Universidad Autónoma del Estado De México
Centro Universitario UAEM Texcoco

"PREVENCIÓN DEL ROBO DE DATOS PERSONALES MEDIANTE APPS DE REDES SOCIALES"

Que para obtener el título de

Licenciada en Informática Administrativa

T E S I N A

Presenta

Carina Islas Zamora

Director (a)

M. en C.C. Ana Luisa Martínez Ávida

Revisores(as)

M. en Ed. Janet Espinoza Pérez

M. en A. María del Rosario San Martín Gamboa

Texcoco, Estado de México a 6 de junio 2018

Universidad Autónoma del Estado de México
Centro Universitario UAEM Texcoco

Texcoco, México a 17 de Abril del 2018

Asunto: Etapa de digitalización

M. EN C. ED. VIRIDIANA BANDA ARZATE
SUBDIRECTORA ACADEMICA DEL
CENTRO UNIVERSITARIO UAEM TEXCOCO
PRESENTE.

AT´N: M. EN C. LETICIA ARÉVALO CEDILLO
RESPONSABLE DEL DEPARTAMENTO DE TITULACION

Con base en las revisiones efectuadas al trabajo escrito titulado "Prevención del robo de datos personales mediante apps de redes sociales" que para obtener el título de Licenciado en Informática Administrativa presenta el (la) sustentante Carina Islas Zamora, con número de cuenta 1015022, se concluye que cumple con los requisitos teórico-metodológicos por lo que se le otorga el voto aprobatorio para su sustentación, pudiendo **continuar con la etapa de digitalización** del trabajo escrito.

ATENTAMENTE

Mtra. Edu. Janet Espinoza Perez
NOMBRE Y FIRMA DEL REVISOR

M. en A. María del Rosario San Martín
NOMBRE Y FIRMA DEL REVISOR

M. en C. C. Ana Luisa Martínez Avila
NOMBRE Y FIRMA DEL DIRECTOR

TITULACION
RECIBIDO
Por
Texcoco, Méx., a 17 de Abril de 18

c.c.p. Sustentante:
c.c.p. Director de trabajo terminal:
c.c.p. Titulación.- M. EN C. LETICIA ARÉVALO CEDILLO

Centro Universitario UAEM Texcoco
Av. Jardín Zumpango s/n. Fracc. El Tejocote
C.P. 56259 Texcoco, Estado de México.
Tels. (595) 9211216 - 9211247 - 9210368 - 9210493
e-mail: cutex.uaem@gmail.com

CUTex

“El mayor enemigo del conocimiento no es la ignorancia, sino la ilusión del conocimiento”

— Stephen Hawking

Agradecimientos

A mi madre Angélica quien admiro, siempre me apoyó, comprendió, orientándome con sus consejos dando lo mejor de ella para que yo entendiera que todo era por mi bien, no alcanzarían las palabras para decirte gracias por todos los esfuerzos, sacrificios. Gracias por el amor sin límites, por prepararme para el mundo.

A mi padre Lucio quien con todos sus sacrificios y esfuerzo saco una familia adelante teniendo la fortaleza de cuidar de la misma, siempre tan responsable, a tu lado nunca pase por ninguna necesidad siempre tuve lo suficiente para crecer y vivir en plenitud. El cansancio sobre tus hombros no impidió pasar momentos felices ciertamente gracias a tu trabajo y apoyo pude estudiar una carrera.

A mi directora de Tesina la maestra Ana Luisa Martínez Ávida le agradezco sinceramente quien es ejemplo a seguir como profesionista y como mujer, transmitió su conocimiento desde mis primeros pasos en aula de clases hasta hoy como directora donde se ven los frutos de aprovechados en el presente trabajo de investigación.

A mis revisoras las maestras Rosario San Martín Gamboa y Janet Espinoza Pérez quienes son unas maestras dedicadas a su profesión. Por darme su apoyo, la entrega de tiempo y compromiso, orientarme con mis dudas y sus aportaciones de conocimientos en esta tesina.

Al maestro Martin Alonso Jafet González Medina por la dedicación de su tiempo, la enseñanza de su conocimiento y los consejos brindados.

A mis amigas quienes formaron parte en las aulas de clases.

Kenia A. Santamaría García siempre me apoyo, dio sus mejores motivaciones, auxilio en materias, gracias por tu amistad la valoro mucho.

Gisela A. Colexcua Espinosa gracias por tu tiempo en darme asesorías, apoyo, amistad y consejos.

Elizabeth Angeles Velázquez mi amiga desde la preparatoria decidimos estudiar diferentes carreras sin embargo no nos impidió seguir con nuestra amistad, gracias por tu apoyo, consejos, escucharme y estar en los mejores y peores momentos.

A Martín A. López Herrera gracias por el apoyo en la vida estudiantil, has estado conmigo en los momentos difíciles, desarrollar esta investigación no fue fácil aun así me motivaste y orientaste. Haces grandes aportaciones en mi vida.

INDICE

INDICE DE ILUSTRACIONES

INTRODUCCIÓN

La presente investigación tiene como objetivo identificar las condiciones presentadas en el robo de datos personales por medio del uso de Apps de redes sociales, al mismo tiempo promover la información de lo valioso que son los datos personales así como analizar de lo que se comparte día con día en las redes sociales mediante las apps. Recopilando información de diferentes investigaciones, así como artículos y algunos libros.

Desarrollando cuatro capítulos en su contenido mostrando la información con los respectivos conceptos básicos junto con su categoría para tener un mejor panorama entendiendo su importancia y utilidad.

En primer lugar se encuentran los antecedentes de los delitos informáticos originados en estados unidos aproximadamente el año 1977, llegando a México en 1969 publicado en el Diario Oficial continuando con los antecedentes de la protección de los datos personales el 27 de abril del 2010. Considerando las estadísticas consultadas se muestra la cantidad de personas dueñas de un dispositivo con acceso a internet, así como la cantidad de aplicaciones móviles subidas, los resultados también muestran que en México internet es usado en su mayoría para acceder y enviar mensajes instantáneos a redes sociales como Facebook, WhatsApp, YouTube, Twitter e Instagram, sabiendo que las personas acceden a internet entablando en un mundo virtual donde cualquier dato puede ser usado como herramienta para la manipulación y extorción, algunos de estos pueden ser indicios para robar contraseñas de las mismas redes sociales llegando incluso a suplantar la identidad de una persona llevando a tener malos entendidos, como fraudes perdidas económicas este suceso puede ser una reacción en cadena, es recomendable al ingresar a una cuenta siempre tener una autentificación y controles de acceso para una mejor integridad de los datos.

El desarrollo de la investigación muestra conceptos básicos para tener un mejor panorama, en el capítulo I se encuentran los conceptos, que es un dato personales seguido de sus categorías como son: los de identidad, trabajo, patrimonio entre otros más, junto con la regularización legal los protege, continuando con la intimidad, delitos informáticos con sus categorías y posibles amenazas;

Por ejemplo: espionaje, suplantación, análisis de tráfico, luego se encuentra la definición de App con sus tipos y categorías algunas de ellas son: Aplicaciones nativas, web, hibridas, apps de entretenimiento, sociales, educativas e informativas, etc.

Seguido del concepto de Red social con sus respectivas categorías algunas de ellas son: Redes sociales horizontales, verticales y otras más, luego se define lo que es la identidad y la identidad digital las cuales son muy importantes para las redes sociales y en la vida real, finalmente para terminar el capítulo I se encuentra usuario y sus tipos de usuario es decir: ultras, negociadores, esporádicos entre otros.

En el capítulo II llamado estándares de seguridad en app móviles se encuentran los permisos de acceso quienes son requeridos para acceso e instalación en el dispositivo, el objetivo de esto es para tener un mejor aprovechamiento para su correcta función, desde las tiendas, algunos ejemplos son la identidad, calendario, teléfono y otros más, continuando con el desarrollo del capitulo están las políticas de seguridad en ellas se estipula que los datos personales solicitados en contratos, formularios, aplicaciones, etc. Serán usados tratados y protegidos de acuerdo a lo establecido por la Ley, estas políticas tiene varias secciones las cuales deben ser leídas son: Seguridad y protección de datos personales, Responsabilidad de opiniones, Privacidad, Obtención de información están son solo algunas por mencionar, seguidamente se encuentran las políticas se seguridad es definir las expectativas de la app las cuales deben estar protegidas mediante una organización o empresa de seguridad, sus recursos así como las obligaciones.

Ya se había mencionado anteriormente la institución encarga de proteger los datos personales sin embargo también los protegen en posesión de apps de redes sociales en este apartado se describe más claro su función y sus secciones.

En otro término se despliega los aspectos legales de app móviles encontradas en diversas fuentes, resaltando la del Gobierno Digital Estándar quien brinda veintiocho criterios generales en los que se encuentran Logotipo de la dependencia, Versión de la app, Fecha de última publicación, Dueño de la app y otros más.

A su vez las amenazas de seguridad en app móviles exponiendo tanto en el software y el hardware.

Por su parte el capítulo III privacidad y seguridad en redes sociales da a saber la importancia de la configuración de las mismas, comenzando por la seguridad de los datos es decir su protección ante virus, malware es por eso que las apps de redes sociales se tienen que comprometer a garantizar la protección con los usuarios obteniendo así su confianza, incluye también la transparencia de datos de cuando el usuario quiere saber qué información tiene sobre él y que hacen con ella. Se da una parte del control y brindando transparencia en los datos aumenta la confianza en las redes sociales que proveen el servicio.

Otro aspecto a desarrollado es la privacidad de las redes sociales son usadas para diferentes objetivos ya sea compartir contenido, marketing, entrenamiento entre otros, esto a generando una gran cantidad de datos expuestos al momento en que se contestan campos como el estado civil, la ciudad de residencia, estudios.

Seguidamente se muestra algunas interfaces de las redes sociales más populares en los sistemas operativos con mayor demanda en el mercado.

Finalmente con el capítulo IV Recomendaciones y prevenciones al usuario, como su nombre lo dice son aspectos a considerar de todos los usuarios de redes sociales o fuera de ellas para revisar en que apps confían sus datos para evitar ser víctimas de los delitos informáticos, recordando la falta de seguridad que ya existe en las apps así como también el dejar a un lado las prevenciones renunciando a lógica de no brindar información a desconocidos.

ANTECEDENTES

En el 1983 en París, la OECD (Organización para la Cooperación y el Desarrollo Económicos) comenzó un estudio de las posibilidades de aplicar y concertar en el plano internacional las leyes penales para terminar con el uso ilícito de los programas computacionales llamado “Delitos de Informática: análisis de la normativa jurídica". (Checks, 2011).

Años más tarde el 13 de septiembre de 1989, se fundó el Comité Europeo para los Problemas de la Delincuencia, un nuevo comité de expertos para que llevaran todos los casos registrados en el tema de los delitos informáticos. Con el fin de combatir los delitos informáticos, principalmente en los que eran cometidos a través de las redes de telecomunicaciones (Garavilla, 2008).

En México los delitos informáticos se tomaron en cuenta el 17 de mayo de 1999, en las reformas que se dieron a conocer publicándolo en el Diario Oficial de la Federación ubicados dentro del Título Noveno: Delitos contra la vida y la integridad corporal, Título Octavo: Delitos contra la moral pública y las buenas costumbres, Título Séptimo: Delitos contra la salud, etc. al que se denominó “Revelación de Secretos y Acceso Ilícito a Sistemas” (Durán, 2017).

Mientras tanto la protección de datos personales comenzó naciones de primer mundo en Europa siendo uno de sus derechos más recientes aprobado el 7 de diciembre del 2000 establecido en el artículo 8° de la Carta de los Derechos Fundamentales de la Unión Europea.

Finalmente llego a la protección de datos personas a México el 27 de abril de 2010, con los miembros de Congreso de la Unión aprobaron la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, ubicando nuestro país entre los regímenes que protegen este tipo de derechos, propios de las democracias en el mundo (Asesor, 2011).

OBJETIVO GENERAL

Identificar las condiciones presentadas en el robo de datos personales por medio del uso de Apps de redes sociales mostrando los conocimientos básicos que debe saber un usuario para prevenir el robo de sus datos antes de descargar y usar las apps.

OBJETIVOS PARTICULARES

- Determinar los conocimientos básicos de prevención al delito de robo de datos que debe tener un usuario antes de descargar y usar una app.
- Mostar las políticas y privacidad de apps de redes sociales.
- Identificar las regulaciones legales para la protección del delito de robo de datos personales en México.
- Exponer las vulnerables del usuario en su compromiso al descargar y usar.

DEFINICIÓN DEL PROBLEMA DE INVESTIGACIÓN

Según estadísticas del INEGI (Instituto Nacional de Estadística y Geografía) en México 81 millones de personas tienen acceso a un teléfono celular y el 74.8 % obtuvieron un Smartphone (Anonimo, SDPnoticias.com, 2017). Se muestra en la población un aumento haciendo uso de la tecnología.

Considerando por el periódico universal, 65.5 millones de personas son usuarios en internet, por medios de estos resultado publicados se asume que la población mexicana ya tiene el hábito de estar conectado realizando distintas actividades ya sea laboralmente, de ocio, buscando información, conociendo personas, viendo películas, búsquedas de empleos, entre otras actividades (Islas, 2017).

Aproximadamente 16,000 aplicaciones móviles al día son publicadas en Play Store y Apple Store en su totalidad son 40,0000 en las tiendas, de todas las ya existentes y las nuevas se puede comprobar en su mayoría no han sido descargas debido a que son parecidas unas con otras, pero cuando si son descargadas y no son las apps originales es decir son clones, los criminales proceden al robo de datos incluyendo que al momento en que se descarga se aceptaron las políticas de privacidad de privacidad junto con los permisos de acceso en este momento se tiene que desinstalar la app y hacer un escaneo (Anonimo, Ayuda Ley Protecion de Datos, 2016).

En México el internet es usado acceder a redes sociales (83%), enviar y recibir mensajes instantáneos (77%). Facebook (95%) se mantiene como una de las redes más populares, en segundo puesto por WhatsApp (93%), YouTube (72%), Twitter (66%) e Instagram (59%), (Alonso Rebolledo Ruy, 2017); las estadísticas muestran los resultado de las personas diariamente transmiten y al mismo intercambian muchos datos personales haciendo más vulnerable su seguridad.

Una desventaja de no tener conocimientos por parte de los usuarios, es una gran utilidad para los criminales quienes ocupan la ingeniería social como herramienta para engañar o manipular a las personas mediante el correo electrónico hasta por llamadas hacen preguntas diseñadas estratégicamente con la finalidad que el usuario de contraseñas o credenciales privadas y así tener más rápido el acceso a los datos, es importante saber configurar la privacidad de las redes sociales usadas.

En algunas ocasiones las apps publicadas tienen fallas en la privacidad de los datos e incluso no respetan el acceso de los permisos o el almacenamiento de los mismos no tiene la suficiente seguridad esto hace referencia en la falta de requerimientos establecidos por la ley y normatividades encargadas del seguimiento de las apps.

Por lo que se generan las siguientes preguntas con la intención de saber:

¿Qué conocimiento de las funciones de internet sabe un usuario para prevenir el robo de sus datos personales en el uso de apps?

¿Qué acciones provocan la vulnerabilidad de robo de datos personales de un usuario por medio de internet?

JUSTIFICACIÓN

Es realizada con el objetivo de mostrar los conocimientos básicos e información de los permisos que conceden el acceso a sus datos mediante las apps como usuarios, exhibiendo las vulnerabilidades de todos los usuarios en las apps de redes sociales, se generara más información creando conciencia para su adecuado uso y manejo, configurando la seguridad y privacidad ofrecida por parte de cada una de las apps minimizando la posibilidad de ser víctima de robo de datos personales antes de descargar y usarlas apps de redes sociales.

Informando a los usuarios la posibilidad negarse a aceptar los permisos de acceso que piden la mayoría de las apps en caso muy necesario.

Para tomar medidas de conservando los datos de los usuarios exponiendo los requerimientos que son precisos antes de publicar las apps siguiendo las leyes con sus normativas ya establecidas, dando a conocer recomendaciones una vez que es víctima que se debe hacer en este caso, saber cómo fue la causa de ser víctima en circunstancias de la vulnerabilidad en sus datos para no volver a cometer esos errores.

Capítulo 1: Conceptos Básicos

1. Datos personales

Se refiere a toda información respectiva de un individuo para ser usada de manera en que se pueda identificar a una persona física siendo determinada directa o indirectamente con ayuda física, fisiológica, psíquica, económica, identidad cultural o social, lugar de origen, domicilio actual, edad, trayectoria académica, laboral y profesional, patrimonio, CURP, huella digital, ADN entre otros (Jáuregu, 2009).

Por otra parte la protección de datos personales es una especificación a la libertad para mantener un incentivo de autonomía informativa en el giro de del régimen jurídico, ético y político estableciendo a cada uno como debe y puede decidir la forma en que quiere identificarse y ser identificado, ante el equilibrio entre la dimensión individual y la dimensión social de la identidad y de los datos personales (Rodríguez, 2003), agregando la existencia de la igualdad y a la no discriminación teniendo dignidad ante cualquier situación.

Según la LFPDPPP (Ley Federal de Protección de Datos Personales en Posesión de Particulares) instituye que toda empresa responsable debe informar las vulneraciones de los datos personales a los titulares de los mismos, establecido en el artículo 63 del Reglamento de la LFPDPPP vulnerabilidad de los datos es:

a) La pérdida o destrucción no autorizada de los datos personales en posesión de las personas físicas o morales, que realizan el tratamiento de los datos.
b) El robo, extravío o copia no autorizada de los mismos.
c) Su uso, acceso o tratamiento no autorizado.
d) El daño, la alteración o modificación no autorizada.

Sin embargo cuando se entra en vigor este articulo también se debe mencionar el artículo 20 del mismo reglamento indica aquellas vulneraciones de datos personales que afecten de forma significativa los derechos de las y los titulares de los datos, deben ser notificadas de manera forma inmediata para tomar las respectivas acciones para proteger su información y privacidad.

La empresa tiene la obligación de informar, al menos:

a) La naturaleza del incidente.
b) Los datos personales comprometidos.
c) Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses.
d) Las acciones correctivas realizadas de forma inmediata.
e) Los medios donde puede obtener más información al respecto.

De lo contrario la empresa se somete a procesos de investigación y a la obligación de posibles sanciones económicas (Salazar, 2016 - 2017).

Por parte de la ley mencionada anteriormente es una especie de garantía que tienen las personas titulares de sus datos al saber que acciones pueden y no pueden realizar las empresas. A todo esto los datos y las leyes que existen se puede tomar en cuenta la intimidad se va de la mano con los datos personales, varios autores proponen puede ser vista desde tres aspectos: como fenómeno, como idea y como derecho, todos los estudios coinciden en la necesidad universal de intimidad en este ámbito que es el más significativo desde nuestra perspectiva teniendo derecho a la intimidad (Delgado, 1998).

