View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Repositorio Institucional UNAD

MONOGRAFIA: INGENIERÍA SOCIAL UTILIZADA EN EL ABUSO DE INFANTES A TRAVÉS DE LAS REDES SOCIALES EN COLOMBIA.

IVONNE MILENA BARBOSA LÓPEZ
ANDRÉS EDUARDO OJEDA BARRERA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA.
BOGOTÁ
2018.

MONOGRAFIA: INGENIERÍA SOCIAL UTILIZADA EN EL ABUSO DE INFANTES A TRAVÉS DE LAS REDES SOCIALES EN COLOMBIA.

IVONNE MILENA BARBOSA LÓPEZ
ANDRÉS EDUARDO OJEDA BARRERA

Monografía

Director
Alexander Larrahondo Núñez

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA
ESPECIALIZACIÓN SEGURIDAD INFORMÁTICA.
BOGOTÁ
2018

CONTENIDO

pág.

CONTENIDO DE TABLAS.

Pag.

CONTENIDO DE IMÁGENES.

Pag.

INTRODUCCION

La globalización del internet y la llegada de este a los hogares hace que los niños tengan un acceso regular a este, al navegar sin la supervisión necesaria de los cuidadores, sin la seguridad ni protección ellos entran como en un vecindario cibernético donde acceden a muchos sitios y esto los hace vulnerables por su propia inocencia no tienen el sentido de desconfianza para detectar depredadores cibernéticos al igual que pasa en el mundo real con los delincuentes, por lo cual se decide desarrollar esta monografía de investigación sobre las diferentes técnicas de ingeniería social usadas por los ciber delincuentes en Colombia para lograr detectar las técnicas de ingeniera social aplicadas por los abusadores de menores entre los 8 y 13, como logran ganarse la confianza para cometer tales actos, por eso se usará la información bibliográfica de artículos académicos, entrevistas a los organismos encargados de atrapar estos delincuentes, documentando que se está haciendo en Colombia para evitar este delito, cuanto afecta a los infantes con el fin de poder determinar cómo contribuir a la protección de estos y dar posibles soluciones que contribuyan en pro de la protección de los niños del país.

1. DEFINICIÓN DEL PROBLEMA.

1.1. DESCRIPCIÓN DEL PROBLEMA.

A medida que el avance tecnológico se ha globalizado los niños han quedado expuestos a un sin número de peligros a través de la liberación informática, la presente investigación se enfocara en hacer un análisis relacionado con la problemática del uso de técnicas de ingeniería social para el abuso infantil en las redes en Colombia, para identificar que se está haciendo para controlar los contenidos y como se está protegiendo los niños de posibles casos de abusos, pornografía y demás temas que afecten los niños, se van a investigar las técnicas de ingeniería social sobre cómo estos ciber delincuentes logran ganarse la confianza de los menores para atacar, como por ejemplo: (Amat, 2016) Como es el caso de un niño de la edad de 9 años que conoció supuestamente una niña de 16 en internet y empezaron a chatear y le causo tanta confianza que le envió fotos privadas a la niña y ahí se desenmascaro el hombre adulto y empezó a chantajear el niño, para así encontrar posibles soluciones que contribuyan a la protección infantil.

1.2. FORMULACIÓN DEL PROBLEMA

¿COMO PUEDE LA SEGURIDAD INFORMATICA APORTAR A LA SEGURIDAD INFALTIL DE MENORES ENTRE 8 Y 13 AÑOS DE EDAD EN COLOMBIA?

2. JUSTIFICACIÓN.

Con la globalización tecnológica y la llegada del internet a los hogares los niños tienden a buscar la conexión cibernética para ver sus videos preferidos o compartir con sus amistades en redes sociales lo cual permite que se expongan a los delincuentes con diferentes habilidades en la red y que están listos para atacar a sus víctimas, por eso se hace necesario investigar que técnicas de ingeniería social se están usando para el engaño de los infantes de edades de entre 8 y 13 años y como se está manejando las situaciones de ciber abuso presentadas en Colombia, logrando así hacer un análisis y dar posibles soluciones que contribuyan a la seguridad de los menores colombianos, determinando en que parte se está violentando la seguridad informática, como está afectando los principales pilares de esta como son la confidencialidad, la cual permite la protección de los datos de los usuarios al ser vistos con una autorización de los mismos pero si los menores mediante ingeniería social aplicada por el delincuente permiten la visión de sus datos y aparte entregan su información en chats o imágenes, archivos y demás automáticamente esta confidencialidad es totalmente destruida y permiten el acceso del delincuente a ellos, es ahí donde deben existir medidas que no permitan la filtración de información privada de los niños, la integridad siendo la cualidad de la información donde no se permite la modificación ni eliminación de esta al permitirse el envió de la información al delincuente la integridad de esta queda totalmente expuesta y averiada porque este puede hacer uso de esta y modificarla a su antojo mediantes diferentes programas informáticos por eso la mejor forma de proteger el niño es con la prevención y el no permitir el acercamiento de es estos al menor y disponibilidad de la información que al haberse violentado la confidencialidad e integridad ya está totalmente al servicio del delincuente la información por lo cual es muy importante mantener los requerimientos de privacidad del menor porque una

vez este la tenga en su poder ya puede efectuar sus maniobras delincuenciales asustando, manipulando a los niños y logrando los objetivos de su abuso .

3. ALCANCE Y DELIMITACION DEL PROYECTO.

Con esta Monografía se realizará un análisis sobre cómo se está aplicando la ingeniería social en la ejecución de ataques de carácter abusivo de manera cibernética a menores en las redes sociales de edades entre los 8 y 13 años en Colombia, buscando información en la red sobre que se está haciendo para controlar a estos delincuentes y así formular posibles aportes para contribuir con la seguridad infantil en Colombia, nos acercaremos a entidades como son la Policía Nacional, El Instituto Colombiano de Bienestar Familiar y organizaciones que se encarguen de la protección de los menores en internet como Te Protejo, Red Papaz, identificando las principales aplicaciones que contribuyen a la seguridad de los menores como son Qustodio, Protectio de la policía nacional y la plataforma Te protejo por medio de la cual se están realizando las denuncias de abusos cibernéticos a menores actualmente y está asociada con entidades como el ministerio de las TIC y el bienestar familiar.

4. OBJETIVOS DE PROYECTO.

4.1. OBJETIVO GENERAL.

Estudiar las técnicas de ingeniería social utilizadas en las redes que afectan la seguridad infantil en Colombia, analizar como la seguridad informática puede contribuir y dar posibles soluciones para mejorar la seguridad de los infantes colombianos ante posibles peligros de abusos cibernéticos en Colombia.

4.2. OBJETIVOS ESPECÍFICOS.

- Conocer la información en red sobre las técnicas de ingeniería social y como se están aplicando para ejecutar el abuso en redes en menores entre los 8 y 13 años en Colombia.

- Analizar como la seguridad informática puede contribuir y dar posibles soluciones mediante procedimientos, programas e instrucciones que se están llevando a cabo en cuanto a software para implementar medidas de seguridad infantil, usando la recopilación de información en red y entrevistas a entidades que manejen la seguridad infantil.

- Determinar medidas claras que permitan definir perfiles de posibles criminales y detección temprana de estos para evitar acercamiento con los niños.

5. MARCO REFERENCIAL.

5.1. MARCO TEÓRICO.

A través de la llegada de la tecnología a los hogares colombianos se ha evidenciado como los delincuentes utilizan Ingeniería Social para atacar a los infantes en las edades entre 8 y 13 años los cuales son engañados y manipulados para ejercer delitos en red de acoso, extorsión, abuso sexual, trata de menores y secuestro los cuales una vez se han ganado su confianza mediante mensajes de chat, redes ejercen su actividad criminal, por lo cual es muy importante establecer que parámetros se vienen adelantando para la prevención y para la detección del uso de ingeniería social en redes en Colombia y establecer como **la seguridad informática puede contribuir a la seguridad de los menores dado que mediante estas técnicas a diferencia de otros acosos ellos no tienen como protegerse** debido a que quedan totalmente expuestos psicológica y después físicamente al delincuente al seguir recibiendo mensajes en su computador, permitiendo al atacante tener anonimato al no ser un ataque directo físicamente y además si tiene un buen conocimiento en informática puede usar ciertas técnicas para que no sea detectado en red por ejemplo la Deep Web.

Se investigara la información en red sobre cómo se está aplicando estas técnicas para el abuso en redes en menores entre los 8 y 13 años en Colombia y además dar posibles soluciones mediante procedimientos, programas e instrucciones que se están llevando a cabo en cuanto a software para implementar medidas de

seguridad infantil, usando la recopilación de información en red y entrevistas a entidades que manejen la seguridad infantil y poder determinar medidas claras que permitan definir perfiles de posibles criminales y detección temprana de estos para evitar acercamiento con los niños.

5.2. MARCO CONCEPTUAL.

En esta monografía se utilizará términos importantes como son los siguientes:

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

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

Grooming: Son una serie de conductas donde un adulto se gana la confianza de un menor de edad, lo engaña creando un vínculo emocional con él para que este acceda luego a sus peticiones y el delincuente pueda ejercer sus actos criminales, es una práctica de acoso sexual a niños y adolescentes y por lo regular esto pasa

en redes sociales por lo cual es muy importante tomar medidas de seguridad para la navegación es especial de los niños en internet.

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

Delincuente: Persona que realiza diferentes actos en contra de la ley para que exista un delito es importante que este contemplado en la ley del país en el que se encuentre y que en este se encuentre determinada una condena como tal.

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

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

5.3. MARCO LEGAL.

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

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

La ley 679 de 2001, Esta es la ley base que cobija la protección de los niños, niñas y adolescentes contra la explotación, pornografía y turismo sexual.

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

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

La Ley 1273 de 2009: 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.

6. DISEÑO METODOLÓGICO.

Se ejecutará la monografía de investigación de técnicas de ingeniería social mediante las siguientes técnicas:

6.1. TECNICAS DE ANÁLISIS Y PROCESAMIENTO DE DATOS.

La técnica de análisis de información encontrada en red: Se entrará en la red y se recogerá información de artículos académicos, científicos, y de grandes empresas que manejan información sobre el tema.

Análisis crítico: Una vez se tiene la información de red se procede a realizar el análisis de esta con herramientas como procesador de texto, donde analizaremos toda la información encontrada sobre Colombia.

6.2. POBLACIÓN Y MUESTRA.

Entrevistas a entidades encargadas de manejar las operaciones de delitos de ciberdelincuentes como la policía nacional específicamente en el centro cibernético policía, nos dirigiremos al centro cibernético para solicitar las entrevistas a los encargados de la parte de seguridad infantil para que nos informen sobre las herramientas y como se realiza el análisis para llegar a los ciberdelincuentes.

6.3. METODOLOGÍA DE DESARROLLO.

La investigación se desarrollará en el transcurso de 5 meses del segundo semestre del año 2017, Quienes van a desarrollar la monografía son los ingenieros Andrés Eduardo Ojeda Barrera e Ivonne Milena Barbosa López quienes realizarán la recopilación de información necesaria para el desarrollo del proyecto.

Esta monografía está dirigida al estudio de las técnicas de ingeniería social utilizadas para el abuso de infantes a través de las redes sociales en Colombia.

