INSTITUTO POLITÉCNICO NACIONAL

UNIDAD PROFESIONAL INTERDISCIPLINARIA
DE INGENIERÍA Y CIENCIAS SOCIALES
Y ADMINISTRATIVAS

“PLAN DE CONCIENTIZACIÓN PARA USUARIOS DE DISPOSITIVOS MÓVILES Y REDES SOCIALES EN EDAD INFANTIL”

T E S I N A

QUE PARA OBTENER EL TÍTULO DE
LICENCIADO EN CIENCIAS DE LA INFORMÁTICA

P R E S E N T A N
WENDI NAYELI MATADAMAS HERNÁNDEZ
PATRICIA MAYULI MEZA SOLIS
MARÍA GUADALUPE MORENO GÓMEZ
HILDELISA PORTELA PÉREZ
SERGIO VALLE OCTAVIANO

CIUDAD DE MÉXICO 2016

ÍNDICE

ÍNDICE FIGURAS

Resumen

Debido a que en los últimos años se tiene fácil acceso a los dispositivos móviles, a las aplicaciones y múltiples funciones que éstos ofrecen como por ejemplo las redes sociales, es muy probable que aumenten los riesgos para los usuarios que empiezan a utilizar éstos dispositivos desde temprana edad. Es aquí donde los padres deben participar manteniendo un control sobre los dispositivos para evitar daños, pérdidas o robo y enseñar a sus hijos a que deben establecer contraseñas robustas, así como supervisar las actividades que realizan con los dispositivos móviles y advertirles los riesgos que hay al usar una red WiFi abierta.

Como propuesta a esta problemática se propone un plan de concientización orientado a los niños de entre 5 y 10 años que incluye la participación de los niños, los padres y los docentes y que puede ser aplicado en escuelas de nivel básico y con esto lograr que tengan una mayor conciencia en la seguridad de la información.

Además de la aplicación presencial del plan de concientización, se integran herramientas en línea, en la que todo el material del plan se encuentra en una página web compatible para móviles, y también se maneja un perfil de Facebook en el que se dan consejos para mantener la seguridad de los menores al utilizar sus dispositivos móviles y redes sociales.

El plan se basa en propuestas desarrolladas por grandes empresas, gobierno de México y gobierno de otros países del mundo en los que se están llevando a cabo medidas para proteger a los más pequeños, además de las buenas prácticas propuestas por NIST en el documento de la serie 800-50, adecuado para ser aplicado a la niñez.

El modelo del plan se compone de 4 fases, diseño del plan, desarrollo del material para la presentación del plan, implementación del plan y monitoreo del plan. En cada una de las fases se anidan tareas específicas que deben realizarse para lograr el éxito del mismo.

La primera fase es el diseño del plan, esta es la parte fundamental en donde se definen y detallan todos los puntos que contendrá el plan, se evalúan las necesidades a cubrir, se define la estructura que tendrá y se diseña la estrategia a seguir para su implementación.

En la fase de desarrollo del material se hace la selección de temas, se recopila la información y se desarrolla el material que servirá de apoyo para la implementación del plan.

En la tercera fase se hace la implantación del plan, se da a conocer el material diseñado y desarrollado para realizar la difusión.

Finalmente, en la fase de mantenimiento del plan se revisan los resultados obtenidos, se recibe una retroalimentación y se determina que mejoras se deben hacer.

Introducción

De acuerdo con un estudio realizado por la organización sin fines de lucro Common Sense Media el uso infantil de los teléfonos inteligentes (también conocidos como Smartphone) aumentó de 8 a 40 por ciento en los últimos años, mientras que 63 por ciento de los niños mexicanos entre cuatro y ocho años de edad manejan dichos dispositivos sin ningún problema (Pulso, 2015); sin embargo, la mayoría de éstos usuarios no son conscientes aún de los riesgos, amenazas y vulnerabilidades a los que están expuestos.

Es por este motivo que el presente trabajo aborda la problemática que existe actualmente respecto a la seguridad y el uso de dispositivos móviles, aplicaciones diversas y redes sociales por usuarios en edad infantil. Tomando en cuenta el crecimiento de la población que tiene acceso al uso de tecnologías como lo son los dispositivos móviles y las redes sociales se tiene como objetivo el desarrollar un plan de concientización dirigido a usuarios de dispositivos móviles en edad infantil y a sus padres, teniendo en consideración las recomendaciones que existen actualmente para este tema en diversas partes del mundo y asociaciones gubernamentales y no gubernamentales, y haciendo la difusión del material tanto de forma física como digital en un formato principalmente dirigido a los niños y en segundo lugar a los adultos que son los principales responsables del menor.

La tesina está formada por 6 capítulos, el primer capítulo da a conocer al lector de manera general cual es la problemática que se aborda a lo largo de la tesina, se detallan los objetivos a cumplir con la investigación, así como las técnicas de investigación que se llevan a cabo para dar solución al problema de la falta de conciencia generada por el temprano acercamiento de la población infantil a los dispositivos móviles y las redes sociales.

El segundo capítulo se centra principalmente en la definición de conceptos básicos que se manejan a lo largo de toda la tesina, para que el lector tenga claro el significado de varios términos clave, adicionalmente se da un contexto histórico en el que se explica cuál es el origen de los dispositivos móviles y redes sociales hasta convertirse en lo que hoy en día conocemos.

En el tercer capítulo se explica y desarrolla el problema de falta de conciencia que rodea a los usuarios en edad infantil que tienen acceso a las redes sociales y los dispositivos móviles, se muestra mediante algunas estadísticas de México y otras regiones del mundo la gravedad del problema y la urgencia por dar a conocer una serie de consejos hacía los padres y hacía sus hijos para hacer un mejor uso de las tecnologías antes mencionadas.

Una vez mostrada la importancia de concientizar a los usuarios en edad infantil de redes sociales y dispositivos móviles, en el cuarto capítulo se mencionan las leyes e iniciativas que existen en diferentes países para la protección de usuarios de redes sociales además se muestran una serie de buenas prácticas que deben tomarse en cuenta para el uso consciente responsable de dispositivos móviles y redes sociales. Estas recomendaciones serán dirigidas tanto a padres de familia, como a los niños.

Dentro del quinto capítulo se realiza el desarrollo del modelo del plan de concientización en el cual se detalla el proceso de aplicación y la manera de cómo se va a evaluar los resultados obtenidos del plan, todo de forma teórica.

El sexto capítulo se enfoca en la aplicación del plan de concientización donde se detalla el material desarrollado dirigido hacía los niños y hacia los padres, este material corresponde al utilizado para implementar y difundir el plan de concientización, además incluye una sección en donde se presentan las ventajas, desventajas, evaluación y retroalimentación del plan.

Para finalizar se presentan las conclusiones a las que se llega de la tesina en general y las conclusiones sobre la propuesta del plan de concientización a las que se llega para identificar si se cumplieron los objetivos y si se logra confirmar la hipótesis.

Capítulo I. Marco metodológico

El propósito de éste capítulo es dar a conocer al lector de manera general cual es la problemática que se aborda a lo largo de la tesina, se detallan los objetivos que pretenden cumplirse con la investigación, así como las técnicas de investigación que se llevan a cabo para poder cumplir con los objetivos planteados que den solución al problema de la falta de conciencia generada por el temprano acercamiento de la población infantil a los dispositivos móviles y las redes sociales.

1.1 Planteamiento del problema

La adquisición de dispositivos móviles, como computadoras portátiles, teléfonos inteligentes y tabletas electrónicas ha mostrado un crecimiento acelerado en los últimos años. En un principio, el objetivo primordial de estos equipos móviles, era fundamentalmente, satisfacer las necesidades de comunicación combinada con la ventaja de portabilidad, principalmente en el ámbito laboral.

Las ventajas que nos ofrecen estos dispositivos para desarrollar cada una de nuestras actividades con mayor facilidad en cualquier ámbito de nuestra vida ha sido la principal causa de este crecimiento. A partir de esto, los costos se han reducido considerablemente y actualmente es común que cualquier persona utilice y tenga acceso a alguno de estos aparatos.

Debido al incremento en el uso de dispositivos móviles, surge el desarrollo de una gran variedad de aplicaciones y funciones, por ejemplo, navegar en internet, mensajería instantánea, publicación de fotos y videos, etc. cada una acompañada de diversos riesgos y amenazas.

Con base en el estudio realizado por El Fondo de las Naciones Unidas para la Infancia o Unicef "La seguridad en los niños en línea retos y estrategias" se puede deducir que los riesgos y amenazas afectan a todos los usuarios de dispositivos móviles siendo los niños los más susceptibles, ya que comúnmente desconocen los peligros existentes.

El fácil acceso a los dispositivos móviles en los últimos años, las múltiples funciones y aplicaciones que ofrecen y los riesgos que corren los niños debido al temprano uso de éstas tecnologías; son las razones por las que se decidió diseñar un plan de concientización que oriente a padres e hijos en el control y manejo de riesgos generados por:

- Redes sociales.
- Aplicaciones enfocadas al entretenimiento (juegos, música, videos).

- Llamadas telefónicas.
- Mensajería instantánea.
- Publicación de fotos y videos.
- Correo electrónico.
- Navegación en internet.

Todos estos riesgos incrementan cuando no se tiene conocimiento de su existencia y cuando aun teniendo conocimiento de su existencia no se tiene interés en ellos o no se sabe cómo poder enfrentarlos. Con el plan de concientización se pretende hacer una difusión a través de diferentes medios para dar a conocer tanto a niños como a sus padres y docentes las recomendaciones básicas para el cuidado de uso de dispositivos móviles y redes sociales.

1.2 Objetivo general

Desarrollar un plan de concientización dirigido a usuarios de equipos móviles en edad infantil y a sus padres en el que se aborda la importancia de proteger la información personal en redes sociales, así como recomendar ciertas acciones que ayuden a tener un uso responsable y seguro de los dispositivos móviles.

1.3 Objetivos específicos

Realizar una investigación en sitios de internet para conocer que recomendaciones existen actualmente para los usuarios menores que utilizan dispositivos móviles, así como investigar si hay leyes que regulen el uso de redes sociales.

Mediante encuestas aplicadas a los padres de niños de nivel básico, conocer si actualmente sus hijos cuentan con dispositivos móviles y de qué forma los orientan sobre su uso.

Conocer el porcentaje de niños que cuentan con un dispositivo móvil propio o si utilizan el de sus padres, identificando cuál es el principal uso que le dan.

Identificar qué saben los padres y los niños sobre el uso de dispositivos móviles y protección de su información personal; con base en esto, saber cuál es el punto débil que tienen para poder reforzarlo con recomendaciones hacía los padres e hijos.

Mostrar a los padres de usuarios infantiles de dispositivos móviles, las recomendaciones sobre el control y manejo de riesgos.

Hacer difusión de las recomendaciones de seguridad de una forma simple y didáctica que los menores puedan comprender con facilidad a través de página web, carteles, pláticas y folletos.

Analizar el impacto y concluir si el material proporcionado fue útil para al menos un 80% de los encuestados.

1.4 Técnicas e instrumentos de medición

Las técnicas de investigación que se utilizan son:

Documental. Apoyada en artículos de internet, estudios realizados anteriormente sobre el tema, estadísticas, documentales, vídeos, entre otros materiales teóricos para obtener información científica y poder dar las mejores recomendaciones a los padres de usuarios de dispositivos móviles en edad infantil sobre el uso responsable de éstos, así como la protección de su información personal.

De campo. Se realizan encuestas y entrevistas a los padres de usuarios de equipos móviles en edad infantil, para conocer qué saben sobre protección de datos personales en redes sociales y uso responsable de equipos móviles; y así conocer cuáles son los puntos débiles para enfocar el plan de concientización y reforzar las debilidades.

1.5 Universo y/o muestra

El universo que se toma para la presente tesina son los usuarios de dispositivos móviles y redes sociales de entre 5 y 10 años que habiten en la Ciudad de México y área metropolitana. Como muestra se toman 100 niños que cumplan con tener una edad de entre 5 y 10 años que además sean usuarios de dispositivos móviles.

1.6 Justificación

Nos encontramos en una era en la que la mayoría de las familias que tienen niños pueden tener acceso a un dispositivo móvil, según un estudio realizado por el Gabinete de Comunicación Estratégica (GCE) el dispositivo más popular a nivel nacional para navegar en internet son los teléfonos inteligentes, seguido de la computadora de escritorio, los equipos portátiles y la tableta,

con las cuales se puede acceder a una gran diversidad de aplicaciones, servicios de mensajería, chat, internet y redes sociales con diferentes finalidades como la educación y el entretenimiento de los menores. El principal problema radica en el poco conocimiento que los niños pueden tener sobre el uso adecuado.

De acuerdo al análisis realizado por el Gabinete de Comunicación Estratégico (GCE), el mayor tiempo empleado para el internet a nivel nacional lo tienen las redes sociales, siendo Facebook la más utilizada con 74.2% de uso, WhatsApp con 12.4% y Twitter con 7.4% por lo cual existe la posibilidad de que terceras personas traten de obtener información personal haciendo mal uso de ésta.

Esto nos lleva a pensar, que los niños no están preparados para enfrentar los riesgos que las nuevas tecnologías presentan. Es por ello que se elabora un plan de concientización con el que los niños y niñas aprendan controles de seguridad básicos para mantener sus dispositivos en buen estado, su información personal y familiar resguardada y para saber discernir entre el contenido que es engañoso y puede causar diversos daños en los equipos y en la integridad del menor teniendo como guía los conocimientos sobre seguridad informática y el apoyo de los padres para el cumplimiento de los objetivos.

1.7 Hipótesis

A través del plan de concientización generado y difundido, se orienta a los usuarios en edad infantil y a sus responsables directos sobre el uso responsable y seguro de dispositivos móviles y redes sociales.

Capítulo II. Marco teórico

En éste capítulo se describen conceptos básicos que se manejan a lo largo de toda la tesina, para que el lector tenga claro que significa cada uno de los términos en los que se profundizará, adicionalmente se da un contexto histórico en el que se explica cuál es el origen de los dispositivos móviles y redes sociales hasta convertirse en lo que hoy en día conocemos.

2.1 Conceptos básicos

En éste capítulo de conceptos básicos se aborda la definición de dispositivos móviles, redes sociales, aplicaciones de mensajería instantánea, ingeniería social, suplantación de identidad, concientización y edad infantil, definirlos permite posteriormente conocer como conjugando todos estos elementos y otros factores tenemos como resultado la problemática actual.

2.1.1 Dispositivos móviles

Se define como dispositivo móvil a los aparatos que tienen la característica de ser portables, con capacidades de procesamiento, conexión permanente o intermitente a una red, con memoria limitada que pueden llevar a cabo funciones generales. Entre algunos de los dispositivos móviles están los Smartphone, computadoras portátiles, tabletas, entre otros.

2.1.2 Redes sociales

La Real Academia Española define como red social a la “Plataforma digital de comunicación global que pone en contacto a gran número de usuarios.”

Las redes sociales se pueden definir como una comunidad virtual donde las personas, llamados usuarios, tienen algún tipo de vínculo con los demás usuarios donde puede interactuar y compartir contenido multimedia como son: videos, imágenes, textos, audios, etc.

La mayoría de estas redes sociales son usadas para enviar mensajes instantáneos, mantener la comunicación con la gente que conocen, comunicarse con nuevas personas, reencontrarse con amigos, compartir, intercambiar y encontrar información.

De acuerdo a la página “Comunidad IEBS” se tiene la siguiente clasificación de redes sociales en internet:

- Redes sociales horizontales. Son redes sociales dirigidas a un público en general y que no se concentran en un tema concreto. Las más populares son Facebook, Twitter, Google+, Tuenti.

- Redes sociales profesionales. Son redes sociales que giran al ámbito laboral. Son plataformas muy útiles para realizar contactos profesionales, recomendaciones profesionales, gestión de currículo vitae, búsqueda de oportunidades laborales. Las más populares son: LinkedIn, Viadeo y Xing.

- Redes sociales de geo-localización. Se basan en la localización física de los usuarios. Las más populares son: Foursquare, Facebook Places y Google Places.

- Redes sociales de contenidos. Son las redes sociales en las que las relaciones entre los usuarios están muy unidas a la generación y divulgación de contenidos de diferentes formatos. Algunos ejemplos son: Flickr, Instagram, YouTube, Vimeo, Slideshare, entre otras.

2.1.3 Redes sociales educativas

Según el curso “Redes Educativas” del Departamento de Educación, Universidades e Investigación se define como red social educativa a las estructuras intencionales, con intereses-objetivos comunes en las que todos sus miembros tienen la posibilidad de trabajar y responsabilizarse en igualdad. Las estructuras organizativas que se crean dentro de las redes ofrecen oportunidades de aprendizaje a los profesionales, permitiendo detectar las necesidades de gestión y de dirección.

Algunos ejemplos de redes sociales educativas son:

- Brainly. Se dirige al alumnado de todos los niveles, incluyendo los niños escolarizados en casa, así como a padres y profesorado. S principal objetivo es resolver preguntas de diferentes materias como matemáticas, historia, física y química desde un nivel muy básico.

- Docsity. Permite consultar apuntes, noticias, vídeos didácticos relacionados con temas de interés científico como biología, química, derecho, historia, idiomas, matemáticas o psicología, entre otras materias. Todos los contenidos son orientados a un nivel más especializado que la red de Brainly.

- educaNetwork, Aprendiendo juntos. Brinda la posibilidad de formar grupos de aprendizaje desde los que sus usuarios crean cursos, comparten archivos, chatean, incluyen pruebas multimedia que permiten poner a prueba los conocimientos de sus miembros.

- Edmodo. En 2008, Nic Borg y Jeff O'Hara fundaron esta plataforma educativa que funciona como una red social y en la que pueden participar docentes, familias y alumnos. Permite crear grupos cerrados y privados, enviar trabajos, compartir enlaces y documentos, adjuntar ficheros. También existe la opción de que los docentes inviten a los alumnos a participar en debates en línea, para lo cual es necesario registrarse con un nombre de usuario y contraseña.

- RedAlumnos. Es una plataforma de formación que pone en contacto a docentes y alumnado, de forma que el profesor puede impartir cursos on-line y apoyar sus clases presenciales. También puede ser instalada en un centro de enseñanza y contar con aulas virtuales, exámenes on line, edublogs, chats… Tiene servicios gratuitos y de pago.

Las redes sociales resultan interesantes para los alumnos ya que les permiten estar en contacto directo con sus profesores, sus amigos y compañeros de otros cursos. Esto permite crear un ambiente de trabajo favorable que es uno de los motivos directos del éxito de las redes sociales.

Entre las ventajas que encontramos al trabajar con redes sociales orientadas a la educación tenemos:

- Mejora la comunicación entre profesores y alumnos.

- Centralizar en un único sitio todas las actividades docentes, profesores y alumnos de un mismo centro educativo.

- Facilita la coordinación y trabajo de diversos grupos de aprendizaje.

Se concluye entonces que utilizar las redes sociales como una plataforma educativa, es de gran éxito ya que los alumnos se sienten atraídos al poder conocer e interactuar con gente nueva y los profesores pueden mantener el contacto con sus alumnos fuera del aula lo cual fomenta una buena relación entre ellos.

De esta forma, las redes sociales pueden ser una herramienta que le de ventaja competitiva a los niños en un futuro a corto plazo.

2.1.4 Aplicaciones de mensajería instantánea

Una aplicación es un software orientado a una tarea determinada; así entonces se define a las aplicaciones de mensajería instantánea como todo aquel software que se puede instalar en dispositivos móviles y que cumple con la función de mantener comunicados a los usuarios en tiempo real una vez que se conectan a la red. **(Ponce, 2006)**

En la actualidad mediante estas aplicaciones, no solo se pueden enviar mensajes de texto, sino que además se pueden realizar llamadas y videoconferencias desde cualquier lugar del mundo; así como enviar nuestra ubicación o algún archivo de audio, de imagen o documento.

En la Figura 2.1 podemos ver las principales aplicaciones de mensajería instantánea en el mundo, según un informe de 2014 emitido por Neomobile.

PRINCIPALES APPS DE MENSAJERIA EN EL MUNDO				
App	**Usuarios (millones)**	**Propietaria**	**Principales Mercados**	**Servicios**
WhatsApp	465	Facebook	Estados Unidos, Europa, América Latina	Mensajería
Line	400	Naver Corp. (NHN)	Japón, Taiwán, Sudeste asiático	Mensajería, juegos, llamadas, stickers
WeChat	355	Tencent	China	Mensajería y servicios varios
Viber	300	Rakuten	Japón	Mensajería, llamadas, stickers
Kakao Talk	133	Kakao Corp.	Corea	Mensajería, juegos, stickers

Figura 2.1 Tabla de las principales aplicaciones de mensajería en el mundo.

2.1.5 Ingeniería social

En el libro “Ingeniería Social el Arte del Hacking Personal” se define la ingeniería social como “El acto de manipular a una persona para que lleve a cabo una acción que –puede ser o no- lo más conveniente para cumplir con cierto objetivo. Este puede ser la obtención de información, conseguir algún tipo de acceso o lograr que se realice una determinada acción.”

Se puede clasificar en dos tipos indirecta y directa; la directa es lo que usualmente hacen las personas que se dedican a “adivinar” el futuro, hacen preguntas que de un principio se considerarían inocentes pero se obtiene gran información que podría ser útil para poder predecir la

siguiente respuesta; la forma indirecta de poder obtener información y la que nos interesa más, es por medio de internet, aquí hay muchas formas de obtener información ya sea por medio de correos, mensajería instantánea, virus, etc.

El principal ejemplo que podríamos poner son los correos electrónicos mandados de supuestos bancos pidiendo las claves de acceso de las cuentas bancarias o hipervínculos que descargan virus para después poder extraer la información guardada en la PC, la Figura 2.2 muestra un ejemplo de un correo falso pidiendo que el usuario acceda a su cuenta siguiendo un link, el cual, podría ser un enlace para descargar un virus o una página donde simplemente se guardarían los datos de acceso del usuario.


BBVA

Estimado cliente de BBVA:

Grupo BBVA siempre trata de encontrar sus expectativas mas altas.
Por eso usamos la ultima tecnologia en seguridad para nuestros clientes.
Por lo tanto nuestro departamento de antifraude ha desarrollado un nuevo sistema de seguridad que elimine cualquier posibilidad del acceso
de la tercera persona a sus datos, cuentas ni fondos. Este sistema esta construido en la utilizacion de una pregunta secreta y respuesta.

Su respuesta secreta seria usada para confirmar su identidad cuando haga una operacion de pagos.
Es obligatorio para todos los clientes de **BBVA** en Linea usar este sistema de seguridad.
Nuestro consejo para usted es que introduzca sus datos se acceso para pasar La Verificacion Del Sistema.

Si el registro no es realizado dentro de 48 Horas su cuenta sera suspendida temporalmente hasta que su registro sea completado.
Esto solo le va a costar unos minutos de su tiempo y va a tener una seguridad mucho mas estable.
Para comenzar el registro por favor haga click aqui:

https://www.bbva.es/TLBS/tlbs/esp/segmento/particulares/index.jsp

Figura 2.2 Ejemplo de phishing.

Uno de los principios que usan las personas que se dedican a los fraudes es haciéndole pensar al usuario que el administrador es el que se está poniendo en contacto directamente, así se crea un vínculo de confianza ya que se tiene por entendido que una persona con tal rango debería de proteger toda la información que se le está proporcionando, dicho acto se conoce como “Phishing” o “Suplantación de identidad”.

Según Kevin Mitnick un hacker famoso, la ingeniería social se basa en estos cuatro principios:

- Todos queremos ayudar.

- El primer movimiento es siempre de confianza hacia el otro.

- No nos gusta decir “No”.

- A todos nos gusta que nos alaben.

Todos estamos propensos a este tipo de técnica, pero se puede aprender a identificar los puntos clave de la ingeniería social para poder evitar divulgar información sensible y estar prevenidos ante dicha situación.

2.1.6 Suplantación de identidad

Cuando alguien roba tu información personal y financiera, con la finalidad de suplantar tu identidad para obtener beneficios de forma fraudulenta, se dice que comete robo de identidad.

Tus datos pueden ser utilizados para solicitar créditos o usar los que ya tienes de forma exagerada, crear cheques falsos con tu número de cuenta e incluso obtener a tu nombre algún documento oficial. Cuando esto sucede, no sólo pierdes dinero, también se daña tu reputación financiera. Si solicitan un crédito a tu nombre sin que te des cuenta y por consiguiente nunca se paga, esto dañará tu historial crediticio y es probable que en el futuro las instituciones financieras te nieguen algún crédito. En casos más graves puedes tener problemas con las autoridades, derivados de algún fraude o infracción que el ladrón cometa a tu nombre **(CONDUSEF, 2014)**.

Por lo general, a las víctimas les lleva mucho tiempo darse cuenta de que su identidad ha sido robada y cuando se percatan del fraude, el ladrón ya ha hecho estragos.

En la actualidad existen delincuentes que tratan de obtener la información básica necesaria para intentar robar la identidad de cualquier persona, el robo físico de esta información es Offline y el robo de identidad por medio de la tecnología es Online.

En el tipo Offline, el robo de información puede suceder cuando perdemos o nos roban nuestra cartera, en donde se encuentran nuestras identificaciones y datos personales.

