GUIA DE BUENAS PRÁCTICAS PARA REDUCIR RIESGOS DE ENGAÑOS A MENORES ENTRE 13 A 15 AÑOS EN REDES SOCIALES

GUIDE TO GOOD PRACTICES TO REDUCE RISKS OF DECEPTION TO MINORS BETWEEN 13 AND 15 YEARS OF AGE ON SOCIAL NETWORKS

Mayra Alejandra Peña Sandoval.
Diana Marcela Sánchez Rodríguez.
Héctor Manuel Herrera.

RESUMEN

Las redes sociales a lo largo de los años se han convertido en parte importante de nuestra vida cotidiana, siendo utilizadas para comunicarnos de manera más rápida al realizar procedimientos e intercambio de información de manera más frecuente y con mayor facilidad, es por esto que en el mundo se han realizado debates sobre cómo deberían ser abordadas las buenas prácticas en la ciberseguridad ya que en este extenso campo de redes sociales existen problemáticas como el ciberbullying ,grooming ,suplantación de identidad, phishing, difamación y calumnias entre otras, es por eso que en el presente proyecto de aplicación se abordarán los principales riesgos y vulnerabilidades de este entorno orientado a la población menor de edad ya que su manejo de ciberseguridad en redes sociales no es adecuado en la mayoría de los casos, también serán abordadas las diferentes problemáticas que se han presentado por el manejo incorrecto de los protocolos de seguridad informática y qué repercusiones trae en caso de no adoptar las buenas prácticas, para ello se construirá una guía de buenas prácticas en el uso de las redes sociales.

Palabras Clave: *ciberdelincuente, Red social, vulnerabilidad, Riesgos.*

ABSTRACT

Social networks over the years have become an important part of our daily lives, being used to communicate more quickly by carrying out procedures and exchanging information more frequently and more easily, which is why in the In the world, debates have been held about how best practices in cybersecurity are likely to be addressed, since in this extensive field of social networks there are problems such as cyberbullying, grooming, identity theft, phishing, defamation and slander among others, that is why in This application project will address the main risks and vulnerabilities of this environment oriented to the minor population since its management of cybersecurity in social networks is not adequate in most cases, problems will also be addressed the different that have been presented due to the incorrect handling of computer security protocols and what effects it brings in ca s or of not adopting good practices.

Keywords: *Social network, Risks, Cybercriminal, vulnerability.*

1. INTRODUCCIÓN

La tecnología ha tenido un crecimiento a gran escala en los últimos años, tanto que la gran mayoría ven como una prioridad tener un celular táctil desde muy temprana edad, aun así, no se les ha enseñado a los jóvenes de la nueva generación, la importancia de darles un buen uso a los aparatos tecnológicos. Hoy en día se conocen varias redes sociales en donde los cibernautas interactúan diariamente. Entre las más destacadas encontramos: Facebook, Instagram, Twitter, Tik Tok, WhatsApp, entre otras. Dado que el impacto mediático de las aplicaciones es de uso masivo, no siempre se tienen ciertos cuidados a la hora de usarlas, hecho que puede causar problemas que en ocasiones incluso atentan contra la vida, la familia y el trabajo[1].El uso de redes sociales genera sensación de cercanía permite comunicarse fácilmente pero también se muestran a personas malintencionadas como los ciberdelincuentes que están atentos al menor descuido de los usuarios como dejar sus credenciales guardadas en el sistema o enlazar otro tipo de cuentas a sus redes sociales como por ejemplo las cuentas bancarias. Es de conocimiento global que se pueden generar ciberdelitos en las redes sociales como: phishing, suplantación de identidad, acoso y ciberbullying, difamación, calumnias, chantaje. Muchos de los riesgos a los que nos vemos a diario es a robo de identidad debido a que en redes sociales damos a conocer nuestra información personal sin ningún tipo de restricción, también pueden ser víctimas de acoso ya que al realizar publicaciones de nuestras actividades diarias estamos suministrando la información necesaria para que podamos ser perseguidos y/o acosados, también se corre el riesgo a ser víctimas de difamación ya que debido a la seguridad de las redes sociales la autenticidad de cada perfil no es fiable y tampoco segura.Durante el desarrollo de la guía planteada de las buenas prácticas se abordarán varios temas de interés referentes a las buenas prácticas en el entorno para el uso de las redes sociales, en este caso, enfocándose en menores de edad en el rango de 13 a 15 años que es nuestro enfoque. Luego se procederá a nombrar las principales regulaciones enfocadas en su contenido en los menores de edad, posteriormente se realizará una breve contextualización de los riesgos a los que se pueden ver enfrentados los menores en estos entornos digitales.

[1] De acuerdo al artículo elaborado por Juan pablo Monroy Ramírez, Comunicador social de la uniminuto que tiene por título “Atadura cibernauta, La dependencia a las redes sociales”.

Pregunta de investigación

¿Cómo minimizar los riesgos en ataques cibernéticos en redes sociales a menores de edad de 13 a 15 años, a partir de una guía de buenas prácticas?

Objetivo General

Construir una guía de buenas prácticas que permita minimizar riesgos y vulnerabilidades de la población en menores de edad de 13 a 15 años cuando hacen uso de redes sociales.

Objetivos Específicos

- Identificar los principales riesgos que se presentan en las redes sociales cuando los menores de edad no tienen precaución con la información que proporcionan.
- Analizar las diferentes vulnerabilidades que se han presentado en redes sociales hacia menores de edad y cuáles son las más recurrentes.
- Implementar la guía propuesta hacia una parte de la población de 13 a 15 años de edad.

Alcance

El alcance consistirá en realizar un análisis sobre las pautas que se deben seguir a la hora de tener la responsabilidad de manejar una red social se sabe que los niños y adolescentes adquieren este rol desde muy temprana edad cuando la edad aproximada es 14 años y existen menores de edad que con 9 años están manejando una red social sin supervisión de un adulto. En la actualidad la proyección es generar conciencia con esta guía de buenas prácticas con el fin de minimizar los riesgos y vulnerabilidades principales que han corrido nuestros jóvenes y han terminado con la afectación psicológica y social de estos actos ejecutados por los ciberdelincuentes

que varios de ellos se han llevado a un campo judicial.

Como resultado de este proyecto se tendrá una guía de buenas prácticas para menores de edad de 13 a 15 años para determinar cuáles deben ser las pautas para seguir en el momento de proporcionar información sensible en una red social y así mismo hacerlo de una manera responsable para minimizar los riesgos a los que se ven enfrentados los menores de edad según la ley un menor de edad.

2. MARCO TEÓRICO

En Colombia no hay normativa que hable de seguridad de la información a menores de edad por ellos nos guiamos de la normativa ISO/IEC 27001 y la ley 1581 del 2012, en este escenario de los riesgos de engaños a menores de edad es necesario comprender los demás estudios que se han realizado sobre el tema que abordamos en este documento y que han ayudado ampliamente a tratar esta problemática se puede identificar que la sociedad es responsable de emplear técnicas y guías para que estos riesgos de engaño se reduzcan.

Como es de conocimiento público los menores de edad no conocen a qué riesgos se pueden ver involucrados al usar y proporcionar información en una red social en esta guía se realizará una breve síntesis de algunas investigaciones que se han realizado alrededor de este tema, que si bien es de conocimiento público que existen es necesario abordarlo en su totalidad para minimizar estos entornos de riesgo y vulneración.

Redes sociales: Es un medio de interacción de un individuo hacia otro para compartir intereses en común en tiempo real.

Usuario: Persona que utiliza un equipo de cómputo y/o servicio que se encuentra en la red.

Usuario Victima: Persona que ha sufrido algún tipo de daño por la acción ejecutada de otro individuo

Usuario victimario: Sujeto que ejecuta una acción con el fin de afectar específicamente a otra persona.

Ciberseguridad: Su objetivo es proteger la infraestructura computacional de las organizaciones.

Datos: Información concreta sobre un tema en específico que permite analizar y procesar.

Información: Conjunto de datos recopilados procesados y ordenados para la comprensión de un tema en particular y que es de interés para el área o para las personas que los tratan.

Antecedentes

4.1 Peligros de las redes sociales: Cómo educar a nuestros hijos e hijas en ciberseguridad

En este artículo realizado por (Astorga C, 2019)., indican que "*los principales peligros a los que los jóvenes se ven enfrentados son el cyberbulling, grooming, sexting y adicción. Se aclara que, No obstante, en muchas ocasiones, la manipulación de la información que se realiza es en contra de las políticas de seguridad y privacidad que deberían imperar en el manejo de datos personales, al considerar la vulnerabilidad de la población a la que hace énfasis este estudio"* (Astorga C, 2019).

