UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ

FACULTAD CIENCIAS DE LA COMUNICACIÓN

Carrera: Periodismo

Proyecto de Investigación

CIBERSEGURIDAD: RIESGO Y AMENAZAS DE LOS JÓVENES EN LAS REDES SOCIALES CASO: COLEGIO FISCAL MIXTO CAMILO PONCE

Previo a la obtención del título de: Licenciada en Ciencias de la Comunicación, Mención Periodismo

Presentado por: María Julissa Zambrano Macías

Tutor: Ing. Jorge Guevara Chávez, Mg.

Manta - Manabí – Ecuador

Agosto, 2018

Declaración de autorización y originalidad

Yo, María Julissa Zambrano Macías, certifico que el proyecto de investigación titulado: “Ciberseguridad: riesgo y amenazas de los jóvenes en las Redes Sociales Caso: Colegio Fiscal Mixto Camilo Ponce”, que presento para la obtención de mi título de Licenciada en Ciencias de la Comunicación, mención Periodismo, es original y ha respetado las normas internacionales de citas y referencias para las fuentes consultadas. Por tanto este trabajo no ha sido plagiado ni total ni parcialmente. Los datos presentados en los resultados han sido reales, no han sido falseados, ni duplicados, ni copiados.

De identificarse alguna falta de fraude, plagio, auto plagio, piratería o falsificación, asumo las consecuencias y acciones que de mi acción se deriven.

_____

María Julissa Zambrano Macías

CERTIFICACIÓN DEL TUTOR:

Ing. Jorge Guevara Chávez, Mg. certifica que:

La señorita **Zambrano Macías María Julissa**, con C.I. **131158615-8**, ha realizado bajo mi supervisión la presente investigación con el tema: **"Ciberseguridad: Riesgos y Amenazas de los jóvenes en las Redes Sociales caso Colegio Fiscal mixto Camilo Ponce".**

En cuanto a lo expuesto certifico que la investigación se encuentra lista para presentación y apta para su defensa. Las opiniones y conceptos vertidos en este trabajo de investigación son tributo del trabajo, perseverancia y originalidad de su autora, siendo de exclusiva responsabilidad.

Jorge Guevara Chávez, Ing.,

Tutor de Tesis

AGRADECIMIENTOS
Y
DEDICATORIA

En primer lugar me gustaría expresar mi agradecimiento a Dios, por brindarme la sabiduría y paciencia de seguir adelante.

Seguido por mi docente el Ingeniero Jorge Guevara Chávez, a quien me gustaría expresar mi agradecimiento por hacer posible la realización de este estudio. Muchas gracias por todo el apoyo, por sus consejos, por la paciencia y motivación para acabar este trabajo satisfactoriamente, gracias por su tiempo.

Gracias a mis padres por el apoyo incondicional, por los valores fomentados, por no desanimarme para seguir luchando por mis sueños, recordándome siempre su apoyo y esfuerzo que realizan todos los días por mí.

Por último pero no menos importante a mi novio Jefferson, pues él es el que me recordaba todos los días sobre mi proyecto de tesis, quien me alentó todos los días con paciencia y amor para seguir trabajando en mi investigación para así lograr la meta tan anhelada como es mi licenciatura.

Muchas gracias a todos

ÍNDICE GENERAL

RESUMEN

Actualmente, los jóvenes estudiantes se enfrentan a un sinnúmero de retos tecnológicos, que si bien representan una ayuda académica, por otra parte pueden ser utilizados en su contra, de ahí la necesidad que se conozca sobre ciberseguridad en las escuelas. Es por ello, que el objetivo principal de este trabajo fue describir la situación actual que tienen los jovenes del Colegio Fiscal Mixto Camilo Ponce, en cuanto a los riesgos y amenazas a los que están expuestos en las redes sociales. Para logar este propósito, se utilizó una investigación de tipo cuantitativa y de campo, ya que los datos se recogieron en el mismo sitio de los acontecimientos. El principal instrumente utilizado para la recolección de datos fue el cuestionario de preguntas cerradas, previa operacionalización de las variables. El universo de estudio lo conformaron 380 estudiantes de la escuela mencionada y se aplicó en una muestra de 80 estudiantes entre 12 a 18 años. Entre los principales resultados se puede apreciar qué importancia dan los jóvenes a las políticas de seguridad que les ofrecen las redes sociales y su exposición ante probables abusos y uso de información sin consentimiento.

Palabras Clave: Ciberseguridad, redes sociales, amenazas.

INTRODUCCIÓN

Culturalmente hablando, la adolescencia siempre estará de moda, por lo que representan un grupo interesante para cualquier mercado que desee encontrar compradores o adictos potenciales. Es así como en el mundo tecnológico, esta población representa un objetivo potencial, tal es el caso de las redes sociales y del internet.

Actualmente, jóvenes y adultos están en riesgo de volverse adictos a las nuevas tecnologías. Los jóvenes los más vulnerables, por muchas razones:

> 1.- Han nacido entre teclados y pantallas, forman parte de su entorno vital, se acercan a ellos sin temor. Usar estos aparatos es para ellos tan natural como caminar.
>
> 2.-Tienen generalmente más tiempo libre para dedicarse a su uso que los adultos.
>
> 3.-Los fabricantes han invertido ciencia y dinero en hacerlos vehículo de diversión y de entretenimiento especialmente pensado para los jóvenes (De Vega & Tejada, 2011, pág. 310)

Cabe destacar, que se vive en una época donde el avance tecnológico se ha convertido en una herramienta indispensable para el desarrollo del ciudadano. Es necesario entonces reconocer, parafraseando a Pons (2013) que nuestras ocupaciones están ya mediadas por un entramado de redes, y que hemos pasado del papel al ordenador en muy poco tiempo, >Multimedia<, >CD-ROM<, >Autopista de la información<, >Sonido digital<, >Televisión por Cable<, >Instagram<, son algunas de las novedades que cada día resultan más presentes e inevitables en nuestra vida.

En consecuencia, la tecnología ha producido un cambio radical, no solo en la forma de comunicarnos, sino también en la forma de vivir y de relacionarnos, sobre todo en los adolescentes, llamados nativos tecnológicos, quienes están mucho más expuestos y desprotegidos a la hora de utilizar las redes sociales, ya que el uso de Internet es accesible desde cualquier sitio, a cualquier hora, de forma totalmente anónima y sin un control adecuado para los diferentes contenidos, espacios y servicios que se pueden utilizar en la red. A esto se suma el gran impacto que ha tenido entre la juventud la penetración de la telefonía móvil, haciéndolos más vulnerables ante el mundo digital.

De ahí, la importancia de la valoración de las amenazas actuales y futuras a los que se enfrenta la población juvenil a nivel mundial, por ello hay que enseñar a los jóvenes a usarlo con prudencia. Al respecto, sostienen De Vega & Tejada (2011) lo siguiente:

> El enganche a los diferentes aparatos electrónicos que forman parte de nuestra vida, implica el enganche a un exceso de actividad comunicativa, de entretenimiento e incluso productiva, pero también el enganche a elevados porcentajes de basura y lleva implícitos no pocos riesgos. Se trata, probablemente, de uno de los fenómenos adictivos más extendidos en la actualidad y, en los últimos años, un asunto en el que cada vez se demanda más la intervención de los clínicos (pág.209)

Es por ello que, muchos países como China, EEUU, Japón, Rusia, México, vienen tomando medidas de seguridad informática para proteger tanto al país como a sus habitantes. En la Cumbre de Lisboa en el año 2009, los países participantes presentaron sus preocupaciones ante la constante violación de la privacidad de sus datos e información, declarando así el ciberataque como una amenaza para las naciones, a lo que entonces se le conoce como Ciberseguridad, en tal sentido, resaltaron la importancia en la construcción y uso de sistemas informáticos más seguros.

En Ecuador, de acuerdo con el INEC, el perfil del internauta está definido así: más hombres que mujeres, que usa la red principalmente para comunicarse, informarse, educarse y trabajar. Además, se conecta desde su hogar, un acceso público, instituciones educativas y trabajo. La mayoría de usuarios son jóvenes entre 16 y 24 años.

De igual forma, en el último informe de INEC, reconoce que desde 2006 hasta 2014 se ha incrementado 11 veces el número de usuarios de internet a nivel nacional, y se hace una proyección para 2020 de hasta 22 veces más el número de usuarios.

Por otra parte, el diario El Telégrafo el 21 de marzo de 2017 publicó lo siguiente: A pesar de sus grandes ventajas, la utilización de redes sociales por este medio puede crear adicción, desinformación y uso inadecuado de datos personales.

Sobre la base de lo expuesto hasta aquí, y teniendo en claro que es deber de todo periodista de difundir información de actualidad e interés social, la autora del presente proyecto de investigación, realizó un proceso de documentación bibliográfica de acuerdo con las variables teóricas implícitas en el tema de investigación, donde se consultaron

autores y trabajos de investigación relacionados con la temática. Para una mejor comprensión, se estructuró la presentación del trabajo en capítulos.

Inicialmente, el capítulo I, muestra lo relacionado con la introducción, el marco conceptual y marco teórico. El capítulo II refiere el estado del arte. En el capítulo III se detallan los aspectos metodológicos relacionados con las técnicas e instrumentos de recolección de datos, para luego elaborar las conclusiones y recomendaciones.

Finalmente se presenta el listado de referencias que sirvió de soporte para darle firmeza y objetividad a la investigación.

MARCO CONCEPTUAL

2.1. Planteamiento del problema

Los adolescentes del siglo XXI se caracterizan por haber nacido y crecido con Internet, teléfonos celulares y videojuegos. Su aprendizaje ha sido muy diferente al de las generaciones anteriores, por lo que sus relaciones están medidas por las redes sociales, es así como la capacidad digital de los jóvenes, representa para algunas empresas como Microsoft, Google, Facebook, entre otras, un factor de éxito y crecimiento.

Redes sociales y adolescencia, representan hoy día un binomio interesante para su estudio y análisis, sobre todo desde el punto de vista periodístico, ya que el intercambio de audio y vídeo, el *texting*, los juegos virtuales y otras tecnologías emergentes, arrastra a la adolescencia a una nueva forma de entender la relación las relaciones sociales, de igual forma, las amistades y conexiones con otros se extienden del mismo modo que nuevos intereses aparecen o se solidifican posibilitados por el ciberespacio. Desde el ciberespacio, los adolescentes crean y se relacionan con sus pares, modifican la percepción de sus entornos sociales, y construyen nuevas identidades psicosociales y familiares.

Es imprescindible por ello, que las instituciones y profesionales que interactúan con jóvenes, familiarizarse con el impacto de estas tecnologías sobre la cultura digital del adolescente por lo que se hace imprescindible hablarles de ciberseguridad.

Se considera preciso entonces, establecer los riesgos y amenazas en el ciberespacio para los jóvenes en nuestra sociedad. En el ámbito internacional advierte (Villalba, 2015) sobre el incremento de incidentes de ciberseguridad en el año 2015 y expresa que:

> Pues no podemos negar la realidad por la que la sociedad ecuatoriana atraviesa en la actualidad, cada vez su seguridad se ve amenazada en el uso del sistema informático; tanto así que expertos advierten que en el año 2014 se incrementó el índice de delitos a través de los medios informáticos, y es posible que el número de víctimas sea mayor por el desarrollo económico que experimenta el país. (pág. 79)

Las redes sociales, constituyen uno de los servicios de comunicación interpersonal más utilizados por los internautas y su uso masivo pone de relevancia la importancia estratégica que están adquiriendo (Cerrada, Fojón, Gil, & Coz, 2010). El uso de las redes sociales contituye un problema social, la vulnerabilidad de información que genera, afecta a las personas mas inocentes como son los jóvenes. “Los menores de edad, son el segmento de la población que en mayor proporción hacen uso de Internet y sus servicios. Esto se debe en gran medida, a que crecen y se educan en la época del boom de internet” (Coz & Fojón, 2010, pág. 53). La mayoria de los jóvenes del siglo XXI cuenta con varias cuentas en el ciberespacio.