1.1 Categorías

a) Identidad: Nombre, origen étnico y racial, lengua materna, domicilio, teléfono, correo electrónico, firma, contraseñas, RFC, CURP, fecha de nacimiento, edad, nacionalidad, estado civil.
b) De trabajo: Institución o empresa donde trabaja, cargo, domicilio, correo electrónico institucional o empresarial, teléfono del trabajo.
c) Patrimonio: Sueldo o salario, impuestos, cualquier tipo de crédito, tarjetas de débito, cheques, inversiones (Ibarra Cadena, y otros, 2016) . en esta categoría también se toman en cuenta bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, fianzas, servicios contratados (Anonimo, IVAI, 2017).
d) Educación: Escuelas, calificaciones, títulos, cédulas, certificados, diplomas.

e) Ideología: Religión, afiliación o preferencia política, sindical, participación en organizaciones civiles.
f) Salud: Estado de salud, historial y estudios clínicos, enfermedades, tratamientos médicos, medicamentos, alergias, embarazos, condición psicológica y/o psiquiátrica (Ibarra Cadena, y otros, 2016), se expande en expedientes clínico de cualquier atención médica, referencias o descripción de sintomatologías, incapacidades médicas, discapacidades, intervenciones quirúrgicas, vacunas, consumo de estupefacientes, uso de aparatos oftalmológicos, ortopédicos, auditivos, prótesis.
g) Características físicas: Tipo de sangre, ADN, huella digital, registro de voz, imagen, registro dental, color de piel, iris, cabello, lunares, cicatrices y otras señas particulares.
h) Intimidad: Preferencias y hábitos sexuales, etc.
i) Electrónicos: el correo electrónico no oficial, dirección IP[1], dirección MAC[2], nombre del usuario, contraseñas, firma electrónica; o cualquier otra información empleada por la persona para su identificación en Internet, acceso a sistemas de información u otra red de comunicaciones electrónicas.
j) Procedimientos administrativos: en forma de juicio o jurisdiccional en materia laboral, civil, penal, fiscal, administrativa o de cualquier otra rama del Derecho (Anonimo, IVAI, 2017).
k) Datos atribuidos por el Estado: Su origen en una norma, ley, decreto, acto administrativo o una sentencia judicial. Tales son los casos de la adopción, los antecedentes penales y el matrimonio.
l) Datos generados por la persona: Son aquellos datos que se van conformando a partir de determinadas elecciones de una persona a lo largo de su vida (Liceda, 2011).

[1] Protocolo de Internet
[2] Dirección de control de acceso al medio.

1.2 Intimidad

Según el diccionario de la Real Academia Española define intimidad como “zona espiritual íntima y reservada de una persona o de un grupo”.

“Etimológicamente, el término intimidad procede del latín, del adverbio ‘intus’, que significa ‘dentro, interior’, algo recóndito. Profundo del ser por lo mismo oculto, escondido en su carácter superlativo” (Beresovsky, 2017).

Se podría decir que representa el espacio de la privacidad personal de cada ser humano, esta misma intimidad persona se entrega ya sea a familia, amigos, pareja. Actualmente ha ido avanzando la tecnología con ella la comunicación de la mano van las redes sociales para mantener en contacto con personas a quienes tenemos lejos o simplemente se quiere sentir en constante relación (Anonimo, Definicion abc, 2017).

También puede decidir su forma de ser y estar, disfrutando se su soledad o la convivencia para tener conclusiones de reflexión, analizar, pensar, crear en otras sensaciones manteniendo así su libertad como humano. Anteriormente se mencionaba se puede compartir la intimidad con familia amigos esto incluye la medida que este establezca, tal como las limitaciones asignadas en el interés en su alrededor, los usos y costumbres del individuo.

Además es un derecho ante la constitución, en el Artículo 16° menciona el derecho a no ser molestado injustamente por parte de las autoridades, la inviolabilidad de las comunicaciones y de la correspondencia, en el párrafo noveno menciona la prohibición en categoría de violar todo tipo de comunicación es decir, escrita, telefónica o por cualquier otro medio, dependiendo el caso se puede intervenir las comunicaciones de los particulares funden las leyes (Quintal, 2017).

1.3 Delito informático

Los delitos informáticos se relacionan con la representación de usar la computadora, internet u otro medio ayudando a la facilitación de un crimen, por lo otro lado los delitos informáticos son conocidas como acciones con el propósito de acceder sin autorización a los sistemas de dispositivos de seguridad en otras palabras se puede entender como invasión a computadoras, correos, sistemas de bases de datos estas conductas pueden afectar a bienes jurídicos, entre empresas, y usuarios. Sin embargo no se puede determinar como delitos informático por el solo hecho de usar una computadora, es necesario detallar el cómo fue realizado el crimen y si entran las características establecidas de un delito informático (Terreros, Delitos Informáticos, 2014).

Toda acción ilegal en que una computadora es herramienta u objeto del delito, donde hay implicaciones de actividades criminales tales como robos, hurtos, falsificaciones, perjuicios, estafa, sabotaje. Son acciones ilegales con la intención de acceder sin autorización a cualquier equipo de cómputo o cualquier soporte tecnológico encargado de la entrada, procesamiento, salida de información o en red con datos para ser intersectados con objetivo de robar, estafar, destruir, modificar o sabotaje con el fin de adquirir dinero o dañar.

1.3.1 Categorías de delito informático y otras amenazas.

Existen diversas categorías de delitos informáticos también pueden ser llamados ataques son sucesos incitados por personas externas o internas. Es indispensable tener conocimiento para evitar ser vulnerables se expondrán algunos son:

- Espionaje: Consiste en el acceso no autorizado sea físico o lógico, a la información, mensajes, documentos, o servicios. Su principal objetivo es la infiltración de los datos en la información sustraída.
- Escuchas: Es acción de los usuarios cuando comunican mensajes por un canal no protegido, existe el riesgo de una tercera persona pueda intersectar o acceder a los mensajes comunicados.

- Lectura o copia de información: Es el acceso directo a la información sin tener servicios, ni sesiones autorizadas tomando una copia de la información encontrada mediante el acceso de medios físicos tal como discos o copias de respaldó.
- Suplantación, Intermediarios y Reproducción: la suplantación se trata de cuando una persona finge ser otro ante un tercero, con la intención de tener acciones fraudulentas.
    - La intermediación aplica en la acción de un persona actúa para ambos extremos de la comunicación hacia una persona.
    - La reproducción se origina en el momento en que una persona escucha una comunicación y luego la reproduce con la intención de hacerse pasar como la persona original.
- Análisis de trafico: Es cuando en una comunicación se encuentra cifrada[3] y un atacante la escucha este puede analizar y saber de dónde viene, a donde va, cuantos datos se han transmitido y cuando comenzó a término la transmisión (Canal, Riesgos, 2006).
- Manipulación de los datos: este tipo de delito es también llamado como sustracción de datos, es uno de los más comunes por lo fácil que es llevarlo a cabo y no se hay muchas formas posibles de saber cuándo están sustrayendo los datos. Por su facilidad que se tiene al realizarlo no se requiere de conocimientos técnicos de informática, solo se necesita una persona que tenga acceso a las instalaciones o funciones de los procesadores de datos en la primera de entrada de la adquisición de los mismos.
- La manipulación de programas: Para este delito se requiere un nivel más avanzado de conocimientos en informática, en el mismo acto se pueden modificar los programas ya existentes o se pueden instalar.
    - Un método más sobresaliente y conocido es el caballo de Troya este virus deja en los programas oculto una serie de instrucciones que se van cumpliendo y esto no es autorizado por el usuario pero la función de la computadora no afecta en nada.

[3] Cifrar es transformar información con el fin de protegerla de miradas ajenas.

- Manipulación de los datos de salida: Se establece un objetivo en el funcionamiento de los sistemas informáticos, se pueden manipular las instrucciones en la computadora para la fácil adquisición de los datos, codifican información electrónica falsificando las tarjetas bancarias o de crédito
- Falsificaciones informáticas: Tiene como propósito alterar los datos de los documentos almacenados en digital, a la información almacenada en el momento en que hace la consulta de una base de datos.
- Fraude efectuado por manipulación informática: Es el acceso a los programas ya instalados en un sistema de información, son manipulados ilícitamente para obtener ganancias monetarias (Hall)
- Pharming: Tipo de fraude elaborado mediante del desvío del explorador a sitios Web falsos de entidades bancarias, de lotería o compras por Internet, para que los usuarios ingresen su clave, la cual es guardada por el portal falso continuando para cometer el delito (Anonimo, Revista Vincuando, 2010).
- Acceso no autorizado a Sistemas o Servicios: Infiltrarse ilícitamente en todos los lugares de la redes sin tener acceso a los sitios en las redes.
- Reproducción no autorizada de programas informáticos*:* Duplicación de programas con licencias en copias para distribución (Hall)**.**
- Malware: Es la combinación de virus y gusanos ambos son de tipo software[4] malicioso, presentan un potencial peligro en la seguridad de los usuarios informáticos.
- Código malicioso toma ventaja de una característica fundamental de la arquitectura de los ordenadores: un dato puede ser información del usuario, como instrucciones de la máquina, también direcciones en la memoria de la misma, otra ventaja que toman es en los sistemas operativos los cuales ceden en todo el software su acceso. Por estas acciones es preciso limitar los derechos de instalación de un software para evitar la propagación de un código malicioso.

  Los tipos de software que entran en la categoría de código malicioso son el virus, gusano, exploit, troyano.

[4] Un conjunto de programas, instrucciones y reglas informáticas que permiten ejecutar distintas tareas en una computadora.

- Un exploit es un programa que se aprovecha de la arquitectura de las computadoras con los datos, direcciones y las instrucciones algunas son intercambiables con el motivo de provocar daños o acceder a los derechos de administrador.
- Caballo de Troya: es un programa que se mantiene oculto en el sistema hasta que se activa por instrucciones previamente programadas, algunos de estos se propagan de sistemas en sistemas, otros se hacen pasar por aplicaciones que pasan desapercibos por ejemplo: juegos o salvapantallas; estos son algunos.
    - Keylogger: su principal función es que graba o comunica todo lo que se teclea en el ordenador.
    - Dialer: Se conecta a través del modem haciendo llamadas y el importe se le cobra al usuario.
    - Adware: Muestra anuncios no deseados.
    - Puertas traseras: Proporciona acceso oculto a un sistema con privilegios para el total control de accesos (Canal, Codigo Malicioso, 2006).
- Virus: Es el código malicioso se caracterizan por modificar archivos, tienen diferentes objetivos diversos por ejemplo borrar archivos de todos tipo incluyendo los archivos del sistema, son conocidos por su duplicarse entre ellos.
- Gusano: También se duplica como el anterior a excepción que el gusano vive en la memoria hasta que llegan a duplicarse demasiado hasta minimizar los recursos del sistema.
- Rootkit: Grupo de herramientas y utilidades usualmente son usadas por los hackers al momento de acceder a un sistema, permite encontrar nombres de usuario y contraseñas, lanzar ataques contra un sistema remoto ocultando las acciones al mismo tiempo escondiendo los archivos y diversos procesos al mismo tiempo borrando su actividad de los diarios en el sistema.
- Bot / Zombie: Es un tipo de malware que da acceso al atacante el absoluto control sobre el ordenador afectado son mejor conocidos como zombie a los ordenadores que son afectados (Bradley & Carvey, 2008).

- Fraude: Es la manipulación, alteración, destrucción de los datos con el fin de dar mal uso o extorciones.
- Cyberbullying y Sexting: se refiere al acoso de cualquier tipo, usando la posible divulgación de archivos personales o sensibles y el segundo específicamente al sexual con el objetivo dar ofensas
- Piratería: es la producción y venta ilegalmente de falsificaciones de hardware, software y diversos tipos de programas (Noriega, 2016).
- Sabotaje: es la acción de dañar sistemas de cómputo o red, existen diversas técnica que son usadas en este delito son:
    - Bomba lógica: es la instalación de un programa con un conjunto de instrucciones indebidas que van a actuar en determinada fecha, destruyendo datos del ordenador, distorsionando el funcionamiento del sistema o paralizando el mismo.
    - Rutinas de cáncer: se encargan de distorsionar en funcionamiento del programa, su principal característica es el auto reproducción (Terreros, Delitos Informáticos, 2014).
- Spyware: Es un código malicioso instalado en el ordenador de forma ilegal en el momento de la descarga de software gratuito o pegado a correo electrónico, su propósito es la búsqueda y recopilar información confidencial del usuario para fines publicitarios o para detección de software pirata por empresas.
- Crimeware: se trata de un software que roba la identidad en línea de cuentas bancarias las cuales permiten realizar operaciones comerciales o financieras no autorizadas con fines de lucro como el robo o fraude.
- Phishing: es una estafa para el robo de identidad, adquiriendo información ya sea números de tarjetas de crédito, contraseñas, información de cuentas u otros datos confidenciales por medio de engaños (Anonimo, Revista Vincuando, 2010).
- Ingeniería social: Es una amenaza sencilla y al mismo tiempo tiene sus riesgos, consiste en hacer confiar a un usuario luego de seguir instrucciones para luego poder cometer delitos.

- Hurtos / Robo: Consiste en sustraer bienes sin violencia, sin embargo cuando se usa la violencia se llama robo, para evitar este tipo de acciones se debe utilizar códigos de acceso que impidan el acceso de al personal ajeno.
- Fallos de comunicaciones o almacenamiento.
- Fallos en el hardware o software.
- Permanencia incontrolada de información o servicios: Se relaciona con el paso de los datos por almacenamiento intermedios, el uso de la memoria secundaria que hace el sistema operativo de los medios de almacenamientos, también se suma la memoria cache de los navegadores estos son guardados en el disco duro, registro de la CPU, memoria RAM, Cache y Bufer específicamente del disco duro en estructuras como: Cluser, sectores de disco no usados, Sistemas de archivos (partición, unidad, volumen, etc.) archivos, bases de datos, archivos temporales, swap, coredump.
    - Los mencionados anteriormente guardan los datos y en ocasiones no siempre son del todo eliminados lo cual ocasiona que terceras personas recuperen la información, en aplicaciones guardan información de versiones y cambios anteriores de un archivo generando la recuperación de la información.
- Hoax / Cartas encadenadas / Spam: Son una forma de denegación de servicio causando que el usuario pierda su tiempo y almacenamiento en el correo, lo más común entre estos es recibir una carta con información falsa u obsoleta, usualmente el destinatario se siente obligado a reenviar el correo debió a la superstición de amenaza o premio.
    - Las principales características son: solicitud de enviar a los contactos de la víctima, alertan sobre virus, intoxicaciones alimentarias es decir algún tema para atraer al usuario, alguna noticia sobre fabricas que regalan productos.
- Interfaces pobres: Aplica en las aplicaciones estando mal diseñadas provocando que el usuario accidentalmente realiza acciones como borrar información, confirmar acciones u otras acciones en su consecuencia generando errores graves.

- Error humano: Sin importar las medidas que se lleven en ejecución es posiblemente exista el error humano ya sea por motivos de falta de diligencia, incompetencia, para la protección ante esta amenaza se usan interfaces, sistemas de copia de respaldo, capacitación al usuario.
- Violación de la privacidad (Canal, Capitulo Dos: Riesgos, 2006).

1.4 App

App es la abreviatura de la palabra en inglés: "application", se puede traducir como "aplicación", en el ámbito de la informática. Es un programa informático pequeño desarrollado con el objetivo de facilitar las tareas de un dispositivo (Gutierrez, 2017)

Son creadas por la necesidad de los usuarios permitiendo la fácil ejecución anteriormente las aplicaciones eran más básicas en los dispositivos móviles por ejemplo estaba la calculadora, alarma, cronometro, calendario entre otras. Conforme fueron saliendo modelos de celulares se crearon las tiendas o mercados de aplicaciones como Play Store, App Store, Windows Phone Store y más, su función principal era ofrecer apps que ayudaran a las necesidades de los usuarios fomentando su uso (Anonimo, Mastermagazine, 2017).

1.4.1 Tipos de Apps

a) Aplicaciones Nativas: son todas las apps que fueron creadas con el software que brinda cada sistema operativo, llamado SDK[5] desarrolladas únicamente por su diseño y la plataforma que sea el caso, las más conocidas son iOS, Android y Windows Phone sus requerimientos están planteados para tener una funcionalidad al 100% una vez instaladas en el dispositivo. Se debe tener en cuenta que en la plataforma de Android tienen constates actualizaciones en este proceso el usuario debe descargarla la app nuevamente estas constantes actualizaciones son realizadas para corregir errores o tener mejoras.

[5] Software Development Kit.

Haciendo mención a una de sus características de las app nativas es que usa el sistema operativo del dispositivo aunque no se esté usando y muestra notificaciones de su funcionamiento o solo informando al usuario algún mensaje que tenga. Una ventaja que tienen estas apps es que su funcionamiento no depende de internet, permitiendo el uso de herramientas del hardware[6] terminal. Su diseño e interfaz[7] está desarrollado con el sistema operativo[8] lo cual las hace más familiares y más fáciles de ocupar.

b) App Web: son desarrolladas en lenguaje HTML[9], simultáneamente con JavaScript[10] y CSS[11], a diferencia de las nativas estas aplicaciones se pueden ejecutar en cualquier dispositivo tecnológico ya que tienen diferentes códigos de lenguajes sin importar las plataformas, estas app no son obligatorias para instalarse ya que se pueden visualizar desde un navegador web del dispositivo móvil esto significa que las actualizaciones no afectan al usuario siendo que se encuentran en el navegador el cual está en constate actualización con internet.

   Otra diferencia es que no están en las tiendas de aplicaciones su comercialización es autónoma, su desventaja es que requieren el uso de internet para su funcionamiento y dejando un lado el aprovechamiento del hardware en el dispositivo.

   Su diseño e interfaz es independiente del sistema operativo en el que se está siendo visualizada.

c) App hibridas: es la combinación de las apps anteriores desarrolladas en HTML, con JavaScript y CSS al momento en que esté finalizada se compila y da como resultado una app nativa por el parecido de los códigos permitiendo que se encuentren en las tiendas de aplicaciones, usando también el hardware del dispositivo aprovechándolo. Su diseño e interfaz permiten acceder con botones o controles para ocupar la plataforma según sea el caso (Cuello & Vittone, 2013).

[6] Conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático
[7] Un conjunto de funciones que facilitan el intercambio de mensajes o datos entre dos aplicaciones.
[8] Conjunto de órdenes y programas que controlan los procesos básicos de una computadora y permiten el funcionamiento de otros programas.
[9] Lenguaje de programación que se utiliza para el desarrollo de páginas de Internet.
[10] Lenguaje de programación que te permites realizar actividades complejas en una página web.
[11] Un lenguaje que define la apariencia de un documento escrito en un lenguaje de marcado.