Mencionan que consejos indican los profesionales de ciberseguridad tales como: *"no aceptar solicitudes de amistad de sujetos desconocidos, no tener público los contenidos que sube en la red social, no subir a la red información personal como direcciones, no publicar fotografías de niños y niñas que muestren sus centros educativos y ubicación de los hogares, entre otros"* (Astorga C, 2019).

4.2 Menores y redes ¿sociales?: de la amistad al cyberbullying

En el artículo realizado por (Jorge del Río, 2010) indica textualmente que: *"Lo que parece claro es que esta relación especial que mantienen con la tecnología supone el acceso a múltiples oportunidades en todos los ámbitos, al mismo tiempo que plantea nuevas situaciones que pueden ser problemáticas para los menores. La alarma social se acrecienta cuando estos riesgos son desconocidos para los educadores, los padres y las madres, que han crecido en un contexto no digital",* por lo general, de este fragmento del

articulo podemos realizar un análisis en situaciones que los padres se ven enfrentados a diario como lo son el desconocimiento de los “Amigos” virtuales que tienen sus hijos, la clase de conversaciones que sostienen sus hijos y los tipos de archivos que envían sin conocer las consecuencias que esto les puede traer.

4.3 Características y percepciones sobre el uso de las plataformas de redes sociales y dispositivos tecnológicos por parte de los adolescentes

En el artículo realizado por (García-Jiménez A, 2020) hace referencia a “El crecimiento exponencial del acceso a dispositivos móviles está fomentando un uso continuo y más intensivo de ciertos servicios y aplicaciones online”.

Algunos de los hallazgos tienen que ver con la confirmación de la tendencia de las edades para la adquisición del propio smartphone (media de 11 años); Edad, que también se muestra como el referente para el acceso a las redes sociales. Junto al acceso multipantalla, también se observa un consumo diario superior de Whatsapp en relación con el de las plataformas de redes sociales. “, como se sabe es preocupante la cantidad abismal que existen todos los días de menores de edad con acceso a redes sociales y la poca seguridad basados en la falta experticia que tienen nuestros jóvenes a la hora de ver riesgos en la red, También indican factores determinantes para los adolescentes como lo son: “las necesidades *de socialización y la búsqueda de entretenimiento orientan el uso online de la adolescencia”* (García-Jiménez A, 2020).

4.4 Redes sociales: ¿ambiente apto para menores?

De acuerdo con el articulo realizado por (H, 2010) textualmente cito:

“Estas plataformas tecnológicas también son propicias para reproducir comportamientos humanos reprochables. La invasión a la privacidad, el “voyerismo” o la intimidación, son potenciados en muchos casos en estos ambientes virtuales”. Con esto podemos concluir y basado en la idea del autor que los adolescentes están seguros que si envían una foto o un archivo en video y lo borran lo hacen definitivamente, pero lo que no saben es que en el

momento que se toman fotos o videos con un dispositivo cualquier ciberdelincuente puede acceder a ellos de distintas maneras, también están expuestos a que alguien adulto se haga pasar por un menor de edad ganando su confianza y de esta manera manipulándolo, también el hostigamiento por parte de adultos o de menores de edad por estas redes sociales.

4.5 Redes sociales: riesgos y amenazas

Del artículo realizado por (R, 2017) ,se puede resaltar una parte bastante importante que pretende generar un poco de conciencia*: "a mayor accesibilidad, mayor riesgo y a mayor riesgo, mayor necesidad de supervisión y control de los padres y tutores sobre el uso de las redes sociales por parte de los niños, niñas y adolescentes principalmente"*, El autor se basó en un estudio realizado que lleva por título Estudio sobre Redes Sociales en Centroamérica y el Caribe del año 2016, de esto podemos verificar que a cada avance tecnológico se requiere mayor acompañamiento de un adulto para las actividades que los adolescentes en este caso consideran que son normales y que no son riesgosas.

También realiza un estudio estadístico cito textualmente *"No significa necesariamente que el restante 73% de los usuarios de las redes sociales ignoren o desconozcan los riesgos del internet y sus redes sociales, sino que una lectura distinta nos puede hacer creer que estas personas, aunque conocen de los peligros de la red, los ven como algo lejano a ellos, es decir, que han desarrollado una creencia de autoinmunidad frente a estas amenazas. Ellas y ellos saben de los riesgos, inclusive, han sido testigos directos o indirectos de una serie de casos en los que las redes sociales exponen inclementemente la privacidad y la dignidad de las personas, sobre todo, de nuestros niños, niñas y adolescentes, a pesar de ello se asumen a sí mismos y a su círculo cercano como en una zona "confort" de seguridad."* (R, 2017)

4.6 Las redes sociales y sus factores de riesgos

En el artículo elaborado por (A, 2017)**,** Los jóvenes siempre tienen un gran interés por ver contenido no apto para menores de edad es por esto que recurren a proporcionar información

en sitios web para poder acceder a estos videos o fotos por otro lado la autora indica cito textualmente:

"La red de Internet crece cada día más, a medida que las personas van conociendo este recurso tecnológico, va despertando principalmente en los jóvenes una gran curiosidad por conocer páginas que muestren contenido no apto para menores, lo que ha ocasionado un gran problema en el uso indebido de las redes sociales." Es por esto que se deben realizar acompañamientos por difícil que parezcan por parte de padres, educadores y demás actores relacionados con el desarrollo de nuestros niños. Niñas y adolescentes.

4.7 El uso de las redes sociales virtuales en niños, niñas y adolescentes

Para nuestra investigación tomaremos como referencia el artículo donde citaremos: *"Internet y las redes sociales ocupan un lugar cada vez más preponderante en el proceso de socialización de niños, niñas y adolescentes. Sin embargo, la participación de este proceso supone el acceso a insumos costosos, los cuales profundizan la brecha entre quienes acceden y quiénes no. ¿En qué medida los niños/as y adolescentes de diferentes estratos socioeconómicos acceden a este tipo de tecnología y, cuando acceden, estas diferencias impactan en las razones por las que usan las redes sociales?"* (Torre, 2012),

En este artículo publicado hace 10 años podemos observar la preocupación de que todos pudiéramos acceder a internet sin ningún tipo de limitación hoy en día podemos observar que un gran porcentaje de las personas tiene acceso a internet sin limitaciones, pero esto nos deja un gran interrogante, ¿Cómo estamos controlando la información que compartimos por internet?

4.8 Consentimiento de los menores de edad

En el artículo realizado por (Villanueva, 2017, págs. 8-9),en su artículo pretende darnos a conocer dos tipos de jóvenes que puedes estar enfrentados a realizar la aceptación bajo su responsabilidad que son dos tipos los jóvenes emancipado y los no emancipados también indica que no se puede realizar la conclusión de que joven tiene la suficiente madurez o no ya que no hay una edad estipulada en la que se adquiere dicha madurez pero en los códigos civil indican

que un joven con la edad de 14 años como sabemos el sentido de responsabilidad es bastante debatible también nos relata como han identificado la edad de 14 años para poner como responsable al menor sobre la protección de sus datos personales por esto mismo hemos visualizado no solo en Bolivia como lo menciona el autor sino en varios países como los menores de edad entregan sin mayor reparo sus datos personales a desconocidos por las redes sociales.

4.9 Peligros de las redes sociales: Cómo educar a nuestros hijos e hijas en ciberseguridad

El artículo realizado por (Astorga-Aguilar & Schmidt-Fonseca, 2019), el autor indica que nuestros adolescentes se ven bastante expuestos en la red basándose en los principales delitos de los cuales son víctimas como es la pornografía infantil puede ser que tengan en sus galerías fotos en trajes de baño, pijamadas donde realizan integración entre ellos ya que son objeto de sujetos depravados enfatiza el autor es por esto que realiza la recomendación de estar más atentos a todo lo que suben sus hijos e incluso los archivos que suben a la red los padres de familia, también podemos visualizar el sexting al que se ve expuesto el menor de edad por buscar algún tipo de aprobación por un tercero y es altamente aprovechada por el ciberdelincuente, entre otros.

4.10 Redes sociales, desinformación, cibersoberanía y vigilancia digital: una visión desde la ciberseguridad

En el artículo su autor (BARTOLOMÉ, 2021), menciona que el internauta puede ser configurado a experimentar una fuerte adicción a la red social presentando impaciencia revisando con frecuencia su inicio y sus novedades posteriormente esto puede ser corroborado por un profesional de la salud sin problema alguno ya que en la actualidad estos casos se presentan con frecuencia.