7. RECURSOS NECESARIOS PARA EL DESARROLLO.

7.1. PLANIFICACIÓN DEL PROYECTO.

Esta monografía sobre la ingeniería social utilizada en el abuso de infantes a través de redes sociales en Colombia, se desarrollara con infantes de edades entre 8 y 13 años quienes serán la población objetivo a investigar, que tengan acceso a las redes sociales ya sea desde el hogar, el colegio o la oficina de sus padres, se comenzara con la actividad investigativa sobre cómo los delincuentes están aplicando la ingeniería social para persuadir a los menores, y que herramientas, programas y normas se están usando en Colombia para bloquear estos ataques y proteger a los menores.

Para el desarrollo de la monografía se utilizarán los recursos como son: PC con conexión a internet para la labor de información, se estima que el desarrollo de este proyecto dure aproximadamente 3 meses para hacerlo en el transcurso de la materia proyecto de grado 2 de la especialización de seguridad informática de la UNAD.

En el transcurso de las siguientes actividades:

- Identificar Fuentes en la red para recopilar información
- Recopilación de información en red.
- Recopilación de información en campo, entrevistas.

- Organización y análisis de la información recopilada
- Interpretar los resultados obtenidos
- Redactar el informe
- Entrega de monografía

7.2. CRONOGRAMA DE ACTIVIDADES.

Tabla 1. Cronograma de Actividades.

CRONOGRAMA DE ACTIVIDADES																
MESES	**AGOSTO**				**SEPTIEMBRE**				**OCTUBRE**				**NOVIEMBRE**			
SEMANAS	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**
Actividades																
Identificar fuentes en red para recopilar información	X	X	X	X	X											
Recopilación de información en red.						X	X	X								
Recopilación de información en campo, entrevistas.									X	X						
Organización y análisis de la información recopilada											X	X				
Interpretar los resultados obtenidos												X				
Redactar el informe												X				
Desarrollo de la Monografía																
Portada													X			

Introducción													X			
Resumen													X			
Conclusiones													X			
Bibliografía														X		
Entrega monografía															X	

Fuente: El autor

7.3. COSTOS Y PRESUPUESTOS.

Tabla 2. Costos y Presupuestos.

COSTOS Y PRESUPUESTO		
Concepto	**Ver Unitario**	**Ver Total**
INTERNET	$ 60.000	$ 120.000
TRANSPORTE	$ 20.000	$ 40.000
TELEFONIA	$ 10.000	$ 20.000
ENERGIA ELECTRICA	$ 30.000	$ 60.000
Total:	**$ 120.000**	**$ 240.000**

Fuente: El autor

8. INGENIERÍA SOCIAL UTILIZADA EN EL ABUSO DE INFANTES A TRAVÉS DE LAS REDES SOCIALES EN COLOMBIA.

8.1. INGENIERIA SOCIAL EN REDES.

La ingeniera social se define como la acción, conducta y habilidad social utilizada para obtener información de una persona de la cual no existe limitación al momento de obtener información de estas puede ser tan básica como obtener las respuestas de un cuestionario o la clave personal de un usuario para alguna transacción, la ingeniería social se basa en la persuasión y forma de obtención de información no siempre tiene que ser un engaño en algunos casos se denota que un usuario entrego su contraseña sin ninguna clase de presión, como también se determinan sucesos en los que si hay ataque, acoso, presión y demás, el delincuente genera una situación creíble que le dé el máximo nivel de manipulación si la víctima no tiene un nivel adecuado de precaución va permitir que el ataque del ingeniero social se lleve a cabalidad.

La ingeniería social es una técnica usada para recolectar información por medio de persuasión, de tal forma que la información suministrada por la victima permita de una u otra forma tener la información clave, los métodos de persuasión hacia la víctima es crear situaciones de confianza y creíbles. Donde la victima sienta libertad de dar a conocer su información personal, al tener este control sobre la víctima se puede realizar de forma digital, de ingreso a una aplicación donde tengamos un test con la información o acceso básico a los datos de las víctimas. Cada año caen personas engañadas por Phishing mediante correos y paginas maliciosas o por

teléfono donde entregan supuestos premios por participar en concursos los cuales después salen ganadores

Por lo cual es indispensable estudiar las técnicas, cómo actúan los delincuentes cibernéticos para poder proteger la información por esto la seguridad informática es tan importante y más si nos encontramos con técnicas de ingeniería social aplicada a la obtención de información de menores de edad.

Como objetivos principales la ingeniería social requiere apropiarse de la información para conseguir beneficios económicos como compras en internet, telefónicas y los que se benefician de la información como claves de cuentas bancarias, datos de tarjetas, acceso a internet, acceso a correos electrónicos, datos usuarios de redes, información privada y de carácter sexual, siempre va a destacarse una ganancia para el delincuente mientras la víctima no nota el ataque.

Al tener este control sobre la víctima se puede realizar de forma digital, de ingreso a una aplicación donde tengamos un test con la información o acceso básico a los datos de las víctimas. Cada año caen personas engañadas por Phising mediante correos y paginas maliciosas o por teléfono donde entregan supuestos premios por participar en concursos los cuales después salen ganadores.

Formas de ataque de Ingeniería Social: Con el uso de tecnologías se pueden realizar distintos ataques como son:

Ataque Telefónico: Este ataque permite que el delincuente use todo su potencial pues que no está cara a cara con la victima razón por la cual esta no puede percibir

en su lenguaje corporal cualquier indicio de engaño, Este método de llamada telefónica fue la primera técnica empleada por los ciberacosadores o atacantes, de esta forma las personas o victimas brindaban información personal atreves del ofrecimiento de un servicio. Después con el paso del tiempo y al avanzar de la tecnología los ataques se volvieron más completos y donde ya no solo la información personal era suficiente, comenzaron con el secuestro de información atreves de los virus informáticos o troyanos, al enviar un correo o un mensaje por mensajería instantánea.

Ataques WEB: Es uno de los más frecuentes puesto que se pueden ejecutar a través de correos electrónicos y además por el auge de internet a nivel mundial se puede realizar en cualquier momento además del acceso a redes sociales, chats,
El paso del tiempo, el cambio de tecnología y la llegada de nuevas aplicaciones y del internet de mejor y más fácil acceso a los hogares, el tema de seguridad y de que la información ya no solamente personal sino bancaria empezara a rodar por la red internet; además se sumó la aparición de los teléfonos celulares Smartphone con acceso a internet, donde se cataloga no solamente información sino fotos, notas, conversaciones, claves y aplicaciones.

Si se observa la aplicación de técnicas de ingeniería social de manera más definida donde denota que se trabajan dos caminos uno es la interacción activa que se ha practicado empíricamente y la interacción pasiva donde se tiene a los atacantes que han estudiado conceptos y los han profundizado para mejorar sus técnicas.

Interacción activa: Es cuando se realiza el ataque de ingeniería social directamente con el fin de ejecutar la modalidad delictiva que este debe ejercer, por

la malicia y solamente la intención del ataque la justicia aun no a determinado medio necesarios para castigar estas modalidades delictivas, como ejemplo tenemos a Kevin Mitnick quien esquivo a la justicia por más de 20 años sustrayendo información confidencial de diferentes entidades y actualmente se desempeña en su empresa de seguridad informática, participa en eventos de black hat y es muy conocido por ser pionero en la modalidad de ingeniería social.

Según kevin midnick la ingeniería social se desarrolla en cuatro etapas las cuales vamos a ver a continuación:

1. Investigación: es la investigación en fuentes de información como artículos, formularios, periódicos, páginas web etc.
2. Desarrollar rapport y credibilidad: utilización de información interna, se realizan reclamos a la víctima o se pide ayuda.
3. Explotar la confianza: se logra que la víctima pregunte por el objetivo que ya se tiene demarcado con anterioridad.
4. Utilizar información: si no se ha logrado obtener la información completa se vuelve a iniciar el ciclo hasta conseguir el objetivo.

Interacción pasiva: Es la cual trabaja con la ingeniería social mediante un segundo plano, sin contacto real.

Para Dale Pearson experto en ingeniería social quien considera que los puntos clave de la ingeniería social se pueden resumir en la siguiente frase **"el lenguaje es muy poderoso y la mente tiene vulnerabilidades que se pueden usar"**, la cuestión es hasta donde el atacante quiere llegar, como vemos los ataques de

ingeniería social manejan un alto grado de técnicas psicológicas, mescladas con conocimientos en algún momento informáticos, y además el atacante experto en esta técnica es bastante inteligente, perspicaz, debe tener perfectamente detallado su plan de ataque los cual coloca a los niños en un alto grado de peligro ante delincuentes tan sumamente astutos y si se tiene en cuenta que el grooming y sexting aplican ante la justicia como solo modalidades delictivas, los niños quedan mayormente expuestos a estos delincuentes puesto que tienen una alta probabilidad de escapar de las manos de la justicia. Castigar estas modalidades delictivas, como ejemplo tenemos a Kevin Mitnick quien esquivo a la justicia por más de 20 años sustrayendo información confidencial de diferentes entidades y actualmente se desempeña en su empresa de seguridad informática, participa en eventos de black hat y es muy conocido por ser pionero en la modalidad de ingeniería social.

Ahora se analizará una nueva forma de ingeniería social, es la ingeniera social automatizada donde se automatizan los componentes medio y atacante de la ingeniera social lo cual le da independencia al ataque por la programación con elementos psico-Sociales en su lenguaje.

Los ataques de ingeniería social se caracterizan porque por lo regular se logra el objetivo deseado con accionar el estímulo correcto el atacante puede llegar a conseguir su objetivo, se requiere de mucho esfuerzo para que se logre una relación de confianza con la víctima, el usuario en la red tiene una visión muy limitada de lo que ve lo que permite que un niño por ejemplo en este caso de la población infantil sean más fáciles de persuadir con buenas palabras teniendo en cuenta que ellos no tienen el nivel de malicia o desconfianza de un adulto y aun así los adultos son engañados en la red.

8.2. MANEJO ACTUAL DE REDES SOCIALES.

Con el avance de la tecnología el acceso a redes sociales es muy fácil para los niños por eso vamos a ver cómo están funcionando estas actualmente, las redes sociales se componen de personas que son conectadas a través de un perfil por distintos tipos de relaciones que pueden ser conocidos, amigos, familiares, laborales o con intereses en común que simplemente se quieren conocer más, la forma de operar son solicitudes de amistad entre los perfiles que se dan por personas que ven a través de su perfil intereses en común con ellos y además estos permiten subir fotos y una vez estando conectados pueden chatear, compartir estado de ánimo , fotos , videos y demás, no solo es una moda entre los jóvenes es una tendencia mundial además está cambiando la sociedad y aunque tiene restricción de edad hay formas en la validación con la que menores pueden abrir cuentas, estudios han demostrado que el mal uso de las redes sociales promueve ciertos aspectos negativos como el ciberacoso robo de información , de identidades y demás.

Los niños tienen contacto casi que desde después de su nacimiento con la tecnología, a través de fotos, dispositivos celulares cerca de ellos que son utilizados para la realización de videos y a través de esto se ha llegado al punto en que los niños puedan controlar casi cualquier aparato con sus manos, ellos aprenden muy rápidamente su manejo por lo cual es tan importante la guía para el uso de las tecnologías, con una buena orientación se puede lograr sacar un buen provecho de estas, sin embargo se expondrá algunos riesgos del mal uso de las redes sociales:

- Explotación sexual infantil
- Contacto con posibles delincuentes en red que desean abusar del grado de inconsciencia del niño.

