UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

La Universidad Católica de Loja

MODALIDAD PRESENCIAL

ESCUELA DE CIENCIAS DE LA COMPUTACIÓN

Seguridad de Redes Sociales

Trabajo de fin de carrera previa a la obtención del título de Ingeniero en Sistemas Informáticos y Computación.

AUTOR

Jorge Omar Sisalima Granda

DIRECTORA

Ing. María Paula Espinoza

CODIRECTORA

Ing. Julia Pineda

Loja – Ecuador

2010

CERTIFICACIÓN

Ingeniera.
María Paula Espinoza Vélez
DIRECTORA DE TESIS

CERTIFICA:

Que el Sr. Jorge Omar Sisalima Granda, autor de la tesis SEGURIDAD DE REDES SOCIALES, ha cumplido con los requisitos estipulados en el Reglamento General de las Universidad Técnica Particular de Loja, la misma que ha sido coordinada y revisada durante todo el proceso de desarrollo, por lo cual autorizo su presentación.

Loja, 17 de Noviembre de 2010

Ing. María Paula Espinoza Vélez
DIRECTORA DE TESIS

CERTIFICACIÓN

Ingeniera.
Julia Alexandra Pineda
CODIRECTORA DE TESIS

CERTIFICA:

Que el Sr. Jorge Omar Sisalima Granda, autor de la tesis *SEGURIDAD DE REDES SOCIALES*, ha cumplido con los requisitos estipulados en el Reglamento General de las Universidad Técnica Particular de Loja, la misma que ha sido coordinada y revisada durante todo el proceso de desarrollo, por lo cual autorizo su presentación.

Loja, 17 de Noviembre de 2010

Ing. Julia Alexandra Pineda
CODIRECTORA DE TESIS

CESIÓN DE DERECHOS

Yo, **Jorge Omar Sisalima Granda,** declaro conocer y aceptar la disposición del Art 67. De Estatuto orgánico de la Universidad Técnica Particular de Loja que en su parte pertinente textualmente dice: “Forman parte del patrimonio de la Universidad la propiedad intelectual de las investigaciones, trabajos científicos o técnicos y tesis de grado que se realicen a través, o con el apoyo financiero, académico o institucional (operativo) de la universidad.

_____

Jorge Omar Sisalima Granda

AUTORIA

Las ideas opiniones conclusiones recomendaciones y mas contenidos expuestos en el presente proyecto de tesis son de absoluta responsabilidad del autor.

_____

Jorge Omar Sisalima Granda

DEDICATORIA

Con mucho cariño dedico la presente tesis:

A Dios, el ser supremo que me ha permitido llevar a cabo una más de mis metas.

A mis Padres Jorge Sisalima y Norma Granda, quienes han forjado en mi una persona de bien, siempre han estado brindándome su apoyo pese a las situaciones adversas de la vida, todo lo que soy se lo debo a ellos.

A mis hermanos Mauricio, Danny y Johan Sisalima Granda, que siempre han estado apoyándome.

A mis amigos, amigas y demás personas quienes han compartido su tiempo y sueños conmigo siendo de cierta manera los hermanos y hermanas ocasionales que Dios me ha brindado para alegrar mis días y compartir mis penas.

A todos los maestros que han creído en mí durante el transcurso de toda mi formación educativa, desde los años de primaria hasta los últimos años de mi educación en esta excelente institución la Universidad Técnica Particular de Loja.

AGRADECIMIENTO

Agradezco a todas las personas que de una u otra manera han contribuido a mi formación personal y profesional; en especial a la directora de tesis María Paula Espinoza ya que gracias a su motivación y paciencia he podido culminar con éxito el presente trabajo de investigación.

Jorge Omar

TABLA DE CONTENIDOS

INDICE DE FIGURAS

INDICE DE TABLAS

INTRODUCCIÓN

A través de la historia de la humanidad muchos han sido los inventos que han provocado grandes cambios en la vida de las personas. El internet es uno de ellos y sobre esta plataforma global se han desarrollado grandes avances tecnológicos, pero uno de los más relevantes son las herramientas Web 2.0 que revolucionaron el internet y de manera específica las Redes Sociales que están cambiando la manera como el mundo se comunica.

Las Redes Sociales se han convertido en un poderoso canal de comunicación, interacción social, permitiendo el intercambio de información en tiempo real, propagación de ideas, pensamiento, negocios, etc. Pero, su acelerado crecimiento genera un gran riesgo debido al acceso a la información de carácter personal y al mal uso del cual están siendo objeto. Por esta razón, la *Seguridad de Redes Sociales* ha venido tomando importancia, precisamente porque estas plataformas superaron la función para la que fueron creadas, ya que se cometen delitos y a través de esto se vulneran constantemente algunos de los derechos humanos que todas las personas poseemos. De ahí la importancia del presente estudio ya que ha permitido determinar la incidencia y privacidad de las Redes Sociales en nuestro entorno, y con esto tener una perspectiva de lo que está sucediendo a nivel nacional.

RESUMEN

El uso de las Redes Sociales ha tomado fuerza en diversos entornos principalmente educativos, en nuestra Universidad por ejemplo se hace amplio uso de estas plataformas como herramientas de gestión del conocimiento, pero hasta el momento no se cuenta con estadísticas que permitan determinar cómo se están desarrollando las Redes Sociales a nivel local y nacional.

En el presente estudio, se desarrolla un análisis profundo de las Redes Sociales partiendo desde aspectos fundamentales y centrándose en una tipología para determinar primero la incidencia y luego la privacidad y seguridad de Redes Sociales en entornos educativos secundarios, universitarios y entidades de Gobierno de la Ciudad de Loja. Para concluir con un conjunto de *Políticas de Buen Uso* para gestionar la privacidad de la información y seguridad de Redes Sociales, y desarrollando una propuesta de ley, para la incorporación al sistema legal penal de una normativa que sancione los delitos realizados en la Redes Sociales.

1. FUNDAMENTOS DE REDES SOCIALES

1.1 ¿Qué son las Redes Sociales?

Las redes sociales no son un invento actual, por lo contrario, siempre han existido y de una u otra manera, hemos formado parte una Red de amigos, compañeros de clase, vecinos, etc.. En la actualidad, algunos investigadores hablan de Redes Sociales en Línea o Servicio de Redes Sociales, para referirse a la herramienta Web 2.0 que conocemos como red social. Si bien es cierto, la reciente llegada de la Web 2.0 ha revolucionado la manera en que el mundo se comunica, a través de blogs, redes sociales, microblogging; el estudio específico de las redes sociales se remonta a la Segunda Guerra Mundial, donde, el antropólogo John Barnes motivado por la necesidad de analizar el comportamiento de la sociedad tras la guerra, usó por primera vez el término "Social Network", y la definió de la siguiente manera: "La imagen que tengo es de un conjunto de puntos algunos de los cuales están unidos por líneas. Los puntos de la imagen son personas o a veces grupos, y las líneas indican que individuos interactúan mutuamente". Esta definición sugiere que todo grupo de personas es una red social. La Figura 1 muestra la representación gráfica de una red social.

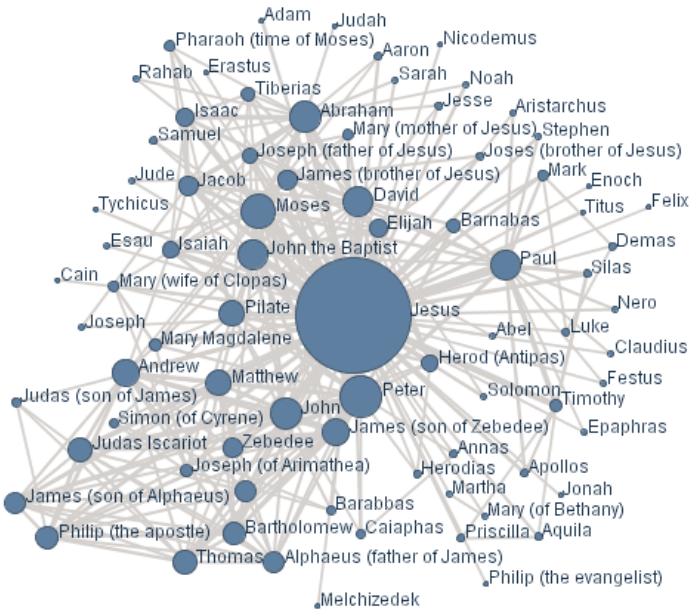

Figura 1. Representación de una red social (1)

Por su parte, el abogado Pablo Fernández Burgueño en el artículo “Las Redes Sociales en la Administración Pública Local” define a las redes sociales como: “Módulos dinámicos de comunicación entre personas, que replican las relaciones existentes en el mundo analógico, maximizando su alcance y efectos” (2). En definitiva, una red social es el equivalente a una gran plaza en la que los ciudadanos se reúnen por grupos de afinidad para hablar, intercambiar opiniones y proponer actividades. Cabe destacar que las redes sociales permiten desarrollar conversaciones que permanecen siempre vivas, son universalmente accesibles y no responde a horarios, clima ni aforos. Un enfoque diferente es el desarrollado por, Jaime Ricardo Valenzuela Gonzales y Gabriel Valerio Ureña en el artículo denominado ‘Redes Sociales en línea ¿Primeros pasos para el e-learning 2.0?’, donde se considera a las redes sociales como “Elemento central del conectivismo” (3). Además, considera que el conectivismo es el proceso de crear conexiones entre los nodos que componen una red, y que las conexiones es donde radica la posibilidad de aprendizaje. Finalmente, Wikipedia define a una red social como “Una estructura social que se puede representar en forma de uno o varios grafos en los cuales los nodos representan individuos y las aristas son relaciones entre ellos” (4).