Otros delincuentes buscan información dentro de los buzones de correo y hasta dentro de la basura. Por ello hay que destruir cualquier documento que lleve nuestros datos antes de tirarlo y pagar nuestros recibos e impuestos por banca electrónica o en los portales oficiales de las

empresas y dependencias correspondientes, asegurándonos siempre de que sea desde un sitio seguro (marcado en la barra de navegación como “https”) y desde una computadora no pública.

En el modo Online, los delincuentes cibernéticos buscan hacerse de su información a través de varios medios; por ejemplo, mandan correos electrónicos falsos en nombre de instituciones reconocidas pidiendo se les mande información personal confidencial. En algunos casos, estos correos pueden contener además virus y software espía.

Otro modus operandi es revisar las redes sociales en búsqueda de información útil sobre su persona.

La recomendación es ignorar los correos sospechosos y editar, a nuestra conveniencia, los filtros de privacidad de nuestras redes sociales, y no incluir información personal que no sea necesaria.

Cuando un criminal logra robar una identidad, la usa para realizar trámites en nombre de la víctima, incluyendo la solicitud de créditos.

2.1.7 Concientización

La concientización es “crear conciencia entre la gente acerca de un problema o fenómeno que se juzga importante” básicamente nuestro problema es el mal uso de las redes sociales y el internet en edad temprana, esto trae consecuencias que podrían dañar la integridad de los niños y sus familias **(CNN México. 2011)**.

En México, el 50% de las denuncias por delitos cibernéticos, presentadas de 2008 a la fecha, se relacionan con este delito, de acuerdo con el Instituto Federal de Acceso a la Información y Protección de Datos (IFAI).

No obstante, no se debe alejar a los niños del internet, pues es una herramienta valiosa en términos educativos.

La mayoría de los jóvenes que tienen acceso a Internet en México utilizan esta herramienta para entrar a redes sociales, intercambiar información y crear relaciones de amistad, lo cual es usado por muchas personas para obtener datos personales de los cibernautas a través de engaños y utilizarlos para cometer delitos contra ellos y sus familias, advirtió la Comisión Nacional de los Derechos Humanos (CNDH).

Es importante promover entre los jóvenes el uso responsable y adecuado de las redes sociales a fin de combatir la trata de personas, el enganche de mujeres y hombres y la pornografía infantil.

2.1.8 Edad infantil

El periodo de la vida humana a la que se le define como infancia comprende desde el nacimiento hasta la adolescencia, que es el periodo donde los seres humanos desarrollan sus capacidades físicas e intelectuales.

En el ámbito jurídico se denomina a los infantes como personas de entre uno y cinco años; el rango de edad que se toma para el presente trabajo es de cinco a diez años siendo la edad más común, según estudios y estadísticas, en que los infantes tienen contacto con la tecnología.

2.1.9 Vulnerabilidad

Se define como vulnerabilidad a la existencia de algún punto débil en un sistema informático, que puede ser aprovechado por un atacante para violar la seguridad y causar daños.

Las vulnerabilidades se presentan en todo tipo de sistemas o dispositivos informáticos; en éste caso centraremos nuestra atención en los dispositivos móviles. **(Tutorial de Seguridad Informática, 2015)**

2.1.10 Modelo

Un modelo es un esquema que representa una situación real con cierta precisión dentro de lo que es posible representar.

Dentro del modelo, es recomendable representar y detallar todos los factores que intervienen en la situación real que se quiere representar, dentro de estos factores que no deben faltar en la definición de un modelo son:

- Un propósito claramente definido.
- Identificar las consideraciones esenciales.
- Desechar consideraciones superfluas (estas son fuente de confusión).

- El modelo debe representar la realidad en forma simplificada, pero sin omitir factores esenciales de la realidad.

2.2 Origen de los dispositivos móviles

Este punto contiene la historia y evolución de los dispositivos móviles, su propósito y el catalizador que impulsó su desarrollo, además de las características básicas y actuales de estos dispositivos.

2.2.1 Historia y evolución de los dispositivos móviles

El propósito de cualquier equipo como computadoras y dispositivos más pequeños como laptops, tabletas o teléfonos inteligentes es poder comunicar alguna información a través de ellos, y a esta información, darle el uso para lo cual es transmitida.

En 1946, máquinas como la ENIAC, tenían el propósito de realizar cálculos aritméticos (cerca de 5000 sumas y 300 multiplicaciones por segundo) para aplicación militar y científica. La ENIAC ocupaba una superficie de 167 m2 y pasaba unas 27 toneladas. Posteriormente con el avance de cada uno de los componentes que integran un equipo de cómputo el tamaño fue disminuyendo y la capacidad para almacenar, procesar y transmitir información fue aumentando.

El auge de Internet, dio la posibilidad de establecer comunicación con otras regiones o lugares, aunque se encuentren separadas por kilómetros de distancia. Con ello la versatilidad, funcionalidad y portabilidad comenzaron a ser posibles y comenzó el desarrollo de dispositivos más pequeños que una computadora personal.

2.2.2 Características de los dispositivos móviles

Para que un dispositivo se considere como móvil debe cumplir con al menos dos características principales las cuales son:

- Portabilidad, los dispositivos son de un tamaño adecuado para poderlos transportar.

- Comunicación inalámbrica, ya sea conexión a internet o conexión de red celular.

En cuanto a las características específicas pueden variar dependiendo del tipo de dispositivo algunos ejemplos son:

- Touchscreen, las pantallas táctiles son una de las características principales y prácticas de los dispositivos móviles hay diferentes tipos de pantallas, por calor, por presión o infrarrojas.

- Sensores, los dispositivos tienen diferentes tipos de sensores entre ellos son los sensores de movimiento, acelerómetro, sensor de luz, sensor de proximidad, sensor magnético, etc.

- Cámaras, las cámaras que están integradas en los dispositivos pueden grabar video y tomar fotos teniendo varias resoluciones y calidad dependiendo de la gama del dispositivo móvil.

- Almacenamiento, la mayoría de los dispositivos ya vienen con memoria interna existen de varias capacidades, pero se puede ampliar la capacidad de almacenamiento dependiendo de las necesidades.

2.3 Origen y evolución de las redes sociales

Este capítulo se enfoca en el origen y evolución de las redes sociales, incluye también Big data y Nube que son ligados de forma importante a las redes sociales mostrando sus ventajas y desventajas, se aborda la teoría de los seis grados.

2.3.1 Historia de redes sociales

En 1995 se crea la primera red social, el propósito de éste sitio web llamado “classmates” era el ponerse o recuperar el contacto con compañeros de la escuela o de la universidad, esto se logra gracias a que en ese entonces estaba el concepto de web 2.0 que fomentaba la comunicación y se adaptaba al usuario.

La teoría que inspiro las redes sociales fue la de seis grados de separación que habla de que todos estamos conectados.

Los círculos de amigos, como se les llamaba en 2002 a las redes sociales, empiezan a ser populares la manera en que se propagaron las redes sociales era invitando a los amigos a unirse, que a su vez invitaban a más amigos y así sucesivamente comenzando a destacar varias páginas como MySpace o Xing, se empieza a abrir un nuevo mercado para las compañías en internet y empiezan a lanzar sus propias páginas de redes sociales como Orkut en 2004 de Google ofreciendo perfiles visibles para los demás, actualización de la libreta de contactos entre otras.
En 2004 se lanza Facebook en la universidad de Harvard, que como un principio era solo para los estudiantes, en 2006 nace Twitter como una red de microblogging que a la fecha son las principales y más usadas redes sociales.

2.3.2 Teoría de los seis grados

Ésta teoría surge en 1929, como una propuesta del húngaro Frigyes Karinthy; pero no es hasta 1967 cuando un sociólogo (Stanley Milgram) desarrolla un experimento para poder probar dicha teoría.

Éste experimento consistió en elegir al azar ciudadanos americanos con el fin de entregar un envío a un desconocido, a miles de kilómetros de distancia. La única información con la que contaban para la entrega era: el nombre, la ubicación genérica ya que no había direcciones concretas y la ocupación del destinatario. Con ésta información el objetivo era entregar a quien ellos creyeran que podía estar ligado al destinatario, siempre que se cumpliera la condición de tratarse de personas que conocían directamente. Esto continuaría como una cadena hasta que el destinatario fuera alcanzado.

Como conclusión se llegó a que solo se necesitaron entre cinco y siete intermediarios para que el envío llegara a su destino.

En el año 2001, la Universidad de Columbia continuó el experimento de Milgram, pero ahora usando internet y tras varias pruebas se encontró que el número de pasos promedio era seis **(Watts, 2006)**.

Actualmente, toda red social se fundamenta en la teoría de los seis grados de separación. No obstante, un estudio de la Universidad de Milán ha permitido comprobar que Facebook permite variar el número de grados necesarios para conectar a los usuarios. Los investigadores de Milán han descubierto que la propuesta de Frigyes Karinthy no solo se cumple, sino que se reduce, ya que los datos presentados aseguran que en 2008 eran necesarios 5,28 grados, mientras que en 2011 eran necesarios 4,7.

En el año 2011 la red social Facebook publicó los datos de su estudio "Anatomy of Facebook" en su blog, confirmando que la red social permite la conexión de dos personas de cualquier parte del mundo en menos pasos de los que se esperaba, «Hemos encontrado que la teoría de los seis grados en realidad exagera el número de enlaces entre los usuarios. El 99,6% de las parejas de usuarios analizados están conectados por 5 grados y el 92% lo hace a través de 4 grados» **(Curiosidades Históricas, 2015)**.

2.3.3 Big data y Nube

Big data se trata de un concepto del que escuchamos constantemente a nuestro al rededor y que consiste en la administración y análisis de grandes cantidades de datos que no pueden ser tratados y procesados de manera convencional debido a que superan los límites de las herramientas que se usan comúnmente para almacenar y procesar datos ya que se trata de grandes volúmenes de información generalmente no estructurada, pero de gran valor para cualquier clase de negocio. El concepto de big data no solo incluye la información, sino que engloba toda la infraestructura, tecnología y servicios que se han desarrollado especialmente para el manejo y procesamiento de esta inmensa cantidad de datos que pueden ser estructurados, no estructurados o semiestructurados como lo son los mensajes de redes sociales, audio, video, correos electrónicos, datos de encuestas, etc.

Un claro ejemplo del uso de big data es el análisis de datos generados por redes sociales, en Twitter son cerca de 12 Terabytes de tweets creados diariamente y Facebook almacena alrededor de 100 Petabytes de fotos y videos, dicha información requiere de ciertos métodos para poder ser procesados y analizados de forma rápida. Otros ejemplos son el almacenamiento de ubicaciones geográficas, transacciones financieras, comportamientos de compras, sitios de internet visitados y muchas más actividades que son realizadas a diario por medio de dispositivos móviles como teléfonos inteligentes y tabletas. **(Barranco, Ricardo. 2012)**

Nube o "cloud computing", se trata del acceso remoto a herramientas, aplicaciones, sistemas e información a través de internet, así como la prestación de servicios sin necesidad de tener la infraestructura y los recursos físicamente en el lugar donde nos encontramos o se encuentra la empresa, los datos y recursos de procesamiento y almacenamiento se encuentran ubicados físicamente en algún centro de datos al que podemos acceder desde cualquier dispositivo móvil o fijo ubicado en cualquier parte del mundo con el simple hecho de contar con conexión a internet, teniendo así disponibilidad de los datos en cualquier momento y en cualquier lugar. Como usuarios finales tenemos acceso a una infinidad de servicios en la nube a diario, como por ejemplo

Facebook, Gmail, Google drive, YouTube, Dropbox son servicios en la nube a los que tenemos acceso en cualquier momento y lugar desde cualquier computadora, tableta o teléfono inteligente.

Gartner Inc., empresa consultora y de investigación de las tecnologías de la información en el año 2013 enlistó dentro de los 10 mejores proveedores de servicios en la nube a: Amazon Web Services, AT&T, Google Cloud Storage, HP, IBM, Internap, Microsoft, Nivanix, Rackspace y Softlayer **(Butler, 2013)**.

Ventajas del uso de servicios en la nube

- Es probable que los estándares de seguridad con los que cuenta el proveedor del servicio en la nube sean más altos que con los que una empresa pequeña o mediana puede contar propiamente, sobre todo si el proveedor cuenta con el cumplimiento de normas ISO y otras prácticas de seguridad.
- Debido a que el proveedor está especializado en el servicio, lo más probable es que cuente con una infraestructura y recursos financieros mejores que los de la empresa pequeña o mediana, lo que representa una menor inversión y mantenimiento de recursos.
- El proveedor del servicio es el encargado y responsable de mantener los datos almacenados, seguros y disponibles según lo acordado.
- Los datos están disponibles incluso cuando existe perdida del equipo personal.
- Se puede acceder a los datos desde cualquier lugar y en cualquier momento siempre y cuando se cuente con una conexión a internet.

Desventajas del uso de servicios en la nube

- Si la conexión a internet es inestable, se pueden tener dificultades para acceder a los servicios de nube **(DELL, 2012)**.
- Existe desconfianza por el hecho de que un tercero completamente ajeno a la empresa sea el encargado de almacenar la información sensible del negocio.
- El cliente se vuelve dependiente tanto de la compañía proveedora del servicio como de su propia conexión a internet, ya que si alguna de estas dos llega a fallar la continuidad del negocio se verá afectada.
- En caso de que el proveedor por alguna situación tenga problemas para brindar el servicio, no hay nada que el cliente pueda hacer hasta que el servicio se restablezca.

- Miedo a la pérdida de datos.

Capítulo III. Planteamiento del problema

A lo largo de este capítulo se explica y desarrolla el problema de falta de conciencia que rodea a los usuarios en edad infantil que tienen acceso a las redes sociales y los dispositivos móviles, se muestra mediante algunas estadísticas de diversos países la gravedad del problema y la urgencia por dar a conocer una serie de consejos hacía los padres y hacía sus hijos para el mejor uso de las tecnologías antes mencionadas.

3.1 Uso de dispositivos móviles y redes sociales

La cultura actual sobre el manejo de dispositivos móviles y redes sociales es un punto importante y decisivo para el desarrollo de esta tesis, el acercamiento de la población infantil a las tecnologías móviles, vulnerabilidades de los dispositivos móviles y los riesgos de utilizar dispositivos móviles y redes sociales a temprana edad.

3.1.1 Cultura actual sobre el manejo de dispositivos móviles y redes sociales

Las redes sociales actualmente las usamos como estructuras compuestas por personas conectadas por uno o varios tipos de relaciones (de amistad, de parentesco, de trabajo, ideológicas) con intereses comunes. Las redes sociales en Internet tienen mecanismos muy específicos de funcionamiento. Suelen comenzar por invitaciones enviadas por amigos, al suscribirse el usuario diseña su “perfil” con información personal, invita a otros amigos, se tiene la posibilidad de subir fotos, comentar el estado de ánimo de los demás, expresar nuestros propios pensamientos, subir enlaces, interactuar con los conocidos conectados en ese momento, etc.

No son sólo una moda adolescente. Están cambiando nuestra realidad social y revolucionarán la economía y el mundo del trabajo, más de lo que lo hizo Internet en toda su historia hasta nuestros días. Empresas, organizaciones civiles, instituciones académicas, gobiernos y en general todas las organizaciones humanas, son de hecho redes sociales. Y su relevancia se mide muchas veces por la capacidad que tienen de crecer su red, o de asociarse con otras redes sociales. Mucho antes de la aparición de Internet en nuestra vida cotidiana, nuestra capacidad de vincularnos con otros, o de revivir vínculos anteriores, era ya un diferenciador importante, por ejemplo, para individuos buscando trabajo, empresas fidelizando o recuperando clientes, instituciones educativas incrementando su acervo intelectual y humano, o campañas políticas asegurando el apoyo ciudadano. El poder de las nuevas tecnologías está revolucionando también la interacción social con fines profesionales y de negocio.

Algunos estudios han demostrado que el uso excesivo de las redes sociales puede generar conductas adictivas hacia éstas y promover aspectos negativos como el bullying, el cibersexo, el robo de información y de identidades, entre otros **(Islas y Ricaurte, 2013)**.

En los últimos años ha habido un incremento en el manejo de internet, el cual ha cobrado una gran importancia pues permea todas nuestras actividades cotidianas. Redes sociales como Facebook, Twitter y LinkedIn, entre otras, son medios de comunicación que han condicionado la forma de interactuar entre los seres humanos; 301 minutos es el tiempo promedio de conexión al día a internet, y el uso de redes sociales es la tercera actividad más frecuente de los internautas mexicanos.

Una persona que dedica mucho tiempo al uso de las redes sociales e internet puede vivir una adicción, en particular si el usuario es muy pequeño y aún no sabe de responsabilidades puede tender más a desarrollar una adicción que se refleje en comportamientos violentos cuando se le retira el dispositivo móvil, bajas calificaciones y déficit de atención.

3.1.2 El acercamiento de la población infantil a las tecnologías móviles

Desde temprana edad los niños tienen contacto directo con la tecnología pueden controlar casi cualquier aparato que se les ponga en las manos, usualmente el primer contacto lo tienen con algún dispositivo móvil, el cual es proporcionado directamente por la familia para el entretenimiento del menor.

Los niños aprenden a una velocidad increíble por lo que es importante guiarlos acerca del uso de las tecnologías ya que la mayoría tienen acceso o contacto con los teléfonos inteligentes, tabletas o laptops, ya sea para entretenimiento, aprendizaje o por el simple hecho de seguir el ejemplo de los adultos.

Con una buena orientación se puede sacar provecho a las tecnologías móviles, ya que al ser de un uso intuitivo los menores fácilmente los pueden manejar y a la vez aprender, en las escuelas de México se han integrado las tabletas como un dispositivo de aprendizaje, pero si no se tiene un control adecuado, puede llegar a convertirse en una desventaja más que en un beneficio.

En México en el 2013 el 80% de los hogares ya contaban con teléfono celular, en España un estudio realizado en 2015 por el Instituto Nacional de Estadística (INE) arroja que el 29.7% de los niños de 10 años poseen un teléfono celular, con estos números se puede generar una idea de que tan importante es la supervisión de los adultos con respecto a las tecnologías ya que cada año se

aumenta la cantidad de menores con dispositivos móviles propios y por lo tanto también aumentan los riesgos que estos pueden conllevar.

3.1.3 Aprendizaje y dispositivos móviles

A partir de la aparición de las computadoras, y posteriormente del internet, se ha evolucionado hasta el punto en que los niños que nacen en esta época están nativamente emergidos en el mundo de la tecnología, no es raro para ninguno de ellos la existencia de los dispositivos móviles.

Debido a esta evolución, las formas de enseñanza también van cambiando adaptándose a las nuevas formas en que se puede transmitir el conocimiento a través de imágenes, audio, videos, juegos y una cantidad ilimitada de herramientas con fines educativos orientados a diferentes edades que se pueden utilizar desde dispositivos móviles ya sea con o sin conexión a internet.

Los dispositivos móviles sin duda tienen beneficios para la educación y el aprendizaje del niño, pero también es cierto que el uso inadecuado de ellos implica riesgos. El uso de las nuevas tecnologías no presenta ningún indicio de alarma si el uso que se hace de ellas no interfiere en las actividades y obligaciones del menor, no es un peligro si es controlado y está equilibrado con el resto de actividades.

Luz María Castañeda de León en su estudio “Tecnología en la Educación: Dispositivos móviles” advierte que en la actualidad la mayoría de los proyectos de educación que utilizan como apoyo el uso de alguna tecnología móvil requiere de una experiencia mayor por parte del profesor, por lo que se debe buscar la forma en que puedan potenciar sus aptitudes mediante capacitación. Así mismo, menciona 2 razones específicas por las que sí incorporar el uso de tecnologías móviles para impulsar la educación, a continuación, se hace referencia a dichas razones:

- Contenidos educativos en Internet: Ayudan a despertar el interés de los estudiantes en temas específicos.
- Dispositivos móviles y plataformas tecnológicas: Proporcionan a los docentes herramientas didácticas fáciles de usar al contar con elementos multimedia, de tal forma que los profesores puedan utilizarlos para establecer vínculos de cercanía y apropiación del conocimiento que corresponda a los planes de estudio (Castañeda de León, 2013).

En México, a partir de junio del año 2014 se comenzó con una distribución de tabletas que forma parte del Programa de Inclusión y Alfabetización Digital, para que los sectores más desfavorecidos

de la población se incorporen a la cultura digital. Con esa iniciativa se proyecta que hacia 2018 todos los niños de quinto y sexto grados de educación primaria del país cuenten con una tableta que puedan utilizar con fines educativos.

Las tabletas fueron precargadas con dos bloques de contenido, el primero con temas de alimentación saludable, convivencia, economía familiar, salud, prevención ante desastres naturales, uso seguro de tecnología, y cuidado de datos y seguridad personal.

El segundo, orientado a jóvenes, incluye temas curriculares organizados por asignatura y bloque didáctico, una biblioteca digital, diccionario escolar y fonoteca digital, así como diversos tipos de software.

Aunque la principal idea fue hacer una inclusión digital y apoyar a una mejor educación, no está muy claro ni bien definidos los objetivos y las estrategias para lograr que la educación sea mejor.

Es por esto que todavía no se tiene un estudio con resultados que demuestren la verdadera utilidad de dichos dispositivos al menos en los estudiantes a quienes se les ha proporcionado esta herramienta.

De acuerdo con Martínez, M. (2007), “a la intersección de la educación en línea y los dispositivos computacionales móviles se le conoce como “aprendizaje móvil” (en inglés, m Learning o mobile learning). Las ventajas que ofrece es que promete el acceso frecuente e integral a las aplicaciones de software que apoyan el aprendizaje “en cualquier momento y en cualquier lugar”. Dicho de otra forma, el aprendizaje móvil puede ser visto como la utilización de dispositivos móviles en el proceso de aprendizaje. El m-Learning se refiere a los ambientes de aprendizaje basados en la tecnología móvil, destinados a mejorar e impulsar los procesos de enseñanza y aprendizaje. En el e-Learning, “el término distancia implica un cambio geográfico entre donde residen los contenidos y el lugar en el que se toman, manteniendo siempre una conexión física entre ellos. En cambio, en el m-Learning el término distancia implica que la recuperación o el acceso al contenido puede hacerse en movimiento, sin importar el lugar y obteniendo un mayor provecho del tiempo disponible”

Debe hacerse poniendo un gran peso en el usuario y, más que desarrollar aplicaciones monolíticas, deben diseñarse herramientas poderosas que permitan a los expertos (como tutores o profesores) adaptar esta tecnología a sus necesidades. Por otro lado, existe una gran variedad de dispositivos móviles en el mercado, por lo que es importante hacer la clasificación correspondiente para identificar los que los usuarios utilizan.

Por otra parte, también existen opiniones sobre las desventajas que representa el uso de tecnologías móviles para la educación. El catedrático de Ciencias Políticas y Sociales de la Universitat Pompeu Fabra, Francesc Pedró discute las ventajas de la tecnología en aula, siempre que se use con sentido, “más tecnología no es igual a mejores resultados porque el tema es qué tipo de pedagogía estamos utilizando. Si utilizas la herramienta mal, puedes causar más daño que beneficio”.

Sostiene que muchos sectores son reticentes al uso de la tecnología, en primer lugar, “con el argumento de la protección del niño, los que consideran que abrir la puerta a Internet es dejarle huérfano en un contexto con peligros”.

Asimismo, hay quienes se oponen por miedo a la “pérdida de conexión con el soporte tradicional de la cultura”, y finalmente por el hecho de que pueda generarse una “pérdida de autoridad del profesor, con el argumento de que se da poder al alumno, que tiene acceso a todo con su tableta”. (Francesc, 2015).

A continuación se mencionan algunas de las desventajas que representa el uso de los móviles en la educación si no se hace de una forma adecuada siguiendo objetivos y estrategias.

- Divergencia de acceso a la tecnología. No siempre todo el alumnado puede realizar todas las actividades bien porque no poseen teléfono, no disponga de la tecnología necesaria. Con todo, esto puede trabajarse realizando usos que no dependan del dispositivo, sino de la acción en sí.

- Normativa diversa a nivel estatal, regional y de centro. Actualmente no existe una normativa igualitaria en todo el Estado, ni dentro de una misma comunidad autónoma y, ni siquiera, entre centros de una misma ciudad. Por ello, es un reto el uso o no de estos dispositivos ya que puede vulnerar normativas concretas y que cada docente deberá tener en cuenta.

- Proceso de adaptación. Es importante marcar normas de uso del smartphone para todas las personas del colegio, también los adultos, e incluso hacer partícipes a los y las estudiantes en su redacción.

- Uso inadecuado del móvil. En ocasiones el uso del móvil puede conllevar acciones negativas hacia otras personas como ciberbullying o ciberacoso, publicaciones

negativas sobre docentes en redes sociales, etc., si bien esto no es consecuencia del uso en el aula, sino del uso de manera genérica, cosa que utilizando el móvil en el aula se podría trabajar en grupo.

