

PROBLEMAS DE INGENIERÍA SOCIAL Y SU IMPACTO EN LA ADOLESCENCIA
COLOMBIANA

CAROLINA MONTES AGUDELO
VIVIANA ROCIO VARGAS FORERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
FACULTAD CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C
2018

PROBLEMAS DE INGENIERÍA SOCIAL Y SU IMPACTO EN LA
ADOLESCENCIA COLOMBIANA

CAROLINA MONTES AGUDELO
VIVIANA ROCIO VARGAS FORERO

MONOGRAFÍA PARA OPTAR AL TÍTULO DE
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

DIRECTOR DEL PROYECTO
HERNANDO JOSÉ PEÑA HIDALGO
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
FACULTAD CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C
2018

Nota de aceptación:

Firma del presidente del jurado

Firma del jurado

Firma del jurado

Bogotá D.C., 04 noviembre de 2018

DEDICATORIA

Dedicamos este trabajo a Dios por permitirnos lograr uno de tantos logros propuestos y así mismo le damos gracias a nuestras familias por acompañarnos en todo este proceso, estando presentes en cada esfuerzo por culminar nuestras metas y animarnos a cumplirlas con amor y dedicación.

CONTENIDO

	pág.
TÍTULO DEL PROYECTO	9
INTRODUCCIÓN	3
1. DEFINICIÓN DEL PROBLEMA.....	4
1.1. DESCRIPCIÓN	4
1.2. FORMULACIÓN DEL PROBLEMA.....	4
2. JUSTIFICACIÓN	5
3. OBJETIVOS.....	6
3.1. OBJETIVO GENERAL	6
3.2. OBJETIVOS ESPECÍFICOS	6
4. MARCO REFERENCIAL.....	7
4.1. MARCO TEÓRICO	7
4.2. MARCO CONCEPTUAL	9
4.3. MARCO HISTÓRICO.....	10
4.4. ESTADO ACTUAL	12
5. DISEÑO METODOLOGICO.....	13
5.1. TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN	14
5.2. CUANTITATIVAS.....	14
6. METODOLOGIA PARA DESARROLLAR OBJETIVOS	16
6.1. REALIZAR UN ANÁLISIS DE LOS ESTUDIOS Y ANTECEDENTES EXISTENTES EN COLOMBIA SOBRE LOS RIESGOS DE LOS ADOLESCENTES FRENTE A LA INGENIERÍA SOCIAL	16
6.2. REALIZAR UN ANÁLISIS SOBRE LOS MÉTODOS, TÉCNICAS Y TÁCTICAS DE SEGURIDAD PROPUESTAS POR ORGANIZACIONES DEDICADAS A LA SEGURIDAD EN COLOMBIA, PARA CONOCER SU GRADO DE EFICIENCIA, EFICACIA Y EFECTIVIDAD.	21
6.3. REALIZAR UN ANÁLISIS DE LOS RESULTADOS DE ATAQUES DE INGENIERÍA SOCIAL POR EL MANEJO INADECUADO DE DATOS PERSONALES, EN LAS REDES SOCIALES POR PARTE DE ADOLESCENTES EN COLOMBIA.....	29

7.	CONCLUSIONES	40
8.	RECOMENDACIONES	41
9.	DIVULGACIÓN	42
	REFERENCIAS BIBLIOGRÁFICAS.....	43
	ANEXO 1. RESUMEN ANALÍTICO EN EDUCACIÓN - RAE.....	46

LISTA DE TABLAS

	pág.
Tabla 1. Metodología de Investigación	13
Tabla 2. Técnica cuantitativa – Variables	14
Tabla 3. (Continuación).....	15
Tabla 5. Evolución de la Ingeniería Social	30
Tabla 6. Tabla Promedio vulnerabilidad por la Ingeniería Social en Colombia	38

LISTA DE ILUSTRACIONES

pág.

Ilustración 1. Estadísticas de Incidentes informáticos del 2014 al 2017	17
Ilustración 2. Ingeniería Social Adolescentes - Año 2013	31
Ilustración 4. Ingeniería Social Adolescentes - Año 2014	32
Ilustración 5. Ingeniería Social Adolescentes - Año 2015	33
Ilustración 6. Ingeniería Social Adolescentes - Año 2016	34
Ilustración 7. Ingeniería Social Adolescentes - Año 2018	35
Ilustración 8. Resultados de los Ataques de Ingeniería Social	36
Ilustración 9. Promedio vulnerabilidad por la Ingeniería Social en Colombia.....	38

TÍTULO DEL PROYECTO

Problemas de ingeniería social y su impacto en la adolescencia colombiana.

INTRODUCCIÓN

Esta monografía presenta un análisis de los problemas a los que se ven abocados los adolescentes a causa de la ingeniería social, en el contexto de las actuales costumbres del manejo de las redes.

La falta de conocimiento en seguridad informática hace que se vean expuestos a gran cantidad de amenazas y riesgos. Por esto se describirá un análisis de esta problemática social en los adolescentes y a su vez el planteamiento de estrategias o recomendaciones que pueden llegar a evitar o minimizar el daño en la sociedad y en las generaciones futuras.

La información que un adolescente sube a las redes sociales divulga información personal acerca de:

- Donde vive
- Cuáles son sus traslados frecuentes
- Cuáles son sus lugares favoritos
- Donde estudia
- Cuáles pueden ser sus contraseñas de redes sociales
- Publicación de fotografías que pueden ser utilizadas para dañar o vulnerar su integridad

Esta monografía se realiza para definir estrategias y prevenir la exposición de esta información personal de los niños y adolescentes entre los 11 a 17 años en Colombia.

1. DEFINICIÓN DEL PROBLEMA

1.1. DESCRIPCIÓN

Respecto a la información cada día se genera más datos a comparación de otros años, se está en plena evolución rompiendo esquemas de seguridad de la información y creando todos los días millones de datos, los cuales están a la merced de amenazas por el volumen y desproporción de crecimiento en la generación de tecnologías avanzadas.

Por la facilidad que las personas tienen con respecto a los dispositivos para la utilización de la información, pues todo lo que ellos quieren está al alcance de un clic en sus dispositivos móviles y también por todas aquellas facilidades de almacenamiento como la nube.

Los adolescentes de esta nueva generación están creados de tal forma que todo lo relacionado con las nuevas tecnologías es sin duda una de sus grandes aficiones y son generadores de datos sin ninguna seguridad de la información y control.

En la actualidad es poca la implementación y aún falta más socialización acompañada de metodologías adecuadas para el manejo responsable de esta información que evoluciona todos los días, esto sin garantizar la privacidad de los datos personales.

Uno de tantos fenómenos que se ve en la actualidad con respecto al manejo de las redes sociales es en un horario de descanso escolar en un colegio, generando gran cantidad de información, pues se evidencia que pueden existir más de 200 dispositivos tecnológicos conectados al mismo tiempo. Esto no se veía en otros tiempos pues la forma de acceder a dichos dispositivos era limitada para las empresas o las personas que tenían medios económicos altos para la adquisición de estos.

Es así como vemos que cada día los adolescentes se ven expuestos al robo de sus datos confidenciales, por medio de criminales disfrazados de usuarios corrientes que no generarían ninguna amenaza aparente, pero están expuestos a abusos y riesgos que pueden llegar a ser fatales.

1.2. FORMULACIÓN DEL PROBLEMA

¿Cómo identificar los riesgos de la ingeniería social en el uso de redes sociales por parte de los niños y adolescentes entre los 11 a 17 años en Colombia?

2. JUSTIFICACIÓN

En Colombia cada día se evidencian más casos de adolescentes víctimas de la ingeniería social, pues se ven inmersos en este medio de comunicación el cual conocen desde pequeños y como nativos digitales creen que no es necesario tener restricciones o controles al utilizar las redes sociales.

Es cierto que internet es una herramienta muy poderosa para los adolescentes quienes lo utilizan para la adquisición de nuevo conocimiento, pero a su vez es un arma que puede ocasionar mucho daño; Existen jóvenes que no tienen en cuenta la implementación de suficientes restricciones en sus datos personales, fotografías, ubicación, intereses entre otros y esta información están a la merced de delincuentes informáticos, acosadores o en algunos casos de sus propios compañeros que hacen que esta información se vuelva en contra de ellos afectando su autoestima.

Existen muchos sitios en internet que fomentan la bulimia, la violencia, el racismo, la depresión, el suicidio, la autolesión, la anorexia los trastornos bipolares en los adolescentes y un sinnúmero de problemas que hacen que sea necesario concientizar y crear campañas de prevención con respecto a la ingeniería social.

Para los inmigrantes digitales con respecto a la tecnología hacía que fueran más precavidos en su utilización y la información que se manejaba en los medios, pero para los nativos digitales es tan simple como mentir respecto a su edad para acceder a información u obtener acceso a contenidos específicos para adultos.

Al realizar esta monografía con un trabajo de investigación según problemáticas actuales en una población tan vulnerable como los adolescentes, aportamos con nuestro análisis en la búsqueda de soluciones o estrategias que aminoren estos riesgos en los adolescentes.

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Proponer Estrategias para disminuir el riesgo de la ingeniería social en el uso de redes sociales por parte de los niños y adolescentes entre los 11 a 17 años en Colombia.

3.2. OBJETIVOS ESPECÍFICOS

- Realizar un análisis de los estudios y antecedentes existentes en Colombia sobre los riesgos de los adolescentes frente a la ingeniería social.
- Realizar un análisis sobre la metodología técnica y táctica de seguridad propuesta por organizaciones dedicadas a la seguridad en Colombia para conocer su grado de eficiencia, eficacia y efectividad.
- Realizar un análisis de los resultados de ataques de ingeniería social por el manejo inadecuado de datos personales, en las redes sociales por parte de adolescentes en Colombia.

4. MARCO REFERENCIAL

Se escribirá una referencia respecto a la problemática de la ingeniería social dirigido a jóvenes que se encuentren en las edades entre los 11 a 17 años en Colombia, en cuanto a la forma inapropiada de la utilización de las redes sociales, el cual nos soportaremos con investigaciones relacionadas a esta problemática, para así contribuir y encontrar una solución o mejoramiento de lo planteado en el presente proyecto, bajo el Marco Teórico y Marco Conceptual.

4.1. MARCO TEÓRICO

De acuerdo con lo investigado y antecedentes analizados respecto al planteamiento del proyecto, se establece que esta problemática sucede a nivel mundial y por diversos factores sociales, ya sean económicos, psicológicos y sociales.

Hoy en día tener acceso a las redes sociales es sencillo, sin embargo, tiene ventajas y desventajas, por esta razón se hace necesario el acompañamiento y supervisión de los padres de familia, los profesores y cualquier persona cercana que pueda ejercer control sobre las actividades que realiza un adolescente en el uso de las redes sociales.

Según la investigación realizada por la Universidad de Politécnica de Madrid, en un proyecto de grado denominado "ESTUDIO DE LAS TÉCNICAS DE LA INGENIERÍA SOCIAL USADAS EN ATAQUES DE CIBERSEGURIDAD Y ANÁLISIS SOCIOLÓGICO", analizan las técnicas más utilizadas de los atacantes y se puede evidenciar que los adolescentes menores a 18 años están más expuestos por su inocencia e inexperiencia.

Además, se investiga acerca de los tipos de ataque, como el de tipo social denominada Phishing, dichos ataques se realizan a través de transferencia de archivos, archivos adjuntos en correos o chat, estos tipos de ataque es un desarrollo de la investigación realizada por la Universidad de Politécnica Salesiana en una tesis denominada "ESTUDIO Y ANALISIS DEL USO DE LAS REDES SOCIALES EN LA CIUDAD DE CUENCA Y ELABORACIÓN DE UN MANUAL DE BUENAS PRÁCTICAS"

Una vez analizada la información de diferentes investigaciones referenciadas en este proyecto, se llega a la propuesta de proponer estrategias para disminuir el riesgo de la ingeniería social en el uso de redes sociales por parte de los niños y adolescentes entre los 11 a 17 años en Colombia.

Según los datos recopilados podemos realizar algunas recomendaciones propias para el manejo de dicha problemática así:

- Advertir a los adolescentes de los peligros a los que pueden estar expuestos en las redes sociales.
- Comparar cómo ha evolucionado los riesgos del manejo de datos personales, en las redes sociales.
- Analizar cuáles son los métodos de seguridad que los adolescentes conocen y a su vez aplican para no verse expuestos a amenazas en la red.
- Sugerir a los padres de familia la utilización de herramientas de control que pueden implementar para garantizar la seguridad cuando sus hijos manejan las redes sociales.
- Basar los conceptos que ya existen en Colombia sobre los riesgos de los adolescentes con respecto a la ingeniería social.
- Concientizar a los adolescentes de la necesidad de limitar el tipo de información que comparten en la red.
- Mostrar a los adolescentes que las acciones en internet pueden tener consecuencias, si no se tienen las debidas precauciones.

Cuál es el nivel de aplicabilidad de la teoría identificada al desarrollo del proyecto.

