudio.

En cuanto al aspecto social, la investigación es relevante puesto que se verán beneficiados directa e indirectamente los padres de los niños quienes pueden contar con un compendio de información confiable sobre cómo prevenir o minimizar los riesgos a los cuales están expuestos los infantes en las redes sociales.

[9] VIDAL, María & HERNÁNDEZ, Luis. El uso de las redes sociales virtuales, 2013, p. 14.

Y es que de hecho en la actualidad podemos comparar la exposición a las redes sociales u otros medios de comunicación, con la exposición en una calle en horas nocturnas, llegando incluso a ser más peligroso lo virtual, es por esto que los niños y niñas son mucho más vulnerables a un sin número de riesgos debido a la liberación informática y el uso desmedido de los dispositivos electrónicos, sobre los cuales, en muchas ocasiones los padres o adultos no tienen control alguno.

Consecuentemente, una vía para reducir la ocurrencia de los hechos delictivos que puedan ocurrir, y que los niños y niñas se conviertan en víctimas a través de esta red social, se relaciona con acciones de prevención. “Los adultos deberían estar preparados para escuchar, apoyar y ayudar a sus hijos en caso de que se produzca algún incidente. Lo recomendable es conocer las circunstancias y usos en los que ocurren todos estos riesgos para el menor, así como progresar en el estudio de sus orígenes, de esta forma poder aplicar las medidas de prevención pertinentes”[10]

[10] SÁNCHEZ, David y ROBLES, María, Riesgos y potencialidades de la era digital para la infancia y la adolescencia 2018, p. 187.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Analizar los riesgos de seguridad a los cuales están expuestos a través de los diferentes métodos de ingeniería social los niños y niñas, con el uso de Facebook, de igual manera la forma en que estos podrían reducirse.

3.2 OBJETIVOS ESPECÍFICOS

1. Identificar los riesgos asociados a las técnicas de ingeniería social a las cuales están expuestos los niños y niñas en Facebook.

2. Reconocer las medidas preventivas utilizadas actualmente frente a las técnicas de ingeniería social en Facebook

3. Indagar la aplicabilidad de la seguridad informática para reducir los riesgos en el uso de Facebook por parte de los niños y niñas.

4. Proponer acciones preventivas frente a las técnicas de ingeniería social utilizadas en la red social Facebook contra los niños y niñas.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

Los avances tecnológicos han acelerado los procesos productivos de las sociedades y con ello, mejorado los medios comunicativos, permitiendo a los individuos acceder a información globalizada, potenciando el desarrollo cognoscitivo, social y productivo de las sociedades.

Es así, como las herramientas tecnológicas conjugadas con las necesidades sociales, se han masificado permitiendo que gran parte de los individuos accedan a estas y las hagan parte de sus vidas; para el caso colombiano, encontramos que para el tercer trimestre del año 2.019 el acceso a puntos fijos de internet fue de 70 millones, y los puntos móviles para este mismo periodo fueron de 28.9 millones[11], estas cifras confrontadas con las del año inmediatamente anterior muestran un crecimiento importante que sigue al alza, evidenciando que en los hogares el uso de internet es cada vez mayor.

Todo esto pone ante nosotros un panorama de fácil accesibilidad al internet en los hogares, evidenciado en la alta interacción de niños, niñas y adolescentes a las diferentes plataformas como Facebook en este caso, lo que presupone de inmediato, la inmersión de éstos a riesgos de difícil control, lo que evidentemente esta interrelacionado con la masificación del internet.

Los medios de comunicación agravan la percepción distorsionada al detenerse en informes de miedo sobre la base de observaciones anecdóticas y comentarios sesgados. Si hay un tema en el que las ciencias sociales, en su diversidad, deben contribuir a la plena comprensión del mundo en el que vivimos, es precisamente el área que ha llegado a denominarse en el ámbito académico como Estudios de Internet. Porque, de hecho, la investigación académica sabe mucho sobre la interacción entre Internet y la sociedad, a partir de una investigación empírica metodológicamente rigurosa, realizada en una pluralidad de contextos culturales e institucionales. Cualquier proceso de cambio tecnológico importante genera su propia mitología. En parte porque entra en práctica antes de que los científicos

[11] MINTIC. Los accesos a Internet móvil aumentaron tres millones en el último año. [En línea]. Recuperado en: 06-06-2020. Disponible en: https://www.mintic.gov.co/portal/inicio/Sala-de-Prensa/Noticias/125653:Los-accesos-a-Internet-movil-aumentaron-tres-millones-en-el-ultimo-ano

puedan evaluar sus efectos e implicaciones, por lo que siempre existe una brecha entre el cambio social y su comprensión. Por ejemplo, Los medios informan a menudo que el uso intenso de Internet aumenta el riesgo de alienación, aislamiento, depresión y alejamiento de la sociedad. De hecho, la evidencia disponible muestra que no existe una relación o una relación acumulativa positiva entre el uso de Internet y la intensidad de la sociabilidad. Observamos que, en general, cuanto más sociables son las personas, más utilizan Internet. Y cuanto más usan Internet, más aumentan su sociabilidad en línea y fuera de línea, su compromiso cívico y la intensidad de las relaciones familiares y de amistad en todas las culturas, con la excepción de un par de estudios iniciales de Internet en la década de 1.990.

Ingeniería social

La Ingeniería Social (IS) consiste en persuadir a una persona con el propósito de influenciar sus acciones, es decir es la manipulación de individuos influenciándolos para que ejecuten determinada acción, que a su vez las lleva a ser víctimas de un delito informático. Las técnicas de ingeniería social buscan generar una situación creíble, un contexto donde la persona sienta confianza, todo planificado. Vale destacar que cuando un ciber delincuente implementa una técnica de IS, la efectividad de esta dependerá del comportamiento del usuario y capacidad de análisis o perceptiva, puesto es este quien, en algunas oportunidades, de forma involuntaria, "contribuye" a que los ciberdelincuentes alcancen su propósito y consigan llevar a cabo el engaño. Por ende, la clave es la precaución del usuario, quien tiene el poder en sus manos para frenar la propagación de un crimen de este tipo[12].

En líneas generales, la ingeniería social comprende una serie de técnicas que utilizan los atacantes cibernéticos basada principalmente en la interacción humana y, a menudo, implica engañar a las personas para que rompan las prácticas de seguridad estándar. El éxito de las técnicas de ingeniería social depende de la capacidad de los atacantes para manipular a las víctimas para que realicen determinadas acciones o proporcionen información confidencial. Hoy en día, la ingeniería social es reconocida como una de las mayores amenazas a la seguridad que enfrentan las organizaciones. La ingeniería social se diferencia del pirateo tradicional en el sentido de que los ataques de ingeniería social pueden no ser técnicos y no implican necesariamente el compromiso o la explotación de software o sistemas. Cuando tienen éxito, muchos ataques de ingeniería social permiten a los atacantes obtener acceso legítimo y autorizado a información confidencial.

En este contexto, destaca que las técnicas de ingeniería social han evolucionado, "han aparecido técnicas como *pharming*, muy similar al *phishing*, pero que en vez

[12] WELIVESECURITY. Las técnicas de Ingeniería Social evolucionaron, ¡presta atención!. [En línea]. Recuperado de: 21-05- 2014. Disponible de: https://www.welivesecurity.com/la-es/2014/05/21/tecnicas-ingenieria-social-evolucionaron-presta-atencion/

de engañar al usuario mediante un enlace enviado por correo electrónico, busca el robo de información mediante la modificación en tiempo real de las consultas realizadas a los servidores DNS o mediante la toma de control del equipo víctima; así, modifica el archivo lmhost, que se encarga de resolver las consultas web, asociando la dirección IP al dominio"[13]

[13] WELIVESECURITY. Las técnicas de Ingeniería Social evolucionaron, ¡presta atención!. [En línea]. Recuperado de: 21-05- 2014. Disponible de: https://www.welivesecurity.com/la-es/2014/05/21/tecnicas-ingenieria-social-evolucionaron-presta-atencion/

4.2 MARCO CONTEXTUAL

A continuación, se caracteriza el marco contextual en el cual se desarrolla la problemática planteada con relación a los riesgos a los cuales están expuestos los niños y niñas debido a las técnicas de ingeniería social que aplican ciberdelincuentes en la web (Internet) a través de la red social Facebook.

Internet

Internet es una red integrada por miles de redes y computadoras interconectadas en todo el mundo mediante cables y señales de telecomunicaciones, que utilizan una tecnología común para la transferencia de datos. Es una red global de computadoras que funciona de manera muy similar al sistema postal, solo que a velocidades inferiores a un segundo. Así como el servicio postal permite a las personas enviarse sobres que contienen mensajes, Internet permite que las computadoras se envíen entre sí pequeños paquetes de datos digitales.

Internet se ha convertido, posiblemente, en el ejemplo más importante y generalizado de red del planeta. Internet conecta a personas del otro lado de la calle y de todo el mundo a casi la velocidad de la luz. "Internet, una arquitectura de sistema que ha revolucionado las comunicaciones y los métodos comerciales al permitir la interconexión de varias redes de computadoras en todo el mundo. A veces denominada "red de redes", Internet surgió en los Estados Unidos en la década de 1.970, pero no se hizo visible para el público en general hasta principios de la década de 1.990. Para 2.020, se estimaba que aproximadamente 4.500 millones de personas, o más de la mitad de la población mundial, tendrían acceso a Internet[14]."

La Web 2.0

La Web 2.0 se refiere a la segunda generación de la Web, en la que las aplicaciones y servicios web interoperables y centrados en el usuario promueven la conexión social, el intercambio de medios e información, los contenidos creados por los usuarios y la colaboración entre individuos y organizaciones[15]. La Web 2.0 trasladó a las personas de una Internet de solo lectura a lo que los expertos llamarían una Internet de "lectura / escritura". De repente, los usuarios pudieron ingresar una

[14] FIB. Historia de internet. [En línea]. Recuperado en 30-11- 2020. Disponible en:: https://www.fib.upc.edu/retro-informatica/historia/internet.html

[15] WILSON, David., LIN, Xiaolin., LONGSTREET, Phil y SARKER, Saonee. Web 2.0: A Definition, Literature Review, and Directions for Future Research. [En línea]. Recuperado en: 05-08-2011. Disponible en: https://www.researchgate.net/publication/220892879_Web_20_A_Definition_Literature_Review_and_Directions_for_Future_Research

variedad de información en los campos web y enviarla de regreso a los servidores, para que pudieran comunicarse con los servidores de alojamiento en tiempo real. No solo podían acceder a la información, sino también enviar información al servidor para obtener información más específica u otros resultados generados por el usuario. Aquí es donde una variedad de servicios web despegó cuando los proveedores pudieron usar esta interactividad para transformar los servicios de software. La herramienta fundamental para estas interacciones ha sido el protocolo de transferencia de hipertexto o HTTP. Aquí es donde el navegador envía al servidor un mensaje correspondiente a la información enviada por el usuario y establece las comunicaciones que impulsan la Web 2.0. Web 2.0 también recibió un gran impulso de la tecnología en la nube, donde la abstracción del hardware del servidor permitió a las empresas soñar en grande cuando se trataba de ofrecer servicios en la web.

La infraestructura de la Web 2.0 es compleja y de naturaleza cambiante, pero siempre incluye: software de servidor, sindicación de contenidos, protocolos de mensajería, estándares de navegación, diversas aplicaciones cliente [16]. Una de las principales incorporaciones que permitió esa nueva tecnología fue la incorporación de las redes sociales.

Historia de las redes sociales

Los canales de redes sociales han estado en todas partes desde principios de la década de 2000, y ha estado creciendo a tasas exponenciales desde entonces. Todos los días pasamos 135 minutos en Facebook, Twitter, Instagram y WhatsApp. Es difícil imaginar un mundo sin él, y tendemos a pensar que antes de Facebook, las redes sociales no existían realmente. ¿Y si te dijéramos que se remonta mucho más atrás que Facebook o incluso Myspace?

Sí, e incluso más allá del primer sitio de redes sociales reconocido "Six Degrees", fundado en 1997 por Andrew Weinreich. Las redes sociales se remontan a principios de la década de 1840: aquí hay una infografía de Redpill[17] que describe la línea de tiempo de las redes sociales desde 1844 hasta 2018.

