MÉTODOS DE INGENIERÍA SOCIAL, UTILIZADOS POR LOS PEDERASTAS PARA COMETER GROOMING EN COLOMBIA

MARÍA CAMILA CLAVIJO CASTAÑEDA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

FACATATIVÁ

2020

MÉTODOS DE INGENIERÍA SOCIAL, UTILIZADOS POR LOS PEDERASTAS PARA COMETER GROOMING EN COLOMBIA

MARÍA CAMILA CLAVIJO CASTAÑEDA

Monografía para optar el título como Especialista en Seguridad Informática

Director

Ing. Hernando José Peña H.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

FACATATIVÁ

2020

Nota de Aceptación

_____

_____

_____

_____

_____

_____

Firma del presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Facatativá, septiembre del 2020

DEDICATORIA

Dedico este trabajo a Dios, a mis Amados Padres quienes con su amor buen ejemplo y dedicación han sido la catapulta para alcanzar el presente logro, en especial a mi Madre, quien ha luchado mucho para lograr que yo sea la persona que soy hoy en día. A mi tía, una mujer maravillosa, quien ha estado siempre conmigo.

También va dedicado a todos los niños de Colombia y el mundo, espero de todo corazón que la información proporcionada en esta monografía sirva como una herramienta de estudio y de aprendizaje para evitar que los delincuentes, y pederastas continúen dañando nuestros niños a adolescentes por medio de las redes sociales.

AGRADECIMIENTOS

A Dios primero que todo, por ser quien día a día, me da las fuerzas necesarias la inteligencia, la sabiduría, para afrontar cada situación que se presenta en mi entorno vivir y sobre todo por darme la oportunidad de estudiar, y de continuar con este posgrado a pesar de las dificultades y obstáculos que se llegan a presentar en el camino.

A mi madre por ser la persona que me inculco el amor por el estudio, y por qué gracias a sus esfuerzos y dedicaciones estoy hoy en día presentando este proyecto de grado.

A la Universidad Nacional Abierta y a Distancia y a todos sus docentes académicos, porque gracias a ellos y a sus metodologías de aprendizaje hoy en día he adquirido muchos conocimientos que en algún momento de mi vida no imagine tener, hoy en día me siento profundamente agradecida y orgullosa de ser Unadista.

TABLA DE CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

RESUMEN

En la actual monografía se busca reconocer los distintos métodos de la ingeniería social que son utilizados por los delincuentes informáticos los cuales hacen uso de redes sociales para contactar a menores de edad por medio de engaños. El documento permite al lector conocer los principales objetivos del porque un ciber acosador, (pederasta), quiere acceder y ganarse la confianza de un menor de edad o adolescente para posteriormente obtener beneficios sexuales, (fotos y videos donde se puede observar al menor de edad desnudo o mostrando sus partes íntimas, lo cual puede ser utilizado por el acosador como material pornográfico para distribuir y vender, puede presentarse, encuentros sexuales entre la víctima y el pederasta, chantajes hacia este y a sus padres para no revelar el material que se tiene, con el fin de obtener dinero) beneficios monetarios, introducir a la niño en el mundo de la pornografía infantil, para que creen material sexual, o para la prostitución de menores de edad, se podrán observar los métodos más comunes que utilizan para ganarse la confianza de estos y posteriormente identificar las consecuencias negativas que trae consigo dichos actos.

También se podrá observar el perfil criminológico de los delincuentes informáticos, que utilizan la ingeniería social para tener contacto con la población infantil, y se

pretende finalizar con un análisis e implementación de técnicas que podrán mitigar o evitar que se presente dicho problema.

Palabras clave:

Ingeniería social, cibercrimen, ciberacoso, grooming, pornografía infantil.

ABSTRACT

This monograph seeks to recognize the different methods of social engineering that are used by computer criminals who make use of social networks to contact minors through deception. The current document allows the reader to know the main objectives of why a cyber stalker, (pedophile), wants to access and gain the trust of a minor or adolescent to later obtain sexual benefits, (photos and videos where you can observe the child of Naked age or showing their intimate parts, which can be used by the stalker as pornographic material to distribute and sell, can occur, sexual encounters between the victim and the stalker, blackmails towards the victim and his parents so as not to reveal the material that is Has the victim by the stalker, in order to obtain money) monetary benefits, introduce the victim to the world of child pornography, so that they create sexual material, or for child prostitution, the most common methods that they use to gain the confidence of the child population and subsequently identify the negative consequences that come with these acts

You can also see the criminological profile of computer criminals, who use social engineering to have contact with the child population, and it is intended to end with an analysis and implementation of techniques that can mitigate or prevent this problem

Keywords:

Social engineering, cybercrime, cyber bullying, grooming, child pornography.

TITULO

MÉTODOS DE INGENIERÍA SOCIAL, UTILIZADOS POR LOS PEDERASTAS PARA COMETER GROOMING EN COLOMBIA.

INTRODUCCIÓN

En los últimos años, los ciberataques y ciberdelitos se han incrementado exponencialmente, de tal manera, que las técnicas empleadas para tal fin se están volviendo cada vez más sofisticados y por ende más eficientes y eficaces, claro, sin olvidar las técnicas más antiguas, que de una u otra forma siguen siendo muy funcionales al momento de atacar a una víctima determinada.

Teniendo en cuenta lo anterior, la monografía que se presenta se centra básicamente en identificar las técnicas que utiliza la ingeniería social para atacar a menores de edad a través de las redes sociales, aprovechando la inocencia, la falta de conocimiento y el miedo que provocan los victimarios a través de la psicología, además se plantearan alternativas que mitiguen este impacto en la población infantil colombiana, que día tras día se ve más afectada por este flagelo.

Es cierto, que la ingeniería social es una técnica que se ha empleado desde el principio de los tiempos, como un método que utiliza la psicología para engañar y sustraer la información necesaria y requerida de sus víctimas, en la antigüedad se hacía de manera personal, cuando la tecnología emerge en el mundo las técnicas se hicieron más eficientes haciendo que esta se convirtiera desde los años setenta en un problema global, y ahora con el surgimiento de la internet, la suplantación se

ha incorporado a la formula, en algunos casos para obtener información sobre cuentas bancarias entre otros, pero se insiste que lo más preocupante se observa cuando los delincuentes comienzan con un trabajo muy fuerte ganándose la confianza de menores de edad para que estos entreguen material delicado, que de alguna manera comprometerá su integridad física y psicológica.

Los datos que se pretenden recolectar como resultado de la monografía son de tipo cuantitativo ya que dentro de los objetivos se quiere obtener el rango de edad de los menores afectados por el grooming.

1. DEFINICIÓN DEL PROBLEMA

1.1. ANTECEDENTES DEL PROBLEMA

En Colombia y en el mundo se encuentra en auge la tecnología y por supuesto de esta se derivan las redes sociales, las cuales permiten al usuario tener una mayor interacción con otros, sin necesidad de tener un acercamiento presencial, por tal motivo y de manera desafortunada se han aumentado los casos de delitos cibernéticos, entre ellos el grooming y la ingeniería social.

Durante el desarrollo de la presente monografía se pretende hablar sobre el grooming y la extorción virtual causada por el sexting que son delitos informáticos, que hoy en día están de moda y, a la que se ve sometida la población de niños colombianos, identificando los métodos de ingeniería social que son utilizados para realizar dicho proceso, según información proporcionada por el periódico ABC, padres e hijos,[1] el grooming ha aumentado un 410% en los últimos años, convirtiéndose en un gran riesgo para la población de los menores de edad y según

[1] ABC, familia. Qué es el «grooming» y por qué ha aumentado un 410% en los últimos años [en línea]. En: ABC. España, marzo 10 de 2019. [Consultado: 16 de septiembre de 2020]. Disponible en: http://uao.libguides.com/c.php?g=529834&p=3623716#Periodico

el periódico CNN[2] en un estudio que realizaron 1 de cada 4 jóvenes ha recibido o enviado mensajes con imágenes sexuales, es notable la conexión que tiene el grooming con el sexting, ya que mediante el grooming uno de los resultados que se logran es el sexting.

La ingeniería social, el grooming y la extorción están directamente relacionadas ya que por medio de la ingeniería social y mediante diferentes tipos de técnicas, en este caso en específico utilizando psicología y redes sociales el delincuente ubica perfiles de menores de edad, procede a entrar en contacto con ellos, mediante perfiles falsos, utilizando diferentes personalidades, (suplantación de identidad), se gana la confianza de los niños, adolescentes y extrae directa o indirectamente información útil entre ellas material sexual, para posteriormente obtener beneficios sexuales y monetarios, afectando en gran manera a las victimas tanto física como psicológicamente.

Es de suma importancia tener presente que según el periódico de La República[3], Colombia es el tercer país, con un 19%, en Latinoamérica donde se presentan más

[2] CNN.1 de 4 jóvenes dice que ha hecho 'sexting', según un estudio [en línea]. En: CNN, febrero 28 de 2018. [Consultado: 16 de septiembre de 2020]. Disponible en: https://cnnespanol.cnn.com/2018/02/28/1-de-4-jovenes-dice-que-ha-hecho-sexting-segun-un-estudio/

[3] MOLANO TORRES, Natalia. Colombia es el tercer país con más ataques de ingeniería social en América Latina [en línea]. En: LA REPUBLICA. Bogotá D.C. marzo 10 de 2019. [Consultado: 16 de septiembre de 2020]. Disponible en: https://www.larepublica.co/empresas/colombia-es-el-tercer-pais-con-mas-ataques-de-ingenieria-social-en-america-latina-2928973

ataques de ingeniería social, después de Costa Rica que obtuvo un 21% y Uruguay con un 24%.

Planteado el contexto, surge la necesidad de identificar los métodos más comunes que utiliza un pederasta, valiéndose de ingeniería social para acercarse a un menor de edad y vulnerar su inocencia, cometiendo delitos sexuales cibernéticos, para posteriormente enseñar la manera de identificar a dichos depredadores y sensibilizar a la población infantil y en general a la comunidad; para tener un mejor habito y uso de las redes sociales para no caer en manos de los delincuentes informáticos.

1.2. DESCRIPCIÓN DEL PROBLEMA

Cuando se desconoce la manera correcta de manejar el internet o una red social, y se carece de información y conocimiento acerca de los delitos informáticos, como en este caso en específico el grooming y la ingeniería social, el usuario (menor de edad) o en general cualquier persona, se convierte en una víctima fácil de asechar y de engañar. Por tal motivo se convierte en algo fundamental para aprender a conocer y a practicar los métodos más sanos, los hábitos correctos de acceder en la web y de comportarnos en el entorno del internet.

1.3. FORMULACIÓN DEL PROBLEMA

El grooming se vale de diferentes técnicas de ingeniería social para acercarse a los menores de edad y cometer actos sexuales, desencadenando una cadena de sucesos y problemas psicológicos y físicos en la victima.

Por los hechos anteriormente mencionados se pretende dar respuesta a la siguiente pregunta:

¿Cómo y con qué hábitos se pueden evitar los casos de acoso sexual cibernético, que son utilizados por la ingeniería social y que afectan directamente a la población infantil en el territorio colombiano?

2. JUSTIFICACIÓN

La tecnología es un elemento muy importante e imprescindible en la vida del ser humano por tal motivo la mayoría de las generaciones la utilizan todos los días, dentro de los beneficios que ofrece la tecnología se encuentran las llamadas redes sociales los cuales son lugares alojados en la internet que permiten al usuario conectarse e interactuar con otra persona sin importar la distancia en la que se encuentren, Hütt Herrera, Harold[4] afirma que “el objetivo de las redes sociales se cumplen al lograrse la comunicación fluida y eficiente”, pero también es importante tener en cuenta que así como las redes sociales le han facilitado la vida a muchos individuos y los ha acercado con sus familiares y amigos acortando virtualmente la distancia y el manejo del tiempo, se ha hecho visible una gran problemática, un aspecto negativo que se ha infiltrado en el uso de las redes sociales, los cuales se encuentran catalogados en la lista de los delitos informáticos, por tal causa se ve necesario realizar una investigación más profunda y exhaustiva. En este caso en específico, dentro de la revisión que se va a realizar, se buscara todo lo relacionado con el grooming, el cual es una práctica que conlleva a cometer delitos informáticos como lo son: ingeniería social y sus métodos, extorción, sexting, suplantación de identidad y que están directamente relacionados con el mal uso de redes sociales.

[4] HÜTT HERRERA, Harold. Las redes sociales: una nueva herramienta de difusión [en línea]. Reflexiones. San José, Costa Rica. Universidad de Costa Rica. 2012. Vol. 91, núm. 2. [Consultado el 30 de septiembre de 2019]. Disponible en: https://www.redalyc.org/pdf/729/72923962008.pdf

Por lo mencionado anteriormente se ve necesario identificar las técnicas de ingeniería social que utilizan los delincuentes informáticos para acceder a menores de edad por medio de las redes sociales, logrando como resultado practicar grooming, extorción cibernética, acoso sexual que son causada por el sexting, a la población infantil del territorio colombiano y después de obtener los resultados, se pretende brindar alternativas de solución y/o recomendaciones que mitiguen estos hechos, que sirvan como material para alertar, prevenir y erradicar dicha problemática, que afecta considerablemente a los niños de Colombia.

3. OBJETIVOS

3.1. OBJETIVO GENERAL:

Identificar los principales métodos que utiliza la ingeniería social para involucrarse en las redes sociales y acceder a la población infantil.

3.2. OBJETIVOS ESPECÍFICOS

- Realizar un análisis de las redes sociales más comunes el cual identifique el nivel de seguridad disponible para los menores de edad.

- Identificar el rango de edades de los niños y adolescentes que han estado expuestos en las trampas de la ingeniería social, teniendo en cuenta fuentes públicas y/o referentes al grooming para el establecimiento o generación de estrategias de protección.

- Recomendar procesos y metodologías que permitan la, identificación, mitigación y reducción del impacto que tiene el grooming en los menores de edad, a la población en general

4. MARCO REFERENCIAL

4.1. MARCO TEÓRICO

Con el aumento de la tecnología y su creciente exponencial se han creado diversas formas de comunicación por medio de internet, ya que es un medio de comunicación que todo el mundo utiliza tanto de forma personal como para empresas. Dentro de las personas que utilizan internet, se incluyen los menores de edad y los adolescentes, que hoy en día están incluidos dentro del llamado grupo de la generación Z. Que son niños y jóvenes que se reconocen porque la gran mayoría de su tiempo, lo emplean en línea, desde los más pequeños hasta los adultos de más o menos unos 23 años.

Pero con el surgimiento del internet surgieron las redes sociales como lo son Facebook, donde el diario El Imparcial[5] informa que esta red social tiene 2.7 millones de usuarios activos al mes, Mejía Llano Juan Carlos[6] quien es consultor y speaker

[5] MEXIA, Marcela. 7 datos de Facebook para el 2020 [en línea]. En: EL IMPARCIAL. México enero 07 del 2020. [Consultado: 20 de septiembre de 2019]. Disponible en: https://www.elimparcial.com/tijuana/columnas/7-datos-de-Facebook-para-el-2020-20200107-0010.html

[6] MEJIA LLANO, Juan Carlos. Estadísticas de redes sociales 2020: usuarios de Facebook, Instagram, YouTube, LinkedIn, Twitter, TikTok y otros [en línea]. Marketing Digital. (febrero 26 de 2020). [Consultado: 26 de abril de 2020]. Disponible en: https://www.juancmejia.com/marketing-digital/estadisticas-de-redes-sociales-usuarios-de-facebook-instagram-linkedin-twitter-whatsapp-y-otros-infografia/#2_Usuarios_activos_de_Instagram

de márquetin digital y transformación digital, en su página web identifica que Instagram tiene 1.000 millones de usuarios activos en un mes, Twitter tiene 339 mil millones, You Tube tiene 2.000 millones, y WhatsApp 1.600 millones, entre otros, plataformas que fueron realizadas con el fin de unir a las personas por medio del internet, las herramientas informáticas y de la comunicación, sin importar si están en diferentes lugares del mundo y las diferencias de horario, también surgió la delincuencia informática por tal motivo quienes la practican y que tienen gustos particulares por los niños (pederastas), aprovechan de esta tecnología creando perfiles falsos para aprovecharse de los niños y adolescentes, lo cual es conocido como grooming, esta problemática no solamente ocurre en Colombia, es una problemática que se presenta a nivel mundial, por eso se han realizado diversas investigaciones acerca del tema, para aprender a tomar medidas preventivas, para reconocer a los pederastas y los perfiles falsos, para reconocer las técnicas de ingeniería social que ejecuta el delincuente para acceder a los niños.

Dentro de los estudios que se han realizado sobre Grooming como antecedentes, se pueden encontrar las siguientes investigaciones relacionadas con el tema:

Algunas consideraciones sobre el meeting a child following sexual grooming through tics (contacto tics preordenado a la actividad sexual con menores). Escrito y publicado en el año 2011 por la profesora de Derecho Penal Lina Mariola Díaz Ortiz, el texto trata sobre el contacto Tics preordenado a la actividad sexual con menores,

Díaz Cortes, Lina Mariola[7] en su investigación realizada explica sobre el uso que le da el adulto a las Tics para poder acercarse a los menores de edad, con el fin de obtener beneficios sexuales (de parte de un menor de edad) como lo son fotos, videos, y encuentros sexuales los cuales le servirán al adulto para difundir el material con fines comerciales, personales, o para compartir en grupos de redes sociales que tengan que ver con adultos que tengan los mismos gustos.

Otra investigación referente al tema fue realizada y publicada por la Escuela de Cadetes de Policía General Francisco de Paula Santander[8], titulada con el nombre de: Caracterización de los factores psicosociales asociados al Grooming en Colombia, en donde se realizó un estudio de forma documental en donde se describen algunos de los patrones comportamentales de los pederastas en el ciberespacio, estas descripciones ayudan a la policía nacional de Colombia a identificar el perfil criminal de dichos delincuentes los cuales vienen atentando de manera progresiva contra el estado psicológico y físico de los menores de edad haciendo uso de las redes sociales

[7] DIAZ CORTES, Lina Mariola, Cuaderno Red de Cátedras Telefónica: Algunas consideraciones sobre el meeting a child following sexual grooming through tics (contacto Tics preordenado a la actividad sexual con menores) [en línea]. España. 4 p Telefónica. Universidad de Salamanca. Mayo 2011. [Consultado: 14 de febrero de 2020]. Disponible en internet: http://catedraseguridad.usal.es/sites/default/files/Cuaderno_02_Contacto_TICS_preordenado_act_sexual_con_menores.pdf

[8] GARCIA TORO, Carlos Mario, GONZALEZ PUENTES José Luis, y MENDOZA CARVAJAL Rafael Eduardo, Caracterización de los factores psicosociales asociados al Grooming en Colombia [en línea]. Administración Policial. Bogotá D.C. Escuela de Cadetes de Policía General Francisco de Paula Santander. Pregrado en Administración Policial. 2017. 35 p. [Consultado: 14 de febrero de 2020]. Disponible en internet: http://biblioteca.policia.edu.co:8080/bitstream/handle/123456789/1220/3017GARCIA.pdf?sequence=1&isAllowed=y

Por otra parte, se pueden encontrar diferentes denuncias en Colombia involucradas con la ingeniería social entre ellas están: en el portal de Min Tic[9] un caso de un periodista de 27 años de edad que entre los años 2011 y 2015 utilizo dos perfiles falsos en Facebook, en uno de ellos se hacía pasar por una mujer con el nombre de Juliana Salazar el cual uso para contactar a estudiantes de estratos altos, entre los rangos de 13 a 16 años para ganarse su confianza y posteriormente obtener fotos de los niños desnudos o con poses insinuantes, después haciendo uso de otro perfil falso en Facebook con el nombre de Andrés Monsalve contactó a las víctimas y los chantajeo pidiéndole más fotos y en otros casos se vio presencialmente con los chicos, la policía tiene la cuenta de que este delincuente tiene aproximadamente 150 víctimas.

4.2. MARCO CONCEPTUAL

En este apartado se podrá observar la descripción de los términos más importantes y que están involucrados con el tema principal.

[9] EN TIC CONFÍO. Tres casos de Grooming en Colombia. Ministerio de las TIC [sitio web]. 16 de febrero 2016 [Consultado: 14 de febrero de 2020]. Disponible en internet: https://www.enticconfio.gov.co/tres-casos-grooming-colombia

Se sabe que el internet es una herramienta muy útil para la humanidad, ya que permite realizar diversas tareas de la cotidianidad, pero también se debe tener en cuenta que detrás de una red de comunicaciones como lo es el espacio cibernético, se encuentra manejado por usuarios con diferentes tipos de personalidades, “buenos y malos” personas éticas, con valores y personas criminales quienes pueden llegar a tener diferentes daños psicológicos o problemas mentales.

Dentro de esas personalidades con problemas psicológicos se encuentran la pedofilia, pedófilo o la hebofilia lo cual se define como:

- **Pedofilia**: ROBAYNA PERERA, Margarita Rosa afirma que “es la inclinación de las personas a sentir una atracción sexual primaria hacia niños prepúberes.”[10]

- **Pedófilo**: ROBAYNA PERERA, Margarita Rosa afirma que “es el adulto que se interesa amorosa o sexualmente por niños o preadolescentes, es decir, aquellos que aún no han tenido el despertar sexual.

[10] ROBAYNA PERERA, Margarita Rosa. Pederastia y pedofilia: estado de la cuestión [en línea]. Agosto, 13, 2012. 1 p. [Consultado: 26 de septiembre de 2019]. Disponible en Internet: http://www.pensamientopenal.com.ar/system/files/2014/12/doctrina38697.pdf

Podría ser un adulto hombre o mujer, interesado por niños o niñas (desde bebés hasta preadolescentes).”[11]

- **Hebofilia:** ROBAYNA PERERA, Margarita Rosa afirma que **“**el adulto se interesa por adolescentes, aquellos que ya han tenido el despertar sexual pero aún no son adultos”[12] a los hebofilios no les interesan los niños, solamente los adolescentes.

- **Pederasta:** ROBAYNA PERERA, Margarita Rosa afirma que, a diferencia de los pedófilos, que son quienes no pasan a la acción, los pederastas son aquellos que tienen contacto físico con los niños o adolescentes, un pedófilo solo ve imágenes, videos y todo material sexual involucrado con niños, pero jamás los toca.

Según lo mencionado anteriormente, existen diferentes términos para identificar a los adultos que gustan de los menores de edad, y cabe destacar que los pederastas son personas que abusan sexualmente de los niños y o adolescentes, y uno de los medios ideales para asechar a la víctima es el internet, ya que por este medio se

---

[11] Ibid., p. 2, ROBAYNA PERERA, Margarita Rosa. Pederastia y pedofilia: estado de la cuestión [en línea]. Agosto, 13, 2012. 1 p. [Consultado: 26 de septiembre de 2019]. Disponible en Internet: http://www.pensamientopenal.com.ar/system/files/2014/12/doctrina38697.pdf

[12] Ibid., p. 2, ROBAYNA PERERA, Margarita Rosa. Pederastia y pedofilia: estado de la cuestión [en línea]. Agosto, 13, 2012. 1 p. [Consultado: 26 de septiembre de 2019]. Disponible en Internet: http://www.pensamientopenal.com.ar/system/files/2014/12/doctrina38697.pdf

han creado las redes sociales, las cuales permiten interactuar con otras personas sin necesidad de estar junto a esa estas o de manera presencial.

Otros términos importantes para continuar con la presente monografía son:

- **Grooming:** en el diccionario de Min Tic[13]**,** se describe como, el acto que realiza un mayor de edad cuando se gana la confianza de un niño y/o adolescente, la mayoría de las veces utilizando perfiles falsos en redes sociales, con el fin de obtener material pornográfico y realizar actos sexuales con las víctimas.

- **Ingeniería Social:** en el diccionario de seguridad informática Ona Systems[14] ingeniería social es, la técnica que se realiza con el fin de extraer información de manera sociable con el objetivo de evadir o ingresar a sistemas de información y poderlos manipular a su gusto, simplemente consiste en extraer información importante de personas, por medio de llamadas telefónicas, correos electrónicos, redes sociales o contacto directo.

- **Red social:** es un sitio alojado en la red, que le permite al usuario compartir información, comunicarse, relacionarse sin importar la distancia por la que estén

[13] MIN TIC. Glosario [en línea]. Bogotá, Colombia. [Consultado: 28 de abril de 2020]. Disponible en: https://www.mintic.gov.co/portal/inicio/Glosario/

[14] ONA SYSTEMS, Glosario de tecnología Ona Systems [en línea]. Bogotá, Colombia. [Consultado: 28 de abril de 2020]. Disponible en: https://www.onasystems.net/wp-content/uploads/2016/10/Glosario-seguridad-Ona-systems-2016.pdf

separados o la diferencia horaria.

- **Delito informático**: en el diccionario de seguridad informática Ona Systems[15] se define el delito informático, como la acción ilícita que se realiza utilizando medios electrónicos o informáticos.

- **Ciberacoso:** en el diccionario de Min TIC[16], se describe al ciberacoso**,** como el acto que se realiza cuando se acosa a una persona o comunidad, por medio de redes sociales, divulgando información personal, falsa, acosando sexualmente, chantajeando, extorsionando entre otros.

- **Cibercrimen:** en el diccionario de seguridad informática Ona Systems[17] define el cibercrimen, como acto ilegal que se realiza utilizando internet dirigido a personas, empresas y organizaciones.

---

[15] Ibíd., p. 4. ONA SYSTEMS, Glosario de tecnología Ona Systems [en línea]. Bogotá, Colombia. [Consultado: 28 de abril de 2020]. Disponible en: https://www.onasystems.net/wp-content/uploads/2016/10/Glosario-seguridad-Ona-systems-2016.pdf

[16] MIN TIC. Op. Cit, p 35. Glosario [en línea]. Bogotá, Colombia. [Consultado: 28 de abril de 2020]. Disponible en: https://www.mintic.gov.co/portal/inicio/Glosario/

[17] ONA SYSTEMS. Op. Cit, p. 3. Glosario de tecnología Ona Systems [en línea]. Bogotá, Colombia. [Consultado: 28 de abril de 2020]. Disponible en: https://www.onasystems.net/wp-content/uploads/2016/10/Glosario-seguridad-Ona-systems-2016.pdf

- **Ciberdelito:** en el diccionario de seguridad informática Ona Systems[18] define el ciberdelito, como acto ilegal que se realiza usando elementos informáticos como redes y computadores.

- **Pornografía Infantil:** divulgación de material sexual y/o pornográfico donde aparecen niños y/o adolescentes.

- **Sexting:** en el diccionario de Min Tic[19], sexting se describe como, el acto de enviar o transmitir por medio de redes sociales, imágenes o videos con contenido sexual.

4.3. MARCO LEGAL

4.3.1. Norma de seguridad informática, Con el crecimiento exponencial que ha tenido la delincuencia informática y específicamente el acoso sexual por medio de internet, al que se ven expuestos los menores de edad, en Colombia se

[18] Ibíd., p. 3. ONA SYSTEMS, Glosario de tecnología Ona Systems [en línea]. Bogotá, Colombia. [Consultado: 28 de abril de 2020]. Disponible en: https://www.onasystems.net/wp-content/uploads/2016/10/Glosario-seguridad-Ona-systems-2016.pdf

[19] MIN TIC. Op. Cit, p 3. Glosario [en línea]. Bogotá, Colombia. [Consultado: 28 de abril de 2020]. Disponible en: https://www.mintic.gov.co/portal/inicio/Glosario/

han creado diferentes tipos de leyes las cuales se encargan de vigilar, y de evitar que se presenten delitos informáticos.

A continuación, usted podrá ver la descripción de los delitos informáticos que se encuentran tipificados en la ley 1273 del 2009 decretada por el Congreso Nacional de la República de Colombia[20], la cual se encarga de castigar cualquier acto que se presente en el territorio colombiano, en este caso en específico, los hechos que se cometen y que tienen como resultado después de hacer grooming.

Es necesario aclarar que el grooming en específico no se encuentra catalogado como delito informático dentro de la ley 1273 del 2009[21], pero las acciones que comete el pederasta al momento de realizarlo si son delitos, como lo es la suplantación de identidad, pornografía con menores de edad, sexting, los posibles encuentros sexuales que tiene el delincuente con el menor de edad y la ley 679 DE 2001, es la ley que se encarga de castigar la pornografía y el turismo sexual infantil, la cual es uno de los resultados que tiene al delincuente al hacer grooming.