Respecto a la teoría y al desarrollo del proyecto, será aplicada frente a las personas que consulten esta monografía y de cómo podemos aportar recomendaciones, opiniones críticas, frente algunas falencias que posee actualmente los entes que controlan esta problemática con los adolescentes. Pues estos se exponen a manejar de forma inapropiada las redes sociales, llegando a ser víctimas de grooming, cyberbullying, sexting y gossip, con el propósito fomentar un precedente ante estas circunstancias con el fin de evitar hechos posteriores para el manejo adecuado de los datos.

4.2. MARCO CONCEPTUAL

Descripción de conceptos asociados a la ingeniería social o a los problemas que pueden surgir de esta problemática.

- **Ingeniería social:** Se conoce donde los ciber-delincuentes convencen a sus víctimas para que realicen ciertas acciones, vulnerando la seguridad, accediendo a información personal o privada de la víctima.
- **Grooming:** Se refiere a la importunación que realiza una persona adulta con el propósito de fundar e influenciar a un menor de edad ya sea un niño, o un adolescente con el fin de profanarlo o abusarlo sexualmente.
- **Ciberbullying o ciberacoso:** Se considera este tipo de manifestación ofensas, blasfemias, coacciones que realizan, adolescentes o menor frente a los mismos jóvenes.
- **Sexting:** Radica en la realización de un envío de fotos o videos sexuales originados por el remitente a través de vía celular el cual los envía a distintas personas con el fin de que sea divulgado y utilizado en contra de la persona que primeramente efectuó el envío.
- **Gossip:** Son las murmuraciones en la red que pueden ser muy perjudiciales, ya que los rumores pueden ser propagados a gran velocidad y afectar a muchas personas, que no pueden hacer nada para defenderse.
- **Nativos Digitales:** Se utiliza este término a los menores y jóvenes en la etapa de nacimiento que corresponde al año 1980 a la presente época, que se les ha facilitado adaptarse con mayor agilidad a la vanguardia de las tecnologías.
- **Inmigrantes Digitales:** Se utiliza este término a los adultos que han nacido antes del año 1980, y les ha sido más difícil adecuarse a las nuevas tecnologías.
- **Pedófilo:** Se utiliza para identificar a las personas mayores de edad que poseen inclinación sexual hacia los menores de edad manteniendo fantasías sexuales con esta población.
- **Pederasta:** Se utiliza para identificar a los delincuentes mayores de edad que abusan sexualmente de los menores de edad.

4.3. MARCO HISTÓRICO

Respecto a la problemática planteada se ha investigado antecedentes de estudios que han efectuado distintas entidades relacionados con el tema de la problemática evidenciados en revisión y recopilación bibliográfica, así mismo se realiza un resumen de otros autores que tienen relación con el objetivo de esta investigación:

- Universidad de Castilla - La Mancha - España, una estudiante realizó un estudio de ¹Proyecto de prevención del mal uso de las nuevas tecnologías, el cual identificó adicción, dependencia y riesgos.

Diagnóstico que deben plantearse acciones preventivas en la Ciudad de Cuenca, para ³niños entre 10 y 12 años, que cursan 5º y 6º de Educación Primaria, ya que, durante esta edad, el proceso de socialización surge de la interacción entre el niño y el entorno que le rodea, sobre el uso de las tecnologías.

- Universidad de Guayaquil – Ecuador, dos estudiantes realizaron un estudio de ²Ingeniería social a través de medios informáticos, análisis de las posibles amenazas existentes en la facultad de ciencias administrativas de la universidad de Guayaquil.

Este estudio desarrolla una aplicación para la realización del análisis de datos de la ingeniería social y los ataques que pueden llegar a ocurrir en la entidades privadas y públicas, para esto fue aplicada dichas pruebas dentro de la universidad de Guayaquil (Ecuador) creando enlaces falsos, logrando así la recopilación de datos personales, datos de usuario, credenciales y cuentas bancarias para luego de una manera educativa enseñar con la capacitación todo lo referente a la correcta utilización de las políticas de seguridad en ambientes universitarios y a nivel personal.

- Estudios realizados en la página, Identidad Digital y Redes Sociales con menores, realizada por los autores Víctor Cuevas y Antonio Soria desde el año 2011, el cual fue creado este sitio para ayudar a orientar a Padres, Madres y profesores para que los adolescentes tengan conciencia de su gran responsabilidad al utilizar las redes sociales por parte, ya que

¹MARTÍNEZ, Walter. Proyecto de prevención del mal uso de las nuevas tecnologías trabajo fin de grado trabajo social [en línea]. <
<https://previa.uclm.es/bits/archivos/trabajos/ANA%20JOS%C3%89%20SERRANO%20L%C3%93PEZ.pdf>> [citado en 4 abril de 2017]

² URRUTIA, José. HERNÁNDEZ, Geovanna. Tesis de Ingeniería social a través de medios informáticos, análisis de las posibles amenazas existentes en la facultad de ciencias administrativas de la universidad de Guayaquil [en línea]. <
<http://repositorio.ug.edu.ec/handle/redug/10741f>> [citado en 8 noviembre de 2018]

evidencian que es importante y necesario enseñar a utilizar las redes sociales, especialmente los menores.

- Universidad del Azuay - Ecuador, realizó un estudio respecto a las ³REDES SOCIALES Y SU INFLUENCIA EN EL COMPORTAMIENTO DE LOS ADOLESCENTES, proyecto de grado, realizando un estudio en cuatro colegios de la Ciudad de Cuenca - Ecuador, con los alumnos de primer año de Bachillerato, el cual realizó el enfoque sobre los diferentes aspectos que influyen en el comportamiento de adolescentes y jóvenes: social, emocional, familiar y formativo, en el tema de las redes sociales y la influencia de éstas sobre la juventud y adolescencia actual., concluyendo es necesario e importante que los adolescentes aprovechen el internet para informarse y descargar programas que los ayuden a proteger sus datos, estableciendo parámetros de privacidad o de búsqueda en modo seguro; no acceder a vínculos desconocidos o sospechosos; crear una contraseña segura y cambiarla periódicamente; revisar que su cuenta quede cerrada cuando la hayan abierto en ordenadores que no son suyos; descargar aplicaciones de fuentes confiables y reconocidas; no proveer información en sitios de dudosa procedencia ni divulgar información personal; entre otras.⁴

En el entorno educativo, se recomienda crear contextos de enseñanza aprendizaje en los cuales se privilegie al trabajo en equipo, ya sea en trabajos dentro o fuera del aula, sobre todo cuando se trata del uso de internet para que el grupo no se desvíe de su objetivo principal que es el de consulta e investigación académica, pues muchas veces el alumno que trabaja solo tiende a distraerse y 79 por tanto, recurrir a páginas que no tienen que ver con la clase o incluso sitios inapropiados o riesgosos.³

³MOLINA, Gabriela. TOLEDO, Ruth. Las redes sociales y su influencia en el comportamiento de los adolescentes [en línea]. < <http://dspace.uazuay.edu.ec/bitstream/datos/3659/1/10335.PDF> > [citado en 4 abril de 2017]

⁴ TRIPTICO COMUNICACION POR REDES SOCIALES [en línea] <<https://www.slideshare.net/melany4/triptico-comunicacion-por-redes-sociales>>[citado en 4 abril de 2017]

- Universidad Don Bosco – El Salvador, un estudiante realiza un estudio de ⁵Ingeniería social, el elemento humano de la seguridad; contramedidas y planes de acción para fortalecer la seguridad en las organizaciones.

Este estudio realiza un análisis de los métodos y formas aplicadas en los ataques, sin olvidar que existe actualmente muchas técnicas y metodologías de seguridad de la información. Siendo el objetivo de este estudio identificar los mecanismos que utilizan los cibercriminales para penetrar la vulnerabilidad de las entidades y así lograr obtener la información importante de las empresas. Por esto dicho estudio sensibiliza en que el actor principal para la realización de un ataque de ingeniería social son las personas, pues ellos son el factor principal de vulnerabilidad en los ataques. Fortaleciendo así estrategias o metodologías preventivas para dicha seguridad.

- Página de Propuesta TIC, respecto a uso educativo de las redes sociales, propuesta presentada por el Eduardo Larequi, el cual presenta un proyecto respecto a ⁶“El trabajo en las aulas con servicios y aplicaciones de redes sociales educativas ofrece una serie de ventajas muy notables desde el punto de vista educativo”.

4.4. ESTADO ACTUAL

- La Policía Nacional cuenta con el proyecto del “Centro Cibernético Policial” este tiene programas para la prevención del phishing, skimming, estafa, malware y smishing.
- El MINTIC cuenta con el programa de “Plan de Capacitación, Sensibilización y Comunicación de Seguridad de la Información para todos los adolescentes en Colombia.
- El Ministerio de Educación y MINTIC cuentan con un concurso llamado “Conciencia” para concientizar a los jóvenes sobre la importancia de acabar con el cibermatoneo en las aulas escolares de todo el país.

⁵ CASTRO, Mauricio. Ingeniería social, el elemento humano de la seguridad; contramedidas y planes de acción para fortalecer la seguridad en las organizaciones [en línea].

<http://rd.udb.edu.sv:8080/jspui/handle/11715/1182> [citado en 8 noviembre de 2018]

⁶ LAREQUI, Eduardo. El uso educativo de las redes sociales adolescentes [en línea]. < <http://propuestastic.elarequi.com/propuestas-didacticas/el-trabajo-en-red-y-las-redes-sociales/el-uso-educativo-de-las-redes-sociales/> >.[citado en 4 abril de 2017]

5. DISEÑO METODOLOGICO

En el presente Proyecto se realizará utilizando una metodología cualitativa, enfocada en la metodología de la investigación no experimental, manejando a su vez las variables Independientes/Dependientes.

Al momento de investigar las variables independientes, estamos recopilando información de la ingeniería social en un entorno estudiantil por medio de trabajos, tesis, artículos de revistas, conceptos de páginas enfocadas a esta problemática, casos judiciales dentro de un contexto natural y real, no olvidando que esta variable no puede ser modificada pues ya ha ocurrido, lo único que hacemos es compilar datos para luego analizarlos.

Luego pasamos a la variable dependiente, en la que tomaremos dicha información para luego bajo el marco de análisis opinaremos, reflexionaremos, analizaremos estos datos sobre la ingeniería social y su impacto en la adolescencia colombiana.

Dando un análisis en aquello que consideremos puedan ser algunas opiniones sobre los casos encontrados para identificar sus posibles causas y así mismo entregar algunas recomendaciones.

Tabla 1. Metodología de Investigación

METODOLOGÍA DE INVESTIGACIÓN	
Técnicas de recolección de información	
Cualitativa	Análisis de fuentes documentales y medios electrónicos
	Tesis
	Trabajos escritos
	Medios Impresos
	Noticias
	Internet
	Sentencias Judiciales

Fuente: El Autor

5.1. TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN

Para recoger dicha información se utilizará técnica cuantitativa.

5.2. CUANTITATIVAS

Para llevar a cabo la técnica cuantitativa en esta investigación no experimental utilizaremos el diseño longitudinal, enfocándonos en el análisis de las variables mencionadas, en la relación a los resultados en el tiempo. Para luego hacer análisis o inferencias.

A si mismo aplicaremos el tipo de diseño longitudinal de tendencia pues nos enfocaremos a recopilar las investigaciones que se han realizado en Colombia y a su vez en una población específica “los adolescentes”.

Análisis de las referencias, según la investigación.

Como punto inicial del proyecto se debe analizar las amenazas por el volumen y desproporción de crecimiento de tecnologías avanzadas, entre más medios tecnológicos existan, más conexión y falta de límites en los datos que se comparten.

Aportes mediante la recolección de antecedentes ocurridos en las redes sociales, llegando a evidenciar que existen adolescentes víctimas de grooming, ciberbullying, sexting y gossip.

Tabla 2. Técnica cuantitativa – Variables

HIPÓTESIS	VARIABLES		RESULTADOS
	Independiente	Dependiente	
La socialización y supervisión de entidades garantizan mitigar los riesgos de la Ingeniería Social en los adolescentes y así mismo defender sus derechos.	Denuncias de adolescentes víctimas de Ingeniería social, los cuales realizan denuncias en CAI VIRTUAL	Investigación de metodologías de socialización, creación de programas y actividades por parte de la Policía Nacional para evitar casos de ciberacoso y ciberbullying	Conocer que la Policía Nacional tiene como herramienta tecnológica el uso de una plataforma denominada CENTRO CIBERNETICO DE LA POLICÍA NACIONAL- CAI VIRTUAL siendo estos instrumentos de denuncia e información para mitigar el impacto del Ciberbullying y la Ingeniería Social en adolescentes.

Fuente: El Autor

Tabla 3. (Continuación).