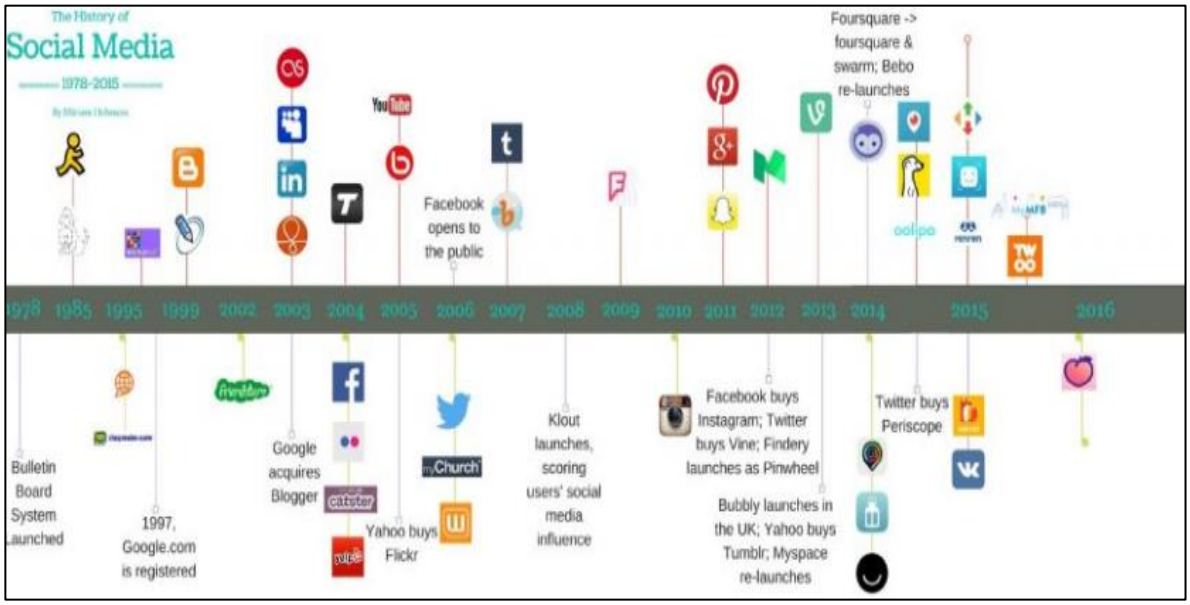
Línea de tiempo de las redes sociales

Es justo decir que la mayoría de nosotros simplemente no seríamos capaces de imaginar el mundo moderno sin las redes sociales, y esto se debe al hecho de que hay tantas formas diferentes en las que las redes sociales han cambiado la forma en que interactuamos entre nosotros. Sin embargo, las redes sociales son un

[16] SFETCU, Nicolae. Web 2.0 / Social media / Social networks. [En línea]. Recuperado en: 03-2017. Disponible en: https://www.researchgate.net/publication/338345786_Web_20_Social_Media_Social_Networks
[17] REDPILL. REDPILL: Influencer Performance Marketing Agency, UK. 2020.

fenómeno bastante reciente, y hace solo diez años no se usaban tan ampliamente como lo son hoy, ni tenían tanto impacto en el mundo que nos rodea como lo hace actualmente, en la figura 1 se evidencia la llegada dichas redes sociales, en ella se presenta una cronología de la evolución de las redes sociales desde 1978, destacando que Facebook, principal objeto de análisis en este estudio, se originó en 2004.

Figura 1. Redes sociales



Fuente. Van Dijck, J. (2019). *La cultura de la conectividad: una historia crítica de las redes sociales*. Siglo XXI Editores.

Impacto de las redes sociales en la forma de comunicación

No es de extrañar que el uso generalizado de las redes sociales para comunicar ideas, historias y experiencias personales y profesionales haya tenido un efecto profundo en la forma general en que las personas se comunican hoy. Las redes sociales se pueden describir como la colección de plataformas en línea que implican compartir y colaborar con una comunidad en línea mediante publicaciones, comentarios e interactuando entre sí. Las plataformas de redes sociales más utilizadas en la actualidad son Instagram, Facebook, Twitter, Pinterest, LinkedIn y Snapchat.

Alrededor de 3 mil millones de personas[18] usan las redes sociales en la actualidad, lo que significa que el 40% del mundo usa las redes sociales para comunicarse. No es de extrañar que este uso generalizado tenga efectos de las redes sociales en la comunicación. El 11% de los adultos informó que prefiere quedarse en casa en Facebook que salir los fines de semana. La comunicación se ve afectada en formas como la expresión personal, nuestras expectativas de los demás y la forma en que las empresas se comunican con los clientes.

Muchas personas tienden a darse atracones en las redes sociales, pasando horas y horas navegando por los sitios. En última instancia, esto puede conducir a un deseo constante de más Internet y más consumo de redes sociales. Mientras más personas obtienen, más quieren, y es difícil detener el ciclo.

Historia de Facebook

Mark Zuckerberg, estudiante de segundo año de Harvard, crea un sitio web llamado Facemash en su dormitorio y comparte el enlace alrededor del campus. Zuckerberg pirateó la base de datos de estudiantes de Harvard para poblar el sitio con imágenes y hacer un juego "caliente o no", en el que los usuarios comparan fotos de estudiantes. Ese juego finalmente se cerró. Zuckerberg y los cofundadores Dustin Moskovitz, Chris Hughes y Eduardo Saverin lanzan Facebook para estudiantes de Harvard. Un mes después se abre a estudiantes de Yale, Columbia y Stanford. Facebook pronto se convertiría en un fenómeno en los campus universitarios de Estados Unidos.

Zuckerberg deja Harvard para trabajar en Facebook desde una casa de alquiler en Palo Alto, California, que sirve como sede. Se une a Sean Parker de Napster, quien luego se convierte en presidente y se muda. El cofundador de PayPal, Peter Thiel, hace una inversión de $ 500,000 y ayuda a dirigir a otros hacia la compañía.
Presenta "The Wall", un área del perfil de un usuario donde amigos y fanáticos pueden publicar mensajes públicos. La función resulta popular y pegajosa, y hace que los usuarios vuelvan a consultar los mensajes con frecuencia. Tres meses después, el 1 de diciembre, la compañía anuncia que ha superado el millón de usuarios activos.

Facebook se expande más allá de los campus universitarios por primera vez y se abre a estudiantes de secundaria. En un movimiento controvertido, pero profético, Facebook rechaza una oferta de adquisición de Yahoo por mil millones de

[18] STATISTA. Number of social media users 2025. Statista, 2017. [En línea]. Recuperado en: 03-02-2021. Disponible en: https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/#:~:text=Number%20of%20global%20social%20network%20users%202017%2D2025&text=Social%20media%20usage%20is%20one,almost%204.41%20billion%20in%202025.

dólares. Según los informes, Zuckerberg pensó que Yahoo! infravalorado el potencial de la empresa. La compañía presenta News Feed, una función divisoria que provoca la indignación de los usuarios por preocupaciones de privacidad. Las protestas son un presagio de lo que vendrá para la empresa de redes sociales. Más tarde ese mes, el 26 de septiembre, Facebook redujo su edad de registro a 13.

Microsoft compra una participación del 1,6% en Facebook por 240 millones de dólares. La inversión valora a la compañía en $ 15 mil millones. Un mes después, la compañía lanza su programa de publicidad Beacon, que rastrea el comportamiento de un usuario de Facebook en sitios de terceros. El producto se convierte en un desastre de relaciones públicas debido a preocupaciones sobre la privacidad del usuario.

Facebook resuelve una demanda de larga data con ConnectU , una empresa fundada en Harvard por los hermanos Winklevoss. Los gemelos habían acusado a Mark Zuckerberg de robar su idea y convertirla en Facebook. El asentamiento no acaba con la batalla. Los gemelos Winklevoss continuarán con acciones legales hasta 2011.

Facebook contrata a la ejecutiva de Google Sheryl Sandberg como directora de operaciones. Sandberg aporta experiencia en liderazgo y perspicacia política de su tiempo como jefa de personal del Departamento del Tesoro bajo Bill Clinton. Muchos la consideran una adulta en la habitación con Zuckerberg. Facebook supera los 2 mil millones de usuarios activos mensuales, una escala casi sin precedentes para una empresa de Internet. "Sentimos que nuestra responsabilidad se está expandiendo, especialmente en torno a superar este hito de 2 mil millones de personas en la comunidad", dijo Zuckerberg. "Hemos estado pensando cuál es nuestra responsabilidad en el mundo y qué tenemos que hacer".

Instagram llega a mil millones de usuarios activos, y es ampliamente visto como el futuro de Facebook en un momento en que se está gestando un éxodo de usuarios por escándalos de privacidad. El número también eclipsa al del rival para compartir fotos, Snapchat, que reportó alrededor de 190 millones de usuarios activos aproximadamente al mismo tiempo.

Peligros constantes de niños y niñas en Facebook

Los niños pequeños (de 4 a 11 años de edad) no están preparados para tener cuentas en las redes sociales. Facebook dice que la aplicación fue diseñada con

expertos en seguridad en línea en respuesta a las llamadas de los padres para tener más control sobre cómo sus hijos usan las redes sociales[19].

El ciberacoso se ha relacionado con la depresión, la ansiedad, el aislamiento social y el suicidio. En comparación con las formas “tradicionales” de acoso escolar, el ciberacoso puede ser presenciado por una audiencia más amplia, el perpetrador puede permanecer en el anonimato y la víctima puede tener dificultades para escapar.

Las plataformas de redes sociales han tomado medidas para abordar el ciberacoso (como el “centro de prevención del acoso” de Facebook), y casi todo el contenido de las redes sociales se puede informar a los administradores del sitio. Pero muchas víctimas no buscan apoyo y la investigación sugiere que el 71% de los adolescentes no cree que las plataformas de redes sociales hagan lo suficiente para prevenir el ciberacoso.

Una actividad común en las redes sociales es ver los perfiles de otras personas. Pero estos retratan con frecuencia versiones editadas de la vida de las personas, como mostrar solo imágenes en las que la persona se ve atractiva o se ve disfrutando.

Por tanto, los niños y niñas pueden tener la impresión de que la vida de otras personas es preferible a la suya propia. Esto puede empeorar por el respaldo social proporcionado por la cantidad de "me gusta " que puede obtener una publicación. En un estudio[20] , casi una quinta parte de los encuestados dijeron que eliminarían una publicación si no recibía suficientes "me gusta".

El posible impacto negativo de las redes sociales en los niños y niñas en riesgo está recibiendo cada vez más atención. Los riesgos identificados incluyen el potencial de contagio o eventos de imitación; compartir información sobre métodos suicidas; estímulo para participar en conductas suicidas; y la normalización de la conducta relacionada con el suicidio como un mecanismo de afrontamiento aceptable.

[19] BBC. “Es irresponsable alentar a los niños a usar Facebook”: la carta de pediatras y educadores a Zuckerberg contra Messenger Kids - BBC News Mundo. [En línea]. Recuperado en 30-11- 2020, Disponible en: https://www.bbc.com/mundo/noticias-42873575

[20] DITCH THE LABEL. The annual bullying survey, [En línea]. Recuperado en 01-11- 2019, Disponible en: https://www.ditchthelabel.org/wp-content/uploads/2019/11/The-Annual-Bullying-Survey-2019-1.pdf

Exposición de vida privada en Facebook

Las líneas de batalla se están trazando entre generaciones. Facebook está encabezado por alguien que aún no ha cumplido los 30, pero que tiene percepciones y suposiciones muy diferentes sobre lo que es privado y lo que no. Debemos reconocer eso con las redes sociales, la geolocalización y tecnología digital, se está restableciendo la barra de privacidad. Facebook se ha visto sometido a una presión significativa para que su sitio sea más seguro para los usuarios. En este sentido, ha implantado algunas acciones para manejar la seguridad de los menores de edad, una de ellas fue la puesta en marcha de una reglamentación que implica un proceso de verificación de los usuarios quienes, al momento de haber realizado el registro de sus cuentas, informaron que eran menores de 13 años [21].

Asimismo, em una acción más fuerte hacia los riesgos que sufren los niños en esta red social, se estableció que podrían bloquear de forma preventiva los perfiles que puedan pertenecer a individuos menores de 13 años, aun cuando en su registro aparezca otra edad; para comprobar la veracidad de esa información s eles solicitará que suban en la plataforma la imagen digitalizada de su documento de identidad oficial, de manera que se pueda comprobar la información. Para determinar si existe un menor de 13 años utilizando un perfil de Facebook se asignarán unos “revisores” encargados de verificar el contenido del perfil bajo investigación, cotejando el texto y fotos publicados, para intentar determinar la edad real del usuario. Si se recopila evidencia que lleve a pensar que la persona que utiliza el perfil es menor de 13 años, la referida cuenta será suspendida y la persona no podrá usar la red social hasta que proporcione un comprobante oficial de su edad [22].

Niños y niñas colombianos en Facebook

Debe tenerse muy en claro que el código de la infancia y la adolescencia incorporó en el artículo 3 la definición que diferencia al niño o niña y adolescente [23] así: "Se

[21] TELESURTV. Facebook e Instagram prohíben su uso a menores de 13 años. [En línea]. Recuperado en: 23-’07-2018. Disponible de: https://www.telesurtv.net/news/facebook-instagram-cerrar-cuentas-seguridad-ninos-20180723-0044.html

[22] TELESURTV. Facebook e Instagram prohíben su uso a menores de 13 años. [En línea]. Recuperado en: 23-’07-2018. Disponible de: https://www.telesurtv.net/news/facebook-instagram-cerrar-cuentas-seguridad-ninos-20180723-0044.html

[23] ICBF. Derecho del Bienestar Familiar. [En línea]. Recuperado en: 12-2020. Disponible en: https://www.icbf.gov.co/cargues/avance/docs/ley_1098_2006.htm#3

entiende por niño o niña, las personas entre 0 y los 12 años y por adolescente las personas entre 12 y 18 años de edad". Ante lo expuesto anteriormente, se puede afirmar que en Colombia la expresión "niño" solamente se refiere a las personas entre los 0 y los 12 años de edad, sin perjuicio de los derechos que tienen los adolescentes por ser menores de 18 años. Los niños y niñas colombianos usan esta red social con el fin de:

- Conocer gente nueva aparte de su círculo social.
- Poder compartir fotos, videos, estados, opiniones, entre otras.
- Compartir con sus familiares.