- Falta de objetivos pedagógicos. Quizá uno de los mayores retos como docentes es la introducción de una nueva herramienta con un sentido, es decir, dentro de una programación y de una metodología. Es necesario entender que el móvil no es la salvación de nuestros alumnos, sino una herramienta más de trabajo. (Proyecta, 2015)

3.1.4 Vulnerabilidades de los dispositivos móviles

Debido a que en los últimos años se ofrecen dispositivos móviles con mayores capacidades y funcionalidades, las personas han incrementado el uso de éstos por comodidad y movilidad; teniendo plena confianza en guardar información sensible como por ejemplo el historial de conversaciones en la mensajería instantánea, calendarios, direcciones, fotos, redes sociales, entre otras aplicaciones contenidas en los dispositivos. Esto provoca que estén expuestos a amenazas y vulnerabilidades que ponen en riesgo la seguridad del dispositivo como de la información contenida en él.

Algunos ejemplos de vulnerabilidades en los dispositivos móviles son:

- Acceso físico a un dispositivo móvil por parte de un intruso.
- Uso fuera de casa u oficina, ya que puede ser robado o extraviado.
- Falta de actualización de software.
- Instalación de software desconocido que pueda tener acceso a la información contenido en el dispositivo.
- Aplicaciones basadas en la localización, ya que permiten obtener la ubicación física del usuario en cualquier lugar del mundo.
- Los dispositivos móviles están expuestos a través de las redes inalámbricas Wifi al conectarse en redes públicas y abiertas, ya que tienen un nivel de seguridad reducido o inexistente.

Con la aparición de nuevas plataformas tecnológicas móviles, nuevas aplicaciones, nuevos servicios, así como su conexión a través de redes de comunicaciones públicas y privadas, se abre

la puerta a novedosas investigaciones de seguridad centradas en el descubrimiento de vulnerabilidades en estos nuevos entornos.

3.1.5 Riesgos de utilizar dispositivos móviles y redes sociales a temprana edad

Se conoce como riesgo a la probabilidad de que una vulnerabilidad sea atacada por una amenaza causando un daño, una situación negativa, un peligro. En el capítulo 2 se definieron los conceptos de “dispositivos móviles” y “redes sociales” por lo que a continuación se mencionan los riesgos más comunes a los que se exponen los niños y niñas al usar estos medios a temprana edad.

- Desarrollo de problemas de atención.
- Compras en línea sin consentimiento.
- Contacto con personas malintencionadas que quieran extraer información personal para dañar al menor y a las personas cercanas a él.
- Robo del equipo con o sin violencia.
- Explotación sexual infantil.
- Fácil acceso a contenido violento, contenido sexual, promoción de autolesiones, violencia, racismo contra otras personas.
- Contacto inapropiado con terceras personas que quieran abusar de la inconsciencia del menor.
- Ciberacoso o ciberbullying.
- Sexting. Intercambio de mensajes con contenido sexual, ya sea por medio de palabras, imágenes, fotos o videos, etc.
- Grooming. Mediante engaño atraer al niño o niña con fines sexuales.
- Adicción y dependencia al móvil.
- Publicación de imágenes, fotos o videos que dañen a terceras personas.
- Se carece de control de información.
- Violación de derecho a la intimidad.
- Sufrir hacking.
- Prostitución de menores.

Se debe tener muy claro que cualquier cosa una vez puesta en internet es difícil si no es que imposible eliminarla, por lo que siempre antes de poner cualquier contenido personal se debe pensar si lo que estamos enviando o compartiendo no puede ser utilizado en nuestra contra, o en la contra de otra persona.

3.2 Estadísticas sobre el uso de dispositivos móviles y redes sociales en México y otras regiones del mundo

En esta sección se muestran estadísticas sobre la cantidad de niños que utilizan o tienen un dispositivo móvil propio, así como los principales usos que le dan ya sea cuando cuentan o no con una conexión a internet. Los países a revisar son: México, España, Chile, Colombia, Argentina y Brasil.

3.2.1 México

En esta sección se presentan los resultados obtenidos a partir de la investigación de campo realizada por el equipo de trabajo que tiene el objetivo de mostrar los hábitos que tienen los menores respecto al uso de los dispositivos móviles y redes sociales, y a la supervisión realizada por sus padres. Esta información corresponde a los resultados del cuestionario que se incluye en el Anexo 1 aplicado a una muestra de 100 niños y niñas de entre 5 y 10 años que utilizan dispositivos móviles y habitan en la Ciudad de México y área metropolitana.

Se muestran las gráficas de los temas de más incumbencia para la realización del plan de concientización.

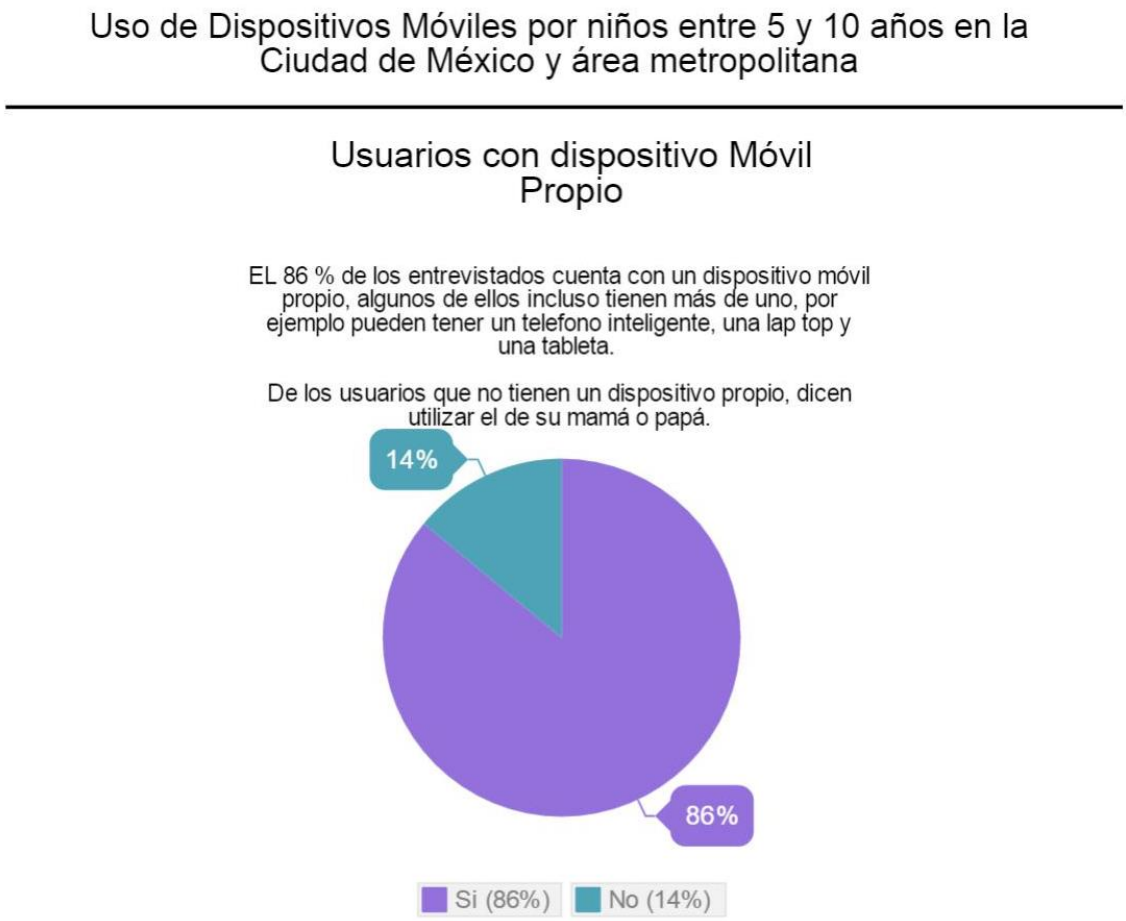


Figura 3.1 Usuarios con dispositivo móvil propio.

En la figura 3.1 se observa que de los niños y niñas encuestados un 86% acepta tener un dispositivo móvil propio (lap-top, teléfono inteligente o tableta). El otro 14% que no cuenta con un equipo propio, indica que el que utiliza le pertenece a mamá o a papá. Como se puede ver, es un alto porcentaje de menores con un dispositivo propio.

En la figura 3.2 se muestra una gráfica con el equipo móvil que cuentan los menores encuestados, el dispositivo que más niños tienen es el teléfono inteligente con un 58%, seguido de las tabletas con un 32% y al final con una computadora portátil con tan solo un 10%. En la información recabada también se aprecia que un 14% tiene los 3 dispositivos mencionados.

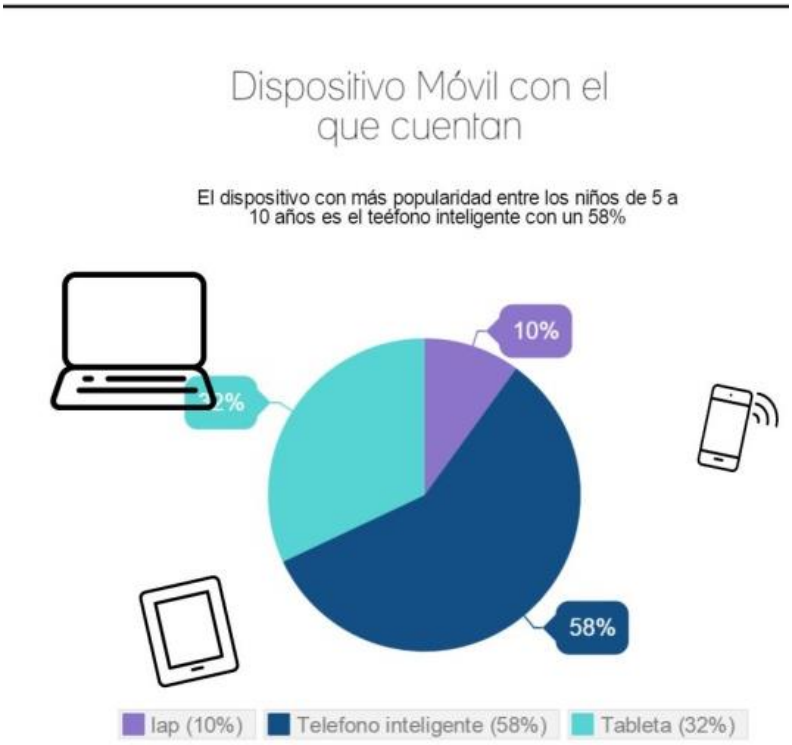


Figura 3.2 Dispositivo con el que cuentan.

Otra información importante es el uso que le dan al dispositivo móvil, como se ve en la figura 3.3 el principal uso es el del entretenimiento (música, videos, ver imágenes), seguido por el de educación (hacer tareas), el uso de redes sociales un 11% y al final la comunicación por medio de llamadas telefónicas y mensajes SMS, ya que este tipo de comunicación ha sido reemplazada por aplicaciones de mensajería instantánea como WhatsApp.

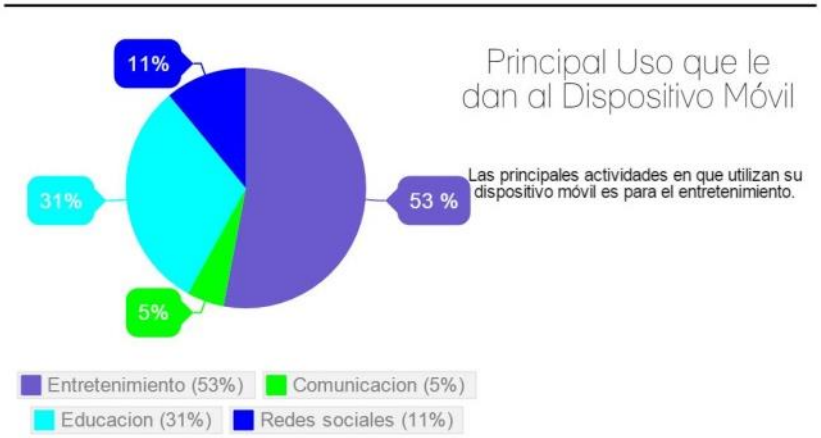


Figura 3.3 Principales usos del dispositivo móvil.

De la mano del uso que le dan al dispositivo móvil, se muestra en la figura 3.4 las aplicaciones más conocidas por este segmento de usuarios.

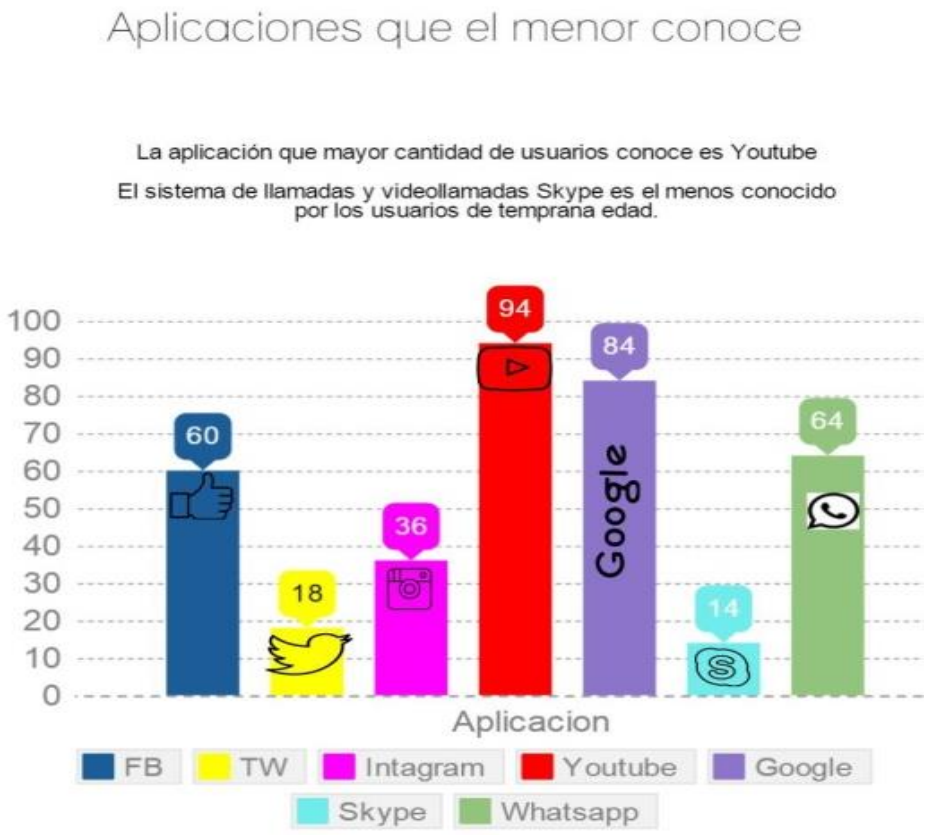


Figura 3.4 Aplicaciones conocidas por el menor.

En correspondencia con el uso que les dan a los móviles, se aprecia que YouTube que es una aplicación para el entretenimiento mediante la reproducción de video y música es conocida y utilizada por el 94% de los encuestados. También en correspondencia se encuentra el buscador de Google se encuentra en segundo lugar como una herramienta de educación para realizar tareas utilizada por el 84%. Otra de las aplicaciones que son reconocidas por más de la mitad de los encuestados es la red social Facebook y la aplicación de mensajería instantánea WhatsApp. En último lugar, conocida tan solo por 14 de los encuestados, se encuentra la aplicación de llamadas y video-llamadas Skype.

De todos los diversos usos que le dan al dispositivo móvil, se estima que son pocos los usuarios que dedican más de 5 horas al día utilizando el equipo móvil. En la figura 3.5 se muestra la distribución de tiempo que le dedican los entrevistados al uso diario del dispositivo móvil. Aunque están distribuidos desde menos de 1 hora y hasta más de 5 horas, poco más del 50% se

concentran en un tiempo de uso de menos de 2 horas. En los resultados únicamente apareció un encuestado que acepta tener uso del dispositivo todo el día, incluso en la escuela.

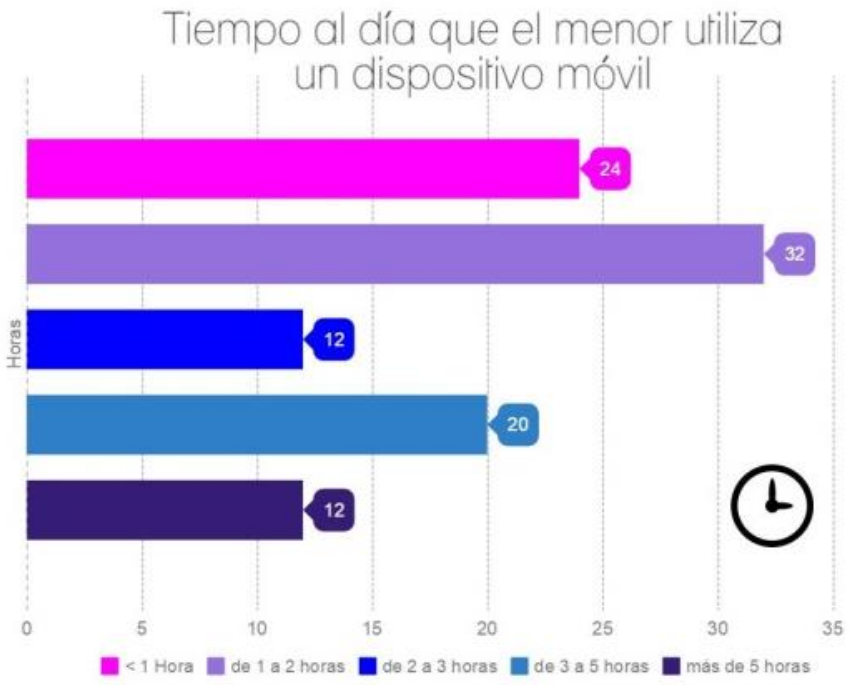


Figura 3.5 Tiempo de uso al día del dispositivo móvil.

Dado que el estudio también abarca el tema particular del uso de redes sociales, en la imagen 3.6 se puede ver que no todos los encuestados tienen registro en alguna red social, sino que el 38% no lo tiene y el 62% si cuenta con una, de este 62% que tiene un registro en al menos una red social, solo el 19% afirma tener entre sus contactos a personas que no conoce en la vida real.

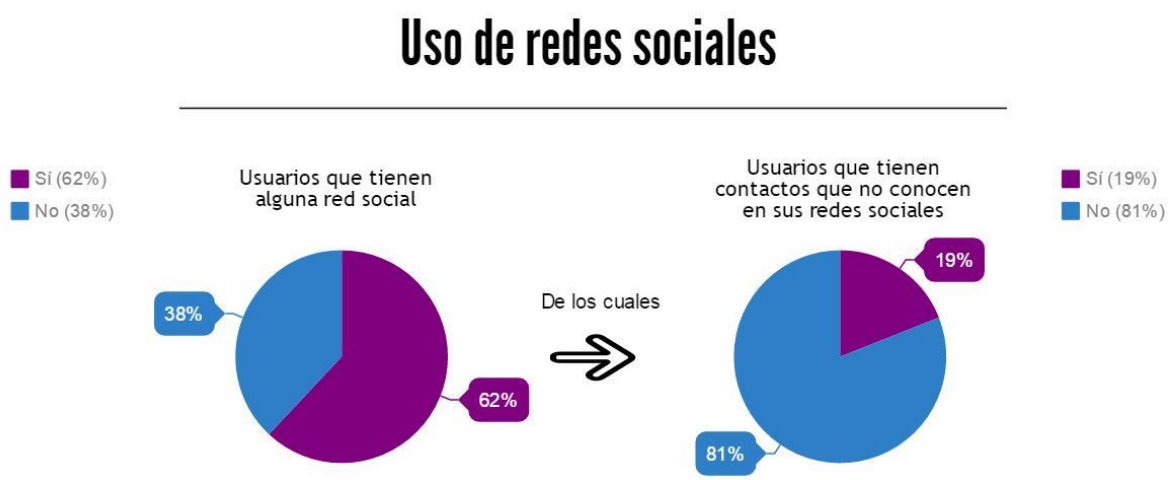


Figura 3.6 Uso de redes sociales.

A pesar de que sí hay usuarios que tienen a personas que no conocen en la vida real, al cuestionarles si alguna de estas ha tenido contacto con ellos y tratado de convencerlos de que se conocieran físicamente quedando de verse en un lugar, todos los encuestados dicen no haber recibido un ofrecimiento como éste, por lo que tampoco han tenido la necesidad de negarse ya que no han tenido el problema.

De los usuarios con registro en alguna red social, el 45% dice que sí comparte algunas o todas sus contraseñas con un familiar de confianza (mamá o abuela) y el otro 55% no lo hace como lo muestra la figura 3.7.

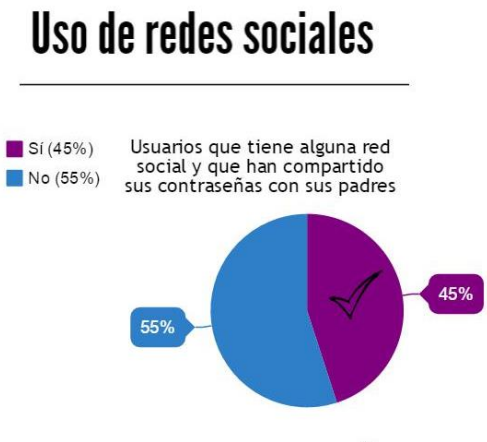


Figura 3.7 Contraseña compartida.

Ya que se conoce la cantidad de encuestados que sí comparte sus contraseñas con sus padres o algún familiar cercano, se analiza cuantos dicen ser supervisados por un adulto mientras hacen uso del dispositivo móvil y sobre todo mientras navegan en internet o chatean. El resultado se describe en la figura 3.8.

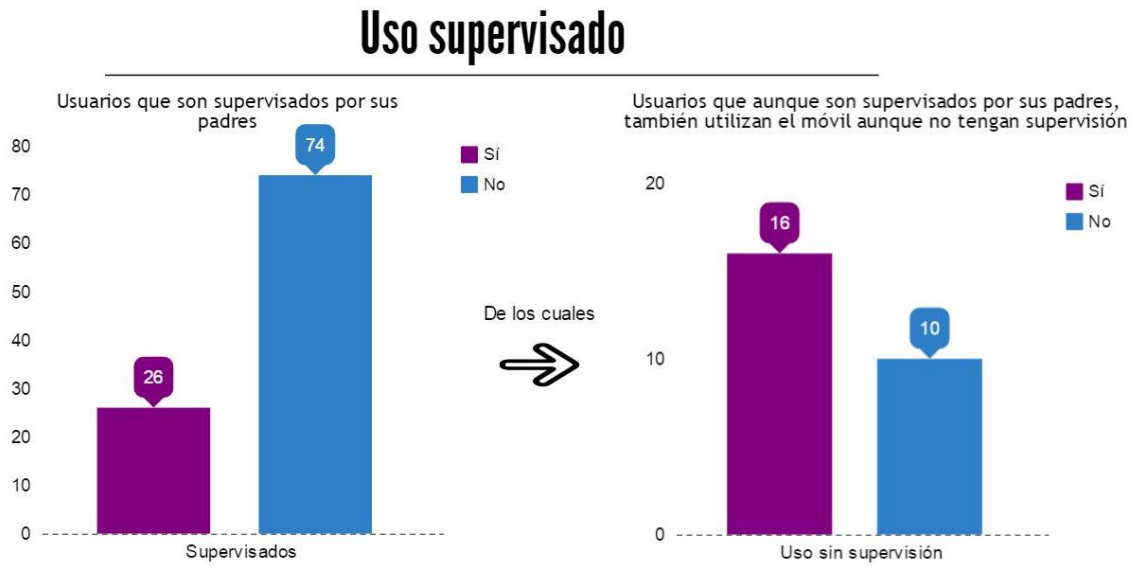


Figura 3.8 Uso supervisado del dispositivo móvil.

74% dice que no es supervisado por un adulto mientras utiliza su dispositivo móvil, durante el análisis de la información se observa que los niños que sí son supervisados por un adulto, son aquellos que pasan menos tiempo utilizando el móvil al día, ya que sus responsables tienen un control sobre su uso. Aun así, de los 26 que asegura si ser supervisado por un adulto, 16 de ellos aceptan que, aunque no haya un adulto supervisando, también utilizan el móvil, dejando solamente a un 10% de menores que al parecer son supervisados todo el tiempo que utilizan un equipo móvil y no lo usan si no tienen autorización.

Otro de los puntos que se les cuestiona a los usuarios en edad infantil es si en algún momento han realizado compras por internet, esta pregunta sirve para estimar que probabilidad de que un menor realice compras sin el consentimiento de un adulto o utilizando sus cuentas almacenadas a lo que un 20% han realizado compras por internet como lo muestra la gráfica 3.9.

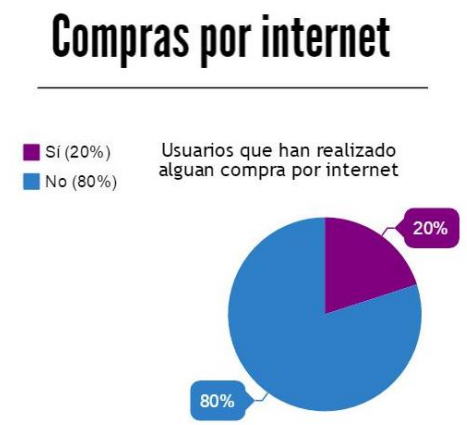


Figura 3.9 Compras por internet.