[20] COLOMBIA. CONGRESO DE LA REPÚBLICA. 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]. Bogotá, D.C. Ministerio de Tecnologías de la Información y las Comunicaciones. p 1,2. [Consultado: 26 de septiembre de 2019]. Disponible en: https://www.mintic.gov.co/portal/inicio/3705:Ley-1273-de-2009

- **Artículo 269g: Suplantación de sitios web para capturar datos personales.**

El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave. En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave. la pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

- **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 1000 salarios mínimos legales mensuales vigentes.

- **Artículo 269H. Circunstancias de agravación punitiva:**

Las penas se imponen de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

- ✓ Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
- ✓ Por servidor público en ejercicio de sus funciones
- ✓ Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
- ✓ Revelando o dando a conocer el contenido de la información en perjuicio de otro.
- ✓ Obteniendo provecho para sí o para un tercero.
- ✓ Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
- ✓ Utilizando como instrumento a un tercero de buena fe.
- ✓ Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

4.3.2. Ley 679 de 2001 (agosto 3). El Congreso de la Republica de Colombia[22] expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución.

- **Artículo 1: Objeto.**

Esta ley tiene por objeto dictar medidas de protección contra la explotación, la pornografía, el turismo sexual y demás formas de abuso sexual con menores de edad, mediante el establecimiento de normas de carácter preventivo y sancionatorio, y la expedición de otras disposiciones en desarrollo del artículo 44 de la Constitución.

- **Artículo 7: Prohibiciones.**

Los proveedores o servidores, administradores y usuarios de redes globales de información no podrán:

[22] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 679 de 2001, Por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución. [en línea]. Bogotá, D.C. Unidad para la atención y reparación integral de las víctimas. 1,7 p. [Consultado: 26 de septiembre de 2019]. Disponible en: https://www.unidadvictimas.gov.co/es/ley-679-de-2001/13668

- ✓ Alojar en su propio sitio imágenes, textos, documentos o archivos audiovisuales que impliquen directa o indirectamente actividades sexuales con menores de edad.
- ✓ Alojar en su propio sitio material pornográfico, en especial en modo de imágenes o videos, cuando existan indicios de que las personas fotografiadas o filmadas son menores de edad.
- ✓ Alojar en su propio sitio vínculos o links, sobre sitios telemáticos que contengan o distribuyan material pornográfico relativo a menores de edad.

5. MÉTODOS DE INGENIERÍA SOCIAL UTILIZADOS POR LOS PEDERASTAS PARA INVOLUCRARSE EN LAS REDES SOCIALES Y ACCEDER A LA POBLACIÓN INFANTIL EN COLOMBIA

En este capítulo se podrá observar el resultado de los procesos que se realizaron para lograr reconocer cuáles son los métodos de ingeniería social que utiliza un pederasta para cometer grooming en Colombia, pero para obtener esos resultados anteriormente mencionados, es necesario que el lector obtenga información sobre ¿qué es ingeniería social?, ¿cuáles son los métodos que utiliza un ingeniero social?, ¿cuáles son los métodos más usados?, ¿qué es el grooming?, cuáles son los delitos sexuales infantiles vinculados con internet que están relacionados al grooming y sus

mecanismos de protección, lo cual podrán ver en un estudio que se realizó en el punto 9.3.

Posteriormente podrán dar lectura a un análisis realizado sobre los resultados obtenidos acerca del objetivo principal: Métodos de ingeniería social utilizados por los pederastas para involucrarse en las redes sociales y acceder a la población infantil en Colombia.

5.1. ¿QUE ES LA INGENIERÍA SOCIAL?

La ingeniería social es el arte de manipular psicológicamente a las personas de manera presencial o utilizando herramientas informáticas y de comunicaciones, para obtener información importante sobre una hombre, empresa u organización con fines ilícitos.

Romero Diego comenta en su investigación que:

> La ingeniería social no es un término moderno su existencia es de muchos años atrás, desde la creación del ser humano, la edad antigua, y la edad moderna, retrocediendo en el tiempo tenemos un primer ejemplo de esta, que ocurrió en la ciudad de Troya ubicada hoy en día en el país de Turquía cuando fue conquistada alrededor del año 1300 a.C. El plan de los griegos en ese entonces

> para su conquista incluía un caballo gigante construido en madera el cual denominaron los griegos “Caballo de Troya,” y que guardaba en su interior los soldados que acabarían con la ciudad entera, lo que parecía un obsequio resultó ser la trampa y la perdición para la ciudad de Troya.[23]

Por lo tanto se puede deducir que la ingeniería social es un delito informático que se ha venido practicando desde hace muchos años atrás, un ingeniero social, precisamente no es un hacker, esa palabra no se refiere a una persona que necesariamente tiene muchos conocimientos en el área de sistemas, simplemente es una hombre que cuenta con buenas habilidades de comunicación e interacción con los demás, la cual es capaz de extraer información privada importante, que le puede servir para cometer delitos informáticos como lo son: el grooming, el phishing, el vishing, el pretexting, entre otros.

[23] ROMERO, Diego. El arte de la ingeniería social [en línea]. Especialización de Seguridad Informática. Bogotá D.C. Universidad Piloto de Colombia. [Consultado: 23 de febrero de 2020]. Disponible en Internet: 2 p. http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6354/El%20arte%20de%20la%20ingenier%c3%ada%20social.pdf?sequence=1&isAllowed=y

5.2. MÉTODOS MAS UTILIZADOS POR LA INGENIERÍA SOCIAL

5.2.1. Phishing. Andalucía Cert[24], clasifica el phishing dependiendo del objetivo y la función del ataque.

5.2.2. Phishing tradicional. Andalucía[25] dentro de su libro especifica que este ataque suele ser el más común y empleado en las campañas intensivas, por lo general su método de actuar es la falsificación de un sitio web, que la víctima utiliza con mucha frecuencia, su funcionamiento consiste en que el usuario introduce sus datos personales en la página web falsificada, esos son capturados y posteriormente son transferidos al atacante, ese tipo de campañas son enviadas a muchas personas para poder estafarlas.

5.2.3. Spear phishing. De igual manera Andalucía[26] identifica que con esta modalidad el ataque va dirigido a grupos o personas reducidas, con ese tipo de

---

[24] CERT Andalucía. Informe de divulgación Phishing [en línea]. Centro Andaluza para el Desarrollo de las Telecomunicaciones. CONSEJERIA DE EMPLEO. EMPRESA Y COMERCIO. 06 de noviembre de 2017. 22 p [Consultado: 01 de marzo de 2020]. Disponible en internet: https://www.seguridad.andaluciaesdigital.es/documents/410971/1437699/phising+2017/01950ce7-731f-48a6-821a-79388e571bff

[25] Ibid., p. 4. CERT Andalucía. Informe de divulgación Phishing [en línea]. Centro Andaluza para el Desarrollo de las Telecomunicaciones. CONSEJERIA DE EMPLEO. EMPRESA Y COMERCIO. 06 de noviembre de 2017. 22 p [Consultado: 01 de marzo de 2020]. Disponible en internet: https://www.seguridad.andaluciaesdigital.es/documents/410971/1437699/phising+2017/01950ce7-731f-48a6-821a-79388e571bff

[26] Ibid., p. 4. CERT Andalucía. Informe de divulgación Phishing [en línea]. Centro Andaluza para el Desarrollo de las Telecomunicaciones. CONSEJERIA DE EMPLEO. EMPRESA Y COMERCIO. 06 de noviembre de 2017. 22 p [Consultado: 01 de marzo de 2020]. Disponible en internet:

ataque se emplea la ingeniería social, ya que va dirigido a personas y grupos estudiados con anterioridad con el fin de atacar de manera efectiva una empresa o red.

5.2.4. Whale phishing. Andalucia[27] en su informe identifica que esa modalidad va dirigida a personas que tienen cargos altos en una empresa, hay que tener estudios previos sobre la forma en la que se va a realizar el ataque, para que sea más preciso y confiable.

5.2.5. Vishing. En el libro Metodologías de la Ingeniería Social Rodríguez Rincón Ellien Yulieth [28] resalta que en aquella modalidad se combinan las llamadas telefónicas y la ingeniería social ya que la técnica consiste en realizar llamadas supuestamente de parte de parte de entidades financieras con el fin de sacarle información importante a la víctima, relacionada con sus cuentas bancarias, entre otros y así mismo poder suplantar la identidad y posteriormente obtener beneficios monetarios.

---

https://www.seguridad.andaluciaesdigital.es/documents/410971/1437699/phising+2017/01950ce7-731f-48a6-821a-79388e571bff

[27] Ibid., p. 4. CERT Andalucía. Informe de divulgación Phishing [en línea]. Centro Andaluza para el Desarrollo de las Telecomunicaciones. CONSEJERIA DE EMPLEO. EMPRESA Y COMERCIO. 06 de noviembre de 2017. 22 p [Consultado: 01 de marzo de 2020]. Disponible en internet: https://www.seguridad.andaluciaesdigital.es/documents/410971/1437699/phising+2017/01950ce7-731f-48a6-821a-79388e571bff

[28] RODRIGUEZ RINCON, Ellien Yulieth. Metodologías de la ingeniería social. [en línea]. Trabajo de investigación Magister Universitario en las Seguridad de las TIC. Madrid España Universidad Oberta de Cataluña. Junio 2019. 17 p. [Consultado: 01 de marzo de 2020]. Disponible en internet: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/81255/6/jrodriguezrinTFM0618memoria.pdf

5.2.6. Smishing. Técnica que consiste en enviar mensajes de texto a diferentes números de celulares haciéndose pasar por operadores de telefonías, canales de radio y televisión, entre otros para decirle a la víctima, por ejemplo: que es el feliz ganador de cien millones de pesos y que para reclamarlos debe consignarles cierto valor de dinero, a una cuenta determinada.

5.2.7. Pretexting. Técnica que consiste en que el ingeniero social crea una mentira y suplanta una identidad del personal de una empresa escogida con anticipación para manipular la recepción de la información.

5.2.8. Baiting. Técnica que menciona Rodríguez Rincón Ellien Yulieth,[29] en su investigación, es muy parecida al phishing, ya que consiste en obtener información por medio por ejemplo del ingreso de datos personales importantes con el objetivo o a cambio de que el usuario descargue música o películas gratis, sin saber que posiblemente están dando sus datos a delincuentes informáticos, otra forma es el regalo de medios físicos (infectados) a empleados de una empresa, con el objetivo de que esos medios sean insertados en un computador y secuestren el equipo.

[29] Ibid., p. 16. RODRIGUEZ RINCON, Ellien Yulieth. Metodologías de la ingeniería social. [en línea]. Trabajo de investigación Magister Universitario en las Seguridad de las TIC. Madrid España Universidad Oberta de Cataluña. Junio 2019. 17 p. [Consultado: 01 de marzo de 2020]. Disponible en internet: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/81255/6/jrodriguezrinTFM0618memoria.pdf

5.2.9. Quid pro quo. Método que consiste en un intercambio, es decir que el empleado u operador de una empresa le ayuda a solucionar un problema de la vida real al usuario, a cambio de dinero o información importante, esto se realiza sin estar autorizados por la empresa.

5.2.10. Grooming. El grooming es una práctica que conlleva a cometer diferentes delitos informáticos, el cual consiste en que un adulto suplante una identidad, haciéndose pasar por un niño o adolescente, actor, influencer, cantante o alguien llamativo para lograr utilizando la ingeniería social hacer contacto por medio de redes sociales con los menores, después de hacer contactos con ellos que en este caso son las víctimas, el delincuente que en este caso es un pederasta, entabla una amistad con este, y es ahí donde empieza a sacar información importante de los chicos y la familia, el objetivo del delincuente es obtener imágenes sexuales (sexting), videos pornográficos, encuentros sexuales entre otros, incluso el atacante puede tener como objetivo vender el material pornográfico o aún más vender a las víctimas para turismo y explotación sexual.

5.2.11. Tailgating. Fernández, Manuel[30] en su blog de seguridad y privacidad menciona, que este delito consiste en ingresar infiltrado a un lugar que no esté

[30] Fernández Manuel. Ingeniería Social: ¿qué es el Tailgating (o «ir a rebufo»)? [blog]. Bélgica. 11 de septiembre 2018. [Consultado: 03 de marzo de 2020]. Disponible en: https://blog.mailfence.com/es/que-es-el-tailgating/#pll_switcher

supervisado por personas, o que su ingreso sea mediante por medios electrónicos para acceder a lugares no autorizados donde pueden existir cosas importantes.

5.2.12. Redes sociales. Las redes sociales son un método de la ingeniería social ya que por ese medio se puede estudiar a la víctima, las cosas que le gusta hacer, los lugares que le gusta visitar, su información personal, entre otras cosas más, con el objetivo de más adelante ejecutar alguna acción conveniente para el delincuente.

5.3. MÉTODOS DE INGENIERÍA SOCIAL QUE UTILIZA UN PEDERASTA PARA COMETER GROOMING EN COLOMBIA

Los acosadores son individuos que tienen un objetivo sexual, contra un menor identificado con anterioridad, y son capaces de pasar por encima de cualquier perjuicio que puedan ocasionar a sus víctimas con tal de conseguir su “trofeo”. Son personas inteligentes con una gran perseverancia, paciencia, capacidad de manipulación y embaucación, que juegan con el poder de su madurez contra la indefensión de la inocencia del niño, para que cuando llegue el momento oportuno, poseer la frialdad necesaria para cometer el delito de chantaje emocional y alcanzar su objetivo principal: obtener contenidos sexuales del menor, ya sea mediante el

envío de fotografías, vídeos, audios o incluso llegar a establecer contacto físico con él. Para ello, se ocultan tras una máscara que les permite crear las redes sociales, diseñan un plan de actuación que les sirva para acceder a la vida de un menor haciéndose pasar por alguien afín a él con quien poder charlar, convertirse en su mejor amigo "anónimo-desconocido", y ganar su confianza. Se convertirá en su confidente y adoptará un rol que hará que el chico se sienta cómodo y seguro sin darse cuenta de que la realidad no sabe quién está al otro lado de la pantalla.

El grooming es un conjunto de métodos y técnicas de ingeniería social, (el cual se ejecuta en varias fases), que utiliza un pederasta que también es catalogado como delincuente informático, ya que en este caso usa las redes sociales para lograr acceder a un menor de edad, con el objetivo de entablar una amistad o algún vínculo afectivo con un menor de edad, en este apartado se describirán las técnicas, las fases y los métodos que son utilizados por el este.

Inteco[31] en su guía de actuación contra el ciber acoso mencionan los perfiles que participan en el grooming, y resaltan que la mayoría de las veces son los mismos que participan en el acoso físico, quienes en este caso son los acosadores, la víctima y los espectadores que son quienes están enterados de lo que está

[31] INTECO. Guía de actuación contra el ciberacoso padres y educadores [en línea]. Instituto Nacional de las Tecnologías de la comunicación. Ministerio de Industria Tecnología y Comercio. Octubre 2012. p 15. [Consultado: 02 de mayo de 2020]. Disponible en internet: https://www.alcobendas.org/recursos/doc/Educacion/539233046_42201383324.pdf

sucediendo, pero prefieren callar. Rodríguez Rincón Ellien Yulieth, [32] en su libro Metodologías de la Ingeniería Social identifica un conjunto de técnicas que emplea el pederasta para hacer interacción con este y cometer grooming.

En la tabla 1 denominada Técnicas y fases en empleo para interactuar con la víctima y cometer grooming, se están identificando las técnicas de interacción que utiliza el pederasta al realizar la acción, las cuales están descritas como técnicas pasivas, no presenciales, presenciales no agresivas y agresivas y que se verán descritas a continuación.

[32] RODRIGUEZ RINCON, Ellien Yulieth. Op. cit., p. 17. Metodologías de la ingeniería social. [en línea]. Trabajo de investigación Magister Universitario en las Seguridad de las TIC. Madrid España Universidad Oberta de Cataluña. Junio 2019. 17 p. [Consultado: 01 de marzo de 2020]. Disponible en internet: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/81255/6/jrodriguezrinTFM0618memoria.pdf

Cuadro 1 Técnicas y fases en empleo para interactuar con la víctima y cometer grooming

Pasivas	Presenciales no agresivas	No presenciales	Agresivas
• Implementación de ingeniería social • Observar • Analizar el comportamiento de la victima • Establecer un perfil psicológico (gustos, aficiones y hábitos)	• Resultados • Seguir la victima • Vigilar la casa y empleo de la víctima, sus familiares y personas más cercanas. • Buscar información en su entorno	• Trata de obtener información de la víctima por medio de redes sociales • Suplantación de identidad • Solicitud de información por • Solicitud de información por medio de emails, llamadas	• Extorciones • Presión psicológica • Presión física • Suplantación de identidad física • Abusos • Chantajes • Contacto sexual • Acoso sexual

		mensaje o texto	

Fuente: Propia

5.3.1. Técnicas pasivas y no presenciales. Rodríguez Rincón Ellien Yulieth [33] menciona en su investigación que en esta técnica el pederasta o delincuente informático empieza a implementar la ingeniería social, realizando observación y análisis por medio de las redes sociales de los perfiles o cuentas de los menores de edad que en este caso serán la víctima y que quiere seguir, los cuales le parecen interesantes y se acoplan al gusto del delincuente, como paso seguido elije la o las víctimas, identifica y establece un perfil psicológico de los niños, es decir que hace seguimiento a sus gustos, aficiones, hábitos, lugares que frecuenta. Después de haber elegido los niños que quiere seguir, suplanta la identidad de algún niño o adolescente, influencer, actor, cantante o una persona

[33] RODRIGUEZ RINCON, Ellien Yulieth. Op. cit., p. 17. Metodologías de la ingeniería social. [en línea]. Trabajo de investigación Magister Universitario en las Seguridad de las TIC. Madrid España Universidad Oberta de Cataluña. Junio 2019. 17 p. [Consultado: 01 de marzo de 2020]. Disponible en internet: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/81255/6/jrodriguezrinTFM0618memoria.pdf

famosa que sea llamativa, y que se acomode al gusto de la víctima, posteriormente crea un perfil falso incluyendo datos, imágenes y contenido en general que sea llamativo para las víctimas, después envía la solicitud y al ser aceptada empieza a buscar la forma de entablar conversaciones con las víctimas.

5.3.2. Técnicas presenciales no agresivas. Rodríguez Rincón Ellien Yulieth[34] menciona que en estas técnicas el pederasta al obtener la información personal de la víctima en algunos casos los sigue hasta su casa, incluso sigue a los familiares con el objetivo de buscar información acerca de ellos en el entorno en el que se desempeñan, pero en ese momento no los violenta ya que solamente está recolectando información acerca de sus vidas personales.

5.3.3. Técnicas agresivas. El pederasta empieza a ganarse la confianza de la víctima, se convierte en alguien indispensable, le empieza a pedir información personal, como por ejemplo el lugar donde reside, con quien vive, donde estudia, información sobre los ingresos económicos de la persona acosada, de sus padres y familiares, donde trabajan sus padres y familiares más cercanos, sitios que frecuentan, vienes que tienen, con esta información el delincuente establece si este le puede generar ingresos económicos, el suplantador se vuelve alguien

[34] RODRIGUEZ RINCON, Ellien Yulieth. Op. cit., p. 17. Metodologías de la ingeniería social. [en línea]. Trabajo de investigación Magister Universitario en las Seguridad de las TIC. Madrid España Universidad Oberta de Cataluña. Junio 2019. 17 p. [Consultado: 01 de marzo de 2020]. Disponible en internet: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/81255/6/jrodriguezrinTFM0618memoria.pdf

indispensable, para el niño y empieza a enamorarlo a costa de engaños y de manipulaciones psicológicas hasta q logra ganarse la confianza de este para luego pedirle fotografías insinuantes con cierto tipo de poses, poco a poco lo va convenciendo y con el transcurso del tiempo las imágenes llegaran a ser más íntimas, como por ejemplo mostrando sus partes íntimas, luego le pedirá que se grave mostrando su cuerpo desnudo con las poses que el atacante quiera, este material con características sexuales será enviado por medio de la red social que estén utilizando para contactarse, a él envió de fotos y videos pornográficos se le conoce con el nombre de Sexting, después de que el perseguidor ya tenga todo el material que quiera se volverá más agresivo ya que empezara a obligar a la persona a encontrase de manera personal, y en muchos casos llegando a tener encuentros de tipo sexual, los cuales serán usados, posteriormente por este individuo como elementos para extorsionar a menor en cuestión.

El delincuente puede realizar bastantes actos con ese material sexual, como lo es acosar a la víctima para que sigan manteniendo encuentros sexuales, le podrá pedir dinero a cambio de no publicar el contenido de los videos y/o imágenes, o en otros casos, vender el contenido pornográfico obtenido a personas que sean pederastas es decir que tengan gustos sexuales por los niños y adolescentes, podrá contactar a los padres o familiares de la o las víctimas para chantajearlos a cambio de no realizar ningún tipo de publicación que afecten su integridad emocional, el atacante también puede estar participando en grupos de redes sociales donde se compartan imágenes

y videos pornográficos donde los protagonistas sean menores de edad, incluso durante uno de los encuentros personales que tenga con la victima lo podrá secuestrar y venderlo para trata de blancas.

5.3.4. Fases del grooming. Palmer Padilla Fco Javier[35] explica que aparte de las técnicas y los métodos que utilizan los pederastas para hacer grooming, existen unas fases las cuales se van ejecutando a medida que se va ejecutando el delito, las fases son las siguientes:

- **Fase 1: Buscar la victima**

Como se mencionaba en las técnicas que se usan para hacer grooming, el delincuente en la primera fase busca a la o las víctimas, en redes sociales, hay que tener en cuenta que en Colombia las más utilizadas son WhatsApp, Facebook, Messenger, Instagram, Snapchat, YouTube, Twitter, las características más comunes que el pederasta tiene en cuenta son los niños más solos, depresivos, vulnerables, y que tengan poca atención de sus padres.

[35] PALMER PADILLA, Fco Javier. Seguridad en riesgos, Ciberbullyng, Grooming y Sexting [en línea]. Trabajo de investigación de máster en seguridad informática. España. Universidad Oberta de Cataluña. Facultad de Ciencias Básicas. Departamento de Ingeniera de sistemas. 2017. 27 p. [Consultado: 08 de marzo del 2020]. Disponible en Internet: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/67105/6/fpalmerpTFM0617memoria.pdf

- **Fase 2: Enganche**

En esta fase el acosador empieza a mantener conversaciones con el niño, le pregunta su edad, sus gustos, sus actividades, donde vive, es allí, donde empieza a estrechar lazos de amistad con la víctima.

- **Fase 3: Fidelización**

En esta fase el delincuente empieza a mostrarle al niño que tienen cosas en común, le muestra que tienen los mismos gustos, que realizan actividades similares, que les gusta el mismo género musical, y juegan los mismos videojuegos, de esta manera, lo conquista, y gana la confianza que desea, para sí, pasar a la siguiente fase, la cual consiste en preguntarle sobre los datos de los padres, situación económica, entre otros

- **Fase 4: Aislamiento**

En esta fase el Canal 13,[36] señala que al ser más amigos y tener más confianza, el acosador logra alejar al niño de sus padres y de su círculo social cercano, con el objetivo de convertirse en la persona más cercana e importante para el chico, y que no vaya a contar a nadie lo que está pasando entre los dos, es decir, la victima solo debe confiar en el delincuente.

[36] CANAL 13. Grooming, así opera en internet. [sitio web]. Bogotá. Redacción canal 13. 26 junio 2018. [Consultado: 05 de marzo de 2020]. Disponible en internet: https://canaltrece.com.co/noticias/grooming-que-es-etapas-y-caracteristicas/

- **Fase 5: Seducción**

En esta etapa, el delincuente a ganarse al niño por medio de halagos, de regalos, en muchas ocasiones le da dinero, esto hace que el chico se siente en deuda con el pederasta y que lo idealice como un héroe, es en este momento donde este empieza a acceder al envío de todo tipo de material pornográfico y hasta pueden tener encuentros sexuales.

- **Fase 6: Acoso**

En esta etapa el delincuente se muestra como es, empieza a acosar al niño, a intimidarlo, chantajearlo a cambio de no vender o publicar el material sexual, incluso puede amenazar a los padres o familiares del niño.

5.3.5. Métodos para hacer grooming. García Gachón Jonathan Orlando,[37] en su investigación menciona que “Los groomers o atacantes, siempre están desarrollando nuevas técnicas con el objetivo de evitar ser destacados y ser más efectivos en captar la atención de los menores”.

[37] GARCÍA GACHÓN, Jonathan Orlando. TFM, Ad hoc Seguridad y Riesgos: Ciberbullyng, Grooming y Sexting [en línea]. Trabajo Final de Master MISTIC Estudios de Informática Multimedia y Telecomunicaciones. España. Universidad Oberta de Cataluña, Universidad Autónoma de Barcelona, Universitat Rovira I Virgili, Universitat de les Illes Balears. 2017. 41 p. [Consultado: 02 de mayo de 2020]. Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/72526/6/ingjonathangarciaTFM0118memoria.pdf

El grooming puede tener diversos métodos, como se mencionó anteriormente, se necesitan técnicas y fases para ejecutar el delito, los procedimientos que emplea el delincuente son: crear un perfil falso, suplantar una identidad, puede ser de otro niño, actor, cantante, futbolista, o cualquier personaje importante y famoso de la farándula, y que sea llamativo para el menor de edad, en este caso es la fase de búsqueda y la técnica pasiva, no presencial, identifica los perfiles que más acordes estén con sus gustos, y procede a enviar las solicitudes de amistad, luego entabla amistad con los niños y buscar conversaciones nada fuera de lo común, posteriormente pasa a la fase 2 de enganche donde empieza a ser más amable con él, empieza a hablar con mayor frecuencia, se vuelven amigos, muy cercanos, comienza a obtener información importante utilizando la técnica no presencial, posteriormente, luego pasa a la fase de fidelización ya que comparte gustos comunes con el preadolescente y se vuelve más indispensable para él, posteriormente pasa a la fase de aislamiento, donde el delincuente hace que este, se aleje de los padres y amigos y hace que confié solo en él, la técnica que usa posteriormente ya es agresiva, por que empieza la fase de seducción donde empieza a darle dinero regalos, halagos, empiezan a compartir fotos, videos, el delincuente ya empieza a tener material sexual de parte de la víctima y pasa a la fase del acoso donde ya tienen encuentros sexuales, muchas veces puedes ser obligados por que el delincuente ya está manipulando a la víctima a cambio de no divulgar las imágenes y los videos que obtuvo con anterioridad, el delincuente empieza a pedir dinero, a chantajear a la víctima y a su familia, a cambio de no

contar nada, o en otras ocasiones durante los encuentros sexuales, el delincuente puede robar al individuo en cuestión, para comercializarlo en un mercado de explotación sexual, el cual se encuentra en un crecimiento exponencial y por ende preocupante para las diferentes autoridades mundiales.