4.11 La importancia de la ciberseguridad y los derechos humanos en el entorno virtual

El autor (derechos, 2021),Indican que es larga la rama de delitos ejecutados por ciberdelincuentes en el entorno virtual como por ejemplo el secuestro virtual, este puede darse en el ambiente de una persona amenazada como indican textualmente aprovechándose de su

angustia, su familia que es la contactada para realizar la extorsión y en caso de que no accedan a las peticiones del delincuente podría hasta rea víctima de desaparición forzada.

Podemos ver en un fragmento del artículo donde los autores se refieren a la instigación de suicidio esto lo podemos ver recurrentemente en los adolescentes y sus “Amigos" virtuales realizan una serie de manipulaciones para que el menor atente contra su vida.

4.12 Estudio de ciberseguridad de los últimos 5 años en el tema de delitos informáticos dirigido a los niños, niñas y adolescentes en el departamento del huila

El autor (ORTIZ, 2020) menciona en su estudio realizado que Colombia cuenta con una estructura legislativa para tomar medidas preventivas y correctivas en los actos delictivos considerados por la ley. Con esto no indica que han sido creadas las leyes 1273 del 2009 (de la protección de la información y de los datos) y la ley 1581 del 2012 (Protección de Datos Personales). también hace la referencia de que aun con esas leyes creadas no es suficiente ya que cada día avanzan los ciberdelincuentes en vulnerar nuestros datos personales y que por ende deben ser más eficaces en cuanto a normativas y soluciones que hagan que estas personas reduzcan sus ataques.

4.13 Ciberseguridad para menores, asunto de todos.

El artículo (america, 2018) expuesto, relata que los menores de edad son ciudadanos digitales y por este mismo motivo los adultos tienen la obligación de ejercer responsabilidad en cuanto a la ciberseguridad de los menores, indican que los menores de edad son blanco principal en las redes sociales de personas que generan alteraciones directas en su autoestima ejerciendo presión con bullying indican que en el año 2017 el menor de edad fue víctima de ciberdelitos en un porcentaje del 75% que si vemos es directa la responsabilidad del entorno en el que se encuentra el menor de edad que lo guías las personas adultas ya se en las instituciones educativas y en su mismo hogar para que minimicen las vulneraciones de sus datos como de su intimidad.

4.14 Los riesgos de Internet y las redes sociales para los niños

La guía (Nuevo, 2022) expuesta, nos muestra muchos de riesgos que actualmente encontramos en internet como lo es el Grooming y el Sexting, El Sexting corresponde al intercambio de fotografías o videos eróticos entre los mismos jóvenes o quizás personas desconocidas, con las que después pueden llegar a extorsionarse y puede causar daños psicológicos.

Dentro del articulo también tenemos la edad que nos sugieren un niño puede entrar en las redes sociales, donde nos dicen que es mínimo de 14 años, aunque se evidencia en muchos casos los niños crean perfiles sin autorización de sus padres por eso resaltan la importancia del dialogo y confianza que se tenga de los padres con sus hijos.

4.15 Redes sociales y derecho a la intimidad de los menores de edad

En el artículo de la Universidad Católica de Argentina (Nieto, 2016) podemos resaltar que toda persona tiene derecho a la intimidad dentro del marco legal pero cuando se trata de un menor de edad se debe analizar con demasiada cautela ya que se debe consentir la disposición por parte de los representante legales, se resalta también dentro del articulo la importancia del seguimiento y control de los menores de edad en al redes sociales ya que en muchas de ocasiones los victimarios son otros menores de edad y causan daños irreparables, nos sugiere para evitar que los menores de edad estén tan expuestos a estas vulnerabilidad se manejen cuentas de control parental o seguimiento continuo cuando se hace uso de las redes sociales.

4.15 Seguridad Digital en Colombia

RESOLUCIÓN NÚMERO 00500 DE MARZO 10 DE 2021

El Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) expidió la resolución en la cual establecen los lineamientos y estándares para la seguridad digital además de un modelo de privacidad que deben tener cuenta los entes públicos y/o individuos ya que es necesario conocer ampliamente sus deberes en la ejecución de las pautas para minimizar el desconocimiento poblacional y así mismo disminuir las brechas en la seguridad digital de los ciudadanos en general.

Existe un convenio de MINTIC con CSIRT que es una plataforma de la policía nacional enfocada a emergencias informáticas en esta plataforma se deben reportar los ciudadanos o entes públicos cuando sean víctimas de ataques en la red para no caer en manos de ciberdelincuentes, también como crear contraseñas seguras ya que también es un riesgo latente ser víctimas de robo de credenciales es un grupo netamente enfocado a la seguridad informática y a responder de manera efectiva todas las solicitudes que se les presenten de vulneración ya sea a ordenadores o a los ciudadanos en general con temas cibernéticos de extrema urgencia.

4.16 LEY ESTATUTARIA 1581 DE 2012

Esta ley fue establecida en el año 2012 para la protección de datos personales en esta ley se estipulan varios artículos que la persona natural puede exigir como por ejemplo si una persona va a ser parte de una base de datos que se va a suministrar a terceros esta persona debe dar su consentimiento en caso de no darlo no pueden divulgar su información personal también es legítimo si el ciudadano exige el retiro de su información debe ser destruida su información así mismo la detención de divulgación de la misma.

4.17 LEY 1273 DE 2009

La ley 1273 se denomina textualmente “de la protección de la información y de los datos”, en esta ley se establecen los delitos a los que se puede enfrentar una persona si realiza acceso abusivo a un sistema informático o si capta ilegalmente datos personales de BD de datos externas sin autorización, reglamente el uso de software malicioso para dañar un sistema informático.

Entidades que contribuyen a prevenir los ataques cibernéticos

- **En Tic Confío**

  El Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) creo el proyecto catalogado como En Tic Confío que una plataforma digital en la cual se promueven estrategias para reducir el riesgos en redes sociales va enfocado principalmente a niños entre 6 y 18 años ya que han sido potenciales víctimas de los ciberdelincuentes al mismo tiempo que

de los depredadores sexuales por estos entornos digitales su principal objetivo es sensibilizar a los niños y adolescentes para que puedan fácilmente identificar los riesgos y así prevenirlos.

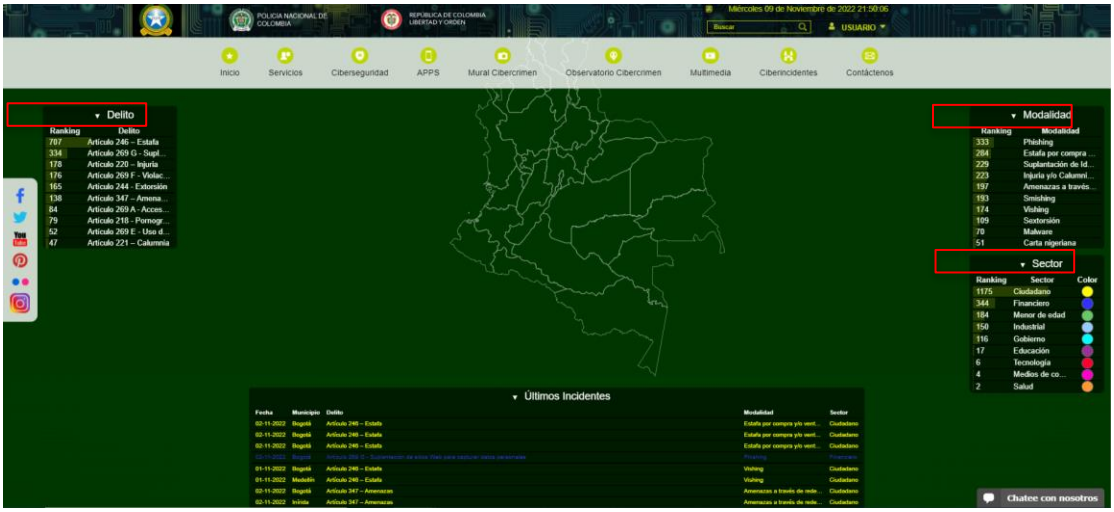
También hay disponibilidad de una academia En Tic Confío para las edades entre 11-28 años en la cual buscan promover el uso positivo del internet y que así mismo sean promotores de las buenas prácticas digitales en su entorno cercano.

- **Centro cibernético policial:**

El centro cibernético fue creado para atender solicitudes de los ciudadanos en delitos informáticos, en esta plataforma podemos visualizar principalmente en tiempo real cuantos ataques se han realizado en un intervalo de tiempo en nuestra demostración realizamos una prueba de 01/10/2022 al 09/11/2022 en esta plataforma podemos visualizar en tiempo real delitos, modalidades y sector en el que se presentan.