En varias investigaciones denotaron que el mal uso de las TIC facilita la omisión de delitos virtuales hacia los menores de edad. Uno de los factores primarios es el anonimato del ciberespacio, esto genera una sensación de seguridad para el agresor, incrementando las conductas delictivas que en el mundo real no tendrían correspondencia. (Merino, 2016)

Tanto en Colombia como en España, la mayoría de los jóvenes de 12 a 15 años utilizan las redes sociales por la necesidad de estar en la Red, la mayoría se sobreexpone, pero esta sobre-exposición va más allá de subir fotografías, en muchos casos los jóvenes utilizan su nombre real, mostrando sin ningún inconveniente sus datos personales como, filiación política, correo electrónico, incluso su número de teléfono (Almansa, 2013)

En tal sentido, las instituciones educativas han generado acciones con el proposito de contribuir con el uso consciente de los aparatos moviles, a traves de normativas que advienten a sus estudiantes sobre los peligros y amenazas en la red.

En el caso específico del Colegio Fiscal mixto Camilo Ponce, ubicado en el Barrio Santa Martha de la Ciudad de Manta, y según testimonios de docentes y personal directivo, existe una crecida preocupación por el uso de aplicaciones tecnológicas que han sido objeto de denuncia e intervención como por ejemplo: difusión de fotos con contenido privado, uso de mensajes anónimos para intimidar a algunos compañeros, alteración de información relacionada con el perfil en cuantas de Facebook, situación está que permitió a la autora del presente trabajo a realizar desde el punto de vista periodístico, una indagación sobre los riesgos y amenazas de los jóvenes de dicho centro educativo en relación a la ciberseguridad, con el fin de aportar posibles soluciones a la problemática planteada.

2.2. Pregunta científica

¿Conocen los jovenes del Colegio Fiscal Mixto Camilo Ponce los riesgos y amenazas a los que están expuestos en las redes sociales?

2.3. Objetivos de la Investigación

Objetivo General

Analizar la situación actual que tienen los jovenes del Colegio Fiscal mixto Camilo Ponce sobre los riesgos y amenazas a los que están expuestos en las redes sociales

Objetivos Específicos

- Describir el conocimiento que tienen los jóvenes del Colegio Fiscal mixto Camilo Ponce sobre ciberseguridad en las redes sociales.
- Identificar el uso que hacen los jóvenes del Colegio Fiscal mixto Camilo Ponce en las redes sociales.
- Analizar la relación entre la Ciberseguridad y el uso de las Redes Sociales en los jóvenes del Colegio Fiscal mixto Camilo Ponce.

2.4. Justificación

El complejo territorio de la adolescencia y el internet, requieren de un cuidadoso análisis, ya que según (Alfaro, 2010) los docentes de hoy, son adultos que viven entre adolescentes y mantienen una relación de enseñanza aprendizaje en un mundo de redes sociales, se encuentran así dos generaciones; los migrantes y los nativos tecnológicos.

En tal sentido, la importancia de la presente investigación está relacionada con el aporte que recibirán los sujetos de estudio para solventar su problemática, así como también contribuir el cumplimiento de los objetivos educacionales de la facultad, ahora bien desde el punto de vista comunicacional, representa un ejercicio bien interesante e innovador para darle a conocer a la población mantense lo relacionado con la ciberseguridad.

Las relaciones sociales, desarrollan en un marco regido por leyes, normas, reglas que estructuran una comunidad social, el problema surge en los espacios donde esas relaciones no son reguladas por ninguna entidad oficial, porque la velocidad de los cambios son significativamente superiores al de su marco de referencia racionalmente establecido (Hernández, 2014).

En una investigacion realizada por Almansa (2013), estudió 200 perfiles de Facebook y 40 entrevistas en profundidad a adolescentes de 12 a 15 años de Colombia y España, que analizaron durante un año para observar sus contenidos en la red social Facebook, y concluyó que el 95% de los jóvenes encuestados utilizan datos personales reales en las redes sociales, volviéndolos vulnerables y sobre-expuestos en el ciberespacio.

Por otro lado, dará un paso hacia un estudio más profundo sobre la vulnerabilidad de los jóvenes en el ciberespacio, y cómo las autoridades realizan proyectos para resolver estos problemas.

BASES TEÓRICAS

2.5. Estado del arte

En la concepción de su tesis doctoral Villalba (2015) gestada en la Universidad Nacional de Educación a distancia España, en su estudio titulado Ciberseguridad en España 2011-2015 una propuesta de modelo de organización, se inspiró en corrientes neo institucionalistas con el fin de aportar un valor a la ciencia política utilizando los estudios científicos.

El emprendimiento del proyecto de modelo de gestión se encontró impulsado por haber participado en el diseño de la primera estrategia de seguridad nacional en España y de realizar en la actualidad labores de asesoramiento al Presidente del Consejo Nacional de Ciberseguridad, desde la constitución de este Consejo a finales de febrero de 2014. (Villalba, 2015)

Para Villalba (2015), este trabajo de investigación se ha construido como un estudio de caso sobre la ciberseguridad en España, estimando su relevancia y su naturaleza en relación con la propuesta de un modelo de organización de la ciberseguridad en España, el cual pueda ser realizable y tenga un impacto positivo en el incremento de los niveles de la seguridad nacional (p.403).

La investigación presentó la evolución de los incidentes de ciberseguridad en España entre 2011 y 2015, encuadrándolos en un contexto general, ya que gran parte de las ciberamenazas son compartidas por otros Estados. En ciberataques se destacaron los “ataques patrocinados para el estado” (Fojón & Sanz, 2010, p. 3) que, en 2014, el CERT

Gubernamental Nacional (CCN-CERT) abordó 12.916 incidentes, de los cuales, 132 fueron catalogados como críticos, apreciándose la tendencia de incremento en número, virulencia y persistencia de los ciberataques en el futuro. (Villalba, 2015).

Esta investigación favorecería a al tema de titulación al ofrecer resultados del impacto e incidencia de los ciberataques hacia los adolescentes y jóvenes de nuestra sociedad, a su vez se encuentra notable los métodos de investigación de los cuales hizo uso el autor, posiblemente sea necesario utilizar los mismos recursos.

En el trabajo de investigación denominado Ciberdelitos y víctima menor de edad, su autor Merino (2016). “El objeto del presente trabajo es realizar un examen de las conductas delictivas cometidas a través de medios informáticos o tecnológicos cuando la víctima es menor de edad” (p.3).

“El hecho de interactuar desde casa proporciona cierto efecto de seguridad, ya que psicológicamente los comunicantes se sienten más protegidos pensando que lo que suceda en el mundo virtual no tendrá consecuencias en el mundo real” (Merino, 2016, p. 29).

Resulta útil como un gran punto a tratar en la investigación de mi tesis universitaria, concretando lo necesario que es este oficio conocer las nuevas tecnologías y prevenir futuros percances.

En la tesis para obtención de licenciatura en derecho “Delitos contra la Seguridad de los activos de los sistemas de información y comunicación: delitos a través de las Redes Sociales” la cual se efectuó en Facultad de Jurisprudencia, Ciencias Políticas y Sociales de la Universidad de Cuenca y su autora Zumba (2015) el presente trabajo básicamente está orientado a generar en la sociedad mayor conocimiento (p.2).

La precaución y concientización en la utilización y manejo de las múltiples herramientas informáticas y servicios que brinda Internet, siendo uno de estos servicios las muy conocidas redes sociales On-line, y en otros casos las mismas han sido transformadas en la herramienta idónea para generar algún daño a determinada persona, grupo de personas, o hasta toda una colectividad. (Zumba, 2015).

Como conclusión a estas tesis se reconoce la importancia de implementar a las redes sociales cuerpos normativos que regulen conductas de esta índole, no es suficiente para combatir la Cyberdelincuencia; en realidad se requiere de la colaboración de todos

los ciudadanos para este fin, creando una concientización acerca del uso de los distintos servicios que brinda la Red, generando una cultura informática. (Zumba, 2015, p. 78).

2.6. Marco teórico

Ciberseguridad y sus riesgos

La Ciberseguridad y la seguridad de la información son conceptos ahora cada vez más importantes. (Comninos, 2013). “Se circunscribe a la esfera de los expertos y no se ha avanzado lo suficiente en el desarrollo de una cultura colectiva en este campo.” (Villasuso, 2010, p. 13)

Las TIC en estos últimos años han generado una conducta delictiva, debido a su fácil anonimato, se trata de nuevas formas penales que han exigido una normativa penal concreta, en la práctica se observa que el uso incorrecto de las TIC facilita la comisión de delitos virtuales hacia los menores de edad. (Merino, 2016)

La UIT (Unión Internacional de Telecomunicaciones) define en su recomendación UIT–T X.1205 Unión Internacional de Telecomunicaciones (2008) a la Ciberseguridad como:

> El conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno.(on line)

Las propiedades de seguridad incluyen una o más de las siguientes:

- Disponibilidad;
- Integridad, que puede incluir la autenticidad y el no repudio;

• Confidencialidad”

2.6.1.1. Definición y Conflictos

La Ciberseguridad se refiere a la capacidad de poder controlar el acceso al nuevo sistema de comunicación o de información como las redes sociales. Sin embargo, donde los controles de Ciberseguridad se encuentran ausentes, el ciberespacio es considerado como tierra de nadie, debido a que no existen normas ni reglamentos que penalicen los ciberdelitos en el ciberespacio. (Leiva, 2015).“El uso de la tecnología ofrece al conjunto de la sociedad que éstos se comuniquen sin límites” (Merino, 2016, p. 5).

> Detectar y prevenir responde actualmente a los objetivos de la Ciberseguridad, pero tradicionalmente el objetivo principal fue prevenir que se concrete un ataque exitoso sin embargo los profesionales de seguridad son conscientes de que simplemente no es posible evitar todos los ataques y que debe existir una planificación y preparación que incluya métodos para detectar ataques en progreso, preferentemente antes de que causen daño. En general se podría decir que la Ciberseguridad se refiere a métodos de uso, procesos y tecnologías para prevenir, detectar y recuperarse de daños a la confidencialidad, integridad y disponibilidad de la información en el ciberespacio. (Leiva, 2015, p. 2)

2.6.1.2. Seguridad de la información

(Rubio 2015) determina que “el robo de información confidencial no sólo afecta a las grandes corporaciones, por motivos obvios, sino que también puede incidir de forma gravosa en la vida de un ciudadano medio” (p. 2-3). Esto determina que los jóvenes no son las únicas personas que sobreexponen su información personal.

(Alfaro 2010) dijo que las redes sociales de hoy, tienen un increíble auge, además de ser espacios en los que las personas exponen con frecuencia sus datos personales, a causa de esto, representan un reto en el tema de privacidad en la red. Estos requieren crear mecanismos para denunciar y procesar legalmente casos de tratantes y/o explotadores sexuales que detectemos en las redes, timadores, impostores de identidad.

"Usualmente se acepta que el objetivo de la ciberseguridad o seguridad informática es descubrir y aclarar la naturaleza de las amenazas y proveer metodologías para mitigarlas" (Barrantes, 2010, pág. 42). De acuerdo con (Sánchez, A 2010) un ámbito abierto al riesgo no se trata sólo de ser objeto de observaciones no deseadas de nuestro intercambio epistolar o de nuestros contactos, apetencias y pecados, sino también por la posibilidad de ser víctimas de nuevas formas de delito y de violencia.