1.4.2 Categorías de Apps

a) Aplicaciones de entretenimiento: son todas las aplicaciones que función es entretener, divertir a los usuarios debido a sus características con gráficos, animaciones y efectos de sonido, permitiendo a los usuarios tener mayor atención en el desarrollo del juego.
b) Aplicaciones sociales: permite la comunicación entre usuarios de diferentes tipos, lugares a través de redes.
c) Aplicaciones utilitarias y de productividad: Estas proporcionan herramientas útiles para los usuarios para la realización de diversas tareas, cortas y rápidas.
d) Aplicaciones educativas e informativas: son aquellas aplicaciones son usadas como consulta de conocimientos y noticias, accediendo al contenido y disponibilidad de la información buscada.
e) Aplicaciones de creación: están enfocadas para la creatividad de los usuarios proporcionando herramientas para editar, retocar, producir sonidos, etc. En imágenes ya pre terminadas o la creación de las mismas con ayuda de las misma apps (Saavedra, 2015).
f) Android wear apps: en esta categoría existen bastante apps de las comunes usadas y mencionadas las categorías anteriores la diferencia radica en que son sincronizadas con un smartwach[12] haciendo que la notificación llegue al reloj.
g) Autos y Vehículos: En esta categoría se encuentra una gran variedad de app su funcionamiento es relacionado con los autos y vehículos cada una de las app contiene su descripción para hacerse promoción de las mismas en funcionalidad.
h) Biblioteca y demostración: Se enfoca a la búsqueda de libros o app que faciliten su búsqueda, en demostración se sugieren varias app en un escenario de simulador para diferentes categorías ya sea en juegos o diseños de casas tanto planos como para la decoración de interiores.

[12] Dispositivo reloj que posee la particularidad de vincularse y sincronizarse con nuestro Smartphone.

i) Comer y beber: ayudan a los usuarios a encontrar restaurantes para poder ir al establecimiento o también ofrecen la posibilidad de que el servicio se a domicilio, en esta categoría también se pueden descubrir recetas de toda tipo de comida y bebidas como cocteles según a las necesidades del usuario.

   Otra característica de apps que se pueden descargar es la información de ciertas bebidas y comida. También hay apps de nutrición, contadores de calorías.

j) Compras: Ofrece en esta categoría la solución de hacer compras desde una apps y sea de ropa, accesorios, muebles, todo depende del tipo de apps que se descarguen algunas son muy varias y ofrecen toda clase de mercancía y otras solo tiene una categoría disponible para vender.

k) Finanzas: en esta categoría ofrecen las apps que son lanzadas por los bancos para que los usuarios tengas más facilidades al usar su dinero ya sea haciendo transacciones o cualquier tipo de movimientos que se requiera.

   O simplemente hay apps que se encargan de ayudarte administrando tus finanzas solo se tiene que insertar datos y en un tiempo muestra los ingresos y egresos.

l) Medicina: en esta categoría se pueden apreciar diferentes apps que tienen como propósito ayudar a los usuarios con diferentes tareas y sea llevar la cuenta de un embarazo en calendarios también se pueden registrar los días de menstruación, apps de farmacias mostrando sus productos, diagnóstico de enfermedades, anatomía del cuerpo humano, registro de presión arterial, chat con médicos en línea, diccionarios médicos, etc.

m) Tiempo: se muestran apps que ayudan a una perspectiva del pronóstico del clima incluyendo el oleaje, viento, las fases de la luna.

n) Viajes: se presentan estas apps algunas desarrolladas para hacer llegar al usuario comentarios de lugares de todo el mundo, otras son para hacer reservación o recibir información acerca de viajes de aerolíneas, autobuses, también para reservar hoteles y otros lugres turísticos.

1.5 Red Social

Es una ciencia social que incluye la antropología, sociología, psicología social, economía, geografía, ciencias políticas, cienciometría[13], estudios de la comunicación, sociolingüísticos y organizacionales (Anonimo, Calameo, 2016).

En cada una de las ciencias y estudios anteriores son ocupados como métodos para establecer un concepto significativo para la sociedad, llegando a la conclusión de que una red social se localiza en sitios de internet para que las personas accedan a conectarse con sus amigos llegando a conocer nuevas amistades, de manera virtual, y compartir contenidos, interactuar, implementar comunidades con intereses relacionados o similares: trabajo, lecturas, juegos, amistad, relaciones amorosas, relaciones comerciales.

Con el objetivo de recuperar y seguir manteniendo comunicación con personas que no estén físicamente en el mismo lugar, llegando a ser más rápidas las respuestas ante solución de problemas o simplemente estableciendo lazos para tener interacciones entre personas de diferentes lugares sin importar la distancia.

1.5.1 Categorías de redes sociales

1. Redes sociales Horizontales: Son dirigidas a todo público, no tienen una temática en especial su objetivo es la interrelación entre personas las más populares son: Facebook, Google, Twitter, Instagram, MySpace, etc (Burgueño, 2009).
2. Redes sociales Verticales: Se dirigidas a un grupo de personas en específico de ahí se desglosa otras dos categorías que son:
    - Verticales profesionales: para generar relaciones en un ambiente laboral entre usuarios.

[13] Estudia los aspectos cuantitativos de la ciencia como disciplina o actividad económica, forma parte de la sociología de la ciencia y encuentra aplicación en el establecimiento de las políticas científicas.

- Verticales de ocio: son para usuarios que las usan en sus actividades de tiempo libre como los videojuegos, deportes, libros, animales, viajes, etc. las más populares son LibraryThing, Wattpad, Dogster, Tripadvisor, Wipley, etc (Sánchez, 2011).
- Verticales Mixtas: es la combinación de las categorías anteriores donde se brinda aplicaciones divertidas y al mismo tiempo profesionales.

3. Redes sociales de geolocalización: es la relación entre usuarios socializando compartiendo la localización física de los mismo, las más populares son: Fousquare, Facebook Places y Google Places.
4. Redes sociales de contenidos: se trata de que los usuarios comparten diferentes contenidos y formatos como videos, fotografías, gif, etc., las más populares son: Flickr, Instagram, YouTube, Vimeo, Quora, Slideshare (Burgueño, 2009).

1.6 Identidad

Se refiere como el conjunto de rasgos que hace una persona su distinción de las demás sabiendo quien es, al mismo tiempo permite la interactuar en su entorno, la identidad va modificando a lo largo de la vida desarrollando con el medio externo y el funcionamiento individual propia del individuo (Peña R. M., 2016).

Por otra parte es considerada como un fenómeno subjetivo de elaboración personal, constituyendo simbólicamente la interacción con otros. Se puede llamar como un proceso dialéctico de formación de la propia identidad, comenzando en la representación imaginaria o construcción simbólica de la misma (Anonimo, Gitanos, 2005).

El proceso de construcción en la que el individuo se va definiendo a sí mismo por medio de la interacción simbólica con otras personas. A través de la habilidad para aceptar las actitudes y expectativas de los otros, finalizando con el objeto de su propia reflexión. Poco a poco el individuo se experimenta a sí mismo no directamente sino indirectamente; se hace partícipe de sí mismo sólo al tomar las actitudes de otros individuos hacia él (Larrain & Hurtado, 2003).

Para terminar la identidad es un grupo de rasgos, atributos y características propias de una persona, en el cual los demás individuos o un grupo de ellos que logran diferenciarlos de los demás, algunos de los rasgos pueden ser hereditarios o como antes se menciono es resultado de las convivencias de relaciones con los demás individuos en su entorno.

1.6.1 Identidad digital

Con la llegada de la tecnología han surgido nuevos aspectos que antes no eran conocidos como la identidad digital la cual es definida como el conjunto de información de un individuo o una organización expuesta en Internet, es decir datos personales, imágenes, registros, noticias, comentarios, etc. Puede conformar una descripción de dicha persona en el ámbito digital.

Su concepto puede llegar a ser amplio pero si solo se enfoca en la vivencia de los ciudadanos en la Red, de forma progresiva, la identidad humana y la identidad digital forman parte de una misma realidad, logrando la dificultad para no poder distinguir entre la actuación realizada en el mundo físico y en la Red, de forma que se puede hablar de aproximación hacia una identidad híbrida.

La OCDE[14] (Organización para la Cooperación y el Desarrollo Económicos) reconoce y expone algunas propiedades de la identidad digital:

a. La identidad digital es esencialmente social: Conforme el individuo proyecta su personalidad en la Red, principalmente en las redes sociales, los demás individuos digitales lo caracterizan y reconocen de forma efectiva, en algunas ocasiones no se ha producido una verificación presencial de la identidad.
b. La identidad digital es subjetiva: Tanto la percepción del “yo” como del “nosotros” están basadas en la experiencia que personas diferentes construyen y que les permiten reconocerse.

[14] Es un organismo de cooperación internacional, compuesto por 35 estados, cuyo objetivo es coordinar sus políticas económicas y sociales.

c. La identidad digital es valiosa: La propia actividad de los individuos genera información para ser ocupada con el objetivo de establecer relaciones personalizadas y para tomar decisiones en las relaciones con las personas, con un mayor grado de confianza.
d. La identidad digital es referencial: Una identidad no es una persona o un objeto, sino una referencia a dicha persona u objeto.
e. La identidad digital es compuesta: La mayoría de la información es entregada de forma voluntaria por los propios usuarios, sin embargo otras sobre los mismos son brindadas por terceros, sin la participación del tutelar.
f. La identidad digital produce consecuencias: Una de ellas es la divulgación de la información en ocasiones puede generar efecto.
g. La identidad es dinámica: Está en constante cambio y modificación permanente. Primordialmente en Internet, la identidad digital se debe ver como un flujo de informaciones.
h. La identidad es contextual: Dado que la divulgación de la información puede generar un impacto negativo empleada en un contexto erróneo, o sencillamente ser irrelevante, mantener las identidades segregadas entre sí permite tener más autonomía.

Los rasgos de identidad usualmente se encuentran agrupados o relacionados entre ellos, formando identidades parciales. Las personas físicas utilizan diferentes identidades parciales en función de los diferentes roles y actividades que desarrollan a lo largo de su experiencia como cibernauta. Cada identidad parcial está sustentada en un servicio o aplicación de Internet, por ejemplo, un usuario mantiene sus perfiles en Facebook, Twitter y LinkedIn o en cualquier Red social, participa con el mismo alias en distintos foros de profesionales, maneja un blog de viajes y aparece ocasionalmente en prensa y webs especializadas, relacionadas con su ámbito profesional.

Todo ello conforma la identidad digital del individuo, lo que genera de todos los servicios mencionados sostiene una identidad parcial, que puede presentarse relacionarse o no con sus demás identidades (Pérez San-José , Gutiérrez Borge, De la Fuente Rodríguez, Álvarez Alonso, & García Pérez, 2012).

Por otra parte la identidad digital sólo puede ser creada por una persona, con lo que rápidamente se comprende que sólo encontraría correspondencia con los datos generados por la persona, siempre y cuando exista correspondencia entre el conjunto de datos en la red y los de una persona real.

Por lo tanto una persona sólo puede tener una identidad real; pero puede crear varias identidades digitales, dependiendo de la forma en que conforme el conjunto de datos en los diferentes ámbitos que habilitan las nuevas tecnologías de la información y las comunicaciones, Entonces en una identidad humana existe una probabilidad de que un usuario pueda tener más de una identidad digital así mismo esa identidad puede estar vacía en las redes sociales (Liceda, 2011).

1.7 Usuario de Redes sociales

Se define como persona u organización que maneja e integra una red social. Por lo general, el nombre de usuario es el nombre real de la persona u organización. También es posible ver usuarios que se identifican en la red mediante un nombre diferente o similar a su nombre real (Financieros, 2014).

En el área de informática es la persona que utiliza un dispositivo u ordenador para comunicarse con otros usuarios, generando contenido mismo que comparte, este usuario no necesita tener conocimiento avanzado para interactuar con un dispositivo u ordenador (Anonimo, Definicion abc, 2012).

1.7.1 Tipos de usuarios

Un estudio que se realizó por parte de la Universidad Winchester en el 2013 identifico a 12 tipos de usuarios de redes sociales dependiendo su comportamiento en las mismas:

1. Ultras: Estos usuarios son muy dependientes de las redes sociales, su necesidad de estar comunicado con amigos o familiares es muy constante, comienzan a sentirse abandonados, incomunicados o perdidos.
2. Los Negadores: Son el grupo de usuarios que se reúsan a aceptar su constante habito de utilizar las redes sociales, con sus actitudes intentan demostrar que no les afecta estar en sus redes sociales.

3. Los Esporádicos: Son aquellos usuarios sin necesidad de estar en sus redes sociales diario incluso pueden pasar días, semanas sin hacer alguna publicación o actualizaciones.
4. Vírgenes: En la actualidad existen personas sin cuentas de redes sociales o también pueden ser aquellos que son principiantes conociendo las redes sociales.
5. Los observadores: Estos usuarios son los que no hacen ninguna actualización en varios días, semanas o meses y solo están de espectadores viendo sus redes sociales, usualmente se quejan se la información innecesaria que hay en las mismas.
6. Los Pavos Reales: Utilizan las redes sociales en forma narcisista haciéndose notar a cada momento, su preocupación es conseguir mayores seguidores.
7. Los Provocadores: Emplean las redes sociales para expresar sus opiniones abiertamente impetuosas, sin sentir empatía de los demás usuarios, piensan que las redes sociales se ocupan para demostrar la libertad de expresión.
8. Los fantasmas: Son quienes les preocupa su privacidad al exponerse públicamente así como sus datos personales, usualmente ocupan seudónimos o incluso crean perfiles falsos.
9. Los Ultiapariencia: Estos usuarios crean varias cuentas bajo varias personalidades con el objetivo de desorientar a los usuarios para que nadie sepa quiénes son en realidad.
10. Los preguntones: Estos usuarios en sus actualizaciones platean preguntas para generar alguna conversación, esto lo hacen con el fin de aportar algo y no sentirse marginados.
11. Informante: Son los usuarios dedicados a investigar profundamente información selecta para ser ellos los primeros que dar la noticia.
12. Los Inseguros: Sienten la necesidad de ser aprobados por sus seguidores, cuando realizan alguna actividad se preguntan la reacción de sus seguidores y ver si son aprobados (Santo, 2013).

Capítulo 11: Estándares de Seguridad en Apps móviles

2.1 Permisos de acceso

Todas las apps requieren permisos de acceso para su instalación en el dispositivo, el objetivo de esto es para tener un mejor aprovechamiento para su correcta función, desde las tiendas como PlayStore, AppStore entre otras, cuando se comienza la descarga aparecerán los siguientes permisos:

a) Identidad: Puede acceder a las cuentas registradas en el dispositivo, tarjetas de contacto propio así como modificarla, agregar o quitar cuentas.
b) Calendario o Contactos: puede realizar las mismas acciones que lo anterior.
c) ID de dispositivo e información de llamadas: La app tiene acceso a ID del dispositivo, número de teléfono y también el número de la persona a la que llamas.
d) Teléfono: La app tiene capacidad marcar números de teléfono.
e) Fotos, datos multimedia y archivos: Este permiso es uno de los más comunes se les da acceso a la memoria donde se guardan estos archivos así como capacidad para verlos, editarlos e incluso eliminarlos.
f) SMS: El permiso para enviar mensajes.
g) Ubicación: Permiso para geolocalizar al usuario.
h) Cámara y/o Micrófono: Acceso para hacer fotos o vídeos / grabar audios.
i) Configuración de datos móviles: Capacidad para controlar parámetros sobre datos móviles en el dispositivo.
j) Dispositivo en historial de apps: puede leer los datos de registro, recuperar el estado interno del sistema, ver el historial de páginas web visitadas y recuperar aplicaciones en ejecución.
k) Información de la conexión Wi-Fi / Bluetooth: Autorización para usar ambos (Anonimo, 20minutos, 2017).
l) Configuración de datos móviles: Puede acceder a controlar parámetros que controlen la conexión de datos móviles.
m) Datos de actividad/sensores wearable: Se ocupa para pulseras de actividad física o smartwatches.

n) Compras directas desde la aplicación: Ofrece productos y carga los pagos a la cuenta de Google Play o según sea el caso de la tienda del usuario. Un ejemplo son juegos que son gratuitos y te permiten avanzar más rápido si pagas un poco.

Desde la aparición de Android 6.0 Marshmallow se pueden gestionar los permisos una vez descargados desde el sistema del dispositivo (Ortega, 2018).

a) Control de acceso: disponible para el usuario donde puede elegir la posibilidad de acceder o prohibir el acceso a su información.
b) Autenticación: elaborada con una identidad única y una contraseña preferiblemente conocida por el usuario.
c) Seguridad y confidencialidad: con uso estándar de AES[15] con una clave cifrada de al menos 128 bits[16] es muy recomendable para garantizar la seguridad.
d) Integridad: es aconsejable usar al menos un código de autenticación basado en clave simétrica por ejemplo AES.
e) Transferencia de datos: usar TLS[17] con métodos de encriptación de 128 bits o redes privadas virtuales[18].
f) Retención de datos: sólo deben ser guardados el tiempo necesario para el propósito establecido ya mencionado en las políticas de privacidad.
g) Alerta de los fallos de seguridad: la empresa desarrolladora debe avisar a las autoridades competentes así como a los usuarios tan pronto como sea posible y debe ayudar al usuario a solucionar los posibles daños causados por dicha brecha (Mocholi, 2015).

[15]Advanced Encryption Standard: La encriptación es el proceso de cambiar los datos de forma que solo puedan ser leídos por el receptor al que va destinado.
[16] Digito binario: menor unidad de información de una computadora
[17] Transport Layer Security: Es un protocolo mediante el cual se establece una conexión segura por medio de un canal cifrado entre el cliente y servidor.
[18] VPN: es una tecnología de red de computadoras que permite una extensión segura de la red de área local

2.2 Políticas de privacidad.

En esta sección de las políticas de privacidad se estipula que sucede con los datos personales solicitados en contratos, formularios, aplicaciones, etc. Serán usados tratados y protegidos de acuerdo a lo establecido por la Ley.

Mencionando el objetivo de la recolección de los datos personales de acuerdo a la app responsable de proveer el servicio, así mismo como la confidencialidad debe estar garantizada y protegida por las medidas de seguridad administrativas técnicas y físicas con el debido control de acceso para permitir a ellos. El propio usuario puede y tiene el derecho de cancelar la obtención y uso de datos en las app así como modificarlos (Anonimo, Banshai, 2017).