Es deber aclarar que en los delitos están catalogados legalmente en el código penal, también que las modalidades que indican son las diferentes situaciones a las que se pueden ver enfrentados los ciudadanos y también los menores de edad no obstante especificando también que nos permite también visualizar los delitos de los que han sido víctimas los sectores financieros, educativos, industrial, gubernamental, tecnológico, salud, medios de comunicación entre otros.

Ilustración 1.Mapa de Ciber incidentes tiempo real.



Fuente: caivirtual.policia.gov.co

También ofrecen servicios tales como:

Ilustración 2.Servicios centro cibernético policial.

Fuente: caivirtual.policia.gov.co

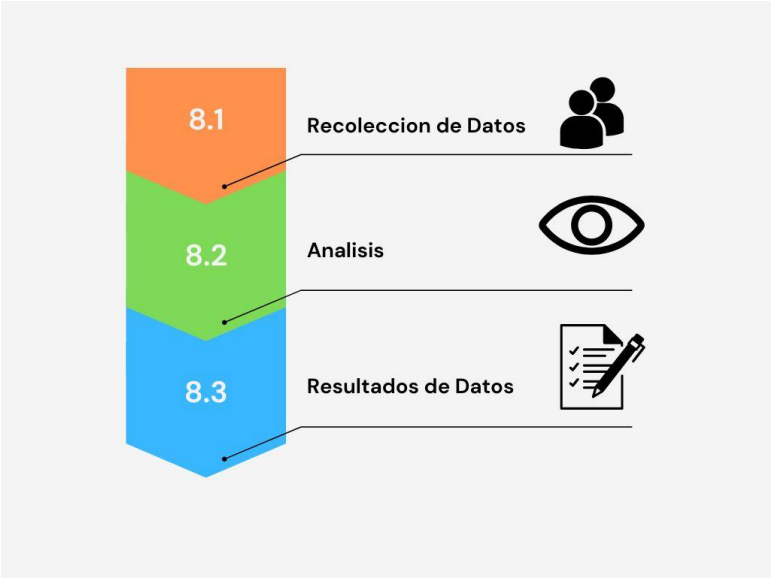
Estos servicios ayudan a minimizar los riesgos que se pueden presentar tales como en una organización ser víctima de ransomware o como persona natural al ser víctima de captación ilegal de datos con el fin de pagar una determinada cantidad de dinero por que el ciberdelincuente libere los datos sin tener la certeza si los devolverá en su totalidad, también encontramos dentro de estos servicios recomendaciones, guías, etc., es de gran ayuda si se tiene poco conocimiento en estos temas y esta plataforma es de gran ayuda para minimizar el riesgo de sufrir ataques cibernéticos.

3. METODOLOGÍA

Se extraerá una muestra de 147 estudiantes en dos instituciones rural y urbana en las cuales serán evaluados mediante una encuesta cualitativa los conocimientos que tienen en ciberseguridad y las diferentes situaciones a las que se han visto expuestos en las redes sociales, para esto se plantearan diferentes situaciones comunes a los que los niños y adolescentes se enfrentan en una plataforma digital con los resultados de dicho estudio se construirá una guía de buenas prácticas

que sea gráficamente atractiva con tips sencillos para que sea de fácil entendimiento para el público infantil y adolescente del cual se pretende obtener atención instantánea para que ellos tenga un control seguro de las redes sociales de las cuales hagan uso frecuentemente.

Ilustración 3.Guía de pasos.



Fuente: Autor

Identificación de Datos

Con el fin de poder analizar dos ambientes diferentes realizaremos nuestra encuesta en dos colegios, el primero será en el Colegio José Manuel Restrepo (IED) ubicado en la localidad de Puente Aranda en la ciudad de Bogotá D.C., el segundo colegio será la Institución Educativa Promoción Social del Municipio de El Pital del departamento del Huila.

A continuación, relacionaremos el link de la encuesta:

- https://forms.office.com/r/KfzifZUWK9

8.1Recolección de Datos

Se realiza muestra a una población de estudiantes 147 entre las edades entre el rango 13 a 15 años, para analizar los conocimientos que tienen en las plataformas digitales, con el fin de identificar si en el momento en que los menores de edad hacen uso de las redes sociales cuentan con la supervisión de sus padres o un adulto responsable. Con la encuesta cuantitativa se busca identificar con qué frecuencia comparten información los menores de edad a través de estas plataformas.

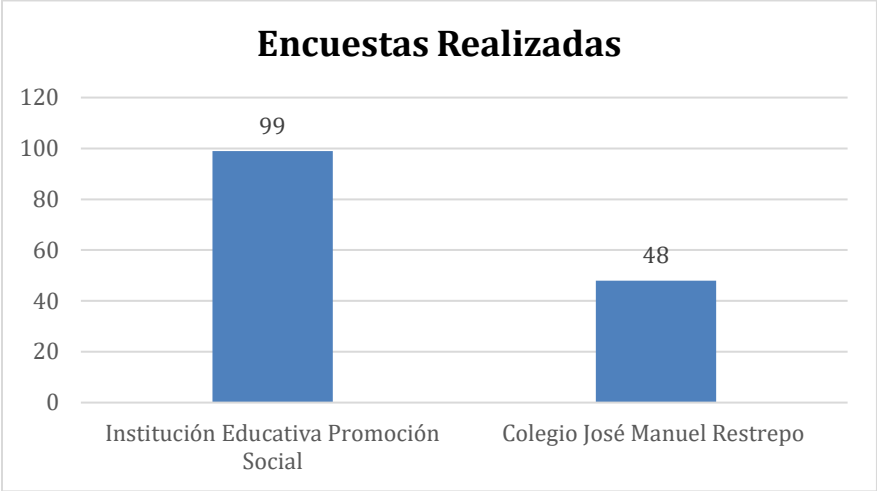
8.2 Análisis

En el entorno digital de las redes sociales existen grandes riesgos y vulnerabilidades más cuando centramos nuestra vista en adolescentes algo que es realmente claro es que nuestros adolescentes no tienen precauciones a la hora de difundir su información personal y tampoco a la hora de exponerse enviando imágenes intimas cabe aclarar que en Colombia no hay leyes que regulen los comportamientos inapropiados y el mal manejo de la información hemos visto en noticias, periódicos y medios digitales todos los delitos que se comenten casi a diario en contra de adolescentes y su vulneración al derecho a la intimidad podemos verlo con adultos que engañan y manipulan para tener acceso a estos archivos sensibles de la misma manera en todo el mundo han sido castigados con penas considerables al ser captados comercializando estas imágenes al ser clasificados como pornografía infantil ya que aunque sea con conocimiento del menor que accedieron a dichas imágenes digitales nunca fue recibido un consentimiento por parte del menor a ser divulgado dicho material.

8.3 Análisis y Resultados

Después de realizar la encuesta en las dos instituciones colegios se evidencian los siguientes resultados:

Gráfico 1.Encuestas Realizadas.



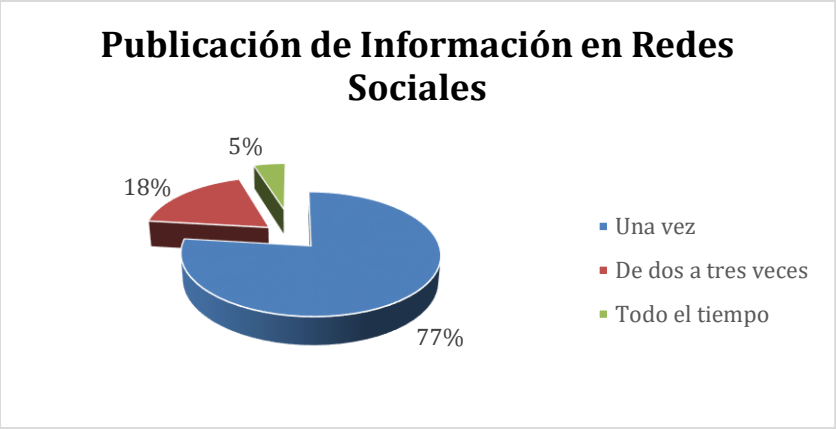
Fuente: Autor

En el Colegio José Manuel Restrepo ubicado en la ciudad de Bogotá zona urbana se realizó la encuesta a 48 alumnos de un total de 50 alumnos en las edades entre 13 a 15 años donde se evidencia que se realizó la encuesta a un total de un **96%.**

En la Institución Educativa Promoción Social ubicado en el Pital - Huila zona urbana se realizó la encuesta a 99 alumnos de un total de 240 alumnos en las edades entre 13 a 15 años donde se evidencia que se realizó la encuesta a un total de un **41%.**

En relación con la pregunta si los alumnos han publicado información personal en redes sociales podemos evidenciar que al menos una vez el 77% de los alumnos comparten información personal al menos una vez, el 18% de dos a tres veces y un 5% todo el tiempo lo hace. (Ver Figura 1).