En cuanto a qué tan seguras son estas actividades, la primera impresión que “venden” a las personas es que es Facebook es una red social inofensiva, que sirve para la recreación, distracción y acercar a las personas, a los familiares que están en otras ciudades o incluso en otros países, constituye un medio por el cual se puede saber más fácil sobre los seres queridos, poder verlos en fotos, videos, chatear, llegando incluso a ser beneficioso para contactar a personas quienes por diversos factores se ha perdido contacto con el paso de los años.

4.3 MARCO CONCEPTUAL

Chat: Participar con una o más personas, a través de Internet, en una conversación en tiempo real, generalmente como una serie de intercambios breves de texto en una aplicación específica, como mensajería instantánea, o mediante el uso de imágenes, voz, video o alguna combinación de estos.

Ciberacoso: Acoso a través de internet.

Ciberdelincuente: Individuos dedicados a planificar y ejecutar crímenes en el ámbito de la web haciendo uso de internet

Cibercriminal social: se trata de una categoría bastante heterogénea, que recoge las características de los sujetos que han cometido delitos cuyo bien jurídico protegido no es ni el económico ni el político.

Ciberintimidacion: Intimidación repetitiva a través de las tecnologías informáticas.

Ciberintimidacion: La actividad de la utilización de la Internet para hacer daño o asustar a otra persona, especialmente con el envío de ellas o envío de mensajes desagradables.

Cyberbulling: Acoso a través de internet.

Cyberstalker: Las características comunes incluyen (pero no se limitan a) el comportamiento clásico de 'acecho': rastrear la ubicación de alguien y monitorear sus actividades en línea y en el mundo real. Se sabe que los acosadores cibernéticos instalan dispositivos GPS en los automóviles de sus víctimas, usan software espía de geolocalización en sus teléfonos y rastrean obsesivamente el paradero de sus víctimas a través de las redes sociales.

Cyberstalker: Se da por medio del uso de algunas tecnologías, principalmente Internet. Se caracteriza por el seguimiento e investigación constante de información sobre una persona o empresa. Es un acto premeditado, repetitivo, obsesivo, y, sobre todo, no deseado.

Deep Web: O internet profunda es el contenido de la red que no está a la vista de todos los usuarios, son páginas que no son indexadas por los distintos motores de búsqueda aun así estas páginas existen, pero son invisibles.

Delito: Acción en contra de la ley realizada a través de internet, redes, los delitos para civiles son aquellos que estos cometen con intención de realizar daño, Los delitos penales se encuentran entre dolosos y culposos depende de cómo se hallan realizado las acciones.

Grooming: Son una serie de conductas donde un adulto se gana la confianza de un menor de edad, lo engaña creando un vínculo emocional con él para que este acceda luego a sus peticiones y el delincuente pueda ejercer sus actos criminales, es una práctica de acoso sexual a niños y adolescentes y por lo regular esto pasa en redes sociales por lo cual es muy importante tomar medidas de seguridad para la navegación es especial de los niños en internet.

Ingeniería social: Se basa en obtener información mediante técnicas de manipulación de las personas, siendo la información el activo más importante de las compañías y el cual necesita protección para lo cual se establecen diferentes tipos de controles para asegurar al máximo esta, pero es en este punto donde se debe contar con la parte humana de la compañía y se debe concientizar de los peligros al exponer la información.

Los atacantes ya saben de esta vulnerabilidad y es ahí donde lanzan sus diferentes técnicas para ganarse la confianza de las personas, mediante métodos de afinidad y diferentes estrategias de manipulación y una vez sumergen la víctima en su burbuja muy posiblemente esta no se haya dado cuenta de que ha sido engañada.

Pharming: El pharming es un tipo de fraude en Internet al manipular el tráfico web, los atacantes de pharming intentan engañar a sus objetivos para que les entreguen información personal valiosa. Debido a que el pharming es tan engañoso, muchas víctimas no se dan cuenta de que han sido estafados hasta que es demasiado tarde.

Phishing: es un tipo de ataque de ingeniería social que se utiliza a menudo para robar datos del usuario, incluidas las credenciales de inicio de sesión y los números de tarjetas de crédito. Ocurre cuando un atacante, disfrazado de entidad de confianza, engaña a una víctima para que abra un correo electrónico, mensaje instantáneo o mensaje de texto. Luego, se engaña al destinatario para que haga clic en un enlace malicioso, lo que puede llevar a la instalación de malware, la congelación del sistema como parte de un ataque de ransomware o la revelación de información confidencial.

Sexting: Se refiere al envío de mensajes de carácter sexual a través, chats y redes sociales, donde el delincuente se gana la confianza del infante y procede a la solicitud de estos, es el acto de referirse explícitamente a mensajes con contenido sexual, esta práctica se ha extendido por el uso de dispositivos móviles y equipos con internet al alcance de los niños.

Síndrome del mensaje múltiple: Impulso por entablar múltiples chats o redes sociales.

Smishing: Enlaces o correos que envían a páginas falsas.

4.4 MARCO LEGAL

Debido a los acontecimientos presentados en nuestro país, durante los últimos años; nuestra ley colombiana ha realizado cambios significativos en la protección de los menores de edad; donde se aplica para dentro y fuera de la red INTERNET, conexiones a redes sociales y uso de las mismas. Nuestras leyes abarcan las posibles conductas con menores de edad de 14 años; donde se incurrirá en penas legales y además de la aplicación de multas en dinero aquellos que se cataloguen como delincuentes contra menores, también como temas de ciberacoso, bullying excesivo con impacto trágicas consecuencias de suicidio, delitos que atenten contra la integridad o acceso no consentido o engañoso a menores de edad donde se quebranten las leyes existentes en Colombia.

Nuestra legislación colombiana actuó, en la actualización de las siguientes leyes; las cuales cobijan penas mayores y multas más altas, así como la reestructuración de las conductas de los delincuentes sexuales a través de medios presenciales y electrónicos. Es de aclarar que el grooming y sexting son modalidades delictivas que conllevan a la realización de delitos como la violación de datos personales y la extorsión, el abuso sexual de un menor, en base a esto las leyes que en Colombia se han generado son las siguientes:

La ley 679 de 2001[24], Esta es la ley base que cobija al menor de edad contra la explotación, pornografía y turismo sexual.

Ley 1336 de 2009[25], Esta ley robustece la ley 679 de 2001, Lucha contra la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes.

La ley 1098 de 2006[26], esta ley colombiana ofrece a nuestros niños, niñas y adolescentes a el derecho a el desarrollo libre, que crezcan sanos en una familia y de la comunidad.

La Ley 1273 de 2009[27]: Artículo 269F: VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

[24]ICBF. Derecho del Bienestar Familiar. [En línea]. Recuperado en 05-06-2020. Disponible en: https://www.icbf.gov.co/cargues/avance/docs/ley_0679_2001.htm

[25] MINTIC. Ley 1336 de 2009 - Ministerio de Tecnologías de la Información y las Comunicaciones. [En línea]. Recuperado en 05-06-2020. Disponible en https://www.mintic.gov.co/portal/inicio/3706:Ley-1336-de-2009

[26] ICBF. Derecho del Bienestar Familiar.[En línea]. Recuperado en 06-06-2020 Disponible en: https://www.icbf.gov.co/cargues/avance/docs/ley_1098_2006.htm

[27] MINTIC. Ley 1273 de 2009 - Ministerio de Tecnologías de la Información y las Comunicaciones. [En línea]. Recuperado en: Disponible en: https://mintic.gov.co/portal/inicio/3705:Ley-1273-de-2009

5 DISEÑO METODOLÓGICO

5.1 UNIDAD DE ANÁLISIS

Como unidad de análisis se tendrán artículos científicos, trabajos de grado y documentos oficiales que aborden la temática de crímenes cometidos contra niños y niñas a través del uso de técnicas de ingeniería social en la red social Facebook.

5.1.1 Población y Muestra

Se toma como población y muestra de investigación los casos de los niños y niñas que durante los últimos años han sido víctimas de ataques de ingeniería social en Facebook, tales como: cyberbullying, suplantación, sexting, grooming, suplantación de identidad, ciberacoso, entre otros casos en esta red social, donde se encuentren registros.

5.2 ESTUDIO METODOLÓGICO

Para el desarrollo de esta monografía, se empleará la investigación tipo documental, la misma "es un proceso basado en la búsqueda, recuperación, análisis, crítica e interpretación de datos secundarios, es decir, los obtenidos y registrados por otros investigadores en fuentes documentales: impresas, audiovisuales o electrónicas"[28]. Como en toda investigación, el propósito de este diseño es el aporte de nuevos conocimientos.

En este sentido, las fuentes de información consultadas serán artículos científicos, investigaciones y otros estudios que hayan sido realizados por expertos en el tema de la ingeniería social en crímenes contra niños y niñas que utilizan la red social Facebook.

Todo ello con el propósito de crear conciencia para los adultos (padres, docentes, representantes) ante dicho tema tan delicado como es; el tema de uso de redes sociales en menores de edad, que para muchas familias o padres creen que es algo ''inofensivo''.

[28] FIDIAS, Arias. El proyecto de investigación. Introducción a la metodología científica. (6ta Ed.) Editorial Episteme, 2012, Caracas.

5.3 ETAPAS DE LA INVESTIGACIÓN

Para el desarrollo del estudio y dar cumplimiento a los objetivos planteados se desarrollarán las siguientes fases:

Fase 1: Diagnóstico de la problemática

En esta fase inicial del estudio se indagó sobre los riesgos a los cuales se encuentran expuestos los niños y niñas al utilizar las redes sociales, específicamente Facebook, documentando los casos registrados a lo largo de estos años, relacionados con ciberdelincuentes que emplean técnicas de ingeniería social, todo ello con el propósito de plantear el contexto de la problemática y su situación actual.

Fase 2: Búsqueda de información documental

En esta etapa del estudio se procedió a realizar una búsqueda documental en diversas bases de datos científicas a las cuales se puede acceder vía *on line*, tales como:

- Dialnet
- Scielo
- El Sevier
- ResearchGate
- Google académico

De las cuales se recopilaron: artículos científicos, tesis de grado, y demás documentos donde se abordan las variables bajo estudio: técnicas de ingeniería social y riesgos a los cuales están expuestos los niños en Facebook.

Fase 3: Identificación de riesgos asociados a las técnicas de ingeniería social a las cuales están expuestos los niños y niñas al en Facebook

Luego de la recopilación de información documental, se realizará el análisis y procesamiento de los datos recopilados para identificar los riesgos en seguridad existentes frente a las diferentes técnicas de ingeniería social a las cuales los niños y niñas están más expuestos con el uso de la red social Facebook.

Fase 4: Reconocimiento de medidas preventivas utilizadas actualmente frente a las técnicas de ingeniería social en Facebook

Posteriormente, se procedió a realizar el reconocimiento de algunas de las medidas preventivas que prevalecen actualmente en relación al uso de las redes sociales dirigidas a la protección de la población infantil que hace uso de las mismas sin supervisión de un adulto responsable, evidenciando cuales han sido las más efectivas durante su implementación.

Fase 5: Indagación sobre la aplicabilidad de la seguridad informática para reducir los riesgos en el uso de Facebook por parte de los niños y niñas

En esta fase de la investigación se enfocó el análisis de la información en la indagación de estudios que evidencien cómo desde la aplicabilidad de la seguridad informática podrían reducirse los riesgos en el uso de Facebook por parte de la población infantil.

Fase 6: Propuesta de acciones preventivas frente al uso de técnicas de ingeniería social en la red social Facebook.

Con base en la revisión bibliográfica realizada, en esta fase del estudio se proponen acciones preventivas frente a las técnicas de ingeniería social aplicadas por ciberdelincuentes, contra los niños y niñas que utilizan la red social Facebook sin supervisión de un adulto.

Fase 7: Formulación de conclusiones y recomendaciones del estudio

Finalmente, una vez que se dé respuesta a cada uno de los objetivos del estudio se presentan las conclusiones y recomendaciones a las que hubo lugar en función de cada uno de los objetivos planteados al inicio de la investigación.