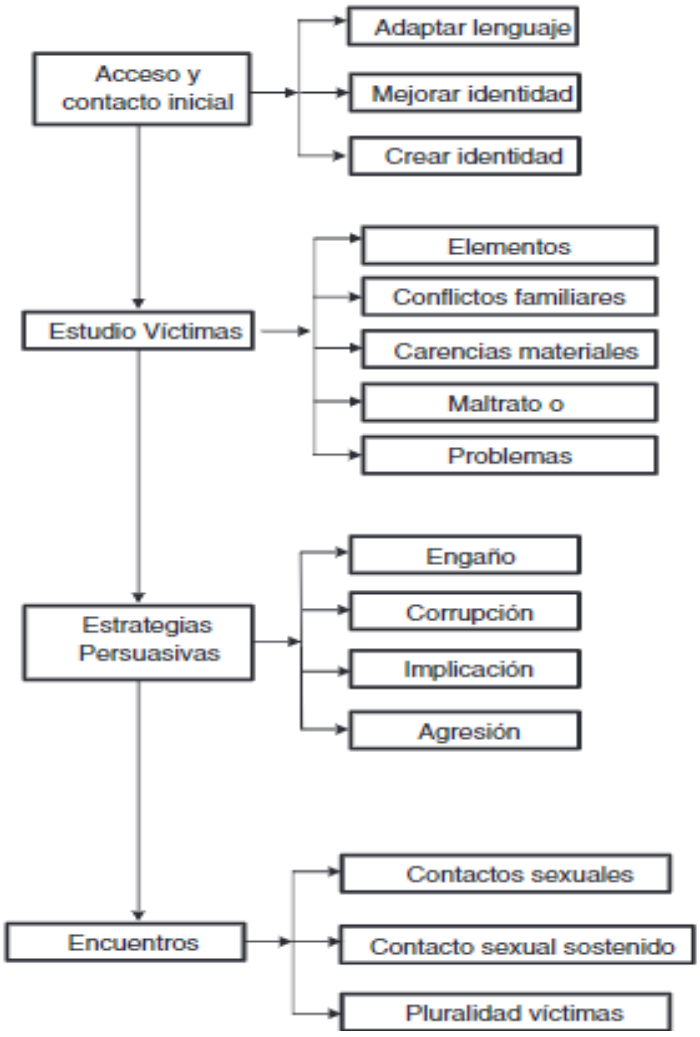
Como se pudo observar en el relato anterior, el pederasta utiliza diferentes métodos para hacer grooming:

1. Investigar la localización del niño
2. Suplantación de identidad
3. Seguimiento de redes sociales
4. Creación de perfiles falsos
5. Lograr hacer planes para reunirse
6. Engaño
7. Corrupción
8. Ofrecimiento de regalos, dinero y halagos a los niños a cambio de sexo
9. Implicación emocional del agresor
10. Investigar el horario de los padres

En la figura 1 Procesos de persuasión en grooming, se puede observar un ejemplo de las forma en la que el pederasta puede usar para acceder a los niños, iniciando desde el acceso y contacto inicial, donde crea y suplanta la identidad,

posteriormente estudia a las víctimas, se encarga de identificar si el chico tiene problemas en su familia o en su colegio, si es maltratado por sus padres, también investiga si tiene carencias económicas, como estrategias persuasivas, las cuales son el engaño, el, acoso, La agresión, entre otras, y finaliza con los encuentros, donde hay contacto sexual puede ser permanente, y pueden ser varias víctimas a la vez.

Figura 1 Procesos de persuasión en grooming



Fuente:

https://reader.elsevier.com/reader/sd/pii/S113205591730011X?token=5A3CDDD2359561962856B731A56243F9A45489B8DD8B71C5BD4CD648971F56A4548785EF83B8AAE8CC9E2FD94B201F20

5.4. El Grooming, y los delitos sexuales infantiles vinculados con internet

Como se ha venido mencionando a lo largo de la monografía, el grooming es el método que utilizan los pederastas para acceder de manera virtual o física a un menor de edad, (niño o adolescente), ganándose su confianza con el objetivo de obtener beneficios sexuales para ellos mismos o para otras personas, monetarios, de explotación y prostitución sexual, el grooming se encuentra catalogado en la ley 1273 de 2009[38], y en la ley 679 del 2001[39] el cual es un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores entre otros.

Dicho acto consiste en acceder a un menor de edad, por medio de redes sociales, el delincuente utiliza una falsa identidad, creando un perfil falso en una red social, en donde se hace pasar por menor de edad, una persona famosa como por ejemplo un influencer, actor o un cantante, posteriormente envía una solicitud de amistad a la víctima, la cual ya ha estudiado con anterioridad, el delincuente se gana la

---

[38] COLOMBIA. CONGRESO DE LA REPÚBLICA. 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]. Bogotá, D.C. Ministerio de Tecnologías de la Información y las Comunicaciones. p 1,2. [Consultado: 26 de septiembre de 2019]. Disponible en: https://www.mintic.gov.co/portal/inicio/3705:Ley-1273-de-2009

[39] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 679 de 2001, Por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución. [en línea]. Bogotá, D.C. Unidad para la atención y reparación integral de las víctimas. p 1,7. [Consultado: 26 de septiembre de 2019]. Disponible en: https://www.unidadvictimas.gov.co/es/ley-679-de-2001/13668

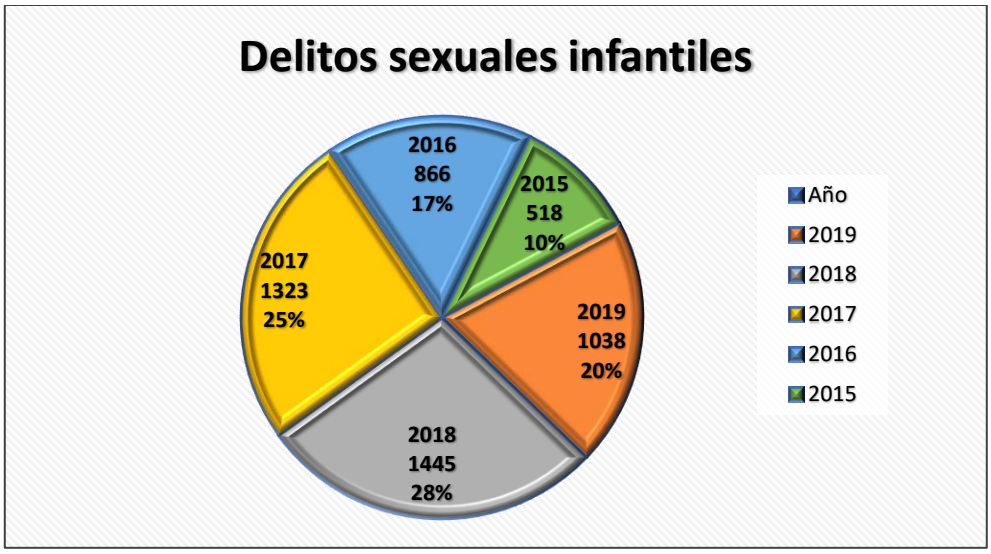
confianza del individuo, es ahí en donde por medio de artimañas empieza a pedirle al niño o niña fotos y videos de sus partes íntimas, las cuales serán utilizadas más adelante para pedir dinero y/o cuadrar encuentros sexuales, como se mencionaba anteriormente al realizar grooming se ponen en práctica diferentes tipos de delitos informáticos y delitos sexuales, como lo son la ingeniería social, el ciberacoso, el sexting, la extorsión virtual y la suplantación de identidad.

Según reportes del periódico el tiempo[40], en los últimos nueve años en Colombia se han presentado 5.583 denuncias de casos de delitos involucrados con pornografía y delitos sexuales vinculados al acceso de internet.

En la figura 2 Delitos sexuales a niños causados en Colombia, durante los últimos años, vinculados con la internet se puede observar el número de reportes, el porcentaje y el año en que estos se realizaron, iniciando en el año 2015 y finalizando en el año 2019, como podemos observar en el año 2015 se presentaron 518 denuncias, aumentando significativamente en los siguientes años, un poco más del doble en el año 2018, con 1445, y en 2019, 1038 acusaciones de delitos sexuales.

[40] JUSTICIA, Casi 4 denuncias al día se reciben por casos de explotación de menores [en línea]. En. El tiempo. Bogotá D.C. septiembre 23 de 2019 [Consultado: 26 de septiembre de 2019]. Disponible en Internet: https://www.eltiempo.com/justicia/delitos/claves-que-pedofilos-usan-para-ocultar-pornografia-infantil-en-internet-414560

Figura 2: Delitos sexuales a niños causados en Colombia durante los últimos años, vinculados con la internet

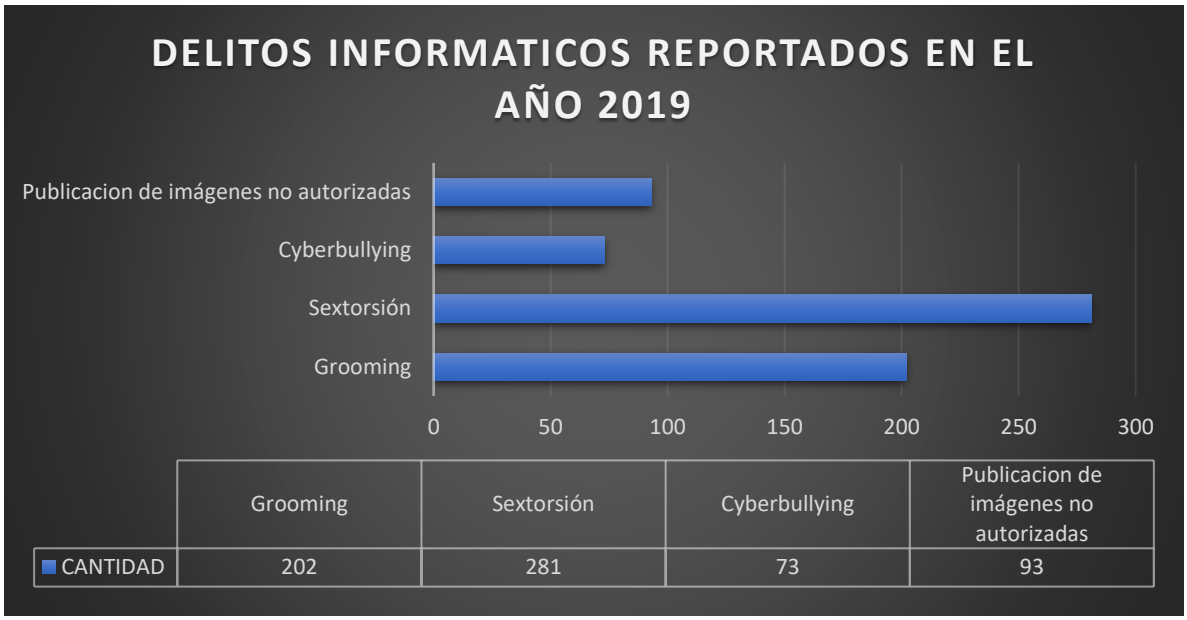


Fuente: Propia

En la figura 3 Delitos informáticos a menores de edad reportados en el año 2019, en la noticia del periódico el Tiempo[41] realizo un reportaje donde informo que, en el mes de septiembre del año 2019, en la ciudad de Medellín, un hombre que fue capturado en una operación entre la fiscalía y la policía, acepto cargos, después de haberle detectado en sus redes sociales más de 10.000 fotografías de niños entre los 9 y los 14 años, los cuales provenían de Colombia, Venezuela, México y Argentina.

[41] Ibid. JUSTICIA, Casi 4 denuncias al día se reciben por casos de explotación de menores [en línea]. En. El tiempo. Bogotá D.C. septiembre 23 de 2019 [Consultado: 26 de septiembre de 2019]. Disponible en Internet: https://www.eltiempo.com/justicia/delitos/claves-que-pedofilos-usan-para-ocultar-pornografia-infantil-en-internet-414560

Figura 3: Delitos informáticos a menores de edad reportados en el año 2019



Fuente: Propia

Según la investigación, Geyner Guerrero Galván desde su café internet, ubicado en el municipio de Hacarí, Norte de Santander, creaba perfiles falsos en los que simulaba ser un menor, con el fin de captar a sus víctimas. Cuando conseguía información personal y la confianza de las menores, les pedía imágenes con contenido sexual y después de obtener las primeras imágenes, el presunto depredador sexual amenazaba a las víctimas y las obligaba a enviarle más material pornográfico, a cambio de no publicar las fotos que ya había adquirido con engaños.[42]

[42] Ibid. JUSTICIA, Casi 4 denuncias al día se reciben por casos de explotación de menores [en línea]. En. El tiempo. Bogotá D.C. septiembre 23 de 2019 [Consultado: 26 de septiembre de 2019]. Disponible en Internet: https://www.eltiempo.com/justicia/delitos/claves-que-pedofilos-usan-para-ocultar-pornografia-infantil-en-internet-414560

El canal 13[43] en un informe que realizo en su página web, sobre cómo proteger a los niños del grooming, comenta que la policía nacional saco un reporte en el año 2019, donde se describe, que como resultado de las investigaciones y denuncias interpuestas ante la fiscalía, aproximadamente 6 niños al día son víctimas de la ciberdelincuencia en Colombia, también afirman que entre el periodo del 1 de enero del 2019 al 10 de julio del 2019, 18 personas fueron judicializadas por realizar grooming, y también se debe tener en cuenta que entre el periodo de enero y noviembre del 2019 la fiscalía realizo 656 investigaciones, y se hicieron 550 denuncias por parte de las víctimas.

Cabe resaltar que dentro de la investigación de esta monografía se encontraron grandes resultados de los esfuerzos que ha venido realizando el Ministerio de las Tic, el centro Cibernético de la Policía Nacional, Red Papaz[44] (red de padres y madres), y INHOPE (Organismo Internacional que regula 51 líneas de denuncias de pornografía infantil), en internet se puede encontrar una página web llamada Te Protejo, la cual ha sido creada entre el “Ministerio de las Tic, ICBF, Fundación Telefónica, el Foro de Generaciones Interactivas (España), Red PaPaz y la unión de otros aliados, esta página web fue creada con el objetivo de canalizar todas las

[43] CANAL 13 Op. Cit., p 37. ¿Cómo proteger a nuestros niños del grooming? [sitio web]. Redacción canal 13. Bogotá. [Consultado: 06 de marzo de 2020]. Disponible en internet: https://canaltrece.com.co/noticias/grooming-en-colombia/

[44] ESCUDOS DEL ALMA FERIA DE BUENAS PRACTICAS, POR AMOR A NUESTROS HIJOS. Ministerio TIC - Redvolución y En TIC Confío [sitio web] PaPaz Red de Padres y Madres. Bogotá D.C. [Consultado: 15 de abril de 2020]. Disponible en: https://www.redpapaz.org/category/logros-y-acciones/logros/

denuncias, conocer y visibilizar la magnitud de la situación de la infancia y la adolescencia"[45]

La página web de Unicef reporta que el día 22 de septiembre "Colombia empezó la implementación de un plan para desarrollar el modelo WePROTECT. Esta es una iniciativa internacional con enfoque intersectorial para prevenir y atender a las víctimas de explotación sexual y abuso en los entornos digitales",[46] todas estas iniciativas son realizadas en convenio por de Red PaPaz, INHOPE, el centro Cibernético de la Policía Nacional, Min Tic, el ICBF, Unicef.

En la página de Te Protejo se pueden encontrar todos los reportes que les han presentado, desde el año 2012 al año 2019, los cuales han sido dirigidos hacia el centro Cibernético de la Policía Nacional.

5.4.1. Reportes anuales del año 2015 al año 2019 realizados por Te Protejo vinculados con el grooming y los delitos sexuales vinculados con internet. A continuación, se podrán observar los reportes de los años 2012 al 2019

[45] ESCUDOS DEL ALMA. Te Protejo. [sitio web] Red Papaz. Bogotá. [Consultado: 06 de marzo de 2020]. Disponible en internet: http://www.redpapaz.org/escudos/index.php?option=com_k2&view=item&id=478:te-protejo&Itemid=104

[46] UNICEF, Colombia. Colombia se suma a los esfuerzos internacionales. Colombia se suma a los esfuerzos internacionales para proteger a niñas, niños y adolescentes frente a la explotación y abuso sexual en línea [sitio web]. Colombia. 2017. [Consultado: 16 de abril de 2020]. Disponible en: https://www.unicef.org/colombia/comunicados-prensa/colombia-se-suma-los-esfuerzos-internacionales

que, Te Protejo[47] ha publicado en su página web con el objetivo de mantener informada a la comunidad y de mostrar las estadísticas de las denuncias realizadas a lo largo de los años anteriormente mencionados.

En la figura 4 Reporte de denuncias en Te Protejo del 20120 al 2018, se puede evidenciar un reporte de las denuncias que fueron recepcionadas desde el año 2012 hasta el año 2018, como se puede identificar hay 9 categorías, en las que se analizaron las que pueden llegar a estar involucradas con el grooming, obteniendo como resultado en el año 2012[48], 2.192 denuncias, dentro de las cuales, hay 462 que tienen que ver con contenidos sobre abuso sexual, explotación sexual, comercial y pornografía infantil, 145 y de contenido inapropiado en medios de comunicación.

Continuando con el análisis de las tres categorías involucradas con el grooming, en el año 2013[49] se evidencia el reporte de las denuncias que fueron recepcionadas, obteniendo como resultado 3.921 entro de las cuales, hay 1.493 que están relacionadas con contenidos sobre abuso sexual, explotación sexual, comercial y pornografía infantil, y 263 de contenido inapropiado en medios de comunicación,

---

[47] TE PROTEJO. Informe tecnico de operaciones [sitio web]. Bogotá D.C. 2019. [Consultado: 06/03/2020]. Disponible en: https://teprotejo.org/que-es-te-protejo/informes-de-operaciones

[48] Ibid., p. 1. TE PROTEJO. Informe tecnico de operaciones [sitio web]. Bogotá D.C. 2019. [Consultado: 06/03/2020]. Disponible en: https://teprotejo.org/que-es-te-protejo/informes-de-operaciones

[49] Ibid., p. 1. TE PROTEJO. Informe tecnico de operaciones [sitio web]. Bogotá D.C. 2019. [Consultado: 06/03/2020]. Disponible en: https://teprotejo.org/que-es-te-protejo/informes-de-operaciones

estas tienen que ver con contenidos sobre abuso sexual, explotación sexual, comercial, pornografía infantil y ciberacoso.

En el año 2014[50] fueron recibidas un total de 6.452 denuncias, mientras que en la pornografía infantil se presentaron 3.724, 49 involucradas con ciberacoso, y 245 de contenido inapropiado en medios de comunicación.

En el año 2015[51] fueron 8.706 denuncias, dentro de las cuales, hay 5.827 que tienen que ver con contenidos sobre Abuso, explotación y comercialización sexual y pornografía infantil, 539 involucradas ciberacoso, y 175 de contenido inapropiado en medios de comunicación.

En el año 2016[52] fueron 10.424 denuncias, dentro de las cuales, hay 7.416 que tienen que ver con contenidos sobre abuso, explotación y comercialización sexual, 724 involucradas con ciberacoso, y 264 de contenido inapropiado en medios de comunicación.

---

[50] Ibid., p. 1. TE PROTEJO. Informe tecnico de operaciones [sitio web]. Bogotá D.C. 2019. [Consultado: 06/03/2020]. Disponible en: https://teprotejo.org/que-es-te-protejo/informes-de-operaciones

[51] Ibid., p. 1. TE PROTEJO. Informe tecnico de operaciones [sitio web]. Bogotá D.C. 2019. [Consultado: 06/03/2020]. Disponible en: https://teprotejo.org/que-es-te-protejo/informes-de-operaciones

[52] Ibid., p. 1. TE PROTEJO. Informe tecnico de operaciones [sitio web]. Bogotá D.C. 2019. [Consultado: 06/03/2020]. Disponible en: https://teprotejo.org/que-es-te-protejo/informes-de-operaciones

En el año 2017[53] fueron 8.991 denuncias, dentro de las cuales, hay 5.187 denuncias que tienen que ver con contenidos sobre abuso sexual, explotación sexual, comercial y pornografía infantil, 724 involucradas con ciberacoso, y 264 de contenido inapropiado en medios de comunicación.

En el año 2018[54] fueron 12.060 denuncias, dentro de las cuales, hay 8.179 que tienen que ver con contenidos sobre abuso sexual, explotación sexual, comercial y pornografía infantil, 1.225 de acoso escolar o ciberacoso, y 167 de contenido inapropiado en medios de comunicación, como se puede observar todas estas acusaciones están involucradas en su gran mayoría con el grooming ya que uno de los objetivos de este es obtener material pornográfico para distribuirlo, el pederasta quien es el individuo que comete el delito, acosa a la víctima, y obviamente publica contenido inapropiado que ha extraído de estas, en los medio de comunicación, como lo son las redes sociales.

[53] Ibid., p. 1. TE PROTEJO. Informe tecnico de operaciones [sitio web]. Bogotá D.C. 2019. [Consultado: 06/03/2020]. Disponible en: https://teprotejo.org/que-es-te-protejo/informes-de-operaciones

[54] Ibid., p. 1. TE PROTEJO. Informe tecnico de operaciones [sitio web]. Bogotá D.C. 2019. [Consultado: 06/03/2020]. Disponible en: https://teprotejo.org/que-es-te-protejo/informes-de-operaciones

Figura 4 Reporte de denuncias en Te Protejo del 20120 al 2018

Categoría		2012	2013	2014	2015	2016	2017	2018	Total	%
Denuncias Procesadas	Material de Abuso Sexual (Pornografía Infantil)	462	1.493	3.724	5.827	7.416	5.187	8.179	**32.288**	61%
	ESCNNA	0	0	36	127	124	81	101	**469**	1%
	Intimidación Escolar	129	126	187	143	175	184	205	**1.149**	2%
	Ciberacoso	0	0	491	539	724	847	1.225	**3.826**	7%
	Contenidos inapropiados en medios de comunicación	145	263	245	175	264	240	167	**1.499**	3%
	Venta de alcohol y otras SPA	143	212	143	150	140	119	121	**1.028**	2%
	Maltrato, trabajo y abuso infantil	101	1.041	988	1.311	1.319	2.046	1.851	**8.657**	16%
	Otros	918	405	606	434	262	287	211	**3123**	6%
	No Aplica	294	381	32	0	0	0	0	**707**	1%
	Total	**2.192**	**3.921**	**6.452**	**8.706**	**10.424**	**8.991**	**12.060**	**52.746**	**100%**

Fuente: https://teprotejo.org/que-es-te-protejo/informes-de-operaciones

Lastimosamente se puede observar que a pesar de los grandes esfuerzos y las campañas que se hacen para mitigar esta práctica delictiva, durante los años 2012 al 2018 se fueron incrementando las denuncias de los casos relacionados con el grooming.

En la tabla 2 Total denuncias y porcentajes, de las 3 categorías relacionadas con el grooming se puede identificar que la categoría de delito que más fue reportada a la página web Te Protejo (las cuales están implicadas con el grooming), del año 2012 al año 2018 fue, Material de abuso sexual (Pornografía) con 32.288 casos, ocupando el 61% de porcentaje, llegando a ser la causa más reportada por este medio digital, mientras que el ciber acoso fue el segundo con más de 3.826 casos,

y el contenido inapropiado en medios de comunicación ocupo el último puesto con 1.499 reportes, dentro de las categorías que están implicadas con el grooming.

Tabla 2 Total denuncias y porcentajes de las 3 categorías relacionadas con el grooming

CATEGORÍA	TOTAL, DENUNCIAS DEL AÑO 2012 AL 2018	PORCENTAJE
Material de abuso sexual (Pornografía)	32.288	61%
Ciberacoso	3.826	7%
Contenido inapropiado en medios de comunicación	1.499	3%
Total	**37.613**	**71%**

Fuente: Propia

En la figura 5 Reporte de denuncias en Te Protejo año 2019, se puede observar que Te Protejo[55], evidencia que durante el año 2019 nuevamente la categoría de material de abuso/explotación sexual (pornografía infantil) ocupo el 86%, esto quiere decir que aumentó un 25% en comparación con los anteriores años que alcanzaron un rango de 61%, el ciberacoso obtuvo el 4.5% de rango, 2.5% menos reportes que los anteriores años, y los casos sobre contenidos inapropiados en medio de comunicación ocuparon 1.1%, 1.9% menos que los anteriores años.

[55] PIÑEROS OSPINA, Carolina. Reporte de denuncias anual año 2019 en porcentajes. En: TE PROTEJO. [Consultado: 08/03/2020]. Disponible en: https://teprotejo.org/que-es-te-protejo/informes-de-operaciones/

Afortunadamente lo que fue ciberacoso y contenidos inapropiados en medio de comunicación disminuyeron, pero la categoría de material de abuso/explotación sexual (pornografía infantil) como se mencionaba anteriormente aumento el 25%.

Figura 5 Reporte de denuncias en Te Protejo año 2019

Fuente: https://teprotejo.org/que-es-te-protejo/informes-de-operaciones/

5.4.2. Logros durante el 2019 por los reportes que fueron canalizados por Te Protejo. A continuación, se podrá observar el reporte que Te Protejo dio de los logros que se obtuvieron durante el año 2019, los cuales estuvieron enfocados

en bloquear páginas y perfiles de redes sociales que se encargaban de hacer grooming y pornografía infantil, en realizar acciones para restablecer los derechos de los menores, encontrar imágenes de abuso y explotación sexual infantil, realizar sanciones monetarias a quienes no bloquearon las páginas con contenido pornográfico infantil, y la promoción de las descargas de la App Te Protejo en los dispositivos móviles de los padres y tutores de los menores de edad.

Te Protejo en el año 2019[56] logro bloquear 3.904 páginas web por que contenían imágenes de abuso sexual y explotación infantil, de las cuales 2.955 URL fueron ingresadas a través de ICCAM-INHOPE, en las que se encontraron 6.694 imágenes de explotación infantil cuyo desmonte fue solicitado a la red INHOPE.

En la figura 6 Logros durante el 2019 de reportes que Te Protejo logro canalizar con el centro cibernético de la Policía Nacional, se puede observar que por medio de las denuncias que canalizo Te Protejo al centro cibernético de la Policía Nacional no se realizaron procesos de judicialización, pero si fueron suspendidas 819 páginas con dominio, por contener material de abuso y explotación sexual. Durante todo el año se realizaron 35.390 descargas en dispositivos móviles en la App Te Protejo. Se efectuaron 128 acciones para restablecer los derechos de las víctimas y se

---

[56] PIÑEROS OSPINA, Carolina. Logros durante el 2019 En: TE PROTEJO. [Consultado: 08/03/2020]. Disponible en: https://teprotejo.org/que-es-te-protejo/informes-de-operaciones/

recaudaron $55,483.772 millones de pesos a 14 ISP por no bloquear páginas con material de abuso y explotación sexual infantil.

Figura 6 Logros durante el 2019 de reportes que Te Protejo logro canalizar con el centro cibernético de la Policía Nacional

Fuente: https://teprotejo.org/que-es-te-protejo/informes-de-operaciones/

5.5. EL GROOMING Y LAS REDES SOCIALES

El grooming está vinculado a las redes sociales, ya que para realizar dicha práctica se emplean herramientas relacionadas con las TIC, a lo largo de la monografía se ha destacado que es necesario hacer uso de redes sociales e internet ya que son las herramientas de comunicación que utiliza el pederasta para lograr acceder al menor de edad.

Es importante recordar que una página web, es una herramienta que permite que las personas puedan estar en contacto permanente, sin importar la distancia o la zona horaria, las redes sociales admiten la creación de comunidades virtuales, intercambio de fotos y cualquier tipo de contenido, lo cual son características que le sirven al delincuente al momento de emplear dicha técnica.

El Ministerio de las TIC[57] en su página web realizo una publicación donde afirman que en los últimos años Colombia evidencio un gran crecimiento por la cantidad de usuarios que se registran en redes sociales.

[57] MIN TIC. Colombia es uno de los países con más usuarios en redes sociales en la región. [Sitio web]. Bogotá D.C. 26 diciembre de 2019. [Consultado el 12 de marzo del 2019]. Disponible en: https://www.mintic.gov.co/portal/inicio/Sala-de-Prensa/Sabia-Ud-que/2713:Colombia-es-uno-de-los-paises-con-mas-usuarios-en-redes-sociales-en-la-region

Facebook y Twitter son las redes sociales que cuentan con más cantidad de reconocimiento, entre la ciudadanía colombiana. Min Tic[58] emitió un reporte donde destacan que actualmente Colombia ocupa el puesto número 14 a nivel mundial por tener más de 15 millones de usuarios registrados en Facebook, por otro lado, la Capital Colombiana es la novena ciudad en el mundo con 6.5 millones de beneficiarios registrados en Facebook.

Twitter tiene un estimado de 6 millones de colombianos registrados en sus portales, esta red es el canal más usado para realizar campañas políticas, es usado también por deportistas, cantantes, entre otros personajes públicos, se destaca que, al tener esta cifra en Colombia, queda por encima del número de usuarios sobre países como lo son Alemania y Francia.