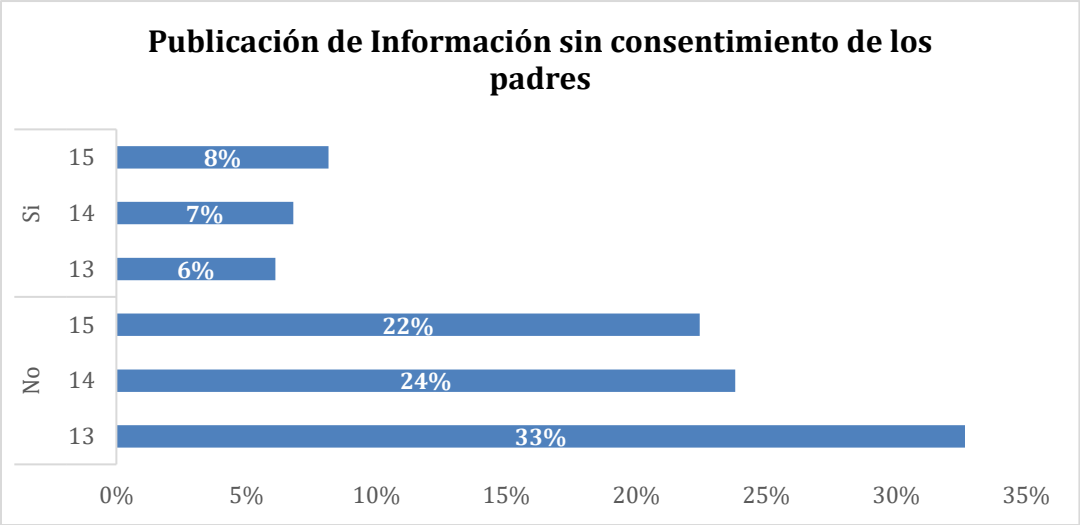
Gráfico 2.Publicación de Información en Redes Sociales.



Fuente: Autor

Aunque la edad aconsejable para utilizar redes sociales en menores de edad pudimos evidenciar que los menores de edad en el rango de 13 a 15 años publican en un 21% información en redes sociales sin consentimiento de sus padres, también se puede evidenciar que de este 21%, el 13% corresponde a alumnos de 13 y 14 años.

Gráfico 3.Publicación de Información Sin Consentimiento de los padres.

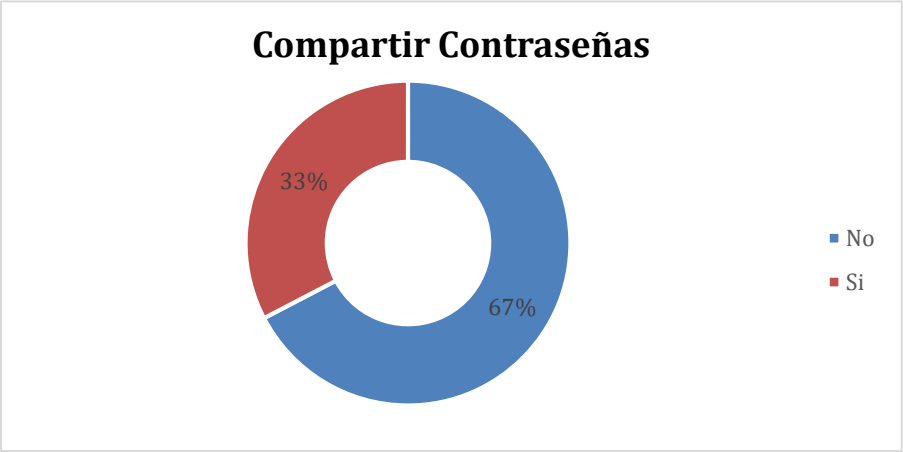


Como nos muestra en el siguiente Blog nos muestra la importancia de compartir información en redes sociales donde “De los que comparten datos, cerca del 50% ha sufrido la

pérdida de datos en sus teléfonos inteligentes, 52% desde su computadora y 20% desde su tableta" (Liderman, s.f.), Esto no muestra como un gran porcentaje de la población pierda información por publicar demasiada información personal en redes sociales.

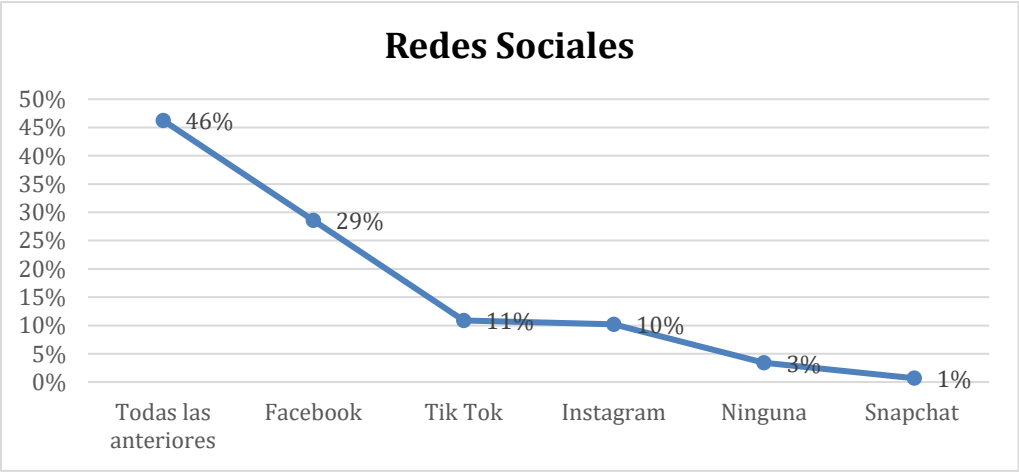
Dentro de nuestro análisis pudimos evidenciar que en nuestros menores de edad un 33% aparte de compartir información personal comparte la contraseña de sus redes sociales con alguien distinto a sus padres, razón de alarma ya que podemos encontrarnos con suplantación y robo de identidades.

Gráfico 4.Compartir Contraseñas.



En relación con las redes sociales que más utilizan pudimos evidenciar que un 46% utilizan varias redes sociales al tiempo, haciendo que en mayor proporción se encuentren más expuestos al robo de información

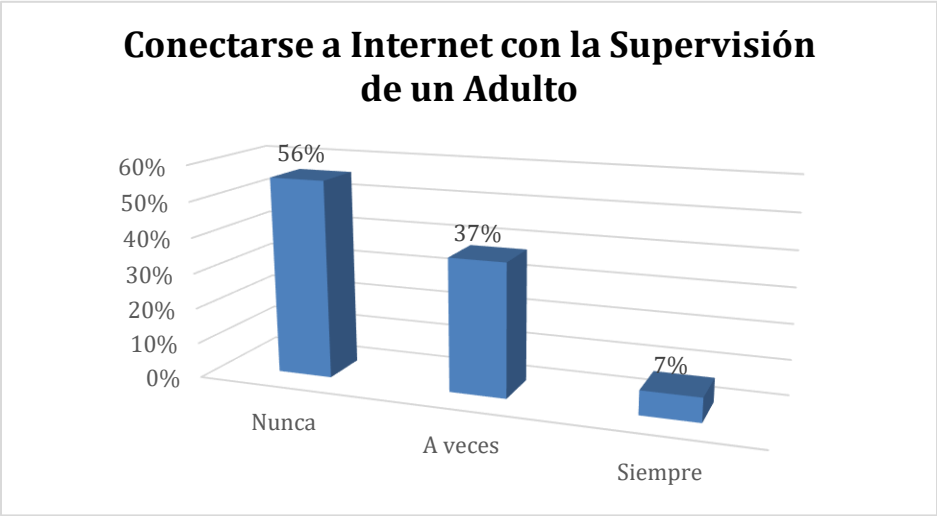
Gráfico 5.Redes Sociales.



Esto nos confirma que las redes sociales más utilizadas por los alumnos son Facebook, Instagram y Tik Tok, exponiéndolos más a delitos como la distribución de material de abuso sexual infantil, delito que pone en riesgo la seguridad digital de los niños, niñas y adolescentes. Por esto es necesario capacitar y afianzar la formación en buenas prácticas de seguridad de la información a nuestros menores de edad.

Dentro de lo recomendado para el uso de redes sociales en menores de edad se recomienda que se haga bajo la supervisión de un adulto, pero evidenciamos que en 56% Nunca se conectar a redes sociales con supervisión, el 37% solo a veces cuenta con supervisión y solo un 7% indica que siempre lo hace con supervisión.