5.4 LÍNEA DE INVESTIGACIÓN

En el marco de los parámetros de investigación establecidos por la escuela de ciencias básicas, tecnología e ingeniería de la Universidad nacional Abierta y a Distancia (UNAD), se seleccionó la línea de investigación:

- Infraestructura tecnológica y seguridad en redes

5.5 INSTRUMENTOS DE RECOLECCIÓN DE DATOS

Como instrumentos de recolección de datos se emplearon:

- Información proporcionada por internet por parte de la fuerza pública y el ministerio de las TICS.
- Legislación colombiana (ley 1273 del 2009).
- Estudios relacionados con el tema. (artículos científicos, tesis de grado, informes oficiales de organismos reconocidos)
- Registro de ataques a menores de edad.

6 RESULTADOS Y DISCUSIÓN

En esta fase de la investigación se presenta el desarrollo de los hallazgos encontrados en función de cada uno de los objetivos del estudio.

6.1. IDENTIFICAR LOS RIESGOS ASOCIADOS A LAS TÉCNICAS DE INGENIERÍA SOCIAL A LAS CUALES ESTÁN EXPUESTOS LOS NIÑOS Y NIÑAS EN FACEBOOK.

Existen diversos riesgos asociados a las técnicas de ingeniería social a las cuales están expuestos los niños y niñas en Facebook, una de las técnicas más utilizadas es la sextorsión, en la tabla 1 y siguientes que se muestran a continuación se narran diversos casos registrado sobre este delito en Colombia, especificando las técnicas de ingeniería social aplicada, descripción de su aplicación, ejemplos de casos registrados, así como los riesgos asociados para la población infantil víctima de la misma.

Tabla 1. Técnica de ingeniería social: Grooming

Descripción de aplicación / ejemplos de casos registrados	Riesgos asociados
CASO 1: Durante el año 2.017, en Colombia se identificaron más de 300 casos de incidentes asociados a la modalidad de grooming (la suplantación de un NNA-niño, niña y/adolescente en la red) y más de 150 grupos de chats de pornografía infantil en WhatsApp de los cuales hacen parte profesores y personalidades de la vida pública en donde se intercambian fotografías y videos de “niños víctimas desde los 3 meses de nacidos hasta los 12 años [29].	• Pornografía infantil • Agresiones psicológicas • Agresiones físicas
CASO 2: En el año 2016, se identificó a un ingeniero industrial de 40 años quien fue capturado por las autoridades en el barrio Ciudad Jardín (Cali) a comienzos de marzo. Su principal característica consistió en crear un perfil falso en Facebook, en el cual utilizaba el nombre y las fotografías de su propia hija de 11 años.	• Acoso • Ciberacoso • Abuso sexual • Pornografía infantil

[29] GRUPO FUNCIONAL DE SEGURIDAD INFORMÁTICA, UNAD. Nueva modalidad de delitos informáticos en Colombia. [En línea]. Recuperado en: 27 -07- 2018. Disponible en: https://noticias.unad.edu.co/index.php/gidt/2333-nueva-modalidad-de-delitos-informaticos-en-colombia

Gracias a esta página ganaba la confianza de niñas de edades similares a quienes, a través de engaños, les pedía fotografías desnudas o en ropa interior. Una vez recibía las imágenes, amenazaba a sus víctimas con publicarlas a menos que se encontraran personalmente con él en algún lugar público de la ciudad [30]. El hombre las obligaba a ir a moteles de Cali, donde ingresaba en un automóvil de vidrios polarizados, con el cual impedía que los empleados de esos establecimientos pudieran percatarse de la edad de sus acompañantes. Al momento de su arresto, tenía dos computadores, dos discos duros y varias memorias USB con material pornográfico. La captura se produjo gracias a la denuncia de la madre de una de sus víctimas, quien se percató de la situación y acudió a las autoridades.	• Agresiones psicológicas • Agresiones físicas
CASO 3: Otro caso registrado en Colombia, es el relacionado con la evidencia de un hombre quien se hacía pasar por cantantes, este sujeto de 23 años sin identificar aún por parte de las autoridades, contaba con dos perfiles falsos en Facebook, a nombre del cantante Maluma. A través de estas presencias en línea se ganaba la confianza de niñas de entre 9 y 12 años, a quienes pedía fotografías y videos en que aparecieran desnudas o en ropa interior. Una vez las menores de edad le enviaban el material que él solicitaba, las amenazaba con publicar las imágenes o enviárselas a sus padres a menos que accedieran a sostener relaciones sexuales con él. En el momento de la captura, la policía realizó la incautación de 15 discos duros, 5 tabletas, 9 celulares, 15 memorias micro sd y 2 memorias usb, que utilizaba para almacenar y distribuir las imágenes. La captura se realizó gracias a la denuncia de una madre de una menor que fue víctima del delincuente. El capturado se encuentra a disposición de la fiscalía, que le dictó medida de	• Pornografía infantil • Abuso sexual • Ciberacoso

[30] EN TI CONFIO. Tres casos de grooming en Colombia. [En línea]. Recuperado en: 16-02-2016. Disponible en: https://www.enticconfio.gov.co/tres-casos-grooming-colombia

aseguramiento en una prisión. afronta una pena de entre 10 y 20 años por el delito de pornografía infantil [31].	
CASO 4: Otro caso documentado, fue el de un periodista de 27 años de edad, quien entre los años 2.011 y 2.015, utilizó dos perfiles falsos de Facebook, en los cuales se presentaba como una mujer llamada Juliana Salazar, para contactar a estudiantes de colegios de estratos altos, de entre 13 y 16 años. Después de ganar su confianza les pedía fotos en las que estuvieran desnudos o en diferentes poses sugestivas. Luego, a través de otro perfil falso a nombre de Andrés Monsalve, extorsionaba para no revelar estas fotografías y videos. En estos casos, les pedía más imágenes o que accedieran a encontrarse con él. Las autoridades estiman que cerca de 150 niños habrían sido víctimas de esta persona. Uno de los padres de las víctimas denunció ante las directivas del colegio está situación, lo que motivó la presentación de una denuncia ante la Fiscalía General. El ente investigador contactó a expertos en delitos informáticos de la Policía Nacional. El acusado se encuentra en libertad condicional, pues pasaron los 60 días establecidos por la Ley para el inicio del juicio, desde la presentación del escrito de acusación [32].	• Abuso sexual • Pornografía infantil • Ciberacoso

Fuente: Tres casos de grooming en Colombia. (16 de febrero de 2016). Recuperado de: https://www.enticconfio.gov.co/tres-casos-grooming-colombia

Tabla 2 Técnica de ingeniería social: Ciber inducción al daño físico y mental

Descripción de aplicación / ejemplos de casos registrados	Riesgos asociados
Esta técnica de ingeniera social se basa en inducir a que las personas, especialmente niños se auto infrinjan heridas con el propósito de avanzar en un supuesto “reto” hasta “ganar” [33].	• Auto agresiones físicas

[31] ENTICONFIO. Tres casos de grooming en Colombia. [En línea]. Recuperado de: 16-02- 2016. Disponible en: https://www.enticconfio.gov.co/tres-casos-grooming-colombia

[32] ENTICONFIO. Tres casos de grooming en Colombia. [En línea]. Recuperado de: 16-02- 2016. Disponible en: https://www.enticconfio.gov.co/tres-casos-grooming-colombia

[33] FERNÁNDEZ, Cristhian. Capacidades Técnicas, Legales y de gestión para equipos Blueteam Y Redteam. Universidad Nacional Abierta y a Distancia. 2020. [En línea]. Recuperado en: 04-06-2020. Disponible de: https://repository.unad.edu.co/bitstream/handle/10596/37232/1088251899.pdf?sequence=1&isAllowed=y

Si un niño no cuenta con las habilidades necesarias para discriminar qué información es cierta y que información es falsa o para interactuar de forma segura en internet, es muy fácil que pueda verse comprometido en uno de estos grupos que promocionan un modelamiento de interacción a base de retos con fines de autolesión, cuya acción criminal atenta en contra de la vida y la integridad de los mismos. CASO 1: Un ejemplo de este tipo de cibercrimen es el conocido como “La Ballena Azul” o “El reto del Hada de Fuego”, que ha ocasionado suicidios y serias lesiones físicas y mentales de adolescentes y jóvenes, en Colombia en el año 2.017, se vieron afectados 6.498.746 usuarios jóvenes [34].	• Muerte (suicidios)

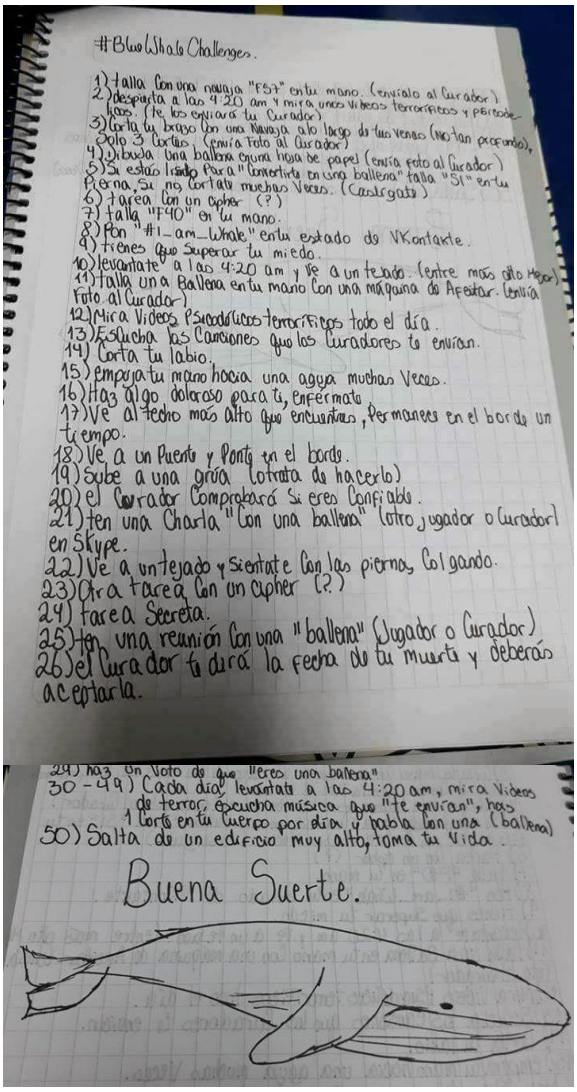
Fuente: Grupo Funcional de Seguridad Informática, UNAD. Nueva modalidad de delitos informáticos en Colombia. (27 de julio de 2018) Recuperado de: https://noticias.unad.edu.co/index.php/gidt/2333-nueva-modalidad-de-delitos-informaticos-en-colombia

En relación con esta técnica de ingeniería social, destaca que la historia del desafío *Blue Whale* o Ballena Azul comenzó con Rina Palenkova. el 22 de noviembre de 2.017, Rina, una adolescente que vive en el sureste de Rusia, publicó una selfie. En la foto ella está parada afuera. Tiene un pañuelo negro envuelto alrededor de su boca y nariz. Ella está levantando su dedo medio hacia la cámara. Parece que está cubierto de sangre seca. La leyenda de la foto decía: "Nya bye". Al día siguiente, se quitó la vida.

Se informó que el "desafío de la ballena azul" era un "juego suicida" en línea dirigido a niños y adolescentes que establecían 50 tareas durante 50 días. Se alegó que el desafío estaba relacionado con numerosas muertes en todo el mundo. Pero poco del "juego" era lo que parecía. En la figura 2 se ilustra la lista de tareas que implicaba el mencionado resto:

[34] GRUPO FUNCIONAL DE SEGURIDAD INFORMÁTICA, UNAD. Nueva modalidad de delitos informáticos en Colombia. [En línea]. Recuperado de: 27-07-2018. Disponible en: https://noticias.unad.edu.co/index.php/gidt/2333-nueva-modalidad-de-delitos-informaticos-en-colombia

Figura 2. Reto “La ballena azul”



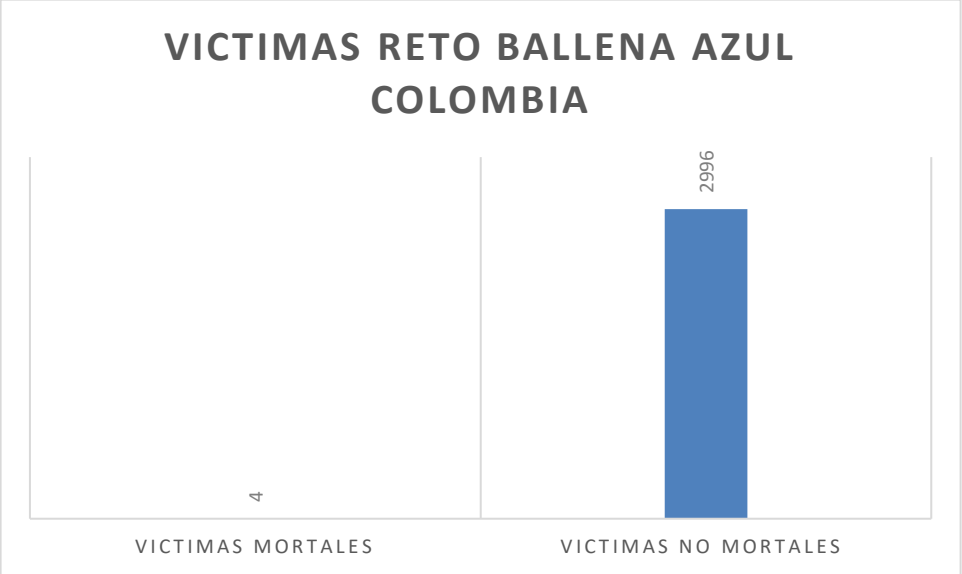
Fuente: BBC NEWS. (2017, April 26). Qué es el peligroso juego de “La ballena azul” y por qué preocupa a las autoridades – BBC News Mundo. From BBC. Recuperado de: https://www.bbc.com/mundo/noticias-39721105

Para el año 2017 los investigadores realizaron un primer barrido y descubrieron en Colombia varios grupos en los que estaban inscritos decenas de menores, quienes, utilizando la red social Facebook, participaban en el tema de la ballena azul. Pero quizás lo que más aterró a los peritos informáticos fue descubrir que el macabro juego ya había dejado víctimas en el país.[35]

[35] SEMANA. Ballena azul: El aterrador juego de la muerte Recuperado de: Semana.com Últimas Noticias de Colombia y el Mundo. [En línea]. Recuperado de: 29-04-2017. Disponible en: https://www.semana.com/nacion/articulo/ballena-azul-el-aterrador-juego-de-la-muerte/523718/

En la figura 3 se puede evidenciar que en abril de 2.017 se reportaron casi 3.000 casos en el juego de la ballena azul siendo 4 de ellos letales la mayoría de estos casos han sido ocasionados por medio de Facebook, se recomienda en Colombia tomar medidas contundentes para castigar a quienes propagan este y demás juegos. Se dice que dicho juego fue creado en Rusia, pero hay quienes por medio de perfiles falsos propagan este juego en Colombia y el mundo entero.