En la siguiente figura 7 Redes sociales más usadas por los niños, se puede observar los resultados de una encuesta realizada por Tigo Une[59] sobre las redes sociales que más usan los niños y/o adolescentes, Facebook ocupa el primer lugar con un 44%, el segundo puesto es ocupado por WhatsApp con un 31%, en tercer posición esta Messenger con un 9%, seguidamente de Instagram con un 9%, y finalizando

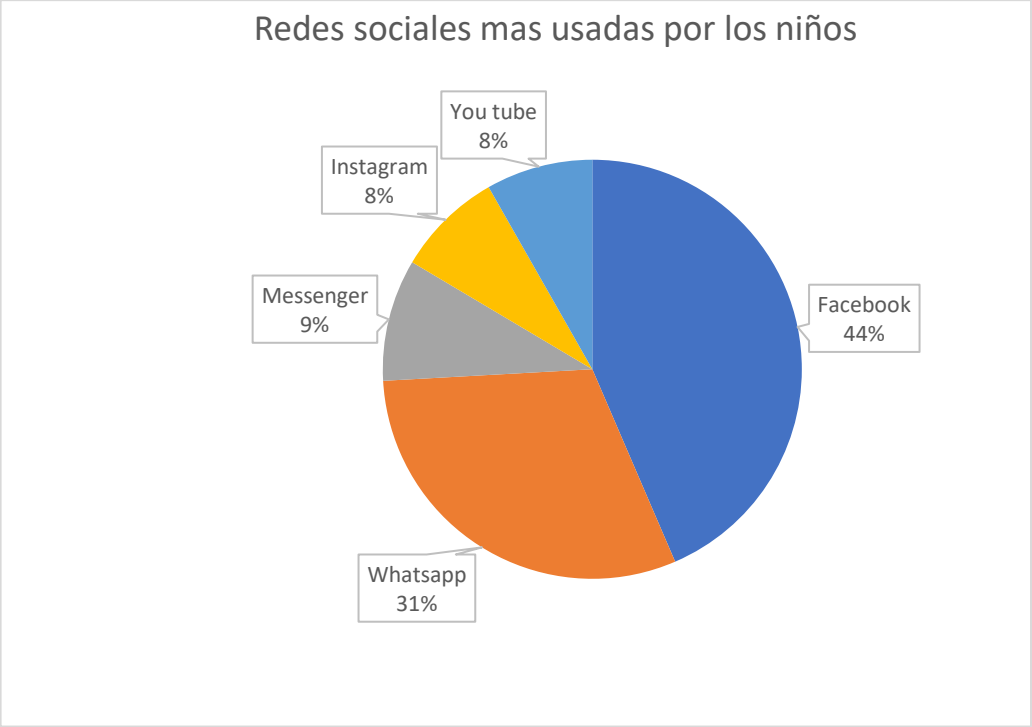
---

[58] Ibid., MIN TIC. Colombia es uno de los países con más usuarios en redes sociales en la región. [Sitio web]. Bogotá D.C. 26 diciembre de 2019. [Consultado el 12 de marzo del 2019]. Disponible en: https://www.mintic.gov.co/portal/inicio/Sala-de-Prensa/Sabia-Ud-que/2713:Colombia-es-uno-de-los-paises-con-mas-usuarios-en-redes-sociales-en-la-region

[59] CONTIGO CONECTADOS. REDES SOCIALES MAS USADAS POR LOS NIÑOS En: Tigo. [Consultado: 12/03/2020]. Disponible en: https://contigoconectados.com/resultados/descargables/

se encuentra You Tube con un 8%, es decir que con los datos que se tienen en este momento se puede llegar a deducir que Facebook y WhatsApp son las redes sociales más propensas para que los pederastas o delincuentes las utilicen para practicar el grooming, el cual permite que dentro de sus prácticas y métodos que utiliza, ejecute delitos como el sexting, el acoso sexual, la pornografía sexual en menores de 8 años y el turismo sexual, etc.

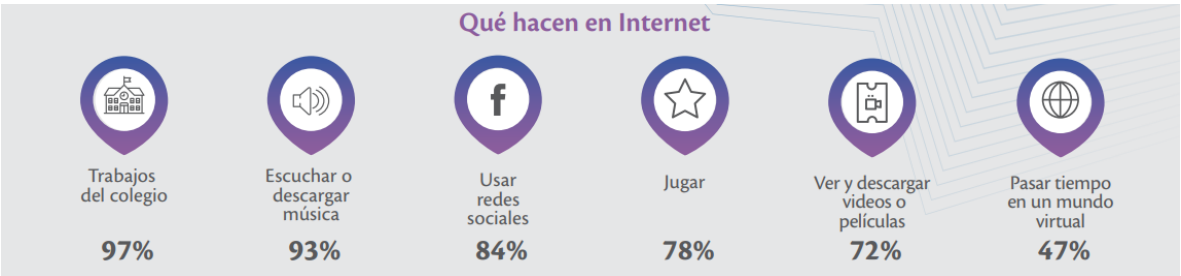
Figura 7 Redes sociales más usadas por los niños



Fuente: https://contigoconectados.com/resultados/descargables/

En la figura 8 ¿Que hacen los niños en internet?, se puede observar el rango de porcentaje de las actividades que los niños realizan en internet, el 97% trabajos del colegio, el 93% escuchar o descargar música, el 84% usan redes sociales, el 78% juegan, el 72% ven videos o descargan películas, y el 47% pasan tiempo en un mundo virtual, como se puede observar el 84% de las actividades que hacen los menores en internet es usando redes sociales, esas cifras se obtuvieron de una encuesta que realizo Tigo Une a niños de entre 9 y 16 años.

Figura 8 ¿Que hacen los niños en internet?



Fuente: https://contigoconectados.com/resultados/descargables/

5.5.1. Medidas de protección tomadas por las redes sociales para proteger a los menores de edad. Se realizó una revisión sobre las diferentes redes sociales que son más famosas y utilizadas por las personas, y en este caso por las víctimas que son los niños y/o adolescentes, obteniendo los siguientes resultados.

En primer lugar, se realizó la revisión si dentro de las políticas de seguridad de Facebook[60], están incluidas restricciones y medios de seguridad que protejan la integridad de los niños y adolescentes que usan las redes sociales y que se pueden ver expuestos con la creación y uso de un perfil, también se indago si dentro de esas mismas políticas existen medidas de prevención para que los padres o adultos que tengan niños y adolescentes a cargo puedan evitar o denunciar algún hecho peligroso que este amenazando la integridad de los menores, para realizar el análisis se procedió a tomar capturas de imagen de las recomendaciones y las políticas de seguridad que se encontraron descritas en las plataformas principales de Facebook, WhatsApp e Instagram, el anterior contenido se buscó en las políticas de seguridad donde se refieren en cuanto a los niños y/o adolescentes menores de 18 años, cabe destacar que para poder tener un perfil social en Facebook, se debe tener una edad mínima de 13 años, lo cual está estipulado en las normas de dicha red social.

[60] FACEBOOK. Tus compromisos con Facebook y nuestra comunidad [sitio web]. California. 31 de julio de 2019. [Consultado: 17 de abril de 2020]. Disponible en: https://es-es.facebook.com/legal/terms

En la figura 9 Desnudos y explotación sexual de menores, se explica la política de seguridad sobre desnudos y explotación sexual a menores, en esa política exponen que Facebook elimina cualquier contenido sexual que aparezca en la red social donde el protagonista sea un niño o adolescente, muchas veces los padres toman fotos a sus niños cuando están desnudos por ejemplo si los están bañando o cambiando de ropa, y estas acciones se hacen de manera inocente, posteriormente estas imágenes son publicadas en la red social pero desafortunadamente otros usuarios pueden ver esas imágenes y utilizarlas para fines pornográficos y puede verse afectada la integridad del menor de edad.

Figura 9 Desnudos y explotación sexual de menores

Fuente:https://es-es.facebook.com/communitystandards/child_nudity_sexual_exploitation

En la figura 10 Normas comunitarias para proteger menores de edad 1, se describen las acciones que Facebook,[61] prohíbe realizar como lo son:

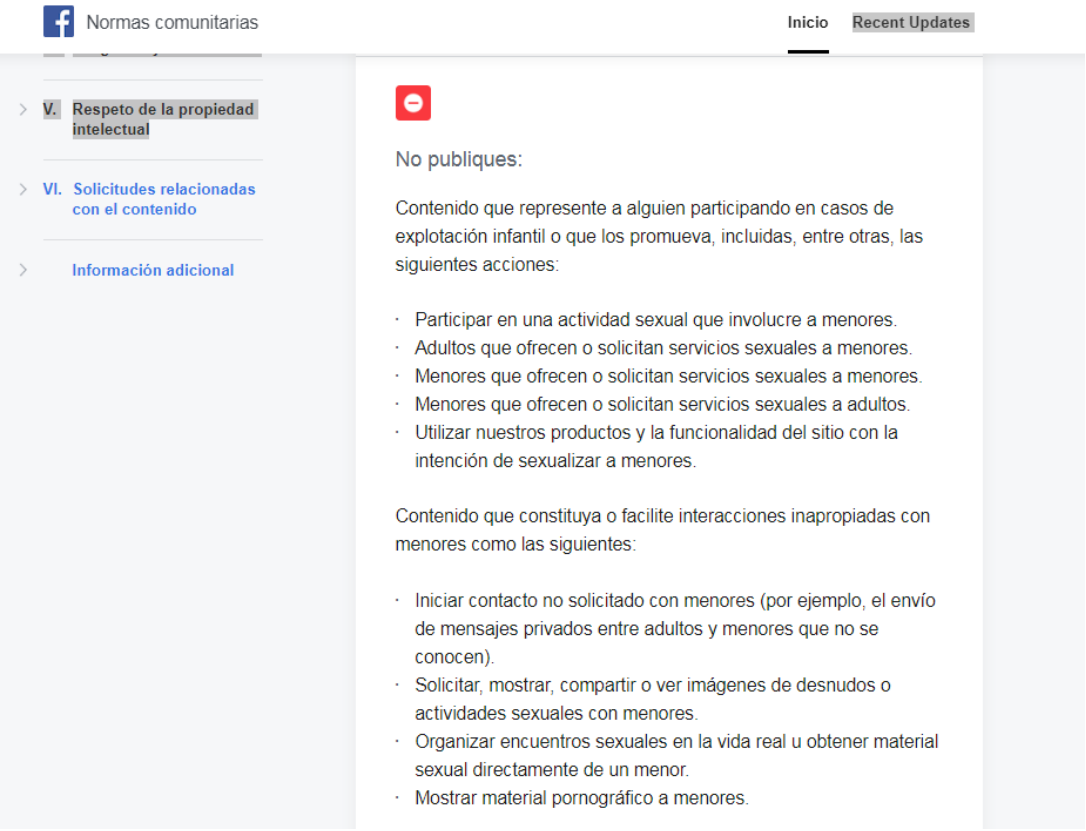
- Adultos solicitando y/o ofreciendo servicios sexuales a menores de edad
- Menores solicitando y/o ofreciendo servicios sexuales a otros chicos.
- Menores solicitando y/o ofreciendo servicios sexuales a adultos.
- Participar en actividades sexuales que involucren a menores de edad.

Facebook también recomienda no tener interacciones inapropiadas con menores de edad, interacciones tales como:

- Enviarse mensajes con menores.
- Compartir contenido sexual por medio de esos mensajes.
- Solicitarles contenido sexual a menores.
- Cuadrar encuentros sexuales con menores de edad.

[61] FACEBOOK. Normas comunitarias para proteger menores de edad [sitio web]. California. 2020. [Consultado: 13/03/2020]. Disponible en: https://es-es.facebook.com/communitystandards/child_nudity_sexual_exploitation

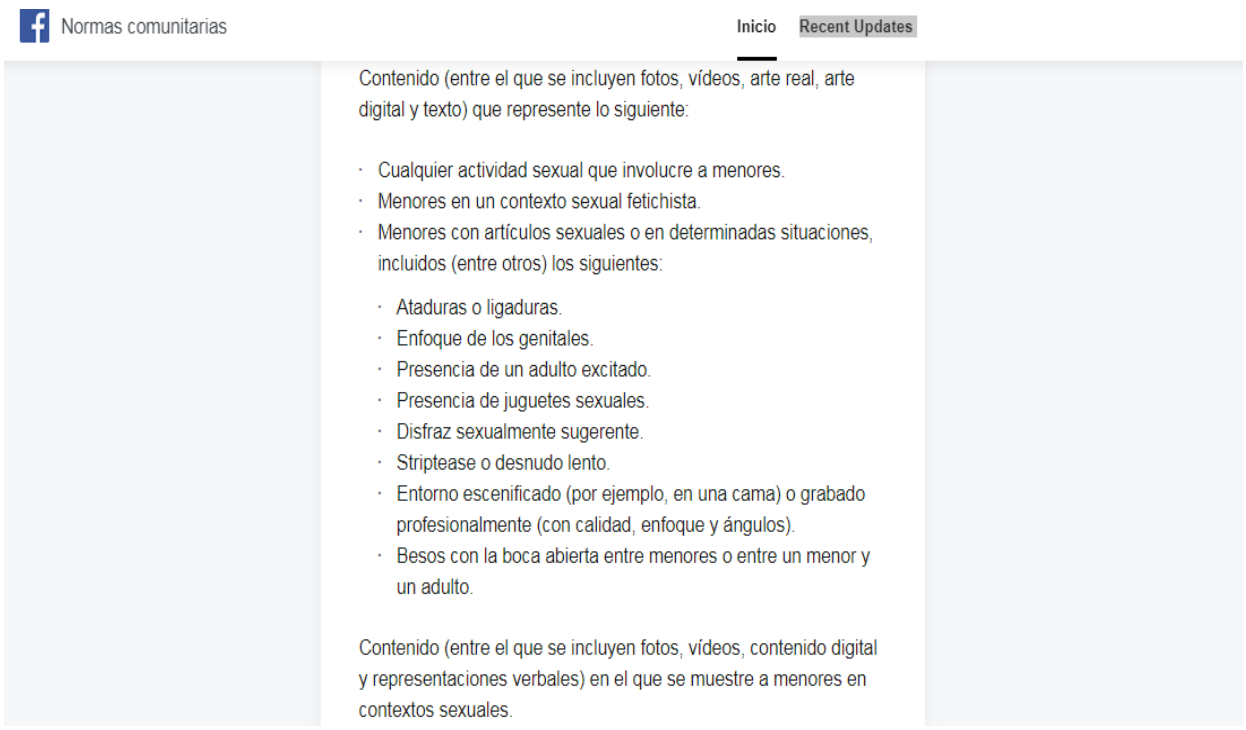
Figura 10 Para proteger los menores de edad se deben seguir estas pautas



Fuente: https://es-es.facebook.com/communitystandards/child_nudity_sexual_exploitation

En la figura 11 Normas comunitarias para proteger menores de edad 1, Facebook describe que no se puede pedir o publicar contenido erótico con menores de edad, ese contenido tiene que ver con ataduras o ligaduras, enfoque de los genitales, disfraces sexuales, imágenes de juguetes sexuales, menores besándose la boca con adultos o besos entre menores.

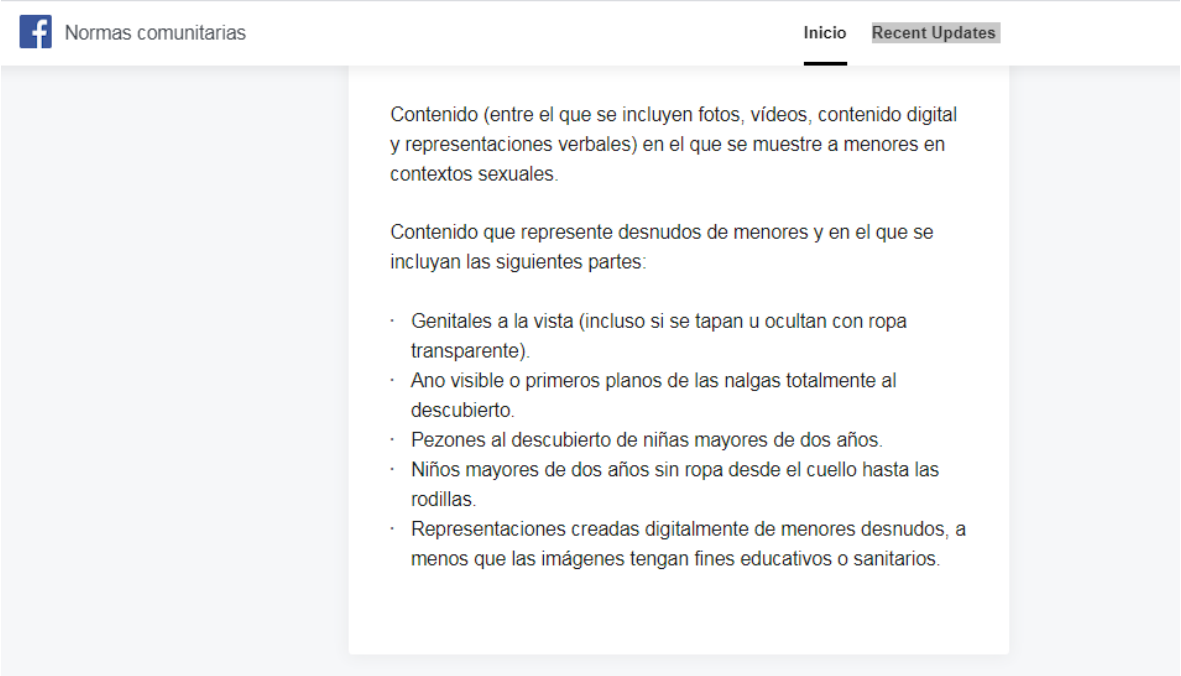
Figura 11 Normas comunitarias para proteger menores de edad 1



Fuente: https://es-es.facebook.com/communitystandards/child_nudity_sexual_exploitation

En la figura 12 Normas comunitarias para proteger menores de edad 2, Facebook describe las partes del cuerpo de los menores que está prohibido mostrar por medio de imágenes o videos, esas partes del cuerpo son los genitales, los pezones, niños mayores de dos años sin ropa representaciones creadas digitalmente de menores desnudos con la excepción de que sea con fines educativos o sanitarios.

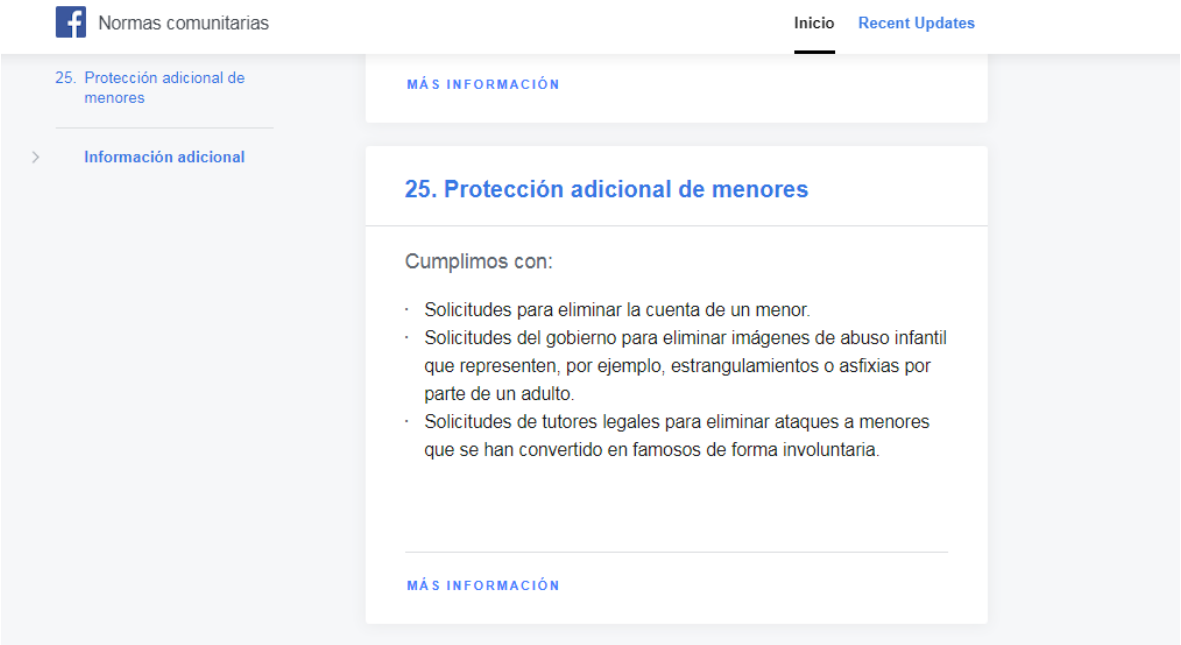
Figura 12 Normas comunitarias para proteger menores de edad 2



Fuente: https://es-es.facebook.com/communitystandards/child_nudity_sexual_exploitation

En la figura 13 Protección adicional de menores, Facebook describe la protección adicional que le brinda a los menores de edad como red social, en este caso cumplen con las solicitudes que los usuarios hacen para eliminar la cuenta de un menor, también atienden las solicitudes del gobierno para eliminar imágenes de abuso infantil, y atienden las solicitudes que hacen los tutores legales para eliminar contenido que evidencie ataques a menores.

Figura 13 Protección adicional de menores



Fuente: https://es-es.facebook.com/communitystandards/child_nudity_sexual_exploitation

En la figura 14 Vulneraciones de privacidad y de los derechos de privacidad de las imágenes, Facebook describe, que como red social les interesa la privacidad y la protección de los usuarios, especifican que se esfuerzan por proteger las cuentas y salvaguardan la información personal de los estos, para impedir daños físicos y económicos, también informan que no se debe publicar información personal o confidencial sobre otras personas sin antes tener su autorización.

Figura 14 Vulneraciones de privacidad y de los derechos de privacidad de las imágenes

Fuente: https://es-es.facebook.com/communitystandards/child_nudity_sexual_exploitation

5.5.2. Recursos sobre seguridad para padres en Facebook. Facebook[62] afirma que ser padres es una tarea difícil, por tal motivo se encontró que dentro de las acciones que realiza la red social para mantener seguros a los menores de edad también existen los recursos de seguridad para padres, lo cual son unas opciones que le permiten a los padres saber que hacer en caso de presentarse diferentes

[62] FACEBOOK. Portal para padres [sitio web]. California [Consultado: 17 de abril de 2020]. Disponible en: https://es-la.facebook.com/safety/parents

escenarios como por ejemplo amenazas y vulnerabilidades que atenten contra la seguridad por medio de los perfiles de los menores de edad.

En la figura 15 Recursos sobre seguridad para padres, se puede observar un listado con la descripción de los recursos sobre seguridad que Facebook proporciona a los padres, en ese listado se encuentran diferentes opciones como lo son:

- ¿Qué medidas toma Facebook para proteger los menores?
- ¿Cómo puedo ayudar a mi hijo o hija adolescente a utilizar Facebook de manera prudente?
- ¿Cómo funciona la configuración de la ubicación en el caso de los menores de Facebook?
- ¿Qué debo hacer si alguien amenaza con compartir cosas que mi hijo quiere mantener en privado (por ejemplo, mensajes, fotos, videos, etc.)?
- ¿Cómo solicito la eliminación de una imagen de mi hijo o hija?
- Quiero denunciar una foto o video que vulnera la intimidad de mi hijo.
- ¿Por qué se ha eliminado una imagen que he publicado de mi hijo?
- Los menores y las etiquetas en Facebook
- ¿Cómo puedo solicitar datos de la cuenta de Facebook de mi hijo menor de edad?
- ¿Cómo puedo solicitar datos de la cuenta de Facebook de mi hijo menor de edad?

Figura 15 Recursos sobre seguridad para padres

Fuente: https://www.facebook.com/help/187948218057965?helpref=uf_permalink

En la figura 16 ¿Qué medidas toma Facebook para proteger a los menores?, se da a conocer que mediante su trabajo para proteger a los menores de edad cuando interactúan por medio de la plataforma, han diseñado diferentes funciones que le recuerdan al menor la forma en que deben compartir la información con quien la deben compartir y se encargan de limitar las interacciones del chico con desconocidos. Es decir que antes de que el niño realice una publicación, la red social le informa que conlleva publicar contenido para que todo el público pueda

acceder, otro método que utilizan, es que evita que la información personal como los datos de contacto, fechas de nacimiento, colegio donde estudia, aparezca en las búsquedas de los usuarios, y también se encargan de tomar las medidas necesarias para recordarle a estos que solo deben aceptar solicitudes de amistades de personas que sean conocidas.

Figura 17 ¿Qué medidas toma Facebook para proteger a los menores?

Fuente: https://www.facebook.com/help/107947710545627 7/?helpref=hc_fnav

En la figura 17 ¿Como puedo ayudar a mi hijo o hija adolescente a utilizar Facebook de manera prudente?, se explica la forma en que el padre le puede ayudar a su hijo

adolescente a utilizar la red social de una manera prudente, se le recomienda al padre consultar en compañía de su hijo, la privacidad y la configuración de la cuenta, para elegir una configuración en la que los dos se sientan mejor, se recomienda al padre que monitoree la cuenta, que converse con su hijo sobre la manera prudente de manejar internet y la tecnología, adicionalmente se sugiere al padre que le enseñe a su hijo normas básicas para manejar redes sociales como por ejemplo nunca compartir contraseñas, pensar antes de publicar cualquier contenido, no aceptar solicitudes de amistad de desconocidos, y denunciar cualquier evento que parezca sospechoso.

Figura 18 ¿Como puedo ayudar a mi hijo o hija adolescente a utilizar Facebook de manera prudente?

Fuente: https://www.facebook.com/help/150965161639522?helpref=uf_permalink

En la figura 18 ¿Como funciona la configuración de la ubicación en el caso de los menores en Facebook?, se les comunica a los padres que a diferencia de los perfiles sociales de un adulto donde se puede elegir si se quiero o no se quiere compartir la ubicación, para los menores esa opción viene desactivada por defecto y en el caso de que los padres o los menores activen la opción saldrá un aviso permanente recordando que la ubicación esta activada.

Figura 19 ¿Como funciona la configuración de la ubicación en el caso de los menores en Facebook?

Fuente: https://www.facebook.com/help/244053012290058?helpref=ufpermalink

En la figura 19 ¿Que debo hacer si alguien amenaza con compartir cosas que mi hijo quiere mantener en privado (por ejemplo, mensajes, fotos, videos, etc.)?,

Facebook le explica al padre que debe hacer en caso de que alguien lo esté amenazando con compartir contenido como fotos o videos privados del menor, para esto lo primero que se debe realizar es denunciar ante los entes de autoridad, se recomienda reportar y bloquear el perfil social de la persona que los está amenazando, el padre debe hablar con el menor para saber qué fue lo que paso, y todos los detalles de la interacción que ha tenido con la persona que maneja el perfil social de donde lo están amenazando.

Figura 20 ¿Que debo hacer si alguien amenaza con compartir cosas que mi hijo quiere mantener en privado (por ejemplo, mensajes, fotos, videos, etc.)?

Fuente: https://www.facebook.com/help/273414072790504?helpref=uf_permalink

En la figura 20 ¿Como solicito la eliminación de una imagen de mi hijo o hija?, se explica la forma en que un padre puede solicitar la eliminación de una imagen del menor, en este caso se recomienda reportar la imagen o el video que quieren que

sea eliminado, y Facebook procederá a estudiar el material y a eliminarlo en el caso en el que infrinja los derechos de privacidad del menor.

Figura 21 ¿Como solicito la eliminación de una imagen de mi hijo o hija?

Fuente: https://www.facebook.com/help/1079477105456277/?helpref=hc_fnav

En figura 21 Quiero reportar una foto o una imagen que vulnera la intimidad de mi hijo, Facebook da a conocer a los padres que en el caso en que quieran solicitar la suprimir una foto o video que quebranta la intimidad del menor, si esto se presenta en un menor de 13 años deben diligenciar un formulario, y si el individuo se encuentra en un rango entre 13 y 17 años, se le recomienda al padre que hable con

su hijo para que el mismo menor se encargue de solicitar la eliminación del contenido.

Figura 22 Quiero reportar una foto o una imagen que vulnera la intimidad de mi hijo

Fuente: https://www.facebook.com/help/1079477105456277/?helpref=hc_fnav

En la figura 22 ¿Porque se eliminó una imagen que publique de mi hijo? Facebook le explica al padre por que en algunas ocasiones se les ha eliminado o se les eliminaran de sus redes sociales fotos de sus hijos, ya que en algunas ocasiones toman imágenes de sus hijos desnudos cuando son muy pequeños, aunque lo hacen sin ninguna mala intención, al realizar dichos actos se están incumpliendo las

normas comunitarias de la red social, y también se eliminan porque otras personas las pueden usar de manera indebida.