Según (Fojón & Sanz 2010), clasifican las amenazas del ciberespacio, de ciberataques en función de su autoría e impacto como:

> Ataques de perfil bajo. Este tipo de ataques son ejecutados, normalmente, por personas con conocimientos TIC que les permiten llevar a cabo ciber-ataques de naturaleza muy heterogénea y por motivación, fundamentalmente, personal (p.3).

2.6.1.3. Ciberseguridad en las redes Sociales

(Sánchez A. 2010) puntualiza que, "los jóvenes de hoy en día construyen su mundo con estos contactos virtuales, con esta vivencia en red donde solo lo tecnológicamente compartido, sea por conexión vía chat o por correo electrónico o por mensajes SMS, realmente existe" (p. 28), puntualizando esto los jóvenes cada vez más se sumergen a una realidad desconocida, donde nadie está libre de ser observado por desconocidos que vulnerar du identidad personal

Para (Zumba 2015) la humanidad ha constituido a la comunicación como un elemento esencial para su desarrollo; por eso las Redes Sociales, como medio de comunicación representa el desarrollo de múltiples actividades, ya sean académicas, comerciales, económicas, entre otras.

Dentro de las redes sociales creamos un perfil y publicamos una imagen que nos represente, ésta puede ser una fotografía u otro tipo de imagen que no necesariamente concuerda con nuestro aspecto físico, situación sobre la cual no existe ningún control que confirme la veracidad de estas identidades. Cuando una joven sube una fotografía suya en ropa interior, el mismo día, en la misma hora después de la subida, puede ser distribuida por diferentes partes del mundo, son que pueda volver a recuperar todas las

copias que se han hecho a su fotografías. Hay entonces una violentarían a los derechos de integridad de las personas, pero nadie nos advierte, no existen alertas para advertir a los adolescentes de que corren éstos peligros (Alfaro, 2010, p. 79-80).

La persona más indefensa a través de las TIC son los menores, los cuales, junto a su preexistente inocencia reciben su primer móvil alrededor de los 7 años de edad. De hecho, teniendo en cuenta los datos facilitados por el Sistema Estadístico de Criminalidad, en cuanto a los ciberdelitos cometidos a personas adultas, vemos que solo un 1,8% responden a delitos sexuales, un 4,6% a delitos contra el honor y un 21,4% a amenazas y coacciones. Sin embargo, si tenemos en cuenta los mismos delitos cometidos a menores de 18 años la cifra asciende a un 33%, un 10% y por último al 33% respectivamente. Por último, vemos que el 76,3% de 4 las cifras registradas por ciberdelitos sexuales afectan a menores, registrándose un total de 647 víctimas (Ministerio del Interior, 2012)

2.7. Menores y Redes sociales

La adolescencia es una etapa donde el ser humano expimerimenta grandes cambios fisico y psiquicos, de hecho, mucho ha evolucionado el término a lo largo de la historia, ahora incluso se habla de pre-adolescencia, adolescencia y pos-adolescencia. (Agreda, Hinojo, & Aznar, 2016).

La especial afinidad que ha surgido entre los menores y las nuevas tecnologías y el origen del término “Nativos Digitales”, proviene de la reflexión del ecléctico determina (Prensky 2001) en su artículo, “Digital Natives, Digital Immigrants”.

En su determinante artículo de forma concisa define a los nativos digitales como la primera generación que ha crecido con las tecnologías digitales y que son "nativos" del lenguaje de los ordenadores, estos jóvenes nacidos a partir de 1990,que son expertos con las computadoras, tienen destrezas y formas para comunicarse con los otros que los mayores no pueden entender. (Ibidenm)

2.7.1.1. Redes Sociales

El acoso sexual a través de las redes sociales es un problema actual que afecta principalmente a los jóvenes adolescentes. Su desconocimiento, la falta de información y la inocencia de estos en la mayoría de los casos, les confiere el rol de posibles víctimas en este ciberespacio anónimo, enmascarado e incontrolado (Luminita, 2015)

En otros de los informes de la Fundación Pfizer (2009) sobre "La juventud y las Redes Sociales en Internet", de septiembre de 2009, señala que un 92% de los jóvenes españoles entre 11 y 20 años son usuarios de redes sociales.

Según un estudio descriptivo que ha sido llevado a cabo en Valladolid y que participó una muestra de 2.1412 escolares, con edades comprendidas entre 13 y 18 años, reveló que el 18,9% de los encuestados había contactado con desconocidos, y el 18,7% había llegado a tener contacto con un extraño con el que se habían citado previamente a través de las redes sociales. El 19,6% reconocía haber grabado o difundido imágenes de otros sin su consentimiento y otro 4,1% había subido a la red fotografías o vídeos de personas de su entorno en posturas provocativas, siendo un 22,8% de los encuestados los receptores de dichas imágenes. El 12,3% de la muestra afirmaba haber recibido llamadas o mensajes de compañeros con insultos o amenazas a través del móvil o del ordenador. Un 14,2% se confesaba autor. En cuanto a compras por Internet, el 15,3% refería haberse gastado grandes cantidades en aplicaciones de juegos o música y finalmente, en el uso general de las TIC, el 96,6% utilizaba el teléfono móvil y el 82,5% se conectaba a diario a Internet (Fierro, Vázquez, & Alfaro, 2013, pp 117-8).

2.7.1.2. Tipos de acoso

Según la página web Pantallas amigas (2015), podemos ver existen varios métodos de acoso escolar que implica la participación de un adulto contra un menor de edad a través de las redes sociales.

2.7.1.3. Ciberacoso escolar

Estas agresiones se definen como una situación donde el sujeto recibe provocaciones de forma reiterada a través de soportes electrónicos y su finalidad es afectar la autoestima y dañar su estatus social.

Un estudio del Gobierno del Principado de Austrias determinó que dos de cada 100 estudiantes de secundaria sufren de acoso escolar grave:

> El consejero de Educación ha presentado hoy los resultados del estudio, que muestra también que el 3,25% del alumnado de esta etapa padece ciberacoso severo. El proyecto, en el que han participado 115 centros y 25. 882 alumnos, persigue reforzar las actuaciones que contribuyen a mejorar la convivencia en los entornos educativos (Alonso, 2017).

Estos estudios concuerdan en la utilización de internet a través de dispositivos móviles, ordenadores entre otros dispositivos electrónicos, estos indicaron que no existía un debido control en cuanto al tiempo de uso y los contenidos a los que accede el alumnado.

También muestra la preferencia por las interacciones sociales en línea en el 2% de la población escolar y la utilización de la red como mecanismo de regulación del ánimo en más de un 10%.

2.7.1.4. Ciberbullying

Este tipo de acoso está ejercido única y exclusivamente por menores. En estos casos no existe la implicación de una persona adulta sino que se produce solo entre menores.

El reciente estudio “Cyberbullying among Young People” (“Ciberbullying entre personas jóvenes”) ofrece una visión general sobre el alcance y las diversas formas de ciberbullying en los Estados miembros de la Unión Europea teniendo en cuenta la edad y el sexo de víctimas y agresores, así como el medio utilizado para realizar el acoso, ilustrando medidas legales y políticas adoptadas ya que aún en la actualidad todavía no se concreta la definición de ciberbullying en el ámbito internacional o Unión Europea (Dalla et all 2016).

Según datos del informe Net Children Go Mobile de Livingstone et al (2014), el 12% de niños y niñas de edades comprendidas entre 9 y 16 fue víctima de ciberbullying; en 2011 esa cifra apenas alcanzaba el 6%.

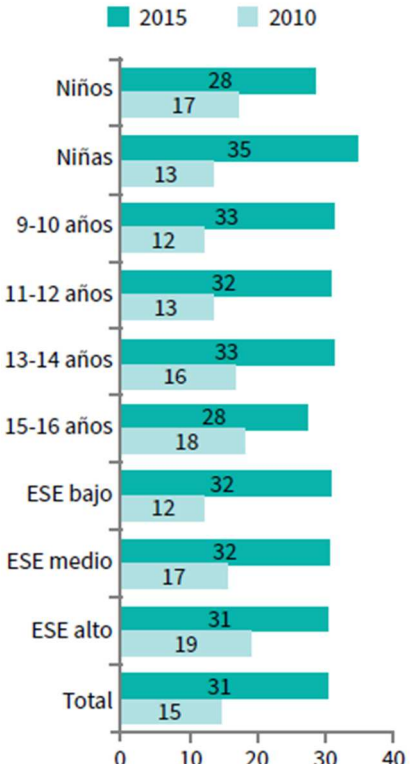

GRÁFICO 1. Informe del Net Go Children Riesgos y oportunidades en internet y uso de dispositivos móviles entre menores", elaborado a partir de encuestas a 500 menores de España y sus progenitores, afirma que el 12% de niños y niñas de 9 a 16 años ha sido víctima de ciberbullying

Además del ciberbullyng, también se ha preguntado a menores de edad por otros riesgos derivados del uso de internet o del teléfono móvil como imágenes de contenido sexual (un 52 % reconoció su visión); encuentros con desconocidos contactados en la red (11 %), o el envío de mensajes sexuales o sexting (31%). El ciberbullying sigue siendo el fenómeno que más daño cree que causa (24%). (Garmendia et al 2016).

2.7.1.5. Grooming

Según el Instituto Nacional de Tecnologías de la Comunicación (INTECO)"se define el Grooming (Engaño Pederasta) como: "El acoso ejercido por un adulto y se refiere a las acciones realizadas deliberadamente para establecer una relación y un

control emocional sobre un niño o una niña con el fin de abusar sexualmente del menor".

En una encuesta realizada por ESET Latinoamérica, se encontró que los niños de entre 11 y 15 años son los más vulnerables de sufrir grooming. En México, de abril de 2013 a febrero de 2014, se detectaron 57 casos de hostigamiento y acoso a menores.

"Para el 68,3% de los adultos encuestados por ESET Latinoamérica, el grooming es una amenaza muy frecuente. En esta línea, el 26,3% confirmó conocer un niño que ha sido víctima de grooming. De estos menores, un 52,9% tiene entre 11 y 15 años, y un 33,7% entre 7 y 10" (Escobar, 2015 prr 6).

2.7.1.6. Sexting

El Sexting se trata del envío de contenidos pornográficos o eróticos a través de dispositivos móviles como teléfonos, tablets, PC's o cualquier otro dispositivo con acceso a internet.

Según un análisis del Departamento de Educación de Gran Bretaña tres mil niños y niñas de las escuelas de dicho país pasaron por un período de suspensión durante el período lectivo 2010-2011 por comportamiento sexual impropio. "Los principales motivos de las expulsiones abarcan desde bullying, acoso y ataques sexuales hasta un comportamiento obsceno" (TheChristianPost, 2013).

Si bien el Sexting es un anglicismo que se refiere al envío de mensajes sexuales, por medio de teléfonos móviles, o dispositivos móviles, este conlleva diversos riegos, en primer lugar una vez que la foto fue enviada a la red, es muy difícil que desaparezca del internet.

Otros de los riesgos de carácter psicológico, legal e incluso de la integridad física de los participantes. Muchos de sus practicantes son menores de edad y no son conscientes de ellos: es el deber de padres, madres y educadores advertirlos. (Pantallasamigas, 2015)

En Brasil los principales riesgos asociados al sexting son la extorsión (59%), ciberbullying (45%), daños al honor, intimidad e imagen (42%) y pornografía infantil (36%). La alarmante sensación es aún más elevada en los trece países de

América Latina, donde hay una mayor percepción de los peligros: un 10% y un 20% más de la población considera la extorsión y los daños al honor, intimidad e imagen riesgos del sexting, el 65% considera que está relacionado con la pornografía infantil, el 57% con el acoso en internet y el 34% con el ciberbullying (eCGlobal, Solutions, eCMetrics, & CLIPS, 2012).