Figura 3. Víctimas por la ballena azul en Colombia



Fuente: SEMANA (2017, April 29). Ballena azul: El aterrador juego de la muerte Recuperado de: Semana.com Últimas Noticias de Colombia y el Mundo: https://www.semana.com/nacion/articulo/ballena-azul-el-aterrador-juego-de-la-muerte/523718/

Tabla 3. Técnica de ingeniería social: Sextorsión

Descripción de aplicación / Ejemplos de casos registrados	Riesgos asociados
CASO 1: En el año 2.017 las autoridades lograron desarticular una red de explotación sexual con menores de edad, tras capturar a 13 de sus integrantes. Entre los detenidos se encontró Éver Dario Méndez, quien fue candidato a la Alcaldía de Cunday y para esa fecha fue contratista vinculado con la Alcaldía de Soacha. Las niñas eran contactadas por redes sociales, incluyendo Facebook, y con engaños eran persuadidas por los integrantes de la red, para ser trasladadas a Carmen de Apicalá y a Cunday (Tolima), donde las explotaban sexualmente. Las víctimas eran ubicadas desde Bogotá y Soacha, por tres mujeres, a las que les pagaban 100 mil pesos por cada niña que enganchaban.[36]	• Abuso sexual • Pornografía infantil • Agresiones psicológicas • Agresiones físicas

Fuente: Publimetro (2017). La incansable lucha de una madre fue la pieza clave para desarticular red de explotación sexual con menores de edad (10-10-2017) Recuperado de: https://www.publimetro.co/co/noticias/2017/10/10/cae-red-de-explotacion-sexual-que-sometia-menores-de-edad-de-bogota-y-soacha.html

Tabla 4. Técnica de ingeniería social: Cyberbullying/ Ciberacoso

Descripción de aplicación / ejemplos de casos registrados	Riesgos asociados
CASO 1: Uno de los casos reportados sobre Cyberbullying en Colombia durante los últimos años fue el de Yhon Rodríguez de 15 años, quien se quitó la vida en octubre de 2.012. Burlas, comentarios ofensivos e incluso alusivos al suicidio inundaron las redes sociales tras conocerse fotos privadas, de contenido sexual, del menor. Yhon y Camila son dos menores de edad que se conocieron por Facebook, con el tiempo se hicieron amigos y luego novios. Se sentían tan bien con su relación que se confiaban y compartían muchas cosas, entre ellas, las	• Ciberacoso • Agresiones psicológicas • Suicidio

[36] PUBLIMETRO. La incansable lucha de una madre fue la pieza clave para desarticular red de explotación sexual con menores de edad. [En línea]. Recuperado en: 10-10-2017. Disponible en: https://www.publimetro.co/co/noticias/2017/10/10/cae-red-de-explotacion-sexual-que-sometia-menores-de-edad-de-bogota-y-soacha.html

contraseñas de sus cuentas en las redes sociales. Tras un descuido mutuo por mantener a salvo esa información, fotos privadas de Yhon terminaron siendo públicas en Internet, su nombre se convirtió en la primera tendencia en Twitter durante varias horas y las imágenes de su cuerpo en un fenómeno viral de matoneo [37].	

Fuente: Montes, C. y Vargas, V. 2018. Problemas de ingeniería social y su impacto en la adolescencia colombiana. Universidad Nacional Abierta y a Distancia – UNAD

Es un hecho que, el escenario de ejecución de la gran mayoría de los casos de ingeniería social como los descritos previamente, son las redes sociales, siendo Facebook una de las más cuestionadas en materia de seguridad, pues se ha juzgado el hecho de que, si esta empresa se preocupa verdaderamente por la seguridad en línea de los niños, entonces, de forma predeterminada, la configuración de Facebook estaría configurada como privada, no pública. Facebook es muy consciente de que muchos niños menores de 13 años ya utilizan el sitio de redes sociales. Según estudio del informe del consumidor, se evidencia que 7.5 millones de niños están usando Facebook antes de los 13 años[38]. Muchos niños mienten sobre su edad para acceder a Facebook. Y, lamentablemente, la verificación de edad no funciona según Hemanshu Nigam, un experto en seguridad de Internet: "Las empresas hacen verificación de edad porque saben que se supone que deben hacerlo, pero todo el mundo sabe que realmente no funciona"[39]. Esto es cierto para todos los sitios web, no solo para Facebook.

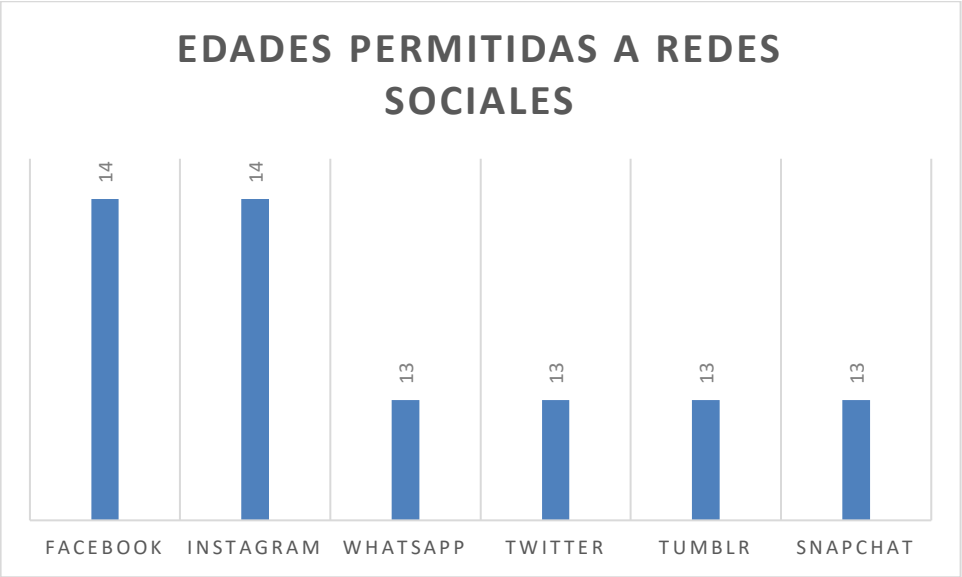
En la figura 4, que se presenta a continuación se observa a qué edad se considera legal tener acceso a algunas redes sociales en Colombia, específicamente: Twitter, Instagram, Whatsapp, Twitter, Tumblr y Snapchat.

[37] MONTES, C. y VARGAS, V. Problemas de ingeniería social y su impacto en la adolescencia Colombiana. [En línea]. Recuperado en 2018. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/22583/41946700.pdf?sequence=1&isAllowed=y

[38] ELNUEVODIA. Estudio del informe del consumidor. 2019.

[39] FERRO VEIGA, José Manuel. Trabajo infantil: la esclavitud del siglo XXI. 2015.

Figura 4. Edades permitidas para acceder a redes sociales



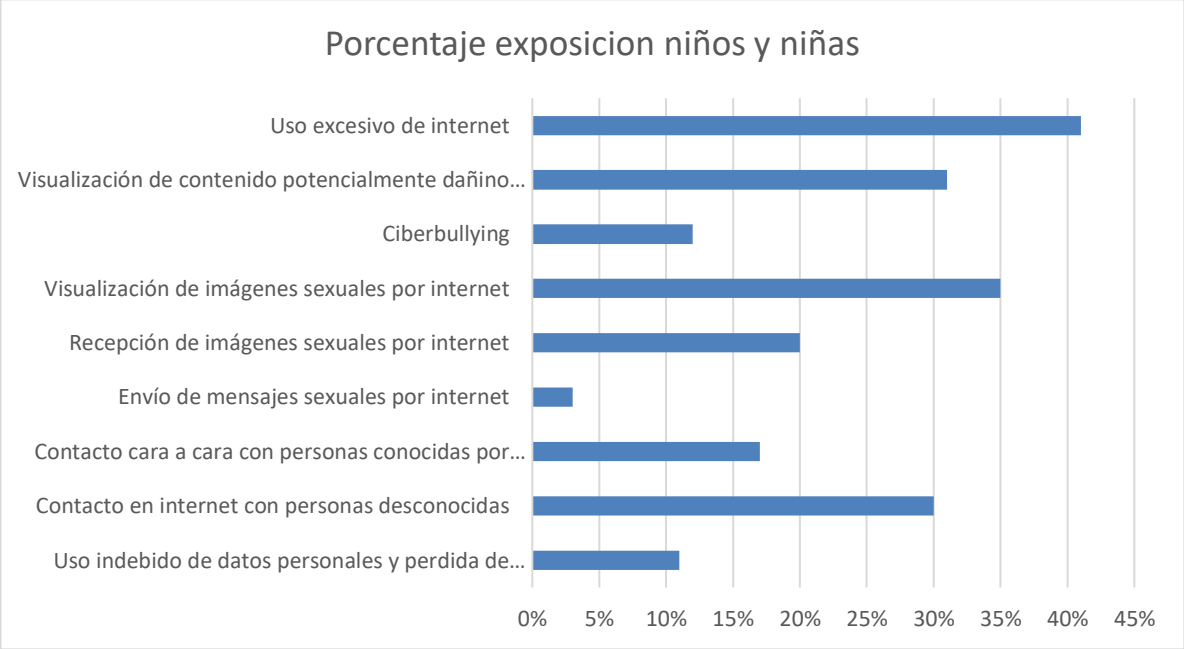
Fuente: La edad mínima no es un capricho. (2019). Recuperado de Presidencia.gov.co website: http://es.presidencia.gov.co/columnas/presidencia/la-edad-m%C3%ADnima-no-es-un-capricho

Los padres, deben detenerse y pensar detenidamente sobre lo que significa que los niños accedan a Facebook. ¿Cuáles son los beneficios para ellos? ¿Cuáles son los riesgos? ¿Cómo podría afectar Facebook a su futuro? Facebook comenzó como una plataforma universitaria y ahora es una parte omnipresente de nuestra cultura y entorno. Es una forma manera de conectarse con familiares y amigos. Muchos profesores se comunican con sus alumnos en esta red social y publican tareas. Pero su utilización también conlleva un riesgo enorme, especialmente para los niños más pequeños y los preadolescentes. Los niños son naturalmente curiosos, impulsivos, carecen de buen juicio y habilidades para la toma de decisiones porque la función ejecutiva del cerebro que ayuda con la toma de decisiones no está completamente desarrollada hasta que un adulto cumple 25 años. Suelen ser impulsivos y correr riesgos. Después de todo, son niños y no adultos en miniatura. Como padres, debemos guiar a nuestros hijos durante la adolescencia.

Muchos niños admiten abiertamente participar en comportamientos riesgosos en línea. Además, el 26% de los niños dijeron que ignoraron las advertencias de sus

padres sobre la seguridad en Internet[40]. En un estudio realizado[41] se evidencia el porcentaje en que los niños y niñas colombianos están expuestos, en la figura 5 se ilustran los resultados obtenidos con respecto al porcentaje de infantes expuestos a elementos como uso excesivo de internet y ciberbullying:

Figura 5 Porcentaje exposición niños y niñas



Fuente: Riesgos - Contigo Conectados. (2020). Contigo Conectados. Recuperado de: https://contigoconectados.com/resultados/riesgos/

Como primera instancia se debe orientar a los padres de familia ya que son las personas más cercanas y directas a los menores, como segunda instancia a los docentes de las instituciones educativas para que realicen instrucciones dando buen uso de estas herramientas como lo son las redes sociales, ya que si se saben manejar de manera responsable y sabiamente se les daría un muy buen uso.