HIPÓTESIS	VARIABLES		RESULTADOS
	Independiente	Dependiente	
La educación utilizando instrumentos tecnológicos aporta significativamente a la reducción de las problemáticas de la Ingeniería Social en los adolescentes.	Relatos vividos de adolescentes víctimas de Ingeniería Social, realizados en videos.	Investigación de la implementación de métodos tecnológicos para la socialización de los temas que relacionan la Ingeniería Social dirigido a los adolescentes.	Identificar que el Ministerio de Tecnología de la Información-MINTIC, desarrollo un programa denominado EN TIC CONFIO, este programa tiene como objetivo socializar y capacitar a toda la población en el buen uso de la tecnología, sobre todo en la población de adolescentes entre 11 a 17 años y así mismo la socialización a los padres de la utilización de herramientas para el manejo de la seguridad de la información.
La creación de leyes y artículos fortalecen las funciones de las entidades para respaldar a los adolescentes en la problemática de la Ingeniería Social.	Sentencias judiciales de casos de Ingeniería Social ocurridas a los adolescentes en Colombia	Investigación de la Normatividad aplicable para apoyar programas enfocados al ciberbullyng y así mismo normas aplicadas o creadas para los colegios del estado.	Aprender la normatividad que el Ministerio de Educación se impulsó denominada "CREACIÓN DEL SISTEMA NACIONAL DE CONVIVENCIA ESCOLAR Y FORMACIÓN PARA EL EJERCICIO DE LOS DERECHOS HUMANOS, Y EDUCACIÓN PARA LA SEXUALIDAD Y LA PREVENCIÓN Y MITIGACIÓN DE LA VIOLENCIA ESCOLAR"

Fuente: El Autor

6. METODOLOGIA PARA DESARROLLAR OBJETIVOS

6.1. REALIZAR UN ANÁLISIS DE LOS ESTUDIOS Y ANTECEDENTES EXISTENTES EN COLOMBIA SOBRE LOS RIESGOS DE LOS ADOLESCENTES FRENTE A LA INGENIERÍA SOCIAL

Metodología: Para este objetivo se referenciaron casos reales en Colombia, los cuales se encuentran en tesis de grado, sentencias de la Corte Constitucional, organizaciones y medios de comunicación.

Es solo un panorama de muchos de los casos que han pasado y que desafortunadamente siguen ocurriendo en el País. La ingeniería social es sin duda una muestra de intolerancia a la diversidad, falta de precaución de los adolescentes en sus prácticas o manejo de sus datos personales, aprovechamiento de adultos delincuentes para cometer delitos de cualquier clase contra la población vulnerable.

Se da inicio a este desarrollo haciendo referencia a los estudios en Colombia como:

En año 2015, en la Universidad Católica de Colombia se realiza la tesis “Ciberacoso de niños, niñas y adolescentes en las redes sociales: un estudio sobre los sistemas de protección y prevención judicial”, de la autora Danyorsa Mabel Rojas Morales sobre “La investigación hace un análisis del ciberacoso contra niños, niñas y adolescentes en las redes sociales, específicamente se enfocará en el estudio sobre los sistemas de protección y los mecanismos de prevención judicial. Se pondrán en consideración algunos delitos que coadyuvan al ciberacoso y por consiguiente se relaciona el internet a partir del cual se funda y desarrollan todas las redes sociales, al mismo tiempo el vehículo por medio del cual los menores acceden y se convierten en víctimas del ciberacoso.”

Esta tesis hace inicialmente un análisis de algunos países y su reglamentación respecto al ciberacoso, pues es una problemática a nivel general sin distinción de lugar. Pero que tan pendientes se encuentran los gobiernos en realizar leyes que contrarresten esta vulnerabilidad hacia los niños y adolescentes.

Como análisis de esta tesis se realiza un énfasis en Colombia, que en este caso es nuestro objetivo y de qué forma existen entidades u organizaciones que se preocupan por esta problemática, pero su desarrollo es muy escaso pues habla que no es tan efectivo por lo que se apoya en la Policía Nacional por medio de un método de denuncia como el CAI VIRTUAL.

A continuación, se mostrarán cifras estadísticas de incidentes informáticos reportados por la Policía Nacional, indicando delitos de la Ingeniería Social como lo son la suplantación de identidad, ciberbullying y otros, en los años del 2014 al 2017.

Ilustración 1. Estadísticas de Incidentes informáticos del 2014 al 2017

Modalidad	2014	2015	2016	2017	TOTAL
Suplantación de identidad	140	592	774	65	1571
Publicación de imágenes/videos con pornografía infantil	N/R	62	212	19	293
Sextorsión	111	70	164	26	371
Sexting	41	20	86	7	154
Cyberbullying	216	43	162	11	432
Grooming	26	44	69	9	148
Total	534	831	1467	137	2969

Fuente: CAI Virtual de la Policía Nacional. Estadística de incidentes informáticos (Seguridad Digital) (en línea). Colombia 2017 (Consultado el 10 de noviembre 2018). Disponible en: http://www.alcaldiabogota.gov.co/sisjur/adminverblobawa?tabla=T_NORMA_ARCHIVO&p_NORMFIL_ID=9369&f_NORMFIL_FILE=X&inputfileext=NORMFIL_FILENAME

La autora analiza el concepto del ICBF, sobre el ciberacoso, no quedando bien el instituto en este aspecto. Faltando un poco así de análisis o investigación de los programas que poseen para contrarrestar este delito.

Se presentan estudios de la Universidad de la Sabana y la universidad de los Andes, respecto a las cifras, revelando que existen actitudes en los adolescentes como la violencia causal de estos problemas inclinando estas cifras más hacia el matoneo de los estudiantes.

Se puede determinar que, en Colombia, se debe buscar la manera de concientizar a los niños, niñas y adolescente en el sentido de prevenir el riesgo de utilizar libremente las redes sociales, el uso indebido del Internet, orientándolos con charlas educativas frente a los casos de ciberacoso y a todos los mecanismos de protección que existen actualmente, de cómo pueden utilizarlo y verse beneficiados en su seguridad. Adicional a esto hay que destacar que existe un respaldo judicial lo que hace que estos delitos derivados de la ingeniería no sean tomados como delitos menores y puedan tener el apoyo deseado por las víctimas.

Cabe resaltar que se debe tomar medidas de protección para evitar las amenazas y riesgos que implica la vulnerabilidad de la ingeniera social, utilizando herramientas de programas informáticos que puedan detectar las debilidades que se encuentren en los dispositivos celulares, a través del uso del Internet, las computadoras etc.

Ahora se hará referencia a los antecedentes

En el año 2010, Bianca una madre angustiada por su hijo Filipo, presento al juzgado veinticuatro Penal Municipal de Depuración de Bucaramanga en diciembre 16 de 2010, denuncia en contra del Colegio en donde su hijo estudiaba, ya que habían ocurrido varios incidentes en contra del menor que vulneraban altamente su salud, dignidad en las redes sociales “Facebook”, algunos compañeros crearon un grupo en el cual realizaban toda clase de publicaciones intimidantes hacia el menor con el nombre de “Después me llama a la casa y dice no le pegue a mi...”, este proceso duro 4 años en los cuales la madre hizo todo lo posible por llevar a cabo esta denuncia y ayudar a su hijo. Este caso referencia a la sentencia T-365/14 de Corte Constitucional de la Republica de Colombia.⁷

Como análisis de este antecedente, no hubo por parte de los entes de control una pronta respuesta o fallo, esto hace que las victimas en este caso solo un niño se viera envuelto en procesos que hacen que no se confié en la justicia y adicional a esto la degradación de no sentirse apoyado y tal vez burlado por haber denunciado estos hechos.

Cada proceso por simple que sea respecto al Ciberbullying hacia los menores o adolescentes debe tener una atención prioritaria, pues con este caso no hubo una atención temprana pues existió una degradación psicológica al no resolver rápido este incidente y aún más sumarle la confrontación con sus victimarios removiendo cada uno de los episodios en cada declaración que se debe realizar. Las entidades encargadas de estos casos deben primar la atención y protección, pues el solo hecho de ser menores de edad se vulneran sus derechos y no deben exponerse a estos procesos tan complejos para ellos.

En el año 2012, un adolescente llamado Yhon Rodríguez y su novia Camila fueron víctimas de ingeniería social, al ser expuestas fotografías privadas lo que genero matoneo por parte de sus compañeros clase, ciberbullying y comentarios suicidas. Esto fue por un descuido en el manejo de sus datos personales haciéndose viral su nombre y su identidad en Twitter. Esta información fue tomada del periódico El Tiempo el 05 de Julio de 2012, haciendo alusión a esta problemática y de todos los alcances que puede conllevar a intimidaciones, degradación personal y a su vez informando que en este año las autoridades hacían un llamado a los colegios y padres de familia de este fenómeno.⁸

El análisis del caso del joven Yhon Rodríguez es solo uno de muchos en Colombia y por esto la necesidad de educar a los adolescentes en el uso correcto de sus datos

⁷ SENTENCIA T-365/14 [en línea]. <http://www.corteconstitucional.gov.co/relatoria/2014/t-365-14.htm> [citado en 20 mayo de 2018]

⁸ YHON, UN NUEVO CASO DE 'CYBERBULLYING' EN COLOMBIA [en línea]. <http://www.eltiempo.com/archivo/documento/CMS-12003683> [citado en 24 abril de 2018]

personales o de que información es delicada y no se debe manejarse en las redes sociales. Uno de los temas de desarrollar en las capacitaciones es el manejo de seguridad en los dispositivos móviles, de cómo realizar restricciones de acceso no autorizado, como manejar aplicaciones de alertas en caso de ser víctima de intrusos. Esto no solo hace que sean más precavidos, debido a que generaría curiosidad en nuevas áreas de conocimiento.

En el año 2014, un adolescente de 16 años llamado Sergio Urrego, se quitó la vida lanzándose desde la terraza del centro comercial Titán Plaza en la ciudad de Bogotá D.C., tras ser víctima de ingería social en este caso directamente en su propio colegio “Gimnasio Castillo Campestre” en la ciudad de Bogotá D.C. Víctima de homofobia tras acceder a sus datos personales en este caso el celular, encontrando fotografías privadas por uno de los docentes y haciéndolas públicas entre el círculo de directivos. Lo que desencadenó un fatal desenlace y así mismos comentarios por las redes sociales. Este caso es referenciado en la página de www.dejusticia.org donde se encuentran todos los archivos jurídicos del caso en mención.⁹

El análisis del caso de Sergio, desafortunadamente traspasa todos los límites de lo que puede ocurrir en estos casos de ciberacoso y Cyberbullying. Si existen unas leyes claras frente a esta problemática, con unos tiempos cortos de respuesta y un apoyo temprano a las víctimas. No se llegaría a las instancias del suicidio por parte de los adolescentes. Así mismo la importancia que desde el interior de la familia se esté pendiente de cambios de comportamiento de los adolescentes, el aislamiento, sus expresiones frente a la vida y a los eventos de frustración. Para que los padres puedan actuar y no permitir que la depresión o el rechazo llegue a este desenlace.

En el año 2014, Gerónimo Ángel un adolescente de 13 años el cual participo en un programa conocido como “La Voz Kids”, fue víctima de cyberbullying o matoneo en redes con comentarios ofensivos y homofóbicos. Insultos anónimos lo que generaría un alto nivel de discriminación en los adolescentes y en niños. El caso fue expuesto en la página oficial de www.teprotejo.org el 10 de abril de 2014. Haciendo alusión que solo es uno de 6 mil casos, lo que es solo una pequeña muestra de lo vulnerables que pueden ser los adolescentes con la ingeniería social.¹⁰

El análisis del caso de Gerónimo lleva al cuestionamiento de cuál es la educación que se está recibiendo en los hogares, en el colegio, en cualquier entorno de enseñanza referente al respeto por la diversidad. Y el daño que puede ser causado

⁹ DEJUSTICIA INTERVIENE EN EL CASO DE SERGIO URREGO EN CONTRA DEL BULLYING HOMOFÓBICO EN LOS COLEGIOS [en línea]. <https://www.dejusticia.org/litigation/dejusticia-interviene-en-el-caso-de-sergio-urrego-en-contra-del-bullying-homofobico-en-los-colegios/> [citado en 13 junio de 2018]

¹⁰ Ciber acoso a menor de La Voz Kids, uno de los 6 mil casos de un fenómeno sin control [en línea]. <http://www.teprotejo.org/index.php/es/apariciones-en-medios-2014/409-10-04-2014-el-pais-ciber-acoso-a-menor-de-la-voz-kids-uno-de-los-6-mil-casos-de-un-fenomeno-sin-control> [citado en 13 junio de 2018]

en la utilización de una red social para realizar Ciberbullying cuando no se está de acuerdo con estas diferencias. Enseñar a los niños y adolescentes al buen uso de las redes sociales y de como un dato errado o mal intencionado puede llegar a generar una falta legal de gran impacto.

En el año 2015, una adolescente de 14 años llamada Karla González, fue víctima de ingería social acusándola de ser bisexual y tener una relación con una de sus amigas; tanto que fue necesario el cambio de lugar de residencia. Esta niña ya era víctima algunos años atrás, lo que generó en ella crisis emocional llevándola a pensar en suicidio que en este caso sería una de las más altas consecuencias que posee la ingería social, pues en su intento por llevarlo a cabo consumió Clopidrogel, pero con ayuda de sus padres fue llevada a tiempo a la clínica. Ese caso se encuentra en los medios de comunicación como el periódico el Herald, pero a su vez es mencionado en el trabajo de grado “Implicaciones Legales y Condenatorias Por Ciberbullying” de la “Universidad de la Costa” Barranquilla (Atlántico).¹¹

El análisis del caso de Karla es uno de los casos que puede ser rescatable de actuar a tiempo por parte de los padres de familia y a su vez de las consecuencias que puede llegar a generar una vulnerabilidad como es ser víctima de noticias falsas y del poder que poseen las redes sociales para divulgar una información a gran escala cuando no es verdad. Dentro de la educación y de los puntos anteriores está el enfatizar en el buen uso de las redes sociales.