2.7.1.7. Conducta Típica

Se ha visto que los acosadores disponen de una estudiada metodología de trabajo, actuando con cautela, precisión, paciencia y determinación. Aunque no todos los acosadores cibernéticos trabajan de la misma manera, tienen en común el desarrollo de un largo proceso que se puede definir en varias fases, que van desde el establecimiento de la amistad, el estrechamiento de la relación, la valoración de los riesgos que puede conllevar cometer este delito hasta la fase final de ataque y el consecuente acoso (Luminita, 2015).

Debido al anonimato que permite las redes sociales, el acosador no tiene la necesidad de desenmascararse desde el principio y encontrarse cara a cara con la víctima, teniendo así las ventajas de poder estrechar lazos amistosos y emocionales, sin preocupación de ser afectado legalmente.

Esta amistad puede desencadenar en una dependencia afectiva, aislándole del mundo real que le rodea y haciendo que su “ciber-relación”, haciendo que el menor olvide totalmente que en el fondo no conoce a la persona que está al otro lado de la pantalla quedando desprotegido eliminando toda posibilidad de permanecer en alerta ante un posible engaño. (O’Connell, 2013)

Redes Sociales y Padres

El conocimiento de la existencia de los peligros que nos rodean es una herramienta fundamental para la protección de nuestra vida cotidiana, es fundamental que un menor reconozca estos peligros que pueden conllevar el mal uso de Internet y las redes sociales,

atendiendo a otra serie de señales que nos puede advertir ante diferentes eventualidades. (DepartamentodeSalud, 2016)

Enseñar a utilizar las redes sociales de forma segura, no introduciendo datos personales que pudieran dar lugar a una localización geográfica del menor, o sus hábitos cotidianos, educando al menor para que tenga la capacidad de decisión a la hora de aceptar en su círculo de amistades a personas desconocidas en su entorno, evitando aceptar invitaciones extrañas a juegos, mensajerías, redes privadas (Que no te la den, 2011)

Es muy importante que el menor comprenda y fomente el sentido de la privacidad y sepa establecer el uso correcto de los dispositivos que ofrezcan la captura o retransmisión de imágenes, fotografías o vídeo como las WebCam, deben estar debidamente controlados mediante contraseña que solo los padres deben conocer para su uso. (Luminita, 2015)

La comunicación con los hijos es fundamental para conocer sus hábitos de vida, permitiéndole averiguar cuando navega, en que redes está conectado, que páginas visita, o con quien se comunica y sobre qué.

Recordar con frecuencia que no debe revelar sus datos a personas desconocidas es importante, ya que le refuerza sus conductas de seguridad. Periódicamente puede preguntarle que nuevos amigos va conociendo, a quienes ha agregado a sus contactos y cómo los ha conocido o a través de quien. y los criterios de configuración sobre las herramientas que utilice en Internet para salvaguardar esta privacidad de aquellos que no deben conocer su información personal. (DepartamentodeSalud, 2016)

2.8. MARCO METODOLÓGICO

2.9. Tipo De Investigación

Cuando se inicia el capítulo de la metodología lo primero que se encuentra el investigador es la definición del tipo de investigación que se desea realizar del tipo de investigación que terminará los pasos a seguir del estudio, sus técnicas y métodos que pueden emplear en el proceso de investigación.

El tipo de investigación utilizado fue de campo, según (Palella & Martins, 2010),

> La investigación de campo consiste en la recolección de datos directamente de la realidad donde ocurren los hechos, sin manipular o controlar las variables. Estudia los fenómenos sociales en su ambiente natural, el investigador no manipula variables debido a que esto hace perder el ambiente de naturalidad en el cual se manifiesta (pag.88).

2.10. Nivel de Investigación

Según, (Hernández, Fernandez, & Pilar, 2015) los niveles de la investigación científica:

En tal sentido, el nivel utilizado fue de tipo descriptivo ya que se pretendió conocer los componentes principales de la realidad en estudio.

2.11. Enfoque de la investigación

Según, (Hernández, Fernandez, & Pilar, 2015), el enfoque de la investigación:

> Es un proceso sistemático, disciplinado y controlado y está directamente relacionada a los métodos de investigación que son dos: método inductivo generalmente asociado con la investigación cualitativa que consiste en ir de los casos particulares a la generalización; mientras que el método deductivo, es asociado habitualmente con la investigación cuantitativa cuya característica es ir de lo general a lo particular.

Debido a la naturaleza de los datos se entiende que el enfoque empleado en esta investigación fue la de tipo cuantitativa.

2.12. Métodos de la investigación

Los métodos utilizados en el presente trabajo de investigación se pueden enunciar de la siguiente manera:

2.13. Técnica e instrumento de datos

(Hernández, Fernandez, & Pilar, 2015) mencionan que las técnicas de recolección de datos son de gran diversidad y herramientas que pueden ser utilizadas por el analista para desarrollar los sistemas de información, los cuales pueden ser la entrevistas, la encuesta, el cuestionario, la observación, el diagrama de flujo y el diccionario de datos (en línea).

La técnica de recolección utilizada en la presente investigación fue la encuesta, la cual se realizó en forma directa los estudiantes del colegio

2.14. Instrumento de recolección de datos

(Hernández, Fernandez, & Pilar, 2015) sostienen que los instrumentos son procedimientos o actividades realizadas con el propósito de recabar la información necesaria para el logro de los objetivos de una investigación, se refiere al cómo recoger los datos. Para recorrer los datos se utilizó como instrumento un cuestionario de preguntas cerradas. (ver anexo)

2.15. Técnica de análisis de datos

(Palella & Martins, 2010) dicen que el análisis de los datos es la técnica que:

> Consiste en el estudio de los hechos y el uso de sus expresiones en cifras para lograr información válida y confiable. La técnica utilizada para el análisis de los datos en esta investigación fue la estadística descriptiva ya que se utilizó cuadros estadísticos, tortas y tabla de frecuencias para interpretar los datos (en línea).

La técnica utilizada fue la estadística descriptiva porque se utilizó cuadros, gráficos y figuras.

2.16. Universo, Población y Muestra

(Hernández, Fernandez, & Pilar, 2015) dicen que la población ‟es el conjunto total de individuos, objetos o medidas que poseen algunas características comunes observables en un lugar y en un momento determinado” (en línea). El universo en esta investigación fueron 380 de edades comprendidas entre 12 a 18 años. La población los estudiantes de decimo curso que suman en total 83, por ser una población pequeña, la muestra fue de tipo poblacional, es decir la misma cantidad de la población a lo que no aplica ninguna fórmula estadística para su cálculo (NO SE APLICAN FÓRMULA ES POBLACIONAL)

RESULTADOS

Una vez procesado el cuestionario, se obtuvo la siguiente información:

1.- ¿Cuándo te suscribes a una página de internet, te tomas el tiempo para revisar las políticas de afiliación?

Tabla 1 Revisión de políticas

RESPUESTA	FRECUENCIA	PORCENTAJE
Siempre	23	27,7
Algunas Veces	31	37,3
Rara Vez	19	22,9
Nunca	10	12,0
Total	83	100,0

Nota:- La revisión de las políticas de afiliación en internet por parte de los usuarios, presenta cierto desinterés al momento de su aceptación

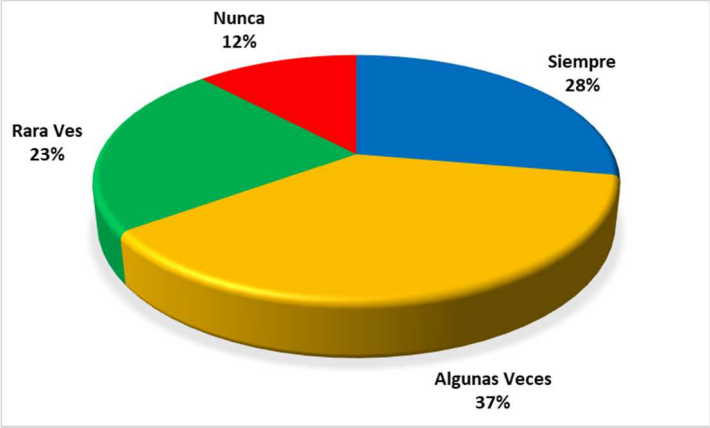

Figura 1.- Revisión de las políticas

Fuente: Elaborado por la Investigadora

De acuerdo con la gráfica, el 28% de los jóvenes cuando se suscribe a una página de internet, siempre se toma tiempo para revisar las políticas de afiliación, un 37% dijo que algunas veces, otro 23% sostuvo que rara vez, el otro 12% nunca revisa las políticas. Como se puede apreciar, los jóvenes del colegio Camilo Ponce, ocasionalmente revisan las políticas de seguridad al momento de suscribirse a una página, esta situación de acuerdo con (Alfaro, 2010) se debe entre otras cosas a la inmediatez de la juventud al momento de hacer uso de las páginas y su impulsividad a lo novedoso.

2.- ¿Recibes invitaciones de amistad de personas que no conoces?

Tabla 2 Invitación de personas desconocidas

RESPUESTA	FRECUENCIA	PORCENTAJE
Siempre	24	28,9
Algunas Veces	29	34,9
Rara Vez	19	22,9
Nunca	11	13,3
Total	83	100,0

Nota: La aceptación de invitaciones por parte de personas desconocidas tiene una significativa respuesta positiva por los usuarios

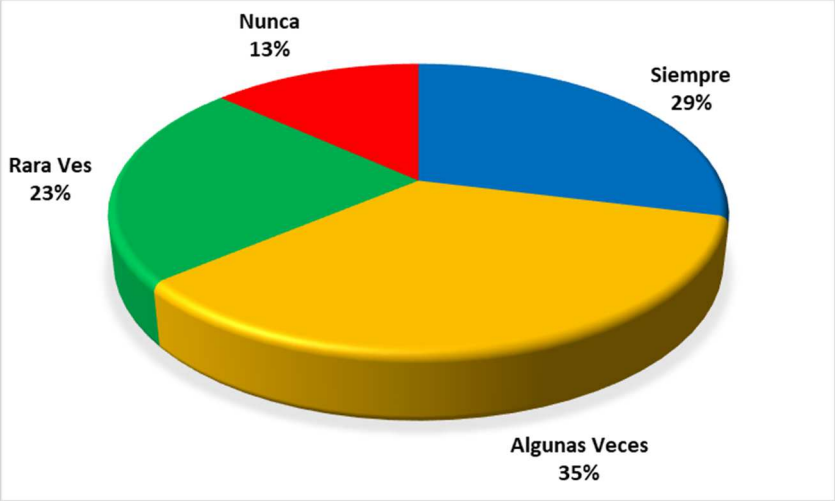

Figura 2.- Invitación de personas desconocidas

Fuente: Elaborado por la Investigadora

Según los resultados, el 29% de los encuestados, dice que siempre recibe invitaciones de amistad de personas que no conocen, otro 35% manifestó que algunas veces, un 23% dijo que rara vez y un 13% sostuvo que nunca ha recibido invitaciones de personas extrañas. Con estos datos e puede inferir que los estudiantes están expuestos a posibles situaciones de inseguridad en la redes como cyberacoso, Grooming, entre otras.

3.- ¿Has recibido ofertas de compras o viajes a tu correo sin tu solicitarla?

Tabla 3 Recepción de ofertas sin solicitud

RESPUESTA	FRECUENCIA	PORCENTAJE
Siempre	35	42,2
Algunas Veces	23	27,7
Rara Vez	15	18,1
Nunca	10	12,0
Total	83	100,0

Nota: La recepción de ofertas por internet sin solicitud de los usuarios representa una alta aceptación por parte de los mismos.