- Ciberacoso
- Sexting: que es el intercambio de imágenes o mensajes de contenido sexual.
- Grooming: Modalidad delictiva mediante la cual atraen menores con objetivos sexuales.
- Publicación de imágenes, videos que dañan la integridad de los niños.
- Violación total de la intimidad del menor
- Prostitución de menores

8.3. ESTUDIO HÁBITOS INTERNET.

Según un estudio realizado por Arena donde se analizaron los hábitos de los niños en internet entre edades de 7 a 9 y 10 a 11 años revelo lo siguiente:

Los niños en edades de 7 a 9 años cuando ingresan a internet tienes como interés particular la información para tareas y juegos, mientras que los niños colombianos entre los 10 y 11 años tienen como intereses empezar la comunicación de chat y redes sociales.

En el uso de las redes sociales el 64% de los menores mayores chatea frente a un 49% con los menores de menor edad y es más atractiva la comunicación por red para los mayores entre 10 y 11 que frente a un 35% para los menores entre 7 y 9 años.

9. MEDIAS DE SEGURIDAD INFANTIL TOMADAS EN COLOMBIA.

Colombia actualmente está posicionado como uno de los mejores países en cuanto a ciber seguridad tanto así que esta al mismo nivel de países como Francia, España, Egipto y Dinamarca, Cuenta con un gran grupo de apoyo para el seguimiento de los delitos informáticos, denuncias y atención a las víctimas de estos como: centro cibernético policial, grupo de respuesta a incidentes informáticos, (Colcert), comando conjunto cibernético.

La policía nacional, el ministerio de tecnologías (MinTIC), Fundación Telefónica, El Instituto de bienestar familia, se unieron el en V encuentro internacional para el manejo y la prevención de la explotación sexual infantil en línea y declararon nuevamente el pacto de cero tolerancia con el material de abuso infantil en internet, organizado por la línea virtual de denuncia **Teprotejo** (www.teprotego.org) esta es una página donde se encuentra formas de denunciar información de los delitos que se existen y que protegen. Esta iniciativa es creada para informar y que la población colombiana y del mundo conozca que se está trabajando a favor de los derechos de los niños y que tengan un futuro informático más placentero y con información de calidad. Donde no se vean agobiados o que su información sea sustraída.

Inicia en Colombia el 20 de febrero de 2008, gracias a la reunión del ministerio de educación y de comunicaciones, también gracias al apoyo de los padres de familia y empresas de los diferentes sectores. Donde se creó una mesa de trabajo para crear en Colombia una forma de promover el uso sano de la tecnología y su

información, que de esta forma se pueda proteger a los niños y jóvenes colombianos. Del nacimiento de esta organización también nacieron otras páginas que día a día enriquecen y florecen para el cuidado y protección entre ellas esta, una de las más importantes: www.tus10comportamientosdigitales.com en esta página se puede encontrar información sobre control parental de las aplicaciones que traen consolas de juegos, también hay guías sobre cómo configurar en cada consola de juegos la cual es muy útil y que muchos padres no conocen, las explicaciones son básicas y se aplican a cabalidad para las consolas de juegos que nuestros niños desde muy jóvenes ya tiene acceso.

Volviendo a la página te protejo; donde se encuentran aliadas grandes empresas de telecomunicación mundiales como es la fundación Telefónica (España) y además de aliadas como red Paz, con el paso de los años se han adherido a esta gran propuesta el ICBF, INHOPE, Tigo Colombia móvil, etc. que quieren salir adelante con su propuesta de apoyo una navegación de los jóvenes segura.

Gracias a las alianzas y crecimiento de apoyo para la violencia infantil se desarrolló una aplicación para teléfonos inteligentes en la cual se pueden dar a conocer las denuncias que se pueden encontrar en internet o que nos están aquejando a los niños y jóvenes, esta aplicación se llama Te Protejo, fue desarrollada para cada uno de los sistemas operativos de teléfonos y Tablet existentes.

Esta página es muy interactiva ya que se encuentran videos con explicaciones de forma muy clara orientada a informar sobre los beneficios de la página TeProtejo; se informa que se debe hacer para denunciar, proteger y reaccionar. Además de las leyes que existen en la constitución colombiana y la legislación penal para la

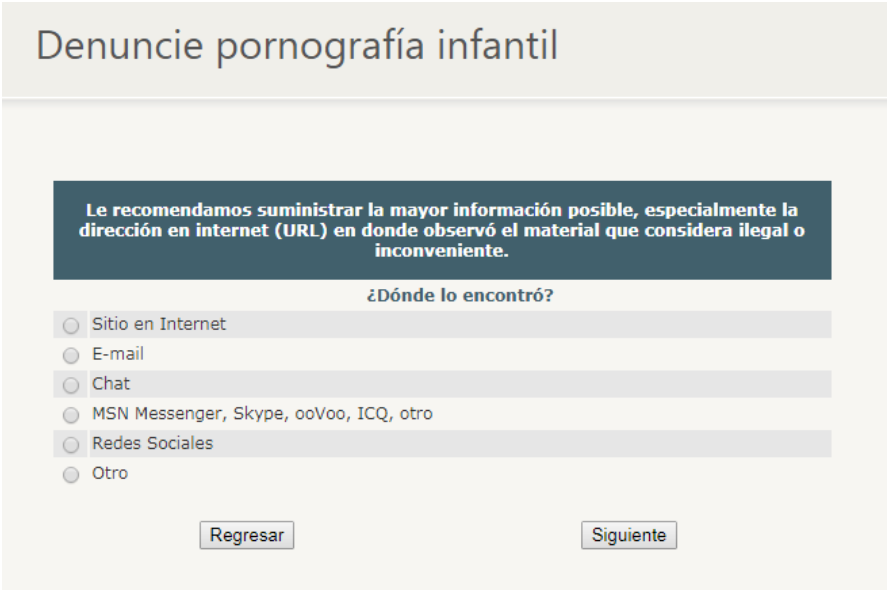
protección de cada uno de los casos que se pueden presentar. Una explicación clara de las leyes, se encuentra respuestas de palabras y frases que se usan dentro del contenido de acoso o ciberacoso. Explicaciones claras y fáciles de entender con explicación.

A continuación, plataforma TeProtejo:

Fig. 1 . Te Protejo.

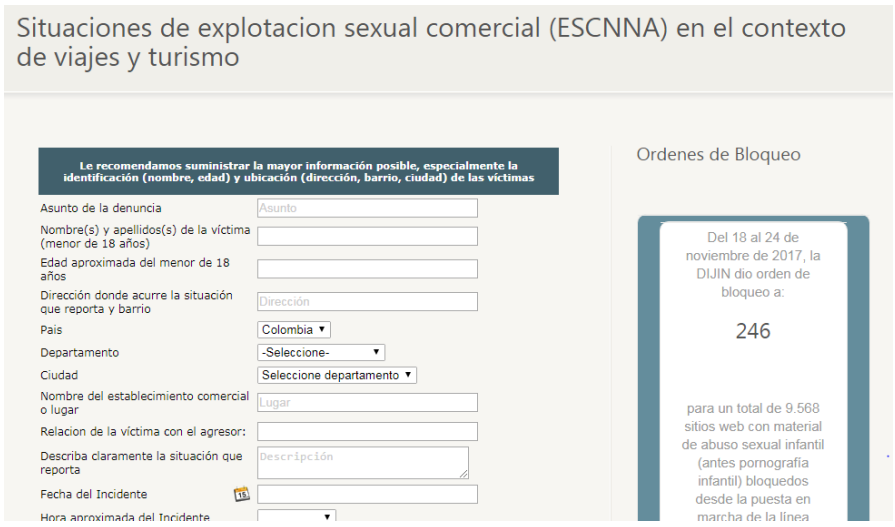
Fuente: http://www.teprotejo.org/index.php/es/

Fig. 2 Denuncia de Pornografía Infantil.



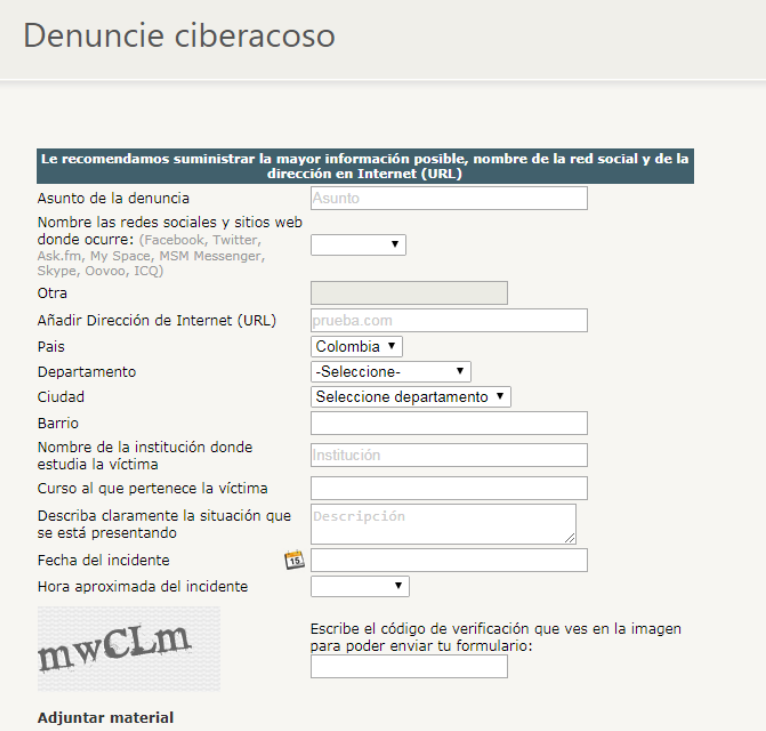
Fuente: http://www.teprotejo.org/index.php/es/denuncia-explotacion-sexual

Fig. 3. Explotación sexual a menores.



Fuente: http://www.teprotejo.org/index.php/es/denuncie-explotacion

Fig. 4. Ciberacoso.



Fuente: http://www.teprotejo.org/index.php/es/denuncie-ciberacoso

Una de las secciones de la página explica realmente que se debe denunciar las situaciones claras que se pueden presentar y denunciar a través de la página; así como cuáles son las etapas que toma una vez hecha la denuncia las comprobaciones por parte de la entidad de justicia.

Se encuentran los porcentajes de las denuncias que se han hecho realizado a través de la página y la entidad INHOPE que se encarga de regular las denuncia a nivel mundial, es un hecho sin precedentes que el material pornográfico de infantes es alto en la red de redes. Donde las más expuestas son las niñas, seguidas por los

niños. Claro está que gracias a la creación de estas organizaciones se ha realizado una gran disminución en el número de cifras en cuanto ataques a menores.

Tabla 3. Informe TeProtejo histórico a 2015.