Sin embargo ya debe ser por un hecho la privacidad de los usuarios en el momento en que se estar desarrollando el software o sistema actualmente existen metodologías que revisan desde el mismo código de la aplicación y que dan pautas para la seguridad entre ellas el cifrado de datos, protocolos SSL-TLS, pruebas de vulnerabilidades, auditorias, mecanismos de autenticación, almacenamiento, etc. (Realpe, 2017).

En pocas palabras es el permiso que el usuario brinda los datos personales una vez que decidió hacer descarga entonces acepta las políticas de privacidad empleando una app en donde se le reconoce la normativa sobre protección de datos de carácter personal, un ejemplo son las siguientes secciones:

a) Seguridad y protección de datos personales: Se ofrece total seguridad de los datos personales, pero al mismo tiempo las app no se hacen responsables de los hackers[19] o terceros que realizan acciones para dañar romper la seguridad de la app.
b) Responsabilidad de opiniones: La app solo se responsabiliza de las publicaciones aquí expuestas a manera de posts[20], mas no de los comentarios de éstas, ya que son realizados por terceros y/o usuarios.

[19] Persona experta en alguna rama de la tecnología, a menudo informática, que se dedica a intervenir y/o realizar alteraciones técnicas con buenas o malas intenciones sobre un producto o dispositivo.
[20]Mensaje, artículo o publicación, generalmente usado en el contexto de foros y blogs en Internet.

c) Privacidad: La app respeta la privacidad de cada uno de sus usuarios. Toda información ingresada por el usuario a través de la misma, será tratada con la mayor seguridad, y sólo será usada de acuerdo con las limitaciones establecidas.

d) Obtención de información: Esta app obtiene los datos personales suministrados directa, voluntaria y conscientemente por cada usuario.

e) Uso de la información: Al bridar datos personales, automáticamente estará autorizando el uso sus datos personales de conformidad a la Política de Privacidad, lo cual comprende los siguientes eventos:
   - Para el propósito específico para la App.
   - Para incrementar ofertas al mercado y hacer publicidad de productos que pueden ser de sumo interés para el usuario; incluyendo los llamados para confirmación de su información.
   - Personalizar y mejorar los productos y servicios.
   - Enviar e-mails con nuestros boletines, responder inquietudes o comentarios, y mantener informado a los usuarios.

f) Acceso a su información: La app tiene el compromiso permanente de presentar nuevas soluciones que mejoren el valor de sus productos y servicios; con el objeto de ofrecer oportunidades especiales de mercado, como incentivos, promociones y novedades actualizadas. no comercializara, venderá ni alquilara su base de datos a otras empresas.

g) Utilización de "Cookies"[21]: Algunas apps utilizan cookies y dirección IP[22] sólo para obtener información general de sus usuarios y para proveer de un sitio personalizado.

[21] Pequeña información enviada por un sitio web y almacenado en el navegador del usuario, de manera que el sitio web puede consultar la actividad previa del usuario.

[22] Número que identifica, de manera lógica y jerárquica, a una Interfaz en red de un dispositivo que utilice el protocolo IP.

Es necesario mantener un registro de: browser[23], sistema operativo[24] usado por el usuario, nombre del dominio[25] del Proveedor de Servicio de Internet. Adicionalmente se actualizara un registro del número total de descargas el que permite realizar mejoras en las apps. Los cookies permiten entregar un contenido ajustado a los intereses y necesidades de usuarios/visitantes.

h) Revelación de información: En ningún momento se utiliza o revela a terceros, la información individual de los usuarios así como los datos sobre las visitas, o la información que se proporcionan: nombre, dirección, dirección de correo electrónico, número telefónico, etc. (Applicantes, 2017).

Incluso existen más políticas de privacidad las cuales cambian de acuerdo a la categoría en que es usada la app.

2.3 Protección de datos en apps.

La Ley Federal de Protección de Datos en Posesión de Particulares, es un cuerpo normativo de México, aprobado por el Congreso de la Unión el 27 de abril de 2010, tiene como propósito regular el derecho a la autodeterminación informativa.

Esta Ley fue publicada el 5 de julio de 2010 en el Diario Oficial de la Federación y entró en vigor el 6 de julio de 2010. Las secciones son aplicables a todas las personas físicas o morales, del sector público y privado, tanto a nivel federal como estatal, están poniendo en marcha el tratamiento de datos personales en el ejercicio de sus actividades, abarcando empresas como bancos, aseguradoras, hospitales, escuelas, compañías de telecomunicaciones, asociaciones religiosas, y profesionistas como abogados, médicos, entre otros, se encuentran obligados a cumplir con lo que establece esta ley (Blanco, 2013).

[23] Software, aplicación o programa que permite el acceso a la Web.
[24] Software básico de una computadora que provee una interfaz entre el resto de programas del computador, los dispositivos hardware y el usuario.
[25] Nombre único que se muestra después del signo @ en las direcciones de correo electrónico y después de www.

Las personas físicas o morales podrán recabar y tratar lícitamente datos personales cuya titularidad será en todo caso de aquellas personas asociadas a los mismos. Con la condición que se lleve con total seguimiento la ley de acuerdo con la misma, un dato personal es cualquier información concerniente a una persona física identificada o identificable de la información que es considerada como sensible, para proteger los datos que puedan afectar en la intimad de su titular, o su utilización indebida pueda dar origen a discriminación o conlleve un riesgo.

Las personas responsables de la recaudación un dato personal de cualquier titular, tiene la obligación de establecer específicamente para qué necesita este dato, qué tratamiento le dará es decir para qué lo utilizará y cómo lo gestionará, esta informe debe hacerlo saber al titular a través de un Aviso de Privacidad.

El tratamiento de datos estará sujeto al consentimiento por parte del titular, la aprobación procede siempre si la voluntad se manifiesta, o tácita cuando habiéndose puesto a su disposición el Aviso de Privacidad, no manifieste su oposición.

En los datos financieros o patrimoniales requerirán la aprobación expresa de su titular. Para el tratamiento de los datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular; éste podrá ser revocado en cualquier momento. Los datos podrán ser transferidos a terceros, siempre que así se establezca en el Aviso de Privacidad, y no exista oposición del titular. Si los datos van a ser tratados por un tercero, el responsable debe asegurarse que este tercero los resguarde y solamente los utilice para el fin convenido.

Los avisos de privacidad son generados las personas físicas y morales deben tener conciencia del modo como recaban así como sus de datos personales; existen dos orígenes de la información: interno y externo.

a. El interno corresponde a la información que la empresa tiene sobre su personal, socios, agremiados y en general personas vinculadas a la compañía por lo regular estos datos son los más obvios.

   En el momento para reclutamiento y selección del personal, y las contrataciones, se recaban datos personales, frecuentemente datos sensibles por ejemplo estado de salud, afiliación sindical, creencias religiosas o políticas, origen étnico, fotografías, etc.

b. Los datos de origen externo son todos que provienen de personas ajenas a la compañía, incluyendo proveedores, clientes, prospectos, datos de mercadeo, etc. Por ejemplo, lo más patente es cuando se hace una base de datos con fines comerciales o de mercadotecnia, las listas que tienen el nombre de la persona y el correo electrónico o datos de contacto, la cartera comercial, o un formulario interactivo en el que un visitante deja sus datos (Anonimo, tuinterfaz, 2011).

Se aconseja antes de llenar algún documento o algún papel en que se expongan los datos personales deben asegurarse hacia donde van a ir o si al menos cuentan con un Aviso de Privacidad el cual ampare.

La LFPDPPP define e informa brevemente otros conceptos establecidos en los Artículos 3 y 6, así como en los Artículos 2 y 9.

- Responsable: Persona física o moral de carácter privado que decide sobre el tratamiento de datos personales.
- Titular: Persona física a quien corresponden los datos personales.
- Tratamiento: Obtención, uso, divulgación o almacenamiento de datos personales por cualquier medio.
- Aviso de privacidad: Documento físico, electrónico o en cualquier otro formato que genera el responsable y pone a disposición del titular previo al tratamiento de sus datos.
- Derechos ARCO: Son los derechos de acceso, rectificación, cancelación y rectificación.

- Entorno digital: Ámbito conformado por el hardware, software, redes, aplicaciones, servicios o cualquier otra tecnología de la sociedad de la información que permita el intercambio o procesamiento informatizado o digitalizado de datos.
- Listado de exclusión: Base de datos que registra la negativa de un titular al tratamiento de sus datos personales.
- Medidas de seguridad administrativas: Conjunto de acciones y mecanismos para establecer la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación y clasificación de la información, así como la concienciación, formación y capacitación del personal, en materia de protección de datos personales.
- Medidas de seguridad físicas: Conjunto de acciones y mecanismos, ya sea que empleen o no la tecnología.
- Medidas de seguridad técnicas: Conjunto de actividades, controles o mecanismos con resultado medible, que se valen de la tecnología para asegurar que los accesos a la base de datos de información sea por usuarios autorizados, para que se realicen sólo las actividades autorizadas, se incluyan acciones para la adquisición de, operación, desarrollo y mantenimiento de sistemas seguros y se lleve a cabo la gestión de comunicaciones y operaciones de los recursos informáticos que se utilicen en el tratamiento de datos personales (Montiel, 2013).

Principalmente se debe encargar de brindar la confidencialidad, integridad autenticidad y disponibilidad de los datos.

2.4 Aspectos legales de las aplicaciones móviles

1. Funcionalidades: Se debe tener claro lo que se puede y no puede al desarrollarse mediante medios legales.
2. Derechos propios y de terceros: Se deben tener los correspondientes permisos para llevar a cabo el desarrollo utilizando licencias ya sea de bibliotecas de programación, Bases de datos, elementos gráficos, textos, etc.

3. Licencia y condiciones de uso: Al momento de crear las app se debe desarrollar una licencia y sus términos de uso para que el usuario tenga conocimiento y aceptar para hacer uso de la misma.
4. Menores: Se deben consultar las leyes correspondientes y las obligaciones impuestas ya que existe una regulación especial en materia de consumidores con usuarios y protección de datos en menores de 14 años.
5. Información y permisos: Se debe mostrar la información y permisos que necesita para su instalación para la mejora de las funciones, accediendo a datos como la agenda, mensajes, llamadas, etc.
6. Markets[26] de aplicaciones: Para dar a conocer y comercializar al público y venderse se tienen condiciones estrictas, También se definen puntos críticos como las comisiones que se deben pagar por el e-commerce[27] desde la app, o los contenidos prohibidos, los avisos específicos, las condiciones técnicas, por poner ejemplo, deben ser estudiados al detalle para evitar problemas una vez acabemos de desarrollar aplicaciones móviles.
7. Política de Cookies: Es muy común navegar por Internet o usando una app cuando se muestra un aviso de política de cookies entonces esto se debe mostrar y aceptar las políticas de cookies mediante avisos con la información básica sobre qué son las cookies, su objetivo, quien las instala y como rechazarlas.
8. Informar al usuario: Es obligatorio cumplir informando a los usuarios de los aspectos marcados por la ley, generalmente estas en los apartados donde dice “acerca de” o “quiénes somos” ahí el usuario conoce información de la app, creadores, nombre y dominio de la empresa, NIF[28], la adhesión a códigos de conducta, etc.
9. Publicidad: Se usa la publicidad en las app gratuitas para generar los ingresos o técnicas de las mismas app (Mocholí, 2014).

[26] Tienda online a la cual tienes que acceder para poder descargarte aplicaciones y juegos para los dispositivos.
[27] Negocios por Internet o negocios online, consiste en la compra y venta de productos o de servicios a través de medios electrónicos.
[28] Número de Identificación Fisca: confiere seguridad al número, de modo que al introducir un NIF en una aplicación informática.

10. Privacidad y geolocalización: Cuando se ocupa en la App el usuario, tener acceso a la configuración de la privacidad así como a la geolocalización y autorizar la misma (Anonimo, Emprendedores, 2015).

El Gobierno Digital Estándar da criterios de pruebas de vulnerabilidades en aplicaciones móviles las cuales son mencionadas:

a. La validación de la aplicación móvil tras varios intentos fallidos con datos incorrectos en el login[29], este se bloquea temporalmente, evitando ataques por medio de fuerza bruta, procede en la aceptación de la misma.
b. Se tiene que mostrar evidencia que la aplicación no permite copiar y pegar en campos que contengan o manejen información sensible. Es decir: Datos de usuarios contraseñas, cuentas bancarias etc.
c. Se especifica o demuestra que la aplicación no almacena información sensible del usuario como nombre de usuario y contraseñas en los registros de la aplicación o que la información almacenada localmente en el dispositivo está protegida.
d. Se comunica el tipo de encriptación que tienen los datos sensibles al ser guardados en localmente en el dispositivo. La encriptación utilizada no es una encriptación débil.
e. Se especifica cuando al salir de la aplicación o al cerrarla no se quede activa la sesión del usuario.
f. Se valida la comunicación utilizando en la aplicación el protocolo TLS actual disponible.

[29] Es el proceso mediante el cual un usuario accede a sus distintas cuentas informáticas.

El listado de reglas de seguridad para el análisis dinámico, se considera la validación de las vulnerabilidades principales de las aplicaciones Móviles según en el TOP 10 de la Open Web Application Security Project (OWASP[30]):

1. Uso incorrecto de la plataforma
2. Almacenamiento de datos inseguro
3. Comunicación Insegura
4. Autenticación insegura
5. Criptografía insuficiente
6. Autorización no segura
7. Calidad del código del cliente
8. Manipulación de código
9. Ingeniería inversa
10. Funcionalidad Extraña

También se muestran la clasificación de los criterios son:

1. Interfaz gráfica: Se refiere a las características de formato de la app, es decir la manera en que está diseñada.

2. Contenido: Es la información contenida en la app.

3. Usabilidad: Se refiere a las características de la app para que ésta le permita al usuario manipular las funciones que ésta ofrece de manera adecuada, útil y sencilla.

4. Desempeño: Son las características técnicas de la app que le permiten hacer un adecuado uso de los recursos del sistema para evitar fallos.

5. Seguridad: Son las características técnicas de la app que le permiten preservar la confidencialidad, integridad de la información del usuario.

[30] Proyecto Abierto de Seguridad en Aplicaciones Web: proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro.

A continuación los criterios generales de las apps son las siguientes y algunos son mostrados en la ilustración 1:

1. Logotipo de la dependencia: La app debe mostrar el logotipo de la dependencia en el encabezado toda vez que se encuentre activa en el dispositivo móvil. Esto también va incluido en las tiendas para su descarga.
2. Versión de la app: Corresponde a la versión de la app publicada o a publicar. Es obligatorio este dato, deberá ser actualizado cada vez que se publique una nueva versión de la app.
3. Fecha de última publicación: Se debe realizar la publicación de versión más reciente de la app.
4. Dueño de la app: El responsable de publicar y administrar la app debe ser una Dependencia de la APF que es la entidad que ofrece la app a la ciudadanía.
5. Correo electrónico de contacto: Debe corresponder a una cuenta institucional de la Dependencia que ofrece la app.
6. Desarrollador: Los datos del desarrollador de la app deberán corresponder a la Dependencia de la APF pues ésta deberá contar con todos los derechos de dicha aplicación.
7. Apartado de derechos de autor: Los derechos de autor de la app deberán corresponder a la dependencia de la APF que la publique.
8. Política de privacidad: Sección informativa de la app en donde la Dependencia de la APF da a conocer a sus usuarios las políticas, basadas en la normatividad vigente aplicable a la protección de datos personales (aplica cuando ya se descargó).

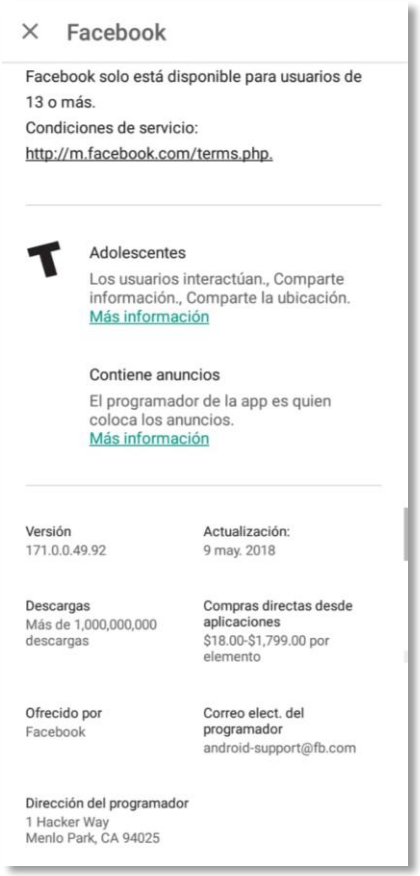

Ilustración 1. Criterios generales para Apps.

9. Términos y condiciones: Sección informativa de la app en donde se dan a conocer las responsabilidades que se tienen como usuario de la app (aplica cuando ya se descargó).
10. Instrucciones de uso: Breve guía que describa la manera de operar la app móvil de forma clara.
11. Nombre de la app: Con el que se le identifica en la tienda y en el ícono correspondiente en el dispositivo móvil.
12. Descripción de la funcionalidad: Tiene que contener una descripción de las funciones que ofrece la app al usuario, deberá corresponder a lo que actualmente opera la versión publicada o a publicar de la app.
13. Lenguaje ciudadano: La información de contenido de la app deberá contar con redacción simple para fácil entendimiento los usuarios, en caso de requerir el uso de conceptos complejos, que éstos se expliquen con claridad.
14. Uso de datos públicos: En caso de que la app haga uso de datos públicos, éstos deberán ser enviados a la UGD como archivos adjuntos en la ficha técnica.
15. Información publicada: Consistente con ficha técnica, la información de la ficha técnica deberá ser la misma que la que sea publicada en la tienda y en el contenido de la app para evitar desconciertos o inconsistencias.
16. Funcionalidad de búsqueda: La app que incluya contenido informativo deberá incluir una opción para facilitar que el usuario pueda realizar búsqueda de información.
17. Liberación de recursos del dispositivo móvil al salir de la app: La app deberá considerar en su funcionamiento, que se liberen los recursos del dispositivo móvil cuando el usuario salga de dicha app.
18. Tamaño de la descarga Medición en Megabytes del tamaño de la app e decir el espacio que ocupará en el dispositivo móvil.
19. Requerimientos técnicos de funcionamiento: Detalle técnico de los requerimientos de la app para su correcto funcionamiento: versiones de SO, memoria interna disponible, etc.