Figura 23 ¿Porque se eliminó una imagen que publique de mi hijo?

Fuente: https://www.facebook.com/help/1079477105456277/?helpref=hc_fnav

En la figura 23 Menores y etiquetado en Facebook, se explica la forma en la que funciona la red social cuando se etiqueta un menor de edad, toda publicación que se realice puede ser etiquetada y vista por cualquier individuo, Facebook tiene tanto para los menores como para los adultos en sus herramientas la opción de revisión de etiquetas, para que el usuario apruebe o lo cancele, en el caso de los menores, esta opción viene activa de manera predeterminada, así cuando el niño no esté de

acuerdo con la mención realizada se puede suprimir o pedirle a la persona que hizo lo realizo, que lo borre.

Figura 24 Menores y etiquetado en Facebook

Fuente: https://www.facebook.com/help/1079477105456277/?helpref=hcfnav

En figura 24 ¿Cómo puedo solicitar datos de la cuenta de Facebook de mi hijo menor de edad?, se explica que en el momento en el que un menor de 13 años tiene una cuenta en la mencionada red social es eliminada inmediatamente junto con toda la información asociada, si el padre o el tutor descubren que el menor de 13 tiene una cuenta puede solicitar toda la información antes de ser eliminada esa cuenta, pero

para esto se debe entregar una declaración certificada de que tienen los derechos del niño.

Figura 25 ¿Cómo puedo solicitar datos de la cuenta de Facebook de mi hijo menor de edad?

Fuente: https://www.facebook.com/help/107947710545627 7/?helpref=hc_fnav

En la figura 26 ¿Como denunció a un menor de 14 años en Facebook?, se explica que en algunas jurisdicciones la edad mínima para tener un perfil social es de 14 años por lo tanto la forma en la que se puede solicitar la eliminación de un perfil que este siendo utilizado por un menor de 14 años.

Figura 27 ¿Como denunció a un menor de 14 años en Facebook?

Fuente: https://www.facebook.com/help/1079477105456277/?helpref=hc_fnav

En la figura 26 Apertura de cuenta en Facebook para niños menores de 13 años, se evidencia la apertura de una cuenta en para que un menor de 13 tenga un perfil social, se puede observar que para registrarse solicitan nombres, apellidos, número de teléfono y fecha de nacimiento que en este caso se la que se ingresó fue el 2 de abril de 2008.

Figura 28 Apertura de cuenta en Facebook para niños menores de 13 años

Fuente: https://www.facebook.com/reg/

En la anterior figura 27 Acceso denegado se observa el resultado de la apertura de la cuenta en Facebook, en este caso sale un aviso el cual informa que no permite procesar ningún registro, ya que la fecha que se puso de nacimiento es de un menor de 13 años, y esa edad está prohibida para abrir cuentas en las políticas de seguridad de Facebook, realizando esta acción lo que se verifico que se cumple con esa restricción, y se concluye que efectivamente un niño que tenga 12 años no puede realizar la apertura de una cuenta en esta red social.

Figura 29 Acceso denegado

Fuente: https://www.facebook.com/r.php?locale=es_LA&display=page

Como se pudo observar durante la revisión que se realizó a la red social de Facebook, sobre el nivel de seguridad que se tiene a la hora de tener como usuarios a menores de edad, se pudo identificar que, en las políticas de seguridad, ellos dentro de sus normas describen que contenido puede ser publicado por estos, también explican que tipo de interacción puede tener un niño con un adulto, así como con otro chico.

Facebook brinda asesoría a los padres y tutores a la hora de saber que acciones en cuanto a contenido, fotos, videos, publicaciones, etiquetados, acoso, amenazas, ubicación y demás dudas se le puedan presentar a los adultos responsables cuando su hijo abre una cuenta, en general se evidencio que esta red social maneja un nivel

de seguridad alto para evitar que los pederastas se aprovechen de los menores de edad por este medio.

5.5.3. Políticas de seguridad para menores de edad en WhatsApp. Durante la revisión de los niveles de seguridad que se realizó en la monografía, se obtuvieron los niveles de seguridad y las políticas de seguridad que son brindados por WhatsApp [63] para conocimiento de los menores de edad, se tomaron diferentes pantallazos como evidencia, para poder analizar los resultados obtenidos.

En la figura 28 Edad mínima para usar WhatsApp, se puede observar que, dentro de su seguridad y privacidad tienen estipulado que para tener una cuenta en esta red social se deben tener mínimo 13 años, lo cual es el requerimiento de la legislación de Colombia y también especifican que si por algún motivo se llegan a abrir cuentas con información falsa o en nombre de otras personas menores de edad será una infracción de las condiciones de la esta red social.

[63] WHATSAPP. Información legal de WhatsApp [sitio web]. California. 2020. [Consultado: 19 de mayo de 2020]. Disponible en: https://www.whatsapp.com/legal/?lang=es#key-updates

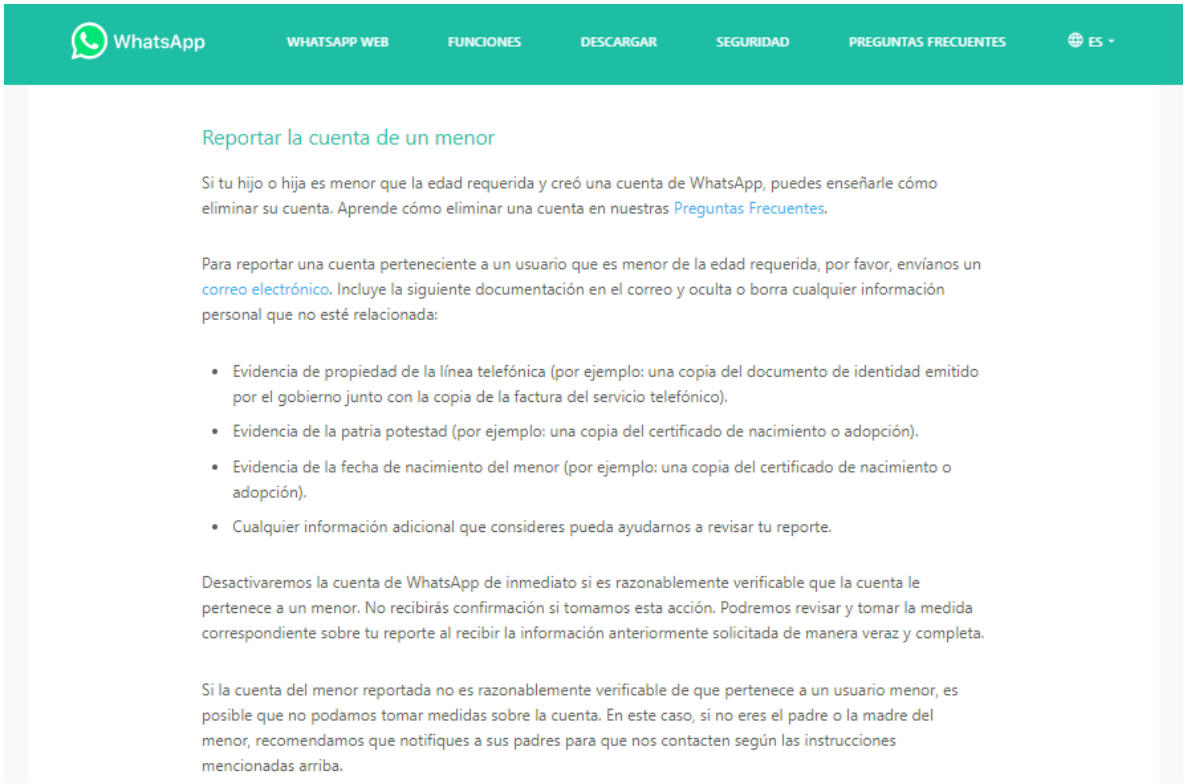
Figura 30 Edad mínima para usar WhatsApp

Fuente: https://faq.whatsapp.com/es/android/26000151/?category=5245250

En la figura 29 Reportar la cuenta de un menor, WhatsApp explica los pasos que debe realizar un padre o tutor para solicitar la cancelación de una cuenta de un niño si llega a ser menor de 13 años, en este caso se debe enviar un correo electrónico a la compañía, adjuntando la fecha de nacimiento del niño, evidencia de la propiedad de la línea telefónica, junto con la copia de la factura del servicio telefónico, y cualquier información adicional que sirva para revisar el reporte.

Si se logra verificar que la cuenta está siendo usada por un menor de 13 años, será cancelada, pero se debe recibir toda la información solicitada anteriormente, para poder cancelarla, de ser contrario es posible que no puedan hacer nada, en ese caso se sugiere que, si la persona que está reportando la cuenta no es el padre o madre del menor, se recomienda hablar con los padres para que reporten la cuenta.

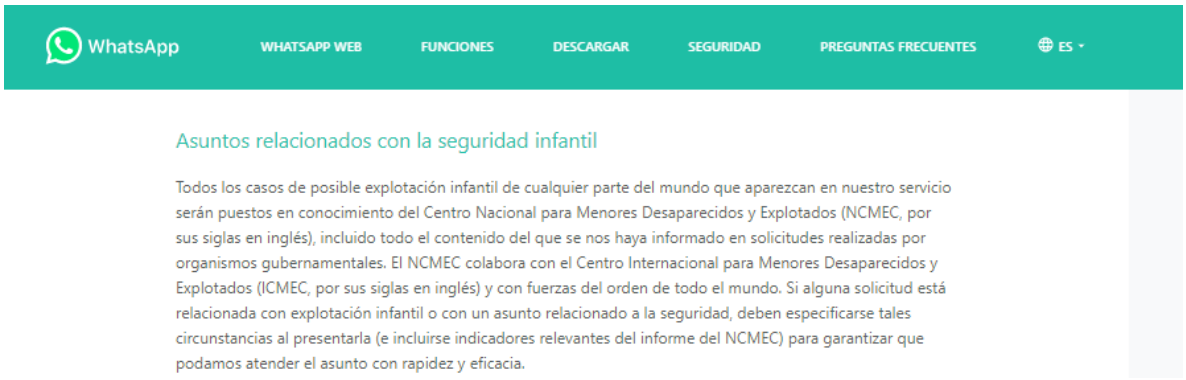
Figura 31 Reportar la cuenta de un menor



Fuente: https://faq.whatsapp.com/es/android/26000151/?category=5245250

En la figura 30 Asuntos relacionados con la seguridad infantil, WhatsApp explica los asuntos relacionados con la seguridad infantil, explican que todos los casos de posible explotación que se presenten en cualquier parte del mundo y que aparezcan en la plataforma de ellos serán puestos en conocimiento del Centro Nacional de Menores Desaparecidos y Explotados, y se incluirá todo el contenido sobre el que se haya dado a conocer en las solicitudes realizadas.

Figura 32 Asuntos relacionados con la seguridad infantil



Fuente: https://faq.whatsapp.com/es/general/26000050/?category=5245250

5.5.4. Políticas de seguridad para menores de edad en Instagram. Para obtener información sobre el nivel de seguridad que maneja Instagram[64] acerca de los menores de edad se procedió a realizar una revisión en las políticas de seguridad, se tomaron pantallazos como evidencia de los resultados que se obtuvieron, los cuales se podrán ver a continuación.

En la figura 31 ¿Puedo tener acceso a la cuenta de Instagram de mi hijo?, Instagram les explica a los padres que a partir de los 13 años el niño puede abrir una cuenta en esta red social y queda como titular autorizado ya que están incluidos de esa forma en las políticas de seguridad, por tal motivo no es posible que el padre tenga acceso a la cuenta del menor de edad.

[64] INSTAGRAM. Centro de seguridad y privacidad, Consejos para los padres [sitio web]. California. 2020. [Consultado: 17 de abril de 2020]. Disponible en: https://es-la.facebook.com/help/instagram/154475974694511/?helpref=hc_fnav&bc[0]=Ayuda%20de%20Instagram&bc[1]=Centro%20de%20privacidad%20y%20seguridad

Figura 33 ¿Puedo tener acceso a la cuenta de Instagram de mi hijo?

Fuente: https://esla.facebook.com/help/instagram/359897877431452?helpref=uf_permalink

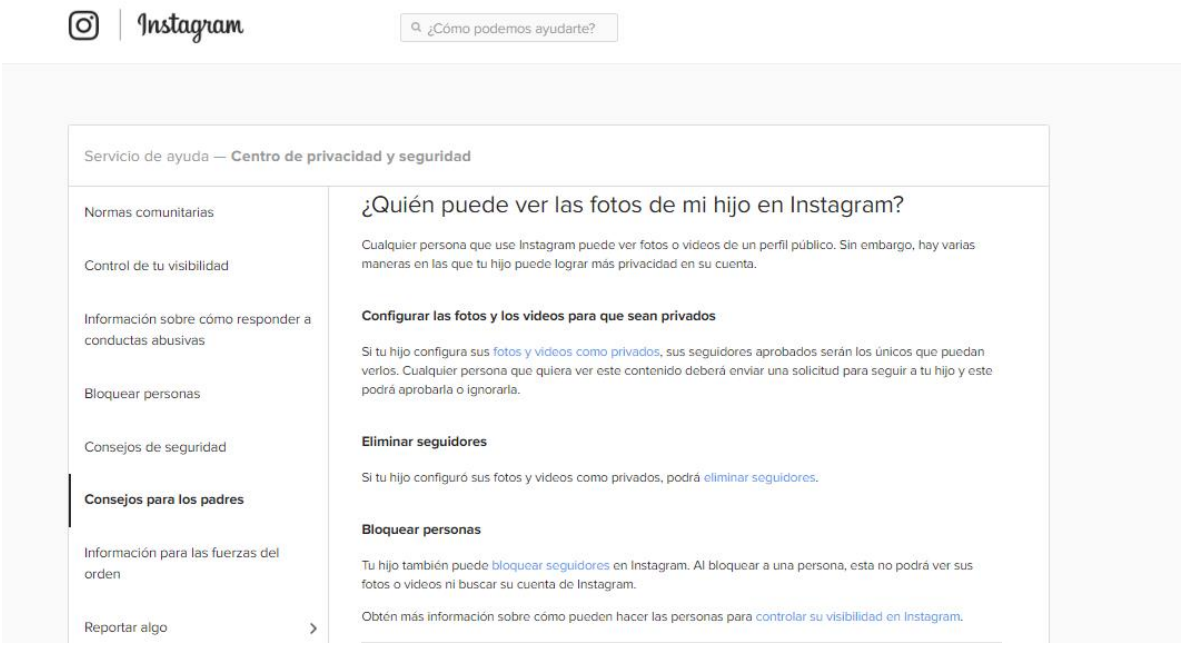
En la figura 32 ¿Por qué se eliminó una imagen que publiqué en Instagram de mi hijo?, al igual que Facebook, Instagram le explica a los padres por que en algunas ocasiones se les ha eliminado o se les eliminaran de sus redes sociales fotos de sus hijos, ya que los padres en diferentes oportunidades toman fotografías de sus niños desnudos cuando son muy pequeños, aunque lo hacen sin ninguna mala intención, al realizar dichos actos se están incumpliendo las normas comunitarias de la red social, y también se borran porque otras personas las pueden usar de manera indebida.

Figura 34 ¿Por qué se eliminó una imagen que publiqué en Instagram de mi hijo?

Fuente: https://es-la.facebook.com/help/instagram/242592952606350?helpref=related

En la figura 33 ¿Quién puede ver las fotos de mi hijo en Instagram? Se les explica a los padres que, si el perfil de la cuenta del menor es público, cualquier persona puede ver el contenido de sus fotos y videos, pero si se configura para que las fotos y videos sean privados, solamente tendrá acceso a estos los seguidores que tengan.

Figura 35 ¿Quién puede ver las fotos de mi hijo en Instagram?



Fuente: https://es-la.facebook.com/help/instagram/514520825226629?helpref=related

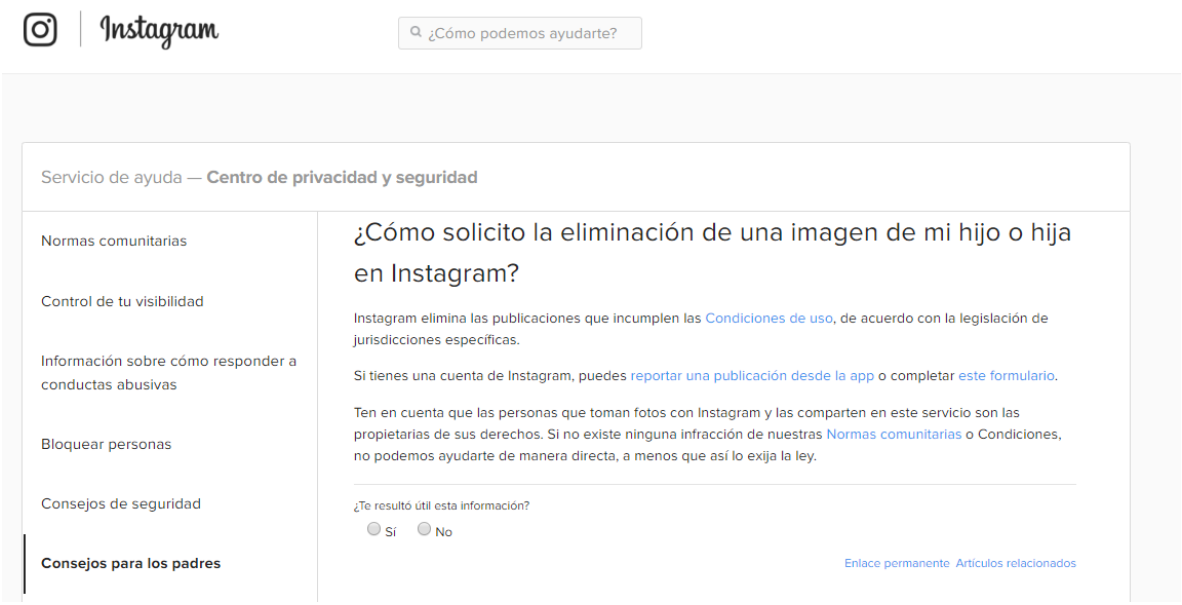
En la figura 34 ¿Cómo reporto a un menor de 13 años en Instagram?, se les explica a los padres que, si su hijo tiene 12 años y tiene una cuenta, esta debe estar administrada por un mayor de edad bien sea alguno de sus padres o un tutor, y eso debe estar evidenciado en la biografía de la cuenta del niño, si no es así la cuenta debe ser reportada y eliminada, si la red social, no encuentra ningún administrador del perfil, esta será eliminada inmediatamente.

Figura 36 ¿Cómo reporto a un menor de 13 años en Instagram?

Fuente: https://es-la.facebook.com/help/instagram/517920941588885?helpref=related

En la figura 35 ¿Cómo solicito la eliminación de una imagen de mi hijo o hija en Instagram?, se explica a los padres que, para eliminar alguna foto o video de la cuenta del menor, el contenido se debe reportar desde otro perfil, así se procederá a realizar la revisión y a verificar si se está violando las normas comunitarias de la red social, de ser así el material será eliminado de inmediato.

Figura 37 ¿Cómo solicito la eliminación de una imagen de mi hijo o hija en Instagram?



Fuente: https://es-la.facebook.com/help/instagram/150792105063683?helpref=related

En la figura 36 ¿Cómo podemos reportar mi hijo o yo comportamientos abusivos o materiales inapropiados u ofensivos en Instagram?, se les explica a los padres que si el menor tiene contenido obsceno o que si otro perfil tiene fotos o videos del menor se pueden reportar para ser eliminadas, si se verifica que dicho material está infringiendo las normas, se les recuerda a los padres que le deben indicar las normas adecuadas para el uso de redes sociales e internet.

Figura 38 ¿Cómo podemos reportar mi hijo o yo comportamientos abusivos o materiales inapropiados u ofensivos en Instagram?

Fuente: https://es-la.facebook.com/help/instagram/489507671074566?helpref=related

Con la revisión que se realizó sobre el nivel de seguridad disponible para menores de edad se pudo observar que Facebook contiene más políticas de seguridad, recomendaciones, y recursos de seguridad para padres, que ayudan a mitigar los riesgos que corren los niños cuando utilizan redes sociales, posteriormente

Instagram sigue en segundo lugar en cuanto al nivel de seguridad que brinda para proteger a los chicos, mientras que WhatsApp se encuentra en el último lugar ya que no se encontraron muchas políticas de seguridad que protejan a estos, incluso dentro de recomendaciones dicen que para eliminar una cuenta se debe enviar la factura de compra y la carta de propiedad de la línea telefónica, es evidente que en la actualidad, adquirir una sim card, una cuenta de WhatsApp entre otros es muy simple para cualquier persona, dado a que se pueden adquirir sin restricción ni control alguno por parte de la comercializadora o el gobierno, en consecuencia buscar, identificar o eliminar una cuenta perteneciente a un menor o a un acosador cada vez es más difícil.

5.6. RANGO DE EDADES DE LOS NIÑOS Y ADOLESCENTES QUE NAVEGAN EN INTERNET, QUE HAN CONOCIDO Y HAN TENIDO ENCUENTROS PERSONALES CON EXTRAÑOS CONOCIDOS POR MEDIO DE LAS REDES SOCIALES E INTERNET

La compañía de Telecomunicaciones Tigo Une[65] en los años 2017 y 2018 realizaron una investigación sobre la interacción que tienen los niños con el internet, los

[65] CONTIGO CONECTADOS. Riesgos y potencialidades del uso de las Tecnologías de la Información y la Comunicación [Sitio Web] Bogotá D.C Universidad EAFIT. Departamento de Comunicación, Escuela de Humanidades. Tigo Une. [Consultado: 22/03/2020]. Disponible en: https://contigoconectados.com/resultados/descargables/

riesgos más trabajados fueron el Grooming, el ciberbullying y lo delitos que están asociados con estas prácticas ilegales, como lo son el sexting, el acoso sexual y/o escolar.

Tigo Une[66] realizo 485 encuestas, a menores de edad con un rango de edades entre los 9 y los 16 años, donde el 50% fueron hombres y el 50% fueron mujeres, las encuestas fueron elaboradas a instituciones educativas de Bogotá, Medellín, Barranquilla, Cartagena, Cali, Manizales, Bucaramanga y Pereira, durante las encuestas que fueron realizadas se trataron diferentes temas como lo son el ciberbullying, la sexualidad, la seguridad, la brecha digital, las adicciones al internet, la salud, la educación entre otros lo cual fueron respuestas de menores entre 9 y 16 años.

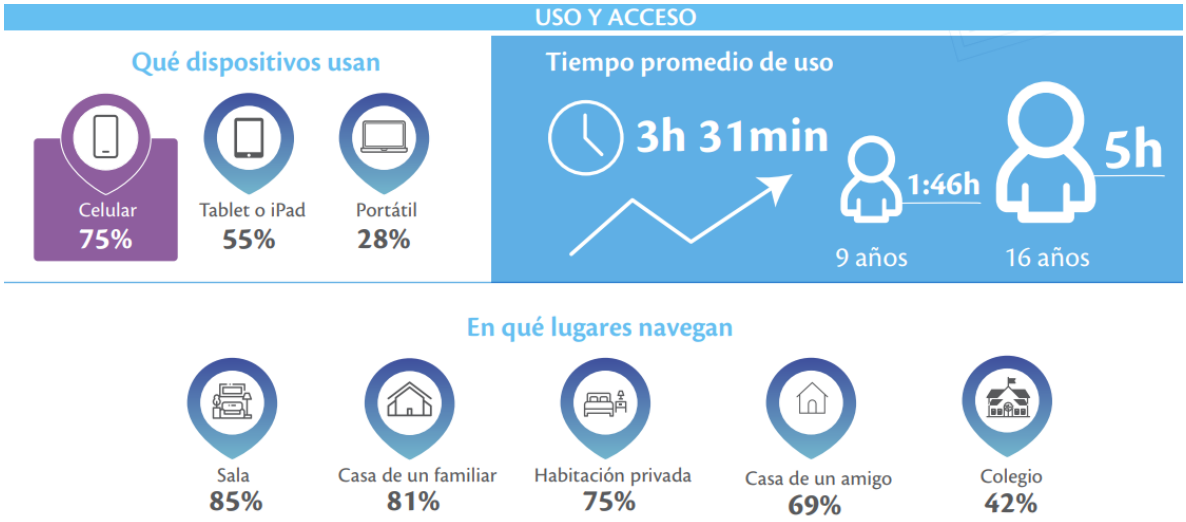
En las siguientes imágenes se podrán observar los resultados del análisis que se ha realizado, a las encuestas que realizo Tigo Une sobre el uso que los niños les dan a las redes sociales dependiendo de la edad en la que están.

En la figura 37 Medios de acceso a la internet, se puede observar que en la encuesta que realizo Tigo Une identificar que los menores usan para navegar en la red, aproximadamente un 75% el celular, las Tablet o iPad un 55% y el portátil lo usan

[66] Ibíd,. CONTIGO CONECTADOS. Riesgos y potencialidades del uso de las Tecnologías de la Información y la Comunicación [Sitio Web] Bogotá D.C Universidad EAFIT. Departamento de Comunicación, Escuela de Humanidades. Tigo Une. [Consultado: 22/03/2020]. Disponible en: https://contigoconectados.com/resultados/descargables/

un 28%, el lugar donde navegan por internet es en la sala un 85%, la casa de un familiar un 81%, la habitación privada un 75%, la casa de un amigo un 69%, y en el colegio un 42%, y el tiempo promedio que los menores le invierten a navegar es de 3 horas 31 minutos al día, los niños de 9 años invierten aproximadamente 1 hora 46 minutos y los niños de 16 años navegan aproximadamente 5 horas diarias

Figura 39 Medios de acceso a la internet



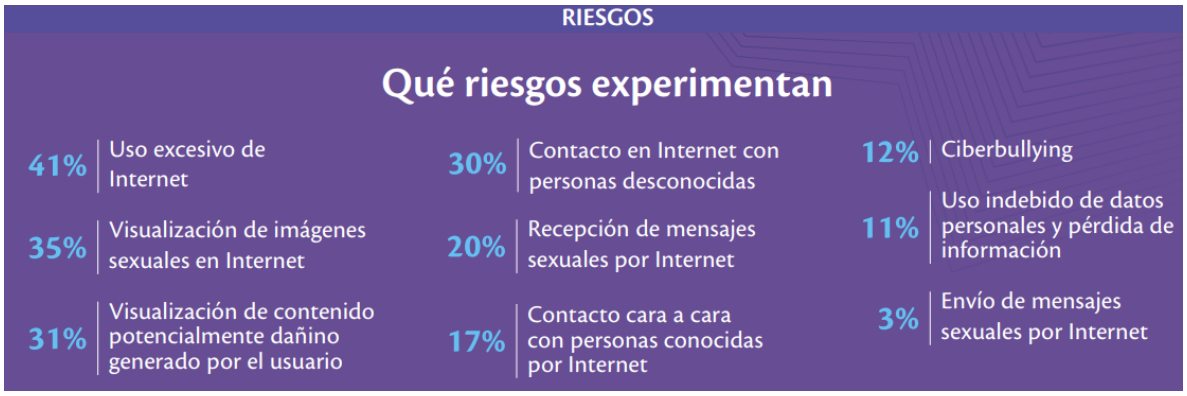
Fuente: https://contigoconectados.com/resultados/descargables/

En la figura ¿Que riesgos experimentan?, se puede observar que en la encuesta que realizo Tigo Une los riesgos que los menores experimentan al usar internet, el 41% uso excesivo de internet, el 35% visualización de imágenes sexuales, el 31% visualización de contenido potencialmente dañino generado por el usuario, el 30% contacto por medio de redes sociales con personas desconocidas, 20% recepción

de mensajes sexuales por internet, 17% contacto cara a cara con personas desconocidas, 12% ciberbullying, 11% uso indebido de datos personales y perdida de información, 3% envió de mensajes sexuales mientras navegan.

Como resultado se pude identificar que los niños en relación con el Grooming se ven expuestos en un 35% a visualizar imágenes sexuales en internet, en un 30% a tener contacto con personas desconocidas, en un 20% recepción de mensajes sexuales por la red, en un 17% contacto cara a cara con personas desconocidas 3% envió de mensajes sexuales en línea, que son las practicas que conllevan a los pederastas a cometer delitos sexuales en menores de edad.