Después de analizar estos antecedentes, debemos identificar que la ingeniería social es una problemática que ha existido desde la difusión de las redes sociales. En algunos años esta problemática se masifico por la falta de controles y conciencia ciudadana al respecto. En cada caso se evidencia la vulnerabilidad de los niños y adolescentes por el uso irresponsable o ingenuo de su información personal, estando expuestos a la vergüenza ante las redes sociales, lo que hace que prefieran guardar silencio. También evidenciamos la importancia de la familia en todos estos antecedentes, pues se convierten en un apoyo psicológico lo que ayuda a los adolescentes a enfrentarse a los hechos ocurridos, realizando las denuncias de forma oportuna.

¹¹ IMPLICACIONES LEGALES Y CONDENATORIAS POR CYBERBULLYING [en línea]. <https://repositorio.cuc.edu.co/xmlui/bitstream/handle/11323/1267/1042439888-1042427867.pdf?sequence=1&isAllowed=y> <http://www.teprotejo.org/index.php/es/apariciones-en-medios-2014/409-10-04-2014-el-pais-ciber-acoso-a-menor-de-la-voz-kids-uno-de-los-6-mil-casos-de-un-fenomeno-sin-control> [citado en 13 junio de 2018]

6.2. REALIZAR UN ANÁLISIS SOBRE LOS MÉTODOS, TÉCNICAS Y TÁCTICAS DE SEGURIDAD PROPUESTAS POR ORGANIZACIONES DEDICADAS A LA SEGURIDAD EN COLOMBIA, PARA CONOCER SU GRADO DE EFICIENCIA, EFICACIA Y EFECTIVIDAD.

Metodología: En Colombia existen varias organizaciones las cuales están realizando acciones, campañas y de más actividades para prevenir la Ingeniería Social.

Se nombrar algunas de las estrategias y a su vez los nombres de quienes están aportando para evitar este delito.

El Centro Cibernético Policial en su compromiso por combatir estos problemas tiene programas para la prevención de la Ingeniería Social en niños y adolescentes.

Uno de estos es el Programa de Prevención "Abre tus Ojos¹²", el cual fue creado para compartir con la comunidad por medio de charlas preventivas a nivel Nacional que orientan respecto a la vulneración de los derechos de los niños y adolescentes con el fin de evitar los riesgos a los que pueden ser expuestos, en nuestro enfoque uno de estos temas es el (Uso: Uso responsable de Internet), en el que se enfoca todo aquello que se desencadena con la Ingeniería Social. Para esto la Policía dicta charlas utilizando métodos de acercamiento y dinamismos como Cine Foros, Conferencias Educativas, dramatizaciones, utilización de herramientas didácticas, obras de teatro, unidades móviles como los buses interactivos. Este programa está dirigido a varias poblaciones, pero en nuestro caso específico a Adolescencia (13-17) años y Familia en situaciones de vulnerabilidad.

Así mismo el programa capacita estudiantes ¹³ con el fin de ser líderes que extiendan las experiencias y los conceptos vistos con el fin de promover las actividades de prevención del programa.

Realizando un análisis de este programa, vemos con buenos ojos estas campañas pues involucra gran parte de población vulnerable a su vez la cobertura que posee pues como podemos ver en redes y en la misma página de la Policía ha sido difundida a nivel Nacional, enfatizando en la población estudiantil para que no se vean expuestos a los delitos de ingeniería social. Estas campañas de socialización reducen esos índices tan altos de ignorancias frente a la seguridad, pues al tocar el tema con los jóvenes permite que estos no se encuentren tan expuestos o al menos

¹² PROGRAMA "ABRE TUS OJOS" [en línea]. <https://www.policia.gov.co/proteccion-infancia/programa-abre-tus-ojos> [citado en 1 agosto de 2018]

¹³ 750 ESTUDIANTES SE GRADUARON EN PROGRAMA 'ABRE TUS OJOS' " [en línea]. <http://www.vanguardia.com/santander/guanenta/261200-750-estudiantes-se-graduaron-en-programa-abre-tus-ojos> [citado en 1 agosto de 2018]

sean un poco más cuidadosos al momento de ingresar a las redes sociales y no sean tan ingenuos al compartir su información personal en las redes.

Así mismo que no sean victimarios pues se enfatiza con estas charlas que si lo hacen están incurriendo en un delito que puede ser penalizado y puede acarrear muchas consecuencias.

Los siguientes programas generan un gran acercamiento entre los adolescentes y la Policía lo que conlleva a facilitar una denuncia en caso de ser víctimas de estos delitos informáticos y así mismo con las indicaciones dadas por el programa podrá identificar cuando están siendo víctimas y cómo prevenir un riesgo como estos.

En TIC confío, es un programa del Ministerio de Tecnologías de la Información, el cual tiene como objetivo la socialización o capacitación a toda la población para el que realicen buen uso de las tecnologías y el internet, de una forma segura y responsable con los demás, buscando una correcta convivencia digital entre todos sus usuarios, no olvidando que el internet como canal de comunicación como su nombre lo indica permite transmitir, compartir, enviar toda clase de información. Rechazando de una manera unánime la difusión de contenidos, hechos y canales que tengan que ver por la vulnerabilidad hacia los menores o adolescentes. Un no rotundo a la pornografía infantil, un abominable delito que los delincuentes comenten por medio del internet y el uso equivocado de las tecnologías.

El programa ofrece varios canales de comunicación dentro de las redes sociales, pues en estas se encuentran la mayoría de la población a la cual quieren llegar. Si el programa promueve estos canales de comunicación donde los adolescentes se encuentran, esto genera confianza y de esta manera podrán llegar más fácil a ellos.

Cada charla o actividad busca que los niños y adolescentes dialoguen entre ellos y expongan sus puntos de vista sobre cada uno de los riesgos a los cuales están expuestos con el uso inadecuado de las redes sociales. Y de una manera abierta entre ellos, de tal forma que si han sido víctimas puedan expresar sus experiencias con el fin de visibilizar la problemática para que no se conviertan en victimarios y así mismo enseñarles cuales son los mecanismos de denuncias o procedimientos a seguir.

El programa orienta paso a paso en caso de ser víctimas, pues una vez los adolescentes son expuestos y no saben cómo reaccionar.

Primer paso en caso de un evento de acoso cibernético, pornografía infantil, cyberbullying los adolescentes pueden realizar la denuncia de forma anónima ingresando a la URL www.teprotejo.org

Una vez se ingresa a esta dirección se escoge que tipo de denuncia que se quiere realizar, en este ejemplo seleccionaremos el ciberacoso el cual una vez se da click

muestra un formulario con unas preguntas que pueden llevar a concluir el incidente o detalles del mismo de una manera anónima, para que el adolescente no se sienta comprometido y pueda realizar la denuncia.¹⁴

Este método es fundamental ya que se relaciona con las TIC lo cual se encuentra en un área de manejo de los adolescentes, como es la iteración de las apps móviles en su vida cotidiana y al tener esta aplicación en sus dispositivos ven una manera fácil de realizar una denuncia a tiempo. No olvidemos que el tiempo en estos casos es el mayor enemigo por lo que facilitaría una pronta solución a esta vulnerabilidad.

Segundo Paso: Se aconseja el bloqueo de aquellos usuarios que están realizando el ciberacoso, el ciberbullying o cualquier otro delito contra los adolescentes como ofensas o chantaje. Estos bloqueos se pueden hacer con herramientas o aplicaciones que poseen las redes sociales para que estos delincuentes no accedan a datos, fotos, publicaciones, ubicación o actividades de la víctima.

En el caso de la red social más conocida que es facebook los adolescentes pueden realizar procedimientos muy sencillos dentro de su perfil como denunciar contenidos fuertes, cuentas falsas, bloquear, reportar como spam y con esto evita aquellos usuarios no deseados o molestos.

La implementación de la seguridad informática en las redes sociales es de gran ayuda, pues en la actualidad se masifican todos aquellos delitos informáticos que hacen que las compañías creadoras de estos servicios sociales por medio de sitios web, creen la necesidad de dicha seguridad o políticas de manejo, así que dentro de estas permiten a los usuarios restringir cualquier acceso no deseado, un contacto no conocido, mensajes ofensivos y demás herramientas de protección aunque no son suficientes para evitar estos delitos.

Tercer Paso: Este es uno de los pasos más importantes y un poco difíciles para los adolescentes que es la confidencia a un adulto de todo lo que está ocurriendo, este paso puede ser el más decisivo para frenar una amenaza o una agresión por medio de los medios digitales o cualquier otra agresión.

El método más efectivo es la comunicación de los padres hacia los adolescentes y aún más en esta etapa. Pero los padres deben estar muy bien informados y advertir a sus hijos de la problemática que existe, de los vulnerables que pueden ser, de los peligros a los cuales están expuestos, de todos aquellos delincuentes que solo utilizan las redes sociales para cazar víctimas.

Haciendo un análisis de esta metodología de en TIC Confío, los padres también deben informarse y capacitarse para saber en qué problemas se están enfrentando

¹⁴ DENUNCIE CIBERACOSO [en línea]. <http://www.teprotejo.org/index.php/es/denuncie-ciberacoso> [citado en 13 junio de 2018]

sus hijos en las redes sociales, que tanto saben del tema del Ciberbullying, ¿están pendientes de sus hijos? y ¿pueden entablar una conversación que le brinde confianza a los adolescentes al respecto? Estos interrogantes son importantes son fundamentales y a su vez el propio comportamiento. ¿Cómo padres estoy formando con ejemplo? Los padres están aplicando unas buenas prácticas en el uso de sus propias redes sociales o de una u otra manera también exponen desde sus propias redes a sus hijos con información personal y fotografías.

El papel de los padres es fundamental pero también debe haber un interés de su parte en actualizarse en estos temas y de aprender sobre seguridad para así saber cómo cuidar a sus hijos y como generar reglas y normas dentro de la familia en la utilización de estas tecnologías.

La campaña o el programa de en TIC confió es una de las más completas y es un método efectivo para tratar la ingeniería social con los adolescentes, pues va enfocada directamente a los niños y adolescentes manejando charlas, actividades y procesos de sensibilización de la problemática, sus riesgos, sus consecuencias, vivencias, experiencias de otros adolescentes. De tal forma que las charlas o foros hacen que exista un acercamiento entre todos los participantes y que exista la confianza suficiente de hablar de algún episodio ocurrido o también de hacer que si existe un adolescente que este cometiendo estas agresiones sepa o comprenda que es una conducta ilegal, perjudicial y tomar la decisión de detenerse en la agresión.

Después de este análisis el programa utiliza una metodología de hablar de todos los temas sin tapujos de la ingeniería social que hace crear conciencia de la vulnerabilidad en la cual se encuentran, de la falta de seguridad, de los peligros a los cuales están expuestos en las redes sociales al momento de compartir fotos personales, información personal y de cómo reaccionar ante un ataque de estos ya mencionados.

Dentro del segundo paso, nombrado anteriormente el cual hacía referencia a la denuncia desde la página “Te Protejo” o también la app con el mismo nombre, es un método de denuncia ciudadana enfocado a delitos o circunstancias que vulneren los derechos de los niños y adolescentes. Esta técnica es un propuesta de varias organizaciones (Ministerio de las TIC, el ICBF, Telefónica Movistar, Foro de Generaciones interactivas de España, la red PaPaz y la Policía Nacional) en la creación de un proyecto gratuito sin ánimo de lucro, con la importancia de asociarse a una red internacional de denuncias de pornografía infantil, esta tiene enlace con 40 países y a su vez hacen parte de una fundación llamada INHOPE los cuales están comprometidos en la erradicación de este delito y en la cooperación con entidades del estado encargadas de seguimientos y captura de los delincuentes, pederastas y pedófilos. Este método es muy acertado para la población a la que

desean dirigir este proyecto, pero detrás de esto está una técnica segura de identificación de redes de abusadores no solo sexuales hacia los niños y adolescentes. Pues el trabajo de colaboración y aún más que este se extienda a nivel internacional hace que la cobertura de captura o trazabilidad de los ataques sea más efectiva.

Si analizamos el Ministerio de las TIC en alianza con otros Ministerios como Educación y organizaciones como Red PaPaz, ETB, Oficina de Delitos Informáticos de la Policía Nacional, Microsoft Colombia, Foro de Generaciones Interactivas, Fundación Alberto Merani se unen con un mismo fin, cuidar la seguridad, integridad de los niños y adolescentes. Pues otras de las estrategias creadas por estas organizaciones es el manejo de las buenas prácticas a nivel de tecnología y de manejo del internet. Para esto reunieron los 10 comportamientos fundamentales al momento de utilizar las tecnologías y de cómo siguiendo estas recomendaciones se logra evitar y prevenir las amenazas cibernéticas.

Estos comportamientos o pautas son:

1. Respeto
2. Libertad
3. Identidad
4. Integridad
5. Intimidad
6. Autonomía
7. Calidad de vida
8. Cuidado y acompañamientos
9. Respeto por la ley
10. Derecho de autor¹⁵

Haciendo un análisis general cada año se aumentan los casos sobre la ingeniería social y aún más a nivel de los adolescentes pues no miden la forma de agresión hacia los demás.