20. Correcta desinstalación: Cuando el usuario requiera desinstalar la app del dispositivo móvil ésta deberá liberar los recursos del dispositivo de forma completa (aplica cuando ya se descargó).
21. Servicios API[31] utilizados: En caso de app híbrida enumerar los servicios web de los cuales hace uso y la explicación de cada uno de ellos.
22. Recursos del dispositivo utilizados: Describe cuáles son los recursos del dispositivo móvil de los que hace uso y con qué finalidad deben estar muy bien redactados con los indicados al aplicar el botón de instalación desde el dispositivo.
23. Permisos: En el caso de que la app opere permisos de acceso éstos deberán funcionar adecuadamente.
24. Reporte de validación funcional: Este reporte deberá ser conforme a la descripción de la app y en incluir el listado de funcionalidades, descripción y el estatus Validado / No validado.
25. Reporte de resultado de pruebas de vulnerabilidades en ambiente productivo Este reporte deberá cumplir con los criterios de evaluación de vulnerabilidades para pruebas en el dispositivo y para pruebas del servicio web (Anonimo, MexicoDigital, 2017).

[31] Interfaz de programación de aplicaciones.

2.5 Amenazas de Seguridad en Aplicaciones Móviles.

Las amenazas se pueden presentar desde software hasta el hardware, existen dos tipos de amenazas: amenazas generadas por el usuario y amenazas externas:

Las amenazas generadas por el usuario incluyen cómo te conectas, dónde te conectas, qué haces cuando estás conectado y finalmente con quién te conectas. Las amenazas externas incluyen cosas como virus, malware, vigilancia, pérdida de datos y más.

Las principales se basan en:

a. Almacenamiento de datos inseguro: Tokens[32] de autenticación, historial, contraseñas, cookies, datos de ubicación y más.
b. Servidores inseguros: Los servidores que están siendo utilizados por las aplicaciones de hoy en día son cada vez mejores, pero esto no significa que se están asegurando correctamente. Las vulnerabilidades de los servidores permiten a los piratas informáticos acceder y robar datos.
c. Conexiones inseguras: Incluso si una aplicación está configurada para ejecutarse en *https,* eso no quiere decir que lo haga. Con demasiada frecuencia, estas conexiones volverán a una conexión http con el fin de aumentar la velocidad/disminuir el ancho de banda
d. Manejo inadecuado de la sesión: El manejo apropiado de la sesión significa que te desconectas después de tantos minutos de inactividad. Las malas aplicaciones, la mayoría de ellas, te mantendrán conectado indefinidamente o hasta que te desconectes (Rinaldi, 2017).

[32] Es un dispositivo electrónico que almacena claves criptográficas como: firmas electrónicas, datos biométricos, PIN.

Capítulo III: Privacidad y Seguridad en Redes sociales

3.1 Seguridad de los datos

Tiene su fundamento en la protección de los datos ante virus, malware es por eso que las apps de redes sociales se tienen que comprometer a garantizar la protección con los usuarios obteniendo así su confianza.

Hoy en día existen diferentes sistemas y niveles de seguridad para la identificación y acceso por ejemplo contraseñas de acceso, CURP, correo electrónico, huella dactilar digitalizada, generadores de código, preguntas de seguridad ya sea para la recuperación de contraseñas, cuentas de respaldo entre otros.

Los mencionados anteriormente en ocasiones no tienen éxito por la usabilidad de los mismos usuarios porque algunos no los configuran bien o simplemente no los usan.

3.1.1 Transparencia de datos

Es cuando el usuario quiere saber qué información tiene sobre él y que hacen con ella. Se da una parte del control y brindando transparencia en los datos aumenta la confianza en las redes sociales que proveen el servicio, con el objetivo de dar oportunidad al usuario de poder corregir, actualizar y borrar sus datos en el momento que lo apetezca, sin embargo hay apps que no dejan hacer muchos cambios bruscos en ciertos días (Peña R. M., 2014)

3.2 Privacidad en las Redes Sociales

Las redes sociales son usadas para diferentes objetivos ya sea compartir contenido, marketing, entrenamiento entre otros, esto a generando una gran cantidad de datos expuestos al momento en que se contestan campos como el estado civil, la ciudad de residencia, estudios, trabajos, religión son habituales en este tipo de redes sociales y mucha gente lo contesta pensando que es obligatorio para su registro para ser más activos pero la realidad es que se exponen al alcance de cualquiera.

Incluso algunos usuarios son fanáticos se exponerse a tal grado de dar a saber su geolocalización a cada instante, en algunas aplicaciones vienen con medidas restrictivas las cuales tiene que ser configuradas sin embargo algunos usuarios no tienen conocimiento de las restricciones, el aceptar a usuarios que no conozcan les da acceso a toda su información en los perfiles, también aplica aquí las restricciones para configurar la privacidad se muestran opciones como, confirmar la solicitud, reportar, bloquear y la opción por lógica se realiza es ignorar (Carrasco, 2011).

3.3 Configuración de seguridad y privacidad en Redes Sociales más populares en México

Se mostraran algunas interfaces de las Redes Sociales más populares en México basándose en los dos Sistemas Operativos móviles con mayor demanda por parte de los usuarios estos son iOS y Android.

1. Facebook V.171.0.0.49.92 / Messenger en Android

Se muestra en la Ilustración 2 los apartados General, Seguridad e inicio de sesión, privacidad, biografía y etiquetado, ubicación, bloqueo, idioma y Configuración de reconocimiento facial.

Ilustración 2. Configuración de la cuenta de Facebook en Android.

En la Ilustración 3: Se observa la Seguridad e inicio de sesión con los apartados: Opciones recomendadas, Donde iniciaste sesión, inicio de sesión, configurar seguridad adicional, opciones avanzadas.

- En opciones Recomendadas da la opción para elegir mínimo a 3 amigos los cuales deben confirmar la identidad del dueño de la cuenta por medio de un código de seguridad, después de registrar el código de seguridad tendrán acceso a la cuenta, este caso puede ser muy útil para recuperar la cuenta en caso de un hackeo.
- Donde iniciaste sesión: muestra el dispositivo, lugar, hora, fecha y si sigue activa la sesión, en caso de no reconocer la sesión se puede cerrar.
- Inicio de sesión: En este apartado hay dos opciones para iniciar sesión, una es la foto de perfil se ahorra el escribir la contraseña, la segunda opción es cambiar la contraseña en caso de cambiar la contraseña se pueden cerrar todas las sesiones activas en todos los dispositivos o simplemente cambiarla.

Ilustración 3. Seguridad e inicio de sesión.

- Configurar seguridad adicional: hay dos opciones, la primera es recibir alertas sobre inicios de sesión no reconocidos es decir, llegara un aviso informando que se ha iniciado una sesión en un dispositivo no conocido, la segunda opción es autenticar en dos pasos: esta opción se desglosan más opciones con métodos de autentificación es decir (U2F) llaves de seguridad mediante un NFC[33], otro son los códigos de recuperación se puede usar para iniciar sesión cuando no se tenga el dispositivo a la mano.

  Otra sección es autentificación de terceros se desglosa en contraseñas de aplicaciones, siguiendo de la autentificación de terceros esta opción sirve cuando no se tiene el dispositivo cerca o no cuenta no internet ni mensajes de texto.

  Por último se encuentra inicios de sesión autorizados, se tiene registrada una lista con los dispositivos ya conocidos usados recientemente estos ya no necesitan códigos de acceso.
- Opciones avanzadas: Se muestra una opción es Navegación segura, se encarga de dar una advertencia en el caso en que la navegación en un sitio web sea peligroso desde Facebook.

[33] Comunicación de campo cercano es una tecnología de comunicación inalámbrica, de corto alcance y alta frecuencia que permite el intercambio de datos entre dispositivos.

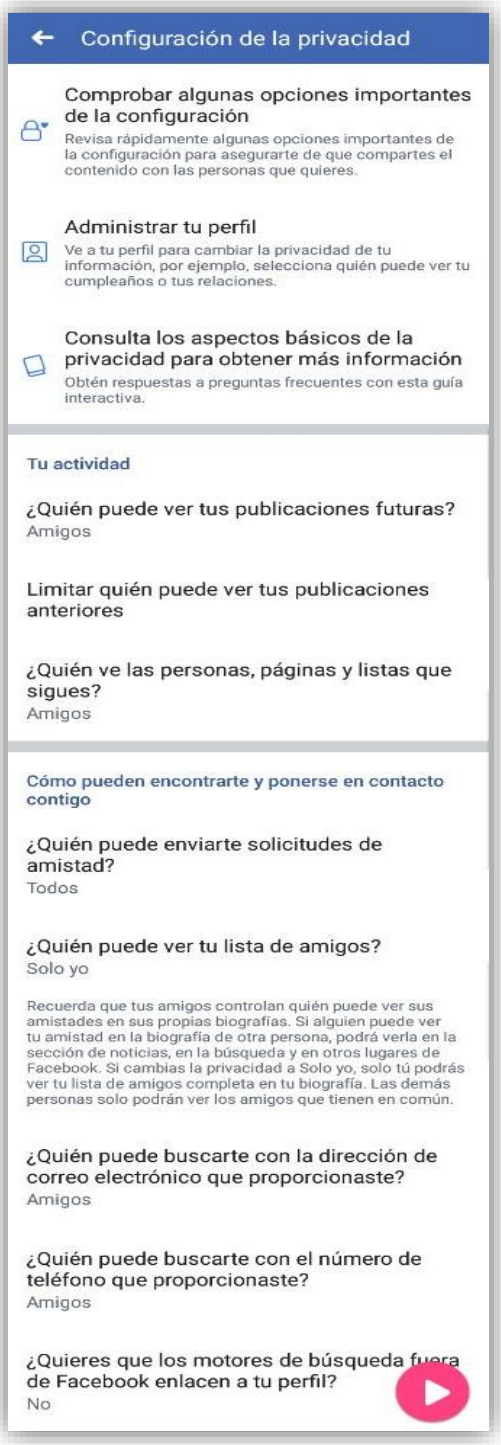

Ilustración 4. Configuración de la privacidad.

En la Ilustración 4 se resume la configuración de la privacidad

- Comprobar algunas opciones importantes de la configuración: Se pueden revisar y configurar del contenido que se comparte.

Es decir, la ubicación de la próxima publicación puede ser que todos vean la publicación, amigos, amigos excepto, amigos concretos, solo yo.

La privacidad del perfil como: teléfono, correo electrónico, fecha de nacimiento, cuidad de origen, situación sentimental, intereses, ciudad actual, formación académica todos estos datos tiene la opción de configurar la privacidad a todos, amigos, amigos excepto, amigos concretos, solo yo.

Privacidad de la aplicación se muestran todas las aplicaciones que se han iniciado sesión con Facebook se puede elegir quien vea la privacidad y otro caso eliminar la aplicación.

- Administrar tu perfil: Desde aquí se puede ver y cambiar la privacidad de la información por ejemplo, agregar formación academia, empleos, aptitudes profesionales, lugares recientemente visitados, información de contacto, información básica, etc.

- Tu actividad: tiene tres apartados donde se cuestiona y al mismo se pueden configurar, ¿Quién puede ver tus publicaciones futuras?, limitar quien puede ver tus publicaciones anteriores, ¿Quién ve las personas, páginas y listas que sigues?
- Como pueden encontrarte y ponerse en contacto contigo: se divide en cinco preguntas al igual que los anteriores se configuran, ¿Quién puede enviarme solicitudes de amistad?, ¿Quién puede ver tu lista de amigos?, ¿Quién puede buscarte con el número de teléfono que proporcionaste? Y ¿Quieres que los motores de búsqueda fuera de Facebook enlacen a tu perfil?

Ilustración 5. Configuración de ubicación.

En la Ilustración 5 se presenta donde se encuentran las secciones:

- Buscar Wifi: Notifica al usuario cuando hay redes de Wifi abiertas.
- Amigos cerca: Muestra a los amigos cuando estén en un rango de distancia o lugares con el usuario, se desglosa otra opción para controlar la privacidad de quien puede ver la actividad.
- Sugerencia de lugares: Mediante la ubicación del usuario Facebook da sugerencias de lugares que le puedan interesar.
- Historial de ubicaciones: Es una opción para guardar todo el historial de lugares que haya registrado su visita el usuario.

En la Ilustración 6 muestra cuando los usuarios bloqueados y desbloquear a otros usuarios quienes ya no podrán visualizar nada del perfil del dueño, incluyendo iniciar conversación, invitación a eventos o aplicaciones.

Ilustración 6. Usuarios bloqueados.

En la Ilustración 7 se observa el permiso y su aviso del sistema para comparar la foto de perfil y otras fotos para saber cuándo usuario aparece en más fotos y notificar.

Ilustración 7. Reconocimiento facial.

Messenger V.165.0.0.25.92

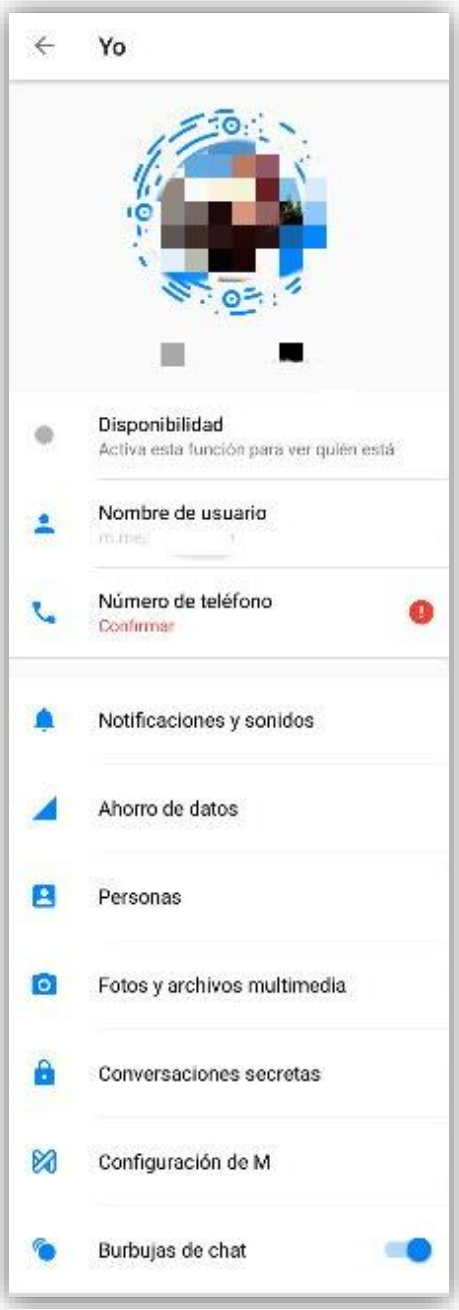

Ilustración 8. Interfaz de cuenta.

En la parte superior izquierda se encuentra la foto de perfil donde se ubican más opciones como se muestra en la ilustración 8.

Hay apartados donde muestra la disponibilidad de aparecer disponibles para los contactos, el nombre de usuario mismo que permite editarlo o copiar el enlace. Después el número de teléfono, notificaciones y sonidos, en la sección de fotos y archivos multimedia se puede configurar para permitir el acceso a al dispositivo y al almacenar.

Las conversaciones secretas se pueden activar, en un apartado se muestra los dispositivos con sesión abierta con su respectiva clave desde ahí se permite la eliminación el dispositivo desconocido en la lista.

1.2 WhatsApp V.2.18.142

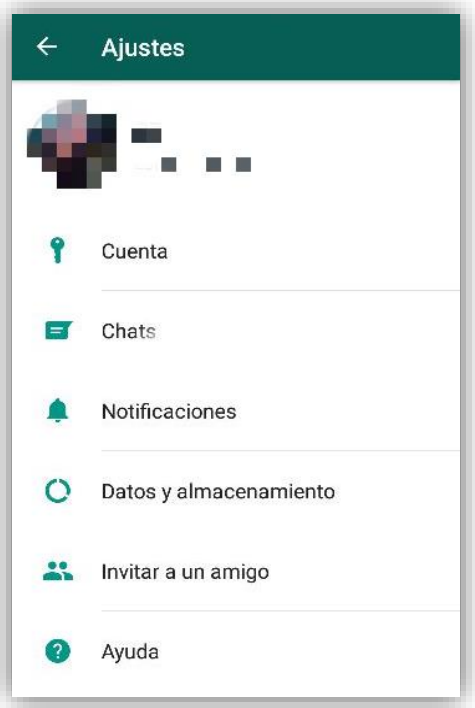

Ilustración 9. Menú de ajustes de WhatsApp.

Ilustración 9 presenta el menú de los Ajustes donde se encuentran opciones para configurar o examinar las configuraciones de privacidad y seguridad:

Ilustración 10. Ajustes de cuenta.

Ilustración 10 se expone la Cuenta: Se divide en cinco secciones:

- Privacidad: desde ahí se configura quien puede ver la información personas como la hora de última vez, foto de perfil, Información, Estado y Ubicación en tiempo real, en cada una de las opciones anteriores de configura como Todos, Mis Contactos y Nadie.

Mensajería se divide en dos secciones:

- Contactos Bloqueados: Esta opción es para no permitir que lleguen mensajes de otro usuario.
- Confirmación de lectura: Muestra cuando una persona ha leído el mensaje enviado, quienes han visto un estado, se puede activar o desactivar esta función sin embargo no aplica en los audios ya que si muestra cuando han sido reproducidos.

Este aparto es muy importante configurar mostramos menos información a personas que no tienen nuestro número telefónico.

- Seguridad: Esta opción habilita la protección de mensajes con cifrado de externo a extremo para que WhatsApp ni terceros no puedan leer ni escucharlos, da una opción de avisar cuando el código de seguridad de un contacto ha sido cambiado.
- Verificación de dos pasos: Es una verificación consiste en generar un PIN[34] cuando se registre el número telefónico de usuario en WhatsApp.
- Eliminar mi cuenta: Se da de baja la cuenta incluyendo el historial de mensajes, grupos y copias de historial.
- Chats: se encuentran varias secciones la más importante son Copia de seguridad e Historial de chats:

  Copia de Seguridad: se hace una copia de todos los chats incluidos los mensajes. Se puede configurar con la cuenta de Gmail que se guarden en la misma copia las imágenes, audios, videos, en la cuenta brindada.

  Historial de Chats: hay cuatros opciones donde se puede:

  Enviar chat por correo, Archivar todos los chats, vaciar todos los chats y eliminar todos los chats.

[34] Es un tipo de contraseña, sólo el dueño del PIN sabe cuál es, eso es para lo que fue creado, y tiene que ser suficientemente seguro, para que no entre gente no autorizada o use computadoras para descifrar el código.

WhatsApp Web: Se genera un scanner lector de código QR[35] se inicia sesión en un dispositivo ya sea en Tablet, PC, Laptop, Smartphone, etc.

También muestra cuando se tiene abiertas sesiones y da la opción de cerrar todas las sesiones o iniciar más.

En esta función de debe mantener un especial cuidado y revisar cotidianamente si se tienen sesiones abiertas sin autorización del usuario siendo víctima de alguien que espié.

1.3 YouTube V.13.17.5

Se resaltan en la ilustración 11.