Las definiciones expuestas coinciden en que los dos aspectos fundamentales en una red social son: Los actores y las relaciones que existen entre ellos. Ahora, desde el punto de vista informático, las redes sociales son aplicaciones web que permiten a los usuarios la socialización virtual, es decir, establecer relaciones, que pueden estar motivadas por aficiones en común, o un vínculo ya existente en la vida offline, mundo laboral o mismas necesidades y problemáticas.

1.2 Breve Historia de las Redes Sociales

El origen de las redes sociales se remonta al año 1995 con la aparición de classmates.com, mas tarde en 1997 aparece la primera red social denominada SixDegress.com que presentaba la estructura básica de las Redes Sociales actuales, es decir, permitía crear un perfil y navegar por el perfil de sus amigos. En 2001 con la aparición de Ryze.com permite la utilización de las redes sociales con fines

profesionales. Al año siguiente fue lanzado Friendster, y posteriormente en 2003 surge una gran cantidad de redes sociales como: MySpace, LastFm, Flickr, Youtube, Hi5, etc.

1.3 Clasificación de Redes Sociales

Desde el surgimiento de las redes sociales, varias han sido las clasificaciones desarrolladas con el objetivo de estructurar categorías que abarquen todas de las redes sociales. Vemos clasificaciones como FaberNobel Consulting en un estudio denominado 'Social Network Werbsites: best practices from leading services' (5) publicado en 2007, agrupa a las redes sociales por su objetivo. Establece cuatro grupos:

TIPO	OBJETIVO
Online communities	Socialización
Bussines networks	Contactos profesionales y empresariales
Online matchmaking	Búsqueda de pareja
Alumni networks	Socialización entre compañeros de clase

Tabla 1 Clasificación según FaberNovel Consulting

Otro estudio denominado 'Young People and Social Networking Services' (6), sugiere una clasificación diferente, establece siete grupos:

- Redes Sociales basadas en perfiles
- Redes Sociales basadas en contenidos
- Redes Sociales para la creación de nuevas Redes Sociales
- Entornos Virtuales de Multiusuario
- Redes Sociales Móviles

- Microblogging
- Buscadores Sociales

Por su parte, Fernández Burgueño clasifica a las redes sociales de la siguiente manera (7):

- Por su público objetivo y temática
- Por el sujeto principal de relación
- Por su localización geográfica
- Por su plataforma

Estas clasificaciones son muy variadas y cada una de ellas tiene un enfoque diferente, pero la clasificación más completa que abarca la totalidad de las redes sociales es la desarrollada en Young People and Social Network Services, a continuación se detallan las categorías:

- *Redes Sociales Basadas en Perfil.-* Están organizadas en torno a la información proporcionada por los miembros, incluyendo fotos y videos. Entre las redes sociales más conocidas en nuestro medio están: Hi5, Facebook, Badoo, Sonico, MySpace, etc.

- *Redes Sociales Basadas en Contenidos.-* En estas redes sociales, el perfil de usuario sigue siendo la parte esencial para la creación de nexos en la red, pero estas redes se especializan en un contenido específico. Por ejemplo Flickr, permite almacenar, ordenar, buscar y compartir fotografías y videos online (8); Youtube, es un sitio web en el cual los usuarios pueden subir y compartir vídeos (9); Shelfari, es una red social sobre discusión de libros, los usuarios de Shelfari crean bibliotecas virtuales de los títulos que poseen o han leído, y pueden puntuar, revisar, etiquetar, y hablar de sus libros (10); Last.fm, es una red social, una radio vía Internet y además un sistema de recomendación de música que construye perfiles y estadísticas sobre gustos musicales, basándose en los datos enviados por los usuarios registrados (11).

- *Redes Sociales para la creación de Nuevas Redes Sociales (White-label).-* Se caracterizan por brindar la funcionalidad de creación de nuevas redes sociales, es decir que los usuarios pueden crear pequeñas comunidades, ejemplo, Ning permite descubrir y crear nuevas redes sociales para sus intereses y aficiones (12).

- *Redes Sociales con Entorno Virtual de Multiusuario.-* Permiten al usuario interactuar con sus amigos a través de un avatar, esto es, mediante la instalación de un software que permite la interacción en 3D. Ejemplo SecondLife.

- *Redes Sociales Móviles.-* Son aquellas que permiten a los usuarios interactuar con sus amigos desde el teléfono celular. Ejemplo, Waze permite identificar cómo llegar a destino en base a las condiciones del tráfico en el momento en que conduce.

- *Microblogging.-* Sitios como Plurk, Twitter o Jaiku permiten al usuario mantener contacto con sus amigos a través de pequeños posts.

- *Buscadores Sociales.-* Estas orientan sus servicio a la búsqueda de personas que se encuentran en alguna red social de las mencionadas anteriormente. Entre los buscadores más populares están Spokeo y Wink.

1.4 ¿Cuáles son las Redes Sociales más Usadas?

Según *top ten reviews* las redes sociales mejor ranqueadas de 2009 son:

#1	#2	#3	#4	#5	#6	#7	#8	#9	#10
Facebook	MySpace	Bebo	Friendster	hi5	Orkut	PerfSpot	Yahoo! 360	Zorpia	Netlog

Figura 2. Top 2009 de Redes Sociales (13)

En la Figura 2 se muestra el top ten de redes sociales, donde, Facebook es el líder indiscutible a nivel mundial, actualmente cuenta con 500 millones de usuarios, solo en Latinoamérica son alrededor de 60 millones y aumentado, ya que cada día se suman nuevos usuarios que prefieren a Facebook sobre otras redes sociales.

1.5 ¿Qué tipo de Redes Sociales analizaremos?

Para el presente estudio, consideraremos las Redes Sociales Basadas en Perfil, ya que, están consolidadas como un referente de las redes sociales a nivel local y mundial, en comparación con las otras categorías. Este tipo de redes sociales están estructuradas por perfiles en torno a la información que proporciona el usuario, estos perfiles son una tarjeta de presentación virtual, donde, se muestra información del usuario como: nombre o nickname, edad, ubicación, lugar de nacimiento, intereses, nivel de educación, lista de amigos y secciones como “acerca de mi” y “lo que busco”. Además, permiten al usuario subir sus fotos, crear álbumes de fotos y compartir contenidos, como videos, enlaces, archivos, etc.. En algunas de las redes pertenecientes a este grupo, se muestra información laboral del usuario, es decir cargo, tiempo que lleva trabajando, nombre de la empresa, etc.. No es obligatorio que el usuario publique toda esta información, pero, redes como Badoo calculan el porcentaje de información ingresada en el perfil, los usuarios con bajo porcentaje no podrán usar todas las aplicaciones que esta red social ofrece, esto, con el objetivo de incentivar a los usuarios a completar los campos faltantes de su perfil.

Para hacer más interesante la utilización de las redes sociales, cada día agregan nuevos componentes; ejemplo, Facebook permite adicionar módulos llamados Aplicaciones. Hi5, en cambio permiten modificar la apariencia del perfil mediante skins.

La visibilidad de estos perfiles varía dependiendo de la red social, por ejemplo, los perfiles de Friendster y Tribe son rastreados por los motores de búsqueda, haciéndolos visibles para cualquier persona, independiente de si es o no usuario de la red. Otras redes sociales como Linkedin controlan lo que el visitante puede observar dependiendo de si el usuario tiene una cuenta de pago o no. Por su parte MySpace permiten elegir al usuario un perfil público o privado. Hi5 permite decidir si el usuario quiere un perfil

que sea visualizado por cualquier persona o solamente visualizado por los amigos de su red. Facebook adopta un enfoque diferente, por defecto, los usuarios que forman parte de la misma "red" puede ver los perfiles de los demás, a menos que un perfil de propietario haya decidido negar el permiso a los usuarios de su red.

1.6 Las Redes Sociales en Latinoamérica

En Latinoamérica al igual que en las demás regiones del mundo, las redes sociales han sido un fenómeno, como se aprecia en la Figura 3, las redes sociales que predominan en Latinoamérica son: Facebook, Hi5 y Orkut. Hi5 fue lanzada en 2003 y fundada por Ramun Yalamnchis, su número de usuarios ha crecido rápidamente y al finalizar el 2007 tenía más de 70 millones de usuarios registrados, la mayoría de ellos en América Latina (14). Facebook creado por Mark Zuckerberg, originalmente era un sitio para estudiantes de la Universidad de Harvard, en Enero de 2010, Facebook contaba con 350 millones de usuario (15), actualmente son más de 500 millones. Orkut fue lanzada en 2004 por Google, diseñado por el actual empleado turco de Google Orkut Büyükkökten (16).

Figura 3. Redes Sociales en Latinoamérica (Creación propia)

La Figura 3 está basada en el Top Sites, by country de Alexa (17), donde se destacan Facebook, Hi5 y Orkut. Facebook domina la región, siendo la Red Social mejor ranqueada en un total de 16 países, Hi5 es la Red Social mejor ranqueada solamente en Perú, pero es la segunda en países como: México, Colombia, Ecuador, El Salvador, Nicaragua, Costa Rica, Honduras, Guatemala, República Dominicana. Orkut es primera en Brasil y Paraguay.

Otras Redes que se destacan son: Fotolog la cual es la segunda con mejor ranking en Argentina, Chile y Uruguay. MySpace es la segunda en Puerto Rico y Sonico es la segunda en Bolivia. El número de usuarios de Facebook en la región asciende a 40 millones de usuarios hasta Enero de 2010,

Algunos de los datos que se han encontrado sobre la incidencia de las Redes Sociales en Latinoamérica se muestran a continuación y han sido tomados de Tendencias Digitales (18).