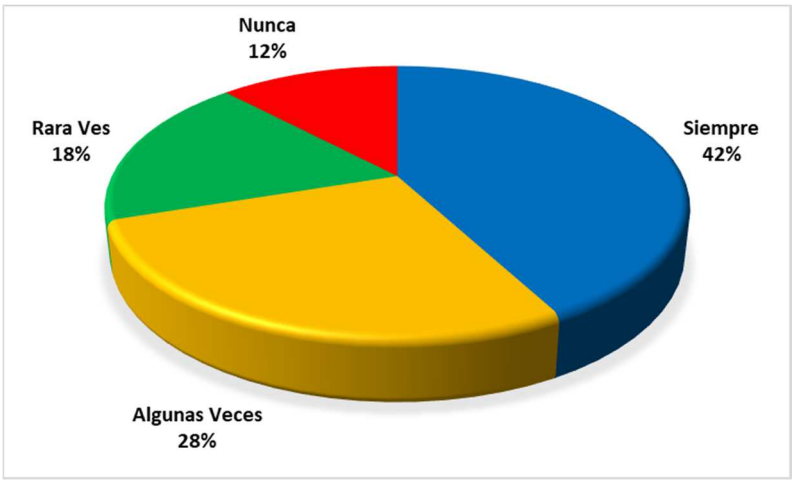

Figura 3.-Recepción de ofertas sin solicitud

Fuente: Elaborado por la Investigadora

De acuerdo con los resultados, un significativo 42% de los estudiantes dice que siempre recibe en sus correos ofertas de compras o viajes sin haberla solicitado, otro 28% dijo que algunas veces, un 18% sostuvo que rara vez y un 12% que nunca ha recibido este tipo de ofertas. Esta situación ha mejorado recientemente a raíz de la interpelación del propietario de Facebook, quienes han creado políticas de protección de datos.

4.- ¿Publicas información muy personal en las redes sociales?

Tabla 4.- Publicación de información muy personal

RESPUESTA	FRECUENCIA	PORCENTAJE
Siempre	21	25,3
Algunas Veces	27	32,5
Rara Vez	23	27,7
Nunca	12	14,5
Total	83	100,0

Nota: Los usuarios tienen una alta tendencia en publicar información muy personal en las redes sociales

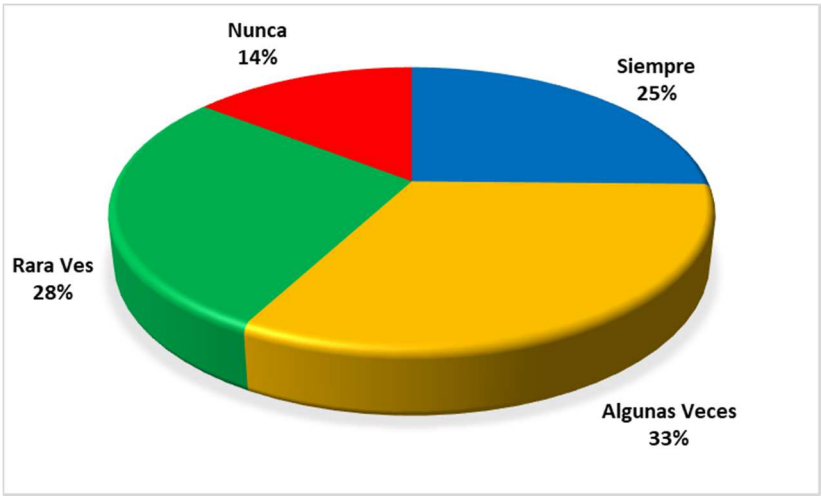

Figura 4.-Publicación de información muy personal

Fuente: Elaborado por la Investigadora

Como se puede observar, el 25% de los estudiantes encuestados, dijo que siempre publica información muy personal en las redes sociales, otro 32% manifestó que algunas veces lo hace, un 28 rara vez y solo el 14% nunca publica información muy personal en las redes sociales. Estos datos son interesantes para la investigación, ya que la ciberseguridad parte de la premisa de resguardar información personal, mediante el consentimiento por parte de los usuarios y el uso de la configuración de privacidad.

5.- ¿Consideras que las redes sociales son seguras?

Tabla 5.- Seguridad de las redes sociales

RESPUESTA	FRECUENCIA	PORCENTAJE
Siempre	12	14,5
Algunas Veces	19	22,9
Rara Vez	27	32,5
Nunca	25	30,1
Total	83	100,0

Nota. - Existe una tendencia entre los usuarios en no considerar la seguridad de las redes sociales

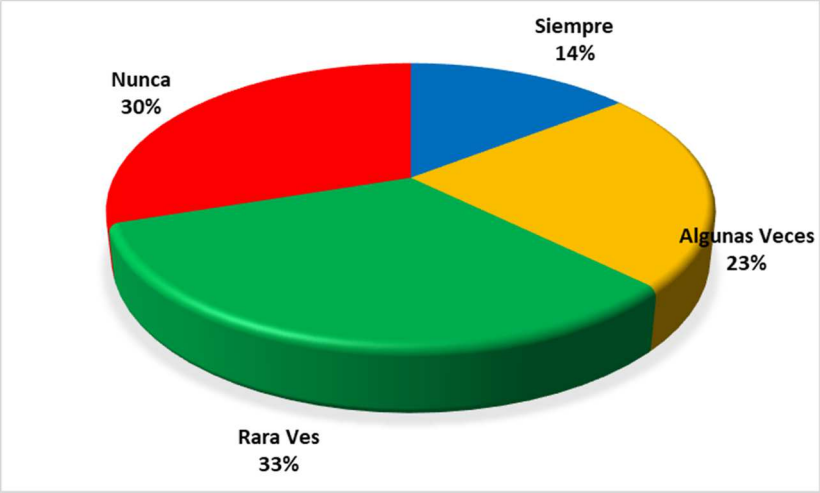

Figura 5.- Seguridad de las redes sociales

Fuente: Elaborado por la Investigadora

De acuerdo con el gráfico, el 14% de los encuestados dijo que siempre considera las redes sociales segura, un 23% algunas veces, otro 33% rara vez y un 30% nunca las considera segura. Según (Giant, 2016) sostiene al respecto que la seguridad en la redes sociales es un aspecto que los países están teniendo presente para evitar tanto el robo de identidad y garantizar la seguridad nacional.

6.- ¿Comparte tu contraseña de las redes con amigos?

Tabla 6.- Contraseña compartida

RESPUESTA	FRECUENCIA	PORCENTAJE
Siempre	9	10,8
Algunas Veces	13	15,7
Rara Vez	9	10,8
Nunca	52	62,7
Total	83	100,0

Nota: .- Compartir la contraseña de las redes sociales con amigos no representa una tendencia entre los usuarios

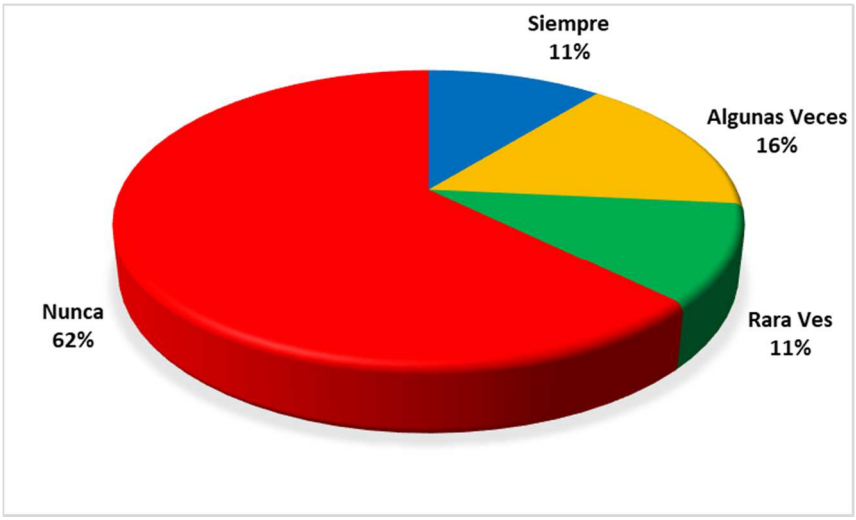

Figura 6.- Contraseña compartida

Fuente: Elaborado por la Investigadora

Los estudiantes encuestados, manifestaron en un 11% que siempre comparten su contraseña de redes con amigos, otro 16% algunas veces, un 11% rara vez y un significativo 62% nunca ha compartido su contraseña con amigos. En todas las recomendaciones que se hacen desde la ciberseguridad lo primero que advierten es no compartir la contraseña, cuestión que los jóvenes encuestados han tomado muy en serio, para o cual hacen cambio periódico de sus contraseñas.

7.- ¿Te aseguras de cambiar tu contraseña?

Tabla 7.- Cambio de contraseñas

RESPUESTA	FRECUENCIA	PORCENTAJE
Siempre	39	47,0
Algunas Veces	21	25,3
Rara Vez	14	16,9
Nunca	9	10,8
Total	83	100,0

Nota: El cambio de contraseñas representa un significativo porcentaje de uso y aceptación entre los jóvenes

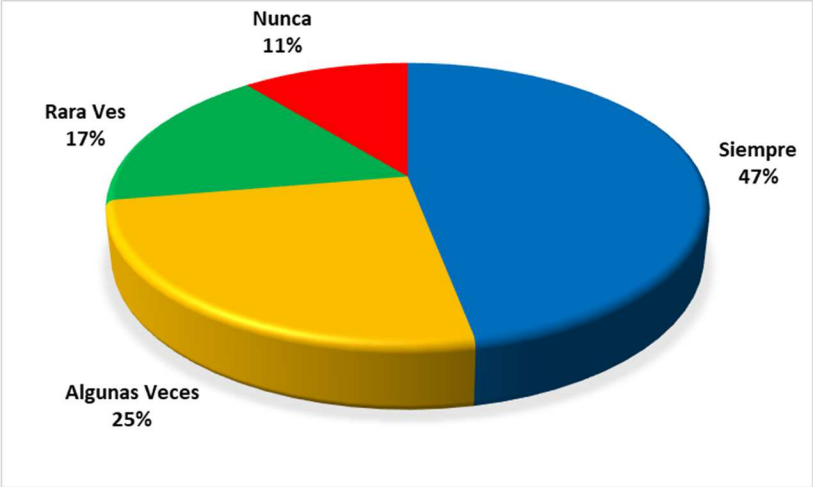

Figura 7.-Cambio de contraseñas

Fuente: Elaborado por la Investigadora

De acuerdo con los resultados, un significativo 47% de los estudiantes encuestados, dice siempre asegurarse de cambiar su contraseña, otro 25% algunas veces, un 17% rara vez y un11% nunca cambia su contraseña. Al cambio periódico que contraseñas es uno de los ejercicios que deben hacer los jóvenes en su redes sociales, como una política efectiva de seguridad.

8.- ¿Tus padres controlan el uso que le das a las redes sociales?