Siendo esto un triste reflejo de la falta de principios dentro de las familias, siendo influenciados por la violencia intrafamiliar, o de la misma sociedad, que no controlan sus emociones de intolerancia hacia los demás, también de los medios de comunicación con titulares negativos, corrupción, guerras, falta de respeto hacia las autoridades, la falta de escrúpulos y un sin número de comportamientos degradantes de la sociedad. Todo esto influye para que los adolescentes busquen mundos ideales en las redes sociales o afecto que no encuentran en el interior de

¹⁵ TUS 10 COMPORTAMIENTOS DIGITALES [en línea].
<http://tus10comportamientosdigitales.redpapaz.org/> [citado en 13 junio de 2018]

sus familias, o llamar la atención, o tener popularidad así sea a costillas de la integridad de otros.

Uno de los métodos o técnicas más efectivos para evitar o controlar el Ciberbullying en Colombia es la implementación de la ley 1620 del 15 de marzo de 2013 "POR LA CUAL SE CREA EL SISTEMA NACIONAL DE CONVIVENCIA ESCOLAR Y FORMACIÓN PARA EL EJERCICIO DE LOS DERECHOS HUMANOS, LA EDUCACIÓN PARA LA SEXUALIDAD Y LA PREVENCIÓN Y MITIGACIÓN DE LA VIOLENCIA ESCOLAR" en el Capítulo I – Artículo 2 (Ciberbullying o ciberacoso escolar: Forma de intimidación con uso deliberado de tecnologías de información (Internet, redes sociales virtuales, telefonía móvil y video juegos online para ejercer maltrato psicológico y continuado). En este artículo enuncia el Ciberbullying como un maltrato, por lo cual se convierte oficialmente en un delito y a su vez en todos los mecanismos en los cuales se puede llevar a cabo esta vulnerabilidad hacia los estudiantes, teniendo en cuenta que se enmarca en la ley de cumplir con una correcta convivencia escolar que respeta altamente los derechos humanos de los niños y adolescentes. Pero también de cómo prevenir para que este riesgo no se cumpla en esta población.

Parte de esta prevención es ofrecer mecanismos para la realización de denuncias o de cómo divulgar que se está siendo víctima de este delito, para esto en el Capítulo II "SISTEMA NACIONAL DE CONVIVENCIA ESCOLAR Y FORMACIÓN PARA LOS DERECHOS HUMANOS, LA EDUCACIÓN PARA LA SEXUALIDAD Y LA PREVENCIÓN Y MITIGACIÓN DE LA VIOLENCIA ESCOLAR" Artículo 8. "Funciones de Comité Nacional de Convivencia Escolar" en el numeral 9 "Coordinar la creación de mecanismos de denuncia y seguimiento en internet, redes sociales y demás tecnologías de información a los casos de Ciberbullying." Nos permite actuar bajo una función declarada en el comité de convivencia para realizar seguimientos o realizar las denuncias pertinentes de casos en el ámbito escolar de Ciberbullying.

En el capítulo III "el sector educativo en el sistema nacional de convivencia escolar y formación para los derechos humanos, la educación para la sexualidad y la prevención y mitigación de la violencia escolar" en el Artículo 16 en el numeral 6 "Promover el desarrollo de las competencias ciudadanas, el ejercicio de los derechos humanos, sexuales y reproductivos, el fomento de estilos de vida saludable y la prevención del acoso escolar y el Ciberbullying en las jornadas escolares complementarias"

Esta impulsa crecimiento de competencias sociales en espacios extracurriculares, pero de entornos escolares. En estos espacios se comparten otras situaciones entre los adolescentes, como sus gustos por la música, deporte y esparcimiento que pueden llevar a compartir información sin restricción y puede llegar a ser delicada, también con estos espacios se puede compartir con otras personas que no son de un entorno seguro y estas pueden llevar a los niños o a adolescentes a ser víctimas de un ciberacoso o ciberbullying.

Cuando una persona realiza hechos de agresión en las redes, lo hace porque puede escudarse detrás de las redes, por la facilidad del anonimato ocultándose con cuentas falsas para no ser descubiertos con el fin de insultar, discriminar, acosar, burlarse, violentar, robar y muchos delitos que algunos no harían si fuera directamente. Pero aun peor van dirigidos a los incautos, descuidados, inexpertos, inocentes adolescentes.

Como analizamos vemos las leyes no son suficientes en el ámbito escolar y aún más en el tema del manual de convivencia. Actualmente existe un mundo de tecnología y los adolescentes utilizan este medio en su vida cotidiana, toda gira entorno a la tecnología a las redes sociales a las comunicaciones. Sí en los colegios se tuviera en cuenta está problemática, Se realizarían cátedras de cómo prevenir estos riesgos y de cómo no ser vulnerables en las redes sociales.

Según todo el análisis e investigación hecho hasta ahora describiría el delito de la ingeniería social como “Cobardía”, sería la palabra utilizada para estas agresiones a través de las redes sociales.

Por esto debemos afianzar todos los mecanismos, métodos, tácticas de seguridad de la información y controles de las entidades, organizaciones, grupos que se encargan de visibilizar esta problemática y proteger de forma radical la violencia contra los adolescentes y también los niños.

Para cumplir con este objetivo hablaremos del grado de Eficiencia respecto al análisis realizado anteriormente, determinando que la eficiencia es cumplida en Colombia. Porque se cuenta con la disponibilidad de entidades encargadas de controlar esos delitos como la Policía Nacional, el ICBF, los ministerios tanto de TIC, Protección Social, Justicia, Educación y así mismo fundaciones creadas para ayudar estas entidades a socializar su labor.

Ahora hablaremos del grado de la Eficacia, o la capacidad de cumplir con el objetivo de todas estas entidades que posee Colombia para combatir esta problemática de la Ingeniería Social, y vemos tristemente que el grado de cumplimiento no es el anhelado o realmente requerido para dicha problemática.

Respecto a la efectividad lo que indica el cumplimiento y la capacidad, no se está logrando, pues los tiempos de respuesta no son los indicados para cada caso, pues se llega al punto crítico encontrar casos de suicidio por parte de los adolescentes, cuando ya han recurrido a estas entidades u organizaciones y no se tiene la suficiente diligencia, respeto, prontitud en dar apoyo psicológico temprano.

Se concluyen que existen organizaciones ya creadas para tales fines, pero aún falta apropiación de esta problemática y así mismo darle más celeridad a los casos en los que estén involucrados los menores de edad. Pues hasta la fecha se ha

trabajado en la implementación de mecanismos, técnicas, tácticas para que los menores de edad no sean vulnerados, pero lo implementado no ha sido suficiente. La Ingeniería Social va creciendo día a día y así mismo deben crecer los controles, normas, leyes para disminuir las estadísticas aún más cuando va dirigida a la población vulnerable que son los menores de edad. Las consecuencias pueden ser irreversibles, teniendo claro que en gran parte es también nuestra responsabilidad, como sociedad, familia, instituciones educativas y no solamente es compromiso del estado.

El restringir, el establecer normas dentro del hogar, límites, reglas y ante todo inculcar el respeto propio y hacia los demás, enseñándoles a los niños para que luego como adolescentes tengan un criterio y entendimiento que todo nuestro entorno es diverso y merece respeto e igualdad.

6.3. REALIZAR UN ANÁLISIS DE LOS RESULTADOS DE ATAQUES DE INGENIERÍA SOCIAL POR EL MANEJO INADECUADO DE DATOS PERSONALES, EN LAS REDES SOCIALES POR PARTE DE ADOLESCENTES EN COLOMBIA.

Metodología: La ingeniería social existe desde tiempo inmemoriales, pero a nivel TIC su máximo precursor fue Kevin Mitnick “Cóndor”.

Mitnick afirmaba que la ingeniería social funcionaba por cuatro preceptos:

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

Los comienzos de esta técnica se basaban en llamadas telefónicas, haciéndose pasar por entidades que brindan un determinado servicio. La finalidad de este llamado era recabar información sobre la víctima. Con la llegada de Internet a cada hogar, comenzaron a aparecer técnicas de Ingeniería Social vía clientes de mensajería instantánea. Comenzó a ser muy común el famoso mensaje mediante Messenger “Fotos_para_adultos_de_alguien.rar”. Enviando código malicioso a los contactos de la cuenta, hubo muchos casos de infección mediante esta técnica.

Hoy en día, los ciberdelincuentes buscan engañar a sus víctimas para que entreguen voluntariamente su información personal. La mutación se dio no sólo hacia sitios web, sino también se ha transformado en mensajes de texto, y cualquier tipo de mensajería móvil. La importancia de este vector de ataque radica en que estos dispositivos móviles almacenan gran cantidad de información personal, como contactos, fotos, conversaciones, usuarios y contraseñas de redes sociales, de correos electrónicos, inclusive geolocalización.

También han aparecido técnicas como Pharming, muy similar al phishing, pero que, en vez de engañar al usuario mediante un enlace enviado por correo electrónico, busca el robo de información mediante la modificación en tiempo real de las consultas realizadas a los servidores DNS o mediante la toma de control del equipo víctima; así, modifica el archivo lmhost, que se encarga de resolver las consultas web, asociando la dirección IP al dominio.

Tabla 4. Evolución de la Ingeniería Social

AÑO	AUTOR	DESCRIPCION
1950	Alan Turing	A través de un artículo para la revista Mind [37], vuelve a formular la pregunta "Can machines think?" con una prueba de concepto conocida como Test de Turing. Esta consiste en, sin poder interactuar físicamente, averiguar si se está comunicando con un humano o una máquina.
1960-1970	phreaks	Nace de combinar las voces inglesas "phone" y "freak, marcar números y teclas al azar, fascinados con la línea telefónica e intentando desentrañar sus secretos
1966	Joseph Weizenbaum	Aplicaciones programadas a partir de reglas y con una base de conocimiento específica, los cuales devuelven una salida acorde a la entrada que reciben.
1980	John Searl	Publica un artículo [38] con el fin de rebatir la eficacia del Test de Turing. Él propone el experimento de la sala china, que consiste en agrupar una serie de elementos que usados en cadena devuelven el resultado esperado
1999	Messenger	Comenzó a ser muy común el famoso mensaje mediante Messenger "Fotos_para_adultos_de_alguien.rar". Enviando código malicioso a los contactos de la cuenta, hubo muchos casos de infección mediante esta técnica.
2000	Pharming	Explotación de una vulnerabilidad en el software de los servidores DNS (Domain Name System) o en el de los equipos de los propios usuarios
Actual	Tro/BankAsh-A	Está diseñado para ser descargado secretamente en la computadora de una persona, donde esperará al acecho hasta que el usuario intente conectarse a uno de una serie de sitios web bancarios

Fuente: Vicente Carrillo, Ingeniería social aplicada al delito informático- Ingeniería social, Christopher Hadnagy

De acuerdo con esta Tabla año tras año podemos evidenciar que mediante la evolución de la tecnología en sistemas se ha buscado las vulnerabilidades respecto a la seguridad de la información. De cómo poder quebrantar o ingresar a un sistema no autorizado. Y cada vez se ha sido exponencial con el agravante que los controles no son los apropiados para evitar amenazas, pues van a un paso de lo que ya se encuentra implementado.

Teniendo en cuenta lo anterior, es de amplia importancia investigar y desarrollar a futuro cuales serían los mecanismos apropiados para prevenir el desarrollo cada vez más sofisticado del delito informático que trae consigo la evolución de la ingeniería social.

Y a su vez, apoyar la creación de más leyes sobre estos delitos para que las penas sean más altas y frenen este fenómeno que crece día a día con el avance de las tecnologías de la información.

Ahora se hará alusión a la Ingeniería Social en Colombia y sus resultados con algunas muestras realizadas en Colombia

Año: 2013

Método: Entrevista – Diarios de Campo – Bitácoras de observación – sistemas de registro tecnológico.

Lugar: Colegio Distrital León de Greiff - Bogotá D.C.

Muestra: 16 Estudiantes

Edades: 11 a 13 años

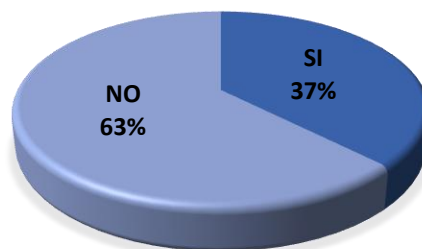
Género: Femenino

Grado: Secundaria

Según estudios y antecedentes entregados en la praxis pedagógica de la Universidad Pedagógica Nacional de Bogotá D.C. en 2012 al 2013 sobre “Ciberbullying: intimidación entre adolescentes a través de la red social Facebook”, de Gómez, A.C., Castillejo, D., Vargas, G., con las siguientes cifras:

Ilustración 2. Ingeniería Social Adolescentes - Año 2013

INGENIERIA SOCIAL ADOLESCENTES - AÑO 2013



Fuente: El Autor

En el año 2013 el manejo de las redes sociales y ser víctimas de esta ingeniería social no era tanto como en la actualidad, pero vemos que ya existía una tendencia del 37% lo que corresponde a una cifra significativa de vulnerabilidad en los adolescentes.