- Sobre un total de 154 millones de personas conectadas (el 27% de penetración poblacional), el 72% de los usuarios latinoamericanos aseguró pertenecer a alguna red social. Entre los países que más penetración en redes sociales se encuentra Chile y Colombia (77%). Uruguay y la Argentina se ubican en la cola, con el 50 por ciento.

- En cuanto al tamaño de las redes, la mayoría de los internautas (52%) poseen en su red una comunidad de 1 a 50 miembros. Brasil es el país con el promedio más alto (151 amigos). Sólo el 9% tiene más de 300 amigos.

- Los usuarios que pertenecen a una red social se conectan a la misma un promedio de 4,4 veces por semana. El 27,5 % lo hace 3 veces por día.

- La mayoría de los usuarios suelen usar varias redes sociales simultáneamente. Las tres principales son Hi5 (34%), Facebook (27%) y MySpace (17%).

- ¿Qué hace un usuario en una red social? La mayoría (71%) usa la red social para escribir mensajes a sus amigos y también ver fotos ajenas (47%), publicar fotos propias y ver videos. Solo el 6% usa las redes para publicar videos.

Según el artículo 'Radiografía de las Redes Sociales en Latam', en marzo de 2008, los usuarios únicos de las redes sociales de Argentina, Brasil, Chile, Colombia y México suman 37 millones. Respecto de la cantidad de visitas que recibieron estas redes sociales debemos destacar a Orkut que logró más de 400 millones de visitas en marzo (dos veces más que el segundo), siendo que MySpace tuvo 180 millones de visitas. Bastante detrás en términos de visitas se ubicaron Facebook con 72 millones y hi5 con unos 52 millones.

- La comunidad Facebook de Argentina pasa los 6 millones (19).

- Colombia supera los 5 millones de usuarios (20).

- Brasil sigue imparable con 700.000 nuevos usuarios cada día, Brasil históricamente dominado por otras redes sociales ya tiene un millón de usuarios de Facebook (21).

- Según el artículo (22) en México los usuarios de Redes Sociales para septiembre de 2008 alcanzo un 73% que tuvo un incremento considerable en relación al año anterior que la cifra llego a 67.3%. Además señala, que en 2008 el total de la población en línea de Latinoamérica alcanzó el 87.2%, incrementado 9.2% en relación a 2007.

1.7 En el Ecuador

Al ingresar al Alexa.com y revisar el ranking de sitios web del Ecuador, se observa que sitios como Hi5 o Facebook, ocupan los primeros lugares del top ten, dejando por debajo a periódicos locales como El Universo en el puesto 12 y a la banca local como el Banco del Pichincha en el puesto 18.

1. Google Ecuador
2. Windows Live
3. Facebook
4. Hi5
5. Youtube

Hi5 tiende a la baja desde Octubre de 2008, cuando alcanzó su nivel más alto de actividad en el país, llegando aproximadamente a 150,000 visitas diarias. Facebook con más de 500 millones de usuarios a nivel mundial, en Ecuador cuenta con un crecimiento imponente, alcanzando tasas superiores al 15 % mensual, según el último reporte y estudio de Formación Gerencial, si la tendencia se mantiene, para el próximo año, Ecuador contará con más de dos millones y medio de usuarios, siendo esto cerca del 20 % de la población de Ecuador que contará con una cuenta en la red social (23). En la actualidad existen 1'559,900 usuarios de Facebook en el Ecuador hasta el 13 de Septiembre de 2010, divididos en las siguientes proporciones y cantidades:

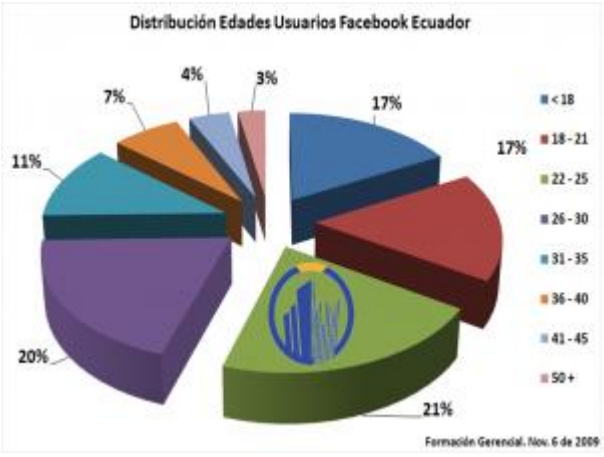

Figura 4. Distribución por edad de usuario de Facebook en Ecuador (23)

Otro estudio desarrollado por Incomecuador, señala que de todos los usuarios de Facebook el 96 % se concentran en Quito y Guayaquil. Cuenca apenas llega a un 2.68

% mientras que Manta y Loja alcanzan un 0.24 % y 0.17 % respectivamente, el 2 % restante corresponde al resto del país (24).

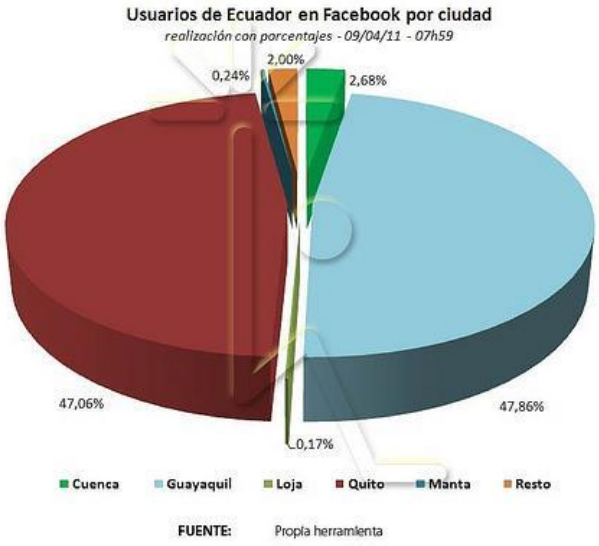

Figura 5. Distribución por ciudad de usuarios de Facebook en Ecuador (24)

2. ANALISIS DE INCIDENCIA DE REDES SOCIALES EN LOJA

2.1 Problemática

De la investigación realizada, no se han identificado estudios que muestren la incidencia y el nivel de penetración de las redes sociales en la Ciudad de Loja, por ello, el presente estudio va encaminado a determinar estos indicadores que hasta la actualidad son desconocidos. En este sentido, se propone la realización de encuestas con el objetivo de determinar el nivel de incidencia y de forma específica, determinar cuáles son las redes sociales que los lojanos están usando, con qué finalidad están siendo utilizadas y de manera especial aspectos relacionados con la privacidad de los datos en las mismas. La investigación detallara el conocimiento, la percepción, hábitos y preferencias que tienen los usuarios de las redes sociales en la Ciudad de Loja.

2.2 Universo

El público a encuestar son las personas de ambos sexos mayores de 15 años de:

Instituciones educativas: Porque son el escenario apropiado para determinar la indecencia de las redes sociales en los más jóvenes. Se ha seleccionado los siguientes establecimientos:

- Universidad Técnica Particular de Loja
- Universidad Internacional de Ecuador - Sede Loja
- Instituto Técnico Superior “Daniel Álvarez Burneo”
- Colegio “Juan Montalvo”

Instituciones de Gobierno: Porque dará una pauta de la influencia de las redes sociales en el ámbito laboral. Se ha seleccionado las siguientes instituciones.

- Consejo Provincial de Loja

- Municipio del Cantón Loja

El universo total es de 7949 personas.

2.3 Muestra

Para determinar la muestra se aplico la formula $n = P/(1+(e^2 xP))$, siendo la más adecuada para los casos de poblaciones grandes. En la encuesta aplicada se estableció un porcentaje de 4% (0.04) de error de muestreo debido a que por ser la población grande se necesita un nivel de significancia menos, obteniendo una muestra que nos de seguridad en los resultados.

$n = P/(1+(e^2 * P))$ *Donde:*

n = tamaño de la muestra ?
P = población 7949
e = nivel de error 0.04%

$N = 7949/(1+(0{,}04^2 * 7949))$

$N = 7949/(1+(12.7184))$

$N = 7949/(13.7184)$

$N = 579$

INSTITUCIÓN	TOTAL	Nro. ENCUESTAS
Universidad Técnica Particular de Loja	4383	319
Universidad Internacional	900	66
Consejo Provincial de Loja	516	38
Municipio de Cantón Loja	1100	80
Instituto Técnico Superior "Daniel Álvarez Burneo"	850	62
Colegio "Juan Montalvo"	200	15
	7949	**579**

Tabla 2. Distribución de encuestados por institución

2.4 Aplicación de Encuesta

La encuesta tiene el objetivo de determinar las redes sociales con mayor penetración en la ciudad de Loja, los hábitos y preferencias de los usuarios en las mismas. La encuesta esta en el ANEXO A.

2.5 Tabulación de Resultados

- Distribución de encuestados por sexo

El número total de personas encuestadas es de 579 de ellos el 48.88% son de sexo masculino y el 51.12% de sexo femenino.