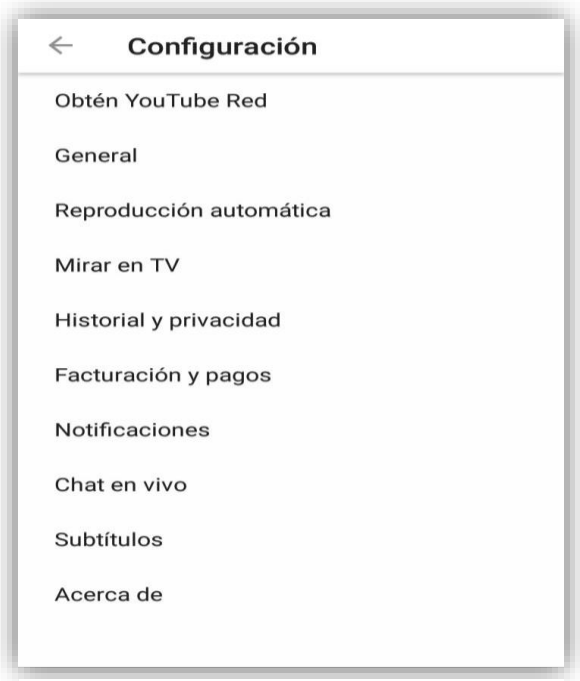

Ilustración 11. Configuración de YouTube.

- General

Ubicación: lugar donde se encuentra el usuario.

[35] Evolución del código de barras. Es un módulo para almacenar información en una matriz de puntos o en un código de barras bidimensional.

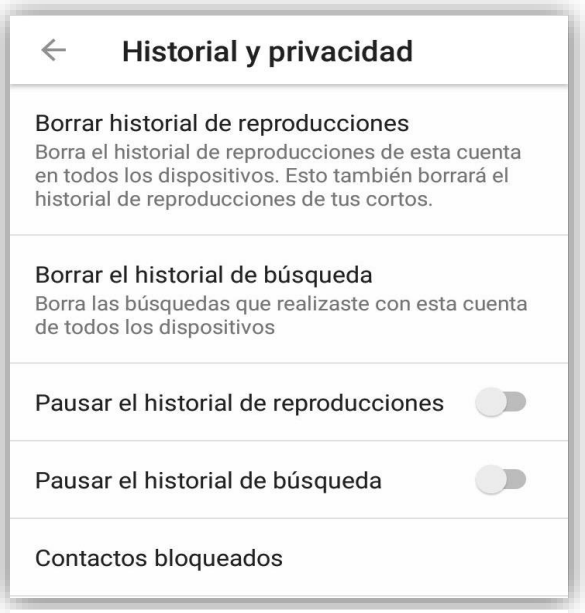

Ilustración 12. Historial y privacidad

- Historial y privacidad, ilustración 12.
  - Borrar historial de reproducciones: se elimina el historial de todos los videos reproducidos en todos los dispositivos con la sesión abierta.
  - Contactos bloqueados: no permite a un usuario seguir teniendo comunicación con el dueño.

1.4 Twitter V. 7.44.0

Se expone en la ilustración 13 donde se observa:

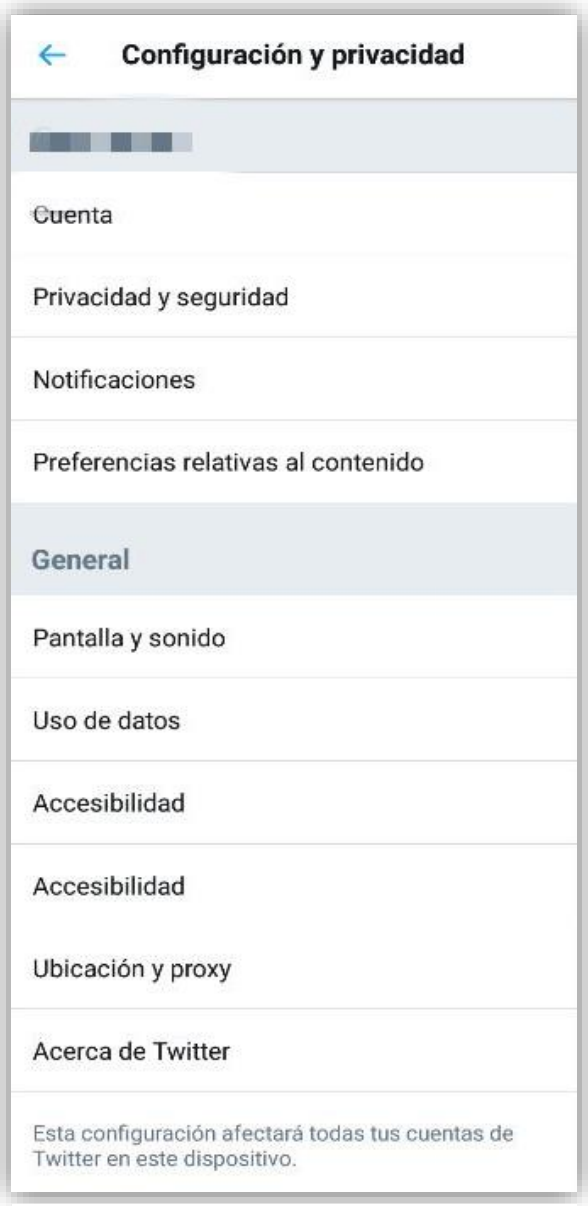

Ilustración 13. Configuración y privacidad de Twitter.

- Cuenta: Opción cambiar e ingresar el nombre de usuario, número de teléfono, correo electrónico, contraseña, seguridad.

  En seguridad cuando se activa es una verificación de inicio de sesión donde pedirá más información para confirmarla identidad y proteger la cuenta.

  Datos y permisos: se muestra el país del usuario y otra sección llamada datos donde muestra los datos de perfil y los de la cuenta que tiene en su posesión Twitter como: nombre de usuario, incluido el ID del usuario, correo electrónico, creación de la cuenta, genero, edad, idioma, ubicación del perfil.

  Número de dispositivos con la sesión abierta y vinculada, lugares donde ha estado, aplicaciones en el dispositivo, intereses de Twitter, intereses de socios, historial de acceso a la cuenta.

Ilustración 14. Privacidad y seguridad.

En la ilustración 14 se observa Privacidad y seguridad:

- Tweets[36]: protege los tweets, da la opción de que se active la opción de solo los seguidores puedan verlos.
- Etiquetado de fotos: da la opción de configurar cualquier persona pueda etiquetar en las fotos, solo las personas que siguen al usuario y desactivado.

Mensajes directos:

- Recibir solicitudes de mensajes se puede activar o desactivar esta opción para que cualquier seguidor envié mensajes.
- Mostrar configuración de lectura: activar o desactivar la opción para avisar que se ha leído el mensaje.

Seguridad:

- Mostrar fotos y videos que puedan incluir contenido delicado: se activa o desactiva.
- Cuentas bloqueadas: Esta opción es para no permitir que lleguen mensajes de otro usuario.
- Cuentas silenciadas: No da notificación de cualquier actividad de este usuario.
- Palabras silenciadas: No se muestra la notificación con palabras activadas.

[36] Mensaje que podemos enviar a través de Twitter.

- Personalización y datos:
    - Personaliza anuncios: se puede activar o desactivar la opción de mostrar anuncios basados en los intereses del usuario.
    - Personaliza en todos tus dispositivos: se usa la misma configuración de personalización en los dispositivos reconocidos.

Ilustración 15 se resalta en la sección de General:

Ilustración 15. Configuración con el apartado general.

Ubicación: permite la ubicación de Twitter se activa desactiva la opción.

1.5 Instagram V.45.0.0.17.93

Se exponen en la ilustración 16 las principales opciones de configuraciones de cuenta:

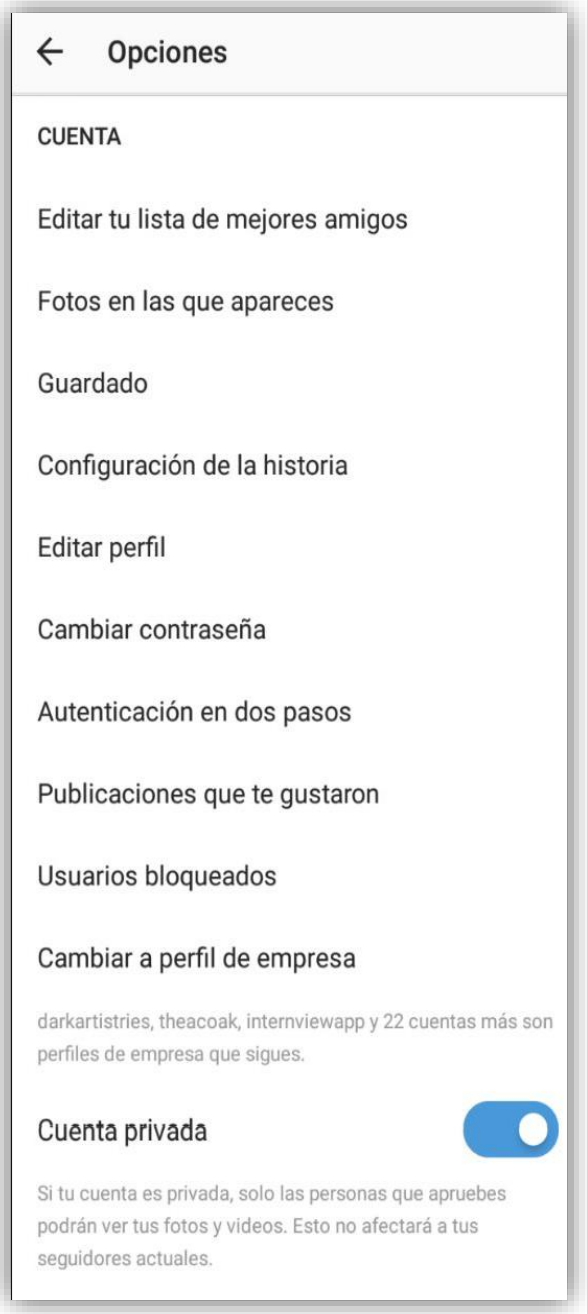

Ilustración 16. Opciones en Instagram.

- Cambiar contraseña.
- Autentificación en dos pasos: Se solicita un código de seguridad para confirmar la sesión.
- Usuarios bloqueados: Esta opción es para no permitir que lleguen mensajes de otro usuario.
- Cuenta privada: Se activa o desactiva el contenido de la cuenta con el fin de tener un control de saber quién ve las publicaciones.

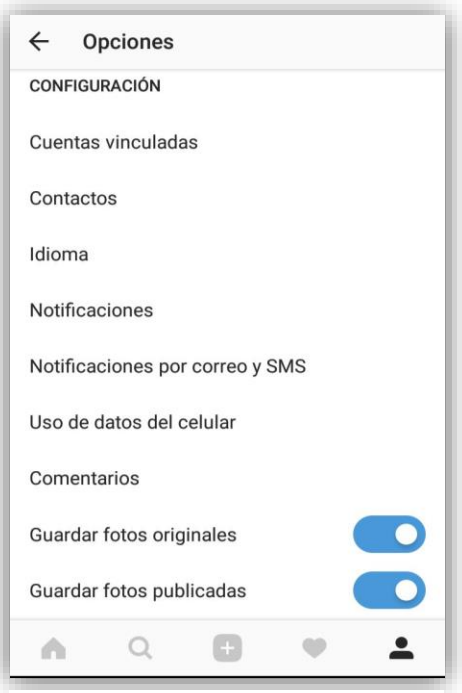

Ilustración 17. Opciones de Configuración.

En la Ilustración 17 muestra

- Cuentas vinculadas: muestra las cuentas que se pueden vincular y las que ya están vinculadas.
- Contactos: se puede sincronizar los contactos con el dispositivo.
- Notificaciones: muestra la opción de quien puede dar Me gusta da a elegir de las opciones: desactivadas, de personas a las que sigo y todos.
- Comentarios: usuarios que pueden comentar da a elegir de las opciones: desactivadas, de personas a las que sigo y todos.
- Me gusta en comentarios: quienes dan me gusta en comentarios da a elegir de las opciones: desactivadas, de personas a las que sigo y todos.
- Me gusta y comentarios en fotos en las que apareces: desactivadas, de personas a las que sigo y todos.
- Solicitudes de Seguidores: quien puede seguirte desactivadas y todos
- Solicitudes aceptadas: desactivadas y todos.
- Amigos de Instagram: desactivadas y todos.
- Solicitudes de Instagram Direct: desactivadas y todos
- Instagram Direct, Fotos en que apareces: desactivadas y todos
- Recordatorios: desactivadas y todos
- Primeras publicaciones e historias: desactivadas y todos
- Novedades de productos: desactivas y activas.
- Número de reproducciones: desactivas y activas.
- solicitud de ayuda: desactivas y activas.
- Videos en vivo: desactivas y activas.
- Encuestas de historias: desactivas y activas.

2. Facebook V.161.0 / Messenger en iOS

En la ilustración 18 se muestra los apartados de las diferentes configuraciones en cada sección.

Ilustración 18. Configuración en Facebook de iOS.

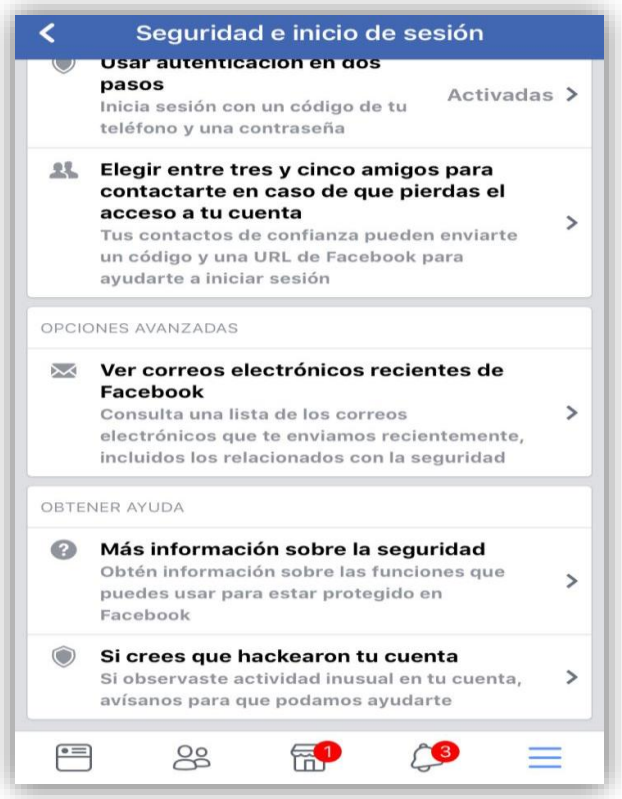

Ilustración 19. Seguridad e inicio de sesión.

En la ilustración 19 se observa las diferentes opciones para iniciar sesión son:

- Usar autentificación en dos pasos: al momento en que se inicia sesión con un dispositivo no reconocido envía notificación al usuario de la cuenta.
- Elegir entre tres y cinco amigos para contactarse en caso de que pierdas acceso a tu cuenta: se eligen a amigos de confianza quienes recibirán un código para poder acceder a la cuenta en caso de que el dueño no pueda.

- En opciones avanzadas se encuentra un apartado para ver correos electrónicos recientes de Facebook, aquí se pueden consultar los correos relacionados con la cuenta y su configuración de seguridad.
- Más información sobre la seguridad: una sección donde hay artículos sobre la configuración y ve cómo funciona.
- Si crees que hackearon tú cuenta: Facebook ofrece diferentes opciones de acciones para realizar en caso de que tu cuenta haya sido víctima.

En la ilustración 20 se presenta los siguientes apartados:

Ilustración 20. Biografía y etiquetado.

- Se puede revisar y al mismo tiempo configurar lo que se quiere mostrar a los amigos de la cuenta y quienes no lo son eso incluye publicaciones del usuarios y las que le hacen, quien las puede ver, quien puede etiquetarte en publicaciones o fotos.
- Revision de etiquetas y aprovechar si desean que aparezcan y se puedan controlar quien las ve.

En la siguiente ilustración 21 se resume la configuración de ubicación, donde se puede mostrar la ubicación o activar notificaciones de amigos que se encuentren cerca así como lugares y WiFi libre. También se puede ver el historial de las ubicaciones que ha estado el usuario.

Ilustración 21. Configuración de ubicación.

Están son algunas de las configuraciones se encuentran en Facebook en iOS al parecer son las parecidas que en Android, solo varia sus interfaces.

Messenger V. 153.0

Ilustración 22. Interfaz de cuenta Messenger.

En la parte superior izquierda se encuentra la foto de perfil donde se ubican más opciones como se muestra en la ilustración 22.

Hay apartados donde el nombre de usuario mismo que permite editarlo o copiar el enlace. Después el número de teléfono, notificaciones y sonidos, en la sección de fotos y archivos multimedia se puede configurar para permitir el acceso a al dispositivo y al almacenar.

Las conversaciones secretas se pueden activar y muestra los dispositivos que tiene la sesión abierta con su respectiva clave también se puede eliminar el dispositivo de la lista.

2.2 WhatsApp V.2.18.30

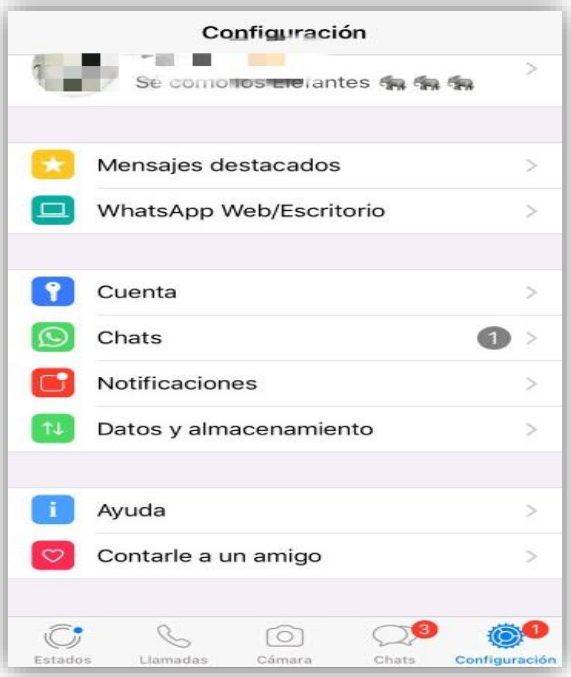

Ilustración 23. Configuración en WhatsApp.

En la ilustración 23 se resalta la configuración general de WhatsApp, donde tiene las opciones de:

- WhatsApp Web / Escritorio: se puede iniciar sesión desde una página oficial WhatsApp en un dispositivo con acceso a internet.