Histórico		2012	2013	2014	2015	Total	%
Denuncias Procesadas	Pornografía Infantil	462	1.493	3.724	4.829	10.508	52,7%
	ESCNNA	0	0	36	121	157	0,8%
	Intimidación Escolar	129	126	187	130	572	2,9%
	Ciberacoso	0	0	491	482	973	4,9%
	Contenidos Inapropiados	145	263	245	160	813	4,1%
	Venta de alcohol y otras SPA	143	212	143	126	624	3,1%
	Maltrato, trabajo y abuso infantil	101	1.041	988	1.139	3.269	16,4%
	Otros	918	405	606	393	2.322	11,6%
	No aplica	294	381	32	0	707	3,5%
	Total	**2.192**	**3.921**	**6.452**	**7.380**	**19.945**	**100%**

Fuente: http://www.teprotejo.org/index.php/es/logros-2015/500-informe-al-31-de-octubre-de-2015

Fig. 5. Te Protejo histórico a 2015.

Fuente: http://www.teprotejo.org/index.php/es/logros-2015/500-informe-al-31-de-octubre-de-2015

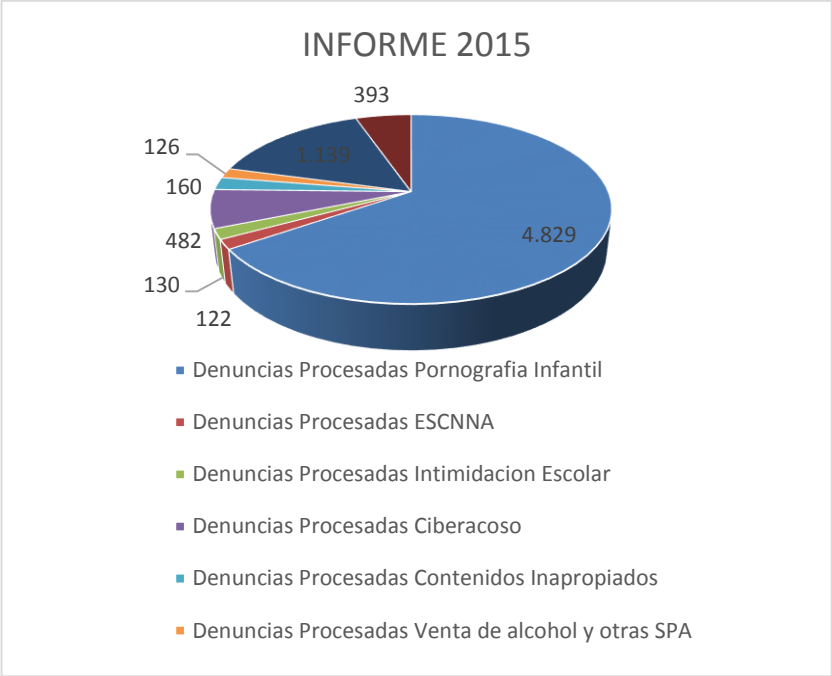
Tabla 4. Informe Te Protejo 2015.

2015		Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Total	%
Denuncias Procesadas	Pornografía Infantil	248	353	481	490	388	691	479	709	504	486	4.829	65,4%
	ESCNNA	2	3	19	18	19	5	9	30	4	13	122	1,7%
	Intimidación Escolar	7	13	16	16	14	2	8	20	22	12	130	1,8%
	Ciberacoso	37	52	57	48	50	33	42	58	55	50	482	6,5%
	Contenidos Inapropiados	19	22	18	22	19	6	9	13	11	21	160	2,2%

	Venta de alcohol y otras SPA	9	12	11	13	18	7	7	14	23	12	126	1,7%
	Maltrato, trabajo y abuso infantil	75	113	103	78	140	121	138	116	162	93	1.139	15,4%
	Otros	36	39	51	39	33	32	34	70	28	31	393	5,3%
	Total	**433**	**607**	**756**	**724**	**681**	**897**	**726**	**1.030**	**809**	**718**	**7.381**	**100%**

Fuente: http://www.teprotejo.org/index.php/es/logros-2015/500-informe-al-31-de-octubre-de-2015

Fig. 6. Gráfico Te Protejo 2015.



Fuente: http://www.teprotejo.org/index.php/es/logros-2015/500-informe-al-31-de-octubre-de-2015

Al 31 de octubre de 2015 se recibieron a través de Te Protejo 19.945 reportes, de los cuales el 52.7% se refieren a contenidos con pornografía infantil, 2.9% casos de intimidación escolar, 4.9% de ciberacoso, 0.8% de explotación sexual comercial de niños, niñas y adolescentes 16.4% a casos de maltrato infantil, abandono, abuso y trabajo infantil; 4.1% de contenidos inapropiados en medios de comunicación, 3.1% sobre situaciones de venta y consumo de alcohol a menores de 18 años; el 11.6% de otros y 3.5% no aplican con relación a las apariciones en medios, hasta el 31 de octubre se han identificado 880 registros. El App de Te Protejo se ha descargado 2375 veces.

Se presenta una estadística de los reportes realizados por la página a la entidad Teprotejo, así como la clasificación de las denuncias realizadas. También se encuentran los informes de gestión de los años que lleva la página activa con resultados y denuncias. Aparición en la televisión de las denuncias y casos presentados.

Al 31 de diciembre de 2014 se recibieron a través de Te Protejo 12.565 reportes, de los cuales el 45% se refieren a contenidos de pornografía con menores de 18 años; el 4% a contenidos inapropiados en radio y TV; 4% de venta y consumo de alcohol y otras sustancias psicoactivas; 16% a maltrato, abandono, abuso y trabajo infantil; 3% a intimidación escolar, 3% de ciberacoso; 0.29% a Explotación Sexual Comercial con Niños, niñas y adolescentes (ESCNNA); 15% a otros y el 7% a No Aplica.

Tabla 5. Informe Te Protejo 2014.

Categoría	May-Dic 2012		Ene-Dic 2013		Recibidas en 2014			Promedio 2014	Total	%
	Recibido	Promedio	Recibido	Promedio	Enero a Abril 2014	Mayo a Ago 2014	Sept - Dic 2014			
Contenidos de pornografía infantil	462	58	1497	124,8	1432	1285	1007	310	**5683**	45 %

Explotación sexual con niñas, niños y adolescentes					0	6	30	3	**36**	0%
Intimidación Escolar	129	16	126	10,5	55	54	78	16	**442**	4%
Ciberacoso					78	208	205	41	**491**	4%
Contenidos inapropiados en medios de comunicación	145	18	153	12,8	74	84	87	20	**543**	4%
Venta y consumo de alcohol y de otras sustancias psicoactivas	143	18	212	17,7	30	35	78	12	**498**	4%
Maltrato, Abandono y Trabajo Infantil			1043	87	329	292	367	82	**2031**	16 %
Otros	918	115	401	33,4	189	150	267	51	**1925**	15 %
No aplica	395	66	489	40,8	32	0	0	3	**916**	7%

Total	**2192**	**291**	**3921**	**327**	**2219**	**2114**	**2119**	**538**	**12565**	**100 %**

Fuente: http://www.teprotejo.org/index.php/es/logros-2014/418-informe-al-31-de-diciembre-de-2014

Fig. 7. Gráfico informe TeProtejo 2014.

Fuente: http://www.teprotejo.org/index.php/es/logros-2014/418-informe-al-31-de-diciembre-de-2014

Al 31 de diciembre, a través de Te Protejo se recibieron un total de 6.113 denuncias, de las cuales el 32% se refieren a pornografía infantil, 14% de Maltrato, Abandono Abuso Infantil; 6% de Venta y consumo de alcohol y de otras sustancias psicoactivas 5% sobre Contenidos inapropiados en medios de comunicación; 4% sobre

Intimidación Escolar, Bullying o ciberacoso; 3% Explotación sexual a menores de 18 años; 22% otros; y 14% No aplican.

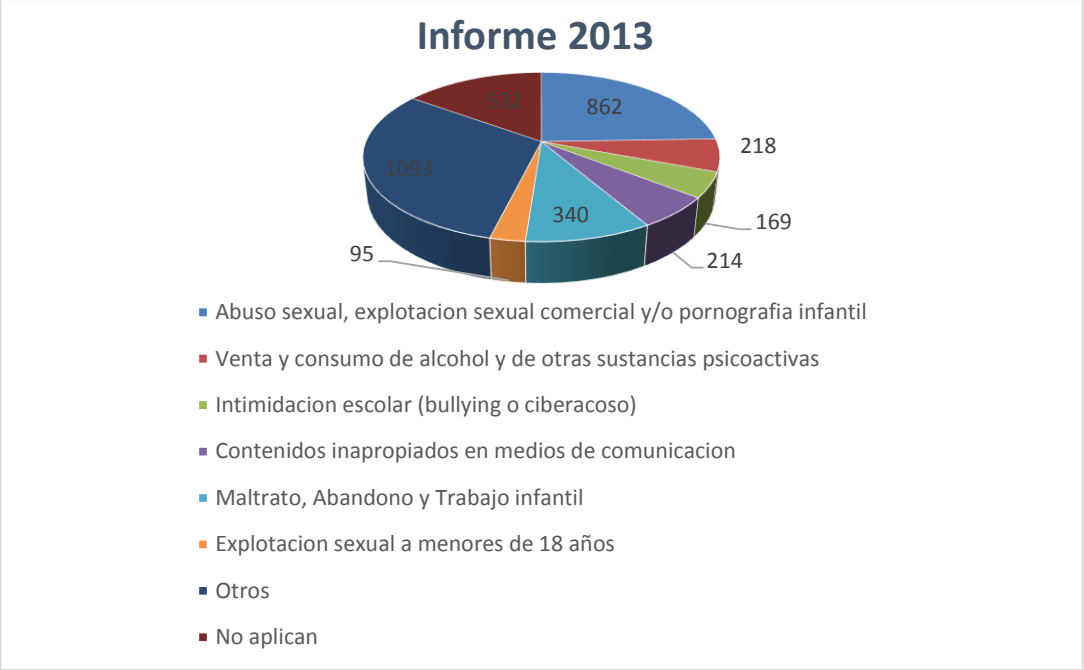
Tabla 6. Informe Te protejo 2013.

Temas de denuncias	Mayo - Dic 2012	Promedio Mayo - Dic 2012	Enero	Febrero	Marzo	Abril	Mayo	Total	%
Abuso sexual, explotación sexual comercial y/o pornografía infantil	462	58	112	46	81	75	86	862	24%
Venta y consumo de alcohol y de otras sustancias psicoactivas	143	18	14	17	8	17	19	218	6%
Intimidación escolar (bullying o ciberacoso)	129	16	7	7	13	1	12	169	5%

Contenidos inapropiados en medios de comunicación	145	18	4	16	22	18	9	214	6%
Maltrato, Abandono y Trabajo infantil			88	62	65	61	64	340	10%
Explotación sexual a menores de 18 años			29	19	17	19	11	95	3%
Otros	918	115	40	28	21	45	41	1093	31%
No aplican	395	66	20	14	52	24	27	532	15%
Totales	**2192**	**291**	**314**	**209**	**279**	**260**	**269**	**3523**	**100 %**

Fuente: http://www.teprotejo.org/index.php/es/logros-2013/132-informe-al-31-de-mayo-de-2013

Fig. 8. Gráfico Informe Teprotejo 2013.