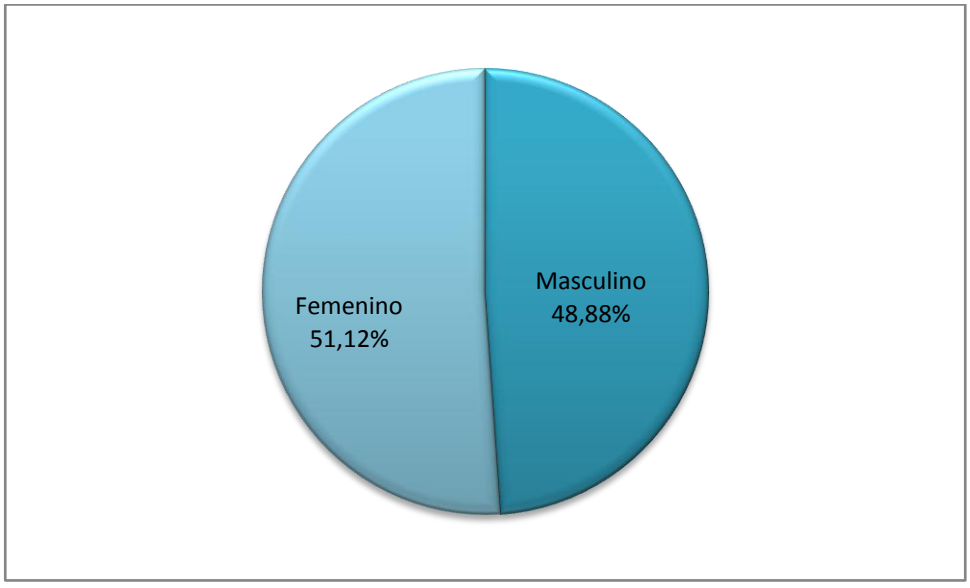

Figura 6. Distribución de encuestados por sexo

- Conocimiento y utilización de Redes Sociales por Institución

En la **Universidad Técnica Particular de Loja**, de un total de 316 personas encuestadas, el 89.25% asegura saber lo que es una red social, mientras que el 10.75% asegura no saber lo que es una red social. Pero solo el 85.44% asegura

utilizar alguna de las redes sociales mientras que el 14.56% asegura no usar ninguna red social.

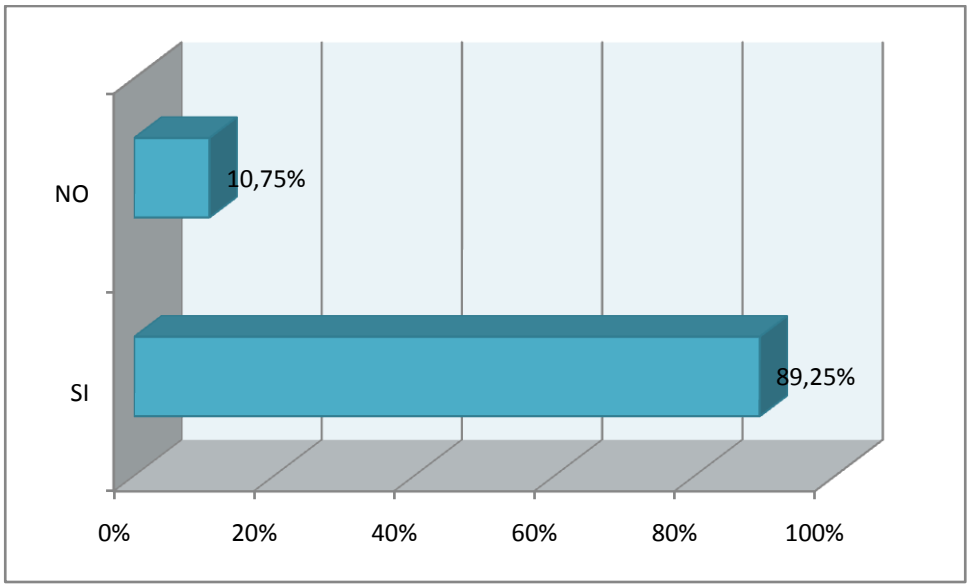

Figura 7. ¿Sabe lo que es una Red Social? UTPL

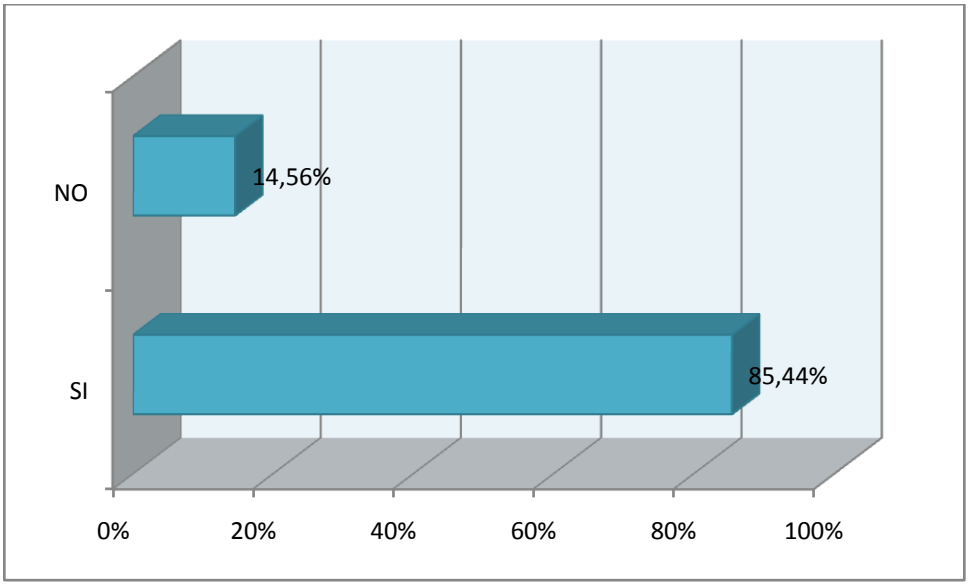

Figura 8. ¿Utiliza Redes Sociales? UTPL

En la **Universidad Internacional del Ecuador Sede Loja**, de un total de 66 personas encuestadas, el 87.87% asegura saber lo que es una red social, mientras que el 12.13% asegura no saber lo que es una red social. Pero solo el 69.47%

asegura utilizar alguna de las redes sociales mientras que el 30.30% asegura no usar ninguna red social.

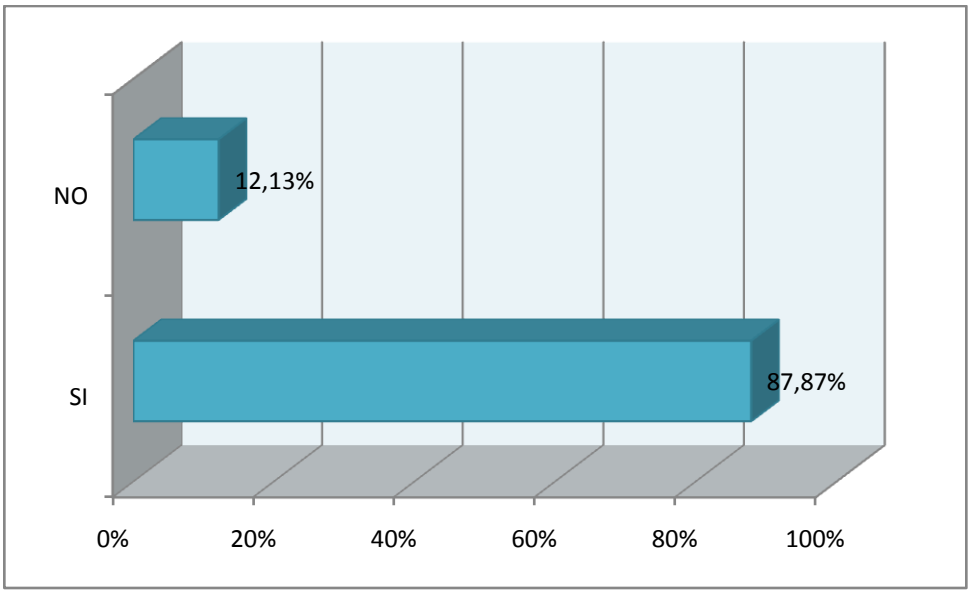

Figura 9. ¿Sabe lo que es una Red Social? UIDE-Loja

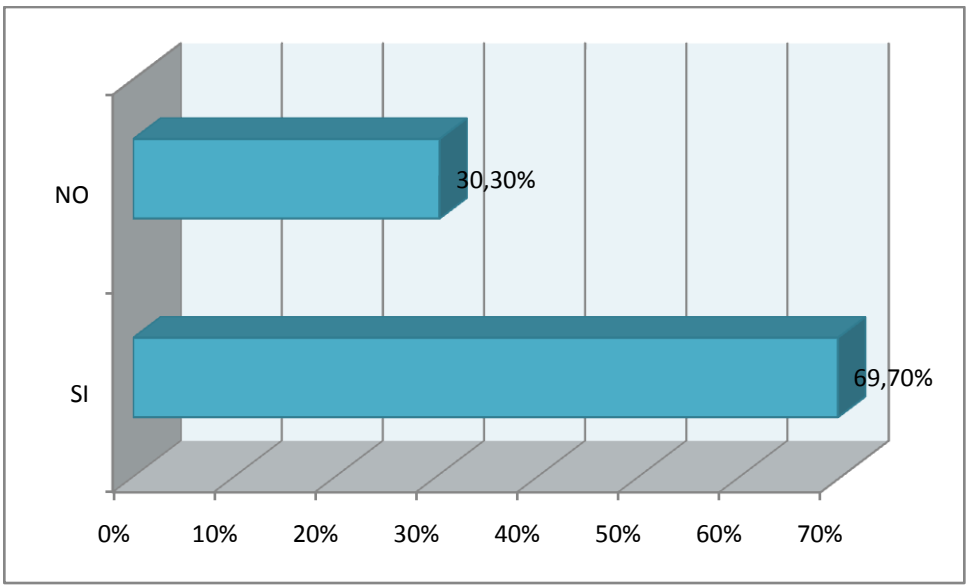

Figura 10. ¿Utiliza Redes Sociales? UIDE-Loja

En el **Consejo Provincial de Loja**, de un total de 38 personas encuestadas, el 57.89% asegura saber lo que es una red social, mientras que el 42.11% asegura no

saber lo que es una red social. Pero solo el 28.95% asegura utilizar alguna de las redes sociales mientras que el 71.05% asegura no usar ninguna red social.