Tabla 8.- Control de uso de redes

RESPUESTA	FRECUENCIA	PORCENTAJE
Siempre	27	32,5
Algunas Veces	39	47,0
Rara Vez	9	10,8
Nunca	8	9,6
Total	83	100,0

Nota: El control de uso de las redes por parte de los padres tiene una alta aceptación en la población encuestada

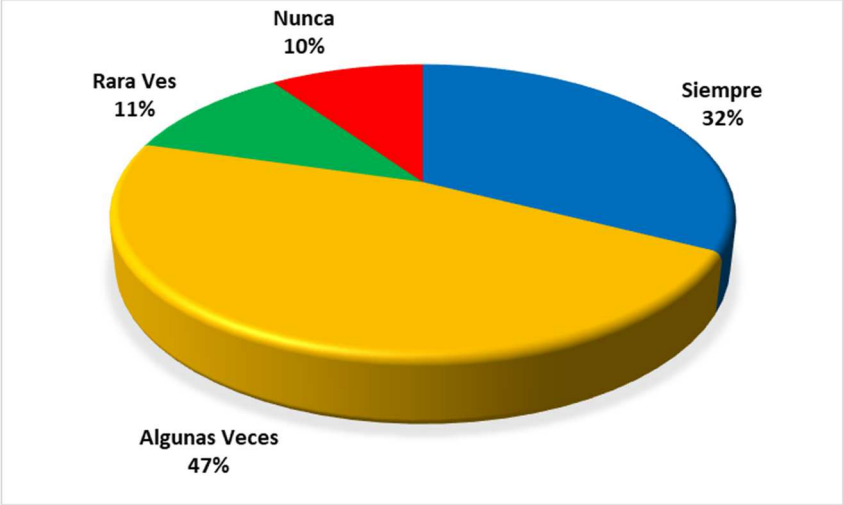

Figura 8.-Control de uso de redes

Fuente: Elaborado por la Investigadora

Según los resultados, el 32% de los estudiantes dice que su padres siempre controlan el uso que le dan a las redes sociales, otro 47% algunas veces, un 11% rara vez y el otro 10% nunca son controlados por sus padres. El problema de Ciberseguridad en los jóvenes también es y debe ser un asunto familiar, en donde los padres tienen las opciones de parental control y reseteo de usuarios y clave.

9.-¿Tus redes sociales te ofrecen políticas de seguridad?

Tabla 9.- Ofrecimiento de políticas de seguridad

RESPUESTA	FRECUENCIA	PORCENTAJE
Siempre	37	44,6
Algunas Veces	23	27,7
Rara Vez	7	8,4
Nunca	16	19,3
Total	83	100,0

Nota: El ofrecimiento de políticas de seguridad por parte de las redes sociales según los encuestados

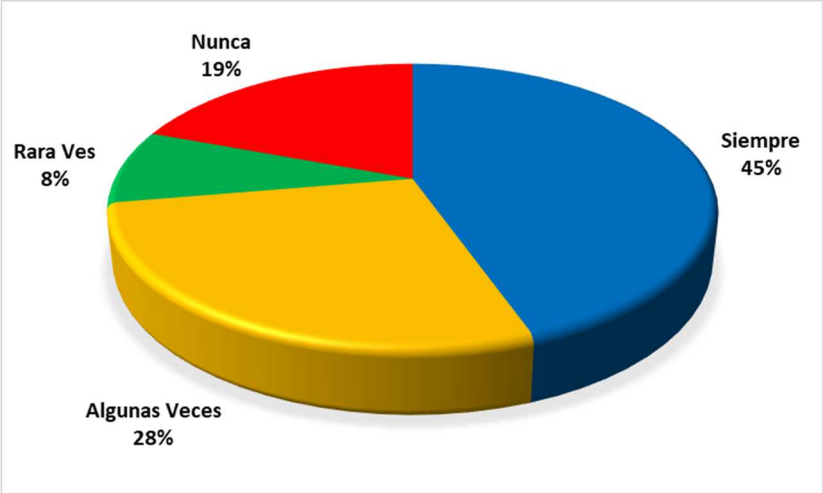

Figura 9.-Ofrecimiento de políticas de seguridad

Fuente: Elaborado por la Investigadora

Los jóvenes encuestados, en un 45% dicen que sus redes sociales les ofrecen políticas de seguridad, un28% dijo que algunas veces, otro 8% rara vez y un 19% nunca.

Las redes sociales actualmente están ofreciendo políticas de seguridad a sus clientes, sobre todo con los últimos acontecimiento surgidos en las grandes empresas como google y Facebook.

10.- ¿Cuáles de las siguientes redes sociales estas suscrito actualmente?

Tabla 10.- Tendencia de suscripción en redes sociales

ALTERNATIVAS	RESPUESTAS	PORCENTAJE
Facebook	83	100%
WhatsApp	83	100%
Instagram	79	80,2
Twitter	23	24,2
YouTube	67	68,2
Skype	42	43,2
Pinterest	19	20,2
Messenger	76	77,2
WeChat	34	35,2
QQ	23	24,2
Google+	79	80,2
Haboo	0	0,0

Nota: La tendencia de suscripción en las redes sociales destaca Facebook, WhatsApp, Instagram como las más solicitadas

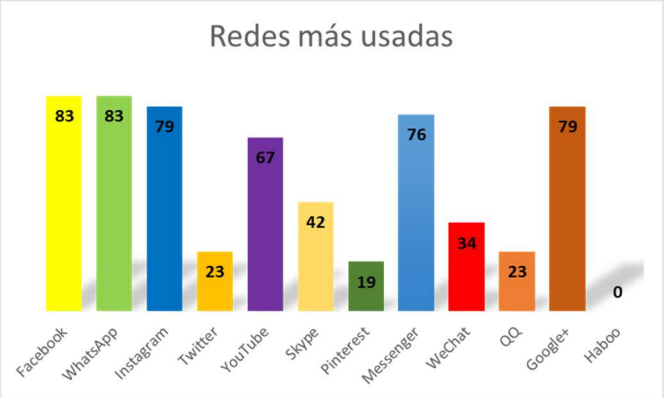

Figura 10.-Tendencia de suscripción en redes sociales

Fuente: Elaborado por la Investigadora

Entre las redes sociales más utilizadas por los jóvenes estudiantes figuran Facebook, WhatsApp, Instagram, Messenger y google+, ninguna usa haboo muy pocos unas WeChat y Twitter. Las redes sociales más comunes causalmente son las que han estado señaladas por violación a las políticas de seguridad e sus clientes.

11.- ¿Por lo general usas tus redes sociales para?

Tabla 11.- Uso de la redes sociales

ALTERNATIVAS	RESPUESTAS	PORCENTAJE
Buscar Amigos	43	51,8
Publicar Fotos	76	91,6
Buscar Información	81	97,6
Subir Videos	35	42,2
Planificar Salidas	16	19,3
Leer Contenidos	77	92,8
Mensajes y Chat	80	96,4
Actualizar Estado	23	27,7
Compartir Contenido	76	91,6
Saber de mis Amigos	57	68,7
Diversión	82	98,8
Conocer Personas	39	47,0

Nota: El uso de las redes sociales destaca publicar fotos, buscar información, leer contenidos, diversión entre otras

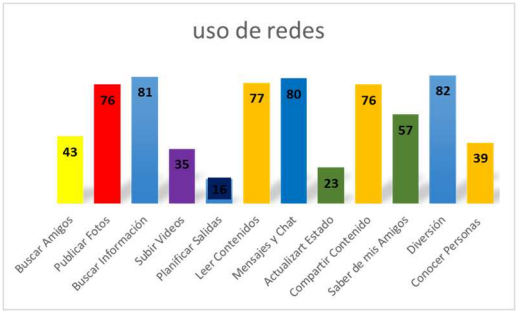

Figura 11.-Uso de las redes sociales

Fuente: Elaborado por la Investigadora

De acuerdo con los encuestados, el mayor uso que los jóvenes le dan a las rede sociales son: Mensaje y chat, buscar información, diversión, publicar fotos compartir contenidos, muy pocos actualizan su estado, algunos buscan amigos y otros para planificar salidas.

2.17. Discusión de los resultados

No todos los jóvenes se toman el tiempo necesario para leer las políticas cuando se suscriben a una página de internet o cuando descargan una aplicación, por lo general reciben invitaciones de amistad de personas que no conocen, producto tal vez de que publican en redes sociales fotos o información muy personal.

Frecuentemente reciben ofertas a su correo electrónicos de viajes, compras o cualquier información sin haberla pedido, igualmente poseen sus dudas sobre la seguridad que les brinda la red, a pesar de que las redes sociales le ofrecen políticas de seguridad.

Algunos estudiantes suelen compartir su contraseña de redes sociales con amigos, a pesar de que se aseguran luego de cambiarla.

No todos poseen vigilancia por parte de sus padres obre el uso que hacen de sus redes sociales.

Entre las redes sociales más utilizadas están Facebook, WhatsApp, Instagram y Google+, y el uso más frecuente que le dan a las redes sociales es subir fotos o información y diversión.

PROPUESTA

2018

Medidas de prevención usos de redes sociales

María Julissa Zambrano Mendoza

Nombre de la Propuesta: Medidas de Prevención para el uso de Redes Sociales

2.18. Introducción

Para los menores las Redes Sociales son atractivas porque suponen un espacio donde son protagonistas, donde se relacionan con otros semejantes, usan su propio lenguaje y donde caben sus gustos e intereses reales. Algunos padres, no puedes competir con eso, así que tendremos que ver cómo usarlo de forma beneficiosa.

Es un hecho constatado que las redes sociales, en cuanto que giran en torno a personas identificadas e identificables, han puesto en compromiso la privacidad de quienes las usamos. La merma de privacidad es un daño en sí mismo, efectivamente, una pérdida. Supone además un factor de riesgo o catalizador en otras circunstancias desagradables puesto que cuanto más se sepa de una persona, sin duda, más vulnerable es: pensemos en el acoso de un pederasta, en un caso de ciberbullying o en un traumático fin de una relación personal.

2.19. Objetivos de la propuesta

Ofrecer información a los padres y docentes sobre cómo evitar riesgos en las redes sociales tanto en el hogar como el colegio

Brindar a los estudiantes orientaciones para el uso efectivo de las redes sociales

Concientizar a los estudiantes sobre el uso responsable de las redes sociales

2.20. ALGUNOS CONSEJOS PARA LAS FAMILIAS

- Seguramente a veces nos pongamos “pesados” con las horas que pasan en Internet, con quien chatean, qué hacen… Deberemos buscar la mejor manera de comunicarnos con ellos.
- No impongas nada desde el principio, establece acuerdos y consensos pactados con respecto al número de horas, cuándo pueden conectarse… Pacta también las consecuencias de incumplimiento.

- Puedes usar programas informáticos para controlar los contenidos o visualizar el uso de los menores en el ordenador. Sin embargo, este tipo de medidas pueden ser contraproducentes: además de no solucionar el problema genera desconfianza.
- Si nuestro hijo nos confiesa que ha conocido a alguien nuevo o incluso quiere quedar con alguien no es una buena estrategia reprenderle de primeras, lo más probable es que no nos diga nada más y siga haciéndolo a escondidas. Interésate por esa persona, ofrécele a tu hijo ideas o preguntas para que descubra realmente cómo es, y si se empeña en quedar con alguien acompáñale.
- Pasa tiempo junto con tu hijo en internet, chatear juntos, realizar búsquedas, leer blogs… Si él/ella no se acerca a ti pídeselo tú.
- Habla con otros padres y madres, comparte información y conocimientos, asiste a charlas como ésta, propón sesiones en el centro escolar de tu hijo
- Mantén actualizado tu antivirus, firewall y sistema operativo. Tanto del ordenador como del móvil. Así mismo, tapa de alguna forma la webcam del ordenador. Cambiar la contraseña del router wifi que viene por defecto y siempre es mejor conectarse por cable.