Finalmente, se interrogó a cada uno de los encuestados si es que conocía recomendaciones para mantener segura su información y su integridad personal, a esta pregunta un poco más de la mitad responde que sí conoce recomendaciones. Las recomendaciones que la mayoría de este 58% conoce son el no hablar con desconocidos, el utilizar contraseñas y el bloquear el dispositivo móvil también mediante alguna contraseña, patrón o pin.

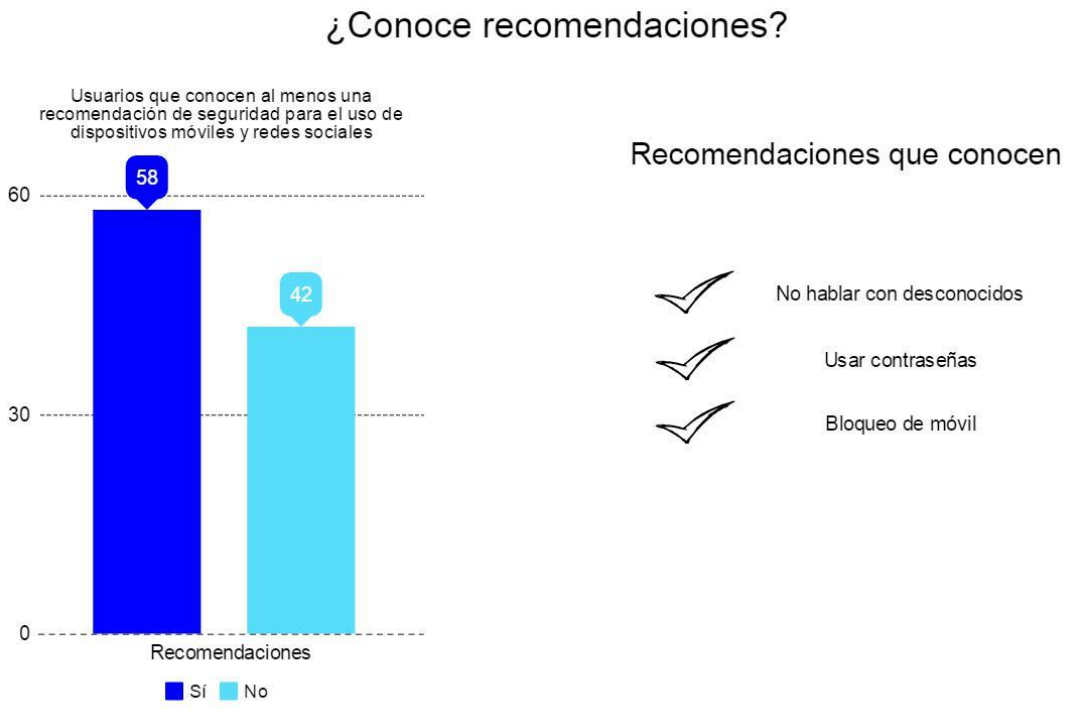


Figura 3.10 Recomendaciones que conoce.

Con esta información se observa claramente que gran parte de la población infantil se encuentra inmersa en el uso de los dispositivos móviles y que en su mayoría conocen lo que son las redes sociales y principalmente utilizan la conexión a internet para ver videos. Como se ha mencionado con anterioridad, el problema no es que hagan uso de la tecnología, si no que no lo hagan de una manera informada, supervisada y responsable para mantener la seguridad propia y de las personas que rodean al menor.

3.2.2 España

En España el estudio “Menores de edad y conectividad móvil en España” realizado por el Centro de Seguridad en Internet “Protégeles” en el año 2013 a una muestra de 1800 niños de entre 11 y 14 años, reveló que el 30% de los niños y niñas españoles de 10 años de edad tienen un teléfono móvil. A los 12 años, casi el 70% ya cuenta con un dispositivo propio y a los 14 años la cifra asciende al 83% de adolescentes con un teléfono móvil.

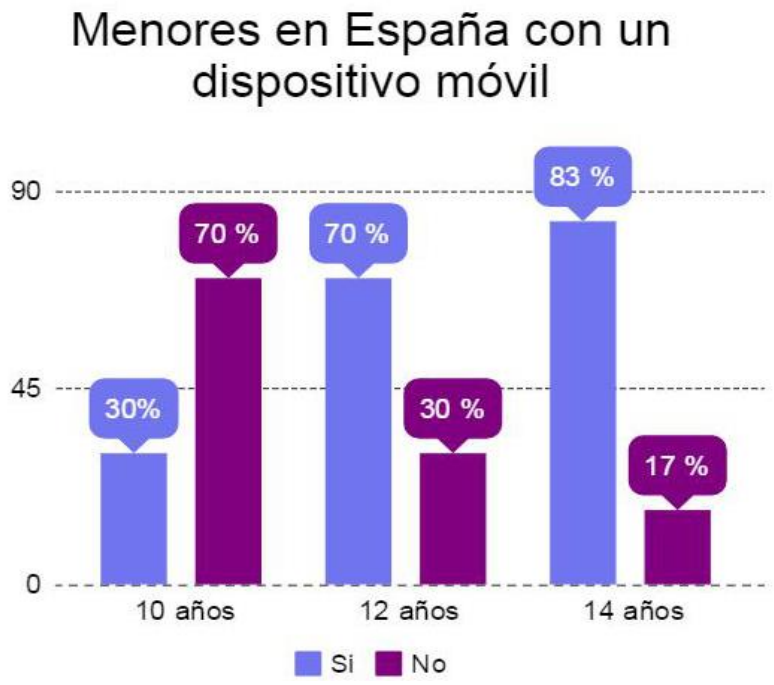


Figura 3.11 Menores en España con un dispositivo móvil.

Del mismo estudio resulta que los juegos, las aplicaciones de TV y YouTube son las aplicaciones con las que los niños se inician en el uso de los teléfonos inteligentes y las tabletas. El estudio también revela que con un aproximado de 2 y 3 años de edad los menores comienzan a utilizar los

dispositivos de sus padres para entretenerse con juegos o capítulos de sus series de televisión favoritas.

Dentro de los principales usos que hacen del dispositivo se encuentran actividades desde ver videos, jugar, buscar información figura 3.13 y publicar fotos y/o video que se representa en la figura 3.12.

El 23% de los menores de 11 a 14 años publica habitualmente fotos y/o vídeos en internet. Otro 33% lo ha hecho en alguna ocasión y un 44% no lo ha hecho nunca.

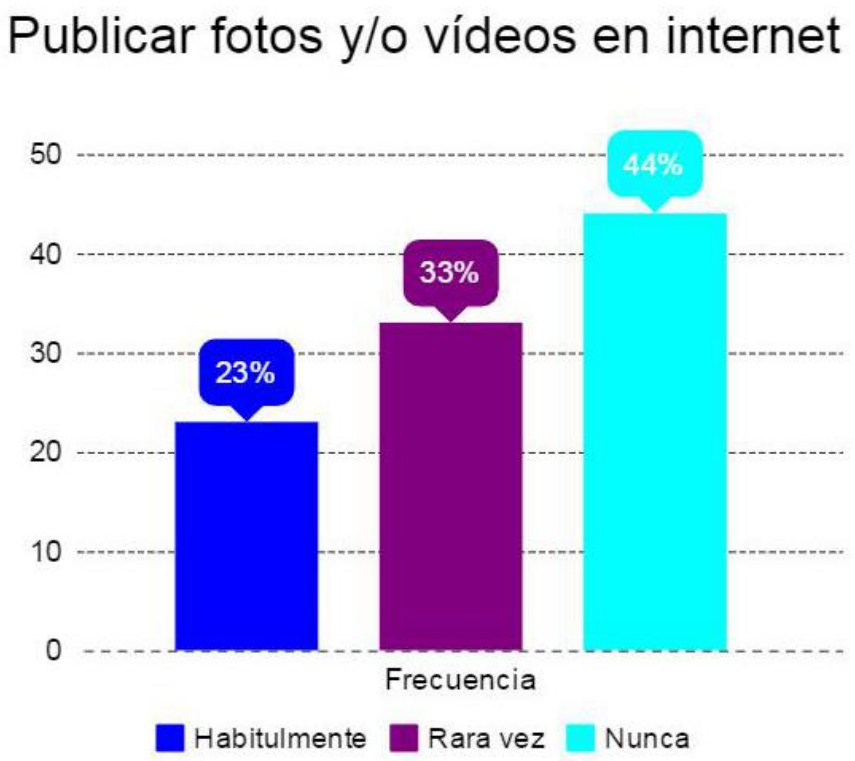


Figura 3.12 Usuarios menores que utilizan su dispositivo móvil para publicar foto y/o video.

El 52,5% de los menores juega habitualmente con sus dispositivos móviles. El 60% navega y busca información a través de internet desde sus Smartphones. Aun un 12% de usuarios menores nunca utilizan está funcionalidad, y otro 27% que sólo lo hace en ocasiones.

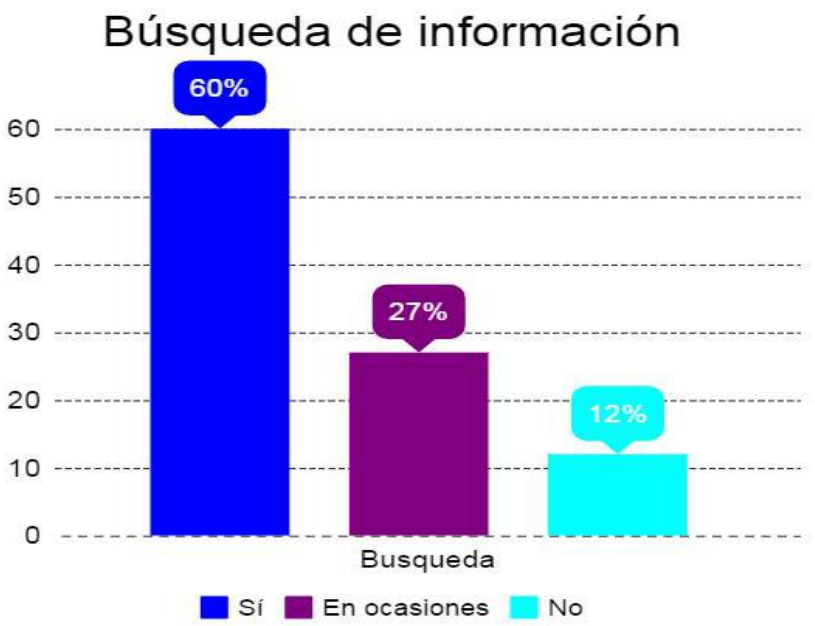


Figura 3.13 Usuarios menores que utilizan su dispositivo móvil para hacer búsquedas de información.

Del mismo modo, el estudio incluye una sección relacionada al uso de redes sociales por los menores, en el que los resultados muestran que El 72% de los usuarios de 11 a 14 años con Smartphone accede a redes sociales a pesar de que en España se fija que la edad mínima para acceder o tener un perfil en alguna red social, es de 14 años.

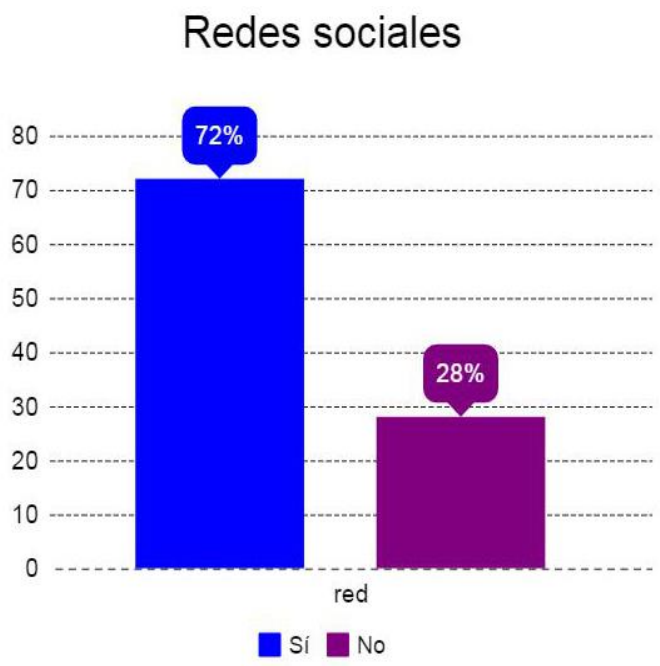


Figura 3.14 Usuarios menores en España que utilizan su dispositivo móvil para acceder a redes sociales.

3.2.3 Chile

Hablando de países del continente americano, según el reciente estudio “Estudio niños y redes sociales” realizado por la empresa chilena de telecomunicaciones VTR Globalcom a 875 padres con hijos de hasta 10 años en mayo del 2015, los principales dispositivos móviles con los que cuentan los menores son el teléfono inteligente, tableta y computadora portátil, siendo estos propios o prestados. En promedio los 5 años la primera vez en que los pequeños tienen un acercamiento con un dispositivo móvil. En la figura 3.15 se muestran los diferentes dispositivos móviles, así como el porcentaje de usuarios que tiene uno propio, un prestad o que no tiene alguno de ellos.

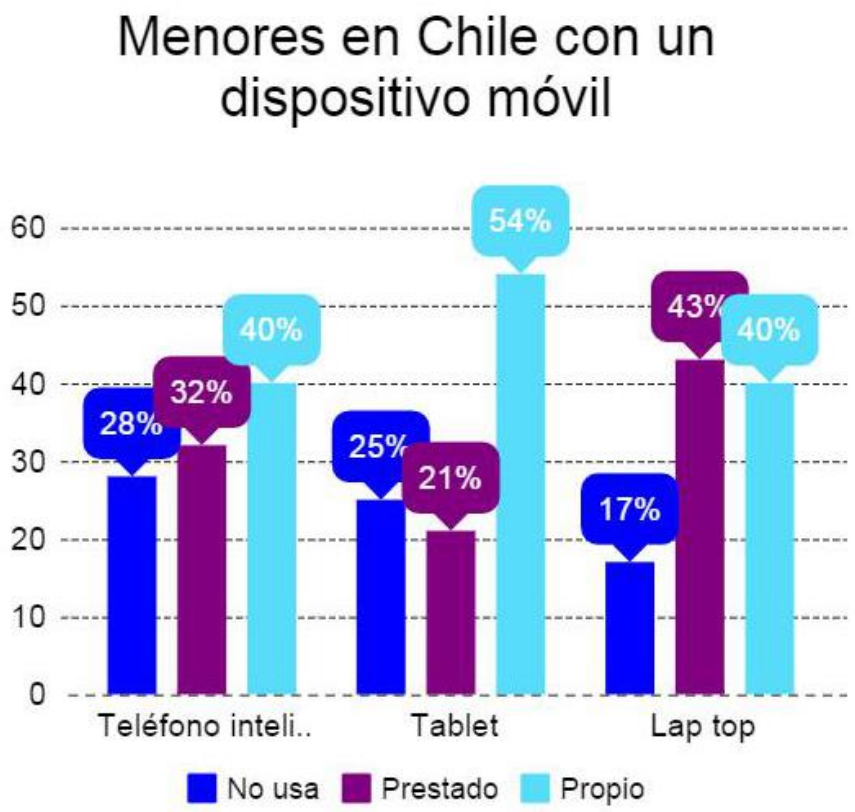


Figura 3.15 Porcentaje de menores en Chile con los diferentes dispositivos móviles.

En cuanto los sitios y aplicaciones más visitadas, la página de videos YouTube lidera en las preferencias de niños de 9 años le sigue Facebook y WhatsApp.

De los encuestados, un 13% dice que el menor no ha tenido acercamiento con las aplicaciones de YouTube, WhatsApp, Facebook y otras aplicaciones que tienen la función de red social.

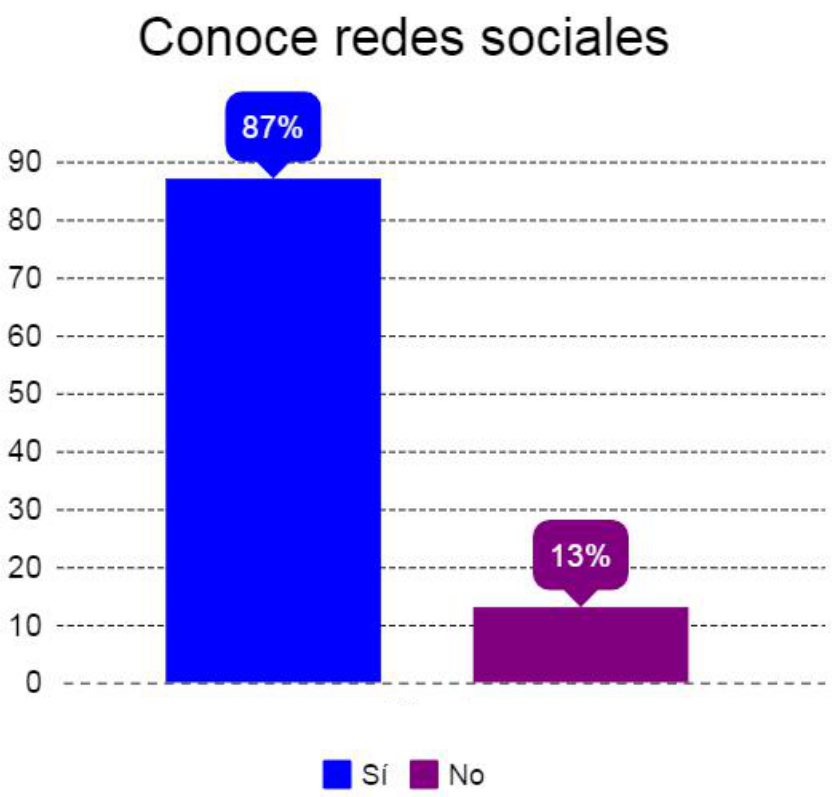


Figura 3.16 Porcentaje de encuestados que conocen redes sociales.

El otro 87% sí conoce estas aplicaciones, YouTube es la aplicación que la mayoría de usuarios menores conoce con un 92%, seguido por WhatsApp con un 42% y en tercer lugar se encuentra Facebook con un 41%, Google+ 29% e Instagram y Twitter con menos del 10%. De los usuarios menores que conocen Facebook un 35% tienen una cuenta.

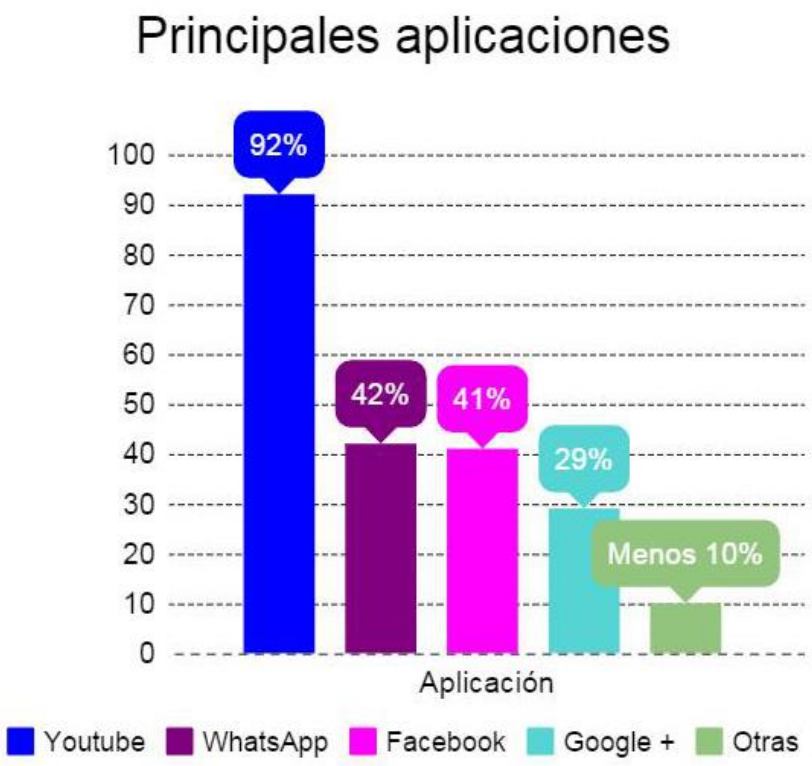


Figura 3.17 Principales aplicaciones conocidas por los menores en Chile.

3.2.4 Colombia

En Colombia, un estudio de la Fundación Telefónica reveló que el 42 por ciento de los niños de 6 a 9 años de edad tiene un celular **(García, José. 2014)**.

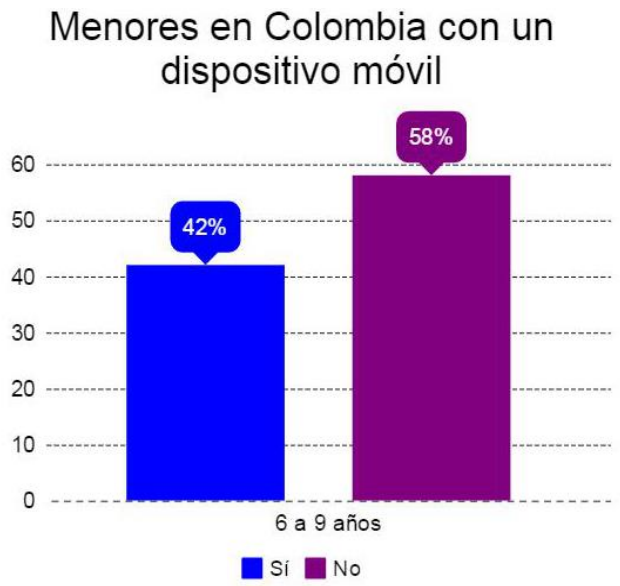


Figura 3.18 Menores en Colombia con un dispositivo móvil.

De la misma forma, el estudio realizado por Arena, empresa perteneciente a la multinacional Havas Media Group, analizó los hábitos en internet de los niños colombianos en dos rangos de edad: 7 a 9 años y 10 a 11 años

Los intereses de los dos grupos de edades son también diferentes. Mientras los más pequeños buscan entretenimiento con juegos online (84%) e información para realizar sus tareas (62%); los niños de 10 a 11 años empiezan a comunicarse más mediante chat y redes sociales.

Figura 3.19 Usos del dispositivo móvil por los menores de Colombia.

En cuanto al uso de redes sociales, un 64% de niños mayores chatea frente al 49% en menores, el uso de redes sociales también les resulta más atractivo a un 48% de los mayores, frente al 35% en menores.

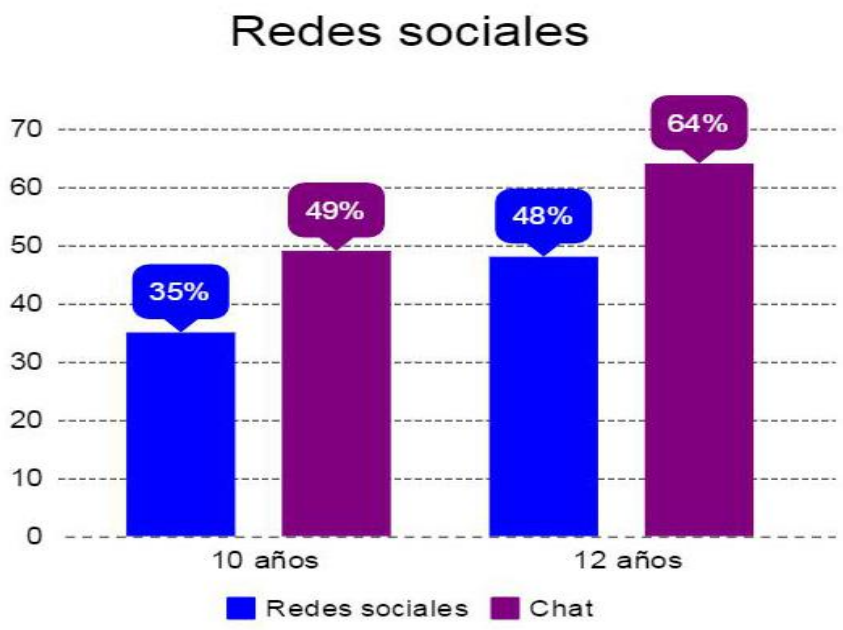


Figura 3.20 Usuarios menores en Colombia que utilizan su dispositivo móvil para acceder a redes sociales.

3.2.5 México, Argentina y Brasil

Ahora se muestran los resultados más relevantes obtenidos por un estudio realizado por La Asociación Civil Chicos.net, con el apoyo de The Walt Disney Company Latin America realizado entre junio y noviembre del 2014, para medir el impacto que tiene la tecnología en la vida de las niñas y niños de Argentina, México y Brasil, fue realizada por la consultora de investigación y tendencias Trendsity, con 1,200 niños de entre 4 y 12 años de edad y sus padres.

Como se ha visto anteriormente, los dispositivos móviles más utilizados son las computadoras portátiles, los teléfonos inteligentes y las tabletas, en Argentina y Brasil la cantidad de computadoras portátiles con los que cuentan los menores es menor que la cantidad en México. Brasil es el líder en uso de teléfonos inteligentes y Argentina es el que menos penetración de tabletas tiene en sus niños. En la figura 3.21 se observa la distribución de los 3 países en cuanto al uso de computadora portátil, teléfono inteligente y tableta, aunque el estudio no recopila la información de si el dispositivo es propio o prestado.