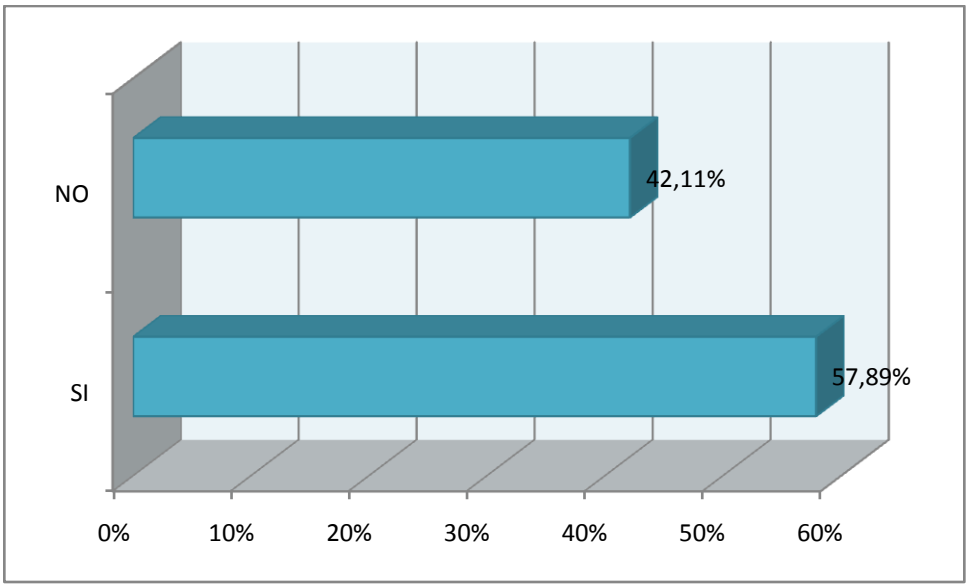

Figura 11. ¿Sabe lo que es una Red Sociales? Consejo Provincial de Loja

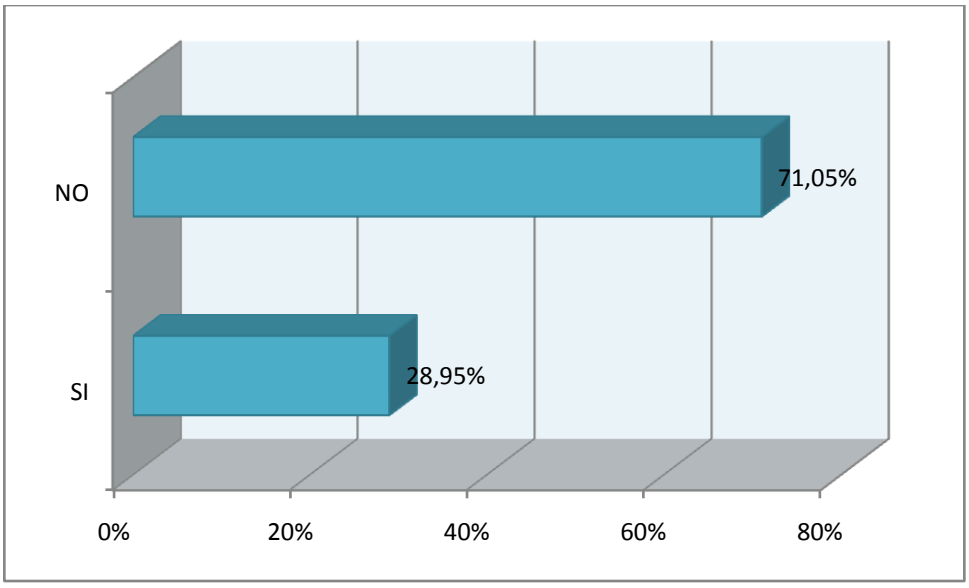

Figura 12. ¿Utiliza Redes Sociales? Consejo Provincial de Loja

En el **Municipio del Cantón Loja**, de un total de 80 personas encuestadas, el 36.25% asegura saber lo que es una red social, mientras que el 63.75% asegura no

saber lo que es una red social. Pero solo el 21.25% asegura utilizar alguna de las redes sociales mientras que el 78.75% asegura no usar ninguna red social.

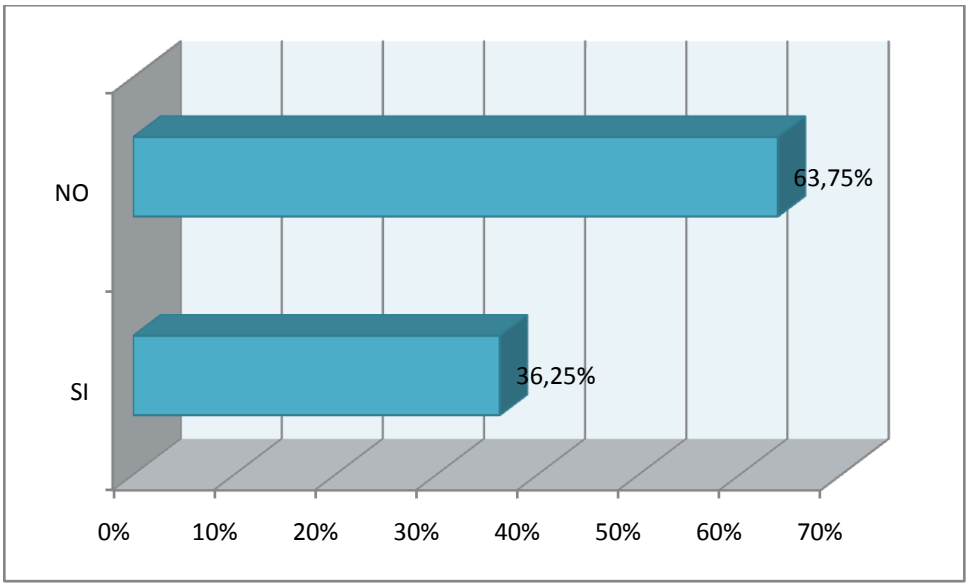

Figura 13. ¿Sabe lo que es una Red Social? Municipio de Loja

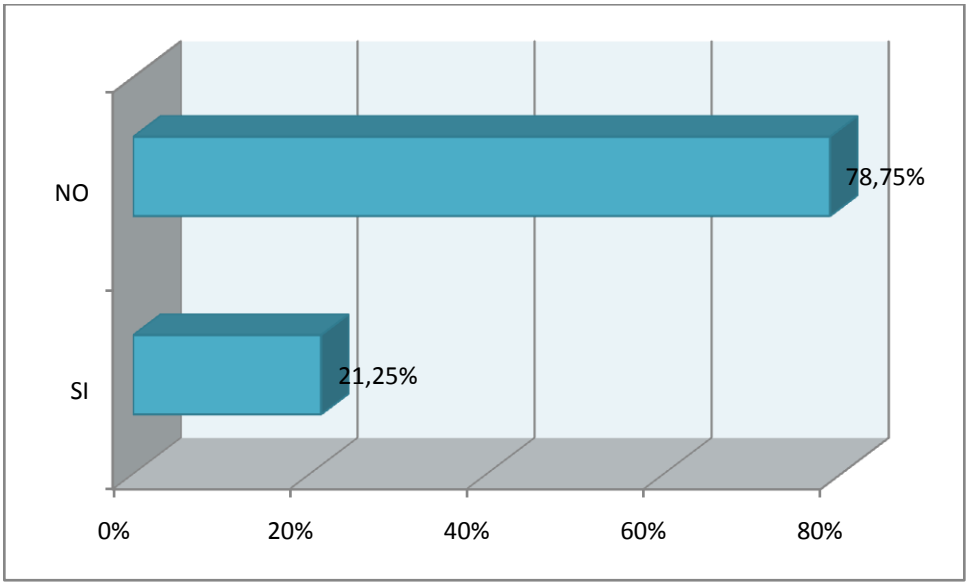

Figura 14. ¿Utiliza Redes Sociales? Municipio de Loja

En el **Colegio "Juan Montalvo"**, de un total de 15 personas encuestadas, el 73.3% asegura saber lo que es una red social, mientras que el 26.7% asegura no saber lo

que es una red social. Pero solo el 86.7% asegura utilizar alguna de las redes sociales mientras que el 13.3% asegura no usar ninguna red social.