2.21. CONSEJOS PARA LOS MENORES

- Mantener un mínimo nivel de privacidad. En la mayoría de las Redes Sociales podemos elegir si queremos que nuestro perfil sea público o privado sólo a determinadas personas o amigos. Revisa tu configuración.
- Así mismo configurar nuestro espacio para que sólo puedan participar de él amigos. Evitaremos que desconocidos publiquen comentarios o no nos lleguen publicaciones no deseadas.
- No aceptar invitaciones de desconocidos, tener una lista de amigos no es una competición ni una colección. Ten en cuenta que son los que tendrán acceso a toda tu información e imágenes.
- No revelar información personal como dónde vivimos, donde estudiamos, números de teléfono… Es más fácil publicar información pero muy difícil suprimirla (o aunque la suprimamos puede que ya haya sido usada). No debemos precipitarnos a publicar algo de lo que luego podamos arrepentirnos.
- Piensa muy bien las imágenes que vas a colgar. Además de que salgas tú en la foto de forma comprometida (recuerda que queda registrado) también estas dando

datos sobre con quién estás (¿has pedido permiso a tus amigos?) o dónde estás (si sale tu casa, coche, colegio… es información que se puede usar para localizarte).

- Ten cuidado si te planteas quedar con alguien a quien no conoces: desconoces quien es realmente y sus verdaderas intenciones. Si decides hacerlo es mejor que vayas acompañada y quedes en algún sitio público con tránsito de gente.
- No compartas tus contraseñas y si tienes indicios de que alguien a entrado con tus datos cámbiala.
- Ten cuidado cuando accedes desde cibercafés, ordenadores púbicos y wifis abiertas ya que en ocasiones dejamos abierta la sesión o los datos se guardan automáticamente. Asegúrate que te has desconectado correctamente y no selecciones la casilla de “recordar datos”.
- Valora usar Nick o nombres falsos en algunas ocasiones, en chats o foros que no sean de confianza.
- Mantén tapada tu webcam, puede ser activada de forma remota sin tu consentimiento.

2.22. SUGERENCIAS

1. Ordenar los contactos en grupos distintos. Separarlos por conocidos, familia, amigos, escuela, etc. Y así, cuando las listas estén armadas, el usuario puede decidir quién puede ver qué cosas.

2. Decidir que se permite ver. Configurar la lista de manera de determinar quién podrá ver la información que se sube a la red social. Hay datos que solo podrán ver los familiares, otros los amigos y los menos privados, los que no comprometen, los conocidos.

3. Dirección y Teléfono. Lo ideal, dicen los especialistas, es no subir a una red social la dirección ni el número de teléfono. Para aquellos que aun así, prefieren hacerlo, lo mejor es que seleccionen cuidadosamente quiénes podrán ver estos datos.

4. No estar siempre disponible. No es necesario –y a veces no es conveniente- estar siempre disponible en una red social. El usuario puede configurar su página para que solo los amigos, o solo los familiares puedan encontrarlo. Y de esta manera evitar a los menos conocidos.

5. Informarse. Leer y utilizar las opciones de privacidad de las redes sociales permitirá crear un ambiente seguro para poder utilizar las redes sociales de manera plena pero sin riesgo.

6. No aceptar a todos los que te envíen invitación: si no conoces a las personas no las agregues.

7. No publiques el lugar donde te encuentras: ya que esto puede ocasionar asaltos a viviendas o secuestros.

2.23. Conclusiones

Describir el conocimiento que tienen los jóvenes del Colegio Fiscal mixto Camilo Ponce sobre ciberseguridad en las redes sociales.

- Los estudiantes de decimo curso poseen conocimientos muy generales sobre la ciberseguridad, y no precisan sus consecuencias por el mal uso de las redes sociales.
- Los cuesta entender que aun siendo jóvenes tienen responsabilidad legal a la hora de hacer un uso indiscriminado de las redes sociales.
- Los estudiantes reconocen haber subido fotos a las redes sin el consentimiento de sus amigos
-

Identificar el uso que hacen los jóvenes del Colegio Fiscal mixto Camilo Ponce en las redes sociales.

- El mayor uso que hacen los estudiantes de las redes sociales están Facebook, Instagram y WhatsApp
- El uso que más predomina es el comunicativo mediante chat, algunos dicen usarlo para ponerse al día con los deberes o consultar entre sus compañeros actividades pendientes.

Analizar la relación entre la Ciberseguridad y el uso de las Redes Sociales en los jóvenes del Colegio Fiscal mixto Camilo Ponce.

- La relación entre ciberseguridad y redes sociales es muy deficiente, puesto que ni la escuela ni los padres han hablado abiertamente sobre el tema.
- No existe una vigilancia en casa en relación a qué tipo de redes sociales y páginas utilizan los jóvenes desde su celular

2.24. Recomendaciones

Dar a conocer los resultados de estwe trabajo a los estudiantes profesores y padres de familia a fin de buscar entre todoas alternativas para concidentizar a los jovenes sobre esta situacion.

- Hacer un campaña informativa institucional para dar a conocer los retos y desventajas ante el ciberespacio

9. Recursos generales

9.1. Recursos materiales

Computadora

Celular

Red de Internet

9.2. Recursos Humanos

Tutorías

Cuestionario

Referencias

Agreda, M., Hinojo, M., & Aznar, I. (2016). ESTUDIO EVALUATIVO DEL IMPACTO DE LAS NUEVAS TECNOLOGÍAS EN LA JUVENTUD Y ADOLESCENCIA EN LA PROVINCIA DE GRANADA, ESPAÑA. IMPACT EVALUATION OF NEW TECHNOLOGIES ON TEENAGERS AND YOUNG ADULTS IN THE PROVINCE OF GRANADA, SPAIN. *Hemispheric & Polar Studies Journal*, 61-77.

Aguaded, J. (2012). La competencia mediática, una acción educativa inaplazable. *Comunicar*, 7-8.

Alfaro, F. (2010). Redes sociales y privacidad. En J. M. Villasuso, *Ciberseguridad en Costa Rica* (págs. 1-433). San José: PROSPIC.

Almansa, A. (2013). Redes sociales y jóvenes. Uso de Facebook en la juventud colombiana y española/Social Networks and Young People. Comparative Study of Facebook between Colombia and Spain. *Comnicar 20(40)*, 127-135.

Alonso, G. (2017). *El informe CiberAstur refleja que dos de cada cien estudiantes de Secundaria sufren acoso escolar grave.* Austria: CiberAstur.

amigas, P. (2 de Marzo de 2015). *Ciberacoso*. Obtenido de Informacion y consejos: http://www.ciberacoso.net/tipos.html

Barrantes, E. G. (2010). Conceptualización de la ciberseguridad. En J. M. Villasuso, *Ciberseguridad en Costa Rica* (págs. 1-433). San José: PROSIC.

Bolívar, G. (Marzo de 2014). *Metodología de la Investigación*. Recuperado el 16 de Agosto de 2016, de http://metodosrecreacion.blogspot.com/p/blog-page_9449.html

Carrillo, N. (3 de Junio de 2011). *slideshare*. Recuperado el 16 de Agosto de 2016, de http://es.slideshare.net/nelsycarrillo/tcnica-de-observacin

Cerrada, A., Fojón, E., Gil, H., & Coz, R. (2010). Cuadro Integral de Mandos como soporte al proceso de Evaluación de la Madurez de una Red Social Virtual en materia de Privacidad. *V International Congress on IT Governance and Service Management: Proposals for Tough Economic Times.* (págs. 1-6). Alcalá de Henares: Universidad Nacional de Educación a Distancia.

Comninos, A. (2013). Una agenda de ciberseguridad para la sociedad civil: ¿qué hay en juego? *APC-201304-CIPP-R-ES-DIGITAL-184*, 1-11.

Coz, R., & Fojón, E. (2010). *Modelo de madurez para la privacidad de una red social virtual.* Madrid: Lulu Enterprises Inc.

Coz, R., & Fojón, E. (2013). Modelos y Enfoques de ciberseguridad en las Redes Sociales Virtuales. *Red Seguridad*, 1-7.

Dalla, V., DiPietro, A., Morel, S., & Psaila, E. (30 de Agosto de 2016). Cyberbullying among Young People. European Parlament Think Tank.

De Vega, J., & Tejada, S. (2011). Adolescencia a Internet. En R. Pereira, *Adoelscentes en el siglo XXI* (pág. 209). Madrid: Morata.

DepartamentodeSalud. (6 de Noviembre de 2016). *Faros.* Obtenido de San Joan de Déu Barcelona Hospital: http://faros.hsjdbcn.org/es/articulo/como-evitar-menores-sufran-grooming-acoso-sexual-internet

de-Salvador, L. (3 de Julio de 2014). *LOS PROBLEMAS ESTRUCTURALES EN EL PLANTEAMIENTO DE LA CIBERSEGURIDAD.* Obtenido de Boletín electrónico del Instituto Español de Estudios Estratégicos:

file:///C:/Users/Julissa/Downloads/LOS_PROBLEMAS_ESTRUCTURALES_EN_EL_PLANTE%20(2).pdf

eCGlobal, Solutions, eCMetrics, & CLIPS, I. d. (2012). *Sexting, una amenaza desconocida.* Brasil, Argentina, Bolivia, Chile, Colombia, Costa Rica, Ecuador, México, Panamá, Paraguay, Perú, Puerto Rico, Uruguay y Venezuela.

Escobar, N. (19 de Mayo de 2015). *Hipertextual*. Obtenido de Qué es el grooming y cómo podemos proteger a los niños en Internet: https://hipertextual.com/2015/05/que-es-el-grooming

ESET, L. (Febrero de 2014). *ESET Digipadres*. Obtenido de https://www.digipadres.com/quienes-somos

Fierro, A., Vázquez, M. M., & Alfaro, M. (2013). Los adolescentes ante las nuevas tecnologías: ¿beneficio o perjuicio? *Boletín pediatría*, (3):117-8, 224.

Fojón, E., & Sanz, A. (2010). *Ciberseguridad en España: una propuesta para su gestión.* Madrid: Real Instituto Elcano (ARI).

FundaciónPfizer. (2009). *La juventud y las Redes Sociales en Internet.* Obtenido de Informe de resultados de la encuesta.: https://www.fundacionpfizer.org

Ganuza, N. (2011). La situación de la Ciberseguridad en el ámbito internacional y de la OTAN. (149), 128-164. En I. E. Estratégicos, *CIBERSEGURIDAD. RETOS Y AMENAZAS A LA SEGURIDAD NACIONAL EN EL CIBERESPACIO* (págs. 128-164). España: Cuadernos de Estrategia.

Garmendia, M., Jiménez, E., Casado, M., & Mascheroni, G. (2016). *Riesgos y oportunidades en internet y usode dispositivos móviles entre menores españoles (2010-2015).* España: Net Children Go Mobile.

Giant, N. (2016). *Ciber-Seguridad para la i-Generación. Usos y riesgos de las redes sociales y sus aplicaciones.* Madrid: Narcea, S.A. ediciones .

Gordo, A. (2008). Jóvenes en peligro o peligrosos?. Alarmas y tecnologías sociales del "desarrollo" y gobierno digital. *Revista de estudios de Juventud*, 103-114{.

Guzmán, M. (2010). *Ciberseguridad en Costa Rica.* San José: PROSIC.

Hernández, L. (2014). Ciberseguridad; Respuesta global a las amenazas cibernéticas del s. XXI las ciberamenazas, un nuevo reto para la jefatura de información de la guardia civil,. *3ª ÉPOCA*, , 1-31.

Hernández, R., Fernandez, C., & Pilar, B. (2015). *Metodología de la Investigción* . México: McGrawHill.