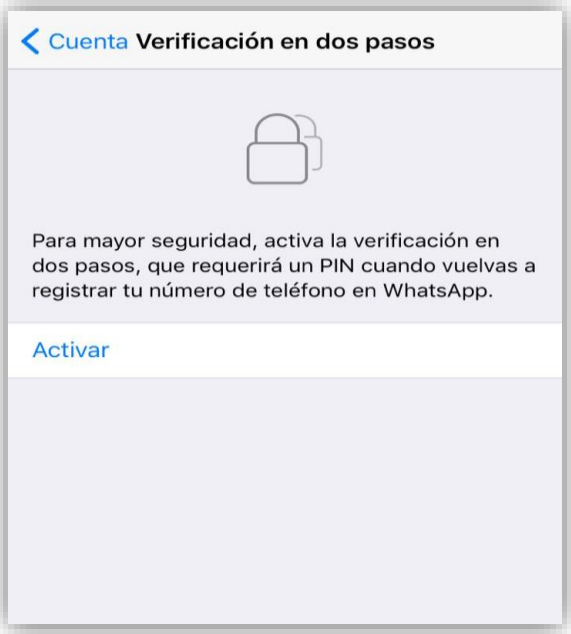

Ilustración 24. Verificación en dos pasos.

En la ilustración 24 en el menú de cuenta se muestra la opción de verificación en dos pasos con el fin de que llegue la notificación si re vuelve a registrar para cambiar de cuenta

Ilustración 25. Opción de Seguridad.

También en el menú cuenta se expone en la ilustración 25, viene la opción de activar el aviso en caso de que un contacto cambie su código se seguridad cifrado.

Ilustración 26. Configuración de Privacidad.

En la ilustración 26 se muestra la configuración de privacidad en última vez, foto de perfil, información, estados, la ubicación en tiempo real en estas opciones aparecen estas configuraciones como son: todos, mis contactos y nadie.

En la ilustración 27 se muestra la configuración de las notificaciones, desde aquí se pueden configurar las notificaciones con sonidos, previa visualización.

Ilustración 27. Configuración de notificaciones.

2.3 YouTube V.13.06

Se observa en la ilustración 28 se observa la configuración así como su privacidad donde se puede borrar el historial de reproducciones, el historial de búsqueda.

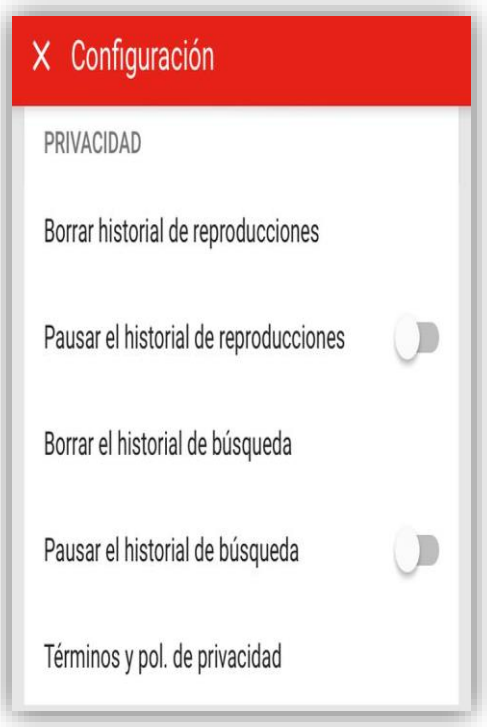

Ilustración 28. Configuración de Privacidad en YouTube.

2.4 Twitter V. 7.17.1

En la ilustración 29 se resaltan las opciones para proteger los Tweets, controlar los mensajes directos ya sea de cualquier persona y mostrar configuraciones de lectura.

Ilustración 29. Privacidad y seguridad en Twitter.

Ilustración 30. Seguridad.

En la ilustración 30 se observa la seguridad donde está la opción de verificar el inicio de sesión para mantener más segura y tener un control de los dispositivos que tiene iniciado la sesión.

2.2 Instagram V.34.0

En la ilustración 31 se encuentran las opciones de cuenta para configurar o cambiar diversas secciones como:

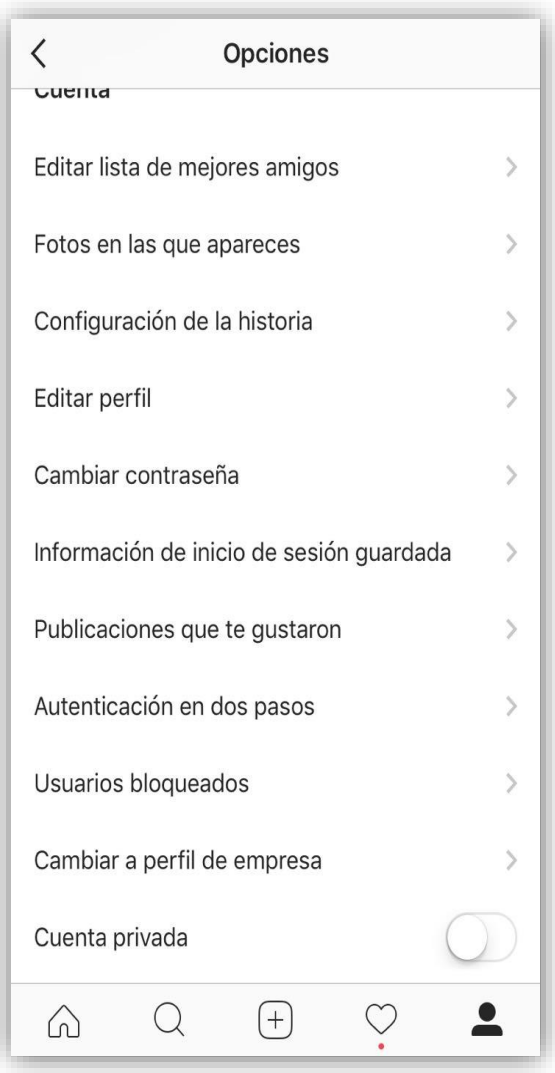

Ilustración 31. Opciones de Cuenta en Instagram.

- Cambiar la contraseña, información de inicio de sesión guardada, autentificación en dos pasos: Se solicita un código de seguridad para confirmar la sesión.
- Usuarios bloqueados: Esta opción es para no permitir que lleguen mensajes de otro usuario.
- Cuenta privada: Se activa o desactiva el contenido de la cuenta con el fin de tener un control de saber quién ve las publicaciones.

Como datos curiosos se menciona los datos a la que tiene acceso Facebook en el momento en que se ingresa a ser usuario en esta Red Social:

1. Localización
2. Edad
3. Genero
4. Idioma
5. Nivel educativo
6. Área de estudios
7. Colegio
8. Propiedad y tipo de vivencia
9. Usuarios con nuevas relaciones
10. Si está lejos de su familia o cuidad natal
11. Usuarios con nuevos trabajos
12. Usuarios recién casados
13. Padres y familia
14. Padres a la espera de un bebé
15. Conservadores y liberales
16. Para quien trabajas
17. Título profesional
18. Intereses
19. Lo que tienes pensado comprar por ejemplo un carro (tipo, marca, precio)
20. Compras recientes y futuras compras
21. Navegador de internet
22. Sistema operativo
23. Si perteneces a una corporación de crédito, banco nacional o regional
24. Número de tarjetas activas
25. Usuarios que escuchan radio
26. Preferencia de programas de televisión
27. Usuarios que han adquirido recientemente un dispositivo móvil
28. Tipo de ropa que usan en casa

29. Momento del año en que el usuario hace más compras
30. Usuarios que compran comestibles, productos de belleza, medicamento, producto para el hogar, productos para niños o mascotas
31. Restaurantes que frecuentan
32. Cuanto tiempo viviste en tu casa
33. Cuando se viaja con frecuencia y el momento en que regreso del viaje. (Villena, 2017)

Con algunos mencionados en caso poner información verdadera y otros casos es lo contrario, es información que se da inconscientemente cotidianamente mediante la interacción con las redes sociales.

Considerando que en la actualidad la mayoría las apps tiene funciones más allá de su objetivo principal con el que fueron creadas es decir recolectan datos sin que los usuarios tengan conocimiento o a excepción de los que si se tomaron el tiempo para leer los permisos y condiciones de las mismas, es posible distinguir dos modalidades principales de recolección de datos en las aplicaciones móviles: la primera son los datos recogidos por la propia aplicación, como las fotos, textos y metadatos que la aplicación por ejemplo Facebook recoge de los usuarios para el uso de la propia plataforma, la otra modalidad cuando las empresas intermedian la relación entre los desarrolladores de las aplicaciones y los servicios de tracking, es decir estas empresas funcionan como intermediarios entre la aplicación y las empresas de tracking; con las modalidades anteriores los desarrolladores de las apps pueden recoger, procesar y vender datos personales, es importante saber a quién se da acceso a los datos personales (Damasio Goulart & Da Silveira Serafim , 2017).

Capítulo IV: Recomendaciones y prevenciones al usuario

Todas las prevenciones y recomendaciones no son obligatorias para ningún usuario, son medidas de seguridad para tener más conocimientos en la utilización y accesos con los datos personales mediante el uso de apps de redes sociales.

4.1 Revisar los permisos de acceso.

En el instante en que quiera descargar una app para el uso en el dispositivo y se da un el botón instalar aparece una pequeña pantalla donde muestra los requerimientos de acceso a ciertas funciones del dispositivo, ya indicados en el Capítulo II estándares de seguridad en apps móviles, además se menciona que después de la actualización de Android 6.0 se pueden desactivar los permios de acceso desde el menú de configuración. Sin embargo se recomendando revisar los accesos que requiere la app y pensar si realmente se requiere esta app en el dispositivo.

4.2 Leer los términos y condiciones.

Se debe considerar leer todo lo que se acepta y más cuando es referente a lo legal y con los datos personales, con lo que se refiere en algunas redes sociales se da permiso a usar todo el contenido en la cuenta por ejemplo, imágenes, videos, las publicaciones, etc. Estas acciones ya se están haciendo muy cotidianas

Se menciona también que es obligación del usuario tener actualizada su información eso en el caso de Facebook, el caso de Twitter consentimos rastrear la dirección IP, tipo de navegador, sistema operativo, página web de referencia, páginas visitadas, ubicación, operador de telefonía móvil, dispositivos y aplicaciones IDs, términos de búsqueda e información de las cookies. Twitter dice ser una red social respetable con sus política de términos y condiciones, esta red social puede cambiarla sin previo aviso a sus usuarios, esto quiere decir tal vez en un futuro sea el dueño de los tweets así como Facebook.

En el caso de Instagram sus términos legales establecen por alguna razón, una idea es considerada interesante por Instagram puede utilizarla libremente, por supuesto sin pagar alguna cantidad monetaria (Zuriguel, 2014).

Las políticas de YouTube son similares a la de Facebook, con la información y/o videos puede retenerlos en su propiedad no importa ya han sido borrado.

Confiar en que las redes sociales tenga la debida privacidad al mantener toda la información de los usuarios es lo único que pueden hacer los usuarios una vez que ya han compartido datos en sus cuentas, y a los usuarios que no han compartido contenido muy excesivo se recomienda verificar si realmente vale la pena compartirlo en su cuenta.

4.3 Uso de configuraciones de seguridad y privacidad.

Anteriormente se muestran los menús en las apps de redes sociales más populares donde se pueden hacer uso.

a. Publico o privacidad la cuenta de usuario, en algunas apps se muestras en acceso directo la privacidad al hacer una publicación se da a elegir al usuario con quien quiere compartir de forma pública o privada, es recomendable inspeccionar como está configurado. En la mayoría de las veces los criminales usan la información que se puede ver en los perfiles para fines de robo, extorciones, fraudes, suplantación entre otras.
b. No aceptar solicitudes ya sea de amistad, seguidores esto depende con la red social, de personas que no sea conocidos frente a eso no es posible que el criminal tenga acceso a los datos personales esto aplica en los usuarios que tenga previamente configurada su privacidad de lo contrario no sirve de nada, también asegúrate de la identidad de todos tus contactos que sean quienes dicen ser.
c. Cuidar lo que publica: Todas las veces que se publica algo en una red social se deja de tener el control sobre ese contenido, no importa que sea borrado por el usuario quedará como mínimo registrado en los servidores de la red social y cualquiera que lo haya visto puede haber hecho uso de esa información, ya sea difundiéndola o copiándola.

d. Virus en redes sociales: Actualmente existen diversas formas de divulgar los virus, en las redes sociales lo más común es encontrase con link de supuestas páginas de interés para el usuario inmediatamente después que se abre el link se descargan los virus o con redirección a páginas donde piden llenar un formulario con los datos personales esto se llama.
e. Considera revisar las aplicaciones instaladas y ten cuidado con publicaciones sospechosas, sin importar si son emitidos de contactos conocidos.
f. Las principales redes sociales se toman muy en serio los problemas de seguridad de sus usuarios. Lo cual significa la su alta respuesta en caso de tener algún problema contactar con ellos a través de los mecanismos de contacto o de denuncia que facilitan.
g. No compartir fotos ni vídeos en los que aparezcas en situaciones comprometidas (sexting) Phishing (Anonimo, Oficina de Seguridad del Internauta, 2016).
h. En caso de usar una cuenta para fines laborales o para dar a conocer negocios evitar publicar contenidos y fotos personales, centrando únicamente a un fin informativo.

4.3.1 Medios de autentificación.

Existen tres formas de identificar a un usuario, por algo que eres, por medio de la biometría, algo que tiene el usuario y contraseña.

Las contraseñas son la forma efectiva y flexible funciona con un proceso de autentificación

- El sistema solicita usuario y contraseña.
- El usuario y contraseña son trasladados hacia el servidor para realizar la comparación con los almacenamientos en el sistema.
- Si la comparación es positiva da el acceso.

Puede tener inconvenientes como:

- Olvido de contraseña.
- Un tercero puede ver cuando se teclea la contraseña o la utilización de programas por ejemplo el keylogger este programa graba todo lo que se teclea en un archivo.
- La contraseña puede ser legible en él envió entre el dispositivo y el servidor.
- Un tercero acceda a la fuerza probando todas las contraseñas posibles.

Se recomienda el uso de estas soluciones.

a. Usar contraseñas fáciles de recordar.
b. Verificar que nadie pueda ver cuando se teclea una contraseña o aislarse.
c. Registrar los intentos fallidos de autentificación por cada fallo sucesivo.
d. Longitud suficiente: usualmente debe der de ocho caracteres, es esencial para prevenir el criptoanálisis.
e. No debe pertenecer al entorno en que se esta es decir no relacionada con la familia, gustos o terminología profesional.
f. Debe tener caracteres diferentes de los habituales, como mayúsculas o números a mitad de palabra.
g. Cambiar de forma regular las contraseñas.
h. Evitar dar o prestar la contraseña a otros usuarios.
i. La autentificación fundamenta en la comprobación de la identidad de una persona, por medio de la comparación, que proporciona usuario una pregunta de seguridad o algún otro medio de autentificación.
j. Cifrado es una técnica popular es ocupado en varios aspectos (Canal, Capitulo tres: Medidas, 2004).
k. Implementar el uso de la verificación en dos pasos están implementadas en las redes sociales como seguridad.

4.4 Recomendaciones generales.

1. Demostrar la educación sin importar si es mediante el uso de redes o en la vida real, omite enviar mensajes ofensivos a los usuarios, siempre es importante mantener una buena comunicación y mostrar los valores. Debes ser respetuoso y tratar con educación a tus contactos.
2. Verificar la apps sea de una fuente confiables es decir de las propias tiendas virtuales en el dispositivo.
3. Explorar los comentarios de los usuarios sobre la app.
4. No descargar apps que no han sido usadas por los demás usuarios, es decir fijarse en el número de descargas sea considerado creíble (Padilla, 2016).
5. Abstente de revelar tu domicilio o teléfono de contacto en las redes sociales para evitar que los criminales la adquieran y tengan acceso directo a ti.
6. Evita comentar que vas a salir de casa o estarás fuera por mucho tiempo para evitar los delincuentes o intrusos.
7. No publicar fotos o vídeos que muestren aspectos negativos o poco llamativos de tu vida. Esto podría hacerte perder muy buenas oportunidades laborales.
8. No facilites los datos de documentos de identificación o tarjetas de crédito que puedan dar lugar a un mal de los mismos (Anonimo, Ayuda Ley Proteccion de Datos, 2016).
9. Evitar que los niños tengan acceso a redes sociales o cuidar que sitios frecuentan de lo contrario se ponen en riesgo de cyberbulling.
10. Configurar la navegación por el protocolo HTTPS[37].
11. Evitar hacer clic en aquellos enlaces publicados por contactos conocidos sin embargo no hay garantía de seguridad.

[37] Cifrado establecido en SSL/TLS para crear un canal cifrado más adecuado para la transferencia de información sensible como son usuario y claves de paso, que el http.

12. Si se sospecha de la legalidad de un mensaje, es recomendable buscar partes del mismo o incluso el link dentro del buscador de la Red social que esté usando y observar tanto su repetición como las opiniones de la comunidad.
13. No acceder a sitios web de dudosa reputación.
14. Actualizar el sistema operativo y aplicaciones.
15. Tener precaución con los resultados arrojados por buscadores web.
16. Evitar la ejecución de archivos sospechosos.
17. Utilizar tecnologías de seguridad, como lo pueden ser antivirus, anti-Malware, limpiadores de basura, etc., (Anonimo, welivesecurity, 2014).
18. Utilización de VPN[38].
19. Uso de Firewall.
20. No usar las redes sociales como inicios de sesión para otros sitios (Rinaldi, 2017).
21. No tener sesiones abiertas automáticas o con contraseñas guardadas.
22. Crear copias de seguridad de los datos e información importante.
23. Desconfiar de mensajes emitidos de empresas con faltas de ortografía.
24. No descargar archivos enviados desde las redes sociales pueden ser virus o desactiva las descargas automáticas.
25. Evita compartir cadenas con links en el contenido de otros contactos se consideran spam.
26. No aceptar mensajes de desconocidos desde las redes sociales usualmente son estafas.
27. Solo tener activo el WiFi, bluetooth, GPS y demás herramientas cuando se tiene habilitadas que sus funciones aumentan el consumo de la batería.

[38] Es una tecnología de red de computadoras que permite una extensión segura de la red de área local sobre una red pública o no controlada como Internet.

Revisar que todas app tengas en su descripción la siguiente información mencionada anteriormente en el Capítulo III en criterios generales de las apps.

En caso de que su dispositivo móvil le dure poco la batería, se escuchen ruidos cuando habla por teléfono, se apaga o reinicia, publicidad sin estar ocupando una app es posible tener un virus usualmente son usados para espiar, se recomienda restablecer el dispositivo de fábrica instalando las apps conocidas y esenciales.