Fuente: http://www.teprotejo.org/index.php/es/logros-2013/132-informe-al-31-de-mayo-de-2013

Hasta el 29 de diciembre de 2012 se recibieron a través de Te Protejo 2192 denuncias, de las cuales el 21% se refieren a contenidos (fotos, videos, etc.) sobre abuso sexual, explotación sexual comercial y/o pornografía con menores de 18 años; el 6% a contenidos inapropiados en radio y TV; el 7% a venta y consumo de alcohol y otras sustancias psicoactivas, 6% a intimidación escolar o ciberacoso; 42% a otros y el 18% a No Aplica.

Tabla 7. Informe TeProtejo 2012.

Tema de denuncia	Abril y Mayo	Junio	Julio	Totales	%
Abuso sexual, explotación sexual comercial y/o pornografía infantil	61	60	20	141	40%
Venta y consumo de alcohol y de otras sustancias psicoactivas	8	18	14	40	11%
Intimidación Escolar, Bullying o ciberacoso	9	14	13	36	10%
Contenidos inapropiados en radio y tv	10	22	28	60	17%
Otros	6	19	47	72	21%
Total	**94**	**133**	**122**	**349**	**100%**

Fuente: http://www.teprotejo.org/index.php/es/logros-2012/55-informe-al-31-de-julio-2012

Fig. 9. Gráfico Informe TeProtejo 2012.

Fuente: http://www.teprotejo.org/index.php/es/logros-2012/55-informe-al-31-de-julio-2012

We protect una herramienta de respuestas coordinadas entre países para prevenir y combatir la explotación sexual en redes de niños donde se busca fortalecer las líneas de denuncia para defender los derechos de los niños colombianos en internet, siendo su primera etapa la implementación del compromiso de la empresa privada, el sector justicia y otras entidades que velan por la protección infantil.

Esta es una realidad que no se quisiera tener que aceptar, pero con la tecnología al alcance de los niños es muy fácil que los abusadores puedan establecer contacto con sus posibles víctimas, compartir imágenes de sus abusos y animarse entre ellos a cometer más delitos.

El ciber abuso en niños incluye variables como:

- La producción y distribución de abuso sexual en línea.

- Preparación de las posibles víctimas en línea para el abuso sexual que hay donde se utilizan las técnicas de ingeniería social para el engaño de niño y sometimiento.

- La transmisión en directo del abuso y la consecución de este en los niños.

Es muy abundante el material de abusos infantiles en línea que tienen los delincuentes y muchos de los niños que están en estos materiales no se han identificado y aún pueden estar en riesgo, evidencias de investigaciones realizadas dan por cuenta que la explotación infantil en línea es muy perjudicial para la víctima y deja afectación psicológica de por vida en los niños.

Por esto se creó la alianza WePROTECT con el fin de terminar abuso en línea de niños siendo este un movimiento internacional que reúne varios países interesados en acabar este delito.

9.1. CENTRO CIBERNÉTICO POLICIAL.

En contacto con la Dijin en el centro de ciber seguridad de la policía nacional y encargados del manejo de estos delitos infantiles se obtuvo información como la siguiente:

En Colombia actualmente estos delitos que son cometidos luego de haber ejecutado las modalidades delictivas en el ámbito cibernético no son tipificadas por edades, pero si se tiene estadísticas durante el año 2016 y 2017 en Colombia se judicializaron 66 capturas por GROOMING vinculado a pornografía infantil, teniendo en cuenta que el grooming y el sexting son modalidad delictivas que conllevan a que se desarrollen delitos como la violación de datos personales, extorsión, abuso a menores de edad y demás.

Para identificar amenazas como el GROOMING, SEXTING, Aplicaciones maliciosas (chat), CIBERACOSO y Explotación sexual infantil se ha realizado una difusión de a través de redes como del cuadrante virtual, twiter (72 cuentas), Facebook (más de un millón de seguidores), youtube con más de 23 millones de reproducciones de video, para un total aproximado de 5 millones de seguidores en las redes sociales de la policía nacional.

Actualmente se tienen acciones totalmente coordinadas con entidades internacionales como son la INTERPOL, EUROPOL y AMERIPOL en contra de las redes dedicadas a la distribución de material y explotación sexual infantil, se tiene operaciones como TANTALIO Y SIN FRONTERAS y nos ponen al tanto de la evidencia de lo internacional que se están manejando estos crímenes.

Desde el año 2012 hasta la fecha se han recibido 36.443 reportes de los cual el 60% hace referencia al material de abuso sexual en infantes en Colombia, el 6% a ciberacoso y el 1% de los casos a explotación sexual comercial infantil y en promedio se analizan 900 URL´s con contenido sexual infantil por mes en Colombia.

Se están llevando procesos muy fuertes de mundialización en casos de grooming, de los cuales en el año 2016 se recibieron 69 reportes y en el año 2017 hasta la fecha 144 con una variación del 75% y se ha presentado un incremento del 09%; teniendo en cuenta casos que se han reportado en el CAI VIRTUAL del Centro Cibernético Policial, siendo este el mecanismo de denuncias con el acompañamiento y coordinación de la Fiscalía General de la Nación.

Desde los años 2014 se realizaron 111 capturas por el delito de pornografía infantil con persona menor de 18 años (Art. 218 CP y 219 A).

Desde el año 2014 hasta la fecha se han recibido 3.500 denuncias por pornografía infantil.

El centro cibernético policial tiene a disposición de los ciudadanos la aplicación llamada PROTECTIO, que es una aplicación para denunciar ciberdelincuentes que estén atacando niños.

Fig. 10. Protectio

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

En esta se registran los datos y le es entregada por el caí virtual una clave para denunciar, lo positivo de esta aplicación es que el incidente es reportado de manera inmediata y directamente a la policía, lo cual permite mayor capacidad de reacción por parte de esta.

Fig. 11. Aplicación Contra ciberdelincuencia.

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

El objetivo de esta aplicación es el reporte de incidentes lo más rápido posible para así lograr mejor reacción, sin embargo, se debe tener especial cuidado al momento de registro y solicitud de clave en la aplicación del caí virtual porque en ocasiones las cuentas no están comunicadas y no permite el ingreso en la aplicación.

Fig. 12. Reportes de incidente.

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

Es una buena herramienta para el reporte de incidentes, por la comunicación directa con el Caí virtual si se logra la conexión se reportan estos de manera inmediata.

10. SOFTWARE UTILIZADOS PARA IMPLEMENTAR SEGURIDAD INFANTIL.

10.1. FILTROS CONTROL PARENTAL.

Un estudio entre el ministerio de Tecnologías de la información y las comunicaciones (MINTIC) y la compañía .CO que en conjunto trabajan para mejorar el uso adecuado de internet, confieren que gracias a investigaciones realizadas a través del tiempo se han creado mejoras en la restricción de acceso a la Red de redes, claro que no todo se debe responsabilizar; en gran medida los aportes a la restricción se pueden y se deben a la conciencia que han tomado los padres de familia y las restricciones aplicadas a los dispositivos móviles, computadores y equipos de tecnología.

Existen en internet varios programas para la protección de contenidos, los antivirus ahora nos brindan esta alternativa en las versiones compradas, tienen y poseen una fácil configuración. Al adquirir la licencia se adquiere un portafolio de seguridad que podemos aplicar y configurar desde una página de internet.

Se mostrará una experiencia de tres aplicaciones encontradas y ofrecidas atreves de internet y que son las más utilizadas, donde las aplicaciones pueden ser gratis y pagadas.

10.2. QUSTODIO.

Fuente: https://www.qustodio.com/es/

Un estudio de la página QUSTODIO informa que el uso de equipos tecnológicos en los niños cada vez es más alto, y que los padres también contribuyen para que este tema de tecnología crezca en los niños, el acceso es más sencillo, flexible y más factible, ahora el internet está en todas partes.

Fig. 13. Uso por edades de dispositivos tecnológicos.

Fuente: https://www.qustodio.com/es/family/why-qustodio/

El tiempo que pasan los menores frente a un equipo tecnológico está comprendido entre 4 y 6 horas, en adolescentes es mayor el tiempo ya que ellos tienen más conocimiento de acceso y acceso a espacios como YouTube y videos en línea.

Fig. 14. Estudio uso internet.

Fuente. https://www.qustodio.com/es/family/why-qustodio/

Qustodio: Es una aplicación que cuenta con el servicio de descarga gratis y Premium (costo por administración de más recursos). En la descarga gratuita se puede contar con la administración de un equipo PC, MOVIL o TABLET y el monitoreo del mismo desde un celular. Además, su panel de administración es muy amigable y cuenta con soporte y aplicación en español.

No solamente prestan el servicio para usuarios de familia, también para control en escuelas y empresas.

Esta herramienta diseñada para controlar y proteger los accesos que hagan los niños a las paginas, tiempo de uso, anuncios y lugares prohibidos para la edad de ellos y para evitar el acceso de aquellas personas que quieren realizar prácticas de pornografía infantil.

Al realizar la instalación de la aplicación en el computador se puede iniciar la configuración y supervisión del mismo, generando reportes de tiempo de navegación, sitios visitados y de esta manera realizar configuraciones extras a medida que pasa el tiempo.

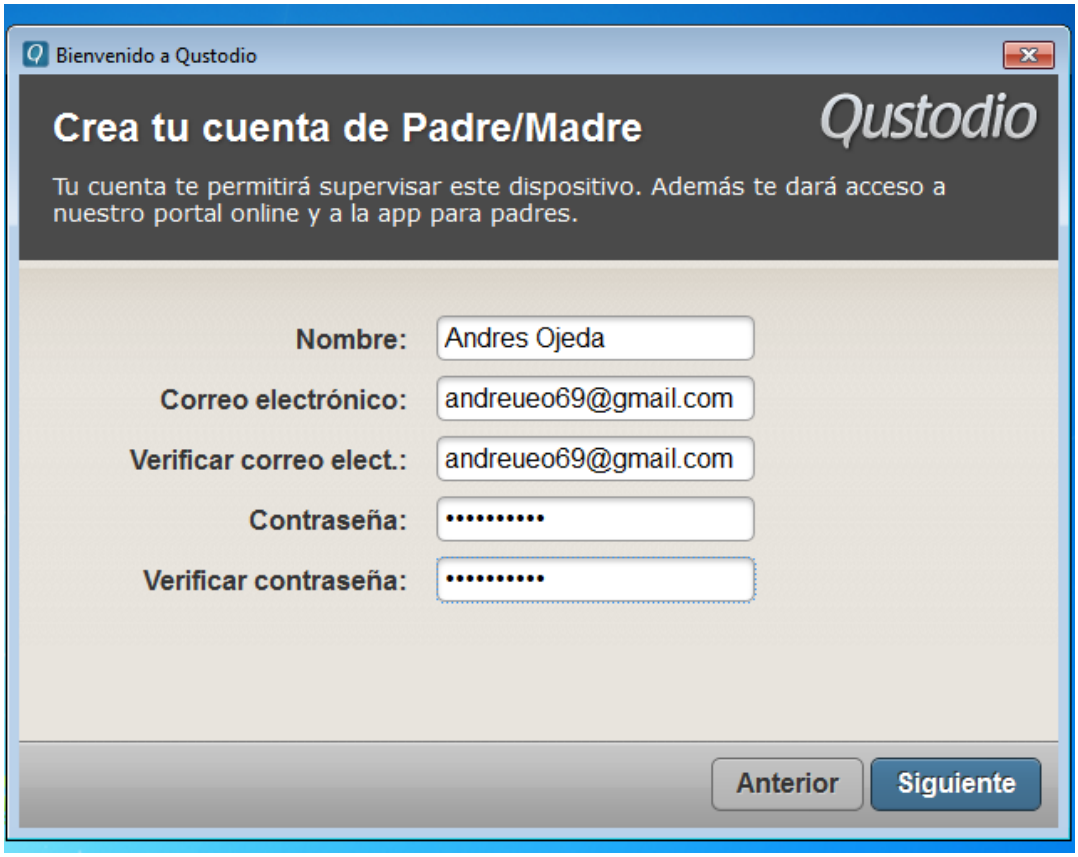
Esta Herramienta cuenta con el control de:

- Control de tiempo en el dispositivo.
- Filtro web.
- Geolocalización.
- Vigilancia de navegación de Facebook.
- Bloqueo en Facebook, juegos y aplicaciones.
- Control de mensajes de texto.
- Informes de Actividades.
- Bloqueo de contenido inapropiado.