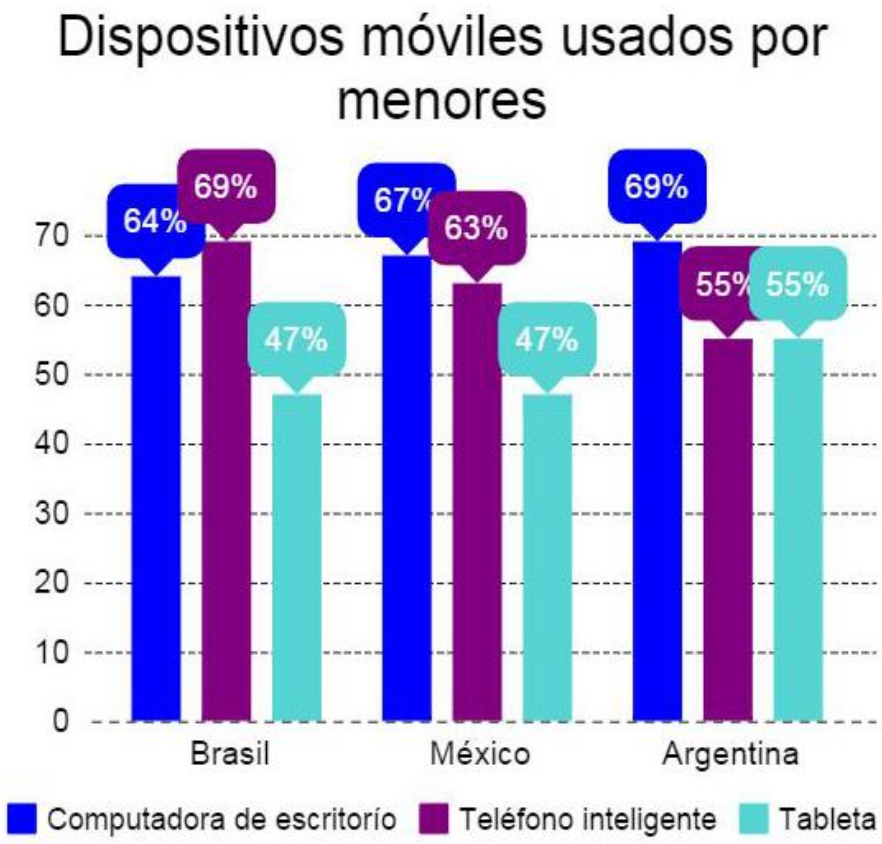


Figura 3.21 Distribución por país de usuarios con dispositivo móvil usado por los menores.

Entre los principales usos que los menores hacen de sus dispositivos móviles conectados a internet está el conectarse con sus amigos, jugar, buscar información para tareas y participar en redes sociales. En la figura 3.22 se muestran los porcentajes para cada una de las actividades mencionadas en Argentina, México y Brasil.

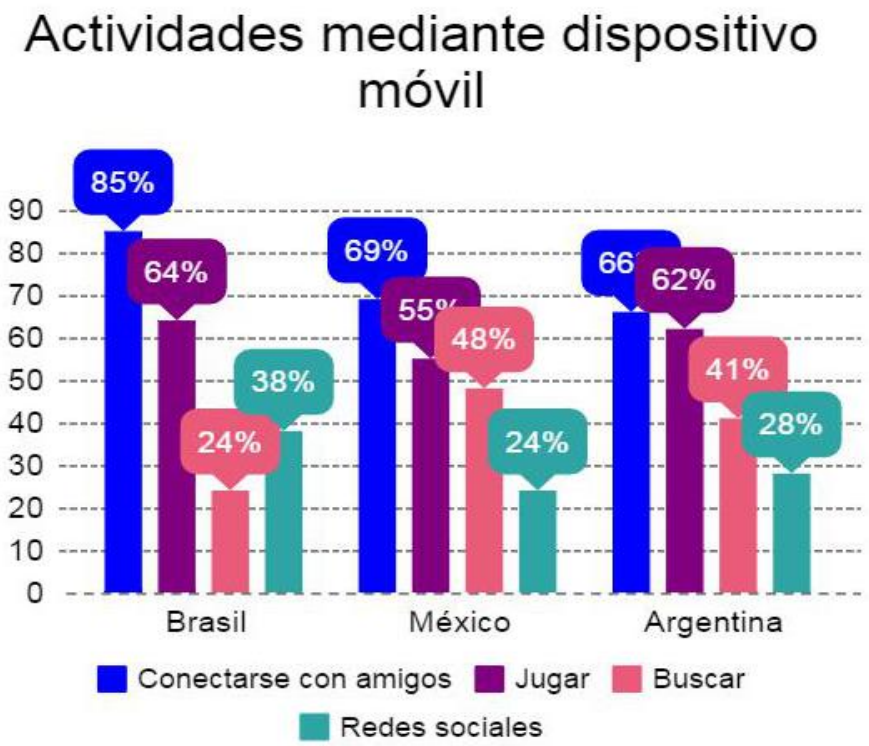


Figura 3.22 Actividades que los menores realizan mediante su dispositivo móvil.

En cuanto al uso de redes sociales, se muestra que la red social favorita para los niños es Facebook: Brasil 89%, Argentina 72% y México 71%. Esto a pesar de que según las políticas de Facebook la edad mínima para abrir un perfil en ella es de 13 años.

En segundo lugar, este YouTube (México 49%, Brasil 48% y Argentina 46%), seguido de Twitter (Brasil: 18%, Argentina: 16% y México 15%) e Instagram, que en Argentina y México tienen 9% y 13% respectivamente, mientas que en Brasil alcanza un 30%, se aprecia en la figura 3.23 adicionalmente, en Instagram hay muchas más niñas que varones con una cuenta.

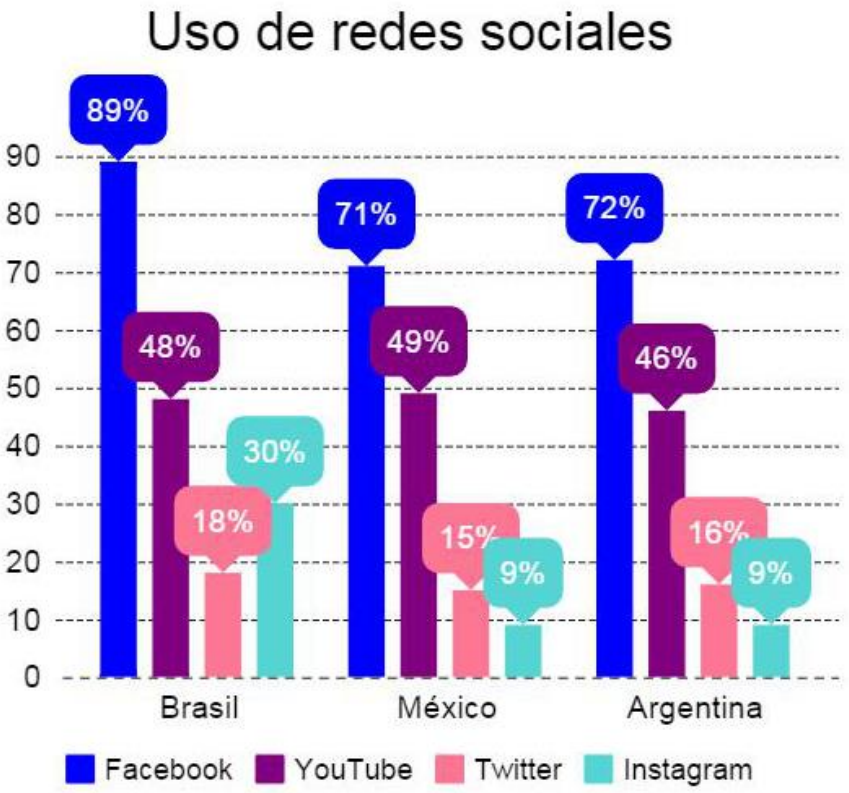


Figura 3.23 Grafica de la comparación de las principales redes sociales en Brasil, México y Argentina.

3.3 Usuarios en edad infantil y el uso de dispositivos móviles e internet en México

De acuerdo a las estadísticas de diferentes países (México, España, Chile, Colombia, Argentina y Brasil) mostradas en los puntos anteriores, se demuestra que el uso de dispositivos móviles en los últimos años ha ido en aumento y que las actividades más realizadas por los usuarios con estos dispositivos son: hablar por teléfono, navegar en internet, uso de mensajería instantánea, estar en las redes sociales, sacar fotos, escuchar música , jugar, leer noticias, enviar y recibir correos electrónicos.

Según la Asociación Mexicana de Internet (AMIPCI) 36 % de los internautas en México se conectan desde la escuela, por lo que la firma de seguridad Raytheon/Websense alertó sobre el peligro que pueden correr los menores por los delincuentes que buscan aprovecharse de ellos.

El mismo reporte del AMIPCI indica que, en promedio, los infantes comienzan a usar internet a la edad de seis años, lo que significa que no tienen plena conciencia de los peligros a los que se exponen en la red.

Otra encuesta realizada por la Alianza por la Seguridad de Internet A.C. a estudiantes de nivel básico, precisó que el 41.1 por ciento de los encuestados aceptó que alguna vez ha compartido su contraseña, de correo o red social; 53.2 por ciento de los niños piensa que la información personal de sus redes está segura si se establece el perfil como privado. En algunos países ya están aplicando medidas respecto a éste problema, como por ejemplo en Estados Unidos, ya que la Ley de Protección Infantil en Internet (CIPA) solicitó a las escuelas proteger a los alumnos contra amenazas que hay en línea, bloquear el acceso a contenido inapropiado y vigilar el uso general que los alumnos dan al internet (El financiero, 2015).

Por lo anterior, se concluye que las personas en edad infantil son los usuarios más vulnerables a diferentes riesgos al usar dispositivos móviles y navegar en internet, como por ejemplo: la suplantación de identidad, robo de información, contacto con personas malintencionadas, ciberacoso, sexting, grooming, etc.

Tomando en cuenta lo que se menciona en el estudio “Regulación Jurídica de Internet” de la Investigadora Parlamentaria Elma del Carmen Trejo García; podemos definir a internet como una ‘red de redes’, es decir, una red que no sólo interconecta computadoras, sino que interconecta redes de computadoras entre sí. Una red de computadoras es un conjunto de máquinas que se comunican a través de algún medio (cable coaxial, fibra óptica, radiofrecuencia, líneas telefónicas, etc.) con el objeto de compartir recursos. Tiene dos funciones básicas:

- Medio de Información, es el centro de documentación más grande y completo del mundo. Acceso a libre información (no límites geográficos, no fronteras, ni jurisdicción).
- Medio de Comunicación, mediante correo electrónico, foros de discusión y servicio de llamadas telefónicas.

La mayoría de las personas no están informados sobre los problemas que pueden provocar el mal uso de los dispositivos móviles y las redes sociales, y no se dan cuenta del daño que podría causarles tanto económica como socialmente. Por lo tanto, es necesario que tengan fácil acceso a material con recomendaciones, las cuales les ayudarán a disminuir los riesgos a los que están expuestos y además a ser usuarios más preparados en un futuro laboral.

Capítulo IV. Normatividad y mejores prácticas sobre el uso responsable de dispositivos móviles y redes sociales

Este capítulo comienza hablando sobre la normatividad que existe en diferentes países del mundo respecto al uso de dispositivos móviles y redes sociales, también se abordan temas sobre buenas prácticas que sugieren los principales fabricantes de dispositivos móviles, las políticas de las principales aplicaciones y redes sociales y el NIST 800-50 como base para el desarrollo del plan de concientización.

4.1 Leyes y normativas que regulan el uso de dispositivos móviles y redes sociales en México y otras regiones del mundo

En este capítulo se abordan las legislaciones de otras regiones como Argentina, Colombia, España, Brasil y Chile que regulan el uso de dispositivos móviles y redes sociales, para México se plasma información acerca del organismo del gobierno mexicano encargado de ciberseguridad, sin embargo, en México no existe legislación para este rubro.

4.1.1 México

Actualmente en México como tal no existe algún tipo de legislación específica que regule el uso de dispositivos móviles y redes sociales, sin embargo, el gobierno tiene en cuenta que en el tema de la seguridad cibernética el eslabón más frágil es el ciudadano, un usuario común, que puede tomar el papel de filtro o facilitador para un ataque. Para prevenir estos ataques, la Policía Federal ha establecido algunas estrategias que incluyen investigación y principalmente la prevención mediante espacios institucionales y proximidad social, con platicas preventivas en escuelas y plazas públicas **(Comisión Nacional de Seguridad, 2015)**.

La Comisión Nacional de Seguridad, refrenda su compromiso por hacer de la tecnología un aliado clave en materia de promoción y fomento a la seguridad, sin embargo la difusión no ha sido de manera masiva o general, pues la mayoría de la gente desconoce estas iniciativas.

Actualmente existe información básica acerca de las recomendaciones generales que ofrece la seguridad cibernética, recomendaciones de compra en línea, recomendaciones para menores y recomendaciones para dispositivos electrónicos y redes sociales.

Esta información carece de difusión y se debe navegar mucho para encontrarla en el sitio actual, se debe saber lo que se está buscando, no se muestra a primera instancia en el sitio de la comisión nacional de seguridad.

4.1.2 Argentina

Grooming. En 2011 se aprobó la ley que tipifica y penaliza el delito de "grooming" es decir el acoso sexual a menores de edad vía Internet, después de algunos años y de modificaciones quedo de la siguiente manera.

Artículo 131: “Será penado con prisión de seis meses a cuatro años el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma”. **(Tazza, Alejandro, 2014)**.

Suplantación de identidad digital. La usurpación de la identidad en medios digitales aun no es una ley en Argentina, pero María de los Ángeles Higonet y Carlos A. Verna han presentado en el Congreso de la Nación un proyecto de Ley que incorpora el art. 138 bis al Código Penal por el cual se tipifica el delito de suplantación de identidad digital.

“Será reprimido con prisión de 6 meses a 3 años o multa de veinte mil a doscientos mil pesos el que sin consentimiento adquiera, tenga en posesión, transfiera, cree o utilice la identidad de una persona física o jurídica que no le pertenezca, a través de internet o cualquier otro medio electrónico y con la intención de dañar, extorsionar, defraudar, injuriar o amenazar a otra persona u obtener beneficio para sí o para terceros”. **(Tomeo, Fernando, 2012)**.

Protección de Datos Personales: Ley 25.326 Disposiciones Generales. Principios generales relativos a la protección de datos. Derechos de los titulares de datos. Usuarios y responsables de archivos, registros y bancos de datos. Control. Sanciones. Acción de protección de los datos personales.

La norma se aplica tanto como a los “bancos de datos destinados a prestar servicios de información crediticia” como a las bases de datos que mantiene el Banco Central de la República Argentina.

Artículo 1° (Objeto):“La presente ley tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de

datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional. Las disposiciones de la presente ley también serán aplicables, en cuanto resulte pertinente, a los datos relativos a personas de existencia ideal. En ningún caso se podrán afectar la base de datos ni las fuentes de información periodísticas ". **(Ministerio de Justicia y derechos humanos, argentina 2000)**.

4.1.3 Colombia

Colombia está considerado dentro de los países del mundo que tienen un alto nivel de ciberseguridad, se encuentra por encima de México y Chile y podría competir al nivel de países como Francia, España, Egipto y Dinamarca. Cuenta con un conjunto de organismos especializados en la recepción, atención y seguimiento de delitos informáticos, algunos de ellos son: Centro Cibernético Policial (CCP), Comando Conjunto Cibernético (CCOC) y el Grupo de Respuesta a Incidentes Informáticos (ColCERT).

Leyes que regulan el uso de redes sociales en Colombia

Debido a que las redes sociales surgieron hace relativamente poco tiempo, algunas leyes no definen estrictamente que son aplicables a las "redes sociales" pero se ha establecido que las redes sociales están bajo aquellas leyes que se encargan de proteger la información de los datos personales y preservan el uso de tecnologías de información y comunicaciones. Por ejemplo, el hecho de difundir mentiras sobre otras personas por medio de Twitter u otra plataforma podría ser acusado de difamación, aunque en la legislación no menciona estrictamente la difamación mediante redes sociales.

Ley 1273 Código Penal de Colombia, año 2009: Se trata de una modificación realizada en el código penal de Colombia en el que se incluyen penas para delitos que consisten en el acceso abusivo a sistemas informáticos, interceptación de datos, uso de software malicioso, violación de datos personales, entre otras. Si una persona accede al perfil de otra y se prueba el acceso ilegal, podría tener castigos de hasta 96 meses en prisión y multas hasta por 1,000 salarios mínimos. Se tipifica un nuevo "bien" denominado "de la protección de la información y de los datos".

Ley Estatutaria 1581 de Habeas Data y protección de datos personales, 17 de octubre de 2012: Dicta disposiciones generales para la protección de datos, así como para la transparencia en la utilización de las bases de datos que contienen la información de los usuarios.

Artículo 1: “Tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos”

Artículo 2: “Los principios y disposiciones contenidas en la presente ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada.”

Con esta ley de protección de datos se da pie a que los usuarios tengan libertad de su información personal, transparencia del uso que se le da a sus datos, confidencialidad y en general seguridad.

Artículo 15 de la Constitución Nacional de Colombia: Brinda a los ciudadanos el derecho a su intimidad personal y familiar. Además, les da derecho a conocer, actualizar y rectificar datos que se hayan recogido y almacenado en bancos de datos y en archivos de entidades públicas y privadas.

4.1.4 España

En cuestión a la protección de menores que hacen uso de redes sociales ya sea por dispositivos móviles u otros medios, en España existe la siguiente ley:

El Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, que establece en su artículo 13 que, como regla general, para recabar los datos de cualquier menor de 14 años es necesario contar con el consentimiento de los padres o tutores. Tomando en cuenta esto en el ámbito de las redes sociales, se debe interpretar que según la normativa española la edad mínima en España para que un menor pueda registrarse en una red social es de 14 años. Facebook ya ha elevado la edad mínima para compartir información en su plataforma adecuándose así a la legislación española. Sin embargo, aún con la existencia de ésta ley aún hay niños que tienen cuentas en redes sociales.

En este sentido, dos ejemplos de buenas prácticas son las medidas llevadas a cabo precisamente por dos redes sociales españolas. Por un lado, Tuenti, viene aplicando desde el pasado verano un protocolo de control de edades entre sus usuarios, de tal modo que cuentan con un equipo de soporte al usuario de más de 20 personas para identificar y borrar los perfiles falsos o que incumplen las condiciones de uso del servicio. El segundo ejemplo es Comunidad Clan, red social infantil impulsada por RTVE (Radio y Televisión Española), donde son los propios padres los que han de crear el perfil de sus hijos, por lo que se garantiza su consentimiento.

Otra alternativa, defendida desde INTECO (Instituto Nacional de Tecnologías de la Comunicación), es la utilización del DNI (Documento Nacional de Identidad) electrónico como fórmula para que los jóvenes mayores de 14 años puedan demostrar fehacientemente que lo son y así poder registrarse y acceder a las plataformas. **(Instituto Nacional de Ciberseguridad, España, 2010)**

4.1.5 Brasil

En Brasil, el Marco Civil de Internet, es una ley integral que establece principios, garantías, derechos y obligaciones para el uso de Internet en este país.

La ley está conformada por cinco capítulos, que son: disposiciones preliminares, derechos y garantías de los usuarios, prestación de aplicaciones de conexión y de internet, desempeño del gobierno y disposiciones finales.

Los artículos que resaltan y son parte de los fundamentos y principios, con referencias a redes sociales son los siguientes:

Artículo 2°. La disciplina de la utilización de internet en Brasil se basa en el respeto a la libertad de expresión, así como:

I. el reconocimiento de la escala mundial de la red;
II. los derechos humanos, el desarrollo de la personalidad y de la ciudadanía en los medios digitales;
III. la pluralidad y la diversidad;
IV. la apertura y la colaboración;
V. la libre empresa, la libre competencia y protección del consumidor; y
VI. la finalidad social de la red.

Artículo 3°. La disciplina de la utilización de Internet en Brasil cuenta con los siguientes principios:

I. garantía de la libertad de expresión, la comunicación y la manifestación del pensamiento, según la Constitución;
II. protección de la privacidad;
III. protección de los datos personales, en forma de ley;
IV. preservación de la garantía de neutralidad de la red;
V. preservación de la estabilidad, seguridad y funcionalidad de la red, por medio de técnicas compatibles con los patrones internacionales y por el estímulo al uso de buenas prácticas;
VI. responsabilizarían de las partes de acuerdo con sus actividades, en los términos de la ley
VII. preservación de la naturaleza participativa de la red

Artículo 8°. La garantía del derecho a la privacidad y a la libertad de expresión en las comunicaciones es condición para el pleno ejercicio del derecho de acceso a Internet. Parágrafo único. Son nulas de pleno derecho las cláusulas contractuales que violen lo dispuesto anteriormente, tales como las que:

I. impliquen ofensa a la inviolabilidad y al secreto de las comunicaciones privadas a través de Internet
II. en la contratación, no ofrezcan al contratante la adhesión al foro brasileño para la solución de conflictos derivados de servicios prestados en Brasil.

Artículo 18°. El proveedor de conexión a internet no será responsabilizado civilmente por daños surgidos por contenido generado por terceros.

Artículo 19°. Con el objetivo de asegurar la libertad de expresión e impedir la censura, el proveedor de aplicaciones de Internet solamente podrá ser responsabilizado por daños que surjan del contenido generado por terceros si, después de una orden judicial específica, no toma las previsiones para, en el ámbito de los límites técnicos de su servicio y dentro del plazo asignado, hace disponible el contenido especificado como infríngete, exceptuando las disposiciones legales que se opongan.

4.1.6 Chile

La ley 19628 habla sobre la protección de datos de carácter personal, teniendo como principal objetivo la protección de la información personal.

Los principales artículos que encontramos en esta ley en al ámbito de protección de información personal y redes sociales son los siguientes:

Artículo 1º.- El tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares se sujetará a las disposiciones de esta ley.

Artículo 2º.- En este artículo se mencionan conceptos que están vinculados con la información personal de cada persona, con la descripción de estos conceptos se deja claro los principios con los que opera la ley y así se determinan responsabilidades jurídicas. A continuación, se enlistan los más importantes:

- Almacenamiento de datos. Se refiere a la conservación o custodia de datos en un registro o banco de datos.

- Registro o banco de datos. Es el conjunto organizado de datos de carácter personal, sea automatizado o no y cualquiera sea la forma o modalidad de su creación u organización, que permita relacionar los datos entre sí, así como realizar todo tipo de tratamiento de datos.

- Datos sensibles. Son aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.

- Responsable del registro o banco de datos. Es la persona natural o jurídica privada, o el respectivo organismo público, a quien competen las decisiones relacionadas con el tratamiento de los datos de carácter personal.

- Titular de los datos. La persona natural a la que se refieren los datos de carácter personal.

- Tratamiento de datos. Cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma.

Artículo 4º. El tratamiento de los datos personales sólo puede efectuarse cuando esta ley u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello. Bajo esta disposición se garantiza el titular de los datos es el único que puede permitir la manipulación de su información. La aprobación o consentimiento de la persona debe estar en un documento escrito.

Artículo 7º. Las personas que trabajan en el tratamiento de datos personales, tanto en organismos públicos como privados, están obligadas a guardar secreto sobre los mismos, cuando provengan o hayan sido recolectados de fuentes no accesibles al público, como asimismo sobre los demás datos y antecedentes relacionados con el banco de datos, obligación que no cesa por haber terminado sus actividades en ese campo.

Artículo 12 º. Se extienden los derechos que tiene el titular de los datos sobre su información:
Exigir al responsable el propósito del almacenamiento y cuáles de sus datos son transmitidos
Derecho a exigir la modificación de sus datos cuando sean erróneos, inexactos o incompletos

Exigir que se eliminen, en caso de que su almacenamiento carezca de fundamento legal o cuando haya perdido vigencia.
Artículo 13º. El derecho de las personas a la información, modificación, cancelación o bloqueo de sus datos personales no puede ser limitado por medio de ningún acto o convención.

Artículo 14º. Si los datos personales están en un banco de datos al cual tienen acceso diversos organismos, el titular puede requerir información a cualquiera de ellos.

4.2 Recomendaciones de uso de dispositivos móviles de los principales fabricantes

Durante el tercer trimestre del año 2015, las ventas de dispositivos móviles, particularmente de teléfonos inteligentes, fueron un total de 353 millones de unidades. Con lo anterior mencionado podemos visualizar que los smartphones están abarcando un gran terreno dentro de los dispositivos móviles.

Cada compañía fabricante de estos equipos nos proporciona información relacionada a su producto, como recomendaciones para evitar lesiones o provocar algún daño material derivado de un uso incorrecto.

Teniendo como base a las dos principales empresas fabricantes de smartphones, se enlistan las recomendaciones específicas que cada una proporciona para el uso del teléfono inteligente.

Samsung

Como característica de su sistema operativo (Android) nos permite crear sesiones de usuario con privilegios establecidos por el dueño del aparato, esta función es de gran utilidad ya que cada persona que usa el dispositivo tiene su información de cuentas, aplicaciones y demás funciones configuradas a su manera, aunque es baja la cantidad de personas que saben de la existencia de este modo de varias sesiones, y son menos aun las que saben cómo funciona.