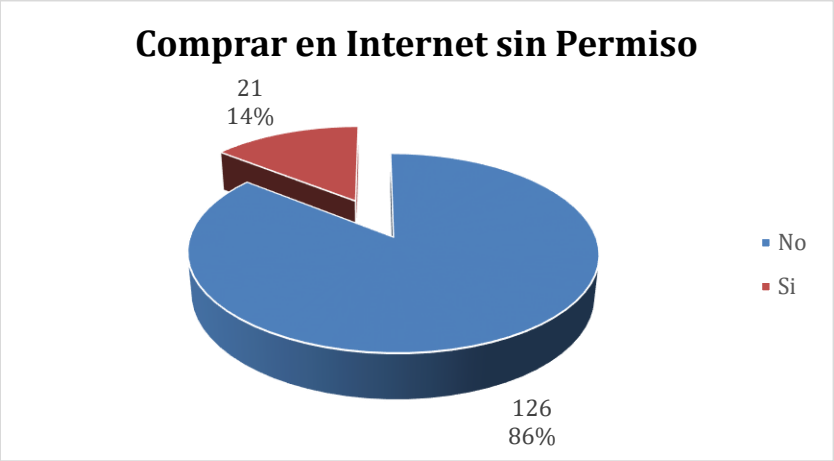
Gráfico 6.Conectarse a Internet con la Supervisión de un Adulto.



Cuando realizamos compras por internet debemos tener precauciones para poder identificar estafas más fácilmente, dentro de alguna de las precauciones como nos muestra en el articulo (Well Fargo, s.f.), que debemos compras solo en sitio Web seguros, evitar vendedores que utilicen tácticas para presionarlos a comprar, establecer alertas para cuentas bancarias.

Dentro del análisis pudimos evidenciar que aunque debemos tener precauciones como adultos a la hora de compras tenemos 21 alumnos para un 14% de estudiantes que realizan compras por internet sin permiso de sus padres, así exponiéndolos a en un mayor porcentaje a robos.

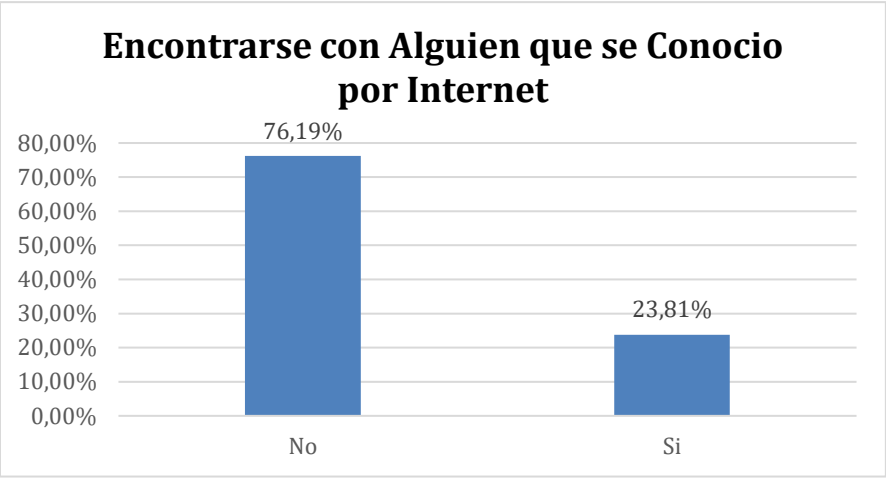
Gráfico 7.Comprar en Internet sin Permiso.



En la página de (El Pais, s.f.), nos muestran que en el 2021 se detectaron 252.000 páginas web a nivel mundial que contenían material de explotación sexual, representando un incremento del 60% en comparación con el 2020, nos resaltan que lo que ha hecho que este número vaya en incremento es la interconectividad a través de internet y el acceso a toda clase de dispositivos electrónicos hayan facilitado este delito.

En la encuesta realizada a menores de edad pudimos evidenciar que el 24% de los alumnos se ha encontrado con alguien que conoció por internet, generando índices de alarma debido a que cuando realizan conexiones en redes sociales en la mayoría de los casos no conocen realmente quien les esta hablando, en muchos casos nos encontramos con perfiles falsos o suplantación de identidad que puede traer riesgos mayores si nos encontramos personalmente con estas personas.

Gráfico 8.Encontrarse con Alguien que se conoció por Internet.



Después de realizado el análisis a las preguntas realizadas a los alumnos podemos encontrar que tenemos un alto porcentaje de desconocimiento de la ciberseguridad donde de los 147 estudiantes 86 estudiantes no conocen el termino, solo 61 estudiantes están familiarizados con el termino, pero tampoco se tiene claro debido a que obtuvieron respuestas como:

- “Si, es no compartir datos personales, contraseñas”.
- “Es como una seguridad de datos personales”.
- “Es lo que protege las redes sociales en casa de algún problema”.

Pero se evidencia que no se tiene la conciencia del uso responsable de las redes sociales ni de la seguridad de la información de manera general.

Después de analizar los resultados encontramos que en la norma técnica **NTC-ISO-IEC COLOMBIANA 27001** (ICONTEC ISO 27001, s.f.) no se enfoca en la protección y cuidado de niños y adolescentes, se determina que podemos seguir las siguientes clausulas ya que aborda la seguridad en sistemas.
Mencionaremos brevemente la cláusula 7.3 y 7.4.

- ✓ **CLAUSULA 7.3 TOMA DE CONCIENCIA**

  En el anexo mencionan la importancia de tener presente la política de la seguridad de la información que de acuerdo con el MINTIC[2] consiste en la preservación de la confidencialidad, integridad y disponibilidad de la información cabe recalcar que es deber de la persona y/o ente público garantizar la privacidad y el cuidado de la información que ha sido suministrada.

- ✓ **CLAUSULA 7.4 COMUNICACIÓN**

  El sistema debe determinar las comunicaciones internas o externas que se lleven a cabo a través del sistema de información para esto se realiza la parametrización de factores que se deben tener en cuenta como el contenido de dicha información que enfocándolo a las redes sociales podrían ser los archivos o conversaciones que son intercambiadas en tiempo real por dos personas (usuarios) en caso tal de que sea un contenido inapropiado que afecte directamente a alguna de las dos personas debe ser un factor de alarma y debe ser controlado por dicho ente público o sitio web.

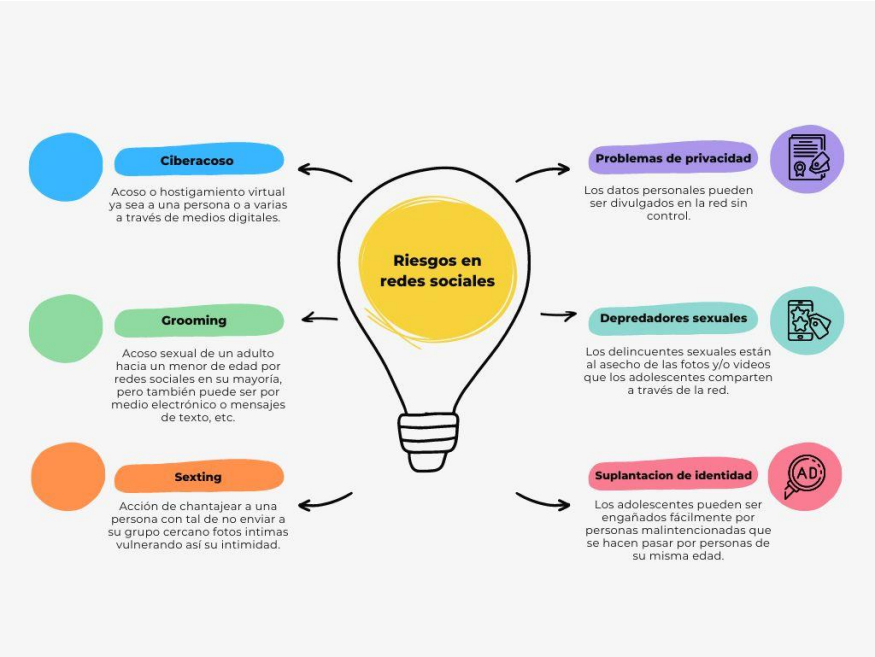
RIESGOS EN LAS REDES SOCIALES

Para dar a conocer los riesgos en redes sociales se encontraron 6 tipos más relevantes dentro de estos tenemos, se evidencia que uno de los factores más peligrosos son los Depredadores

2 De acuerdo con Wikipedia MINTIC indica que,"1.f. Ministerio de Tecnologías de la Información y Comunicaciones."

sexuales ya que los niños y adolescentes pueden tener daños irreparables en su integridad, pero esto sin quitarle relevancia a las demás amenazas.