Figura 40 ¿Que riesgos experimentan?



Fuente: https://contigoconectados.com/resultados/descargables/

En la figura 41 ¿En dónde han visto contenido sexual? se puede observar que en la encuesta que realizo Tigo Une a los menores entre 9 y 16 años se encontró que el contenido sexual que han visto cuando navegan por internet ha sido con un total de 24% en redes sociales, el 13% por medio de ventanas emergentes, 10% películas o videos, 7% en páginas xxx, y el 3% en juegos online, esto quiere decir que las redes sociales son el medio más fácil para que los menores vean contenido sexual

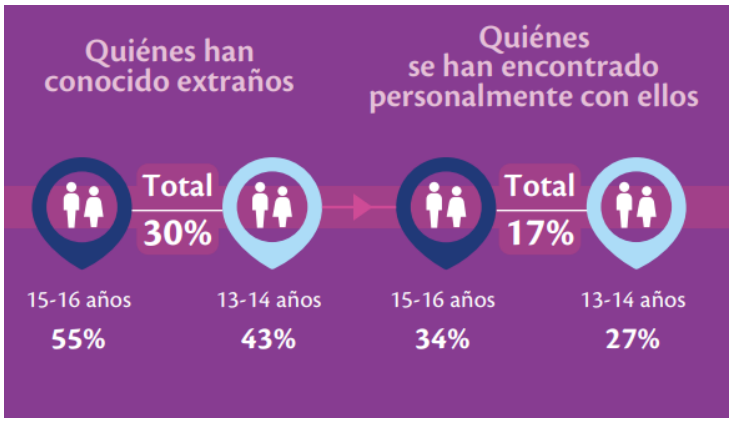
Figura 42 ¿En dónde han visto contenido sexual?

Fuente: https://contigoconectados.com/resultados/descargables/

En la figura 40 ¿Promedio de edades de los menores que han interactuado con adultos extraños?, se muestra la encuesta realizada por Tigo Une en la cual se puede observar que los menores de entre 15 y 16 años con un total de 55% de los cuales encuestados han conocido extraños por medio de la interacción con las

redes sociales e internet, y aquellos comprendidos entre las edades de 13 y 14 años con un total de 43% han conocido extraños por medio de redes sociales, de estos con un total de 17 % se han conocido personalmente con los desconocidos que habían contactado y entre los pre adolescentes de 15 y 16 años con un total de 34% han sido quienes se han encontrado personalmente con los extraños, y de los niños entre 13 y 14 años con un total 27% se han encontrado personalmente con los acosadores que han conocido, es decir que aquellos que tienen entre 15 y 16 años son más propensos a conocer estos delincuentes por medio de la red e internet y a conocerlos personalmente.

Figura 43 ¿Promedio de edades de los menores que han interactuado con adultos extraños?

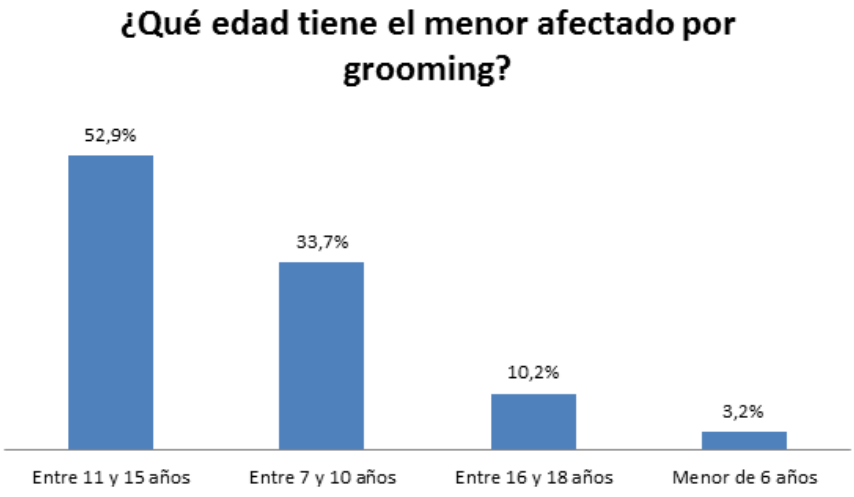


Fuente: https://contigoconectados.com/resultados/descargables/

5.6.1. Rango de edades de los niños y adolescentes que han estado expuestos al grooming. Se realizo una búsqueda en las diferentes fuentes públicas sobre el rango de edades de los niños y adolescentes que han estado expuestos al grooming, suponiendo que algunas edades son más vulnerables que otras, se encontró la siguiente información.

En la figura 41 ¿Qué edad tiene el menor afectado por grooming?, se puede observar que el 52,9% de los menores afectados por grooming oscilan entre 11 y 15 años, el 33,7% tienen entre 7 y 10 años, el 10,2% tienen entre 16 y 18 años y el 3,2% tienen entre 3 y 7 años.

Figura 44 ¿Qué edad tiene el menor afectado por grooming?



Fuente:

https://repositorio.comillas.edu/xmlui/bitstream/handle/11531/30848/TFG%20Alonso%20Gonzalez%2C%20Patricia.pdf?sequence=1&isAllowed=y

Alonzo Gonzales, Patricia[67] en su investigación sobre el Grooming, identifica que el 66% de las mujeres menores de edad son más propensas a ser víctimas de Grooming a diferencia de los hombres quienes ocupan un 36% de afectación.

En un estudio realizado por Garmendia[68] se encontró que un total de 31% de los jóvenes han recibido mensajes que tienen material sexual, se identificó que el mensaje 28% de las mujeres recibieron este tipo de mensajes mientras que el 35% de los hombres también recibieron este tipo de mensajes. También se encontró en ese estudio que el sexting que está directamente relacionado con el grooming y el internet, se aumenta con edad de los menores, ese estudio fue realizado a chicos de 9 a 16 años, identificando así que el 19% entre 11 y 12 años se ven afectados, el 34% de 13 y 14 y el 42% de 15 y 16 han realizado estas prácticas.

[67] ALONZO GONZALES, Patricia. Online Grooming [en línea]. Trabajo de investigación Ciencias Humanas y Sociales. Madrid España. Comillas Universidad Pontificia. Facultad Ciencias Humanas y Sociales. 2019. 16 p. [Consultado: 26/03/2020]. Disponible en: https://repositorio.comillas.edu/xmlui/bitstream/handle/11531/30848/TFG%20Alonso%20Gonzalez%2C%20Patricia.pdf?sequence=1&isAllowed=y

[68] GARMENDIA, M. JIMÉNEZ, E., CASADO, M.A. y MASCHERONI, G. Net Children Go Mobile: Riesgos y oportunidades en internet y el uso de dispositivos móviles entre menores españoles (2010-2015) [en línea] Madrid España. Universidad del País Vasco. Citado por. VILLANUEVA BLASCO Víctor José. SERRANO BERNAL, Sara. Patrón de uso de internet y control parental de redes sociales como
predictor de sexting en adolescentes: una perspectiva de género [en línea]. Consejo General de la Psicología. 2019 17 p. [Consultado: 26/03/2020]. Disponible en: http://eds.b.ebscohost.com.bibliotecavirtual.unad.edu.co/eds/pdfviewer/pdfviewer?vid=4&sid=0d4399a9-20c4-40fc-a61d-5a458c2ebb47%40sessionmgr103

6. MÉTODOS QUE LE PERMITEN A LA POBLACIÓN EN GENERAL IDENTIFICAR, MITIGAR Y REDUCIR EL IMPACTO QUE TIENE EL GROOMING EN LOS MENORES DE EDAD

GARCIA, Polkan.[69] Afirma que para que la navegación en internet de los menores sea sana los padres deben guiar a los hijos y comunicarse con ellos constantemente.

Después de observar todos los riesgos a los que los menores de edad están expuestos hoy en día, por causa de un mal uso de la internet, riesgos tales como el grooming, el sexting, la suplantación de identidad, el acoso sexual cibernético, las extorciones, los chantajes, hasta inclusive corren el riego de un posible secuestro muchas veces para trata de blancas, se ve necesario recomendar procesos y métodos que permitan evitar, mitigar y reducir el impacto que tiene el grooming en los chicos, por tal motivo se podrán observar los pasos que se deben seguir para enseñarle a estos a manejar de una forma correcta el internet y las redes sociales, y se podrán observar las plataformas donde se pueden denunciar el grooming, la sextorsión y todos los delitos informáticos relacionados con niños.

[69] GARCIA, Polkan. Los niños y jóvenes colombianos usan internet tres horas y media al día [en línea]. En. La República. Bogotá D.C. 4 de agosto 2018. [Consultado: 01 de abril de 2020]. Disponible en: https://www.larepublica.co/internet-economy/los-ninos-y-jovenes-colombianos-usan-internet-tres-horas-y-media-al-dia-2756640

6.1. MANUAL PARA PADRES, EDUCADORES HE HIJOS, SOBRE EL CORRECTO USO DE LA INTERNET Y LAS REDES SOCIALES

Después de haber observado todos los métodos para hacer grooming, los riesgos en los que se ven sometidos los menores, los medios que se han creado para denunciar y mitigar el grooming, las redes sociales que más se usan y las posibilidades que nos administran dichas redes sociales se deben implementar medidas para mitigar el riesgo al que se ven expuestos, en la Guía Clínica sobre el ciberacoso para profesionales en la salud[70], se enfatiza en que los padres, educadores, y menores deben implementar métodos que permitan realizar un buen uso de las Tic, por tal motivo en el siguiente apartado se podrá observar un manual de recomendaciones que deben seguir los padres, educadores e hijos el cual les servirá para hacer un buen uso de la internet y sobre todo libre de riesgos.

6.1.1. Prevención y educación. Es necesario que los padres y educadores utilicen métodos de enseñanza que les permitan evitar que los menores sean engañados en las redes sociales, la prevención es la parte más importante, ya que

[70] RED.ES, SEMA. Guía clínica de ciberacoso para profesionales de la salud. Plan de confianza del ámbito digital del Ministerio de Industria, Energía y Turismo. Hospital Universitario La Paz, Sociedad Española de Medicina del Adolescente, Red.es. Madrid. 2015. 6 p. [Consultado el 17 de abril de 2020]. Disponible en: https://www.observatoriodelainfancia.es/ficherosoia/documentos/4514_d_Guia_Ciberacoso_Profesionales_Salud_FBlanco.pdf

si los estos aprenden a seguir unas normas de uso y a comportarse en las redes sociales se evitara que caigan en las redes de los pederastas.

6.1.2. Prevención en casa, García, Beatriz[71] en su libro resalta que son bastantes los estudios que afirman el riesgo y el peligro que corren los menores al hacer uso de la internet y las redes sociales, ya que los niños hacen uso de estos por largas horas, es por eso que es de gran importancia que los padres realicen monitorio contante y sigan algunas indicaciones para que los sus hijos tengan un uso correcto de redes sociales y no caigan en riesgos por causa del grooming, sexting, y todas aquella prácticas a las que se ven expuestos hoy en día, a continuación usted podrá encontrar algunos pasos que debe establecer cuando el inicie su vida digital y haga uso constante de la internet y las redes sociales:

- Para que el niño realice la apertura de una cuenta en una red social debe tener como mínimo 13 años, si tiene 12 y hace uso de estas, debe estar el 100% del tiempo monitoreado por el padre.
- Antes de que el menor habrá una cuenta en una red social, es importante que los padres hablen con anticipación sobre la internet explicando las ventajas, los riesgos y los peligros que pueden encontrar a partir de que empiece a utilizar el mundo digital, para esto los padres deben tener una comunicación fluida, de

[71] GARCIA, Beatriz Catalina. Los padres ante el uso de Internet y redes sociales por menores. Control y protección [en línea]. España. Revista Latina. Universidad de La Laguna. Diciembre 2013. [Consultado el 19 de abril de 2020]. Disponible en: http://www.revistalatinacs.org/13SLCS/2013_actas/077_Catalina.pdf

confianza y tener una participación activa para que el niño no se sienta obligado a mantener conversaciones sobre el tema y así los chicos puedan conversar con sus padres cuando necesiten ayuda o se sientan en peligro.

- Es de suma importancia establecer normas y horarios para el uso de redes sociales.
- Los padres deben estar presente cuando el menor realice la apertura de la red social.
- Los padres deben enseñarle al menor la forma correcta de usar una red social.
- Los padres deben enseñarle al menor a reconocer las páginas que no son confiables y deben dejarles en claro que no deben entrar en ellas, las contraseñas deben ser seguras y se deben cambiar constantemente.
- Dentro de las normas que se le van a establecer al menor, se le debe dejar muy en claro que el padre debe tener el usuario y la contraseña de la red social para monitorear en caso de ser necesario.
- Se debe administrar la privacidad de la cuenta para que no sea publica, debe estar en modo privado, la ubicación debe estar desactivada, y el etiquetado también debe estar desactivado, aunque estas dos últimas vienen en modo desactivado de manera predeterminado por la red social, es importante estar monitoreándolo.
- Se deben administrar las interacciones en las redes sociales, para que solamente pueda interactuar con los amigos.

- Se le debe enseñar al menor que solamente debe aceptar solicitudes de amistad de personas conocidas, al igual que solo debe enviar solicitudes de amistad a personas conocidas.
- Se le debe enseñar al menor que no debe compartir información personal ni del ni de ninguno de sus familiares o amigos por medio de redes sociales.
- Se le debe enseñar al menor que debe hacer caso omiso, reportar y bloquear y avisar a los padres sobre perfiles en el caso en el que le envíen mensajes pidiéndole fotos o videos mostrando sus partes íntimas o citándolo a encuentros personales, y se le debe dejar en claro que si es algún conocido quien le está pidiendo fotos o videos debe realizar el mismo procedimiento que se mencionó anteriormente.
- Es muy importante explicarle que es el grooming, el sexting, el acoso sexual cibernético, el ciber bullying, la suplantación de identidad, y mostrarle casos de la vida real para que el menor conozca los riesgos a los que se puede ver expuesto en caso de no cumplir con las pautas mencionadas anteriormente.
- Cuando el menor navega por internet se recomienda que no esté solo ni encerrado en su cuarto, siempre debe estar bajo supervisión de un adulto responsable.
- Los padres deben implicar el uso de filtros y control parental.
- Instalar programas de protección como antivirus y firewall, en los computadores, Tablet y teléfonos móviles.

- Se debe actualizar el navegador y activar el bloqueo de la ejecución automática de programas y funciones maliciosas en la web.
- Se debe cambiar la contraseña del wifi de manera periódica.
- Se debe limitar el acceso a cafés internet.
- Se debe tener desactivada la cámara web o taparla.

6.1.3. Prevención desde los colegios. Inteco[72] resalta en su guía s.o.s contra el grooming padres y educadores que, así como se debe hacer una labor de prevención en la casa, también es de suma importancia que los colegios y los docentes se unan a esta tarea, y empiecen a realizar una labor de prevención y mitigación, la cual permita evitar que los niños y los adolescentes se vean afectados por el grooming. En los colegios se deben realizar pasos muy parecidos a los que deben seguir los padres, los cuales se verán descritos a continuación:

- Realizar campañas de socialización y charlas acerca del uso de la internet y las redes sociales para los alumnos y padres.
- Realizar campañas de socialización y charlas acerca de los peligros y delitos a los que se ven expuestos los menores de edad, como lo son el grooming, el

[72] INTECO. Guía s.o.s contra el grooming padres y educadores [en línea]. Instituto Nacional de las Tecnologías de la comunicación. Ministerio de Industria Tecnología y Comercio. España. p 9. [Consultado: 20 de abril de 2020]. Disponible en internet: https://www.adolescenciasema.org/usuario/documentos/sos_grooming.pdf

acoso sexual cibernético, el sexting, la suplantación de identidad, el ciberbullying, entre otros, para los alumnos y padres.

- Dar a conocer casos y testimonios de víctimas del grooming.
- Limitar los tiempos de uso del celular en clases y espacios académicos.
- Crear una red de apoyo para prevención y mitigación entre padres, docentes y alumnos.
- Coordinar entre padres y los colegios protocolos para el uso de la tecnología y las redes sociales.
- Bloquear el ingreso a redes sociales y plataformas online desde los equipos de cómputo de los colegios.
- Establecer mecanismos de acción y ayudas psicológicas en caso de tener o sospechar de víctimas o victimarios de grooming en el colegio.

6.1.4. Prevención desde los menores. Es importante darle a conocer a los menores que de ellos depende en la gran mayoría que no se vean afectados por el grooming, hay que enseñarles a identificar a los pederastas, es mejor que ellos identifiquen muy bien los métodos de acción del delincuente, y se recomienda que ellos identifiquen los pasos que se encomiendan y que deben seguir para hacer un uso correcto de redes sociales, los cuales podrán ver a continuación:

- Debes tener como mínimo 13 años para hacer apertura de una red social y contar con la previa autorización de los padres.
- Configurar el perfil de la red social en modo privado.
- No compartir información personal ni de ningún familiar o amigo con desconocidos.
- No aceptar ni enviar solicitudes de amistad a personas que no conozca.
- Utilizar contraseñas seguras y cambiarlas constantemente.
- No publicar fotos ni videos mostrando partes íntimas.
- Limitar el tiempo de navegación ya que puede interferir con el tiempo de estudio y de compartir con la familia.
- Mantener informados a los padres o educadores, sobre cualquier interacción anormal o algún mensaje raro o sospechoso por recibido por medio de redes sociales.
- No enviar imágenes, ni fotos personales a personas desconocidas, así sean menores de edad.
- Antes de realizar alguna publicación, se debe analizar muy bien si el contenido es el adecuado para compartir.
- No acordar encuentros personales con desconocidos así sean menores de edad.

6.1.5. Pasos para denunciar en caso de ser víctima de grooming. Inteco[73] en su Guía s.o.s contra el Grooming, proporcionan unos pasos a seguir cuando los padres, los educadores y el menor de edad se dan cuenta que están siendo víctimas del pederasta por medio del grooming es necesario que sigan algunos pasos los cuales permitirán dejar de caer en manos del delincuente y se debe denunciar al pederasta, teniendo en cuenta las siguientes recomendaciones:

- Se debe evitar que el menor continúe manteniendo cualquier tipo de interacción con el pederasta.
- No ceder a los chantajes y a las extorciones a las que el pederasta quiere llevarlos.
- Hablar con el menor de edad brindándole confianza para que cuente todo lo sucedido.
- Recopilar todas las pruebas como capturas de pantalla con las conversaciones entre el menor y el pederasta, no borrar ninguna conversación, ni ocultar material ya que cualquier prueba, aunque sea mínima es necesaria para la investigación policial.
- Reportar y bloquear la cuenta o el perfil social del pederasta.

[73] Ibíd., p. 8, 11. INTECO. Guía s.o.s contra el grooming padres y educadores [en línea]. Instituto Nacional de las Tecnologías de la comunicación. Ministerio de Industria Tecnología y Comercio. España. p 8. [Consultado: 20 de abril de 2020]. Disponible en internet: https://www.adolescenciasema.org/usuario/documentos/sos_grooming.pdf

- Entablar la denuncia ante los entes de control, como lo son la Policía, la Fiscalía o en Te Protejo de Red PaPaz.
- Si la persona que se da cuenta no es el padre, debe hablar inmediatamente con los padres del menor, si ellos no hacen caso, entablar la denuncia con los entes de control como la Policía, la Fiscalía o en Te Protejo de Red PaPaz.
- Proveer al menor, ayuda psicológica.
- Así el pederasta haya dejado de chantajear o acosar al menor, se debe establecer la denuncia.

6.1.6. Medios de prevención y denuncia online. Existen diferentes medios digitales para realizar las respectivas denuncias en caso de ser víctima del grooming, como lo son las plataformas y las aplicaciones móviles creadas por la Red PaPaz[74], que es la plataforma Te Protejo que se encuentra en una página web o se puede descargar como aplicación en el celular, otro medio de denuncia que se puede encontrar en internet es el centro cibernético de la policía nacional, y la página de la fiscalía.

[74] ESCUDOS DEL ALMA. Op. cit. Aplicación web Te Protejo. [sitio web] Red Papaz. Bogotá. [Consultado: 06 de marzo de 2020]. Disponible en internet: http://www.redpapaz.org/escudos/index.php?option=com_k2&view=item&id=478:te-protejo&Itemid=104

6.2. DENUNCIAS ONLINE EN TE PROTEJO DE RED PAPAZ

Red PaPaz creo una plataforma llamada Te Protejo, con el objetivo de canalizar las denuncias por diferentes delitos cometidos a menores de edad para posteriormente enviarlas a la policía nacional, dentro de los delitos que se pueden denunciar en Te Protejo están: Material de Explotación Sexual de niñas, niños y adolescentes (Pornografía Infantil), explotación sexual comercial (ESCNNA), ciberacoso, intimidación escolar, p y contenidos inapropiados, venta de tabaco, alcohol, y otras drogas, maltrato, abuso y trabajo infantil, otras situaciones.

A continuación, usted podrá ver la descripción de la forma en que se utiliza la plataforma para realizar una denuncia.

En la figura 42 Denuncias en Te Protejo, se pueden observar los delitos que se pueden denunciar por medio de la plataforma Te Protejo, los delitos son Material de Explotación Sexual de niñas, niños y adolescentes (Pornografía Infantil), explotación sexual comercial (ESCNNA), ciberacoso, intimidación escolar, p y contenidos inapropiados, venta de tabaco, alcohol, y otras drogas, maltrato, abuso y trabajo infantil, otras situaciones.

Figura 45 Denuncias en Te Protejo

Fuente: https://teprotejo.org/

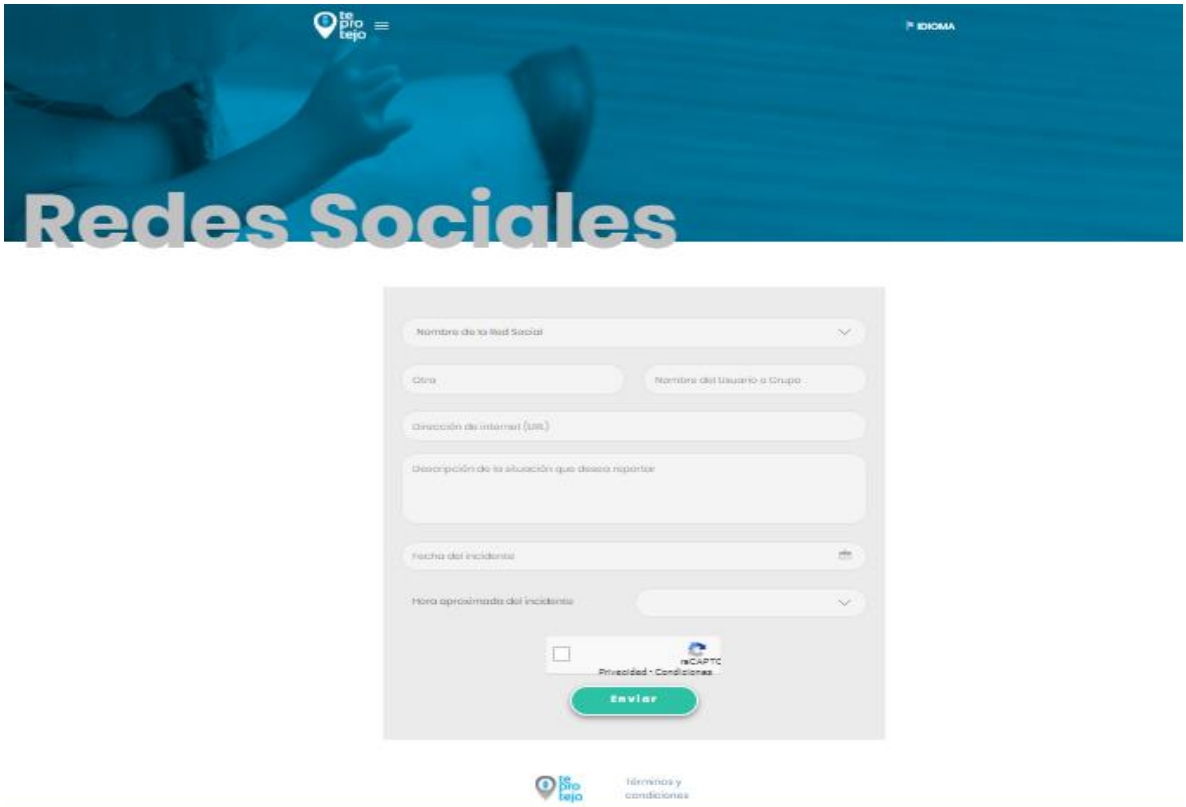
En la figura 43 Denuncia de Material de Explotación Sexual de niñas, niños y adolescentes (Pornografía Infantil), se puede observar que al elegir un ítem el cual en este caso fue Material de Explotación Sexual de niñas, niños y adolescentes, lleva al usuario a elegir el medio por el cual se está cometiendo el delito, en este caso se puede elegir si el delito es cometido por un sitio en internet, E-mail, Chat, MSN Messenger, Skype, ICQ, otro, redes sociales u otro medio.

Figura 46 Denuncia de Material de Explotación Sexual de niñas, niños y adolescentes (Pornografía Infantil)

Fuente: https://teprotejo.org/categorias-de-reporte/material-de-abuso-sexual/

En la figura 44 Denuncia de un acoso ocurrido por medio de redes sociales, se eligió realizar una denuncia de un caso de acosos ocurrido en redes sociales, por tal motivo la plataforma solicita el nombre de la plataforma, el nombre del perfil de la cuenta del acosador, la dirección o el url de internet, la descripción del incidente ocurrido, fecha y la hora aproximada del suceso, posteriormente se da clic en el botón enviar y con esto ya queda la denuncia, luego la plataforma canaliza la acusación a la policía y ellos continúan con el seguimiento del caso.

Figura 47 Denuncia de un acoso ocurrido por medio de redes sociales



Fuente: https://teprotejo.org/categorias-de-reporte/material-de-abuso-sexual/redes-sociales/

Para realizar una denuncia en Te Protejo de clic en el siguiente enlace: https://teprotejo.org/

6.2.1. Denuncias online Centro Cibernético de la Policía Nacional. Otra forma de realizar denuncias sobre casos de grooming donde está involucrado el sexting, el acoso sexual cibernético, la suplantación de identidad y los delitos

relacionados con el grooming es por medio del Centro Cibernético de la Policía Nacional[75], a continuación, podrá ver la forma de realizar las denuncias.

En la figura 45 Denuncias en el Centro Cibernético de la Policía Nacional, se puede observar el interfaz grafico de la plataforma Online del Centro Cibernético de la Policía Nacional, como se puede observar está disponible el ingreso al CAI Virtual donde se podrán establecer las denuncias pertinentes con el grooming.

Figura 48 Denuncias en el Centro Cibernético de la Policía Nacional

Fuente: https://caivirtual.policia.gov.co/

[75] CENTRO CIBERNÉTICO DE LA POLICÍA NACIONAL. Denuncias en el Centro Cibernético de la Policía Nacional [sitio web]. Policía Nacional. Bogotá D.C. 2020. [Consultado: 02/04/2020]. Disponible en: https://caivirtual.policia.gov.co/

Para realizar una denuncia en el Centro Cibernético de la Policía Nacional de clic en el siguiente enlace: https://caivirtual.policia.gov.co/

6.3. SISTEMA NACIONAL DE DENUNCIA VIRTUAL POLICÍA NACIONAL Y FISCALÍA DE LA NACIÓN

Otra forma de realizar una denuncia sobre grooming y los delitos implicados como el sexting, el acoso sexual cibernético, y la suplantación de identidad es por medio del sistema Nacional de Denuncia Virtual[76], a continuación, se podrá observar la forma en la que se puede realizar una denuncia por este medio.

En la figura 46 Sistema Nacional de Denuncia Virtual ... ¡A Denunciar!, se puede observar la plataforma que tiene la Policía Nacional y la Fiscalía General de la Nación, en esa plataforma se pueden realizar diferentes denuncias incluyendo los delitos informáticos y el material con contenido de explotación sexual infantil.