[40] PANDA SECURITY, "Uno de cada tres adolescentes contacta con desconocidos a través de Internet - Panda Security Mediacenter," Panda Security Mediacenter. [En línea]. Recuperado en: 10-10-2020. Disponible en: https://www.pandasecurity.com/es/mediacenter/notas-de-prensa/uno-de-cada-tres-adolescentes-contacta-con-desconocidos-a-traves-de-internet/

[41] CONTIGO CONECTADOS (2020). Riesgos. [En línea]. Recuperado en: 30-10-2020. Disponible en: https://contigoconectados.com/resultados/riesgos/

Es un hecho que los ciberdelincuentes expertos saben que la ingeniería social funciona mejor cuando se centra en las emociones y el riesgo humanos. Aprovechar las emociones humanas es mucho más fácil que piratear una red o buscar vulnerabilidades de seguridad.

En líneas generales, los niños y niñas suelen utilizar Facebook para mantener y recuperar conexiones sociales y para el 'trabajo de identidad' que incluye compartir y etiquetar fotografías, la creación de 'actualizaciones de estado' y formas asociadas de aprobación social, como 'dar me gusta' a las publicaciones. Estos intercambios pueden ayudar a unir a una comunidad, pero también pueden inducir varias formas de ansiedad social. Esto es particularmente cierto para los niños y niñas que buscan la aprobación social para reforzar su propio sentido de sí mismos, y que a veces pueden verse afectados negativamente por los procesos de comparación social que acompañan al intercambio de redes sociales.

Los procesos de comparación social invitados por redes sociales son bien reconocidos. Por ejemplo, las selfies son moneda corriente en muchos sitios de redes sociales, pero la publicación de selfies también se asocia con ciertas presiones sociales, como la necesidad de publicar selfies 'divertidas' positivas y tratar de obtener suficientes 'me gusta' o arriesgarse a dañar la autoestima. Es mucho más probable que estos procesos de comparación tengan lugar cuando los otros miembros de una comunidad de redes sociales son similares a uno mismo, ya sea por edad, sexo u otras dimensiones de identidad. Los niños y niñas pasan muchas horas viendo las publicaciones de otras personas similares e inevitablemente se ven arrastrados al proceso de comparación social. Este proceso, descrito por primera vez por Festinger (1954)[42] , implica dos actos posibles: las personas pueden compararse desfavorablemente con los demás, haciendo una comparación ascendente que se dice que forman parte del impulso hacia superación personal o pueden compararse a sí mismos favorablemente con los demás, haciendo comparaciones descendentes que pueden usarse para restaurar la autoestima amenazada y crear un afecto positivo. Estas comparaciones ascendentes y descendentes son parte de la auto presentación. Afectan la creación de un yo deseado e informan las elecciones personales sobre cómo 'verse bien', esto ha influido en nuestra comprensión de las formas en que las personas pueden utilizar la auto presentación para reclamar la pertenencia a un grupo o comunidad.

[42] APA PSYCNET. [En línea]. Recuperado en 30-11-2020, Disponible en: https://psycnet.apa.org/record/2017-40848-056

6.2. Reconocer las medidas preventivas utilizadas actualremente frente a las técnicas de ingeniería social en Facebook

En Colombia, a lo largo de los años se han implementado esfuerzos para minimizar los riesgos relacionados con la ingeniera social los niños y niñas, en este sentido en el año 2.019 el país logró la certificación en la lucha contra sitios web asociados al material de abuso sexual infantil, la organización de origen inglés Internet Watch Foundation (IWF), certificó una reducción del 99,7% en los dominios .co que se encontraban asociados a este tipo de material[43].

Dicha situación convierte al internet en un escenario predilecto de los ciber delincuentes, quienes utilizan las herramientas tecnológicas disponibles para para acceder a la información que comparten los menores en la web y manipularla según sus intereses, bien sea transmitirla, venderla, pornografía infantil, entre otros. A pesar de que el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia ha implementado diversas políticas públicas enfocadas en prevenir o minimizar los riesgos a los cuales se encuentran expuestos los niños y niñas en las redes sociales, por ejemplo los programas “Te protejo” y “En Tic Confió”, entre otros, los cuales han tenido resultados positivos para su mitigación, aún no existen políticas claras enfocadas en el fomento de una cultura de prevención y buenas prácticas en materia de seguridad informática. Este plan por la protección de la infancia y la adolescencia en Colombia cuenta con dos importantes proyectos que los ciudadanos pueden consultar para denunciar y buscar asesoría:

- En TIC Confío: es la estrategia del MinTIC enfocada en la promoción del uso seguro y responsable de Internet y de las nuevas tecnologías. En dicha plataforma se ayuda a la sociedad ara que sea capaz de desenvolverse e interactuar de forma responsable con las TIC, al mismo tiempo que promueve la convivencia digital y la cero tolerancia con el material de abuso sexual infantil. Su sitio web es https://www.enticconfio.gov.co.[44]

- Te Protejo: es una iniciativa para la efectiva protección, a través de Internet, de la infancia y la adolescencia. Su sitio web es http://www.teprotejo.org allí es posible denunciar espacios digitales con temáticas como material de abuso sexual infantil, ciberacoso, entre otros[45]. Uno de los principales logros del programa “Te protejo”, es que en el marco de su articulación con la Red mundial de líneas de denuncia INHOPE y el análisis realizado de los sitios web bloqueados en Colombia, en programa clasificó 5.037 imágenes de abuso sexual de niñas, niños y adolescentes, las cuales fueron enviadas a sus países de origen para solicitar su desmonte de la

[43] MINTIC. Colombia logra certificación en la lucha contra sitios web asociados al material de abuso sexual infantil.. [En línea]. Recuperado en 2019. Disponible en: https://mintic.gov.co/portal/inicio/Sala-de-Prensa/Noticias/102756:Colombia-logra-certificacion-en-la-lucha-contra-sitios-web-asociados-al-material-de-abuso-sexual-infantil
[44] MINTIC. Idem.
[45] MINTIC. Idem.

web y de esta manera frenar la revictimización de los niños y niñas que aparecen en ellas[46].

Otra iniciativa muy relevante en los últimos años, es el modelo WePROTECT, esta decisión surgió a partir de julio del año 2017, frente el reconocimiento de que el riesgo de vulneración del derecho a la integridad sexual de los niños, niñas y adolescentes se ha extendido a los espacios virtuales, con énfasis en las redes sociales, Colombia inició la implementación de un plan para desarrollar el modelo WePROTECT, el mismo constituye una iniciativa internacional que presenta un enfoque intersectorial orientado a prevenir y atender a las víctimas de explotación sexual y abuso en entornos web[47].

6.3. Indagar la aplicabilidad de la seguridad informática para reducir los riesgos en el uso de Facebook por parte de los niños y niñas.

Es un hecho que, mayoría de los niños, niñas y adolescentes utilizan Internet como un mecanismo o herramienta de recreación, dentro de sus principales usos están: chatear con familiares y amigos, jugar en plataformas *on line* (incluyendo redes sociales como Facebook), para buscar y escuchar música, entre otros. Sin embargo, a nivel de seguridad informática no existe ninguna medida estandarizada establecida para su acceso a las redes sociales y uso de internet. De lo anterior, deriva la importancia de dar a conocer de forma masiva la cultura de la seguridad informática, promoviendo el uso adecuado y responsable de las TIC al momento de utilizar diversas herramientas tecnológicas, así como el acceso a redes sociales de forma segura y con conocimiento por parte de los padres, docentes o representantes, de los tipos de riesgos con los que se pueden encontrar los niños al hacer uso de las mismas [48].

Para hacer una aplicación adecuada de la seguridad informática, tal como se mencionó previamente es necesario considerar que los niños, niñas y adolescentes centran el uso de internet en el ámbito socio-relacional y recreativo, utilizando principalmente las herramientas TIC. El ámbito socio relacional de los menores se centra en uso de redes sociales (Facebook, Twitter, Tuenti, etc.), Juegos (Wii, PlayStation, Xbox, etc.), Comunicación inmediata (WhatsApp, Google Meet, Line,

[46] UNICEF. Colombia se suma a los esfuerzos internacionales. [En línea]. Recuperado en: 22-09-2017. Disponible en: https://www.unicef.org/colombia/comunicados-prensa/colombia-se-suma-los-esfuerzos-internacionales

[47] UNICEF. Ídem.

[48] NAVARRO, William., CÁRDENAS, Sonia., BAREÑO, Raúl. La importancia de la cultura en seguridad informática como experiencia innovadora en entidades de formación por competencias SENA. Recuperado en: 2016. Disponible en: https://www.researchgate.net/profile/Nau_Silverio_Gutierrez2/publication/321603716_Gestion_del_Talento_Humano_Enfoques_y_Modelos/links/5a289d43a6fdcc8e8671bcb4/Gestion-del-Talento-Humano-Enfoques-y-Modelos.pdf

etc.), multimedia (Instagram, YouTube, Pinterest, Spotify, etc.), y almacenamiento (Dropbox, Google Drive, etc.), por ende, en esos ámbitos es donde deben enfocarse la mayor cantidad se esfuerzos en cuanto a protección y seguridad informática. En relación a esto, una forma de promover la seguridad informática desde las instituciones educativas, es en el marco de proyectos de aprendizaje, donde involucren a los padres de familia y a la comunidad en general, realizar cuestionarios diagnósticos para determinar el nivel de conocimiento en terminología y acciones preventivas relacionadas seguridad informática y en uso controlado o no del acceso a RR. SS. de los menores, así como sus hábitos de uso por parte de los estudiantes.

En este sentido, resulta alarmante el alto grado de desconocimiento que poseen directivos, docentes, padres e incluso orientadores sobre las distintas vulnerabilidades y riesgos que presenta el uso de las TIC, especialmente en cuanto a temas de seguridad informática en el uso de Internet. Se ha evidenciado que la gran mayoría no es capaz de identificar acciones preventivas tales como: evitar entrar en ciertas páginas web, facilitar datos personales a extraños o en plataformas de dudosa reputación, o intercambiar contenidos de naturaleza personal (fotos, videos, teléfonos, dirección, nombres y apellidos, números de identificación, entre otros). Usualmente, los jóvenes repiten las advertencias que hacen principalmente sus padres, familiares y docentes; sin embargo, no son conscientes de que el peligro en la red es real, aunque muchos están convencidos de que los peligros planteados son algo ficticio, y que no están expuestos a esos riesgos, consideran que a ellos no les pasará nada relacionado con las técnicas de ingeniería social ni serán víctimas de ciberdelincuentes, pero no toman precauciones para que esto sea así [49]. Muchos desconocen lo que es una buena o mala práctica en el uso de las TIC, los más jóvenes de 11 años o menos, desconocen un uso inadecuado o existencia de riesgos y comenten errores como:

- No informar a adultos (padres, docentes o familiares) sobre situaciones confusas o extrañas experimentadas durante su uso de internet
- Ingresan en páginas web no autorizadas o prohibidas
- Se dejan engañar fácilmente, especialmente los más jóvenes
- Descargan archivos sin verificar su legalidad, sin saber el contenido real d ellos mismos, exponiendo sus equipos a virus o programas que extraigan información personal
- Envían fotos, videos u otros materiales audiovisuales que pueden ser comprometedoras para su integridad física y mental

[49] NAVARRO, William., CÁRDENAS, Sonia., BAREÑO, Raúl. La importancia de la cultura en seguridad informática como experiencia innovadora en entidades de formación por competencias SENA. Recuperado en: 2016. Disponible en: https://www.researchgate.net/profile/Nau_Silverio_Gutierrez2/publication/321603716_Gestion_del_Talento_Humano_Enfoques_y_Modelos/links/5a289d43a6fdcc8e8671bcb4/Gestion-del-Talento-Humano-Enfoques-y-Modelos.pdf

- Contactan de forma permanentemente con personas desconocidas; a los cuales luego de caer en engaños o manipulaciones les facilitan datos personales propios y de familiares, datos de su vivienda, económicos, entre otros [50].

Frente a estas problemáticas, desde la seguridad informática es posible hacer uso de los denominados programas de "*Parental control*", a través de ellos es posible limitar el acceso de los niños a todos los contenidos que los padres consideren inapropiados, algunas de las herramientas más completas de este tipo utilizadas actualmente para controlar y educar los hábitos de los menores de edad en internet son[51]: Qustodio, ESET Parental Control, Web Filter PC, Amigo Control Parental y Kidbox[52].

Dentro de las funcionalidades de estos programas destaca: poder consultar el historial de sitios visita web, bloquear acceso a páginas específicas, limitar el tiempo de uso del internet estableciendo un horario, grabar en todo momento lo que ocurre en pantalla durante el tiempo de uso de internet por parte de los niños, También es posible restringir el acceso a los chats, establecer un límite para las descargas de archivos, así como programas y contenidos inapropiados, entre otros beneficios.