Ilustración 4.Mapa Riesgos en redes sociales.



CONCLUSIONES

Después de realizar la encuesta se evidencio que la mayoría de los alumnos no cuentan con conocimientos suficientes para realizar uso de las redes sociales de manera responsable, evidenciando que estarían dispuestos a encontrarse con alguien que conocieron en redes sociales, que se conectan a internet sin la supervisión de un adulto y en muchas ocasiones comparten contraseñas con alguien diferente a sus padres.

Por tal motivo se decidió realizar la implementación de la Guía de buenas prácticas en ambos colegios:

Ilustración 5.Estudiantes José Manuel Restrepo (IED).

Colegio José Manuel Restrepo (Bogotá D.C)

Ilustración 6.Estudiantes institución educativa promoción social.

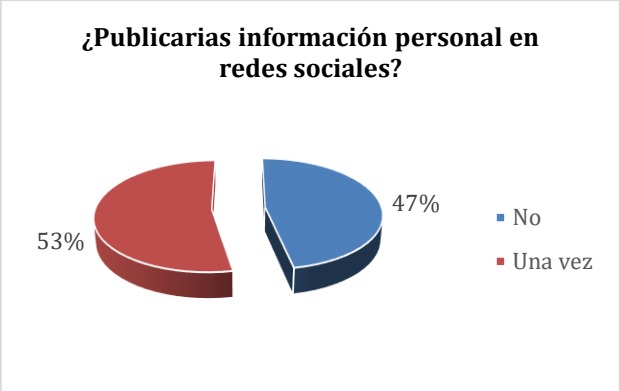
Institución Educativa Promoción Social (El Pital – Huila)

A partir de la aplicación de la Guía se evidencio un notable cambio en la concientización de los alumnos, como:

Se realizó la pregunta de si publicarías información en redes sociales y se evidencio en la primera encuesta el 77% de los alumnos indico que al menos una vez había publicado información en redes sociales, pero después de aplicada la guía se redujo en un 24% ya que el en esta ocasión el 53% indico que publicaría información personal en redes sociales.

ANTES

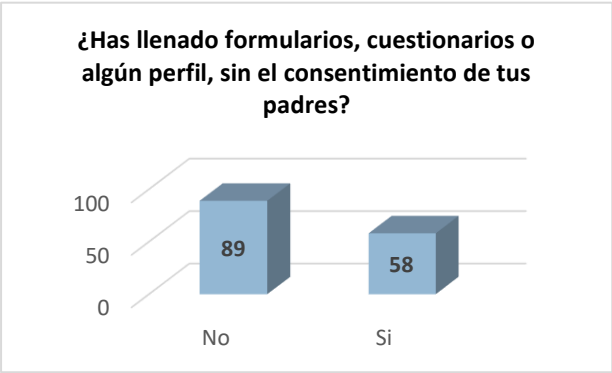
DESPUES



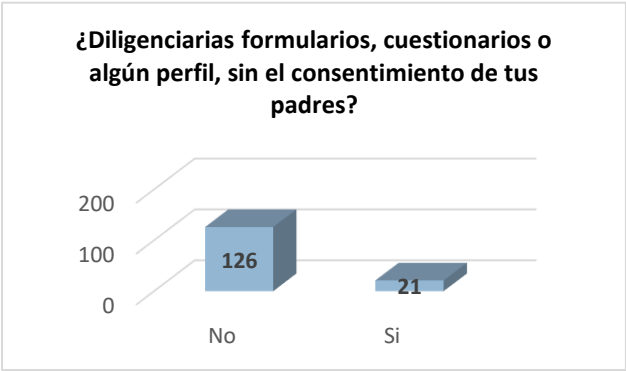
En la segunda pregunta donde indicábamos si llenaría formularios, cuestionarios o algún perfil sin el consentimiento de los padres pudimos evidenciar que en la primera encuesta 58 estudiantes indicaron que sí, pero ya en la segunda encuesta aplicada se pudo evidenciar que solo 21 indicaron que si llenarían formularios, teniendo esto como un resultado 37 estudiantes adicionales que se concientizaron y tuvieron en cuenta que esto no se debe hacer.

Debido a la gran cantidad inseguridad en la que nos encontramos hoy en día en redes

ANTES

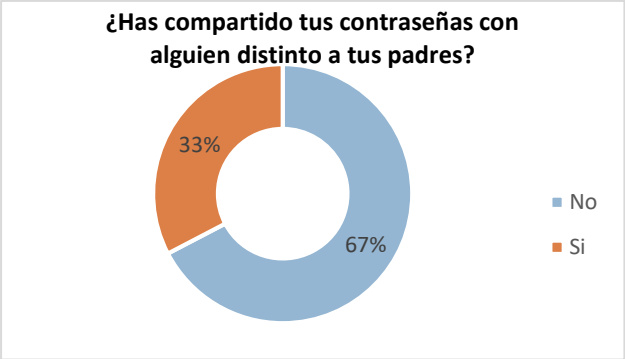


DESPUES



sociales, uno de las fugas de información más grandes es que nuestros niños comparten algo tan importante como la contraseña con cualquier persona sin tener las precauciones del caso, en la guía de buenas de prácticas se enfatizó en las contraseñas seguras y en la importancia de las mismas, después de realizada la segunda encuesta tuvimos una mejoría significativa ya que un 22% adicional de los estudiantes indico que no compartiría sus contraseñas con alguien distinto de sus padres.

ANTES

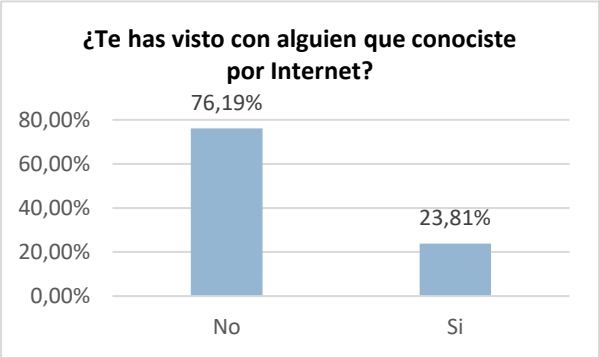


DESPUES

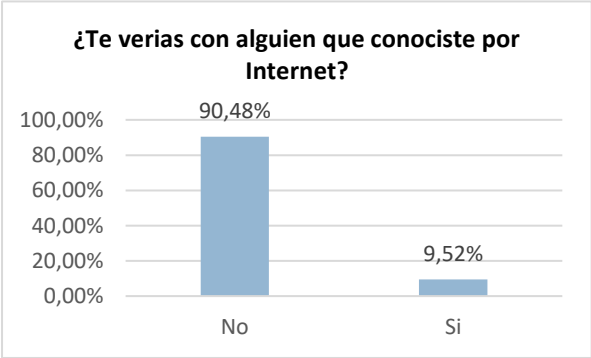
Otro de las preocupaciones constantes que se tienen con los niños a la hora que utilicen

redes sociales es que puedan ser engañados por personas malintencionadas llegando a ser víctimas de estas personas, después de implementada la guía se evidencio que inicialmente un 23,81 de los alumnos se vería con alguien que conoció en internet mientras que en la segunda encuesta se evidencia que se redujo a un 9,52%.

ANTES



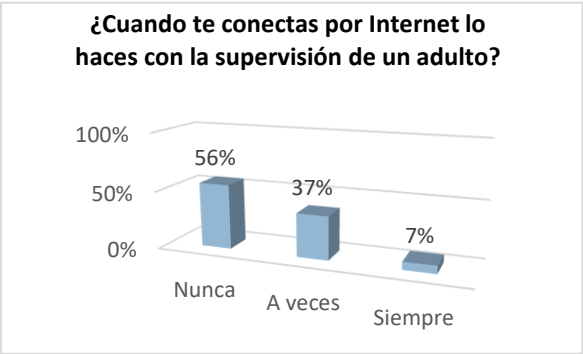
DESPUES



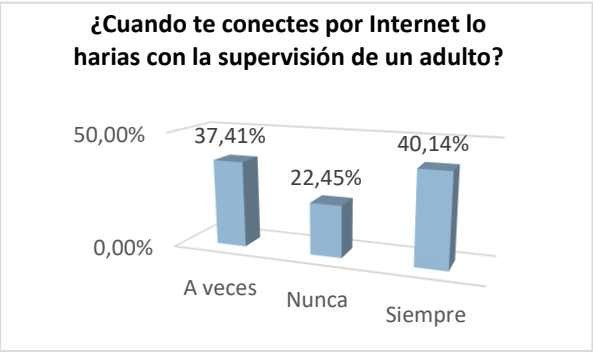
El acceso a redes sociales para menores de edad cada día es menos restringido haciendo que debido a las ocupaciones de los padres y falta de tiempo los niños acceden a estas redes sociales en gran porcentaje solos, en la primera en cuenta pudimos evidenciar que un 56% de los alumnos siempre se conectaban solos a redes sociales, pero después de aplicada la guía indicaron que cuando se conectaran a internet en próximas ocasiones lo realizarían en acompañamiento de un adulto mejorando 34%.