Cuenta con soporte para las tecnologías actuales: ANDROID, IOS, WINDOWS, MAC Y KINDLE.

La instalación de la aplicación QUSTODIO es sencilla y solo con llenar unos pocos campos para la configuración de la aplicación.

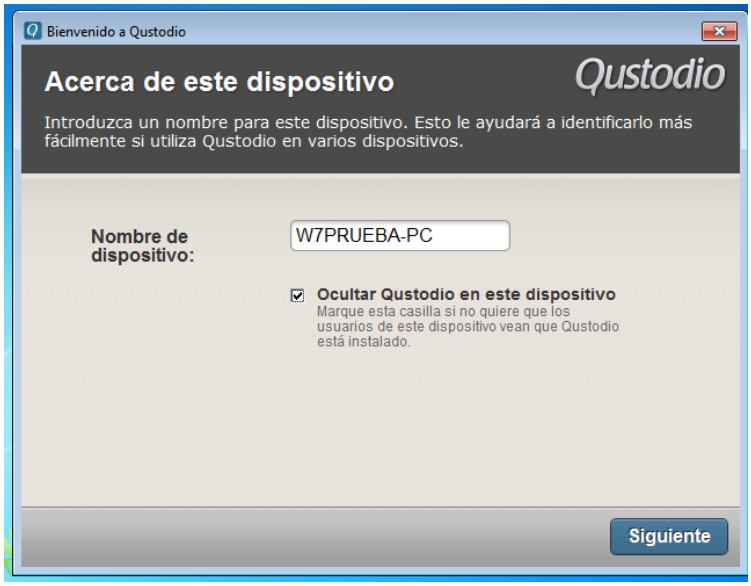
Fig. 15. Qustodio 1.



Fuente: El autor.

Se puede instalar en los equipos pc sin que el usuario sepa que esta activo, para esto se debe configurar una sesión como usuario normal, sin privilegios de administrador.

Fig. 16. Qustodio 2



Fuente: El autor.

Fig. 17. Qustodio 3

Fuente: El autor.

Después de la configuración básica de la aplicación, se puede direccionar al panel de control que se realiza a través de la página https://family.qustodio.com/?locale=es, donde el acceso se realiza con el usuario (Correo) y clave configuradas previamente. En este panel se encuentra la actividad en redes sociales, salas de chat, acceso y tiempos de navegación en páginas web.

Fig. 18. Qustodio 4

Fuente: El autor.

La versión Premium por la cual se debe pagar un precio anual que no sobrepasa los 150 dólares, entre sus funcionalidades tiene un panel de control estricto para Facebook, mostrando conversaciones, publicaciones, acceso a historiales de navegación, tiempo de uso, etc. Esta aplicación tiene el control total del equipo donde está instalado, se puede restringir aplicaciones a usar, límite de tiempo en

navegación, se maneja en días y horas. Es una herramienta muy completa aun en su parte gratuita.

Esta herramienta es de gran utilidad y muestra un estado en porcentajes del tiempo que utiliza y para que el equipo. En los dispositivos móviles se puede validar los mensajes de texto, llamadas, además la restricción inmediata a contenido no apto para niños y adolescentes.

Al intentar desinstalar la aplicación de esta notifica por correo electrónico que algo está pasando con dicho dispositivo y además necesita como confirmación la clave de administrador, es una gran ventaja no poder eliminar la aplicación fácilmente.
Lo reportes de la aplicación nos dan a conocer el tiempo implementado en cada página web, los contenidos, las charlas en WhatsApp, Facebook, aplicaciones usadas, mensajes de texto y llamadas telefónicas (así sean borradas desde el teléfono).

Fig. 19. Qustodio 5

Fuente: https://family.qustodio.com/user-activity/timeline/view/user-rules-panic button/context/upgrade-button/locale/es/user/1979360/days/7

Es una herramienta tan completa que puede bloquear hasta las llamadas de un número de celular el cual no se quiera recibir o llamar.

10.3. K9 WEB PROTECTION.

Fuente: http://www1.k9webprotection.com/

Es un software de aplicación de protección de control parental que también ofrece de forma gratuita y pago de su servicio. Esta aplicación es una de las más conocidas, es compatible con cualquier sistema operativo Windows, Mac y iPhone. Esta aplicación es soportada en idioma inglés.

Cubre con la configuración de protección y control de acceso a sitios WEB, aplicaciones, contenidos, protección de malware. Además, posee un sistema de comprobación de páginas web que se llama DRTR (Dynamic Real-Time Racting) esta herramienta válida la clasificación que contiene a través de internet la página y su contenido.

La configuración de esta aplicación es también sencilla se inicia con el ingreso a la página http://www1.k9webprotection.com/; se selecciona descargar, ahí configuramos la cuenta con la cual vamos a tener la administración del portal web para el monitoreo de acciones en los dispositivos que se configuren.

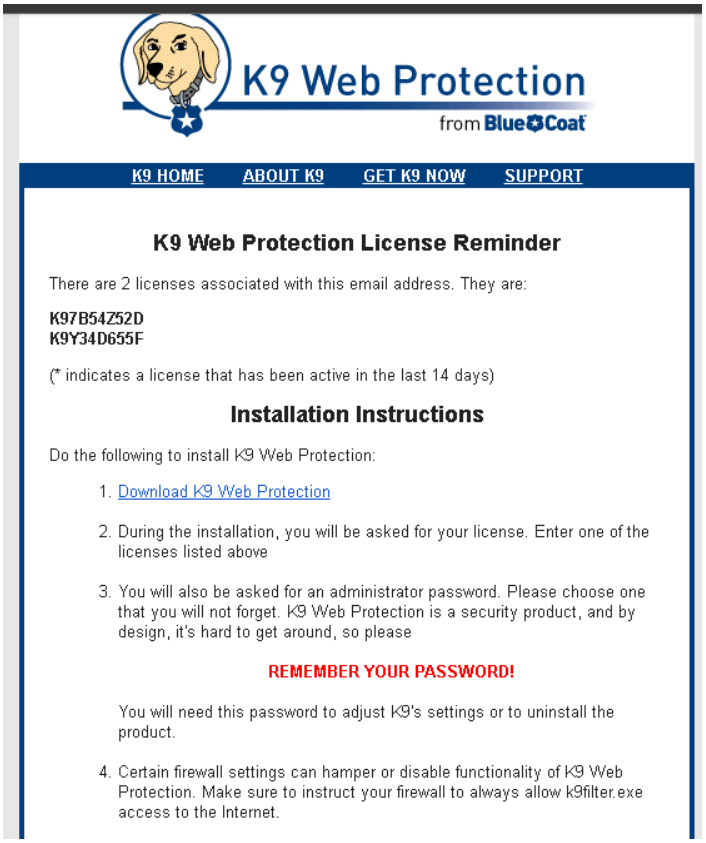
Con unos pocos datos ya tenemos acceso a un correo de confirmación el cual nos brinda una licencia de uso (Gratis o Paga).

Fig. 20. K9webprotection

Fuente:http://www1.k9webprotection.com/get-k9-web-protection-free

Se recibe un correo el cual contiene la información de licencia, instrucciones para descarga y un link para el soporte

Fig. 21. K9webprotection 2



Fuente: El autor.

Al iniciar la instalación aparece una ventana donde se incluye la licencia y clave de configuración del portal, unas ves se ingresan al portal con la clave predestinada, aparece el menú de configuración donde se puede encontrar todos los eventos que se realizan en el computador.

Fig. 22. K9webprotection 3

Fuente: El autor

Se puede bloquear por categorías y niveles de seguridad, donde se explican los contenidos bloqueados, contiene un buen número de configuraciones fáciles de aplicar y entender. También posee tiempo de permitido de navegación y uso, donde se puede bloquear el acceso a páginas web durante el tiempo predeterminado. Aplicación de permisos a ciertas páginas web, contiene un filtro para contenido de YouTube, toda esta aplicación se configura para recibir notificaciones a través de correo electrónico.

Fig. 23. K9webprotection 4

Fuente: El autor.

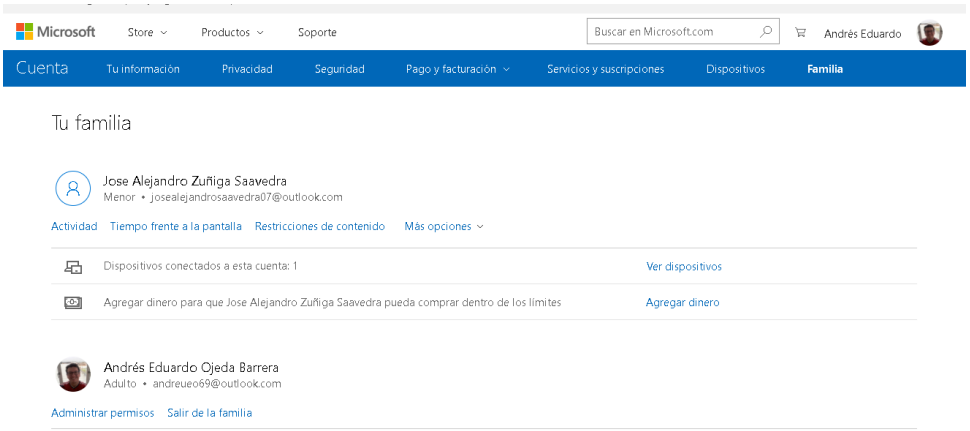
10.4. WINDOWS LIVE FAMILY SAFETY.

Fuente: https://account.microsoft.com/account/ManageMyAccount?refd=familysafety.live.com&ru=https%3A%2F%2Faccount.microsoft.com%2Ffamily%3Frefd%3Dfamilysafety.live.com&destrt=FamilyLandingPage

Microsoft como el grande de la informática también está haciendo pinos en prestar un servicio a través de su sistema operativo de seguridad de acceso, control de actividades en el equipo, tiempo de uso y bloqueo de aplicaciones, juegos y sitios web.

Se puede integrar a través de una cuenta en Outlook con perfil de menor de edad o hijo, a su cuenta de correo personal, llegan correos informando la actividad realizada en el equipo, se puede realizar restricciones, restricción de tiempo de acceso frente a la pantalla, restricciones de contenido.