[76] POLICÍA NACIONAL, FISCALÍA NACIONAL. Sistema Nacional de Denuncia Virtual ¡A Denunciar! [en línea]: Policía Nacional. Bogotá. 2020. [Consultado: 02/04/2020]. Disponible en: https://adenunciar.policia.gov.co/adenunciar/default.aspx

Figura 49 Sistema Nacional de Denuncia Virtual ... ¡A Denunciar!

Fuente: https://adenunciar.policia.gov.co/adenunciar/default.aspx

En la figura 47 Denuncia por delitos informáticos, se puede observar que, al elegir el ítem para realizar la denuncia por delitos informáticos, el sistema va a pedir todos los datos personales del denunciante, incluyendo nombres y apellidos, sexo, edad, fecha de nacimiento, documento de identidad, entre otros.

Figura 50 Denuncia por delitos informáticos

Fuente: https://adenunciar.policia.gov.co/adenunciar/frm_denuncia_di.aspx

Para realizar una denuncia en el Sistema Nacional de denuncias de la Policía Nacional y la Fiscalía siguiente enlace: https://adenunciar.policia.gov.co/adenunciar/frm_denuncia_di.aspx

7. CONCLUSIONES

- Durante el desarrollo de la monografía se logró identificar que la ingeniería social consiste en manipular de forma psicológica, de manera presencial o utilizando elementos de telecomunicación, con el objetivo de obtener información importante de una persona, empresa u organización, el resultado de esa información el delincuente la utilizara en este caso específico del grooming para acosar, extorsionar, o lograr cuadrar encuentros personales que serán utilizados para cometer actos sexuales con los menores de edad.

- Se logro obtener como resultado la identificación de los diferentes métodos que utiliza la ingeniería social para involucrarse con la población infantil, acto que ejecutan mediante técnicas y fases, las técnicas que utiliza el pederasta para hacer ingeniería social son pasivas (implementación de ingeniería social, observar, analizar el comportamiento de la víctima, establecer un perfil psicológico), técnicas presenciales no agresivas (resultados, seguir la víctima, vigilar la casa y empleo de la víctima, sus familiares y personas más cercanas, buscar información en su entorno), técnicas no presenciales (trata de obtener información de la víctima por medio de redes sociales, suplantación de identidad, solicitud de información por medio de correos electrónicos, llamadas, mensajes de texto) y técnicas agresivas (extorciones, presión física, presión psicológica,

suplantación de identidad, abusos, chantajes, contacto sexual, acoso sexual), y las fases que ejecutan son: Fase 1 (consiste en buscar a la víctima), Fase 2 (Enganche), Fase 3 (Fidelización), Fase 4 (aislamiento), Fase 5 (seducción).

- Se logro identificar que el grooming es un método de la ingeniería social, el cual es utilizado por los pederastas para acercarse a los menores de edad principalmente por medio de redes sociales, quien se vale de diferentes métodos para lograr entablar una amistad con los niños, como lo son, suplantación de identidad, amabilidad, dar regalos costosos a estos, ganarse la confianza de la víctima, el victimario logra ser la persona más importante en la vida del niño, se convierte en alguien imprescindible, es decir en la persona más cercana a la víctima, para que no le cuente a nadie lo que está sucediendo realmente, todo esto lo hace el acosador con diferentes objetivos como hacer que el acosado le envié material sexual, fotos y videos personales con poses sexuales y mostrando las partes íntimas, las cuales serán utilizadas más adelante por el para acosar al niño y mantener encuentros sexuales con el menor, con el objetivo posteriormente de extorsionarlo a él y a los padres y obtener beneficios monetarios, también para vender el material sexual obtenido de parte del infante o para publicarlo en chats sexuales online, incluso él puede hacer grooming con el objetivo de secuestrar a los menores y venderlos para trata de blancas.

- Se lograron identificar los diferentes términos y los contrastes que existen entre la pedofilia, que es la inclinación de los adultos a sentir atracción sexual hacia los prepúberes, el pedófilo que es el adulto que se interesa por sentir atracción sexual y amorosa por niños y niñas preadolescentes, la hebofilia que es el adulto que se interesa por adolescentes, los cuales ya han tenido el despertar sexual, y el pederasta quien es el único que pasa a tener contacto físico con los menores de edad, a diferencia del pedófilo quien es el que solamente ve material sexual pero jamás toca a un chico.

- Se realizo una búsqueda del incremento de delitos sexuales infantiles del año al año 2019 obteniendo como resultado, que en el año 2015 se presentaron 518 denuncias teniendo un total del 10%, en el año 2016 se presentaron 866 teniendo un total de 17%, en el año 2017 se presentaron 132 teniendo un total 25%, en el año 2018 se presentaron 1323 teniendo un total 28%, en el año 2019 se presentaron 1038 teniendo un total 20% en comparación con los años anteriores, teniendo como resultado que en el año 2015 se presentaron menos casos y en el año 2018 fue el año donde se presentaron más casos.

- Se realizo una búsqueda de los delitos informaticos donde se ven involucrados menores de edad los cuales fueron reportados en el año 2019, donde se identificó que el grooming tuvo 202 casos reportados, la sextorsión 281, el ciberbullying 73, y la publicación de imágenes no autorizadas fueron 93.

- Se lograron identificar y describir en la monografía las leyes que penalizan los delitos sexuales que se tienen como resultado de practicar el grooming, dichas leyes son: Ley 1273 del 2009, la cual se encarga de castigar cualquier delito informático en el territorio colombiano, y la Ley 679 de 2001 (agosto 3), la cual se encarga de prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores.

- Se logro identificar que existen plataformas creadas para reportar casos de prácticas de grooming y delitos informaticos como lo son el sexting, el acoso sexual cibernético, la extorsión, la suplantación de identidad, tales plataformas son: Te Protejo que también funciona para descargar como APP en androide, la cual es creada por Red Papaz, y se encarga de recepcionar denuncias de delitos causados a menores de edad y canalizarlos con el centro cibernético de la policía nacional, o directamente con la policía nacional y la fiscalía que también ya cuentan con plataformas virtuales donde se pueden hacer este tipo de denuncias.

- Se realizo un análisis a los casos reportados por Te Protejo donde se hacen reportes acerca de material de abuso sexual (pornografía infantil), ciberacoso, contenidos inapropiados en medios de comunicación, los cuales están vinculados con el grooming, donde se obtuvieron las siguientes cifras: En el año 2012, 2.192 denuncias, dentro de las cuales, hay 462 que tienen que ver con contenidos sobre

abuso sexual, explotación sexual, comercial y pornografía infantil, 145 sobre contenido inapropiado en medios de comunicación.

- En el año 2013 se evidencia el reporte de las denuncias que fueron recepcionadas, obteniendo como resultado 3.921 denuncias dentro de las cuales, hay 1.493 que tienen que ver con contenidos sobre abuso sexual, explotación sexual, comercial y pornografía infantil, y 263 sobre contenido inapropiado en medios de comunicación.

- En el año 2014 fueron recibidas un total de 6.452 denuncias, mientras que en la pornografía infantil se presentaron 3.724, 491 involucradas con ciberacoso, y 245 sobre contenido inapropiado en medios de comunicación.

- En el año 2015 fueron 8.706 denuncias, dentro de las cuales, hay 5.827 que tienen que ver con contenidos sobre abuso sexual, explotación sexual, comercial y pornografía infantil, 539 involucradas ciberacoso, y 175 sobre contenido inapropiado en medios de comunicación.

- En el año 2016 fueron 10.424 denuncias, dentro de las cuales, hay 7.416 que tienen que ver con contenidos sobre abuso sexual, explotación sexual, comercial y pornografía infantil, 724 involucradas con ciberacoso, y 264 sobre contenido inapropiado en medios de comunicación.

- En el año 2017 fueron 8.991 denuncias, dentro de las cuales, hay 5.187 que tienen que ver con contenidos sobre abuso sexual, explotación sexual, comercial y pornografía infantil, 724 involucradas con ciberacoso, y 264 sobre contenido inapropiado en medios de comunicación.

- Esto quiere decir que del año 2012 al año 2018 el caso más reportado, fue el Material de abuso sexual (Pornografía) con 32.288 casos, ocupando el 61% de porcentaje, mientras que el ciber acoso fue el segundo delito más reportado con 3.826, y el contenido inapropiado en medios de comunicación ocupo el último puesto con 1.499, dentro de las categorías que están implicadas con el grooming en el año 2019, nuevamente la categoría de material de abuso/explotación sexual (pornografía infantil) ocupo el 86%, esto quiere decir que aumentó un 25% en comparación con los anteriores años que ocuparon un rango de 61%, el ciberacoso obtuvo el 4.5% de rango, 2.5% menos reportes que los anteriores años, y sobre contenidos inapropiados en medio de comunicación ocuparon 1.1%, 1.9% menos que los anteriores años. Afortunadamente lo que fue ciberacoso y contenidos inapropiados en medio de comunicación disminuyeron, pero la categoría de material de abuso material de abuso/explotación sexual (pornografía infantil) como se mencionaba anteriormente aumento el 25%.

- Se logro identificar que Te Protejo durante el año 2019 logro bloquear 3.904 páginas web, ya que contenían abuso sexual y explotación infantil, de las cuales

2.955 URL fueron ingresadas a través de ICCAM-INHOPE, en las que se encontraron 6.694 imágenes de explotación infantil cuyo desmonte fue solicitado a la red INHOPE, y de las denuncias que canalizo Te Protejo al centro cibernético de la policía nacional fueron suspendidas 819 páginas con dominio, por contener material de abuso y explotación sexual.

- Se realizo un análisis de las redes sociales más comunes y que son más utilizadas por los menores de edad obteniendo como resultado que Facebook es utilizado en un total del 44%, WhatsApp el 31%, el 9%, Instagram el 8%, y You Tube el 8%, también se identificó en una encuesta realizada por Tigo Une que el 84% de los niños cuando usan internet destinan su tiempo a usar redes sociales, dentro de los análisis que se hizo también se investigó el nivel de seguridad que utilizan las redes sociales para proteger a los niños, haciendo un paralelo entre las políticas de seguridad de Facebook, WhatsApp e Instagram y se encontró lo siguiente:

  A comparación con las políticas de seguridad para menores de edad que proporciona Facebook e Instagram, y las recomendaciones que le brinda a los padres respecto a las dudas que tengan con las cuentas de los niños, WhatsApp no enfatiza de manera profunda sobre la seguridad que le brinda a este cuando tiene una cuenta en esta red social, mientras que Facebook e Instagram cumple

con políticas y recomendaciones seguras que evidencian el trabajo que hacen para evitar que los chicos se vean involucrados en casos de grooming.

- Se realizo un análisis para identificar el rango de edades de los niños y adolescentes que se han visto expuestos en las trampas de la ingeniería social logrando identificar que el 52,9% de los menores afectados por grooming oscilan entre 11 y 15 años, el 33,7% tienen entre 7 y 10, el 10,2% tienen entre 16 y 18 y el 3,2% tienen entre 3 y 7.

- Se recomendaron procesos y métodos que le permiten a los padres, a la comunidad en general y a los niños poner en práctica diferentes métodos que eviten mitigar y reducir el impacto que causa el grooming en los menores de edad como por ejemplo, los padres deben explicar a los niños las ventajas, las desventajas y los peligros que presentan el uso de la internet y de las redes sociales, establecer normas y tiempo para navegar en internet y hacer un buen uso de las redes sociales, se deben crear redes de apoyo entre los padres y los educadores para realizar campañas en contra del grooming, cambiar contraseñas periódicamente tanto de redes sociales como de wifi, utilizar programas de protección como antivirus y firewall, limitar el acceso de internet, desactivar la cámara web, monitorear constantemente a los niños cuando están navegando.

8. RECOMENDACIONES

- Se recomienda a la gobernación y a las administraciones municipales encomendar a las direcciones de informática y a las secretarias de las TIC, desarrollar programas de prevención en los colegios para socializar los métodos de la ingeniería social que se utilizan para hacer grooming y los diferentes delitos informáticos que afectan a los menores de edad en Colombia.

- Se recomienda crear grupos de apoyo entre los padres, alumnos y colegios que se encarguen de hacer campañas de prevención en contra del grooming, que permitan evitar y mitigar los riesgos a los que se ven expuestos los menores de edad de Colombia.

- Se recomienda que los niños menores de 13 años no tengan redes sociales y si las tienen que sean supervisadas por adultos responsables el 100% del tiempo durante el que ellos naveguen por él ciberespacio.

- Se recomienda a los padres y tutores ejecutar un rol activo en el aprendizaje y uso de las herramientas tecnológicas y redes sociales de los menores de edad.

- Se recomienda tener en cuenta los métodos que se administraron en la monografía para hacer un buen uso de las redes sociales y evitar que los menores de edad caigan en las redes del grooming.

9. BIBLIOGRAFIA

- ABC, familia. Qué es el «grooming» y por qué ha aumentado un 410% en los últimos años [en línea]. ABC. España, marzo 10 de 2019. [Consultado: 16 de septiembre de 2020]. Disponible en: http://uao.libguides.com/c.php?g=529834&p=3623716#Periodico

- ALONZO GONZALES, Patricia. Online Grooming [en línea]. Trabajo de investigación Ciencias Humanas y Sociales. Madrid España. Comillas Universidad Pontificia. Facultad Ciencias Humanas y Sociales. 2019. 34 p. [Consultado: 26/03/2020]. Disponible en: https://repositorio.comillas.edu/xmlui/bitstream/handle/11531/30848/TFG%20Alonso%20Gonzalez%2C%20Patricia.pdf?sequence=1&isAllowed=y

- CANAL 13. Grooming, así opera en internet [en línea]. Bogotá. Redacción canal 13. 26 junio 2018. [Consultado: 05 de marzo de 2020]. Disponible en internet: https://canaltrece.com.co/noticias/grooming-que-es-etapas-y-caracteristicas/

- CENTRO CIBERNÉTICO DE LA POLICÍA NACIONAL. Denuncias en el Centro Cibernético de la Policía Nacional [sitio web]. Policía Nacional. Bogotá D.C. 2020. [Consultado: 02/04/2020]. Disponible en: https://caivirtual.policia.gov.co/

- CERT Andalucía. Informe de divulgación Phishing [en línea]. Centro Andaluza para el Desarrollo de las Telecomunicaciones. CONSEJERIA DE EMPLEO. EMPRESA Y COMERCIO. 06 de noviembre de 2017. 22 p. [Consultado: 01 de marzo de 2020]. Disponible en internet: https://www.seguridad.andaluciaesdigital.es/documents/410971/1437699/phising+2017/01950ce7-731f-48a6-821a-79388e571bff

- CNN.1 de 4 jóvenes dice que ha hecho 'sexting', según un estudio [en línea]. En CNN, febrero 28 de 2018. [Consultado: 16 de septiembre de 2020]. Disponible en: https://cnnespanol.cnn.com/2018/02/28/1-de-4-jovenes-dice-que-ha-hecho-sexting-segun-un-estudio/

- COLOMBIA. CONGRESO DE LA REPÚBLICA. 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]. Bogotá, D.C. Ministerio de Tecnologías de la Información y las Comunicaciones. 4 p. [Consultado: 26 de septiembre de 2019]. Disponible en: https://www.mintic.gov.co/portal/inicio/3705:Ley-1273-de-2009

- COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 679 de 2001, Por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución. [en línea]. Bogotá, D.C. Unidad para la atención y reparación integral de las víctimas. 11 p. [Consultado: 26 de septiembre de 2019]. Disponible en: https://www.unidadvictimas.gov.co/es/ley-679-de-2001/13668

- CONTIGO CONECTADOS. REDES SOCIALES MAS USADAS POR LOS NIÑOS En: Tigo. [Consultado: 12/03/2020]. Disponible en: https://contigoconectados.com/resultados/descargables/

- CONTIGO CONECTADOS. Riesgos y potencialidades del uso de las Tecnologías de la Información y la Comunicación [Sitio Web] Bogotá D.C Universidad EAFIT. Departamento de Comunicación, Escuela de Humanidades. Tigo Une. [Consultado: 22/03/2020]. Disponible en: https://contigoconectados.com/resultados/descargables/

- DIAZ CORTES, Lina Mariola, Cuaderno Red de Cátedras Telefónica: Algunas consideraciones sobre el meeting a child following sexual grooming through tics (contacto Tics preordenado a la actividad sexual con menores) [en línea]. España. Telefónica. Universidad de Salamanca. Mayo 2011. 28 p. [Consultado: 14 de febrero de 2020]. Disponible en internet: http://catedraseguridad.usal.es/sites/default/files/Cuaderno_02_Contacto_TICS_preordenado_act_sexual_con_menores.pdf

- EN TIC CONFÍO. Tres casos de Grooming en Colombia. Ministerio de las TIC [sitio web]. 16 de febrero 2016 [Consultado: 14 de febrero de 2020]. Disponible en internet: https://www.enticconfio.gov.co/tres-casos-grooming-colombia

- ESCUDOS DEL ALMA. Te Protejo. [sitio web] Red Papaz. Bogotá. [Consultado: 06 de marzo de 2020]. Disponible en internet: http://www.redpapaz.org/escudos/index.php?option=com_k2&view=item&id=478:te-protejo&Itemid=104

- FACEBOOK. Normas comunitarias para proteger menores de edad [sitio web]. California. 2020. [Consultado: 13/03/2020]. Disponible en: https://es-es.facebook.com/communitystandards/child_nudity_sexual_exploitation

- FACEBOOK. Portal para padres [sitio web]. California [Consultado: 17 de abril de 2020]. Disponible en: https://es-la.facebook.com/safety/parents

- FACEBOOK. Tus compromisos con Facebook y nuestra comunidad [sitio web]. California. 31 de julio de 2019. [Consultado: 17 de abril de 2020]. Disponible en: https://es-es.facebook.com/legal/terms

- FERNANDEZ, Manuel. Ingeniería Social: ¿qué es el Tailgating (o «ir a rebufo»)? [blog]. Bélgica. 11 de septiembre 2018. [Consultado: 03 de marzo

de 2020]. Disponible en: https://blog.mailfence.com/es/que-es-el-tailgating/#pll_switcher

- GARCÍA GACHÓN, Jonathan Orlando. TFM, Ad hoc Seguridad y Riesgos: Ciberbullyng, Grooming y Sexting [en línea]. Trabajo Final de Master MISTIC Estudios de Informática Multimedia y Telecomunicaciones. España. Universidad Oberta de Cataluña, Universidad Autónoma de Barcelona, Universitat Rovira I Virgili, Universitat de les Illes Balears. 2017. 56 p. [Consultado: 02 de mayo de 2020]. Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/72526/6/ingjonathangarciaTFM0118memoria.pdf

- GARCIA TORO, Carlos Mario, GONZALEZ PUENTES José Luis, y MENDOZA CARVAJAL Rafael Eduardo, Caracterización de los factores psicosociales asociados al Grooming en Colombia [en línea]. Administración Policial. Bogotá D.C. Escuela de Cadetes de Policía General Francisco de Paula Santander. Pregrado en Administración Policial. 2017. 35 p. [Consultado: 14 de febrero de 2020]. Disponible en internet: http://biblioteca.policia.edu.co:8080/bitstream/handle/123456789/1220/3017GARCIA.pdf?sequence=1&isAllowed=y

- GARCIA, Beatriz Catalina. Los padres ante el uso de Internet y redes sociales por menores. Control y protección [en línea]. España. Revista Latina. Universidad de La Laguna. Diciembre 2013. 17 p. [Consultado el 19 de abril de 2020]. Disponible en: http://www.revistalatinacs.org/13SLCS/2013_actas/077_Catalina.pdf

- GARCIA, Polkan. Los niños y jóvenes colombianos usan internet tres horas y media al día [en línea]. En. La República. Bogotá D.C. 4 de agosto 2018. [Consultado: 01 de abril de 2020]. Disponible en: https://www.larepublica.co/internet-economy/los-ninos-y-jovenes-colombianos-usan-internet-tres-horas-y-media-al-dia-2756640

- GARMENDIA, M. JIMÉNEZ, E., CASADO, M.A. y MASCHERONI, G. Net Children Go Mobile: Riesgos y oportunidades en internet y el uso de dispositivos móviles entre menores españoles (2010-2015) [en línea] Madrid España. Universidad del País Vasco. Citado por. VILLANUEVA BLASCO Víctor José. SERRANO BERNAL, Sara. Patrón de uso de internet y control parental de redes sociales como predictor de sexting en adolescentes: una perspectiva de género [en línea]. Consejo General de la Psicología. 2019 17 p. [Consultado: 26/03/2020]. Disponible en:

http://eds.b.ebscohost.com.bibliotecavirtual.unad.edu.co/eds/pdfviewer/pdfviewer?vid=4&sid=0d4399a9-20c4-40fc-a61d-5a458c2ebb47%40sessionmgr103

- HÜTT HERRERA, Harold. Las redes sociales: una nueva herramienta de difusión [en línea]. Reflexiones. San José, Costa Rica. Universidad de Costa Rica. 2012. Vol. 91, núm. 2. 9 p. [Consultado el 30 de septiembre de 2019]. Disponible en: https://www.redalyc.org/pdf/729/72923962008.pdf

- INSTAGRAM. Centro de seguridad y privacidad, Consejos para los padres [sitio web]. California. 2020. [Consultado: 17 de abril de 2020]. Disponible en: https://es-la.facebook.com/help/instagram/154475974694511/?helpref=hc_fnav&bc[0]=Ayuda%20de%20Instagram&bc[1]=Centro%20de%20privacidad%20y%20seguridad

- INTECO. Guía de actuación contra el ciberacoso padres y educadores [en línea]. Instituto Nacional de las Tecnologías de la comunicación. Ministerio de Industria Tecnología y Comercio. Octubre 2012. p 15. [Consultado: 02 de mayo de 2020]. Disponible en internet:

https://www.alcobendas.org/recursos/doc/Educacion/539233046_42201383324.pdf

- INTECO. Guía s.o.s contra el grooming padres y educadores [en línea]. Instituto Nacional de las Tecnologías de la comunicación. Ministerio de Industria Tecnología y Comercio. España. p 8. [Consultado: 20 de abril de 2020]. Disponible en internet: https://www.adolescenciasema.org/usuario/documentos/sos_grooming.pdf

- JUSTICIA, Casi 4 denuncias al día se reciben por casos de explotación de menores [en línea]. En. El tiempo. Bogotá D.C. septiembre 23 de 2019 [Consultado: 26 de septiembre de 2019]. Disponible en Internet: https://www.eltiempo.com/justicia/delitos/claves-que-pedofilos-usan-para-ocultar-pornografia-infantil-en-internet-414560

- MEJIA LLANO, Juan Carlos. Estadísticas de redes sociales 2020: usuarios de Facebook, Instagram, YouTube, LinkedIn, Twitter, TikTok y otros [en línea]. Marketing Digital. (febrero 26 de 2020). [Consultado: 26 de abril de 2020]. Disponible en: https://www.juancmejia.com/marketing-

digital/estadisticas-de-redes-sociales-usuarios-de-facebook-instagram-linkedin-twitter-whatsapp-y-otros-infografia/#2_Usuarios_activos_de_Instagram

- MEXIA, Marcela. 7 datos de Facebook para el 2020 [en línea]. En: EL IMPARCIAL. México enero 07 del 2020. [Consultado: 20 de septiembre de 2019]. Disponible en: https://www.elimparcial.com/tijuana/columnas/7-datos-de-Facebook-para-el-2020-20200107-0010.html

- MIN TIC. Colombia es uno de los países con más usuarios en redes sociales en la región. [Sitio web]. Bogotá D.C. 26 diciembre de 2019. [Consultado el 12 de marzo del 2019]. Disponible en: https://www.mintic.gov.co/portal/inicio/Sala-de-Prensa/Sabia-Ud-que/2713:Colombia-es-uno-de-los-paises-con-mas-usuarios-en-redes-sociales-en-la-region

- MIN TIC. Glosario [en línea]. Bogotá, Colombia. [Consultado: 28 de abril de 2020]. Disponible en: https://www.mintic.gov.co/portal/inicio/Glosario/

- MOLANO TORRES, Natalia. Colombia es el tercer país con más ataques de ingeniería social en América Latina [en línea]. En LA REPUBLICA. Bogotá D.C. marzo 10 de 2019. [Consultado: 16 de septiembre de 2020]. Disponible en: https://www.larepublica.co/empresas/colombia-es-el-tercer-pais-con-mas-ataques-de-ingenieria-social-en-america-latina-2928973

- ONA SYSTEMS, Glosario de tecnología Ona Systems [en línea]. Bogotá, Colombia. 12 p. [Consultado: 28 de abril de 2020]. Disponible en: https://www.onasystems.net/wp-content/uploads/2016/10/Glosario-seguridad-Ona-systems-2016.pdf

- PALMER PADILLA, Fco Javier. Seguridad En Riesgos, Ciberbullyng, Grooming Y Sexting [En Línea]. Trabajo De Investigación De Máster En Seguridad Informática. España. Universidad Oberta De Cataluña. Facultad De Ciencias Básicas. Departamento De Ingeniera De Sistemas. 2017. 27 p. [Consultado: 08 De marzo Del 2020]. Disponible En Internet: Http://Openaccess.Uoc.Edu/Webapps/O2/Bitstream/10609/67105/6/Fpalmerptfm0617memoria.Pdf

- PIÑEROS OSPINA, Carolina. Logros durante el 2019 En: TE PROTEJO. [Consultado: 08/03/2020]. Disponible en: https://teprotejo.org/que-es-te-protejo/informes-de-operaciones/

- POLICÍA NACIONAL, FISCALÍA NACIONAL. Sistema Nacional de Denuncia Virtual ¡A Denunciar! [en línea]: Policía Nacional. Bogotá. 2020. [Consultado: 02/04/2020]. Disponible en: https://adenunciar.policia.gov.co/adenunciar/default.aspx

- RED.ES, SEMA. Guía clínica de ciberacoso para profesionales de la salud. Plan de confianza del ámbito digital del Ministerio de Industria, Energía y Turismo. Hospital Universitario La Paz, Sociedad Española de Medicina del Adolescente, Red.es. Madrid. 2015. 128 p. [Consultado el 17 de abril de 2020]. Disponible en: https://www.observatoriodelainfancia.es/ficherosoia/documentos/4514_d_Guia_Ciberacoso_Profesionales_Salud_FBlanco.pdf

- ROBAYNA PERERA, Margarita Rosa. Pederastia y pedofilia: estado de la cuestión [en línea]. Agosto, 13, 2012. 14 p. [Consultado: 26 de septiembre de

2019]. Disponible en Internet: http://www.pensamientopenal.com.ar/system/files/2014/12/doctrina38697.pdf

- RODRIGUEZ RINCON, Ellien Yulieth. Metodologías de la ingeniería social. [en línea]. Trabajo de investigación Magister Universitario en las Seguridad de las TIC. Madrid España Universidad Oberta de Cataluña. Junio 2018. 65 p. [Consultado: 01 de marzo de 2020]. Disponible en internet: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/81255/6/jrodriguezrinTFM0618memoria.pdf

- ROMERO, Diego. El arte de la ingeniería social [en línea]. Especialización de Seguridad Informática. Bogotá D.C. Universidad Piloto de Colombia. [Consultado: 23 de febrero de 2020]. Disponible en Internet: 10 p. http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6354/El%20arte%20de%20la%20ingenier%c3%ada%20social.pdf?sequence=1&isAllowed=y

- TE PROTEJO. Informe de operaciones [sitio web]. Bogotá D.C. 2019. [Consultado: 06/03/2020]. Disponible en: https://teprotejo.org/que-es-te-protejo/informes-de-operaciones

- UNICEF, Colombia. Colombia se suma a los esfuerzos internacionales. Colombia se suma a los esfuerzos internacionales para proteger a niñas, niños y adolescentes frente a la explotación y abuso sexual en línea [sitio web]. Colombia. 2017. [Consultado: 16 de abril de 2020]. Disponible en: https://www.unicef.org/colombia/comunicados-prensa/colombia-se-suma-los-esfuerzos-internacionales

- WHATSAPP. Información legal de WhatsApp [sitio web]. California. 2020. [Consultado: 19 de mayo de 2020]. Disponible en: https://www.whatsapp.com/legal/?lang=es#key-updates