6.4. Proponer acciones preventivas frente a las técnicas de ingeniería social utilizadas en la red social Facebook contra los niños y niñas.

Desde la ingeniería de telecomunicaciones, se considera que algunas de las acciones preventivas que pueden implementarse para afrontar las técnicas de ingeniería social utilizadas en la red social Facebook por ciber delincuentes contra los niños y niñas, es que a través de la aplicación de la telemática es posible acceder a las redes sociales para establecer canales de seguridad y protocolos que minimicen la posibilidad de riesgos asociales a la ingeniería social.

Adicionalmente, una de las mejores acciones preventivas que pueden implementarse frente a las técnicas de ingeniería social es que los padres, docentes adquieran conocimientos y se auto instruyan sobre cuáles son los *modus operandi*

---

[50] NAVARRO, William., CÁRDENAS, Sonia., BAREÑO, Raúl. La importancia de la cultura en seguridad informática como experiencia innovadora en entidades de formación por competencias SENA. Recuperado en: 2016. Disponible en: https://www.researchgate.net/profile/Nau_Silverio_Gutierrez2/publication/321603716_Gestion_del_Talento_Humano_Enfoques_y_Modelos/links/5a289d43a6fdcc8e8671bcb4/Gestion-del-Talento-Humano-Enfoques-y-Modelos.pdf

[51] WAYRA, F. Herramientas para controlar los hábitos de tus hijos en internet. Barcelona [En línea]. Recuperado de: 28-12-2015. Disponible en: https://www.lavanguardia.com/tecnologia/internet/20151228/301074636856/control-parental-internet-hijos.html

[52] Idem

de los ciberdelincuentes con respecto a esto, el sitio web www.protecciononline.com, constituye un recurso de gran utilidad pues contiene abundante información actualizada y detallada para niños, niñas, adolescentes, jóvenes y adultos sobre las buenas prácticas del uso de internet, así como medidas de prevención, consejos, e incluso recursos informáticos, para realizar una navegación más segura en internet[53]. Algunas de las herramientas prácticas que se proporcionan en este sitio web para contribuir a minimizar esta problemática son:

- Guía para usuarios sobre identidad digital y reputación online
- Aplicaciones para encontrar *smartphones* perdidos
- Tutoriales para el uso de programas de control parental como Magic Desktop u otros
- Blogs informativos sobre aplicaciones gratuitas que protegen los documentos de la pc y móviles, entre otros.

La divulgación y utilización de estas herramientas en Colombia y otros países puede contribuir de forma significativa a minimizar los casos de crímenes de ingeniería social llevados a cabo en las redes sociales contra los niños y niñas, quienes han sido víctimas de abusos físicos y psicológicos a lo largo de los años debido a estas prácticas criminales.

[53] PROTECCIÓN ON LINE (2021). Protección on line. [En línea]. Disponible en: www.protecciononline.com,

RECOMENDACIONES

Con base en la investigación realizada se establecen las siguientes recomendaciones, enfocadas en brindar alternativas de solución frente a la problemática planteada:

- Desde el Ministerio de Tecnologías de la Información y Comunicaciones (MINTIC), es necesario concientizar a los padres a través de la implementación de políticas públicas enfocadas en la educación de la sociedad en general sobre los riesgos de la ingeniería social en niños y niñas.

- Igualmente, el MINTIC utilizando sus plataformas virtuales puede promover una mayor divulgación de las estadísticas de crímenes de ingeniería social, modus operandi de los cibercriminales, aportando información clave a los ciudadanos, educándolos para que sean capaces de reconocer alguna de estas situaciones adversas de llegarse a presentar y tomar las acciones adecuadas para eliminar la amenaza a sus hijos en entornos virtuales.

- Se debe fomentar la necesidad y conveniencia del acompañamiento por un adulto que guíe y proteja a los infantes de los posibles riesgos existentes en las redes sociales, esto puede lograrse a través de una mayor supervisión en el hogar por parte de los padres quienes pueden hacer uso de herramientas de control de contenido conocidos como control parental para tener una mayor supervisión de los contenidos a los cuales acceden los infantes.

- Los padres deben crear una cultura de autoeducación frente a las estrategias de ingeniería social y las formas de combatirlas, teniendo presente que, todo niño con acceso a internet puede estar expuesto a las mismas, de allí la necesidad de que los padres asuman un rol protagónico en el uso correcto de internet por parte de sus hijos.

- Se recomienda fomentar el uso de los programas de parental control desde los colegios a través de la implementación de proyectos de aprendizaje donde se involucren activamente la familia y comunidad, se manera que se asimile la importancia de los mismos generando aprendizajes significativos en todos los miembros de la comunidad educativa.

- Son diversos los estudios que se han llevado a cabo referente a estas temáticas que afecta la seguridad de niños en Colombia y el mundo entero. Sin embargo, debido al constante avance de la tecnología y el surgimiento de nuevas herramientas tecnológicas, las cuales también están al alcance de los cibercriminales, se ha hace necesario continuar indagando sobre este tema, de manera que se puedan generar alternativas de solución tanto a las estrategias

de ingeniería social existentes, como a todas aquellas que puedan llegar a surgir en un mediano o largo plazo.

CONCLUSIONES

Con base en los principales hallazgos de la investigación, se presentan las siguientes conclusiones:

- De acuerdo a la indagación documental realizada, pudo evidenciarse que la técnica de ingeniería social mayormente utilizada en el contexto colombiano a través de la red social Facebook en contra los niños y niñas es el Grooming, son diversos los casos registrados a lo largo de los años con respecto a este crimen y siendo víctimas cientos de infantes quienes han estado expuestos a riesgos tales como: abuso sexual, ciberacoso, pornografía infantil, agresiones físicas y psicológicas.

- Es un hecho que la seguridad informática puede aplicarse para intentar reducir los riesgos en el uso de Facebook por parte de los niños y niñas, pero para lograr esto es esencial que los padres, docentes y adultos responsables de supervisar a los niños, adquieran conocimientos útiles sobre las medidas preventivas que pueden aplicarse para prevenir o minimizar estos riesgos.

- Las acciones preventivas propuestas frente a las técnicas de ingeniería social utilizadas en la red social Facebook contra los niños y niñas, procuran fomentar una conciencia social sobre esta problemática presente en la actualidad, destacando que las tecnologías de la información y comunicación (TIC) a pesar de contribuir a grandes avances en la sociedad, también constituyen un mecanismo que puede ser utilizado por ciberdelincuentes, quienes están dirigidos a sectores vulnerables de la población como lo son los niños y niñas que utilizan las redes sociales sin supervisión.

7 BIBLIOGRAFÍA

AHLGRIM, B., y TERRANCE, C. Perceptions of cyberstalking: impact of perpetrator gender and cyberstalker victim relationship. Journal of interpersonal violence, 0886260518784590.

AVILA GUERRERO, Edward. Influencia de las redes sociales en los niños [en línea]. Disponible en: http://influredessociales.blogspot.com.co/p/fichas-bibliograficas.html

BORGHELLO, C., y TEMPERINI, M. G. I. Suplantación de identidad digital como delito informático.

CALDERA, M. I. F., HERNÁNDEZ, M. G., y CUENCA, A. B. R. Sexting: Nuevos usos de la tecnología y la sexualidad en adolescentes. International Journal of Developmental and Educational Psychology, 1(1), 521-533.

CARACOL RADIO. Rango de edad de jóvenes. [en línea]. Disponible en: http://caracol.com.co/radio/2012/10/31/nacional/1351677000_788427.html

CARLOS, L. Ciber-acoso en niñas y niños. Atlantico. [en línea]. Disponible en:http://sedici.unlp.edu.ar/bitstream/handle/10915/59753/Documento_completo.pdf-PDFA.pdf?sequence=1

CHACÓN-LÓPEZ, H., BARRIGA, J. F. R., Carretero, Y. A., y CARA, M. J. C. Construcción y validación de la escala de conductas sobre sexting (ECS). Revista Española de Orientación y Psicopedagogía, 27(2), 99-115.

SEMANA. cibercrimen en Colombia. [en línea]. Disponible en: https://www.semana.com/nacion/articulo/cibercrimen-en-colombia-balance-de-2020/551979

CNN. Peligro de Jóvenes en Facebook. [en línea]. Disponible en: http://cnnespanol.cnn.com/2020/10/05/tener-12-anos-el-peligro-de-merodear-en-redes-sociales/

COLOMBIA DIGITAL. Conceptos TIC [en línea]. Disponible en: http://repositorio.cepal.org/bitstream/handle/11362/37139/S1420568_es.pdf?sequence=1yisAllowed=y

COLOMBIA. CONGRESO DE LA REPUBLICA. Proyecto de ley 050/2020C (28 de julio de 2020). Ley contra Crímenes Cibernéticos. Cámara de Representantes.

COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Ley 1273. (5, enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado "de la

protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones [en línea]. Disponible en:

http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

DEL PERAL, J. A. M., y NAVARRO, P. V. Bullying, ciberbullying y sexting. Ediciones Pirámide.

DORANTES, J., TRUJANO, P., y TOVILLA, V. Cyberbulling: Acoso on line. Revista Electrónica de Psicoterapias. com.

EDUCATIVO SEGURIDAD INFORMÁTICA. Spoofing [en línea]. Disponible en: http://segurdadenredes.blogspot.com.co/2020/11/pagina-enconstrucion.html

EL ESPECTADOR. Colombianos en Facebook. [en línea]. Disponible en: https://www.elespectador.com/noticias/colombianos/Usuarios-facebook-articulo-753040

EL ESPECTADOR. Padres pueden revisar cuentas de redes sociales. [en línea]. Disponible en: https://www.elespectador.com/noticias/judicial/padres-pueden-revisar-cuentas-de-redes-sociales-y-corre-articulo-576846

EL PAÍS. Internet no salvara al mundo. [en línea]. Disponible en: https://elpais.com/tecnologia/2013/11/04/actualidad/1383563820_084036.html

EL TIEMPO. Más de 3000 millones de usuarios en Facebook. [en línea]. Disponible en: http://www.eltiempo.com/tecnosfera/novedades-tecnologia/tipos-de-usuarios-de-facebook-segun-investigacion-118442

EL TIEMPO. De caras lindas y perfiles falsos en Facebook. [en línea]. Disponible en: http://blogs.eltiempo.com/el-lado-oscuro-de-internet/2020/04/28/de-caras-lindas-y-perfiles-falsos-en-facebook/

ENRIQUE, C. Victimización infantil sexual online: Valencia. [en línea]. Disponible en: https://www.researchgate.net/profile/Irene_Montiel/publication/275273999_Victimizacion_Infantil_Sexual_Online_Online_Grooming_Ciberabuso_y_Ciberacoso_sexual/links/553692660cf268fd001870be/Victimizacion-Infantil-Sexual-Online-Online-Grooming-Ciberabuso-y-C

ESPINOZA TRUJILLO, Sarita. Influencia de las redes sociales en los jóvenes. Disponible en: http://es.slideshare.net/SAwuita15/redes-socialesppt-34459822/

ESTRELLA, Á. M. Delitos y Redes Sociales: mecanismos formalizados de lucha y delitos más habituales. El caso de la suplantación de identidad. Revista GENERAL DE DERECHO PENAL, (22), 5.

FERNÁNDEZ, J. R., CHAMORRO, E. F., GIL, R. H., y SOMOLINOS, J. A. Evaluación de la privacidad de una red social virtual. RISTI-Revista Ibérica de Sistemas e Tecnologias de Informação, (9), 59-73.

GALENCE, V. P. El ciber-acoso con intención sexual y el child-grooming. cuadernos de criminología: revista de criminología y ciencias forenses, (15), 22-33.

GARCÍA, A. F. T. La web profunda, un sitio entre sombras y realidades/The deep web, a place between shadows and realities/A teia profunda, um lugar entre sombras e realidades. Ventana Informatica, (39).

GARCIA, Carlos. Hablemos de Spoofing [en línea]. Disponible en: https://hackingetico.com/2010/08/26/hablemos-de-SPOOFING/

GARCÍA-MALDONADO, G., MARTÍNEZ-SALAZAR, G. J., SALDÍVAR-GONZÁLEZ, A. H., SÁNCHEZ-NUNCIO, R., MARTÍNEZ-PERALES, G. M., y DEL CARMEN BARRIENTOS-GÓMEZ, M. (2012). Factores de riesgo y consecuencias del cyberbullying en un grupo de adolescentes. Asociación con bullying tradicional. Boletín médico del hospital infantil de México, 69(6), 463-474.

GLOSARIO DE INFORMÁTICA E INTERNET. Chain e-mail [en línea]. Disponible en: http://www.internetglosario.com/849/Chainemail.html

HERNÁNDEZ, C. ingeniería social phishing y baiting. [en línea]. Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6349/Ingenieria%20social%20Phishing%20y%20Baiting.pdf?sequence=1yisAllowed=y

HOOTSITE. reporte digital Colombia [en línea]. Disponible en: https://datareportal.com/reports/digital-2020-colombia

LA VANGUARDIA. La vanguardia. Amistades peligrosas. [en línea]. Disponible en: http://www.lavanguardia.com/cultura/20200311/54428050094/amistades-peligrosas-asaltan-goya.html

LAGO, M. J. D. Un acercamiento al nuevo delito child grooming: entre los delitos de pederastia. Diario La Ley, (7575), 1.