En la pregunta ¿Aceptas y chateas con personas desconocidas en tus redes sociales? Se

ANTES

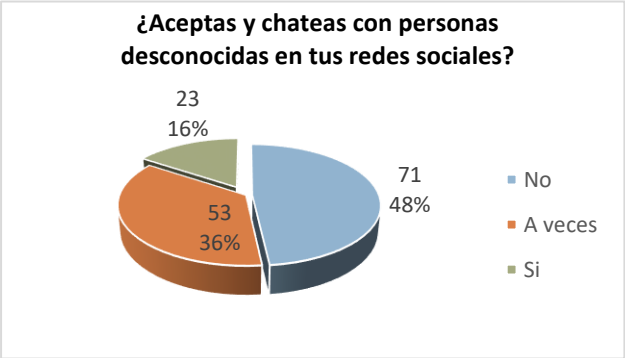


DESPUES



obtuvo una mejoría como se evidencia en la gráfica de un total de 53 niños y adolescentes respondieron que a veces accedían a interactuar con desconocidos en sus redes sociales luego de realizar la concientización con la guía de buenas prácticas un total de 110 contestaron que no aceptarían interactuar con un desconocido por las plataformas digitales con esto.

ANTES

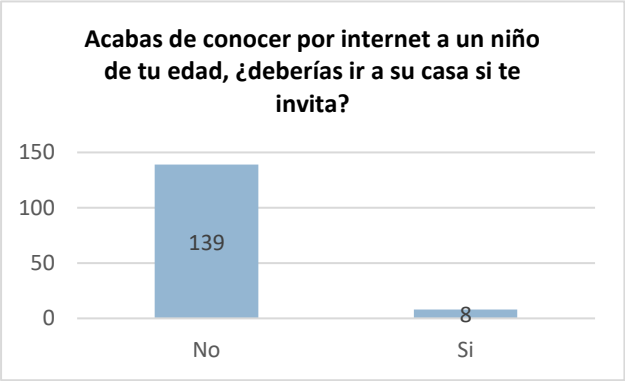


DESPUES

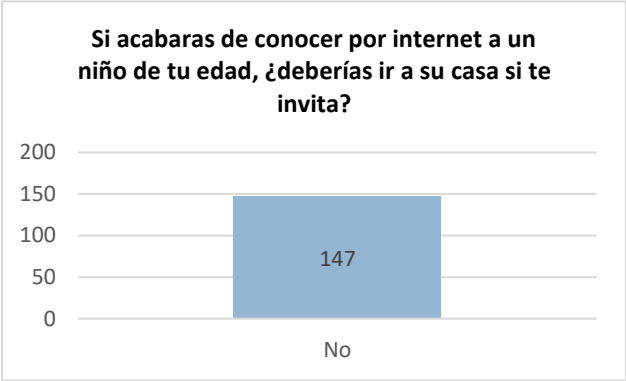
En la pregunta Acabas de conocer por internet a un niño de tu edad, ¿deberías ir a su casa si te invita?, Cuando se planteó la pregunta anteriormente mencionada en la encuesta los niños y adolescentes en una cantidad aproximada de 8 respondieron que si aceptarían ir al encuentro y

después de realizada la prevención en contra de estas peticiones en la guía de buenas prácticas un total de 147 respondieron que definitivamente no accederían a ir a la casa en caso tal de que le hicieran la invitación es decir que nos sirvió en un 100% la guía como prevención a conductas que no deben ser normalizadas.

ANTES



DESPUES



AGRADECIMIENTOS

El presente proyecto de aplicación se lo dedicamos a nuestros padres por su apoyo, esfuerzo diario para ayudarnos a destacar y no solamente en lo profesional sino en el ámbito personal para ser cada día mejores personas y aprender a valorar siempre esos pequeños detalles, aprender a perseverar porque este paso que damos es la mejor recompensa para nuestros padres y para nosotros, agradecemos todo el acompañamiento de nuestro tutor Héctor Manuel Herrera por ayudarnos en cada proceso acompañado de la mejor actitud y responsabilidad para llegar a un buen término con nuestro propósito y ayudarnos a ampliar todo nuestro conocimiento, agradecemos a todas y cada una de las personas que estuvieron con nosotras a lo largo de esta especialización llena de buenos momentos y mucho conocimiento ,que nos apoyaron incondicionalmente con todo esto nos ayudaron a realizar el modelamiento de nuestro articulo para entregarlo con excelencia terminado.

REFERENCIAS

america, S. e. (22 de mayo de 2018). *Seguridad en america*. Obtenido de Seguridad en america: https://www.seguridadenamerica.com.mx/noticias/articulos/15712/ciberseguridad-para-menores-asunto-de-todos

Ángela del BARRIO FERNÁNDEZ, I. R. (2014). LOS ADOLESCENTES Y EL USO DE LAS REDES SOCIALES. *Revista Internacional de Psicología Educativa y del Desarrollo*.

Astorga-Aguilar, C., & Schmidt-Fonseca, I. (2019). Peligros de las redes sociales: Cómo educar a nuestros hijos e hijas en ciberseguridad. *Revista Electrónica Educare, vol. 23, núm. 3*, 10-11.

BARTOLOMÉ, M. C. (2021). Redes sociales, desinformación, cibersoberanía y vigilancia digital: una visión desde la ciberseguridad. *Revista de Estudios en Seguridad Internacional*.

CSIRT. (s.f.). *CSIRT PONAL*. Obtenido de CSIRT PONAL: https://cc-csirt.policia.gov.co/

derechos, L. i. (2021). Erick Francisco Tapia Hernández, Raúl Ruiz Canizales y. *Revista Misión Jurídica*.

EL DERECHO A LA INTIMIDAD Y EL CONSENTIMIENTO DE LOS MENORES DE EDAD. ESPECIAL REFERENCIA A LAS REDES SOCIALES. (2017). *Alejandro Villanueva Turnes*, 8-9.

El Pais. (s.f.). Obtenido de https://www.elpais.com.co/judicial/alerta-por-aumento-de-la-explotacion-sexual-de-ninos-en-internet.html#:~:text=Seg%C3%BAn%20la%20organizaci%C3%B3n%20Internet%20Watch,60%20%25%20en%20comparaci%C3%B3n%20con%202020.

Icontec ISO 27001. (s.f.). Obtenido de https://img1.wsimg.com/blobby/go/b653c9ee-535c-4528-a9c5-bb00166ad0dc/downloads/1cd65ml0r_919353.pdf

ICONTEC ISO 27001. (s.f.). Obtenido de https://img1.wsimg.com/blobby/go/b653c9ee-535c-4528-a9c5-bb00166ad0dc/downloads/1cd65ml0r_919353.pdf

Liderman. (s.f.). Obtenido de https://liderman.com.pe/blog-riesgos-publicar-datos-redes-sociales/

Nieto, M. B. (2016). *Pontificia Universidad Catolica de Argentina.* Obtenido de https://repositorio.uca.edu.ar/bitstream/123456789/3048/1/redes-sociales-derecho-intimidad-nieto.pdf

Nuevo, M. (16 de 05 de 2022). *Guia Infantil.* Obtenido de https://www.guiainfantil.com/articulos/educacion/nuevas-tecnologias/internet-y-las-redes-sociales-riesgos-para-los-ninos/

ORTIZ, H. A. (2020). ESTUDIO DE CIBERSEGURIDAD DE LOS ÚLTIMOS 5 AÑOS EN EL TEMA DE. neiva-hulia, colombia: repositorio unad.

Retana, D. P., & Ficoseco, V. (2021). VIOLENCIA Y DESCORTESIA EN REDES SOCIALES. *Revista Káñina*.

Villanueva, A. (2017). EL DERECHO A LA INTIMIDAD Y EL CONSENTIMIENTO DE LOS MENORES DE EDAD. ESPECIAL REFERENCIA A LAS REDES SOCIALES. *Revista Boliviana de Derecho*, 8-9.

Well Fargo. (s.f.). Obtenido de https://www.wellsfargo.com/es/privacy-security/fraud/bank-scams/online-shopping-scams/

ANEXOS

- Página Web: https://dmsanchezr5.wixsite.com/redessociales

- Guía de Buenas prácticas en formato PDF.