Analizando estas cifras vemos que es claro según resultados entregados, los jóvenes se ven afectados por el uso de las redes sociales en especial Facebook pues entre ellos es la más popular, haciendo de ella un lugar donde se realiza discriminación, amenazas, burla, intimidación y otros males que son altamente nocivos para los adolescentes que los llevan al aislamiento y a las relaciones interpersonales con sus familias y el entorno en general, con el agravante que estos en su mayoría son anónimos lo que hace que sea difícil la detección temprana de ellos.

Vemos según el artículo y muchos otros que la manera de combatir o disminuir estos índices de acoso por parte de los adolescentes es un acompañamiento familiar y así mismo del acompañamiento estudiantil.

Año: 2014

Método: Encuestas

Lugar: Liceo Infantil Personitas de la Dorada Caldas, Francisco de Paula Santander de Villavicencio, I.E.D. Fernando Mazuera Villegas de Bosa, Universidad Gran Colombiana, Universidad Minuto de Dios de Bogotá

Muestra: 262 Estudiantes

Edades: 10 a 20 años

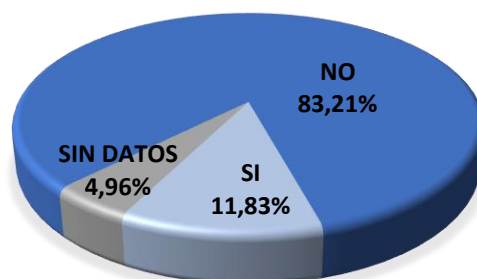
Género: Femenino y Masculino

Grado: Secundaria y Pregrado

Según análisis realizado de la Revista Científica General José María Córdova, Bogotá, Colombia, julio 2014, Simbiosis vital para describir el Ciberbullying en Colombia, en este caso tomaremos una de las preguntas la cual es "Ha sufrido algún ataque cibernético" de Rincón Rueda, A. I. y Ávila Díaz, W. D.

Ilustración 3. Ingeniería Social Adolescentes - Año 2014

INGENIERIA SOCIAL ADOLESCENTES - AÑO 2014



Fuente: El Autor

En el año 2014, el 83.21% de los estudiantes nunca han sido víctimas de ataques cibernéticos, solo el 11.83 % contestaron que alguna vez fueron amenazados por este tipo de ataque de ciberbullying.

Analizando estas cifras vemos que los resultados inesperados para esta investigación de bajo índice de agresión de ciberbullyng, podría deberse que en la época en que se realizó la encuesta los estudiantes no tenían la facilidad y el acceso que se tiene hoy en día que les proporcionara ingresar por cualquier medio tecnológico, obteniendo un menor impacto en estas instituciones educativas.

Recientemente, investigadores han determinado que los efectos el Ciberbullyng ha aumentado como lo evidenciamos a lo largo del presente proyecto de las diversas situaciones que se han reportado conllevando a que en los últimos años se debe prevenir, basados en los efectos que causaría a los adolescentes ser víctimas de este tipo de ataques.

Año: 2015

Método: Encuesta

Lugar: 16 Colegios de Bogotá D.C.

Muestra: 1240 Estudiantes

Edades: 11 a 16 años

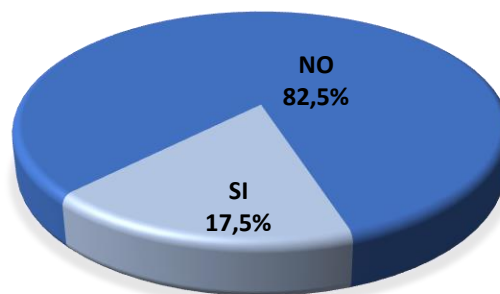
Género: Femenino y Masculino

Grado: Secundaria

Según estudios entregados en el proyecto de grado del Instituto Alberto Merani de Bogotá D.C. sobre “Ciberbullying: El acoso escolar en la era virtual”, de Guerrero Torres, D., Moncayo Salas, L., Parra Torres, J., con las siguientes cifras:

Ilustración 4. Ingeniería Social Adolescentes - Año 2015

INGENIERIA SOCIAL ADOLESCENTES - AÑO 2015



Fuente: El Autor

En el año 2015 el manejo de las redes sociales era algo en pleno furor, moda o tendencia, pues de 1240 estudiantes 217 fueron víctimas del ciberbullying, siendo esto una cifra alarmante, lo que corresponde a la facilidad de acceso a las redes por la tenencia de dispositivos en conectados. En este trabajo de grado los adolescentes no solo son víctimas, sino también victimarios convirtiéndose en un año crítico en esta problemática, en cuestión comparativo.

Pero es aún más alarmante, ver que esta encuesta fue realizada por estudiantes que compartían la misma edad con los encuestados, siendo esto un factor de confianza que hacía que los jóvenes dejaran sus temores al momento de contestarla. Y hablaran abiertamente de esta problemática, divulgando que eran partícipes, cómplices, víctimas o espectadores.

Los controles por parte de los adultos responsables, como padres, profesores, coordinadores o cualquier otra figura que se encuentre a cargo de los adolescentes es fundamental, pues vemos que la falta de límites, reglas o vigilancia maximiza esta vulnerabilidad y riesgos.

Año: 2016

Método: Encuestas

Lugar: Colegio Atenas I.E.D de Bogotá D.C.

Muestra: 42 Estudiantes

Edades: 12, 14 y 15 años

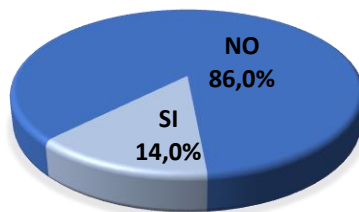
Género: Femenino y Masculino

Grado: Secundaria

Según trabajo de grado de la Fundación Universitaria Los Libertadores de Bogotá D.C. sobre “Las TIC una herramienta didáctica para identificar y mitigar el cyberbullying”, de Castelblanco Burbano, D. A., Sánchez Bustamante, M. T., Ruiz Ramírez, T.

Ilustración 5. Ingeniería Social Adolescentes - Año 2016

INGENIERIA SOCIAL ADOLESCENTES - AÑO 2016



Fuente: El Autor

En el año 2016, el 86% de los estudiantes nunca han sido víctimas de ataques cibernéticos, solo el 14 % contestaron que alguna vez fueron amenazados por este tipo de ataque de ciberbullying.

Analizando estas cifras y el trabajo presentado en el 2016, se sigue conservando la desinformación, la intimidación al momento de denunciar, la falta de conocimientos en seguridad por parte de los adultos y a su vez de los adolescentes.

Dentro de los entornos escolares se vive el ciberbullying y el denunciarlo hace o existe la percepción que van a seguir siendo acosados y aun peor después de manifestar dicho acoso. Por esto cada año se debe enfatizar en afianzar las políticas de seguridad en los colegios y en casa enfatizar en los problemas a los cuales se pueden ver envueltos.

Año: 2018

Método: Encuesta

Lugar: Universidad Autónoma del Pregrado de Ingeniería Industrial y adultos entidad estatal de Bogotá D.C. – Colombia

Muestra: 30 Personas

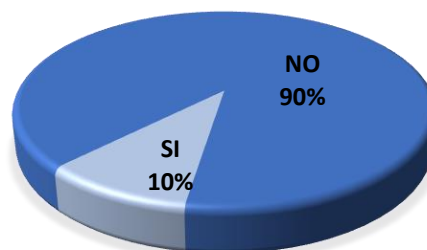
Edades: Adolescentes y Adultos

Género: Femenino y Masculino

Según trabajo de grado de la Universitat oberta de catalunya, Universitat Rovira i Virgili y la Universitat Autònoma de Barcelona sobre “Metodologías de la Ingeniería Social”, en este caso tomaremos una de las preguntas la cual es “¿Alguna vez ha sido víctima de Ingeniería Social?” de Rodríguez Rincón, E. Y.

Ilustración 6. Ingeniería Social Adolescentes - Año 2018

INGENIERIA SOCIAL ADOLESCENTES - AÑO 2018

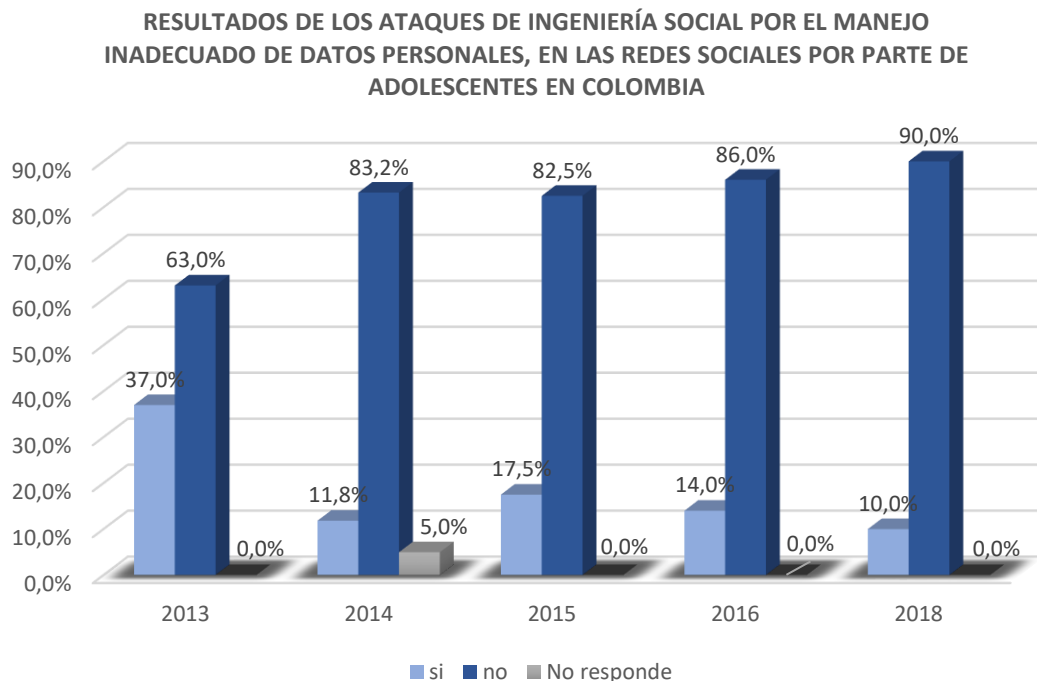


Fuente: El Autor

En el año 2018 el manejo de las redes sociales y ser víctimas de esta ingeniería social se ve de la misma forma que otros años. Aun no existe una disminución considerable en estas cifras pues estamos hablando de 10% de una muestra pequeña, por lo tanto, es una cifra significativa de vulnerabilidad en los adolescentes.

Esta tesis de grado aplica varias preguntas lo que nos demuestra que existe gran desconocimiento aun estando en la actualidad de la Ingeniería Social, de los riesgos y amenazas. Es aún más preocupante que la muestra no solo tomo adolescentes, pues también abarco adultos con el fin de evaluar algunos padres. Y aun así había desconocimiento de una forma igualitaria.

Ilustración 7. Resultados de los Ataques de Ingeniería Social



Fuente: El Autor

Como análisis de los resultados se toman las muestras de cada año investigado trabajos de grado, tesis o datos estadísticos de solo Colombia, con el fin de consolidar y evidenciar según las cifras si existe un crecimiento o disminución en referencia a los ataques hacia los adolescentes por medio de la Ingeniería Social.

Como vemos en la gráfica el primer año existe un porcentaje considerable frente a la muestra de ataques por Ingeniería Social. Pero a partir del segundo año

consultado vemos que tiende a una tendencia al mismo porcentaje o manteniéndose sobre la muestra, aunque en el 2018 vemos que el porcentaje es alto en relación con los ataques y aunque existen ataques el porcentaje ha sido el más bajo.

Esto en parte se debe a todas las campañas de socialización y capacitación hacia los adolescentes, sobre la Ingeniería Social, los peligros que corren al publicar sus datos personales sin ninguna restricción. Exponiéndose a riesgos que pueden llegar a ser fatales.

Para la recopilación de estos datos, específicamente haciendo énfasis en “¿Ha sido víctima de Ingeniería Social en Colombia?”, nos encontramos con grandes dificultades, pues no existen datos estadísticos que manejen la misma muestra, la misma población, las mismas características año a año, para que así de unos resultados más acertados en cuanto a dicha evolución o tendencia en el tiempo.

Existe muchos trabajos que hablan de esta problemática, pero no correspondían a Colombia; hacían énfasis en otros países que si manejan los controles de una forma más estricta con el fin de acabar esta problemática como España.

Las cifras encontradas en Colombia son muy escasas, por lo tanto, existe una gran falencia de información respecto a estos datos los cuales son fundamentales para evidenciar el control que se lleva frente a tantos métodos y actividades implementadas en el país para contrarrestar estos delitos hacia los niños y adolescentes.

La entidad que más denuncias puede recibir y a su vez entregar estos balances es la Policía Nacional o el Ministerio de Tecnologías de Información por medio de su página de denuncias, pero no es así, no existen esos informes anuales que involucren unos ítems enfocados hacia la población de niños y adolescentes en referencia a la vulnerabilidad o amenazas de Ingeniería Social, con totales o porcentajes de estas denuncias.