10. ANEXOS

Anexo A Formato RAE

Fecha de Realización: 6/02/2020
Título: Métodos de ingeniería social, utilizados por los pederastas para cometer grooming en Colombia
Autor: CLAVIJO CASTAÑEDA, Maria Camila
Palabras Claves: Ingeniería social, cibercrimen, ciberacoso, grooming, pornografía infantil.
Descripción: La presente monografía se realiza con el objetivo de presentarse como trabajo de grado para obtener el título como especialista en seguridad informática.
Fuentes: ➢ ABC, familia. Qué es el «grooming» y por qué ha aumentado un 410% en los últimos años [en línea]. ABC. España, marzo 10 de 2019. [Consultado: 16 de septiembre de 2020]. Disponible en: http://uao.libguides.com/c.php?g=529834&p=3623716#Periodico ➢ ALONZO GONZALES, Patricia. Online Grooming [en línea]. Trabajo de investigación Ciencias Humanas y Sociales. Madrid España. Comillas

Universidad Pontificia. Facultad Ciencias Humanas y Sociales. 2019. 16 p. [Consultado: 26/03/2020]. Disponible en: https://repositorio.comillas.edu/xmlui/bitstream/handle/11531/30848/TFG%20Alonso%20Gonzalez%2C%20Patricia.pdf?sequence=1&isAllowed=y

- CANAL 13. Grooming, así opera en internet [en línea]. Bogotá. Redacción canal 13. 26 junio 2018. [Consultado: 05 de marzo de 2020]. Disponible en internet: https://canaltrece.com.co/noticias/grooming-que-es-etapas-y-caracteristicas/

- CENTRO CIBERNÉTICO DE LA POLICÍA NACIONAL. Denuncias en el Centro Cibernético de la Policía Nacional [sitio web]. Policía Nacional. Bogotá D.C. 2020. [Consultado: 02/04/2020]. Disponible en: https://caivirtual.policia.gov.co/

- CERT Andalucía. Informe de divulgación Phishing [en línea]. Centro Andaluza para el Desarrollo de las Telecomunicaciones. CONSEJERIA DE EMPLEO. EMPRESA Y COMERCIO. 06 de noviembre de 2017. 22 p. [Consultado: 01 de marzo de 2020]. Disponible en internet: https://www.seguridad.andaluciaesdigital.es/documents/410971/1437699/phising+2017/01950ce7-731f-48a6-821a-79388e571bff

- COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 679 de 2001, Por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución. [en línea]. Bogotá, D.C. Unidad para la atención y reparación integral de las víctimas. p 1,7. [Consultado: 26 de septiembre de 2019]. Disponible en: https://www.unidadvictimas.gov.co/es/ley-679-de-2001/13668

- COLOMBIA. CONGRESO DE LA REPÚBLICA. 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]. Bogotá, D.C. Ministerio de Tecnologías de la Información y las Comunicaciones. p 1,2. [Consultado: 26 de septiembre de 2019]. Disponible en: https://www.mintic.gov.co/portal/inicio/3705:Ley-1273-de-2009

- CONTIGO CONECTADOS. Riesgos y potencialidades del uso de las Tecnologías de la Información y la Comunicación [Sitio Web] Bogotá D.C Universidad EAFIT. Departamento de Comunicación, Escuela de

Humanidades. Tigo Une. [Consultado: 22/03/2020]. Disponible en: https://contigoconectados.com/resultados/descargables/

- CONTIGO CONECTADOS. REDES SOCIALES MAS USADAS POR LOS NIÑOS En: Tigo. [Consultado: 12/03/2020]. Disponible en: https://contigoconectados.com/resultados/descargables/

- CNN.1 de 4 jóvenes dice que ha hecho 'sexting', según un estudio [en línea]. En CNN, febrero 28 de 2018. [Consultado: 16 de septiembre de 2020]. Disponible en: https://cnnespanol.cnn.com/2018/02/28/1-de-4-jovenes-dice-que-ha-hecho-sexting-segun-un-estudio/

- DIAZ CORTES, Lina Mariola, Cuaderno Red de Cátedras Telefónica: Algunas consideraciones sobre el meeting a child following sexual grooming through tics (contacto Tics preordenado a la actividad sexual con menores) [en línea]. España. Telefónica. Universidad de Salamanca. Mayo 2011. [Consultado: 14 de febrero de 2020]. Disponible en internet: http://catedraseguridad.usal.es/sites/default/files/Cuaderno_02_Contacto_TICS_preordenado_act_sexual_con_menores.pdf

- ESCUDOS DEL ALMA. Te Protejo. [sitio web] Red Papaz. Bogotá. [Consultado: 06 de marzo de 2020]. Disponible en internet:

http://www.redpapaz.org/escudos/index.php?option=com_k2&view=item&id=478:te-protejo&Itemid=104

- EN TIC CONFÍO. Tres casos de Grooming en Colombia. Ministerio de las TIC [sitio web]. 16 de febrero 2016 [Consultado: 14 de febrero de 2020]. Disponible en internet: https://www.enticconfio.gov.co/tres-casos-grooming-colombia

- FACEBOOK. Tus compromisos con Facebook y nuestra comunidad [sitio web]. California. 31 de julio de 2019. [Consultado: 17 de abril de 2020]. Disponible en: https://es-es.facebook.com/legal/terms

- FACEBOOK. Normas comunitarias para proteger menores de edad [sitio web]. California. 2020. [Consultado: 13/03/2020]. Disponible en: https://es-es.facebook.com/communitystandards/child_nudity_sexual_exploitation

- FACEBOOK. Portal para padres [sitio web]. California [Consultado: 17 de abril de 2020]. Disponible en: https://es-la.facebook.com/safety/parents

- FERNANDEZ, Manuel. Ingeniería Social: ¿qué es el Tailgating (o «ir a rebufo»)? [blog]. Bélgica. 11 de septiembre 2018. [Consultado: 03 de

marzo de 2020]. Disponible en: https://blog.mailfence.com/es/que-es-el-tailgating/#pll_switcher

- GARCIA, Beatriz Catalina. Los padres ante el uso de Internet y redes sociales por menores. Control y protección [en línea]. España. Revista Latina. Universidad de La Laguna. Diciembre 2013. [Consultado el 19 de abril de 2020]. Disponible en: http://www.revistalatinacs.org/13SLCS/2013_actas/077_Catalina.pdf

- GARCÍA GACHÓN, Jonathan Orlando. TFM, Ad hoc Seguridad y Riesgos: Cyberbullyng, Grooming y Sexting [en línea]. Trabajo Final de Master MISTIC Estudios de Informática Multimedia y Telecomunicaciones. España. Universidad Oberta de Cataluña, Universidad Autónoma de Barcelona, Universitat Rovira I Virgili, Universitat de les Illes Balears. 2017. 41 p. [Consultado: 02 de mayo de 2020]. Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/72526/6/ingjonathangarciaTFM0118memoria.pdf

- GARCIA, Polkan. Los niños y jóvenes colombianos usan internet tres horas y media al día [en línea]. En. La República. Bogotá D.C. 4 de agosto 2018. [Consultado: 01 de abril de 2020]. Disponible en:

https://www.larepublica.co/internet-economy/los-ninos-y-jovenes-colombianos-usan-internet-tres-horas-y-media-al-dia-2756640

- GARCIA TORO, Carlos Mario, GONZALEZ PUENTES José Luis, y MENDOZA CARVAJAL Rafael Eduardo, Caracterización de los factores psicosociales asociados al Grooming en Colombia [en línea]. Administración Policial. Bogotá D.C. Escuela de Cadetes de Policía General Francisco de Paula Santander. Pregrado en Administración Policial. 2017. 35 p. [Consultado: 14 de febrero de 2020]. Disponible en internet: http://biblioteca.policia.edu.co:8080/bitstream/handle/123456789/1220/3017GARCIA.pdf?sequence=1&isAllowed=y

- GARMENDIA, M. JIMÉNEZ, E., CASADO, M.A. y MASCHERONI, G. Net Children Go Mobile: Riesgos y oportunidades en internet y el uso de dispositivos móviles entre menores españoles (2010-2015) [en línea] Madrid España. Universidad del País Vasco. Citado por. VILLANUEVA BLASCO Víctor José. SERRANO BERNAL, Sara. Patrón de uso de internet y control parental de redes sociales como predictor de sexting en adolescentes: una perspectiva de género [en línea]. Consejo General de la Psicología. 2019 17 p. [Consultado: 26/03/2020]. Disponible en: http://eds.b.ebscohost.com.bibliotecavirtual.unad.edu.co/eds/pdfviewer/pd

fviewer?vid=4&sid=0d4399a9-20c4-40fc-a61d-5a458c2ebb47%40sessionmgr103

- HÜTT HERRERA, Harold. Las redes sociales: una nueva herramienta de difusión [en línea]. Reflexiones. San José, Costa Rica. Universidad de Costa Rica. 2012. Vol. 91, núm. 2. [Consultado el 30 de septiembre de 2019]. Disponible en: https://www.redalyc.org/pdf/729/72923962008.pdf

- INSTAGRAM. Centro de seguridad y privacidad, Consejos para los padres [sitio web]. California. 2020. [Consultado: 17 de abril de 2020]. Disponible en: https://es-la.facebook.com/help/instagram/154475974694511/?helpref=hc_fnav&bc[0]=Ayuda%20de%20Instagram&bc[1]=Centro%20de%20privacidad%20y%20seguridad

- INTECO. Guía de actuación contra el ciberacoso padres y educadores [en línea]. Instituto Nacional de las Tecnologías de la comunicación. Ministerio de Industria Tecnología y Comercio. Octubre 2012. p 15. [Consultado: 02 de mayo de 2020]. Disponible en internet: https://www.alcobendas.org/recursos/doc/Educacion/539233046_42201383324.pdf

- INTECO. Guía s.o.s contra el grooming padres y educadores [en línea]. Instituto Nacional de las Tecnologías de la comunicación. Ministerio de Industria Tecnología y Comercio. España. p 8. [Consultado: 20 de abril de 2020]. Disponible en internet: https://www.adolescenciasema.org/usuario/documentos/sos_grooming.pdf

- JUSTICIA, Casi 4 denuncias al día se reciben por casos de explotación de menores [en línea]. En. El tiempo. Bogotá D.C. septiembre 23 de 2019 [Consultado: 26 de septiembre de 2019]. Disponible en Internet: https://www.eltiempo.com/justicia/delitos/claves-que-pedofilos-usan-para-ocultar-pornografia-infantil-en-internet-414560

- MEJIA LLANO, Juan Carlos. Estadísticas de redes sociales 2020: usuarios de Facebook, Instagram, YouTube, LinkedIn, Twitter, TikTok y otros [en línea]. Marketing Digital. (febrero 26 de 2020). [Consultado: 26 de abril de 2020]. Disponible en: https://www.juancmejia.com/marketing-digital/estadisticas-de-redes-sociales-usuarios-de-facebook-instagram-linkedin-twitter-whatsapp-y-otros-infografia/#2_Usuarios_activos_de_Instagram

- MEXIA, Marcela. 7 datos de Facebook para el 2020 [en línea]. En: EL IMPARCIAL. México enero 07 del 2020. [Consultado: 20 de septiembre de 2019]. Disponible en: https://www.elimparcial.com/tijuana/columnas/7-datos-de-Facebook-para-el-2020-20200107-0010.html

- MIN TIC. Glosario [en línea]. Bogotá, Colombia. [Consultado: 28 de abril de 2020]. Disponible en: https://www.mintic.gov.co/portal/inicio/Glosario/

- MIN TIC. Colombia es uno de los países con más usuarios en redes sociales en la región. [Sitio web]. Bogotá D.C. 26 diciembre de 2019. [Consultado el 12 de marzo del 2019]. Disponible en: https://www.mintic.gov.co/portal/inicio/Sala-de-Prensa/Sabia-Ud-que/2713:Colombia-es-uno-de-los-paises-con-mas-usuarios-en-redes-sociales-en-la-region

- MOLANO TORRES, Natalia. Colombia es el tercer país con más ataques de ingeniería social en América Latina [en línea]. En LA REPUBLICA. Bogotá D.C. marzo 10 de 2019. [Consultado: 16 de septiembre de 2020]. Disponible en: https://www.larepublica.co/empresas/colombia-es-el-tercer-pais-con-mas-ataques-de-ingenieria-social-en-america-latina-2928973

- ONA SYSTEMS, Glosario de tecnología Ona Systems [en línea]. Bogotá, Colombia. [Consultado: 28 de abril de 2020]. Disponible en: https://www.onasystems.net/wp-content/uploads/2016/10/Glosario-seguridad-Ona-systems-2016.pdf

- PALMER PADILLA, Fco Javier. Seguridad En Riesgos, Ciberbullyng, Grooming Y Sexting [En Línea]. Trabajo De Investigación De Máster En Seguridad Informática. España. Universidad Oberta De Cataluña. Facultad De Ciencias Básicas. Departamento De Ingeniera De Sistemas. 2017. 27 p. [Consultado: 08 De marzo Del 2020]. Disponible En Internet: Http://Openaccess.Uoc.Edu/Webapps/O2/Bitstream/10609/67105/6/Fpalmerptfm0617memoria.Pdf

- PIÑEROS OSPINA, Carolina. Logros durante el 2019 En: TE PROTEJO. [Consultado: 08/03/2020]. Disponible en: https://teprotejo.org/que-es-te-protejo/informes-de-operaciones/

- POLICÍA NACIONAL, FISCALÍA NACIONAL. Sistema Nacional de Denuncia Virtual ¡A Denunciar! [en línea]: Policía Nacional. Bogotá. 2020. [Consultado: 02/04/2020]. Disponible en: https://adenunciar.policia.gov.co/adenunciar/default.aspx

- RED.ES, SEMA. Guía clínica de ciberacoso para profesionales de la salud. Plan de confianza del ámbito digital del Ministerio de Industria, Energía y Turismo. Hospital Universitario La Paz, Sociedad Española de Medicina del Adolescente, Red.es. Madrid. 2015. 6 p. [Consultado el 17 de abril de 2020]. Disponible en: https://www.observatoriodelainfancia.es/ficherosoia/documentos/4514_d_Guia_Ciberacoso_Profesionales_Salud_FBlanco.pdf

- ROBAYNA PERERA, Margarita Rosa. Pederastia y pedofilia: estado de la cuestión [en línea]. Agosto, 13, 2012. 1 p. [Consultado: 26 de septiembre de 2019]. Disponible en Internet: http://www.pensamientopenal.com.ar/system/files/2014/12/doctrina38697.pdf

- RODRIGUEZ RINCON, Ellien Yulieth. Metodologías de la ingeniería social. [en línea]. Trabajo de investigación Magister Universitario en las Seguridad de las TIC. Madrid España Universidad Oberta de Cataluña. Junio 2018. 17 p. [Consultado: 01 de marzo de 2020]. Disponible en internet: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/81255/6/jrodriguezrinTFM0618memoria.pdf

- ROMERO, Diego. El arte de la ingeniería social [en línea]. Especialización de Seguridad Informática. Bogotá D.C. Universidad Piloto de Colombia. [Consultado: 23 de febrero de 2020]. Disponible en Internet: 2 p. http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6354/El%20arte%20de%20la%20ingenier%c3%ada%20social.pdf?sequence=1&isAllowed=y

- UNICEF, Colombia. Colombia se suma a los esfuerzos internacionales. Colombia se suma a los esfuerzos internacionales para proteger a niñas, niños y adolescentes frente a la explotación y abuso sexual en línea [sitio web]. Colombia. 2017. [Consultado: 16 de abril de 2020]. Disponible en: https://www.unicef.org/colombia/comunicados-prensa/colombia-se-suma-los-esfuerzos-internacionales

- TE PROTEJO. Informe de operaciones [sitio web]. Bogotá D.C. 2019. [Consultado: 06/03/2020]. Disponible en: https://teprotejo.org/que-es-te-protejo/informes-de-operaciones

- WHATSAPP. Información legal de WhatsApp [sitio web]. California. 2020. [Consultado: 19 de mayo de 2020]. Disponible en: https://www.whatsapp.com/legal/?lang=es#key-updates

Contenido del documento:

En esta monografía se reconocieron los distintos métodos de la ingeniería social, que son utilizados por los delincuentes informáticos los cuales hacen uso de redes sociales para contactar a menores de edad por medio de engaños. El actual documento permitió al lector conocer los principales objetivos del porque un ciber acosador, (pederasta), quiere acceder y ganarse la confianza de un menor de edad o adolescente para posteriormente obtener beneficios sexuales, (fotos y videos donde se puede observar al menor de edad desnudo o mostrando sus partes íntimas, lo cual puede ser utilizado por el acosador como material pornográfico para distribuir y vender, puede presentarse, encuentros sexuales entre la víctima y el acosador, chantajes hacia la víctima y a sus padres para no revelar el material que se tiene de la víctima por parte del acosador, con el fin de obtener dinero) beneficios monetarios, introducir a la víctima al mundo de la pornografía infantil, para que creen material sexual, o para la prostitución infantil, se pudieron observar los métodos más comunes que utilizan para ganarse la confianza de la población infantil y posteriormente identificar las consecuencias negativas que trae consigo dichos actos.

También se pudo observar el perfil criminológico de los delincuentes informáticos, que utilizan la ingeniería social para tener contacto con la población infantil, y se pretende finalizar con un análisis e implementación de técnicas que podrán mitigar o evitar que se presente dicho problema, se pueden encontrar las cifras de las diferentes denuncias que tienen que ver con el grooming en Colombia, se pueden observar las diferentes plataformas que están disponibles para realizar las denuncias de los menores víctimas del grooming, se puede identificar el rango de edades de los menores que han sido víctimas de los diferentes delitos informaticos, y para finalizar se pueden observar los diferentes métodos que se pueden ejecutar para evitar caer en las redes de los pederastas que hacen grooming en Colombia.

Metodología: Cuantitativa

Conceptos nuevos: Te Protejo, Red PaPaz, Centro cibernético, Policía Nacional.

Conclusiones:

- Durante el desarrollo de la monografía se logró identificar que la ingeniería social consiste en manipular de forma psicológica, de manera presencial o utilizando elementos de telecomunicación, con el objetivo de obtener

información importante de una persona, empresa u organización, el resultado de esa información el delincuente la utilizara en este caso específico del grooming para acosar, extorsionar, o lograr cuadrar encuentros personales que serán utilizados para cometer actos sexuales con los menores de edad.

- Se logro obtener como resultado la identificación de los diferentes métodos que utiliza la ingeniería social para involucrarse con la población infantil, acto que ejecutan mediante técnicas y fases, las técnicas que utiliza el pederasta para hacer ingeniería social son pasivas (implementación de ingeniería social, observar, analizar el comportamiento de la víctima, establecer un perfil psicológico), técnicas presenciales no agresivas (resultados, seguir la víctima, vigilar la casa y empleo de la víctima, sus familiares y personas más cercanas, buscar información en su entorno), técnicas no presenciales (trata de obtener información de la víctima por medio de redes sociales, suplantación de identidad, solicitud de información por medio de correos electrónicos, llamadas, mensajes de texto) y técnicas agresivas (extorciones, presión física, presión psicológica, suplantación de identidad, abusos, chantajes, contacto sexual, acoso sexual), y las fases que ejecutan son: Fase 1 (consiste en buscar a la víctima), Fase 2 (Enganche), Fase 3 (Fidelización), Fase 4 (aislamiento), Fase 5 (seducción).

- Se logro identificar que el grooming es un método de la ingeniería social, el cual es utilizado por los pederastas para acercarse a los menores de edad principalmente por medio de redes sociales, quien se vale de diferentes métodos para lograr entablar una amistad con los niños, como lo son, suplantación de identidad, amabilidad, dar regalos costosos a estos, ganarse la confianza de la víctima, el victimario logra ser la persona más importante en la vida del niño, se convierte en alguien imprescindible, es decir en la persona más cercana a la víctima, para que no le cuente a nadie lo que está sucediendo realmente, todo esto lo hace el acosador con diferentes objetivos como hacer que el acosado le envié material sexual, fotos y videos personales con poses sexuales y mostrando las partes íntimas, las cuales serán utilizadas más adelante por el para acosar al niño y mantener encuentros sexuales con el menor, con el objetivo posteriormente de extorsionarlo a él y a los padres y obtener beneficios monetarios, también para vender el material sexual obtenido de parte del infante o para publicarlo en chats sexuales online, incluso él puede hacer grooming con el objetivo de secuestrar a los menores y venderlos para trata de blancas.

- Se lograron identificar los diferentes términos y los contrastes que existen entre la pedofilia, que es la inclinación de los adultos a sentir atracción sexual hacia los prepúberes, el pedófilo que es el adulto que se interesa por sentir atracción sexual y amorosa por niños y niñas preadolescentes, la hebofilia que

es el adulto que se interesa por adolescentes, los cuales ya han tenido el despertar sexual, y el pederasta quien es el único que pasa a tener contacto físico con los menores de edad, a diferencia del pedófilo quien es el que solamente ve material sexual pero jamás toca a un chico.

- Se realizo una búsqueda del incremento de delitos sexuales infantiles del año al año 2019 obteniendo como resultado, que en el año 2015 se presentaron 518 denuncias teniendo un total del 10%, en el año 2016 se presentaron 866 teniendo un total de 17%, en el año 2017 se presentaron 132 teniendo un total 25%, en el año 2018 se presentaron 1323 teniendo un total 28%, en el año 2019 se presentaron 1038 teniendo un total 20% en comparación con los años anteriores, teniendo como resultado que en el año 2015 se presentaron menos casos y en el año 2018 fue el año donde se presentaron más casos.

- Se realizo una búsqueda de los delitos informaticos donde se ven involucrados menores de edad los cuales fueron reportados en el año 2019, donde se identificó que el grooming tuvo 202 casos reportados, la sextorsión 281, el ciberbullying 73, y la publicación de imágenes no autorizadas fueron 93.

- Se lograron identificar y describir en la monografía las leyes que penalizan los delitos sexuales que se tienen como resultado de practicar el grooming, dichas leyes son: Ley 1273 del 2009, la cual se encarga de castigar cualquier delito

informático en el territorio colombiano, y la Ley 679 de 2001 (agosto 3), la cual se encarga de prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores.

- Se logro identificar que existen plataformas creadas para reportar casos de prácticas de grooming y delitos informaticos como lo son el sexting, el acoso sexual cibernético, la extorsión, la suplantación de identidad, tales plataformas son Te Protejo que también funciona para descargar como APP en androide, la cual es creada por Red Papaz, y se encarga de recepcionar denuncias de delitos causados a menores de edad y canalizarlos con el centro cibernético de la policía nacional, o directamente con la policía nacional y la fiscalía que también ya cuentan con plataformas virtuales donde se pueden hacer este tipo de denuncias.

- Se realizo un análisis a los casos reportados por Te Protejo donde se hacen reportes acerca de material de abuso sexual (pornografía infantil), ciberacoso, contenidos inapropiados en medios de comunicación, los cuales están vinculados con el grooming, donde se obtuvieron las siguientes cifras: En el año 2012, 2.192 denuncias, dentro de las cuales, hay 462 que tienen que ver con contenidos sobre abuso sexual, explotación sexual, comercial y pornografía infantil, 145 sobre contenido inapropiado en medios de comunicación.

- En el año 2013 se evidencia el reporte de las denuncias que fueron recepcionadas, obteniendo como resultado 3.921 denuncias dentro de las cuales, hay 1.493 que tienen que ver con contenidos sobre abuso sexual, explotación sexual, comercial y pornografía infantil, y 263 sobre contenido inapropiado en medios de comunicación.

- En el año 2014 fueron recibidas un total de 6.452 denuncias, mientras que en la pornografía infantil se presentaron 3.724, 491 involucradas con ciberacoso, y 245 sobre contenido inapropiado en medios de comunicación.

- En el año 2015 fueron 8.706 denuncias, dentro de las cuales, hay 5.827 que tienen que ver con contenidos sobre abuso sexual, explotación sexual, comercial y pornografía infantil, 539 involucradas ciberacoso, y 175 sobre contenido inapropiado en medios de comunicación.

- En el año 2016 fueron 10.424 denuncias, dentro de las cuales, hay 7.416 que tienen que ver con contenidos sobre abuso sexual, explotación sexual, comercial y pornografía infantil, 724 involucradas con ciberacoso, y 264 sobre contenido inapropiado en medios de comunicación.

- En el año 2017 fueron 8.991 denuncias, dentro de las cuales, hay 5.187 que tienen que ver con contenidos sobre abuso sexual, explotación sexual, comercial y pornografía infantil, 724 involucradas con ciberacoso, y 264 sobre contenido inapropiado en medios de comunicación.

- Esto quiere decir que del año 2012 al año 2018 el caso más reportado, fue el Material de abuso sexual (Pornografía) con 32.288 casos, ocupando el 61% de porcentaje, mientras que el ciber acoso fue el segundo delito más reportado con 3.826, y el contenido inapropiado en medios de comunicación ocupo el último puesto con 1.499, dentro de las categorías que están implicadas con el grooming en el año 2019, nuevamente la categoría de material de abuso/explotación sexual (pornografía infantil) ocupo el 86%, esto quiere decir que aumentó un 25% en comparación con los anteriores años que ocuparon un rango de 61%, el ciberacoso obtuvo el 4.5% de rango, 2.5% menos reportes que los anteriores años, y sobre contenidos inapropiados en medio de comunicación ocuparon 1.1%, 1.9% menos que los anteriores años. Afortunadamente lo que fue ciberacoso y contenidos inapropiados en medio de comunicación disminuyeron, pero la categoría de material de abuso material de abuso/explotación sexual (pornografía infantil) como se mencionaba anteriormente aumento el 25%.

- Se logro identificar que Te Protejo durante el año 2019 logro bloquear 3.904 páginas web, ya que contenían abuso sexual y explotación infantil, de las cuales 2.955 URL fueron ingresadas a través de ICCAM-INHOPE, en las que se encontraron 6.694 imágenes de explotación infantil cuyo desmonte fue solicitado a la red INHOPE, y de las denuncias que canalizo Te Protejo al centro cibernético de la policía nacional fueron suspendidas 819 páginas con dominio, por contener material de abuso y explotación sexual.

- Se realizo un análisis de las redes sociales más comunes y que son más utilizadas por los menores de edad obteniendo como resultado que Facebook es utilizado en un total del 44%, WhatsApp el 31%, el 9%, Instagram el 8%, y You Tube el 8%, también se identificó en una encuesta realizada por Tigo Une que el 84% de los niños cuando usan internet destinan su tiempo a usar redes sociales, dentro de los análisis que se realizaron también se investigó el nivel de seguridad que utilizan las redes sociales para proteger a los niños, realizando una paralelo entre las políticas de seguridad de Facebook, WhatsApp e Instagram y se encontró lo siguiente:

  A comparación con las políticas de seguridad para menores de edad que proporciona Facebook e Instagram, y las recomendaciones que le brinda a los padres respecto a las dudas que tengan con las cuentas de los niños, WhatsApp no enfatiza de manera profunda sobre la seguridad que le brinda a este cuando tiene una cuenta en esta red social, mientras que Facebook e

Instagram cumple con políticas y recomendaciones seguras que evidencian el trabajo que hacen para evitar que los chicos se vean involucrados en casos de grooming.

- Se realizo un análisis para identificar el rango de edades de los niños y adolescentes que se han visto expuestos en las trampas de la ingeniería social logrando identificar que el 52,9% de los menores afectados por grooming oscilan entre 11 y 15 años, el 33,7% tienen entre 7 y 10 años, el 10,2% tienen entre 16 y 18 años y el 3,2% tienen entre 3 y 7 años.

- Se recomendaron procesos y métodos que le permiten a los padres, a la comunidad en general y a los niños poner en práctica diferentes métodos que eviten mitigar y reducir el impacto que causa el grooming en los menores de edad como por ejemplo, los padres deben explicar a los niños las ventajas, las desventajas y los peligros que presentan el uso de la internet y de las redes sociales, establecer normas y tiempo para navegar en internet y hacer un buen uso de las redes sociales, se deben crear redes de apoyo entre los padres y los educadores para realizar campañas en contra del grooming, cambiar contraseñas periódicamente tanto de redes sociales como de wifi, utilizar programas de protección como antivirus y firewall, limitar el acceso de internet,

desactivar la cámara web, monitorear constantemente a los niños cuando están navegando.
AUTOR: Maria Camila Clavijo Castañeda