LEON ROJAS, Juan. Ataque de suplantación de identidad(mail-spoofing) [en línea]. Disponible en: http://cala.unex.es/cala/cala/mod/forum/discuss.php?d=7875

MACÍAS VILLARREAL, D. P. Derecho a la protección de datos personales de niños, niñas y adolescentes en redes sociales (Facebook) (Bachelor's thesis, Quito: Universidad de las Américas, 2017).

MALDONADO, C. E. (2018). La web profunda y las dinámicas de la información. En: Le Monde diplomatique, edición Colombia, Nro, 179, 34-35.

MANRIQUE SANDOVAL, S., LANCHEROS RODRÍGUEZ, J. P., ACOSTA CERVERA, T., y QUITIAN PEÑA, Y. Cartilla dirigida a directivos docentes para afrontar las incidencias negativas de la red social facebook en el comportamiento sexual de los niños y niñas de edades de ocho a diez años.

MENDEZ, L. Que es el Mail Spoofing y cómo evitarlo usando SPF [en línea]. Disponible en: https://www.webempresa.com/blog/que-es-el91mail-spoofing-y-como-evitarlo-usando-spf.html

MERCADO CONTRERAS, C. T., PEDRAZA CABRERA, F. J., y MARTÍNEZ MARTÍNEZ, K. I. Sexting: su definición, factores de riesgo y consecuencias. Revista sobre la infancia y la adolescencia, (10), 1-18.

MINTIC. Colombia es uno de los países con más usuarios en redes sociales en la región. [en línea]. Disponible en: http://www.mintic.gov.co/portal/604/w3-article-2713.html

MOLINA. Leonela. Delitos informáticos [en línea]. Disponible en: http://es.calameo.com/books/005155407963f214f1a28

MONTIEL, I. Cibercriminalidad social juvenil: la cifra negra. España. [en línea]. Disponible en: (http://www.redalyc.org/html/788/78846481008/).

NAVARRO, M. A. Violencia en la escuela secundaria maltrato entre iguales (Doctoral dissertation, Universidad del Salvador).

SARMIENTO, Oscar. Herramientas web 2.0 efecto en los aprendizajes de los jóvenes colombianos. [en línea]. Disponible en: http://www.redalyc.org/articulo.oa?id=31048902010

PAEZ, Andrea. Tipos de spoofing [en línea]. Disponible en: http://andrea0712.blogspot.com.co/2011/05/ejercicios_11.html

LA VANGUARDIA. Peligro en las redes Sociales.. [en línea]. Disponible en: http://www.vanguardia.com/mundo/tecnologia/323781-los-peligros-de-las-redes-sociales-para-ninos-y-jovenes

PHILLIPS, L. F., BAIRD, D., y FOGG, B. J. Facebook para educadores. A Secretaria Geral de Educação a Distância da Universidade Federal de São Carlos

(SEaD/UFSCar), s/a. Disponível em:< http://www. sead. ufscar. br/outros/Facebook% 20para% 20Educadores>. Acesso em, 31.

PUJOL, F. A. Detección automática de ciberbullying a través del procesamiento. Universidad de alicante, España. [en línea]. Disponible en: (https://rua.ua.es/dspace/bitstream/10045/64300/1/Psicologia-y-educacion_288.pdf).

RCN. El juego de la ballena azul. [en línea]. [Consultado 15 de marzo de 2020]. Disponible en: https://www.noticiasrcn.com/internacional-mundo/ballena-azul-no-un-juego-ninos-cinco-datos-demuestran-su-peligrosidad 77

REVISTA SEMANA. ¿Por qué nos exhibimos en redes sociales [en línea]. Disponible en: https://www.semana.com/cultura/articulo/por-que-nos-exhibimos-en-redes-sociales/489607

RICO, M. N. Derechos de la infancia en la era digital. América Latina: CEPAL. [en línea]. Disponible en: https://www.cepal.org/es/publicaciones/37139-derechos-la-infancia-la-era-digital

ROSERO, Manuel Antonio. Los riesgos en las redes [en línea]. Disponible en: http://cucuta.extra.com.co/noticias/columnistas /los-riesgosen-las-redes-231027

SALUD INVESTIGA. Población, unidad de análisis, criterios de inclusión y exclusión. Muestra: identificación y reclutamiento [en línea]. Disponible en: http://www.saludinvestiga.org.ar/pdf/tutorias/poblacionymuestra.pdf

SANCHEZ VALVERDE, A. G. Ciberintimidación en estudiantes de secundaria asociado a trastornos del sueño en un Colegio de Lima-Leru Diciembre 2018.

SÁNCHEZ-TERUEL, D., y ROBLES-BELLO, M. A. Riesgos y potencialidades de la era digital para la infancia y la adolescencia. Educación y Humanismo, 18(31), 186-204.

SANDOVAL VALDERA, E. El delito de difamación en la modalidad de suplantación de identidad a través de la red social Facebook.

SEMANA. Con la internet estamos entre la espada y la pared. [en línea]. Disponible en: https://www.semana.com/tecnologia/articulo/leonard-kleinrock-experto-en-internet-habla-sobre-el-futuro-de-la-red/432212-3

SITES GOOGLE. Principales riesgos en redes sociales [enlínea]. Disponible en: https://sites.google.com/site/riesgosredes sociales2011/home/

SMITH, A. M. Protection of Children Online: Federal and State Laws Addressing Cyberstalking, Cyberharassment, and Cyberbulling. Congressional Research Service.

LA VANGUARDIA. Suplantación de Facebook. [en línea]. Disponible en: http://www.vanguardia.com/entretenimiento/farandula/244662-cristina-hurtado-denuncia-suplantacion-en-facebook

UNICEF. ¿Qué es la ciberintimidación? [en línea]. Disponible en: https://www.unicef.org/es/end-violence/ciberacoso-que-es-y-como-detenerlo

CNN. Usuarios de Facebook. [en línea]. Disponible en: http://cnnespanol.cnn.com/2020/04/11/que-debes-hacer-si-toda-tu-informacion-de-facebook-fue-expuesta-en-el-escandalo-de-cambridge-analytica/

VELÁSQUEZ DÍAZ, Noé. Redes sociales, gran influencia en los jóvenes [en línea]. Disponible en: http://es.slideshare.net/Velnoesitho/redessociales-gran-influencia-en-los-jvenes

VIDAL, M., VIALART, M. N., y HERNÁNDEZ, L. Redes sociales. Educación Médica Superior, 27(1), 146-157.

VILLADA, D., y JIMÉNEZ, A. La Web Semántica y la Web Profunda como Sistemas de Información: Análisis a una realidad. Revista Antioqueña de las Ciencias Computacionales, 7(1).

Fecha de Realización:	27/10/2021
Programa:	Especialización en seguridad informática
Línea de Investigación:	Infraestructura tecnológica seguridad en redes
título:	Análisis de los riesgos de seguridad a los cuales están expuestos los niños y niñas con el uso de la red social Facebook y cómo estos podrían reducirse.
Autor(es):	Arango Niño Julián Andrés
Palabras Claves:	Seguridad, cuidado, infancia, redes sociales, Facebook.
Descripción:	El presente trabajo el cual hace uso de la metodología de consulta y revisión de masas documentales, se permitirá profundizar respecto a los riesgos principales existentes con el uso frecuente e indiscriminado por parte de los niños y niñas de la red social a través de los diferentes métodos de ingeniería social con Facebook, en muchos casos con la inobservancia y falta de guía de un adulto responsable, lo cual es altamente aprovechado por delincuentes informáticos, para de esta manera dar a conocer la aplicabilidad de la seguridad informática en estas situaciones, así como de las posibles prácticas de prevención por parte de niños(as) y adultos que pueden ayudar a reducir estos riesgos.

Fuentes bibliográficas destacadas:

Sánchez-Teruel, D., & Robles-Bello, M. A. (2020). Riesgos y potencialidades de la era digital para la infancia y la adolescencia. Educación y Humanismo, 18(31), 186-204.

En TIC confío - Colombia. (2018). Así usan redes sociales los niños y

jóvenes en Colombia, from Enticconfio.gov.co

website: https://www.enticconfio.gov.co/Asi-usan-redes-sociales-los-ninos-y-

jovenes-en-colombia

Prevenga y proteja a sus hijos de caer en manos de los ciberdelincuentes a través de las redes sociales - Prevenga y proteja a sus hijos de caer en manos de los ciberdelincuentes a través de las redes sociales. (2019)., from MinTIC Colombia website: https://www.mintic.gov.co/portal/inicio/Sala-de-

<table>
<tr><td colspan="2">Prensa/Noticias/101798:Prevenga-y-proteja-a-sus-hijos-de-caer-en-manos-de-los-ciberdelincuentes-a-traves-de-las-redes-sociales

Platero, A., & Acedo, Á. (2016). La privacidad de los niños y adolescentes en las redes sociales: referencia especial al régimen normativo europeo y español, con algunas consideraciones sobre el chileno. Revista de Derecho y Tecnología, 5(2). https://doi.org/10.5354/0719-2584.2016.42557

AVILA GUERRERO, Edward. Influencia de las redes sociales en los niños [en línea]. Disponible en Internet en: http://influredessociales.blogspot.com.co/p/fichas-bibliograficas.html</td></tr>
<tr><td>Contenido del documento:</td><td>Hoy por hoy la tecnología está en la vida de mayoría de personas facilitando la comunicación entre sí, con el simple hecho de tener acceso a un dispositivo tecnológico, para nadie es un secreto que el internet es la red más grande del mundo, la cual permite que sea mucho más fácil y amigable interactuar con otros usuarios. Indiscutiblemente la tecnología llego y no se irá, así facilitando las actividades diarias que se hacen en dichas herramientas.

Muchas herramientas informáticas vienen de la mano con el internet la cual permiten la comunicación e interacción en los individuos que usan la web, dichas herramientas han tenido gran acogida, en varios casos cambian el destino de los individuos que usan las redes sociales, de igual manera estas herramientas facilitan tareas comunes en una persona sobre su vida cotidiana.

Un claro ejemplo de estas herramientas son las redes sociales que usan la mayoría de personas alrededor del planeta, pues estas son empleadas por un poco menos de la mitad de habitantes del mundo esta cifra se estima que aumenta anualmente en un 15% siendo así Facebook la red social con más popularidad en el planeta y por ende la más utilizada.</td></tr>
</table>

	Facebook está presente en muchas personas a nivel mundial y recolectó datos en el año 2.019 de 187.000 usuario y 34.000 de ellos menores de edad, así sea para trabajo o diversión, a lo que vamos, no podemos dudar que esta herramienta, la interacción entre usuarios se facilita. Facebook como red social trae consigo diversos beneficios, de igual manera también tiene sus riesgos si se hace un uso indebido de la misma, siendo tan lamentables los riesgos que pueden llevar a perder la vida. Se debe tener muy presente que los niños y niñas como menores de edad, están más propensos a los riesgos de Facebook, ya que los delincuentes que operan bajo esta red, los ven con inexperiencia e inocencia, lo que los hace una víctima fácil. La llegada de la tecnología trae una cantidad de delitos conectado con las diversas redes sociales, cabe resaltar que está, la suplantación de identidad el cyberbullying, el grooming, el sexting, y la pornografía infantil etc. Todos estos métodos de ingeniería social y como evitarlos lo encontraremos en nuestra investigación.
Marco Metodológico:	Análisis documentos científicos e información de la internet
Conceptos adquiridos :	Definiciones sobre los diferentes tipos de ingeniería social y como estos pueden ser prevenidos en la población infantil creación de matrices de análisis de riesgos
Conclusiones:	El trabajo de investigación permitió conocer que para el correcto uso de Facebook es necesario seguir las sugerencias tanto antes como después de crear nuestra cuenta relacionado a evitar los diferentes tipos de ingeniería social que pueden estar expuestos en los menores de edad sabiendo de antemano que a pesar de que hay restricciones para la creación de cuentas para menores ellos las omiten.

	Uno de los puntos más importantes es no brindar información la cual ponga en riesgo a tus familiares ni a ti mismo, de igual manera direcciones o fotos con algún tipo de contenido sexual. Adicional tener nuestro perfil de forma privada para que solo nuestros conocidos tengan acceso a nuestras publicaciones Tener presente que un ‘’me gusta’’ no cambia ni es relevante en nuestras vidas y de esta manera concientizar a los niños y niñas de que dicha plataforma es para compartir mas no para poner en riesgo nuestra integridad al momento de exponer la vida privada. Acatar las reglas de edad ya que estas están estipuladas en los términos y condiciones de dicha red social. La edad adecuada para comenzar a hacer uso de Facebook es a los 14 años bajo la supervisión de un tutor o padre.