Aun cuando algunas cifras encontradas se centran en la pornografía infantil, existen más amenazas que deben ser tenidas en cuenta, pues generan unos registros alarmantes de suicidio; aunque no se ven en cifras, si se evidencian por medios de comunicación como noticias, material impreso, emisoras y en algunos casos las mismas redes sociales.

La recomendación que se haría según esta investigación es crear en cada página estos informes, de una manera detallada de cada uno de los ítems denunciados, a su vez muy centrada en la población de niños y adolescentes con una misma muestra. Para evidenciar la evolución año a año de este flagelo de la Ingeniería Social. Para ello se puede realizar encuestas a nivel país utilizando, invitaciones a realizarla en las redes, pues es en este ámbito es donde se encuentra la población a encuestar. Hacerla con herramientas de encuestas en línea que darán un puesto

a la ciudad que las aplique, realizar campañas de motivación y enfatizar que esto se hace en pro de resguardar los derechos de los niños y adolescentes fomentando la denuncia temprana y así mismo de los riesgos que se puede correr al realizar estas actividades de discriminación, burla hacia los demás.

Con esto los adolescentes a los cuales se enfocarían más estas encuestas, verían que los entes de control están alertas en esta situación y que no solo realizan estas campañas de vez en cuando generando conciencia, pero no reforzando el tema con la prevención continua y acompañada permanentemente.

Se podría extender estas encuestas hacia los padres y docentes para incluirlos en los controles que en gran parte dependen de ellos para que nuestros adolescentes no se vean involucrados. Afianzando así periódicamente la capacitación y actualización en las tecnologías.

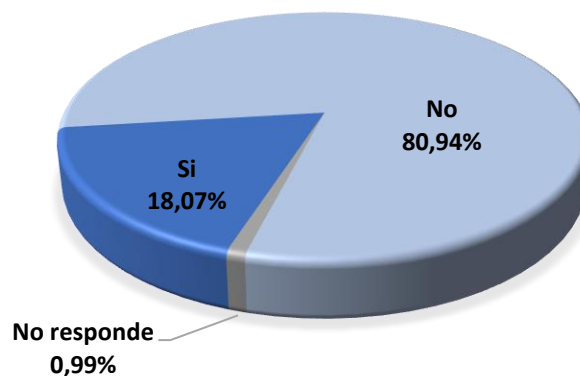
Tabla 5. Tabla Promedio vulnerabilidad por la Ingeniería Social en Colombia

AÑOS	2013	2014	2015	2016	2018	PROMEDIO
Si	37,0%	11,8%	17,5%	14,0%	10,0%	18,07%
No	63,0%	83,2%	82,5%	86,0%	90,0%	80,94%
No responde	0,0%	5,0%	0,0%	0,0%	0,0%	0,99%

Fuente: El Autor

Ilustración 8. Promedio vulnerabilidad por la Ingeniería Social en Colombia

PROMEDIO VULNERABILIDAD POR LA INGENIERÍA SOCIAL EN COLOMBIA



Fuente: El Autor

Para esto realizamos un sumatoria de los porcentajes recopilados año a año, según trabajos encontrados en la investigación con relación a la vulnerabilidad de haber sido víctima de Ingeniería Social. Dando como dato final un promedio del 18.07% de víctimas a lo largo de 5 años en Colombia.

7. CONCLUSIONES

- Se planteo metodologías como la capacitación u orientación a los niños y adolescentes entre los 11 a 17 años en Colombia, con esto ayudamos en la educación de cómo pueden llegar a manejar sus datos personales y a si mismo políticas de seguridad para no verse expuestos a posibles ataques.
- Se realiza un análisis según todos los estudios y antecedentes investigados en Colombia, identificando así todos los riesgos que corren los adolescentes con la ingeniería social, encontrando que cada año se han presentado episodios de ataques que pueden ser evitados con el seguimiento y acompañamiento de los padres o de adultos.
- Se identifica según un análisis de cifras y resultados año a año que los ataques de ingeniería social se enfocan más en la población vulnerable la cual acude a los niños y adolescentes, que a su vez son los generadores de datos en la red.
- Se realiza análisis sobre la metodología técnica y táctica de seguridad propuesta por organizaciones dedicadas a la seguridad en Colombia para conocer su grado de eficiencia, eficacia y efectividad.
- Se realiza análisis sobre el grado de conocimiento y apropiación por parte de los padres o adultos responsables en el uso de herramientas recomendadas por Organizaciones que garanticen la seguridad de los adolescentes en las redes sociales.
- Identificamos que la ingeniería social es una problemática que nos afecta de manera general a la comunidad colombiana, solo que este proyecto delimita en niños y adolescentes pues ellos constituyen nuestro futuro y está en nuestras manos dar pautas para el correcto manejo de la información y datos en las redes sociales, Si bien es cierto que las organizaciones dedicadas a la seguridad en Colombia han realizado programas para la disminución en la ingeniera social en los adolescentes, es pertinente que sea un tema nacional tratado en todos los colegios, comunidades de diferentes estratos socioeconómicos y prevenir antes de corregir.
- Con la realización de este proyecto damos a conocer algunos programas que apoyan y contribuyen con la seguridad informática. Pues Colombia se ha visto afectada por delitos informáticos y la inclusión de los padres y tutores en la adecuada y oportuna supervisión de los niños y adolescentes.

8. RECOMENDACIONES

- Después de realiza esta monografía podemos recomendar un trabajo a fondo con los padres de familia en identificar y a su vez como actuar y ayudar a sus hijos a manejar correctamente las redes sociales.
- Las autoridades nacionales deben implementar programas de capacitación sobre ingeniería social a padres y adolescentes que presentan mayor riesgo de ataques.
- Difundir con más campañas educativas el uso de las herramientas tecnológicas que permiten a padres y tutores identificar un riesgo inminente de ingeniería social.
- Generar alertas en las instituciones educativas, crear concursos para que de esta manera se aumente la participación en los adolescentes para evitar ataques de ingeniería social.
- Crear estadísticas año a año de denuncias de todos los delitos que encierra la Ingeniería Social, en las entidades u organizaciones garantes para frenar esta problemática en Colombia y así mismo promocionar el interés de estas organizaciones en cumplir el acompañamiento permanente que promueven en las capacitaciones.

9. DIVULGACIÓN

La divulgación del presente proyecto no posee ninguna restricción, pues la información desarrollada es completamente pública y orientadora. Por esto la divulgación se realizará en el repositorio de la UNAD, para que éste pueda ser consultado por los estudiantes de la UNAD y el resto de los usuarios que ingresen a dicho repositorio.

REFERENCIAS BIBLIOGRÁFICAS

ICONTEC INTERNATIONAL. NORMA TÉCNICA COLOMBIANA - NTC 1486. {En línea}. {Consultado abril 2017}. Disponible en: http://www.unipamplona.edu.co/unipamplona/portallG/home_15/recursos/01_general/09062014/n_icontec.pdf

PLAN DE CAPACITACIÓN, SENSIBILIZACIÓN Y COMUNICACIÓN DE SEGURIDAD DE LA INFORMACIÓN {En línea}. {Consultado abril 2017}. Disponible en: https://www.mintic.gov.co/gestionti/615/articulos-5482_G14_Plan_comunicacion_sensibilizacion.pdf

CRECE EL ACOSO VÍA INTERNET ENTRE ESCOLARES EN COLOMBIA {En línea}. {Consultado abril 2017}. Disponible en: <http://www.mineduccion.gov.co/observatorio/1722/article-300085.html>

LEY 1620 - MINISTERIO DE EDUCACIÓN NACIONAL {En línea}. {Consultado abril 2017}. Disponible en: http://www.mineduccion.gov.co/1759/articulos-327397_archivo_pdf_proyecto_decreto.pdf

LA INGENIERÍA SOCIAL: EL ATAQUE INFORMÁTICO MÁS PELIGROSO {En línea}. {Consultado abril 2017}. Disponible en: <http://www.enter.co/guias/lleva-tu-negocio-a-internet/ingenieria-social/>

EL USO EDUCATIVO DE LAS REDES SOCIALES {En línea}. {Consultado abril 2017}. Disponible en: <http://propuestastic.elarequi.com/propuestas-didacticas/el-trabajo-en-red-y-las-redes-sociales/el-uso-educativo-de-las-redes-sociales/>

FORMATO - NTC 1486. {En línea}. {Consultado abril 2017}. Disponible en: <https://sig.unad.edu.co/>

ABDOLLAH, Mohd. FAIZAL, Ahmad. RABIAH, Yusof. ROBIAH, Zaki. MOHD, Freese. Generic Taxonomy of Social Engineering Attack. Melaka, 2015. Universiti Teknikal Malaysia. Malaysia.

ACKROYD, Richard. Social Engineering Penetration Testing. Elsevier Science. 2014.

AKKER, Ramón. The weakest link: assessing Social Engineering threats. Utrecht, 2014. Utrecht University. Países Bajos.

BERMÚDEZ, Edilberto. Ingeniería social: un factor de riesgo informático inminente en la Universidad Cooperativa de Colombia sede Neiva. Neiva, 2015. UNIVERSIDAD ABIERTA A DISTANCIA – UNAD. Tolima.

CALVO, Santiago. PULIDO, Cristina. Retos y riesgos del uso de Internet por parte de los menores. ¿Cómo empoderarlos? En: Comunicar. Vol.; 20. No. (oct.2012); p. 65-72.

CASTRO, Mauricio. Ingeniería social, el elemento humano de la seguridad; contramedidas y planes de acción para fortalecer la seguridad en las organizaciones. San Salvador, 2016. Universidad Don Bosco. El Salvador.

FREIRE, Teresa. CORTEZ, María. Las vulnerabilidades humanas en relación a la Seguridad Informática para evitar la fuga de información confidencial en el Departamento de Recursos Humanos de la Universidad Técnica. Ambato, 2013. Universidad Técnica de Ambato. Ecuador.

GARCIA, Gerardo. JOFFRE, Víctor. MARTINEZ, Gerardo. LLANES, Arturo. Cyberbullying: forma virtual de intimidación escolar. En Revista Colombiana de Psiquiatría. Vol.; 40. No. (Mar.2011); p. 115-130.

HADNAGY, Christopher. Ingeniería social. El arte del hacking personal. Anaya Multimedia-Anaya Interactiva, 2011. 400p

HEIRMAN, Wannes. WALRAVE, Michel. Como predecir la perpetración adolescente del ciberacoso escolar: aplicación de la Teoría de la Conducta Planificada. En: Picotea. Vol.; 24. No. (nov.2012); p. 614.

MARÍN, Daniel. RUIZ, Geraldine. Raigoza, Mónica. El acoso sexual en los jóvenes a través de las redes sociales en los grados noveno del colegio corazónista en la ciudad de Medellín. Medellín, 2016. COORPORACION UNIVERSITARIA UNIMINUTO. Colombia

OOSTERLOO, Bernard. Managing Social Engineering Risk - Making social engineering transparent. Enschede, 2008. University o Twente. Países Bajos.

ORTEGA, Jessica. BUELGA, Sofía. CAVA, María. Influencia del clima escolar y familiar en adolescentes, víctimas de ciberacoso. En: Comunicar. Vol.; 24. No.(Feb.2016); p. 57-65.

PIÑAR, José. RODOTÀ, Stefano. BUTARELLI, Giovanni. BENYEKHLEF, Karim. Murillo, Pablo. GREGORIO, Carlos. FLEISHER, Peter. Redes sociales y privacidad del menor. Editorial Reus S.A., 2011. 336 p

SÁNCHEZ, Carmen. MORENO, Willebaldo. Violencia a través de redes sociales en estudiantes universitarios: bullying y cyberbullying. Ciudad de México, 2016. Universidad Nacional Autónoma de México. México.

URRUTIA, José. HERNÁNDEZ, Geovanna. Ingeniería social a través de medios informáticos, análisis de las posibles amenazas existentes en la facultad de ciencias administrativas de la universidad de Guayaquil. Guayaquil, 2015. Universidad de Guayaquil. Ecuador.

DUARTE, María Claudia. LONDOÑO. *DigiApuntes*. {En línea}. {Consultado abril 2017}. Disponible en: 17 de 03 de 2014. <http://blogs.colombiadigital.net/digiapuntes/cyberbullying-o-acoso-cibernetico-y-la-ley-1620-en-colombia/>.

RODRÍGUEZ, Ellien Yulieth. Trabajo Final – Ad hoc. {En línea}. {Consultado agosto 2018}. Disponible en: junio de 2018. <http://openaccess.uoc.edu/webapps/o2/bitstream/10609/81255/6/jrodriguezrinTFM0618memoria.pdf>

CASTELBLANCO, Diana Angélica. SÁNCHEZ, Marco Tulio. RUIZ, Teodomedes. Trabajo de Grado {En línea}. {Consultado agosto 2018}. Disponible en: septiembre de 2016. <https://repository.libertadores.edu.co/bitstream/handle/11371/934/RuizRam%C3%ADrezTeodomedes.pdf?sequence=2&isAllowed=y>

GÓMEZ, Astrid Carolina. CASTILLEJO, Diana. VARGAS, Germán. Praxis Pedagógica {En línea}. {Consultado agosto 2018}. Disponible en: enero de 2013. <http://revistas.uniminuto.edu/index.php/praxis/article/view/990>

GUERRERO, David. MONCAYO, Laura. PARRA, Juanita. Tesis de Grado {En línea}. {Consultado agosto 2018}. Disponible en: 2015. http://www.institutomerani.edu.co/publicaciones/tesis/2015/cyberbullying%20_acoso_escolar_era%20virtual.pdf.