INTECO, I. N. (Marzo de 2009). *Estudio sobre hábitos seguros en el uso de las TIC por niños y adolescentes y e-confianza de sus padres.* Obtenido de https://www.incibe.es

INTECO, I. N. (s.f.). *Guía legal sobre Ciberbulling y Grooming.* Obtenido de Área jurídica de la seguridad y las TIC.: URL:http://www.academia.edu/

Interior., M. d. (03 de Diciembre de 2012). *Estudio sobre la cibercriminalidad en España, año 2015.* Obtenido de interior.gob.es: http://www.interior.gob.es/es/prensa/balances-e-informes/2015

Lebet, G. (Enero de 2003). Recuperado el 16 de Agosto de 2016, de https://gabriellebet.files.wordpress.com/2013/01/tecnicas-de-recoleccic3b3n4.pdf

Leiva, E. A. (2015). Estrategias Nacionales de Ciberseguridad: Estudio Comparativo Basado en Enfoque Top-Down desde una Visión Global a una Visión Local. *Revista Latinoamericana de Ingenieria de Software*, 161-176.

Livingstone, S., Mascheroni, G., Olafsson, K., & Haddon, L. (2014). *Children's online risks and opportunities: comparative findings of EU Kids Online and Net Children Go mobile.* Net Children Go Mobile & EU Kids Online joint report.

Lozano, G. (3 de Abril de 2010). *Analisis de Datos.* Recuperado el 16 de Agosto de 2016, de http://es.slideshare.net/Prymer/anlisis-de-datos-3631192

Luminita, L. (2015). EDUCACIÓN PARA LA SALUD PARA EVITAR EL ACOSO SEXUAL A TRAVES DE LAS REDES SOCIALES EN ADOLESCENTES CON EDADES ENTRE 12 y 16 AÑOS. *Grooming*. Madrid, España: Universidad Francisco de Vitoria.

Martín, P. (24 de Julio de 2015). *INSEGURIDAD CIBERNÉTICA EN AMÉRICA LATINA: LÍNEAS DE REFLEXIÓN PARA LA EVALUACIÓN DE RIESGOS.* Obtenido de Boletín electrónico del Instituto Español d eEstudios Estratégicos: http://www.ieee.es/en/Galerias/fichero/docs_opinion/2015/DIEEEO79-2015_InseguridadCibernetica_AmericaLatina_PaulE.Martin.pdf

Matadamas, W., Meza, P., Moreno, M., Portela, H., & Valle, S. (2016). Plan de concientización para usuarios de dispositivos móviles y redes sociales en edad infantil. México, Mexico: Instituto Politécnico Nacional.

Merino, V. (1 de Noviembre de 2016). *Ciberdelitos y víctima menor de edad.* Obtenido de documentospenales.com.ar: http://www.pensamientopenal.com.ar/system/files/2017/02/doctrina44901.pdf

Ministerio de defensa de España. (2010). *Ciberseguridad: retos y amanezas en el ciberespacio.* España: Autor.

Morales, M. (7 de Enero de 2016). Plataforma Experimental de CIberseguridad, sobre infraestructura virtualizada para mitigar los ataques de denegación de servicio. *Trabajo de titulación, previo a la obtención del título de Ingeniero en Sistemas e Informática*. Quito, Pichincha, Ecuador: ESPE.

Negroponte, N. (1995). *Ser Digital.* Barcelona. España: BSA.

O'Connell, R. (2013). A typology of child cybersexploitation and online grooming practices. (págs. 1-19). Cyberspace Research Unit University of Central Lancashire .

Oliveira, J. (23 de Junio de 2017). Se busca 350.000 expertos en ciberseguridad. España.

Palella, S., & Martins, F. (2010). Metodología de la investigación cuantitativa. Caracas - Venezuela: 2a. ed.

Pantallasamigas. (2015). Obtenido de http://www.sexting.es/peligros/

Pereira, R. (2011). *Adolescentes en el siglo XXI.* Madrid: Morata.

Pons, A. (2013). *El Desorden Digital.* Barcelona. España: Siglo XXI.

Prenky, M. (2001). Digital Natives, Digital immigrants. *On the Horizon, Vol. 9 Issue,* 5, pp.1-6.

Que no te la den. (10 de Abril de 2011). Obtenido de http://www.protegeles.com

Ramírez, B. (2 de Diciembre de 2016). Medición de madurez de CiberSeguridad en MiPymes colombianas. Bogotá, Colombia: Universidad Nacional de Colombia Facultad de Ingeniería, Área Curricular de Ingeniería de Sistemas e industrial.

Remarkable. (2017). *TecnoTrust security made easy*. Obtenido de Ciberseguridad en Redes Sociales, Exposición Mediática e Internet: http://tecnotrust.com/seguridad-en-redes-sociales-e-internet/

Ríos, D., & Villa, J. (17 de Junio de 2017). Los grandes retos de la ciberseguridad. España.

Rodríguez, G. (2016). Ciberseguridad realidad y tendencias en Venezuela. *Cuestiones Jurídicas*, 13-39.

Rodríguez, G. (2016). La ciberseguridad: una asignatura pendiente en la sociedad de la información. *Frónesis*, 1-10.

Rubio, J. A. (23 de Octubre de 2015). Un Marco para el Análisis de Riesgos en. *Doctoral dissertation*. España: Universidad Rey Juan Carlos.

Ruiz, M. (2010). *eumed.net - enciclipedia virtual*. Recuperado el 29 de Agosto de 2016, de http://www.eumed.net/tesis-doctorales/2012/mirm/cualitativo_cuantitativo_mixto.html

Sánchez, A. (26 de Noviembre de 2015). Ciberseguridad y redes sociales, desatendidas por empresas mexicanas: PWC. México.

Sánchez, A. C. (2010). Hacia un concepto de “ciberseguridad”. En J. M. Villasuso, *Ciberseguridad en Costa Rica* (págs. 1-433). San José: PROSIC.

Tamayo, M., & Munóz, S. (16 de Octubre de 2007). Recuperado el 20 de Agosto de 2016, de Bitácora. Introducción al lengua de la ciencia: http://angelicamarialo.blogspot.com/2007/10/diseo-metodologico-segn-mario-tamayo-y.html

Telecomunicaciones, U. I. (21 de Mayo de 2008). *UIT-T X.1205 Serie X: Redes de Datos, Comunicaciones de Sistemas Abiertos y Seguridad.* Obtenido de Unión Internacional de Telecomunicaciones: https://www.itu.int/rec/T-REC-X.1205-200804-I/es

TheChristianPost. (2 de Abril de 2013). Escolas britânicas afastam 3 mil alunos por ano por conduta sexual imprópria.

Union Internacional de telecomunicasiones . (23 de junio de 2018). *Comprometida para conectar al mundo*. Obtenido de https://www.itu.int/es/Pages/default.aspx

Vargas, R., Recalde, L., & Reyes, R. (2017). Ciberseguridad y ciberdefensa modelo ecuatoriano de gobernanza. *Urvio*, 30-45.

Velásquez, M., López, S., & Arellano, A. (2013). Sexting: La sexualidad responsable también debe ejercerse en las redes sociales. *In XXIX congreso latinoamericano de sociología*, (págs. 1-10). Santiago.

Villalba, A. (2015). *La cibersefuridad en España 2011-2015 una propuesta de modelo de organización.* Madrid: Universidad Nacional de Educación a Distancia. Tesis Doctoral.

Villasuso, J. (2010). *Ciberseguridad en Costa Rica.* San José: PROSIC.

Wigodski, J. (14 de Julio de 2014). *Metodología de la investigación*. Recuperado el 16 de Agosto de 2016, de http://metodologiaeninvestigacion.blogspot.com/2010/07/poblacion-y-muestra.html

Zumba, A. (8 de Mayo de 2015). DELITOS CONTRA LA SEGURIDAD DE LOS ACTIVOS DE LOS SISTEMAS DE INFORMACIÓN Y COMUNICACIÓN:

DELITOS A TRAVÉS DE LAS REDES SOCIALES. *MONOGRAFÍA PREVIA A LA OBTENCIÓN DEL TÍTULO DE ABOGADA DE LOS TRIBUNALES DE JUSTICIA DE LA REPUBLICA Y LICENCIADA EN CIENCIAS POLÍTICAS Y SOCIALES*. Cuenca, Azuay, Ecuador: Universidad de Cuenca.

ANEXOS

Cronograma de actividades realizadas

Miércoles, 20 septiembre	- Trabajo del proyecto de tesis en marco conceptual
Jueves, 28 septiembre	- Presentación con el docente tutor
Miércoles, 4 octubre	- Aplicación de correcciones.
Viernes, 6 octubre	- Tutorías, revisión del marco teórico y del modelo de análisis del gobierno electrónico.
Lunes, 9 octubre	- Material de evaluación
Miércoles, 18 octubre hasta miércoles, 15 de noviembre	- Permiso para evaluar en el distrito de Educación - Realizar las encuestas respectivas
Viernes, 17 noviembre hasta miércoles, 22 noviembre	- Tabulación de resultados, conclusiones y recomendaciones.
Martes, 28 noviembre	- Correcciones en las conclusiones y recomendaciones para que cuadren con los objetivos. - Culminación del borrador preliminar.

Viernes, 1 diciembre	- Tutorías, revisión del borrador preliminar completo.
Jueves, 7 diciembre	- Entrega de documentación e información para la presentación del borrador final.

Anexo 1.-**Permisos y Material de evaluación respectivo**

Universidad Laica “Eloy Alfaro” de Manabí

Facultad Ciencias de la Comunicación

Manta, 6 de Noviembre del 2017

Solicitud de permiso dirigido al distrito de Educación Zona n ° 4, dirigiéndome a ustedes como María Julissa Zambrano Macías con C.I. 131158615-8, egresada en la facultad de Ciencias de la Comunicación en la carrera de Periodismo, para solicitarles el permiso respectivo para realizar una encuesta a los alumnos de décimo año del plantel educativo mixto Camilo Ponce de la ciudad de Manta.

Este estudio tendrá un fin netamente investigativo, que servirá para la obtención de mi licenciatura en comunicación.

La encuesta es totalmente anónima sin vulnerar los datos personales de ningún estudiante menor de edad.

Esperando su pronta respuesta saludos cordiales,

María Julissa Zambrano Macías

Egresada en Ciencias de la Comunicación - Periodismo

Cuestionario Ciberseguridad

Estimado joven:

Actualmente me encuentro desarrollando mi tesis de grado, la cual esta relacionada con la ciberseguridad. A continuación se te presentan una serie de preguntas, responde lo más sincero posible, la información que aquí nos dé, será utilizada sólo para la investigación, por favor no firme ni coloque datos personales en este cuestionario.

Coloca una “X” en la(s) respuesta(s) que mejor represente tu alternativa.

PREGUNTAS	RESPUESTAS			
	Siempre	Algunas veces	Rara ves	Nunca
1.- ¿Cuándo te suscribes a una página de internet, te tomas el tiempo para revisar las políticas de afiliación?				
2.- ¿Recibes invitaciones de amistad de personas que no conoces?				
3.- ¿Has recibido ofertas de compras o viajes a tu correo sin tu solicitarla?				
4.-¿Publicas información muy personal en las redes sociales?				

5.- ¿Consideras que las redes sociales son seguras?				
6.- ¿Comparte tu contraseña de las redes con amigos?				
7.- ¿Te aseguras de cambiar tu contraseña?				
8.-¿Tus padres controlan el uso que le das a las redes sociales?				
9.-¿Tus redes sociales te ofrecen políticas de seguridad?				

10.- ¿Cuáles de las siguientes redes sociales estas suscrito actualmente?

Facebook_____ WhatsApp_____ Instagram____ Twitter____ YouTube_____ Skype____

Pinterest____ Messenger____ WeChat____ QQ____ Google+____ Haboo____

11.- ¿Por lo general usas tus redes sociales para?

Buscar amigos____ Publicar fotos____ Buscar información____ Subir videos_____

Planificar salidas____ Leer contenidos____ Mensajes y chat____ Actualizar estado____

Compartir contenido____ Saber de tus amigos____ Diversión_____ Conocer personas____