Las principales recomendaciones que hacen son:

- Cuando utilice el dispositivo, asegúrese de realizar copias de seguridad de los datos importantes. Samsung no se responsabiliza por la pérdida de ningún dato.

- Lea la pantalla de permisos cuidadosamente al descargar aplicaciones. Tenga particular cuidado con las aplicaciones que tienen acceso a varias funciones o a una cantidad importante de su información personal.
- Controle sus cuentas regularmente para descartar el uso sospechoso o no autorizado. Si encuentra algún signo de mal uso de su información personal, contacte a su proveedor de servicios para eliminar o cambiar la información de su cuenta.
- En caso de perder el dispositivo o que se lo roben, cambie las contraseñas de sus cuentas para proteger su información personal.
- Evite el uso de aplicaciones de fuentes desconocidas y bloquee el dispositivo con un patrón, una contraseña o un PIN.
- No entre en sitios web poco fiables.
- Elimine los mensajes de texto o de correo electrónico sospechosos de remitentes desconocidos.
- Establezca una contraseña y modifíquela con regularidad.
- Desactive las funciones inalámbricas, tales como Bluetooth, cuando no las utilice.
- Si el dispositivo se comporta de forma anormal, ejecute un programa de antivirus para detectar una posible infección.
- Ejecute un programa de antivirus en el dispositivo antes de iniciar aplicaciones y archivos que acaba de descargar.
- Instale programas de antivirus en su ordenador y ejecútelos con regularidad para detectar posibles infecciones.
- No edite los ajustes de registro ni modifique el sistema operativo del dispositivo.

Adicional a estas sugerencias y como una funcionalidad exclusiva de la marca Samsung posee un “modo seguro” que permite comprobar si alguna aplicación es la causante de algunas fallas que pudiera presentar el dispositivo.

Apple

Los dispositivos de Apple funcionan con el sistema operativo IOS, el cual es exclusivo de la marca.

Para poder llevar a cabo muchas de las recomendaciones para los equipos de Apple es necesario instalar el software iTunes en la computadora y además tener una cuenta registrada con la compañía.

Las principales recomendaciones que mencionan para sus dispositivos son:

- Manejo: Manipule el dispositivo con cuidado. Está fabricado en metal, vidrio y plástico y posee componentes electrónicos sensibles en su interior. Si se cae, se quema, se pincha, se aplasta o entra en contacto con líquidos, podría sufrir daños. No utilice un equipo que esté dañado (por ejemplo, si la pantalla está rajada), puesto que podría ocasionar lesiones. Si le preocupa que la superficie del teléfono se raye, puede utilizar una funda.
- Reparación: No abra el teléfono ni trate de repararlo usted mismo. Si desmonta el teléfono, podría dañarlo o podría lesionarse usted.
- Usar un código con protección de datos. Para aumentar la seguridad, puede establecer un código que deberá introducirse cada vez que se encienda o active el equipo.
- Restablecer del dispositivo. Si tiene problemas con el equipo, puede restablecer los ajustes de red, el diccionario del teclado, la disposición de la pantalla de inicio y los ajustes de ubicación y privacidad. También puede borrar todo su contenido y ajustes.
- Realizar copias de seguridad. Puede utilizar iCloud o iTunes para realizar copias de seguridad automáticamente.

Como se puede ver, existen diversas recomendaciones por los fabricantes tanto a nivel seguridad física como a nivel seguridad lógica (aplicaciones), sin embargo, no existe una suficiente difusión y conocimiento por parte de la población que tiene uno de estos dispositivos, y mucho menos por los que son niños.

4.3 Políticas de seguridad de las principales aplicaciones y redes sociales

A continuación, se hace una breve descripción sobre las recomendaciones y métodos de seguridad que tienen algunas de las aplicaciones más populares utilizadas por los menores caso de estudio de la presente tesina.

YouTube

YouTube es una red donde se pueden ver y subir videos de cualquier índole pero tiene restricciones al momento de compartir contenido, para poder subir videos es necesario tener una cuenta de correo electrónico vinculada pero no es necesaria para poder ver los videos que circulan en la red , una de las principales políticas de seguridad que tiene esta red es, que no puedes ver videos que están clasificados para mayores de edad si no compruebas con alguna cuenta de correo que eres mayor de edad, otra de las políticas es que solo los usuarios que decidas podrán ver los videos que publiques, de igual forma puedes solo mostrar los datos de tu cuenta que quieras incluso tienen una página donde se pueden consultar las normas de seguridad https://www.youtube.com/yt/policyandsafety/es/communityguidelines.html.

Facebook

Ya que una de las principales redes sociales tienes varios puntos para proteger la información de los usuarios y la seguridad de los mismos. En la página de ayuda de Facebook se proporciona información acerca de la seguridad, privacidad y configuración en general de la cuenta, por mencionar algunas:

- Configuración y herramientas de privacidad básica, se configura quien puede ver el contenido de las publicaciones y en general del perfil.
- Revisar el contenido en el que te etiquetan, se puede controlar las menciones que hacen de tu perfil, se pueden ocultar o mostrar en tu muro.
- Menores y privacidad, se dan consejos acerca de las publicaciones y predeterminadamente está bloqueado la opción de publicar la ubicación.
- Información de seguridad general, proporciona información general sobe las contraseñas, los bloqueos de personas, reportar una página, entre otros.
- Centro de seguridad para familias, es un apartado donde se pone a disposición del usuario herramientas, información y recursos para la seguridad.

La información completa y detallada se puede consultar en la página de internet https://www.facebook.com/safety.

WhatsApp Ayuda.

Cómo protegerse en WhatsApp, en este artículo se destacan las herramientas y funciones que se pueden utilizar. También se proveen enlaces a otros recursos con información que puede ayudar a mantener tu seguridad en Internet.

Términos de Servicio, detallan actividades prohibidas como contenido (en estados, fotos de perfil o mensajes) ilegal, obsceno, amenazante, con muestras de odio, racista, ofensivo, o cualquier otra materia inapropiada. Molestando a otros usuarios también constituye una violación de nuestros Términos de Servicio. Si creemos que un usuario está violando los Términos de Servicio, suspendemos su cuenta.

Herramientas

En WhatsApp, se han creado algunas configuraciones que se pueden ajustar en base a las necesidades para ayudar a protegerte.
Controla quién puede ver tu información. Se puede cambiar los ajustes de la hora de tu última vez con actividad, tu foto de perfil y/o estado de las maneras siguientes:

- Todos: Todos los usuarios de WhatsApp pueden ver la hora de tu última vez, tu foto de perfil y/o tu estado.

- Mis contactos: Solo los contactos guardados en tu lista de contactos pueden ver la hora de tu última vez, tu foto de perfil y/o tu estado.

- Nadie: Nadie puede ver la hora de tu última vez, tu foto de perfil y/o tu estado.

Si desactivas las Confirmaciones de lectura nadie puede ver las confirmaciones de lectura de los mensajes que te envían y tampoco puedes ver las confirmaciones de lectura cuando un contacto lee un mensaje que le envías.

Controla la información que ves y con quién intercambias mensajes, existe la opción de bloquear a contactos en WhatsApp si los bloqueas no podrán enviarte ni ver la hora de tu última vez, tu foto de perfil y/o tu estado.

Cuando recibes por primera vez un mensaje de alguien desconocido tienes un botón en el chat para reportar spam.

Cuentas suspendidas, se puede suspender una cuenta si creemos que hay actividad que viola los Términos de Servicio. Usamos herramientas automatizadas y reportes de otros usuarios para decidir si vamos a suspender una cuenta. Sin embargo, cuando recibimos reportes de nuestros usuarios de actividad que puede ser una violación a nuestros Términos de Servicio no siempre suspendemos la cuenta en cuestión.

Instagram

Instagram al igual que las otras redes sociales ofrece varios puntos en seguridad los cuales tienen varios apartados y se citan a continuación:

- Consejos sobre privacidad y seguridad Instagram te brinda una divertida oportunidad para compartir tu vida a través de fotos y vídeos.

- Conoce las normas sobre la edad de los usuarios Ten en cuenta que el uso de Instagram está limitado a mayores de 13 años. Animamos a nuestros usuarios a que nos informen del uso por parte de menores a través de nuestro servicio de ayuda.

- Denuncia contenido conflictivo Puedes denunciar cualquier contenido que pueda infringir nuestras políticas, tanto directamente desde la aplicación de Instagram como a través de las funciones de denuncia integradas.

- Comparte con personas concretas Al seleccionar el icono de "Instagram Direct" en la esquina superior derecha de la aplicación, podrás escoger si deseas compartir solo con unas cuantas personas (hasta un máximo de 15) en lugar de con todos tus seguidores.

- Activa la privacidad de tus publicaciones Cuando estableces tus publicaciones como privadas, aquellos que quieran ver tus fotos, vídeos, seguidores o listas de seguimiento tendrán que enviarte una solicitud de seguimiento que puedes aprobar o ignorar.

- Decide si quieres usar tu mapa de fotos La opción de añadir ubicaciones a las fotos, conocida como "Mapa de fotos" está desactivada para todas las fotos que se cargan a Instagram. Esto quiere decir que las fotos no aparecerán en el mapa de fotos de nadie sin su permiso.

- Bloquea a alguien siempre que sea necesario Cuando un usuario utiliza la función de bloquear, la persona bloqueada no puede ver sus publicaciones ni buscar su cuenta de Instagram.

También tiene una guía para padres la cual toca los puntos importantes como la visibilidad del contenido que se publica, el bloqueo de las cuentas, la edad mínima para poder tener una cuenta, incluso menciona los riesgos que conlleva utilizar ésta red el articulo completo se encuentra en la siguiente liga:
https://fbcdn-dragon-a.akamaihd.net/hphotos-ak-ash2/t39.2365-6/10734300_481935391948704_92634154_n.pdf

De la misma forma que con las recomendaciones hechas por los fabricantes de dispositivos, el usuario promedio tiende a no leer e informarse sobre cómo puede proteger sus datos y sobre todas

las herramientas que cada aplicación ofrece, así entonces al darle un dispositivo móvil al niño, no se tiene el cuidado de explicarle o dejarle una configuración en la que se exponga lo menos posible.

4.4 NIST 800-50

Debido a que en la situación de concientización para menores no existe una norma ISO 27000, un ITIL o COBIT aplicable, se acude al uso de las buenas practicas definidas por el NIST serie 800-50.

El Instituto Nacional de Normas y Tecnología, NIST por sus siglas en inglés, es un organismo federal no regulador que forma parte de la administración de tecnología del departamento de comercio de los estados unidos. El objetivo de éste instituto es promover patrones de medición, normas y tecnología con el fin de realzar la productividad, facilitar el comercio y mejorar la calidad de vida.

La FISMA (Federal Information Security Management Act) de Estados Unidos, otorgó al NIST el desarrollo de un conjunto de documentos SP-800, la serie 800 del NIST es una serie de documentos de interés general sobre seguridad de la información. Dichas publicaciones comenzaron en 1990 y son un esfuerzo de industrias, gobiernos y organizaciones académicas para todos los interesados en la seguridad.

En ese capítulo se habla especialmente del “NIST 800-50 construcción de un programa de concientización y entrenamiento de seguridad de tecnologías de información”, el cual fue publicado en octubre de 2003; este programa habla sobre la conciencia de seguridad y la formación, las cuales deben centrarse en todos los usuarios de la organización. Es necesario llevar a cabo un programa de sensibilización, que debe comenzar con un esfuerzo que puede ser desplegado e implementado de diferentes maneras y está dirigido a todos los niveles de la organización, incluyendo los altos directivos y ejecutivos.

En éste documento se establece que, para implementar un programa para desarrollar la cultura de seguridad de la información, se tienen tres componentes principales que son:

Concientización. - Menciona que hay que enfocar la atención en la seguridad de la información, hacer que el público reconozca los temas de interés, estableciendo al inicio qué comportamientos se quieren reforzar, por ejemplo, usar de forma adecuada las contraseñas, hacer copias de respaldo, usar el correo responsablemente, etc.

Entrenamiento. - Consiste en producir habilidades y competencias en seguridad de la información relevantes y requeridas con el fin de que el público objetivo las aprenda y aplique en el día a día.

Educación. - Se trata de integrar habilidades de seguridad y competencias de las diferentes especialidades funcionales dentro de un cuerpo común de conocimientos, enfocándose en producir especialistas de seguridad.

Se debe tomar en cuenta que en éste ciclo el aprendizaje es continuo, ya que inicia con concientización y prosigue con el entrenamiento y desarrollo a través de la educación hacía la creación de cultura de seguridad de la información.

El NIST 800-50 toma en cuenta cuatro fases para lograr el desarrollo de los planes de concientización y entrenamiento en seguridad de la información, las cuales son:

1.- Diseño: En ésta primera fase se debe estructurar el programa, se evalúan las necesidades, se desarrollan las estrategias y planes, se definen las prioridades, etc.

2.- Desarrollo de material: Se seleccionan los temas a tomar en cuenta para la concientización, y se revisan los cursos de entrenamiento.

3.- Implementación del Programa: Se deciden las técnicas para la entrega del material, ya sea posters, videos, conferencias, boletines, concursos, etc.

4.- Mantenimiento: En la última fase se lleva a cabo el monitoreo del programa, se revisan los métodos de evaluación y retroalimentación, se ve la gestión del cambio y la mejora continua.

En resumen, para que un programa de concientización en seguridad de la información sea exitoso, se requiere el compromiso y aprobación por parte de la alta dirección, la definición clara de un alcance, objetivos, responsables, entregables y fechas de compromiso en un marco de tiempo realizable en la organización, y la supervisión, evaluación y retroalimentación por parte del personal en el programa. Orientándose hacia los niños, se requiere la participación y compromiso por parte de los padres, los docentes y el menor en sí.

El punto más fuerte que se toma del NIST 800-50 para el desarrollo de la presente tesina, es la parte de la concientización, en la que se aclara que la concientización no es un entrenamiento. El propósito de la concientización es enfocar de una manera simple la atención del público objetivo en el tema a abordar, en este caso el uso de dispositivos móviles y redes sociales en edad infantil. La

concientización le permite al usuario (En primer lugar, hijos y en segundo padres) entender las preocupaciones que se le quieren transmitir y responder acorde a lo esperado para su seguridad.

En la sensibilización el alumno es el principal destinatario de la información para que entienda la problemática mediante técnicas atractivas y dinámicas que lo hagan reflexionar y cambiar su forma de actuar.

Capítulo V. Propuesta de plan de concientización para usuarios de dispositivos móviles y redes sociales en edad infantil

En este capítulo se plantea un modelo de concientización sobre dispositivos móviles y redes sociales el cual va dirigido a niños de entre 5 y 10 años y sus respectivos padres con el objetivo de dar a conocer los riesgos y vulnerabilidades a los que están expuestos, proporcionar recomendaciones para incrementar la seguridad respecto al uso de dispositivos móviles y redes sociales y hacer una difusión a través de diferentes medios.

5.1 Modelo de concientización para usuarios de dispositivos móviles y redes sociales en edad infantil

Se propone un plan de concientización para el buen uso de dispositivos móviles y redes sociales que se implemente a lo largo de 2 semanas de manera presencial y de forma permanente y actualizada de manera digital, en este plan se involucra a los niños, los padres y uno o varios instructores (docentes) con conocimiento en manejo de grupos infantiles.

El objetivo del plan es el de crear conciencia sobre la seguridad de los usuarios en edad infantil de dispositivos móviles y redes sociales, es que el individuo mismo sea capaz de comprender lo que debe y no debe hacer con su dispositivo, teniendo como principal guía a sus padres o responsables directos y a sus profesores. Todo esto mediante material atractivo visualmente para los niños y de fácil comprensión, así como de forma interactiva mediante una página web.

El plan puede ser aplicado por los profesores o cualquier otro personal capacitado y se enfocará en la concientización ya que el propósito es enfocar la atención para posibilitar que el público objetivo (menores y sus padres) reconozca los temas de interés, estableciendo al inicio qué comportamientos se quieren reforzar, por ejemplo, usar de forma adecuada las contraseñas, supervisar a los menores, cuidar la información personal y sensible, etcétera. Con esto, lograr una mejor conciencia y cultura de los menores que en un futuro puedan desarrollarse como usuarios responsables respecto a la seguridad de la información personal y de la empresa en la que se desarrollen.

Tomando en cuenta las fases del NIST 800-50, se muestra en la figura 5.1 el modelo a seguir para el desarrollo del plan de concientización para usuarios de dispositivos móviles y redes sociales en edad infantil.

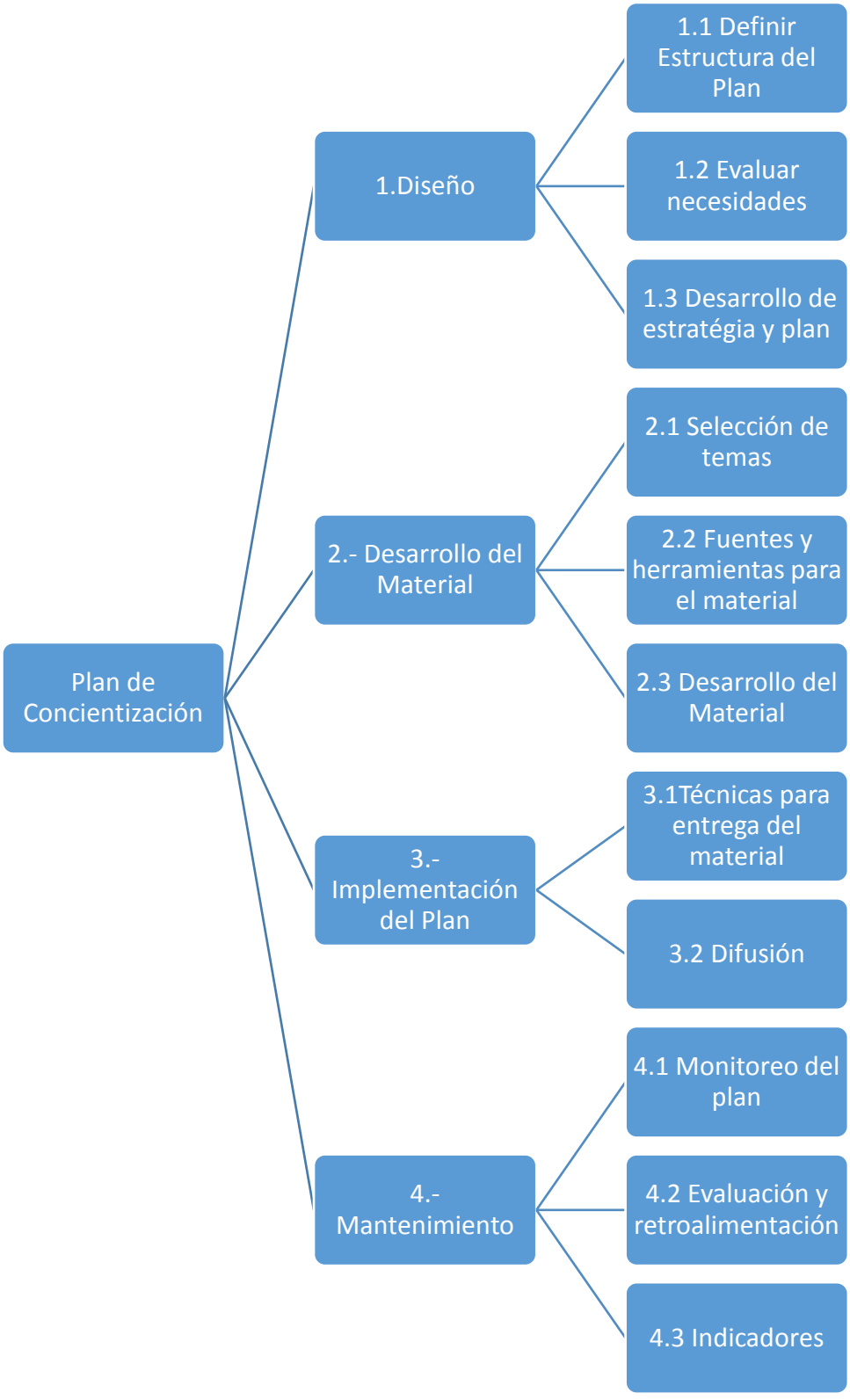


Figura 5.1 Modelo del plan de concientización.

5.1.1 Diseño

El diseño es la parte donde se definen todos los puntos que el plan de concientización contendrá, las necesidades que se desean cubrir, el detalle de cada una de las secciones en que se divide y la forma en que se hará llegar la información a los niños para que les llame la atención y sea fácil de entender y retener.

Corresponde al primer punto señalado en el modelo del plan de concientización (Figura 5.1) que además contiene las tareas de:

Definir estructura del plan. Se detallan las secciones que contendrá el plan y nombres de las secciones.

El plan se divide en 5 secciones, que se muestran en la figura 5.2

Figura 5.2 Estructura del plan de concientización.

- Proporcionar información necesaria y ejemplos de los riesgos y peligros que existen al usar dispositivos móviles
- Recomendaciones de seguridad
- Material referente al control parental
- Reafirmación de conocimientos

- Evaluación y retroalimentación

A lo largo de estas 5 secciones es mediante las cuales se pretende lograr la concientización de los menores y de sus padres.

Evaluar necesidades. Contiene las necesidades que debe cubrir el plan.

Mediante la aplicación de cuestionarios a padres e hijos (Anexo 1) se identifican las necesidades que debe cubrir el plan. El cuestionario sirve para conocer la situación actual de los menores respecto al uso de éstas tecnologías, que debilidades hay y que fortalezas ya han desarrollado. También se incluyen necesidades que se deben cubrir debido a que el público objetivo son niños.

- Proporcionar la información con material llamativo para los menores, como son videos cortos, imágenes y página web interactiva.
- Dar a conocer las sugerencias de seguridad para el menor de forma simple y con vocabulario de fácil comprensión.
- Involucrar a los padres ya que son los responsables directos de los menores.
- Involucrar a los docentes que son los segundos encargados del aprendizaje de los menores.
- Dar a conocer los riesgos que representa el uso de dispositivos móviles y redes sociales en edad infantil.
- Dar a conocer herramientas mediante las cuales los padres pueden proteger a sus hijos (control parental).
- Dar a conocer la información mediante los canales de comunicación que más utilizan los menores (videos de youtube y redes sociales).

Desarrollo de estrategia y plan. Se muestran todas las secciones definidas anteriormente y se detalla cada una de las actividades que se deben realizar.

Se convoca a los padres y a sus hijos a 4 sesiones distribuidas en 2 semanas en las cual se presentarán las 5 secciones definidas. Para un mejor manejo, debe estar presente uno o más de los profesores responsables del grupo. Para un mayor entendimiento se realiza difusión antes, durante y después mediante carteles, folletos y canales digitales. El prototipo de la página web y el material de difusión se presenta en la fase de “Desarrollo del Material”.

A continuación, se detalla el contenido de cada una de las 5 secciones de las que está conformado el plan y que se muestran en la figura 5.2.

Sección 1. Información de riesgos al usar dispositivos móviles

Mediante el apoyo de videos se dan a conocer de una forma dinámica y entretenida los riesgos de utilizar dispositivos móviles.

En esta sección se muestran los riesgos de no supervisar ni enseñar a los menores, los cuidados que deben tener al usar internet y redes sociales mediante sus dispositivos móviles. Esta serie de videos es dirigida hacía los padres o responsables del menor.

Mostrar mediante una serie de videos los riesgos que se corren al usar internet y redes sociales mediante sus dispositivos móviles. Esta serie de videos es dirigida hacía los niños.

Sección 2. Recomendaciones de seguridad

Presentación o video informativo en el que se incluyan todas las recomendaciones de seguridad propuestas por el equipo de trabajo tanto a los padres como a los niños. Se enlistan todas las recomendaciones que se quieren dar a conocer debido a que el material existe, pero no tiene la suficiente difusión y no se le da la importancia necesaria, no es que a los niños se les prohíba el uso de un dispositivo móvil, sino desarrollar toda una actitud digital para obtener el máximo beneficio posible de las tecnologías de forma segura.

Recomendaciones para el menor respecto al uso de dispositivos móviles:

- Utilizar contraseña o algún método de autenticación para acceder al contenido del dispositivo móvil. y para acceder a redes sociales.
- Cumplir con las actividades acordadas respecto a tareas y responsabilidades.
- Pedir autorización al responsable directo para la instalación de aplicaciones.
- Evitar conectarse a internet fuera del hogar o sin la supervisión de un responsable.
- Evitar el uso del dispositivo en la calle o lugares públicos. Es mejor solo utilizar el dispositivo dentro del hogar, el auto o la escuela si es que está permitido por los profesores para evitar que lo roben.

Recomendaciones para el responsable del menor respecto al uso general de dispositivos móviles:

- Apoyar al menor a implementar una contraseña para el dispositivo móvil. El uso de un patrón de desbloqueo es el que más fácilmente pueden utilizar.