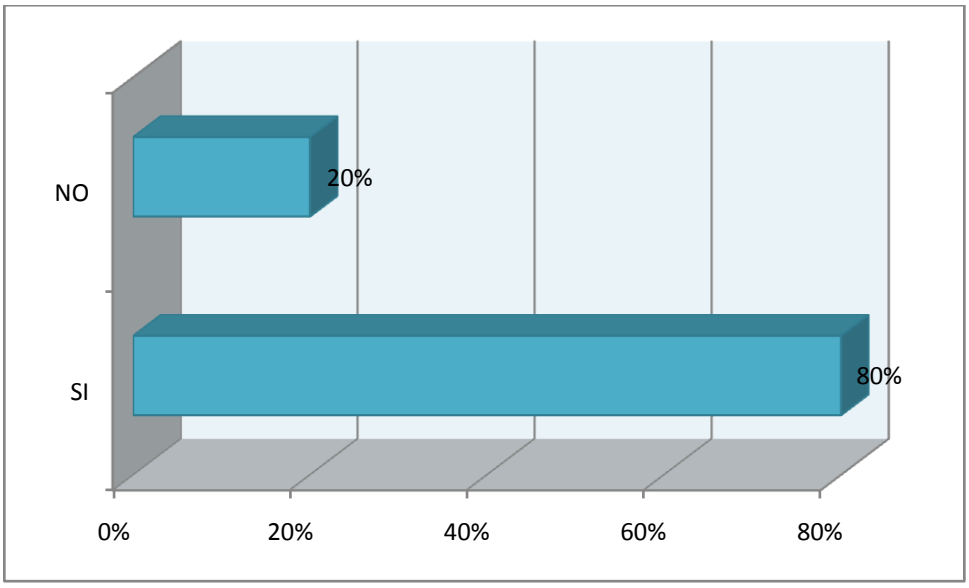

Figura 15. ¿Sabe lo que es una Red Social? Colegio Juan Montalvo

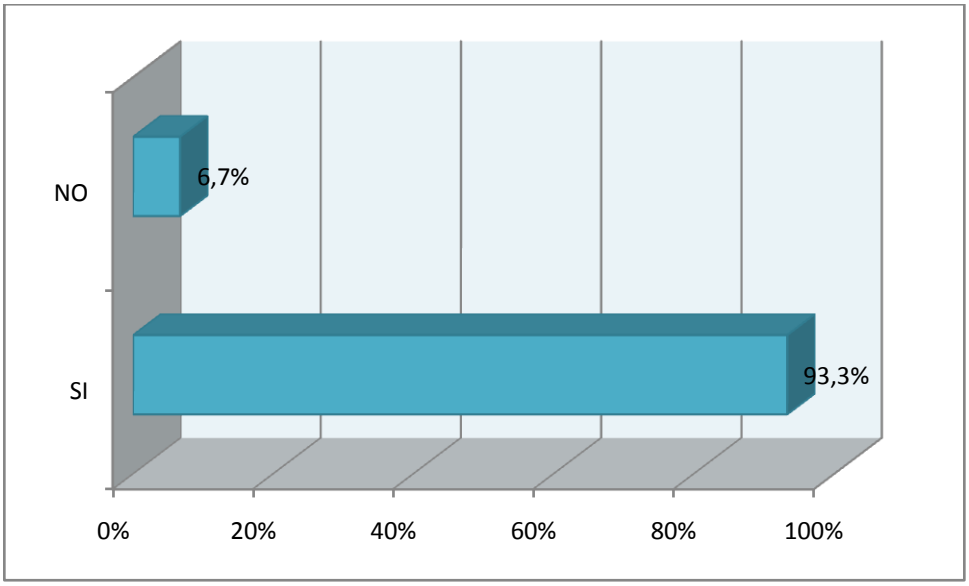

Figura 16. ¿Utiliza Redes Sociales? Colegio Juan Montalvo

En el **Instituto Técnico Superior "Daniel Álvarez Burneo"**, de un total de 62 personas encuestadas, el 95.16% asegura saber lo que es una red social, mientras

que el 4.84% asegura no saber lo que es una red social. Pero solo el 88.70% asegura utilizar alguna de las Redes Sociales mientras que el 11.30% asegura no usar ninguna Red Social.

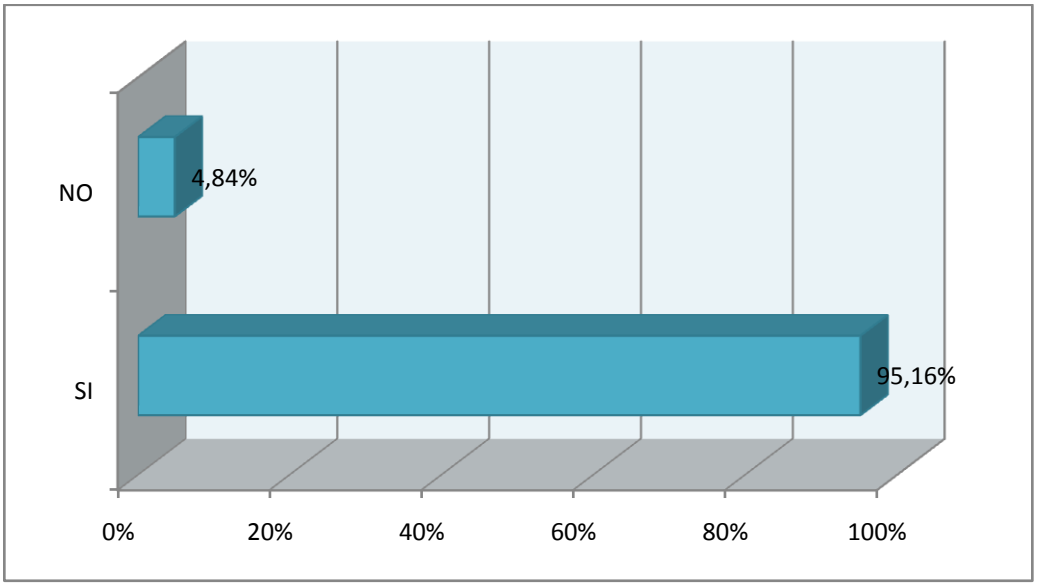

Figura 17. ¿Sabe lo que es una Red Social? ITS "DAB"

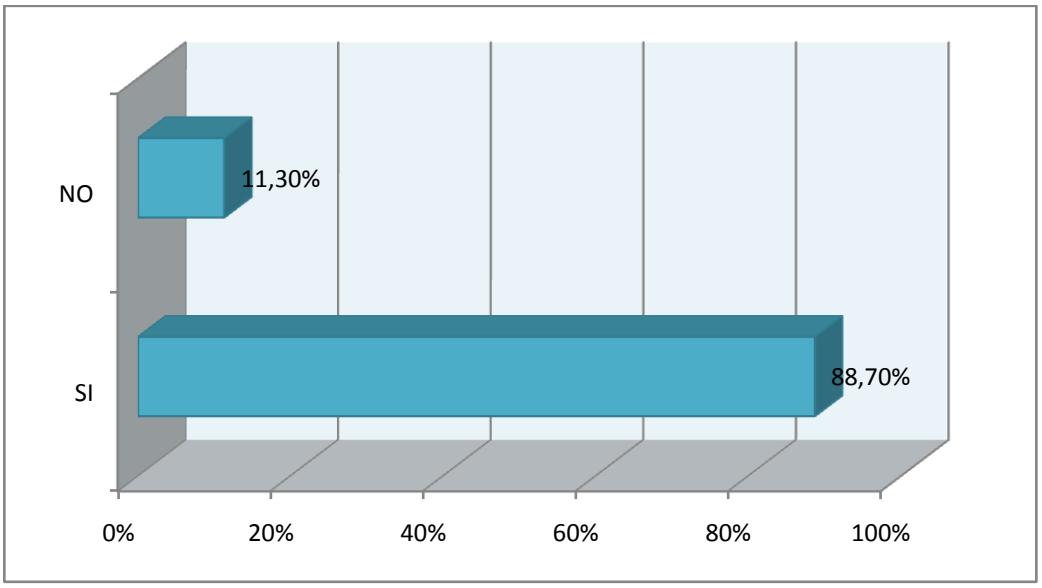

Figura 18. ¿Utilización de Redes Sociales? ITS "DAB"

En términos generales, el 18.65% no saben lo que es una red social, mientras que el 81.35% sabe lo que es una red social.

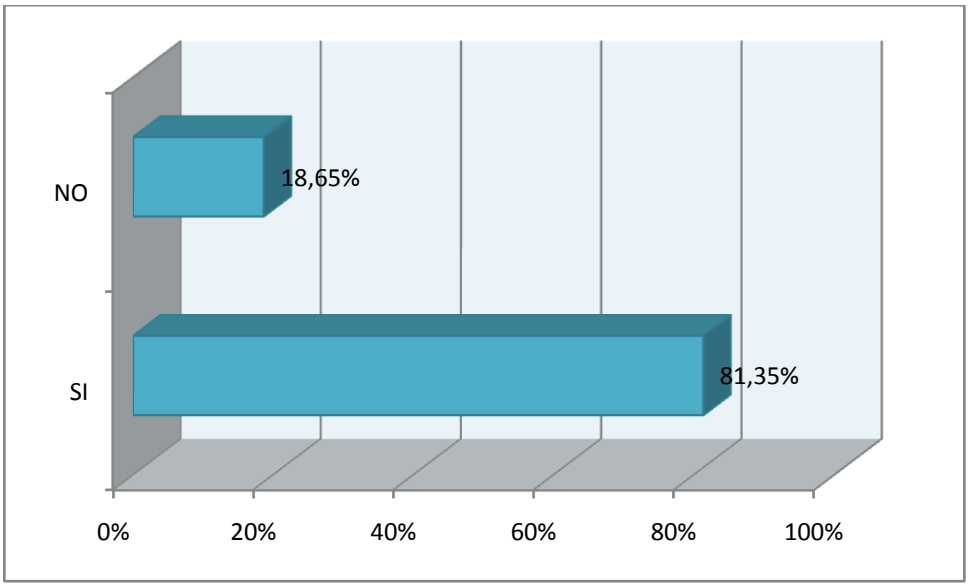

Figura 19. ¿Sabe lo que es una Red Social?