RINCÓN, Alberto. ÁVILA, William. Simbiosis vital para describir el Cyberbullying en Colombia, en este caso tomaremos una de las preguntas la cual es “Ha sufrido algún ataque cibernético” {En línea}. {Consultado agosto 2018}. Disponible en: 2014. <http://www.scielo.org.co/pdf/recig/v12n14/v12n14a09.pdf>

ANEXO 1. RESUMEN ANALÍTICO EN EDUCACIÓN - RAE

Fecha de Realización: 04/11/2018
Título: PROBLEMAS DE INGENIERÍA SOCIAL Y SU IMPACTO EN LA ADOLESCENCIA COLOMBIANA
Autor: MONTES AGUDELO CAROLINA VARGAS FORERO VIVIANA ROCIO
Palabras Claves: Ingeniería social, Grooming, prevención, Cyberbullying, Ciberacoso, Gossip, Nativos Digitales, Inmigrantes Digitales.
Descripción: Esta monografía se realiza como proyecto de grado para el programa de especialización en seguridad informática.
Fuentes: PLAN DE CAPACITACIÓN, SENSIBILIZACIÓN Y COMUNICACIÓN DE SEGURIDAD DE LA INFORMACIÓN {En línea}. {Consultado abril 2017}. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G14_Plan_comunicacion_sensibilizacion.pdf CRECE EL ACOSO VÍA INTERNET ENTRE ESCOLARES EN COLOMBIA {En línea}. {Consultado abril 2017}. Disponible en: http://www.mineducacion.gov.co/observatorio/1722/article-300085.html LEY 1620 - MINISTERIO DE EDUCACIÓN NACIONAL {En línea}. {Consultado abril 2017}. Disponible en: http://www.mineducacion.gov.co/1759/articles-327397_archivo_pdf_proyecto_decreto.pdf LA INGENIERÍA SOCIAL: EL ATAQUE INFORMÁTICO MÁS PELIGROSO {En línea}. {Consultado abril 2017}. Disponible en: http://www.enter.co/guias/lleva-tu-negocio-a-internet/ingenieria-social/ EL USO EDUCATIVO DE LAS REDES SOCIALES {En línea}. {Consultado abril 2017}. Disponible en: http://propuestastic.elarequi.com/propuestas-didacticas/el-trabajo-en-red-y-las-redes-sociales/el-uso-educativo-de-las-redes-sociales/ ABDOLLAH, Mohd. FAIZAL, Ahmad. RABIAH, Yusof. ROBIAH, Zaki. MOHD, Freese. Generic Taxonomy of Social Engineering Attack. Melaka, 2015. Universiti Teknikal Malaysia. Malaysia. ACKROYD, Richard. Social Engineering Penetration Testing. Elsevier Science. 2014. AKKER, Ramón. The weakest link: assessing Social Engineering threats. Utrecht, 2014. Utrecht University. Países Bajos.

BERMÚDEZ, Edilberto. Ingeniería social: un factor de riesgo informático inminente en la Universidad Cooperativa de Colombia sede Neiva. Neiva, 2015. UNIVERSIDAD ABIERTA A DISTANCIA – UNAD. Tolima.

CALVO, Santiago. PULIDO, Cristina. Retos y riesgos del uso de Internet por parte de los menores. ¿Cómo empoderarlos? En: Comunicar. Vol.; 20. No. (oct.2012); p. 65-72.

CASTRO, Mauricio. Ingeniería social, el elemento humano de la seguridad; contramedidas y planes de acción para fortalecer la seguridad en las organizaciones. San Salvador, 2016. Universidad Don Bosco. El Salvador.

FREIRE, Teresa. CORTEZ, María. Las vulnerabilidades humanas en relación a la Seguridad Informática para evitar la fuga de información confidencial en el Departamento de Recursos Humanos de la Universidad Técnica. Ambato, 2013. Universidad Técnica de Ambato. Ecuador.

GARCIA, Gerardo. JOFFRE, Víctor. MARTINEZ, Gerardo. LLANES, Arturo. Cyberbullying: forma virtual de intimidación escolar. En Revista Colombiana de Psiquiatría. Vol.; 40. No. (Mar.2011); p. 115-130.

HADNAGY, Christopher. Ingeniería social. El arte del hacking personal. Anaya Multimedia-Anaya Interactiva, 2011. 400p

HEIRMAN, Wannes. WALRAVE, Michel. Como predecir la perpetración adolescente del ciberacoso escolar: aplicación de la Teoría de la Conducta Planificada. En: Picotea. Vol.; 24. No. (nov.2012); p. 614.

MARÍN, Daniel. RUIZ, Geraldine. Raigoza, Mónica. El acoso sexual en los jóvenes a través de las redes sociales en los grados noveno del colegio corazonista en la ciudad de Medellín. Medellín, 2016. COORPORACION UNIVERSITARIA UNIMINUTO. Colombia

OOSTERLOO, Bernard. Managing Social Engineering Risk - Making social engineering transparent. Enschede, 2008. University o Twente. Países Bajos.

ORTEGA, Jessica. BUELGA, Sofía. CAVA, María. Influencia del clima escolar y familiar en adolescentes, víctimas de ciberacoso. En: Comunicar. Vol.; 24. No. (Feb.2016); p. 57-65.

PIÑAR, José. RODOTÀ, Stefano. BUTARELLI, Giovanni. BENYEKHFLEF, Karim. Murillo, Pablo. GREGORIO, Carlos. FLEISHER, Peter. Redes sociales y privacidad del menor. Editorial Reus S.A., 2011. 336 p

SÁNCHEZ, Carmen. MORENO, Willebaldo. *Violencia a través de redes sociales en estudiantes universitarios: bullying y cyberbullying*. Ciudad de México, 2016. Universidad Nacional Autónoma de México. México.

URRUTIA, José. HERNÁNDEZ, Geovanna. *Ingeniería social a través de medios informáticos, análisis de las posibles amenazas existentes en la facultad de ciencias administrativas de la universidad de Guayaquil*. Guayaquil, 2015. Universidad de Guayaquil. Ecuador.

DUARTE, María Claudia. LONDOÑO. *DigiApuntes*. {En línea}. {Consultado abril 2017}. Disponible en: 17 de 03 de 2014. <http://blogs.colombiadigital.net/digiapuntes/cyberbullying-o-acoso-cibernetico-y-la-ley-1620-en-colombia/>.

RODRÍGUEZ, Ellien Yulieth. Trabajo Final – Ad hoc. {En línea}. {Consultado agosto 2018}. Disponible en: junio de 2018. <http://openaccess.uoc.edu/webapps/o2/bitstream/10609/81255/6/jrodriguezrinTFM0618memoria.pdf>

CASTELBLANCO, Diana Angélica. SÁNCHEZ, Marco Tulio. RUIZ, Teodomedes. Trabajo de Grado {En línea}. {Consultado agosto 2018}. Disponible en: septiembre de 2016. <https://repository.libertadores.edu.co/bitstream/handle/11371/934/RuizRam%C3%ADrezTeodomedes.pdf?sequence=2&isAllowed=y>

GÓMEZ, Astrid Carolina. CASTILLEJO, Diana. VARGAS, Germán. Praxis Pedagógica {En línea}. {Consultado agosto 2018}. Disponible en: enero de 2013. <http://revistas.uniminuto.edu/index.php/praxis/article/view/990>

GUERRERO, David. MONCAYO, Laura. PARRA, Juanita. Tesis de Grado {En línea}. {Consultado agosto 2018}. Disponible en: 2015. http://www.institutomerani.edu.co/publicaciones/tesis/2015/cyberbullying%20_acoso_escolar_era%20virtual.pdf.

RINCÓN, A. ÁVILA, W. Simbiosis vital para describir el Cyberbullying en Colombia, en este caso tomaremos una de las preguntas la cual es “Ha sufrido algún ataque cibernético” {En línea}. {Consultado agosto 2018}. Disponible en: 2014. <http://www.scielo.org.co/pdf/recig/v12n14/v12n14a09.pdf>

Contenido del documento:

Esta monografía presenta un análisis de los problemas a los que se ven abocados los adolescentes a causa de la ingeniería social, en el contexto de las actuales costumbres del manejo de las redes, con el fin de definir estrategias y prevenir la exposición de esta información personal de los niños y adolescentes entre los 11 a 17 años en Colombia.

La falta de conocimiento en seguridad informática hace que se vean expuestos a gran cantidad de amenazas y riesgos. Por esto se describirá un análisis de esta problemática social en los adolescentes y a su vez el planteamiento de estrategias o recomendaciones que pueden llegar a evitar o minimizar el daño en la sociedad y en las generaciones futuras.

La información que un adolescente sube a las redes sociales divulga información personal acerca de: (Donde vive - Cuáles son sus traslados frecuentes - Cuáles son sus lugares favoritos - Donde estudia - Cuáles pueden ser sus contraseñas de redes sociales - Publicación de fotografías que pueden ser utilizadas para dañar o vulnerar su integridad)

Uno de tantos fenómenos que se ven en la actualidad con respecto al manejo de las redes sociales puede ser en un horario de descanso escolar, evidenciando el manejo de más de 200 dispositivos tecnológicos conectados al mismo tiempo, desbordando la generación de información en unas pocas horas o minutos.

Esto no se veía en otros tiempos pues la forma de acceder a dichos dispositivos era limitada para las empresas o las personas que tenían medios económicos altos para la adquisición de estos.

Vemos como cada día los adolescentes se ven expuestos al robo de sus datos confidenciales, por medio de criminales disfrazados de usuarios corrientes que no generarían ninguna amenaza aparente, pero vemos como están expuestos a abusos y riesgos que pueden llegar a ser fatales.

Esta monografía fue seleccionada de tal forma que aportara a nuestro conocimiento y puntos de vista con respecto al daño que puede estar causando la ingeniería social en nuestros adolescentes colombianos. Evidenciando que tienen el mayor flujo de acceso a las redes sociales, convirtiéndose así en uno de los puntos más débiles, al generar casi la mitad de los datos que existen en la red. Y su falta de conocimiento en seguridad informática hace que se vean expuestos a gran cantidad de riesgos y vulnerabilidades.

Si nos enfocamos en concientizar las nuevas generaciones como son los adolescentes, estamos aportando a la sociedad en el cuidado personal, manejando controles, reglas, normas o buenas prácticas en el uso de las redes sociales, para que no se vean expuestos a delincuentes o a su vez, comprendan las implicaciones legales y penales que pueden incurrir por la falta de respeto hacia la diversidad de los demás, controlando así sus comentarios o publicaciones en las redes sociales.

Metodología: Monografía.

Conceptos nuevos:

- **Grooming:** Se refiere a la importunación que realiza una persona adulta con el propósito de fundar e influenciar a un menor de edad ya sea un niño, o un adolescente con el fin de profanarlo o abusarlo sexualmente.
- **Gossip:** Son las murmuraciones en la red que pueden ser muy perjudiciales, ya que los rumores pueden ser propagados a gran velocidad y afectar a muchas personas, que no pueden hacer nada para defenderse.
- **Nativos Digitales:** Se utiliza este término a los menores y jóvenes en la etapa de nacimiento que corresponde al año 1980 a la presente época, que se les ha facilitado adaptarse con mayor agilidad a la vanguardia de las tecnologías.
- **Pedófilo:** Se utiliza para identificar a las personas mayores de edad que poseen inclinación sexual hacia los menores de edad manteniendo fantasías sexuales con esta población.
- **Pederasta:** Se utiliza para identificar a los delincuentes mayores de edad que abusan sexualmente de los menores de edad.
- **Ley 1620 del 15 de marzo de 2013** "POR LA CUAL SE CREA EL SISTEMA NACIONAL DE CONVIVENCIA ESCOLAR Y FORMACIÓN PARA EL EJERCICIO DE LOS DERECHOS HUMANOS, LA EDUCACIÓN PARA LA SEXUALIDAD Y LA PREVENCIÓN Y MITIGACIÓN DE LA VIOLENCIA ESCOLAR"

Conclusiones: La ingeniería social es una problemática que afecta de manera general a toda la población, en este proyecto nos enfocamos en los niños y adolescentes pues ellos constituyen nuestro futuro. Por lo tanto, está en nuestras manos mostrar que existen entidades, organizaciones, grupos que enseñan buenas prácticas en el correcto manejo de la información personal en las redes sociales y así mismo la de los demás, por medio de actividades, programas y leyes que garantizan la prevención o el apoyo si son víctimas de este flagelo en Colombia.

Si se forma en esta etapa de la niñez y adolescencia, se disminuye en el futuro gran cantidad los ataques, amenazas por la falta de conocimiento de la ingeniería social, formado jóvenes con bases en los sistemas de gestión de la seguridad de la información para así convertirlos en garantes de una correcta, responsable y consiente utilización de las tecnologías.

AUTOR: MONTES AGUDELO CAROLINA
VARGAS FORERO VIVIANA ROCIO