- Limitar el uso del dispositivo, más no prohibir el uso total. Se logra dando a conocer ventajas y desventajas, y negociando de acuerdo a las actividades del menor, como tarea, ayuda en la casa, cuidado de la mascota, etc.
- Instalar un antivirus.
- Solo instalar software de fuentes confiables. Se debe tener especial cuidado al instalar software, ya que algunos programas pueden infectar los dispositivos móviles o pueden ser programas para el robo de información del dispositivo.
- Alertar al menor de no conectarse a internet en redes públicas ya que al conectarse es vulnerable a la extracción de información o manipulación del dispositivo móvil.
- Supervisar al menor cuando utiliza el dispositivo. Sobre todo si éste tiene conexión a internet.
- Desactivar Bluetooth o GPS cuando el menor utiliza el dispositivo. Se recomienda no tener encendido el Bluetooth ya que se puede estar propenso a recibir algún virus o programa malicioso por este medio, de igual forma se recomienda que no se tenga activado el servicio de localización ya que se podría rastrear el dispositivo con fines maliciosos.
- Ser cuidadoso en el uso del dispositivo en espacios públicos para evitar el robo físico del dispositivo. Esta recomendación es vital para la seguridad personal, ya que estamos propensos al robo físico del dispositivo y puede estar en peligro nuestra integridad física.
- Si el dispositivo móvil va a cambiar de dueño, ya sea porque se venda o regale, asegúrate de borrar todo el contenido antes de entregarlo.

Recomendaciones para el menor respecto al uso de redes sociales e internet:

- Pedir apoyo de un responsable mayor si se quiere abrir una cuenta en una red social. Se sugiere que el responsable apoye con la creación de la cuenta y la contraseña.
- Si alguien te molesta por medio de internet, debes avisar a tu papá, mamá o algún otro adulto al que le tengas confianza, ellos te apoyarán.
- Respetar los horarios acordados para el uso de redes sociales e internet. Evitar utilizarlo por la noche.
- Tener mucho cuidado con la información que se publica, evitar dar direcciones, ocupaciones de los padres, horarios de casa, escuela a la que se asiste, fotografías que muestren la casa o los autos que se tienen, etc. Especialmente cuando alguien te insiste mucho o te pregunta cosas extrañas.
- Recuerda que igual que en la vida real, en la vida virtual es peligroso hablar con personas que no conozcas, solo acepta a personas que sí conoces en la vida real. Elimina todos aquellos contactos que no sepas quienes son para que no tengan acceso a tu información, fotos, videos, personas amigas, familia, etc.

- Si platicas por personas que no conoces más que en línea, por ninguna razón aceptes verlos en persona. Acude a un adulto si esta persona se vuelve agresiva, violenta o muy insistente, no aceptes por nada.
- Antes de exponer un contenido al todo el público piensa ¿Esto que publicas, te atreverías a hacerlo en la vida real?, recuerda que una vez puesto en internet puede llegar a verlo cualquiera.
- Debes respetar a las demás personas, antes de publicar contenido sobre alguien que no seas tu, piensa si esa persona se sentiría incomoda o si fueras tu si te gustaría que dijeran esas cosas de ti. Respeta la privacidad de tus amigos, familiares, profesores, etc.
- Actúa responsablemente cuando se encuentren con contenidos inconvenientes para ti.
- Comunícate responsable y respetuosamente. Recuerda que detrás de un perfil hay una persona, y se deben seguir las mismas reglas de educación y respeto que garantizan la convivencia en la vida real.
- Desconéctate cuando estés con tus seres queridos, disfruta de la compañía.
- Internet no es solo para entretenimiento, dale oportunidad a las aplicaciones que tus padres sugieren.

Recomendaciones para el responsable del menor respecto al uso de redes sociales e internet:

- Si el menor quiere abrir una cuenta propia en una red social, debe crearla con el consentimiento y apoyo del responsable, El responsable debe darse a la tarea de investigar las características de las redes sociales, foros y otros sitios en los que el menor pide participar, además de configurar su cuenta para que todo el contenido sea visualizado solo por personas que tenga en su red de amigos.
- Apoyar al menor en la implementación de contraseñas. De preferencia debe contener mayúsculas, números y un carácter especial. Se sugiere que sea fácil de recordar y difícil de descifrar, evite utilizar nombres de familiares, fechas de nacimiento o secuencias de números como 1234. En su lugar, puede por ejemplo poner el lugar favorito de vacaciones, por ejemplo, “playa” puede ser una contraseña robusta si se coloca de la siguiente forma: pl@Y@fb1.
- Hablar abiertamente sobre temas como el ciberbullying, chantajes, y diferentes amenazas que representa el navegar el internet. Debe crear confianza en el niño para que en caso de que se presente una situación de peligro, el pequeño se sienta en libertad de comunicárselo.
- Establecer reglas sobre el tiempo y los momentos en que se podrá utilizar, evitar que naveguen por la noche. Estas reglas no deben ser impuestas, sino que acordadas entre

ambas partes. Ambas partes debe tratar de cumplir las reglas establecidas, de lo contrario se perderá confianza sobre todo si el que falla en el cumplimiento es el adulto responsable.

- Enseñar al menor a no proporcionar información sensible ni personal como dirección, ocupación de los padres, escuela a la que asisten, si tienen auto, si se encuentra solo en algún momento del día, contraseñas o datos de la familia con desconocidos, ni subirlos o publicarlos en sitios públicos etc.
- Supervisar el uso de Internet en que el niño exprese abiertamente que es lo que hace cuando lo utiliza y que no se sienta en un interrogatorio hostil, si no que sienta confianza.
- El adulto responsable debe tener al menos el mismo nivel que el menor en conocimientos sobre el manejo de internet, si no los tiene, es un buen momento para aprender.
- Generar espacios de confianza para que los niños puedan comentar sus dudas o las situaciones que les parezcan extrañas o incómodas.
- Hacerlos pensar en que todo lo que no se atreverían a hacer en la vida real, tampoco deben hacerlo en la vida “virtual”.
- Enseñarles que al igual que en la vida real, es peligroso que en la vida virtual hablen con personas que no conocen.
- Apoyar al menor en todo momento si se acerca contigo por algún problema que tenga en la red social. Recuerda que debe tener confianza en ti.
- Enseñarles a respetar la privacidad de amigos, conocidos, familiares, no identificando a las personas que aparecen en sus fotos o videos sin su autorización; y a hacerse respetar cuando se sientan incómodos por alguna referencia a ellos en algún sitio, solicitando su eliminación.
- El niño sigue tu ejemplo, así que si quieres que este más cercano a ti que a su dispositivo móvil, empieza dándole el ejemplo, no te pases el día entero pegado al móvil e invita al menor a pasar tiempo juntos.
- Sugiere a tus niños el uso de algunas aplicaciones o páginas educativas. Por ejemplo Brainly, educaNetwork y Edmodo.

Sección 3. Material referente al control parental

En esta sección se explica a los padres lo que significa el control parental y se les proporciona una lista de aplicaciones con las que puede aplicarlo.

El control parental es un programa que puede o no venir preinstalado en los dispositivos móviles, algunas compañías dedicadas a la venta de software manejan varios programas y cada uno tiene sus características pero el principal objetivo de estos programas es la de dar un control a los padres o los responsables de un menor de edad, restringiendo el acceso a ciertas páginas web,

restringir el acceso a juegos, controlar el tiempo que los menores puedan acceder a internet, entre otras muchas funcionalidades.
Los ejemplos que se muestran son ESET Multidispositivo y Qustudio.

ESET Multidispositivo

Características principales:

- Roles de usuario: Desde el módulo de control parental los padres pueden controlar y monitorear el acceso a internet a través de la configuración de un rol para cuentas de usuario de Microsoft Windows.
- Bloqueo de Páginas Web: Otra de las principales características del control parental es la capacidad de restringir el acceso a contenido inapropiado por medio del bloqueo del acceso a ciertos sitios web.
- Restricción de acceso por categoría: Los padres pueden también restringir el acceso agregando o eliminando elementos desde la lista de categorías web para cada rol. Si el casillero próximo a cada categoría se encuentra seleccionado entonces se otorgará el permiso. Deseleccionando una categoría específica, los padres pueden bloquearla para una cuenta en particular. Al pasar el puntero del mouse sobre una categoría aparecerá una lista de sitios web que encuadran en cada una de ellas.
- Registro de actividad: Permite observar un registro detallado de la actividad del control parental (sitios bloqueados, la cuenta para la cual el sitio fue bloqueado, razón, etc.) con el fin de optimizar el monitoreo de la actividad de su equipo en Internet.
- Selección rápida: Los padres pueden configurar rápidamente el rol de un usuario por medio de la selección de una configuración predeterminada (Niño, Padre y Adolescente) o una cuenta de usuario existente y haciendo clic en copiar para copiar la lista de categorías permitidas para esa cuenta.

Qustodio

Características Superiores

- Filtros “Inteligentes”: Protege a los menores de páginas potencialmente dañinas, que escapan a controles comunes. La tecnología “inteligente” de Qustodio es capaz de filtrar páginas sin categorizar utilizando un sofisticado algoritmo que funciona en todos los navegadores web.

- Supervisión social: Los niños pasan tanto tiempo en redes sociales como Facebook que es fundamental vigilar su actividad social en internet. Qustodio ayuda a mantener a los menores a salvo mostrándole quienes son sus amigos y qué tipo de contenido está siendo compartido.
- Control de acceso: Utilice los controles de Qustodio para adaptar el uso de Internet de cada niño. Se pueden bloquear páginas, limitar el tiempo de navegación y el acceso ciertos días u horas del día, y activar la “búsqueda segura” para evitar que páginas perjudiciales aparezcan en sus resultados.
- Control de Aplicaciones: Muestra las aplicaciones que se utilizan y por cuánto tiempo.
- Seguimiento de ubicación: La funcionalidad de Qustodio para el seguimiento de localización, permite conocer la posición de sus hijos en tiempo real, asegurando que siempre estará al tanto de su paradero, ya sea de día, o de noche.
- Botón de Pánico: En caso de emergencia el menor puede activar un botón especial de SOS en su teléfono. Los padres y sus contactos de confianza recibirán un mensaje de "Necesito ayuda" del menor con la información de su localización.
- Monitorización y Bloqueo de Llamadas y SMS: Se puede saber a quién llama y manda SMS su hijo, y establecer una lista de contactos permitidos y bloqueados. Se puede fácilmente limitar las llamadas y SMS a familiares o bloquear llamadas no deseadas.
- Múltiples usuarios y dispositivos permiten la creación de múltiples cuentas para así personalizar el uso de Internet de cada niño. También permite supervisar tantos ordenadores y dispositivos como sean necesarios.
- Gestión Online: En cualquier lugar, podrá hacer seguimiento de los menores utilizando el panel de control online de Qustodio. Basta con acceder al portal a través de cualquier ordenador, tableta o dispositivo móvil con acceso a Internet.
- Reportes de Actividad: Se puede ver lo que los menores hacen exactamente gracias a los informes de actividad de Qustodio. Toda la información que se necesita es presentada en gráficos interactivos fáciles de entender y disponibles en periodos de tiempo seleccionables.
- Avisos importantes: Qustodio revisa la actividad sospechosa en internet y manda alertas si el menor visita un sitio potencialmente peligroso. Además, recibirá un correo diario con su resumen de actividad.

Sección 4. Reafirmación de conocimientos

- Se realiza un repaso de las recomendaciones sugeridas mediante un juego, página web o aplicación.

- Se invita a todos los participantes a que lleven a la práctica las recomendaciones durante al menos 1 semana para que posteriormente nos cuenten su experiencia.

Durante la sesión se atenderán dudas sobre conceptos teóricos que se manejaron a lo largo de la concientización, así como también se dará una lista de aplicaciones educativas que los niños pueden utilizar para entretenerse y aprender al mismo tiempo, y así el dispositivo móvil sea una herramienta en lugar de solo una distracción.

Terminada la sesión se dará un plazo de dos semanas para que tanto padres como niños apliquen lo aprendido, al término del plazo se hará un pequeño "examen" con el que se pueda medir en nivel de aprendizaje de las recomendaciones, además de poder medir que impacto tuvo el plan y se de una retroalimentación de lo que se puede mejorar.

Sección 5. Evaluación y retroalimentación

La evaluación del impacto causado por el plan de concientización se realiza mediante la división de las recomendaciones en los dos rubros principales que aborda la tesina: Uso del dispositivo móvil y uso de redes sociales. Se dividen todas las recomendaciones propuestas en estos dos rubros para que cada participante del grupo piloto indique la siguiente información a partir del desglose de los temas de manera puntual lo siguiente:

- Cuáles de las recomendaciones ha aplicado a partir de que le fueron recomendadas.
- Cuáles le parecen complicadas de aplicar o sin sentido.
- Si al utilizar esa recomendación siente mayor confianza y seguridad mientras el menor utiliza el dispositivo.
- Que no le gustó del plan.

El cuestionario que se realizará se encuentra en el Anexo 5.

5.1.2 Desarrollo del material

En esta parte se definen los temas a abordar durante la implementación del plan, así como el desarrollo de todo el material a emplear para llevar a cabo lo detallado durante el diseño. Está conformado por las tareas de:

Selección de temas

Se seleccionaron los siguientes temas para ser abordados durante la concientización:

- Uso de contraseñas, un pequeño cambio hace la diferencia
- Antivirus, descarga de aplicaciones y conectividad a redes publicas
- Privacidad, cuídate a ti mismo y a los que te rodean
- Ciberbullying, ni victima ni victimario
- Supervisión, reglas para el uso de internet y control parental, no los dejes solos
- Dispositivo móvil para la educación, aprovecha la herramienta
- Comunicación padre-hijo-docente, la confianza es lo más importante
- Respeto

Fuentes y herramientas para el desarrollo del material

Se utilizan como fuentes de información:

- Videos de Youtube que serán mostrados en la sección 1 del plan.
- Recomendaciones de instituciones varias
- Herramientas de diseño y de desarrollo web
- Recomendaciones de la Policía Cibernética de la Ciudad de México en materia de Ciberseguridad.
- Recomendaciones desarrolladas por Walt Disney Company.
- Configuraciones de seguridad de las aplicaciones más populares que se describieron en el punto 4.3 “Políticas de seguridad de las principales aplicaciones y redes sociales”
- Información recabada en el capítulo IV respecto a normatividad en otros países del mundo ya que en México no existen aún.
- Se utilizan herramientas de desarrollo web, aplicaciones de diseño y edición de imagen y video.

Desarrollo del material

Se debe tener especial cuidado en el vocabulario que se utiliza y en la forma de presentar el material, ya que al ser dirigido para niños si el contenido es extenso, con palabras poco comprensibles y no llama su atención, será difícil que se enfoquen y que comprendan el mensaje que se trata de transmitir. Un elemento que no debe faltar en el desarrollo de temas y material son los colores y las imágenes.

En la figura 5.4 se muestra un prototipo de página web compatible con móviles que contiene toda la información proporcionada durante la aplicación del plan de concientización.

Tanto los niños como sus padres, podrán acceder en cualquier momento para reforzar y difundir los conocimientos que anteriormente se les proporcionaron.

La página está conformada de la siguiente manera:

Al iniciar, se muestran diferentes imágenes que ilustran ejemplos de algunas recomendaciones para los niños. Se decidió mostrar como primer plano imágenes ya que de ésta forma es más fácil llamar su atención.

En la parte superior derecha, encontraremos un link que nos llevará a la sección de "Controles", ésta sección está más enfocada a los padres ya que se dan a conocer las herramientas existentes de control parental. Del mismo lado, pero en la parte inferior aparecerán semanalmente las recomendaciones de mayor importancia, respecto a la seguridad en los dispositivos móviles y redes sociales.

La parte central de la página está dedicada totalmente a los niños, ya que nos lleva a actividades interactivas como por ejemplo juegos (sopa de letras, crucigramas, memoramas, etc) y acertijos, basados en las recomendaciones de seguridad que se les dio anteriormente.

Para finalizar, en la parte superior encontrarán una breve presentación del equipo que realizó el sitio y la página de Facebook en donde se estarán agregando continuamente nuevas recomendaciones, así como herramientas o tips que serán de ayuda para inculcar la cultura de la seguridad en dispositivos móviles y redes sociales.

Figura 5.3 Prototipo de página web en PC y en dispositivo móvil Anexo 4.

5.1.3 Implementación del plan

Se describe brevemente los canales y técnicas que se utilizan para hacer llegar el mensaje a la mayor cantidad de personas los contenidos de concientización del plan, así como la difusión qué se le va a dar tanto en escuelas con en lugares públicos a través de Internet.
Se conforma por las actividades:

Técnicas para entrega del material

Para la entrega del material se realizarán pláticas, exposiciones orientadas a padres e hijos, entrega de folletos y uso de medios digitales como son una página web y página de Facebook.

Difusión

La difusión es una actividad que se lleva a cabo antes, durante y después de la implementación del plan en un grupo del centro educativo.

El material será difundido mediante videos de youtube, posters en lugares muy visibles de la escuela, folletos con tips y sugerencias de páginas, página de Facebook con contenido relacionado a la seguridad del menor en la red, página de internet compatible con dispositivo móvil y app. En los medios digitales se realizará una actualización al menos 1 vez a la semana incluyendo nuevo material. Todos los carteles son en colores e imágenes llamativas con poca letra para mejor retención por parte de los menores.

Se tiene estimado que la página web sea de acceso desde cualquier dispositivo con internet para que puedan compartirla con personas que no hayan tomado la concientización de forma presencial.

5.1.4 Mantenimiento

Con la parte de mantenimiento, se realiza un seguimiento continuo para saber si se están presentando mejoras en las cuestiones de seguridad por medio de indicadores que forman parte importante de cualquier plan o modelo que se quiera tomar; sirven, como su nombre lo dice, para indicar qué desempeño ha tenido la iniciativa, puede ser un porcentaje, una cifra o un cualitativo que nos muestre el avance hasta determinado momento.

Esta parte ayuda a medir como estaban antes los padres e hijos y como se sienten y que piensan después de haber participado en la implantación del plan de concientización, de este modo conocer el impacto y mejorar las técnicas de desarrollo y difusión del material.

Capítulo VI. Caso Práctico

En este capítulo se aplica el plan diseñado en el capítulo cinco, se detalla el material entregado al Centro Educativo Melchor Muzquiz; también se explican las recomendaciones mediante carteles para los niños y los padres acerca del buen uso de los dispositivos móviles y redes sociales, basadas en la información recopilada por las encuestas y entrevistas, además de la investigación documental. Finalmente se hace una evaluación para conocer el impacto generado por las recomendaciones propuestas.

6.1 Entorno de Aplicación

El plan de concientización se aplica en el Centro Educativo Melchor Muzquiz ubicado en calle Capiro #312 en Ciudad Nezahualcóyotl Estado de México. Dado que la escuela es el segundo lugar donde los niños pasan más tiempo y además donde se hacen de una formación básica, se considera a las escuelas como el escenario idóneo para realizar la concientización.

6.2 Aplicación del Plan de Concientización

Tomando en cuenta el modelo definido en el capítulo cinco, se desarrolla cada una de las partes del modelo aplicándolas al centro de estudios.

Sección 1. Información de riesgos al usar dispositivos móviles

Se muestra los siguientes Videos, dirigidos a los padres:

Se hace un experimento social donde se crea un perfil falso el cual se usa para contactar a niñas pidiéndoles que se vean en algún lugar.

Se muestra los peligros que conlleva el subir fotos a internet.

El video muestra de una manera cómica lo que se denomina como sexting y el riego que existe en compartir fotos personales.

Video que explica el grooming y la manera en que pueden contactar a los menores.

Se dan recomendaciones básicas para el uso de internet y redes sociales.

Al término de la sesión los padres reaccionaron a los videos y empezaron a interesarse en la manera de evitar que les sucediera a sus hijos lo que vieron, también comenzaron a hacer preguntas para saber si podían controlar las páginas que visitan los menores al navegar en internet.

Se muestra los siguientes Videos, dirigidos a los niños:

Video que muestra el peligro que existe en las redes sociales y como combatirlo.

Las cosas que podemos hacer en internet.

Después de ver los videos los niños preguntaron acerca de lo que podían y no podían hacer a la hora de ocupar un dispositivo móvil, algunos comentaron que si hacían lo que decía el video o que les había pasado algo similar sobre todo en el caso de las redes sociales. Lo preocupante es que la mayoría no sabe qué hacer en esos casos y no consultan a un adulto, sino que toman su propia decisión y terminan por aceptar o dar información personal.

La figura 6.1 es un volante que se reparte a todos los padres de los menores después de mostrarles los videos, con esto se dan de forma breve las recomendaciones más importantes que se busca reforzar.

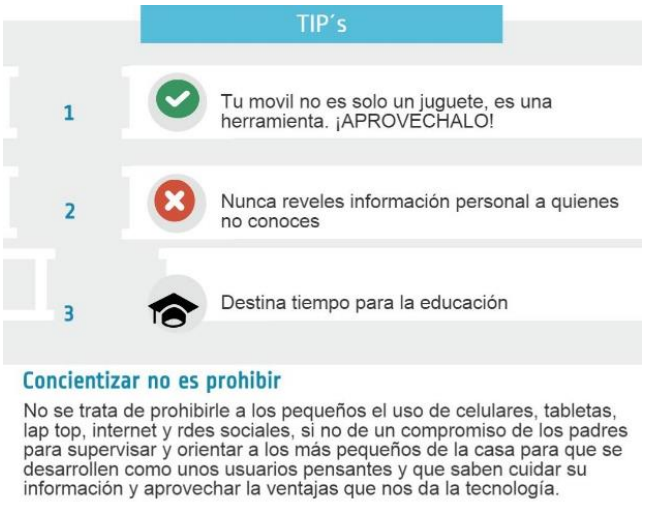


Figura 6.1 Poster “Recomendaciones”, se incluye en Anexo 3.

Sección 2. Recomendaciones de seguridad

Al presentar las recomendaciones los padres comentaron que sí tenían conocimiento de las recomendaciones, pero no sabían cómo aplicarlas, la mayoría solo utiliza los dispositivos móviles para comunicarse, entrar a facebook o entretenerse.

En cuanto a los menores no tenían conocimiento de la mayoría de las recomendaciones, solo usan los dispositivos móviles como les han indicado sus padres.

Adicional se entregó carteles a la escuela con las principales recomendaciones tanto para menores como para sus responsables la cual viene en la figura 6.1

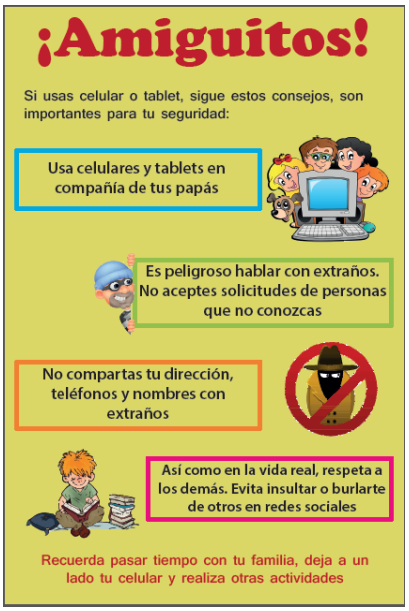


Figura 6.2 cartel dirigido a los menores.

Sección 3. Material referente al control parental

A la hora de hablar de control parental la mayoría de los padres no conocía el concepto y por lo tanto no hacía uso de este, al concluir con la explicación y los ejemplos del control parental varios padres decidieron implementar dicho control principalmente por la restricción de los horarios y la restricción de las páginas o poder ubicar a sus hijos. Aunque existen varias aplicaciones, para la mayoría se debe comprar una licencia y así poder aprovecharlas al 100%; éste punto no les agradó, pero de igual forma estuvieron muy interesados por adquirir algún programa para el control parental.

Sección 4. Reafirmación de conocimientos

Se les invitó a los padres y menores que visiten la página web creada www.mary5015.wix.com/planconcientizacion y la página en Facebook para que sigan aprendiendo más recomendaciones. Se les pidió que siguieran las recomendaciones dadas por al menos una semana.

También se aclararon dudas sobre conceptos técnicos que se mencionan, a lo cual se tuvieron muchas dudas sobre conceptos que se manejan cotidianamente en el área de tecnología, como por ejemplo el significado de aplicación, software, virtual, etc.

La figura 6.3 contiene un prototipo de cartel que se utiliza como medio de difusión en complemento con la página web y el perfil de Facebook. Este material se coloca en lugares muy visibles del centro educativo.

Figura 6.3 Poster “Familia”, se incluye en Anexo 2.

Sección 5. Evaluación y retroalimentación

Se les aplica un pequeño cuestionario a los padres para medir el impacto que tuvo el plan a lo cual se obtuvieron los siguientes resultados:

- Un 90 % aplicó las recomendaciones.
- La mayoría de los menores y padres aplicaron mínimo el 80% de las recomendaciones.
- Los niños se adaptaron rápido al cambio
- Un 90 % de los padres quieren seguir aplicando las recomendaciones y aprender más.
- Se obtuvieron muchas propuestas de ampliar el plan para abarcar más aspectos de seguridad.

Ventajas y desventajas

Entre las ventajas del plan se tiene que es aplicable en cualquier escuela de cualquier sector de la población o incluso poder llegar a difundirlo de manera digital para que llegue a más personas, siempre y cuando se cumpla con aplicarlo a menores de entre 5 y 11 años de edad. Otra de las ventajas es que el plan, no solo sirve para los niños sino también se ven beneficiados los responsables del menor ya que ellos son los que deben de hacer cumplir las recomendaciones dadas en el plan y por lo tanto lo pueden aplicar a más menores que conozcan.