Conclusiones y aportaciones

Al realizar esta investigación me informe de muchos significados así como sus funciones que son representados en la vida cotidiana tanto para personas usuarias de redes sociales y las que no tienen cuenta, no obstante todos son poseedores de datos personales en el momento de hacer algún trámite actualmente ya todo con la ayuda de la tecnología y brindan sus datos personales, esto significa que también pueden ser víctimas.

Respecto a los usuarios de redes sociales es muy común hoy en día tener una cuenta, es usada como medio de comunicación entre familia, amigos, parejas incluso de negocios, todas estas relaciones se comunican, intercambian mensajes tal vez con cierto contenido de información importante o simplemente información sin importancia pero esto lo decide los criminales ya que pueden usar análisis de tráfico para poder tener conocimiento y poder usar al usuario con pequeños detalles de su vida personal por ejemplo, robo, estafa, suplantación, cyberbulling, espionaje, lectura o copia de información, manipulación de datos, existen otras más amenazas.

Investigando en el desarrollo de aplicaciones observe que hay muchas páginas de sitios web o aplicaciones que ayudan a programar o desarrollar más aplicaciones según sea el propósito, entonces la persona no tiene conocimiento de con que código o categoría se genera su aplicación, esto es un punto vulnerable ya que no conoce debidamente su aplicación.

Al tener una cuenta en las redes sociales instantáneamente se hace una identidad digital es igual que la identidad real solo que en la digital es más sencillo mentir o hacer cosas sin tener la conciencia esto no bueno para la reputación en la identidad real, en algunos casos las empresas realizan búsquedas e inspeccionan el perfil de los candidatos esto significa que puedan ayudar o perjudicar la imagen requerida por la empresa u organización, es importante saber que se debe compartir y que no se debe compartir.

El configurar y hacer uso de las medidas de seguridad ofrecidas en cada red social ayuda a que por lo menos en criminales de clase baja no tengan tan fácil el acceso a nuestros datos, si está en nuestras manos el poder restringir algunos datos usémonosla por nuestra seguridad y tranquilidad.

Recuerda que hay redes sociales en donde por seguridad piden la edad de 15 años para ser usuarios ya que más que una red puede ser un peligro para la integridad sumando el incumplimiento con las normas, haciendo referencia a toda la población que crean cuentas sin cumplir con los requerimientos adecuados a su vez exponiendo sus datos por todo el mundo, como hemos dicho la protección de datos empieza con la conciencia de uno mismo.

Es impórtate saber o tener presente todos los delitos o amenazas que existen para evitar ser víctimas ya que un gran número de delitos cometidos es por la mala configuración con los usuarios ellos mismos dan los datos inconscientemente mediante la ingeniería social.

No hay aplicaciones móviles seguras de una intervención por hackers o criminales, así como tampoco, hay redes sociales que protejan al 100% los datos personales siempre hay una forma de cometer un delito informático no importa que la tecnología avance y vaya actualizándose, los criminales igual se van actualizando es decir avanzan en conjunto.

Concluyendo si al menos las redes sociales no son seguras por sus debidas políticas de seguridad y sus términos de condición, nosotros como usuarios fomentemos y tengamos la lógica y conciencia de no compartir información privada de clase alta así como datos personales sensibles, una vez que entras en la red se pierde el control de su privacidad.

Esta investigación aporta:

a. Los conocimientos en la seguridad de apps de redes sociales.
b. Saber cuánto saben de nosotros las redes sociales, para que son usados los datos personales y quienes pueden tener acceso a ellos en el momento en que son dados a conocer mediante las redes sociales.
c. Crear seriedad y prudencia al leer los términos y condiciones antes de simplemente dar aceptar.
d. Reflexionar el contenido que compartimos en las redes sociales sabiendo que puede ser público y ser utilizado en contra de nosotros haciéndonos vulnerables.
e. Desde la perspectiva en informática dar conocer los delitos y amenazas minimizando el número de los robos y/o delitos.
f. Conocer que hay un marco de legalidad el mundo de las apps de redes sociales.
g. Desde el ámbito familiar se debe considerar configurar el uso de Internet ante los menores de edad.

Referencias

Alonso Rebolledo Ruy. (18 de Mayo de 2017). *El economista*. Obtenido de 7 datos sobre los usuarios de internet en México en el 2017: https://www.eleconomista.com.mx/empresas/7-datos-sobre-los-usuarios-de-internet-en-Mexico-en-el-2017-20170518-0161.html

Anonimo. (2005). *Gitanos*. Obtenido de https://www.gitanos.org/publicaciones/guiapromocionmujeres/pdf/03.pdf

Anonimo. (13 de Enero de 2010). *Revista Vincuando*. Obtenido de Cómo disminuir los delitos cibernéticos y su impacto económico: http://vinculando.org/articulos/software_antivirus_y_delitos_ciberneticos_impacto_economicos.html

Anonimo. (Septiembre de 2011). *tuinterfaz*. Obtenido de Hacia una cultura en el manejo de la información: https://tuinterfaz.mx/articulos/2/13/ley-federal-de-proteccion-de-datos-personales-en-posesion-de-los-particulares-lfpdppp/

Anonimo. (2012). *Definicion abc*. Obtenido de Definición de Usuario: https://www.definicionabc.com/tecnologia/usuario.php

Anonimo. (Enero de 2014). *welivesecurity*. Obtenido de Guía de Seguridad: https://www.welivesecurity.com/wp-content/uploads/2014/01/documento_redes_sociales_baja.pdf

Anonimo. (23 de Noviembre de 2015). *Emprendedores.* Obtenido de Requisitos legales que debe cumplir una app: http://www.emprendedores.es/gestion/requisitos-legales-app-lanzar-aplicacion

Anonimo. (03 de Octubre de 2016). *Ayuda Ley Proteccion de Datos*. Obtenido de Descubre cómo proteger tus datos personales en Internet: https://ayudaleyprotecciondatos.es/2016/10/03/proteger-datos-personales-internet/

Anonimo. (06 de Junio de 2016). *Ayuda Ley Protecion de Datos*. Obtenido de Guía de Protección de Datos para desarrolladores de aplicaciones móviles: https://ayudaleyprotecciondatos.es/2016/06/06/normativa-lopd-aplicaciones-moviles/

Anonimo. (2016). *Calameo*. Obtenido de Redes sociales y Delitos informaticos: http://es.calameo.com/read/00147548937c39a0510af

Anonimo. (2016). *Oficina de Seguridad del Internauta*. Obtenido de El dia en que Alicia descubrio que habia "otra" Alicia: https://www.osi.es/es/redes-sociales

Anonimo. (28 de Enero de 2017). *20minutos*. Obtenido de Permisos que concedes al instalar aplicaciones en el móvil: ¿sabes qué significan?: https://www.20minutos.es/noticia/2938118/0/permisos-aplicaciones-que-significan/

Anonimo. (09 de Mayo de 2017). *Banshai*. Obtenido de Aplicaciones Móviles - Política de Privacidad: http://banshai.com/docs/poltica-de-privacidad-aplicaciones-moviles/

Anonimo. (2017). *Definicion abc*. Obtenido de Definición de Intimidad: https://www.definicionabc.com/social/intimidad.php

Anonimo. (2017). *IVAI.* Obtenido de Categorias de Datos Personales: http://ivai.org.mx/DatosPersonales/Archivos/Interes/CuadroCategorias.pdf

Anonimo. (Noviembre de 2017). *Mastermagazine*. Obtenido de Definición de Aplicación: https://www.mastermagazine.info/termino/3874.php

Anonimo. (Noviembre de 2017). *MexicoDigital.* Obtenido de Gobierno Digital Estándar en aplicaciones móviles: https://www.gob.mx/cms/uploads/attachment/file/275885/Est_nda_de_aplicaciones_m_viles.pdf

Anonimo. (15 de Marzo de 2017). *SDPnoticias.com*. Obtenido de 3 de cada 4 usuarios de telefonía celular en México tienen smartphone: INEGI: https://www.sdpnoticias.com/tecnologia/2017/03/15/3-de-cada-4-usuarios-de-telefonia-celular-en-mexico-tienen-smartphone-inegi

Applicantes. (2017). Obtenido de Política de Privacidad: http://applicantes.com/politica-de-privacidad/

Asesor. (29 de Junio de 2011). *ProDato*. Obtenido de Antecedentes: http://www.protecciondedatospersonales.org/2011/06/29/%C2%BFa-quien-le-pertenecen-los-datos-personales/

Beresovsky, A. (09 de Octubre de 2017). *La Voz*. Obtenido de La intimidad en la era de las redes sociales: http://www.lavoz.com.ar/salud/la-intimidad-en-la-era-de-las-redes-sociales

Bradley, T., & Carvey, H. (2008). Terminos Malware. En T. Bradley, & H. Carvey, *Proteccion del PC y seguridad en Internet* (págs. 70- 71). Madrid: ANAYA MULTIMEDIA.

Burgueño, P. F. (02 de Marzo de 2009). *Pablo F. Burgueño*. Obtenido de Clasificación de Redes Sociales: https://www.pablofb.com/2009/03/clasificacion-de-redes-sociales/

Canal, V. A. (2004). Capitulo tres: Medidas. En V. A. Canal, *Seguridad de la Informacion: Expectativas, riesgo y tecnicas de proteccion.* (págs. 30-32 y 80). España: Limunsa,S.A de C.V.

Canal, V. A. (2006). Riesgos. En V. A. Canal, *Seguridad de la informacion: Expectativas, riesgos y tecnicas.* (págs. 26-28). España: Limusa,S.A. de C.V.

Canal, V. A. (2006). Capitulo Dos: Riesgos. En V. Aceituno, *Sistemas de Informacion: Expectativas, Riesgos y Tecnicas de proteccion* (págs. 34-42). España: Limusa,S.A. de C.V.

Canal, V. A. (2006). Codigo Malicioso. En V. A. Canal, *Seguridad de la informacion: Expectativas, riesgos, y tecnicas de proteccion.* (págs. 34-35). España: Limusa,S.A. de C.V.

Canal, V. A. (2006). Politicas de Seguridad. En V. A. Canal, *Seguridad de la Informacion: Expectativas, riesgos y tecnicas* (pág. 98 y 131). España: Limusa, S.A. de C.V.

Carrasco, D. O. (17 de Noviembre de 2011). *Observatorio Tecnologico*. Obtenido de Privacidad y seguridad en Redes Sociales: http://recursostic.educacion.es/observatorio/web/en/internet/recursos-online/1015-daniel-ortega-carrasco

Checks. (22 de Noviembre de 2011). *blogspot*. Obtenido de Delitos informaticos: http://delitosinformaticoslaschecks.blogspot.mx/

Cuello, J., & Vittone, J. (2013). *appdesignbook*. Obtenido de Las aplicaciones: http://appdesignbook.com/es/contenidos/las-aplicaciones/

Damasio Goulart, G., & Da Silveira Serafim , V. (05 de Mayo de 2017). *Antivigilancia*. Obtenido de ¿Qué saben las aplicaciones móviles sobre nosotros?: https://antivigilancia.org/es/2017/05/que-saben-apps-moviles-sobre-nosotros/

Delgado, L. R. (1998). Derechos de la Personalidad y Datos Personales. *Derecho Político,*, 154-155.

Durán, G. M. (24 de Julio de 2017). *doctrina.* Obtenido de Los delitos informáticos en el Derecho penal de México y España: https://doctrina.vlex.com.mx/vid/delitos-informaticos-derecho-penal-mexico-71182844

Financieros, F. F. (Diciembre de 2014). *Campaña Educativa 2014*. Obtenido de Glosario de términos: http://flamboyanfoundation.org/wp/wp-content/uploads/2014/12/Glosario-de-t%C3%A9rminos-redes-sociales.pdf

Garavilla, M. E. (26 de Mayo de 2008). *unifr.* Obtenido de DELITOS INFORMÁTICOS: https://www.unifr.ch/ddp1/derechopenal/articulos/a_20080526_32.pdf

Gutierrez, A. (29 de Julio de 2017). *Aboutespañol.* Obtenido de ¿Qué es una app y cómo descargarlas?: https://www.aboutespanol.com/que-es-una-app-y-como-descargarlas-3507717

Hall, A. (s.f.). *Tipos de delitos informáticos.* Argentina .

Ibarra Cadena, B. L., López Salas, M., Ramírez Ricardez, G. S., Romero Gaytán, M., Alcalá Méndez, A., Castillo Martínez, M., . . . Viveros Reyes, P. V. (2016). *INFOEM.* Obtenido de El abc de los datos personales: http://www.infoem.org.mx/doc/publicaciones/ABC_Datos.pdf

Islas, O. (24 de Marzo de 2017). *El Universal*. Obtenido de ¿Crece el uso de Internet en México?: http://www.eluniversal.com.mx/entrada-de-opinion/columna/octavio-islas/techbit/2017/03/24/crece-el-uso-de-internet-en-mexico

Jáuregu, M. C. (Diciembre de 2009). *Instituto de Acceso a la Información Pública del Distrito Federal.* Obtenido de Manual de autoinformacion sobre la Ley Federeal de Datos Personales para el Distrito: http://www.cevat.org.mx/retaip/documentos/material_apoyo/manuales/manualdatospersonales.pdf

Larrain, J., & Hurtado, A. (2003). El Concepto de identidad . *FAMECOS*, 31.

Liceda, E. (2011). *sedici*. Obtenido de La identidad digital: http://sedici.unlp.edu.ar/bitstream/handle/10915/20717/Art%2023.pdf?sequence=1

Mocholí, A. (9 de Mayo de 2014). *Yeeply*. Obtenido de Decálogo de buenas prácticas: Aspectos legales de las aplicaciones móviles: https://www.yeeply.com/blog/decalogo-de-buenas-practicas-aspectos-legales-de-las-aplicaciones-moviles/

Mocholi, A. (18 de Agosto de 2015). *yeepply*. Obtenido de Seguridad móvil al programar apps: Permisos de acceso: https://www.yeeply.com/blog/seguridad-movil-al-programar-apps-permisos-de-acceso/

Montiel, J. E. (2013). *Fondo de Información y Documentación.* Obtenido de Implementación de La Ley Federal de Protección de Datos Personales en Posesión de Particulares: https://infotec.repositorioinstitucional.mx/jspui/bitstream/1027/225/1/Proyecto%20Integrador%20Jes%C3%BAs%20Ernesto%20Brise%C3%B1o%20Montiel%20VF%204nov13.pdf

Noriega, S. (01 de Enero de 2016). *Cetsuperior*. Obtenido de Protección de Redes: Delitos Informáticos en México: https://www.certsuperior.com/Blog/proteccion-de-redes-delitos-informaticos-en-mexico

Ortega, L. (20 de Enero de 2018). *Androidpit*. Obtenido de Permisos de aplicaciones: ¿qué significan exactamente?: https://www.androidpit.es/permisos-aplicaciones

Padilla, M. (29 de Marzo de 2016). *BlogNyce*. Obtenido de El mercado de app's en México y el tratamiento de datos personales: https://www.nyce.org.mx/blog/el-mercado-de-apps-en-mexico-y-el-tratamiento-de-datos-personales/

Peña, R. M. (2014). La Gestion de la identidad digital. En R. M. Peña, *Identidad Digital: El nuevo usuario en el mundo digital* (págs. 42-43). España: Ariel, S.A., 2014.

Peña, R. M. (2016). Identidades digitales frente a indentidades fisicas. En R. M. Peña, *Ciberseguridad, la protección de la informacion en el mundo digital.* (págs. 15-16). España: Ariel, S.A.,2016.

Pérez San-José , P., Gutiérrez Borge, C., De la Fuente Rodríguez, S., Álvarez Alonso, E., & García Pérez, L. (Julio de 2012). *av-asesores.* Obtenido de Guía para usuarios: identidad digital y reputacion online: http://www.av-asesores.com/upload/590.PDF

Quintal, M. A. (2017). Archivos Juricos. En M. A. Quintal, *La Proteccion de intimidad como Derecho Fundamental de los Mexicanos* (pág. 73 y 96). Mexico. Obtenido de La Proteccion de la intimidad como Derecho Fundamental de los Mexicanos: https://archivos.juridicas.unam.mx/www/bjv/libros/5/2253/9.pdf

Realpe, G. (2017). *Cloud Seguro*. Obtenido de LA PRIVACIDAD EN LAS APLICACIONES MÓVILES: https://www.cloudseguro.co/la-privacidad-en-las-aplicaciones-moviles/

Rinaldi, P. (31 de Juilo de 2017). *LE VPN*. Obtenido de LA SEGURIDAD DE APLICACIONES MÓVILES: APLICACIONES MÓVILES QUE ESTÁN PONIENDO TU PRIVACIDAD Y SEGURIDAD EN RIESGO: http://www.le-vpn.com/es/seguridad-de-aplicaciones-moviles/

Rodríguez, J. A. (2003). Ética, Derecho y datos personales. *Cuadernos de Derecho Público*, 122.

Rojas, J. R. (2017). *Seguridad: cultura de prevencion para ti.* Obtenido de Delitos Informáticos En México: https://revista.seguridad.unam.mx/numero26/delitos-inform-ticos-en-m-xico.html

Saavedra, C. M. (2015). *blogspot.* Obtenido de Categoria de Apps : http://aplimovs.blogspot.mx/2015/11/categorias-de-apps.html

Salazar, G. (Septiembre y Noviembre de 2016 - 2017). *sontusdatos.org.* Obtenido de Ante Vulneraciones de Datos Personales ¿Qué Hacen Las Empresas En México?: https://sontusdatos.org/2017/01/18/ante_vulneraciones_de_datos_personales_que_hacen_las_empresas_en_mexico/

Sánchez, E. (27 de Septiembre de 2011). *La ventana de Elia*. Obtenido de Redes sociales verticales y horizontales: https://laventanadeelia.wordpress.com/2011/09/27/redes-sociales-verticales-y-horizontales/

Santo, C. (15 de Abril de 2013). *PuroMarketing*. Obtenido de 12 Tipos de Usuarios de Redes Sociales en Funcion de sus Comportamiento: https://www.puromarketing.com/16/15829/tipos-usuarios-redes-sociales-funcion-comportamiento.html

Terreros, F. V. (2014). Delitos Informáticos. *ius et veritas*, 293-294.

Terreros, F. V. (2014). Delitos Informáticos. *ius et veritas*, 286 - 287.

Villena, J. C. (Diciembre de 2017). *Educa Sistemas.* Obtenido de http://www.educasistemas.com/2017/12/estos-son-los-98-datos-que-facebook.html

Zuriguel, C. (29 de Julio de 2014). *Inboundcycle*. Obtenido de Lo que deberías saber sobre los términos de uso de las redes sociales: https://www.inboundcycle.com/blog-de-inbound-marketing/los-t%C3%A9rminos-de-uso-lo-que-todos-deber%C3%ADamos-leer-pero-casi-nadie-hace-al-inscribirse-en-una-red-social