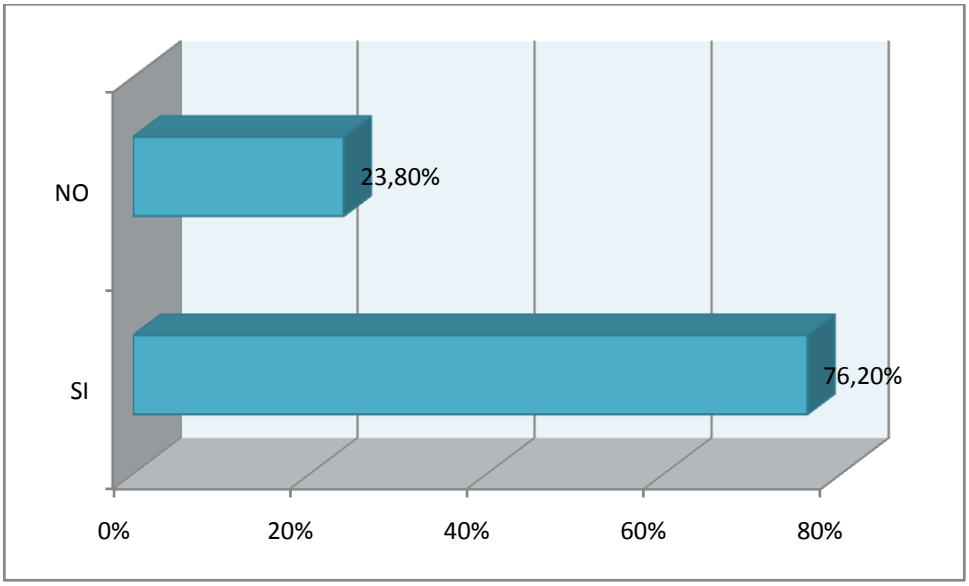

Figura 20. ¿Utiliza Redes Sociales?

- Redes Sociales con mayor incidencia

Una vez que se ha determinado que 441 personas de las 579 encuestadas usan alguna de las redes sociales, es decir el 76.20%. Ahora el siguiente paso es determinar cuáles son las redes sociales que están siendo mayormente utilizadas en la Ciudad de Loja.

De total de 441 de personas que aseguran usar redes sociales el 27.9% son usuarios únicos es decir que usan una sola red social, mientras el 72.1% aseguran usar más de una red social.

Como se observa en la Figura 21. Las redes sociales más usadas son Hi5 y Facebook con el 50.41% y 44.72% respectivamente. Otras redes sociales como Sonico llega al 2.44% y MySpace con 1.62% las demás redes sociales no llegan ni al 1%.

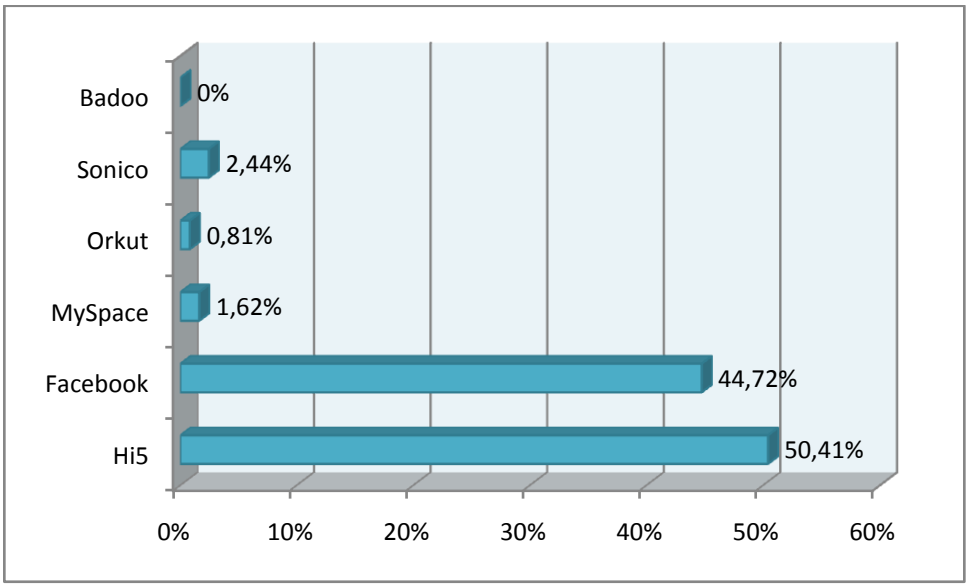

Figura 21. Usuarios únicos de Redes Sociales

- Usuarios de Múltiples Redes Sociales

De los usuarios de múltiples redes sociales, el 48.25% usan dos redes sociales, el 23.81% usan tres redes sociales y el 27.94% usan más de cuatro redes sociales.

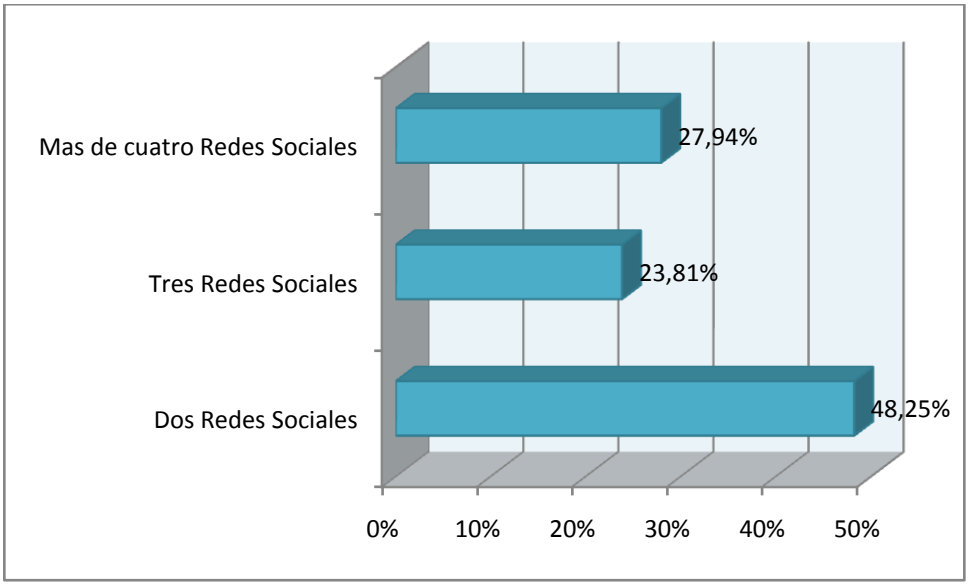

Figura 22. Usuario de múltiples Redes Sociales

- Número de Amigos en Redes Sociales

Al ser preguntado por el número de amigos que tiene en su red social, el 34.25% asegura tener menos de 100 amigos, el 26.98% asegura tener entre 100 y 200 amigos, el 13.83% asegura tener entre 200 y 500 amigos y finalmente el 24.94% asegura tener más de 300 amigos.

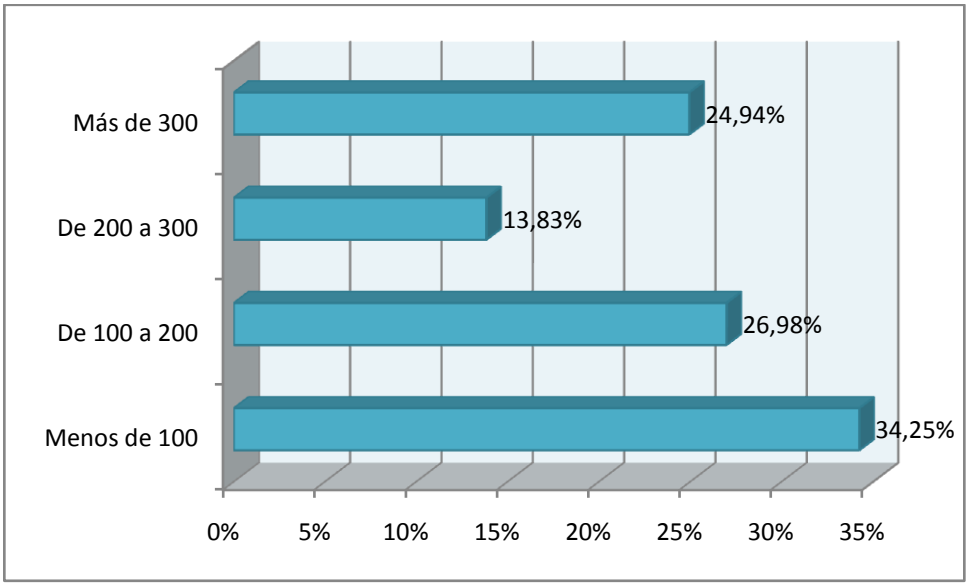

Figura 23. Número de amigos en Redes Sociales

❖ Comunidades o Grupos de amigos

La cantidad de personas que están formando parte de comunidades o grupos de amigos dentro de su red social alcanza el 73.18% y el 26.82% no forma parte de ninguna comunidad.

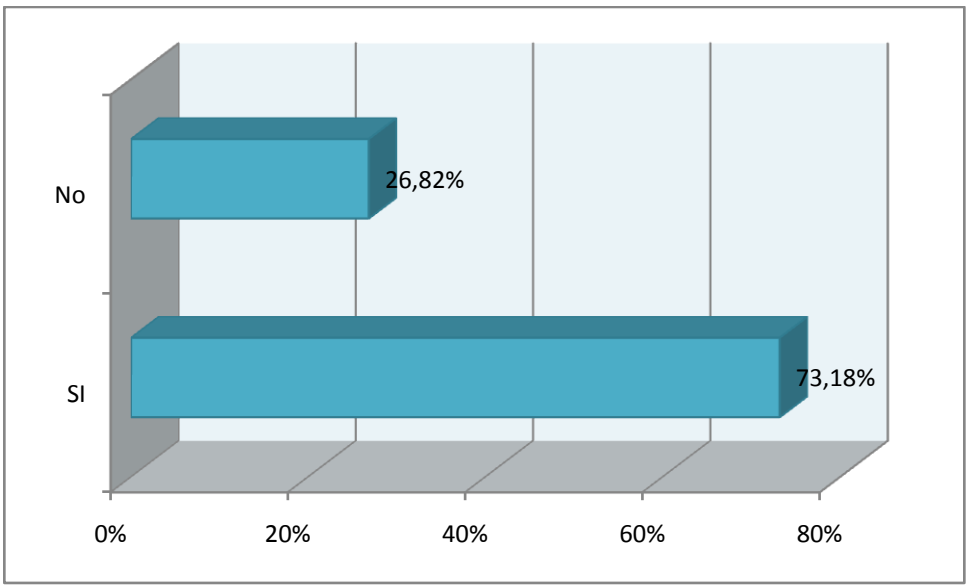

Figura 24. Usuarios en Comunidades o Grupos

❖ Frecuencia de Uso

La frecuencia con la que los usuarios acceden a las redes sociales es la siguiente: el 25.34% accede cada día, el 35.29% accede varias veces por semana, el 28.28% accede al menos una vez a la semana y el 11.09% casi nunca accede a las redes sociales.