Por otra parte, entre las desventajas se tiene que es muy fácil que los niños caigan en distracciones, lo cual hace que las recomendaciones no sean aplicadas tal cual como se dijeron. Respecto a los padres, no les agradó la idea que la mayoría de herramientas de control de parental sean de paga, lo cual representa una desventaja porque no están dispuestos a comprarla y por lo tanto no la usarían.

Conclusiones

Como resultado de la investigación documental y de campo llevada a cabo para el desarrollo del plan de concientización orientado a usuarios de dispositivos móviles y redes sociales en edad infantil, se observa que actualmente existe mucha información relacionada al uso de dispositivos móviles y redes sociales por parte de menores, sin embargo, en México no existen muchas iniciativas que apoyen a que los menores sean conscientes y tengan conocimientos para tener seguridad de su información. Es decir, la información existe y se tiene presente el problema que representa, pero no se realizan acciones para atacar el problema.

Con el estudio también se demuestra un panorama general de que éste es un problema no solo en México, sino en todo el mundo, aunque a diferencia de México, en algunos países ya se están tomando medidas más enfocadas en los niños.

Con el plan de concientización propuesto se ataca directamente el problema ya que apoya a la concientización de niños desde la escuela y el hogar para que en conjunto con padres de familia y docentes se haga frente a los riesgos a los que se exponen los menores al hacer uso de dispositivos móviles y redes sociales, dándoles además herramientas para sacar más provecho de esta tecnología y que no sirva simplemente de entretenimiento y distracción.

Se concluye que el plan de concientización para usuarios de dispositivos móviles y redes sociales en edad infantil cumplió con el objetivo de concientizar en el uso responsable de los dispositivos móviles y redes sociales, de acuerdo a los resultados obtenidos los padres estuvieron muy interesados en conocer los riesgos y en conocer de qué forma pueden proteger a los pequeños.

Los padres ahora conocen y son conscientes de los riesgos a los que se exponen en internet y en las aplicaciones que más usan (redes sociales) como Facebook o YouTube y los niños toman con mayor responsabilidad el uso de sus equipos.

Finalmente, para mejorar la aplicación del modelo de concientización aplicado se considera que se puede trabajar en conjunto con un especialista en educación de menores para que les ideas planteadas puedan ser transmitidas de una forma más adecuada.

Bibliografía

Ardila, Ignacio (2013). *COLOMBIA: Penetración del 100% en telefonía celular y del 30% en smartphones*. Recuperado el 18 de noviembre de 2015, de http://www.revistapym.com.co/noticias/marketing-movil/colombiapenetracion-100-telefonia-celular-30-smartphones

Asociación Mexicana de internet (2015).*Hábitos del Internauta Mexicano.* Recuperado el 19 de noviembre de 2015, de https://amipci.org.mx/images/AMIPCI_HABITOS_DEL_INTERNAUTA_MEXICANO_2015.pdf

Barranco Fragoso, Ricardo (2012). *¿Qué es Big Data?* Recuperado el 18 de noviembre de 2015, de www.ibm.com/developerworks/ssa/local/im/que-es-big-data

Butler, Brandon (2013). *Los 10 mejores proveedores de almacenamiento en la nube, según Gartner.* Recuperado el 18 de noviembre de 2015, de http://www.pcworld.com.mx/Articulos/27313.htm

Calvopiña Ponce, Johnn (2012). *¿Qué es una aplicación informática?* 2012 Recuperado el 28 de noviembre de 2015, de http://johnnjc.blogspot.mx/2012/04/que-es-una-aplicacion-informatica.html

CNN México (2011). *Consejos que deben seguir los niños para evitar riesgos en Internet.* Recuperado el 19 de noviembre de 2015, de http://mexico.cnn.com/nacional/2011/11/23/10-consejos-que-deben-seguir-los-ninos-para-evitar-riesgos-en-internet

Comisión Nacional de Seguridad, (2015). *Ciberseguridad.* Recuperado el 19 de noviembre de 2015, de http://www.cns.gob.mx

Condusef.gob.mx, (2014). *Protege tu Identidad.* Recuperado el 19 de noviembre de 2015, de http://www.condusef.gob.mx/Revista/index.php/usuario-inteligente/consejos/307-protege-tuidentidad

Curiosidades Históricas (2015). Recuperado el 28 de noviembre de 2015, de http://www.erroreshistoricos.com/curiosidades-historicas/888-la-teoria-de-los-seis-grados-de-separacion.html

Del Carmen Trejo García, Elma (2006). *Regulación Jurídica de Internet*. Recuperado el 28 de noviembre de 2015, de http://www.diputados.gob.mx/sedia/sia/spe/SPE-ISS-12-06.pdf

DELL (2012). *Ventajas y desventajas de la informática en la nube para las pequeñas empresas*. Recuperado el 18 de noviembre de 2015, de http://www.dell.com/learn/co/es/cobsdt1/sb360/sbnewsletter-3-2012-2

El Financiero (2015). *Alertan sobre uso de internet libre en escuelas*. Recuperado el 28 de noviembre de 2015, de http://www.elfinanciero.com.mx/tech/alertan-sobre-uso-de-internet-libre-en-escuelas.html

Emol (2014). *Chile está entre las naciones emergentes con mayor uso de internet y telefonía móvil* Recuperado el 8 de diciembre de 2015, de http://www.emol.com/noticias/tecnologia/2014/02/13/644734/chile-esta-entre-las-naciones-emergentes-con-mayor-uso-de-internet-y-telefonia-movil.html

Instituto Nacional de Ciberseguridad, (2010). *Menores y Redes Sociales*. Recuperado el 28 de noviembre de 2015, de https://www.incibe.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/Menores_y_redes_sociales

Islas, Octavio y Ricaurte, Paola (2013). I*nvestigar las redes sociales.* Recuperado el 19 de noviembre de 2015.

Manpower, insurgentes sur. 688 piso 3, col. del valle. México D.F. 03100 tel: (52 55) 54 48 14 67 tel: 01 800 451 1400 www.manpower.com.mx

Ministerio de Justicia y derechos humanos, argentina (2000), *Protección de los datos personales* recuperado el 19 de noviembre de 2015, de http://www.jus.gob.ar/media/33481/ley_25326.pdf

Pan, Ignacio (2013), *Cómo es el perfil del usuario argentino de internet,* recuperado el 19 de noviembre de 2015, de http://www.infobae.com/2013/10/30/1520229-como-es-el-perfil-del-usuario-argentino-internet

PULSO, Diario de San Luis Potosí (2015). *Aumenta uso de dispositivos móviles en niños mexicanos de dos años*. Recuperado el 18 de noviembre de 2015, de

http://pulsoslp.com.mx/2015/07/01/aumenta-uso-de-dispositivos-moviles-en-ninos-mexicanos-dedos-anos/

Sánchez, María Alejandra (2015). *Penetración de redes sociales en Colombia alcanza 71% y es la quinta de la región*. Recuperado el 18 de noviembre de 2015, de http://www.larepublica.co/penetraci%C3%B3n-de-redes-sociales-en-colombia-alcanza-71-y-es-laquinta-de-la-regi%C3%B3n_284276

Tazza, Alejandro (2014). *El delito de grooming* recuperado el 19 de noviembre de 2015, de http://penaldosmdq.blogspot.mx/2014/04/el-delito-de-grooming-art-131-cod-penal.html

Tecnosfera (2015). *Dispositivos móviles cambian la forma de hacer negocios en el país*. Recuperado el 18 de noviembre de 2015, de http://www.eltiempo.com/tecnosfera/novedadestecnologia/uso-de-celulares-transformaron-la-forma-de-hacer-negocios-en-colombia/15372015

Texto: María Luisa Santillán Gráfico: Salvador Gutiérrez Dirección general de divulgación de la ciencia / cienciaunam@unam.mx

Tomeo, Fernando (2012). *La usurpación de identidad en la era digital* recuperado el 19 de noviembre de2015, de http://gestionpublica.info/sociedad-detalles-noticias/items/la-usurpacion-de-identidad-en-la-era-digital.html

UNAM (2015). *Tutorial de Seguridad Informática*. Recuperado el 28 de noviembre de 2015, de http://redyseguridad.fi-p.unam.mx/proyectos/tsi/capi/Cap2.html

Glosario

Aplicación: Software que se instala en dispositivos móviles o tablets para ayudar al usuario en una labor concreta, ya sea de carácter profesional o de ocio y entretenimiento.

Banco de datos: Bancos de información que contienen datos relativos a diversas temáticas y categorizados de distinta manera, pero que comparten entre sí algún tipo de vínculo o relación que busca ordenarlos y clasificarlos en conjunto.

Bluethoot: Especificación industrial para Redes Inalámbricas de Área Personal (WPAN) que posibilita la transmisión de voz y datos entre diferentes dispositivos mediante un enlace por radiofrecuencia.

Bullying: Acoso físico o psicológico al que someten, de forma continuada, a un alumno sus compañeros.

Chat: También conocido como cibercharla, designa una comunicación escrita realizada de manera instantánea mediante el uso de un software y a través de Internet entre dos, tres o más personas.

Ciberbullying: Uso de los medios telemáticos (Internet, telefonía móvil y videojuegos online principalmente) para ejercer el acoso psicológico.

Comunidad virtual: Espacios en Internet destinados a facilitar la comunicación entre los miembros del grupo al que pertenecen y que se encuentran en distintos puntos geográficos.

Concientización: Implica hacerle tomar conciencia a una persona sobre determinas circunstancias, fenómenos, elementos de su personalidad o actitud, para mejorar su calidad de vida.

Control Parental: Programas informáticos que permiten controlar y bloquear el acceso a distintos contenidos en diversos dispositivos como los móviles, ordenadores, televisores, tabletas o videoconsolas.

Dispositivos móviles: Aparato de pequeño tamaño, con algunas capacidades de procesamiento, con conexión permanente o intermitente a una red, con memoria limitada, que ha sido diseñado específicamente para una función, pero que puede llevar a cabo otras funciones más generales.

GPS: Sistema de Posicionamiento Global de navegación y localización mediante satélites.

Grooming: Forma de acoso y abuso hacia niños por medio de internet.

Hacking: Término con el cual se refiere a la re-configuración o re-programación de un sistema, de una forma no prevista originalmente por el propietario, el administrador o el diseñador.

Hipervínculo: (También llamado enlace, vínculo, hiperenlace o link) es un elemento de un documento electrónico que hace referencia a otro recurso, como por ejemplo otro documento o un punto específico del mismo o de otro documento.

Ingeniería social: Práctica de obtener información confidencial a través de la manipulación de usuarios legítimos.

Internautas: Describir a los usuarios habituales de Internet o red.

ISO: La Organización Internacional de Normalización

Link: Elemento de un documento electrónico que permite acceder automáticamente a otro documento o a otra parte del mismo.

Mensajería instantánea: Forma de comunicación en tiempo real entre dos o más personas basada en texto, también conocida como chat.

Microblogging: También conocido como nanoblogging, es un servicio que permite a sus usuarios enviar y publicar mensajes breves, generalmente solo de texto.

Multimedia: Difusión por varios medios de comunicación combinados, como texto, fotografías, imágenes de video o sonido, generalmente con el propósito de educar o de entretener.

Navegador: Programa que permite navegar por internet u otra red informática de comunicaciones.

Navegar. Desplazarse de una página o documento a otro en una red informática, como Internet, a través de ciertos vínculos preestablecidos.

Nube: Trata de un servicio que funciona a través de internet que permite a los usuarios guardar información cualquier tipo: música, videos, en General y poderlos tener alojados en servidores dedicados.

Offline: Fuera de línea o red.

On-line: Que está disponible o se realiza a través de internet.

Página web: Documento que forma parte de un sitio web y que suele contar con enlace.

Perfil: Término usado en redes sociales para describir la página personal del usuario/a.

Petabytes: Unidad de medida informática que equivale a 1024 Terabytes.

Pishing: Técnica de ingeniería social utilizada por los delincuentes para obtener información confidencial.

Plataforma: Un sistema operativo, un gran software que sirve como base para ejecutar determinadas aplicaciones compatibles con este.

Publicaciones: Se refiere a la acción usada en redes sociales para compartir contenido multimedia en las mismas por medio de una conexión a internet.

Red (Informática). Conjunto de computadoras y otros equipos interconectados, que comparten información, recursos y servicios.

Red Social. Página web en la que los internautas intercambian información personal y contenidos multimedia de modo que crean una comunidad de amigos virtual e interactiva.

Remailers: Servidor que recibe correos electrónicos en un formato especial, los procesa eliminando las cabeceras, y los dirige hasta el destinatario del mensaje.

Rol: Función o papel que cumple alguien o algo.

Sexting: Envío de mensajes, fotos o videos de contenido sexual por medio de teléfonos celulares.

Sistema informático: Sistema que permite almacenar y procesar información; es el conjunto de partes interrelacionadas: hardware, software y personal informático.

Smartphone o teléfonos inteligentes: Teléfono celular (móvil) que ofrece prestaciones similares a las que brinda una computadora (ordenador) y que se destaca por su conectividad.

Software: Conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas.

Spam: Correo electrónico no solicitado que se envía a un gran número de destinatarios con fines publicitarios o comerciales.

Tablets o tabletas: Dispositivo electrónico que tiene un tamaño intermedio entre el ordenador y el móvil.

Terabytes: Unidad de medida informática que equivale a 1024 Gigabytes.

Virus: Programa de computadora confeccionado en el anonimato que tiene la capacidad de reproducirse y transmitirse independientemente de la voluntad del operador y que causa alteraciones más o menos graves en el funcionamiento de la computadora.

WiFi: Mecanismo de conexión de dispositivos electrónicos de forma inalámbrica.

Anexos

Anexo 1. Cuestionario para niños sobre hábitos de uso de dispositivos móviles y redes sociales.

Instituto Politécnico Nacional

UPIICSA

"Uso de dispositivos móviles en edad infantil"

Buenos días (tardes).

Somos alumnos del Instituto Politécnico Nacional (IPN) y estamos trabajando en una investigación que servirá para conocer los hábitos que tienen actualmente los niños entre 5 y 10 años respecto al uso de dispositivos móviles (teléfonos inteligentes, tabletas, computadora portátil).

Te pedimos de tu apoyo para responder una serie de preguntas relacionadas a la investigación, toda la información recolectada será confidencial y anónima y únicamente será utilizada con fines de estudio.

Agradecemos contestes lo más claro posible, en caso de que tengas dudas pregunta a la persona que te proporcionó el cuestionario.

Muchas gracias por tu tiempo y apoyo.
Edad _____ Niño ___ Niña ____

1.- ¿Utilizas algún dispositivo móvil?

a) Sí b) No

¿De quién es?

2.- De los siguientes dispositivos, indique con cuales y cuantos cuenta.

a) Laptop ___
b) Teléfono inteligente ___
c) Tableta ___
d) Otro, especificar cuál _____

3.- ¿Cuál es el principal uso que le das a tu dispositivo móvil?

a) Entretenimiento (música, videos, imágenes, juegos)
b) Comunicación (llamadas y mensajes sms)
c) Educación y aprendizaje (búsqueda de información en internet)
d) Redes sociales (mensajería instantánea, publicación de fotos y videos, comentarios)

4.- ¿Cuánto tiempo le dedicas al día al uso de tu dispositivo móvil?

a) Menos de una hora
b) De 1 a 2 horas
c) de 2 a 3 horas
d) de 3 a 5 horas
e) más de 5 horas. Especificar un aproximado _____

5.- De los siguientes “iconos” marque con una ‘X’ cuales has usado

6.- --Dependiendo de la respuesta, describir las actividades que realizan en cada una de las seleccionadas y cuánto tiempo suele dedicarle—

7.- ¿Accedes a alguna red social o juego en el que convivas con otras personas en la red?

a) Sí b) No

8.- ¿Tienes entre tus contactos a personas que no conozcas?

a) Sí b) No

9.- ¿Alguna vez esas personas que no conoces te han pedido que los veas en algún lugar?

a) Sí b) No

10.- ¿Has accedido en alguna ocasión?

a) Sí b) No

11. ¿Conoces algunas recomendaciones de seguridad para tu dispositivo móvil?

a) Sí b) No c) ¿Cuáles?

12.- ¿Has compartido contraseña con alguien?

a) Sí b) No

13.- ¿Con quién?

14.- ¿Tus padres conocen tus contraseñas?

a) Sí b) No

15.- Cuando navegas en internet, o utilizas el móvil. ¿Eres supervisado por algún adulto?

a) Sí b) No

16.- Cuando no estas con algún adulto ¿Has utilizado el dispositivo móvil?

a) Sí b) No

17.- ¿Alguna vez has realizado compras por internet?

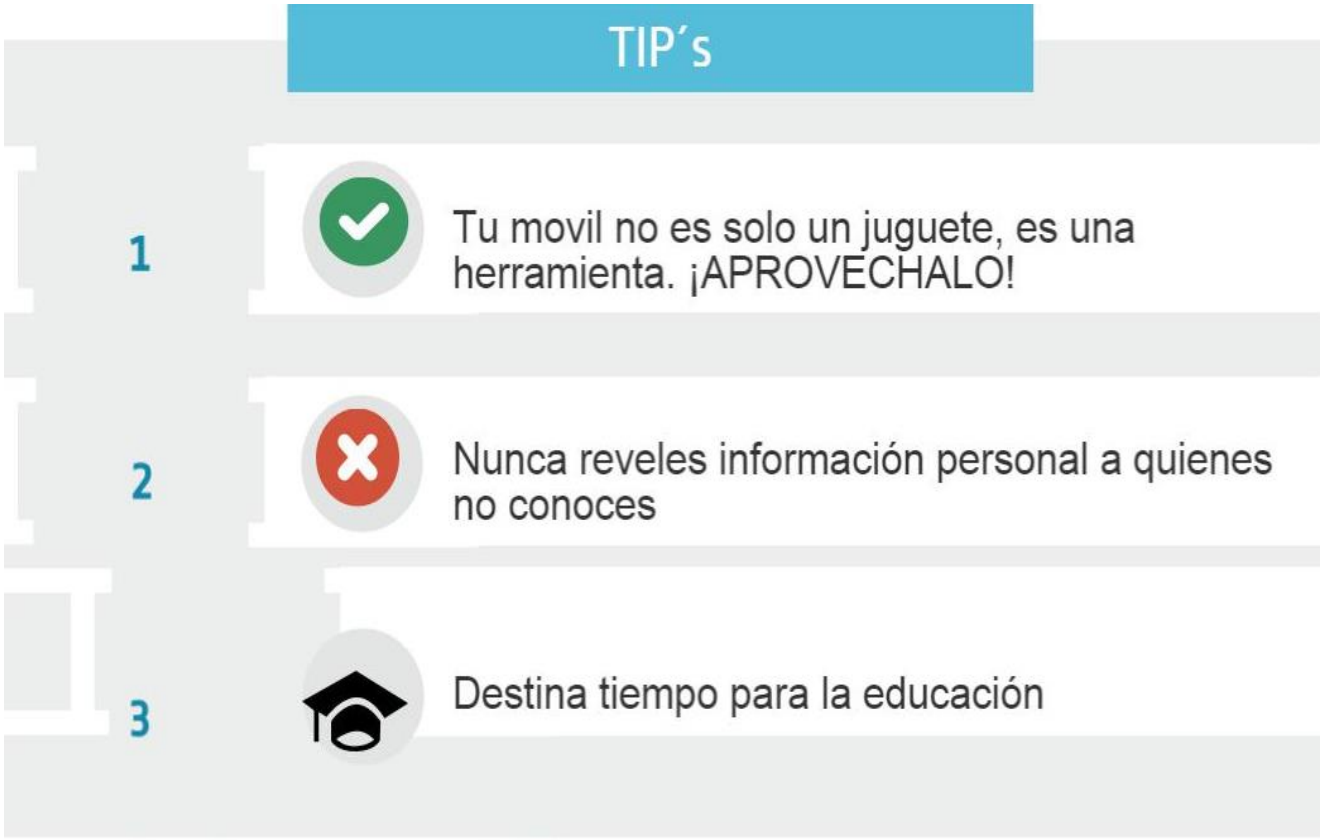
a) Sí b) No

Nuevamente agradecemos su tiempo para responder.

Hasta luego! ☺

Anexo 2. Poster “Tu familia”

Anexo 3. Poster "Recomendaciones".



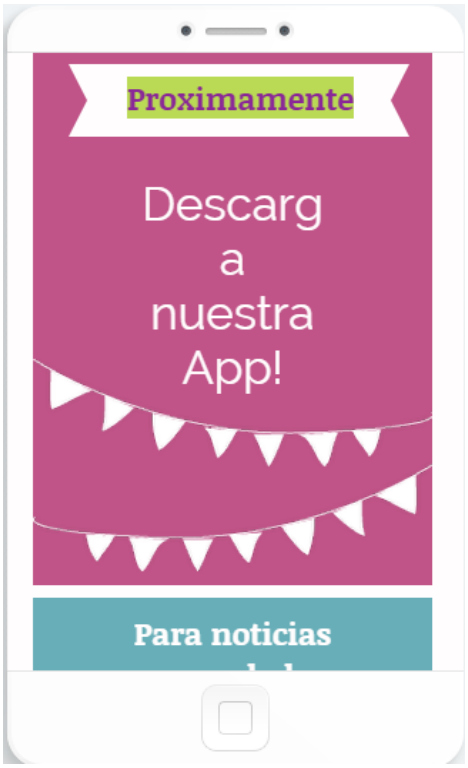
Concientizar no es prohibir

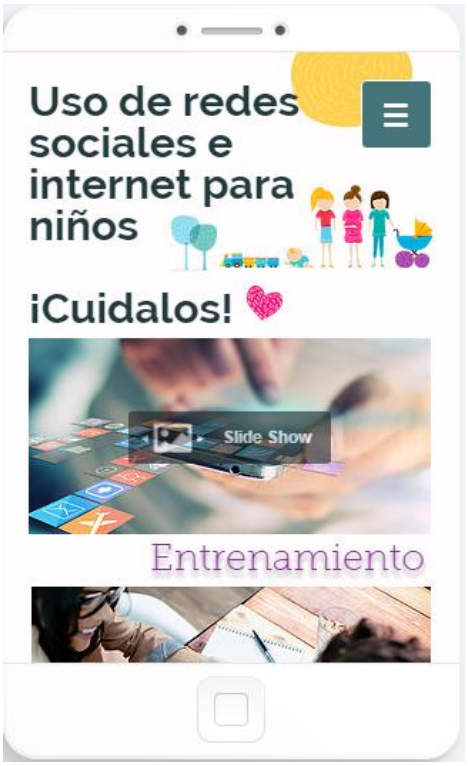
No se trata de prohibirle a los pequeños el uso de celulares, tabletas, lap top, internet y rdes sociales, si no de un compromiso de los padres para supervisar y orientar a los más pequeños de la casa para que se desarrollen como unos usuarios pensantes y que saben cuidar su información y aprovechar la ventajas que nos da la tecnología.

Anexo 4. Prototipo de la aplicación.

Pantalla versión PC

Prototipo pantalla versión móvil





Anexo 5.

Cuestionario de evaluación.

Instituto Politécnico Nacional

UPIICSA

"Uso de dispositivos móviles en edad infantil"

Agradecemos el tiempo invertido en aplicar las recomendaciones respecto al uso de los dispositivos móviles e internet en tu hogar, por ultimo te pedimos contestar las siguientes preguntas con el fin de saber si estas recomendaciones son de utilidad para tu hogar.

Siente la confianza de responder en absoluta libertad y sinceridad, recuerda que los resultados son datos para nuestra investigación.

1.- ¿Aplicaste las recomendaciones del plan que te fue entregado?

a) Si b) No

2.-De ser la pregunta anterior afirmativa, ¿En qué porcentaje consideras que seguiste las recomendaciones del plan?

a) 10% b) 30% c) 50% d) 70% e) 100%

3.- Tus hijos obedecieron a tus consejos y medidas preventivas

a) Si b) No

4.-De ser la pregunta anterior afirmativa, ¿En qué porcentaje consideras que tus hijos se adaptaron?

a) 10% b) 30% c) 50% d) 70% e) 100%

5.- ¿Notaste algún cambio en su comportamiento y nivel de desempeño en general de tus hijos al seguir estas recomendaciones?

a) Si b) No ¿Por qué?

6.- ¿Consideras un beneficio el plan que te fue entregado?

a) Si b) No ¿Por qué?

7.- ¿Consideras seguir las recomendaciones descritas en el plan, posterior a este periodo de prueba de estudio que ha concluido?

a) Si b) No ¿Por qué?

8.- Tu opinión es muy importante para nosotros, en general como calificarías este plan de recomendaciones para el uso de dispositivos móviles e internet en niños

a) Malo b) Regular c) Bueno d) Muy bueno

9.- ¿Recomendarías este plan de recomendaciones para el uso de dispositivos móviles e internet en niños?

a) Si b) No ¿Por qué?

10.- ¿Que recomendarías que podríamos cambiar/implementar en esta iniciativa?

Gracias de antemano por tu tiempo al contestar esta encuesta de satisfacción, te recordamos que la seguridad de los niños en cualquier circunstancia es primordial, te invitamos a seguir con estas recomendaciones en adelante, ya que con ello podremos disminuir riesgos, peligros y daños sociales, morales y físicos que se encuentran expuestos los niños en el mundo de las redes sociales e internet.