Fig. 24. Windows live family safety

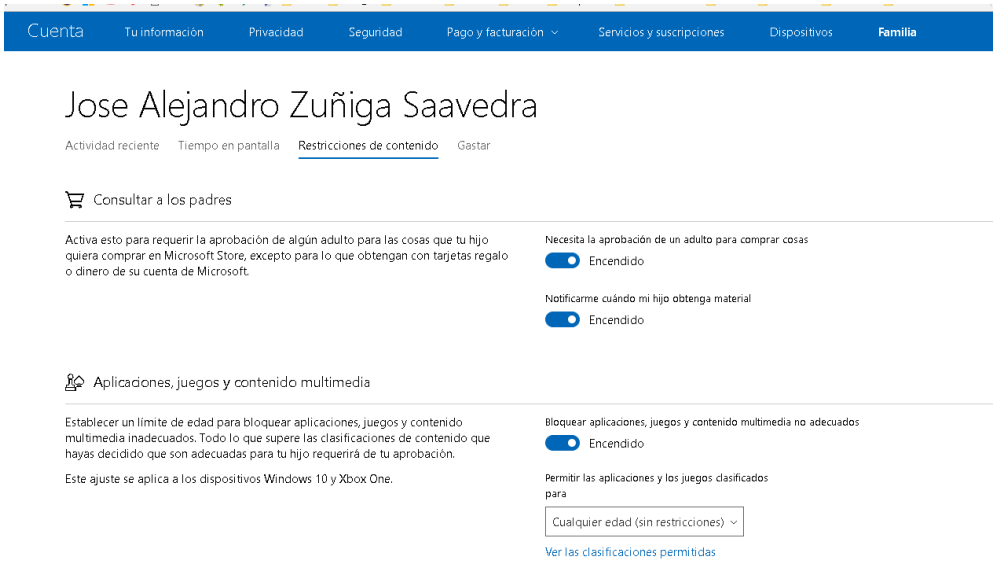


Fuente: https://account.microsoft.com/family/

Es menos restrictivo que las anteriores aplicaciones, pero trabaja y cumple con su cometido de seguridad, además Microsoft está creciendo en este tipo de aplicaciones; ya que solamente presta el servicio para equipos con sistema operativo Windows.

El menú de configuración también es muy fácil de configurar y brinda la información clara de que se está aplicando al equipo.

Fig. 25. Windows live family safety 2



Fuente: El autor

11. PERFIL DEL ABUSADOR DE NIÑOS.

Estos delincuentes que operan actualmente en las redes sociales actúan engañando a las víctimas dándose a conocer como posibles amigos del mismo colegio donde estudian o amigos de sus amigos con intereses similares y logran acercarse a los menores para chantajearlos y abusar de ellos.

Comienzan enviando solitudes de amistad de otra aparente niña o viceversa por la red social y se gana su confianza teniendo aparentemente cosas en común puesto que su primer objetivo es generar empatía con los niños, chatean durante aproximadamente un mes y al presenciar un acercamiento comienza a pedirles fotos de índole sexual para después proceder al chantaje y poder llegar al abuso presencial, este es un típico caso del delito grooming que basándose en técnicas de ingeniería social se gana la confianza de la víctima para después explotar sexualmente al menor.

Las denuncias se han extendido a medida que el uso de las nuevas tecnologías también se ha globalizado y los niños tienen un mayor acceso a estas, a través del CAI Virtual de la policía han llegado 24 denuncias por grooming en el transcurso del año, al 1 de junio de 2015 se bloquearon 1.677 página web por contenido de pornografía infantil.

Es imposible definir un solo perfil delictivo de un abusador en línea de niños en línea solo se puede hablar de rasgos que estos posiblemente mantengan en común:

- Acceso a las redes sociales
- Conocimientos básicos de tecnología en cuanto al manejo del computador el acceso a internet y redes.
- Tiene muy marcada una inmadurez emocional y psicológica.
- Es posible que estos sean víctimas de abusos perpetrados en su niñez
- Exposición a relaciones de carácter abusivo.
- Son personas que se caracterizan por una inseguridad en sí mismos y tienen tendencia a tener carácter explosivo.
- Es muy frecuente que estos se encuentren en el ambiente del niño ya sea familiar, escolar, vecindario, pero por lo regular conocen el ambiente de desempeño del menor.

Actualmente se habla de dos tipos de abusador los cuales son los siguientes:

Abusadores de carácter pedófilo:

En esta categoría se destacan los abusadores de un carácter obsesivo que perpetran distintos abusos fuera de su entorno familiar con distintos menores de manera compulsiva y generando un patrón de comportamiento crónico y repetitivo, generalmente este tipo de abusadores no tienen relaciones adultas porque tienen un gusto maléficamente desarrollado hacia los menores, por lo general al momento de ejecutar el abuso tienen a usar la manipulación y la violencia, cuando los niños son contactados por redes sociales se enfocan en aquellos que muestren carencias afectiva, económicas y emocionales.

Abusadores de carácter Regresivo:

Este tipo de abusador se caracteriza por ejecutar abusos dentro de su entorno familiar y sus explosiones abusivas se destacan al tener una crisis de pareja o familiar, estos si tienen relaciones con adultos y pueden ser estables, pero generan su conducta regresiva en estas crisis y tienden a repetir estas.

Y el resto es una incógnita puesto que cualquier persona se puede delatar en un instante como posible abusador, lo que sí se puede es proteger los niños evitando que estos tengan acceso a ellos.

Y entramos en un tema muy importante sobre el porqué no es detectado el ciber delincuente abusador de los niños a tiempo, según el general de la policía salamanca influye mucho la falta de atención de los padres sobre los hijos, hoy en día a algunos padres según él les preguntan dónde están los hijos y no saben porque no hay comunicación basada en el afecto con los hijos ni dialogo permanente, el mundo se está llenando de padres distraídos en las nuevas tecnologías o inmersos en sus múltiples ocupaciones laborales para sostener el hogar por lo que se está general una individualización entré los padres y sus hijos y esto permite que al utilizar la tecnología de manera irresponsable los niños estén en expuestos a peligros, por lo cual se desarrolló la alianza con distintos países y entidades como Facebook, Yahoo! para proteger a los niños e identificar estos delincuentes.

RECOMENDACIONES.

Como recomendaciones para los niños se generan las siguientes:

- Es importante fomentar en los niños entre edades de 8 y 13 años que el uso de internet sea para fines educativos, de participación y creatividad, para que se puedan desarrollar todas las características con un ambiente sano y de aprendizaje infantil, además de apoyar la búsqueda de temas propios para el niño que le ayuden en su aprendizaje estudiantil.

- Se deben compartir responsabilidades de la seguridad en redes por ejemplo enseñarles que si son espectadores de un caso de ciberacoso no deben quedarse callados deben contarles a sus padres o al adulto encargado del niño que le está sucediendo este para efectuar las medidas urgentes de protección.

- Se les debe concientizar de respetar los límites de acceso a contenidos en internet, con mucho dialogo enseñarles sobre los peligros y por qué no deben pasar las barreras de estos, siendo así que sus padres, profesores, cuidadores deben estar siempre pendientes de sus comportamientos y conexión a la red.

- Es importante ejecutar estrategias que antecedan a los peligros y protejan a los niños ejecutando el bloqueo de mensajes y contenidos no deseados, además de contactos que no sean convenientes y ejecutando herramientas de protección, por ejemplo Facebook está terminando de desarrollar un área para Facebook de niños donde estos van a ser debidamente monitoreados, van a tener iconos de emociones acordes a su edad y se restringe muchos contenidos visuales en el sector infantil, incluyendo anuncios y contenidos que no deben estar activos para los niños.

- La comunicación y confianza eficiente es muy importante para enseñarles y recalcarles a los niños que lo primero que deben hacer en caso de sufrir un acoso por parte de cualquier adulto avisar y buscar la ayuda de uno de sus padres inmediatamente.

- Es importante revisar la configuración de seguridad del pc que utiliza el niño, además de no compartir información personal con desconocidos, ni se deben publicar tantas imágenes de los menores en redes.

- Se deben realizar evaluaciones con herramientas que permitan denunciar en caso de riesgo y enseñarle su uso a los niños, como es la aplicación que actualmente funciona en acompañamiento con la policía como es PROTECTIO, o la página web te protejo sensibilizarlos de la importancia de su uso.

- Según el ministerio de las TIC el gobierno colombiano a adoptado como estrategia para el manejo de ciberabuso en menores el modelo WEProtect con el cual invita a los padres a denunciar estos casos mediante la plataforma establecida, además de adoptar medidas como son la configuración completa de los perfiles de seguridad de los niños para el correcto manejo de la privacidad de ellos.

- Es importante informarse en la página del ministerio de las Tic sobre temas como el ciberacoso y abuso sexual a través de las redes en la página https://www.enticconfio.gov.co/actualidad/ciberacoso están disponibles diferentes videos y temas informativos.

CONCLUSIONES.

Al realizar la documentación de información sobre las técnicas de ingeniería social utilizadas para la ejecución de actividades delictivas en menores entre los 8 y 13 años en Colombia se ve la necesidad de generar ciertas prácticas para protegerlos de los atacantes cibernéticos, como primera medida se debe establecer un plan de concientización hacia los padres de familia sobre la importancia del uso adecuado de las herramientas tecnológicas, del no abandonar sus hijos por el trabajo y auto remplazarse con computadoras y celulares durante el transcurso de los años de los menores, el mal uso de las redes sociales en la temprana edad conlleva a exponer la integridad física y psicológica de los menores y por ende de toda la familia, tampoco se debe extremar al punto de alejar a los niños del uso de internet porque también es un recurso que es muy valioso como herramienta de educación pero todo debe ser en la medida en que los padres de familia estén pendientes de sus hijos y los acompañen en su diario vivir, de ahí los valores que deben ser enseñados a los menores los cuales deben infundirse como raíces para que ellos aprendan a tener su propia integridad ante cualquier evento.

Se debe establecer herramientas de protección en los Pc usados por los niños y en los celulares, utilizando herramientas como PROTECTIO, la página web te protejo y lo más importante estar muy pendientes de los niños, es muy importante que se ejecuten medidas de protección puesto que según las fuentes consultadas como el centro cibernético policial, el bienestar familiar y la red paz cada día va en aumento estas actividades delictivas sobre los menores tan solo entre el 2016 y el año 2015 se registró un aumento en más de 40 por ciento de estas denuncias sobre delitos

como pornografía infantil, violación de datos personales, extorsión, basándose en actitudes delictivas como grooming, sexting y ciberacoso, las cuales se pueden evitar si se establecen los parámetros correspondientes de seguridad informática, se informa a los menores de los medios que tienen para denunciar al igual que los padres y se les concientiza de los peligros latentes a los que están expuestos diariamente en las redes si no hacen de ellas un lugar de uso educativo y positivo para su desarrollo.

En los ataques de ingeniería social se utilizan diferentes técnicas como la interacción activa y la pasiva con la víctima además del manejo psicológico que se le da a esta para obtener la persuasión necesaria para ejecutar el ataque, es importante que se establezcan las medidas necesarias de acompañamiento con los menores para que el riesgo de estos de caer en manos delincuenciales sea mínimo.

Existen dos tipos de perfiles de abusadores de menores, los de carácter pedófilo y regresivo y tienen diferente forma de actuar y es ahí donde lo más importante es evitar su aproximación a los menores restringiendo el contacto totalmente a ellos por esto hay que estar pendiente del manejo en redes sociales puesto que los principales perfiles para ellos ataca son los niños con carencias afectivas y económicas.

DIVULGACION.

El presente proyecto de Monografía para el grado de la especialización en seguridad informática desarrollada en la UNAD, será expuesto en el repositorio de la universidad nacional abierta y a distancia UNAD, y quedará al servicio de la comunidad para fines educativos, además se enviará por el entorno de seguimiento y evaluación para que sea evaluado para la materia proyecto de grado 2 y se publica en el foro de opciones de grado Para la revisión del director de proyecto.

BIBLIOGRAFIA.

O,.UBORGHELLO, C. (2009). *El arma infalible: la Ingeniería Social.* Latinoamerica. Disponible en: (http://s3.amazonaws.com/academia.edu.documents/43527639/arma_infalible_ingenieria_social.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1494355037&Signature=Wfw%2FYSy18B2FnATerHEU7mcUfQc%3D&response-content-disposition=inline%3B%20filename%3DEl_arma_infa).

(2015). *Ciberacoso de niños, niñas y adolescentes en las redes sociales: un estudio sobre los sistemas de protección y prev*).

PÉREZ, A. G. (2008). *Perfiles Criminales en el Ámbito de la Cibercriminalidad Social.* España. Disponible en: (http://www.skopein.org/ojs/index.php/1/article/view/95/88).

PUJOL, F. A. (2015). *Detección automática de ciberbullying a través del procesamiento.* Universidad de alicante, España. Disponible en: (https://rua.ua.es/dspace/bitstream/10045/64300/1/Psicologia-y-educacion_288.pdf).

RICO, M. N. (2014). *Derechos de la infancia en la era digital.* America Latina: CEPAL. Disponible en:

(http://repositorio.cepal.org/bitstream/handle/11362/37139/S1420568_es.pdf?sequence=1&isAllowed=y).

JOSE, B. M. (2014). *Conductas de ciberacoso en niños y adolescentes.* España. Disponible en: (file:///C:/Users/latitude/Downloads/287060-396455-1-PB%20(1).pdf).

MONTIEL, I. (2016). *Cibercriminalidad social juvenil: la cifra negra.* España. Disponible en: (http://www.redalyc.org/html/788/78846481008/).

ENRIQUE, C. (2013). *VICTIMIZACIÓN INFANTIL SEXUAL ONLINE:.* Valencia. Disponible en: (https://www.researchgate.net/profile/Irene_Montiel/publication/275273999_Victimizacion_Infantil_Sexual_Online_Online_Grooming_Ciberabuso_y_Ciberacoso_sexual/links/553692660cf268fd001870be/Victimizacion-Infantil-Sexual-Online-Online-Grooming-Ciberabuso-y-C).

FERNANDO, M. P. (2012). *MEDIDAS DE PROTECCIÓN INFORMÁTICA PARA EVITAR EL ROBO DE.* Ecuador. Disponible en: (file:///C:/Users/latitude/Downloads/Tesis_t728si.pdf).

CARLOS, L. (2015). *Ciber-acoso en niñas y niños.* Atlantico. Disponible en: (http://sedici.unlp.edu.ar/bitstream/handle/10915/59753/Documento_completo.pdf-PDFA.pdf?sequence=1)

ANEXO A.

RESUMEN ANALITICO ESPECIALIZADO R.A.E.

TEMA	Ingeniería Social
TÍTULO	Ingeniería social utilizada en el abuso de infantes a través de las redes sociales en Colombia
AUTORES	Ivonne Milena Barbosa López Andrés Eduardo Ojeda Barrera
FUENTES BIBLIOGRÁFICAS	O,.UBORGHELLO, C. (2009). El arma infalible: la Ingeniería Social. Latinoamérica. Disponible en: (http://s3.amazonaws.com/academia.edu.documents/43527639/arma_infalible_ingenieria_social.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1494355037&Signature=Wfw%2FYSy18B2FnATerHEU7mcUfQc%3D&response-content-disposition=inline%3B%20filename%3DEl_arma_infa). (2015). Ciberacoso de niños, niñas y adolescentes en las redes sociales: un estudio sobre los sistemas de protección y prev). PÉREZ, A. G. (2008). Perfiles Criminales en el Ámbito de la Cibercriminalidad Social. España. Disponible en: (http://www.skopein.org/ojs/index.php/1/article/view/95/88). PUJOL, F. A. (2015). Detección automática de ciberbullying a través del procesamiento. Universidad de alicante, España. Disponible en: (https://rua.ua.es/dspace/bitstream/10045/64300/1/Psicologia-y-educacion_288.pdf). RICO, M. N. (2014). Derechos de la infancia en la era digital. América Latina: CEPAL. Disponible en: (http://repositorio.cepal.org/bitstream/handle/11362/37139/S1420568_es.pdf?sequence=1&isAllowed=y). JOSE, B. M. (2014). Conductas de ciberacoso en niños y adolescentes. España. Disponible en: (file:///C:/Users/latitude/Downloads/287060-396455-1-PB%20(1).pdf). MONTIEL, I. (2016). Cibercriminalidad social juvenil: la cifra negra. España. Disponible en: (http://www.redalyc.org/html/788/78846481008/). ENRIQUE, C. (2013). VICTIMIZACIÓN INFANTIL SEXUAL ONLINE:. Valencia. Disponible en: (https://www.researchgate.net/profile/Irene_Montiel/publication/275273999_Victimizacion_Infantil_Sexual_Online_Online_Grooming_Ciberabuso_y_Ciberacoso_sexual/links/553692660cf26

	8fd001870be/Victimizacion-Infantil-Sexual-Online-Online-Grooming-Ciberabuso-y-C). FERNANDO, M. P. (2012). MEDIDAS DE PROTECCIÓN INFORMÁTICA PARA EVITAR EL ROBO DE. Ecuador. Disponible en: (file:///C:/Users/latitude/Downloads/Tesis_t728si.pdf). CARLOS, L. (2015). Ciber-acoso en niñas y niños. Atlántico. Disponible en: (http://sedici.unlp.edu.ar/bitstream/handle/10915/59753/Documento_completo.pdf-PDFA.pdf?sequence=1)
AÑO	2018
RESUMEN	La globalización del internet y la llegada de este a los hogares hace que los niños tengan un acceso regular a este, al navegar sin la supervisión necesaria de los cuidadores, sin la seguridad ni protección ellos entran como en un vecindario cibernético donde acceden a muchos sitios y esto los hace vulnerables por su propia inocencia no tienen el sentido de desconfianza para detectar depredadores cibernéticos al igual que pasa en el mundo real con los delincuentes, por lo cual se decide desarrollar esta monografía de investigación sobre las diferentes técnicas de ingeniería social usadas por los ciber delincuentes en Colombia para lograr detectar las técnicas de ingeniera social aplicadas por los abusadores de menores entre los 8 y 13.
PALABRAS CLAVES	Ingeniería social, Grooming, Sexting, Delincuente, Delito, Deep Web.
CONTENIDOS	Monografía de investigación sobre las diferentes técnicas de ingeniería social usadas por los ciber delincuentes en Colombia para lograr detectar las técnicas de ingeniera social aplicadas por los abusadores de menores entre los 8 y 13.
DESCRIPCION DEL PROBLEMA	Análisis relacionado con la problemática del uso de técnicas de ingeniería social para el abuso infantil en las redes en Colombia.
OBJETIVOS	OBJETIVO GENERAL: Estudiar las técnicas de ingeniería social utilizadas en las redes que afectan la seguridad infantil en Colombia, analizar como la seguridad informática puede contribuir y dar posibles soluciones para mejorar la seguridad de los infantes colombianos ante posibles peligros de abusos cibernéticos en Colombia. OBJETIVOS ESPECÍFICOS.

	Conocer la información en red sobre las técnicas de ingeniería social y como se están aplicando para ejecutar el abuso en redes en menores entre los 8 y 13 años en Colombia. • Analizar como la seguridad informática puede contribuir y dar posibles soluciones mediante procedimientos, programas e instrucciones que se están llevando a cabo en cuanto a software para implementar medidas de seguridad infantil, usando la recopilación de información en red y entrevistas a entidades que manejen la seguridad infantil. • Determinar medidas claras que permitan definir perfiles de posibles criminales y detección temprana de estos para evitar acercamiento con los niños.
METODOLOGÍA	La investigación se desarrolla en el transcurso de 5 meses del segundo semestre del año 2017, esta monografía está dirigida al estudio de las técnicas de ingeniería social utilizadas para el abuso de infantes a través de las redes sociales en Colombia.
PRINCIPALES REFERENTES TEÓRICOS	Se investigara la información en red sobre cómo se está aplicando estas técnicas para el abuso en redes en menores entre los 8 y 13 años en Colombia y además dar posibles soluciones mediante procedimientos, programas e instrucciones que se están llevando a cabo en cuanto a software para implementar medidas de seguridad infantil.
PRINCIPALES REFERENTES CONCEPTUALES	**Ingeniería social**: se basa en obtener información mediante técnicas de manipulación de las personas. **Grooming:** Son una serie de conductas donde un adulto se gana la confianza de un menor de edad. **Sexting:** Se refiere al envío de mensajes de carácter sexual a través, chats y redes sociales. **Delincuente**: Persona que realiza diferentes actos en contra de la ley para que exista un delito. **Delito:** Acción en contra de la ley realizada a través de internet, redes. **Deep Web:** O internet profunda es el contenido de la red que no está a la vista de todos los usuarios.
RESULTADOS	• Es importante ejecutar estrategias que antecedan a los peligros y protejan a los niños ejecutando el bloqueo de mensajes y contenidos no deseados, además de contactos que no sean convenientes y ejecutando herramientas de protección. • Se deben realizar evaluaciones con herramientas que permitan denunciar en caso de riesgo y enseñarle su uso a los niños, como es la aplicación que actualmente funciona en

	acompañamiento con la policía como es PROTECTIO, o la página web te protejo sensibilizarlos de la importancia de su uso. • Según el ministerio de las TIC el gobierno colombiano a adoptado como estrategia para el manejo de ciber abuso en menores el modelo WEProtect con el cual invita a los padres a denunciar estos casos mediante la plataforma establecida, además de adoptar medidas como son la configuración completa de los perfiles de seguridad de los niños para el correcto manejo de la privacidad de ellos.
CONCLUSIONES	En los ataques de ingeniería social se utilizan diferentes técnicas como la interacción activa y la pasiva con la víctima además del manejo psicológico que se le da a esta para obtener la persuasión necesaria para ejecutar el ataque, es importante que se establezcan las medidas necesarias de acompañamiento con los menores para que el riesgo de estos de caer en manos delincuenciales sea mínimo. Existen dos tipos de perfiles de abusadores de menores, los de carácter pedófilo y regresivo y tienen diferente forma de actuar y es ahí donde lo más importante es evitar su aproximación a los menores restringiendo el contacto totalmente a ellos por esto hay que estar pendiente del manejo en redes sociales puesto que los principales perfiles para ellos ataca son los niños con carencias afectivas y económicas.