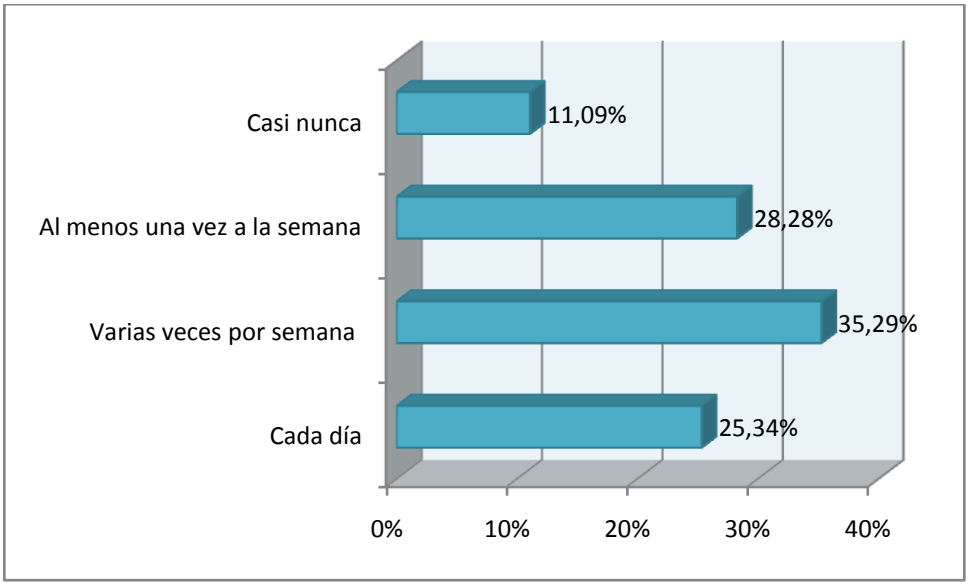

Figura 25. Frecuencia de uso de Redes Sociales

- Tiempo uso de Redes sociales

El tiempo en que los usuarios dedican a visitar las redes sociales es el siguiente:

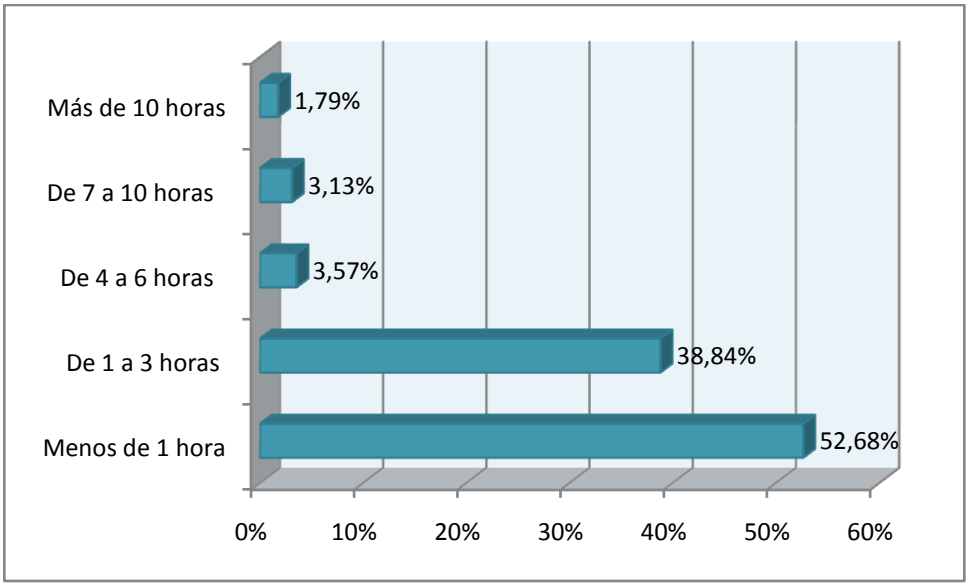

Figura 26. Tiempo de utilización de Redes Sociales

Es decir que el 52.68% usa menos de una hora a la semana, el 38.84% usa de 1 a 3 horas a la semana, el 3,57% usa de 4 a 6 horas a la semana, el 3,13% usa de 7 a 10 horas a la semana y finalmente el 1,79% usa más de 10 horas a la semana.

- Actividades Realizadas

Al ser preguntados por las actividades que suelen realizar en las redes sociales: el 31.76% ven fotos o videos, el 8.41% usa aplicaciones o juegos, el 21.83% sube fotos, el 18.43% envía mensajes, el 17.30% se relaciona con amigos y finalmente el 2.27 busca pareja.

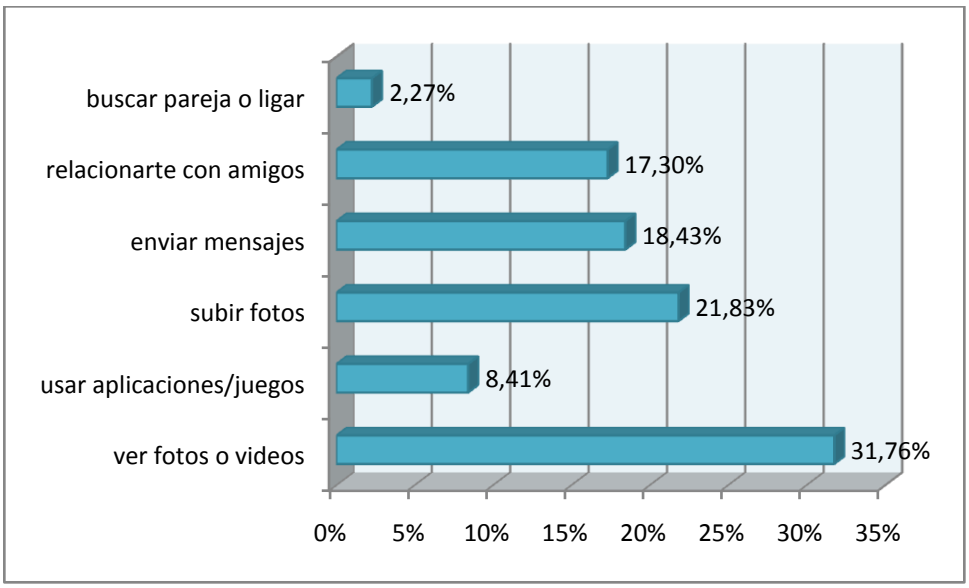

Figura 27. Actividades realizadas en Redes Sociales

- Lugar de acceso a Redes Sociales

Al momento de usar las redes sociales los usuarios suelen conectarse en: Casa el 23.59%, trabajo el 9.55%, Universidad o Colegio el 21.13%, Ciber Café 34.74%.

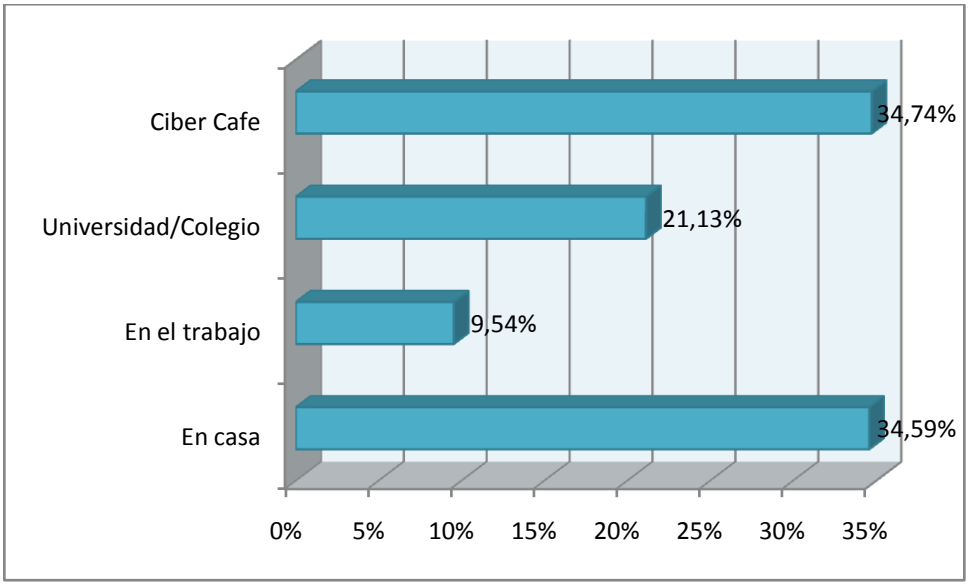

Figura 28. Lugar de acceso a Redes Sociales

- Relaciones Sociales

Cuando usa las redes sociales para relacionar con quien lo suele hacer: el 30.23% con amigos actuales, el 21.72% con amigos antiguos, el 18.06% con familiares, el 17.50% con compañeros de estudio, el 7.72% con compañeros de trabajo y el 4.77 con desconocidos.

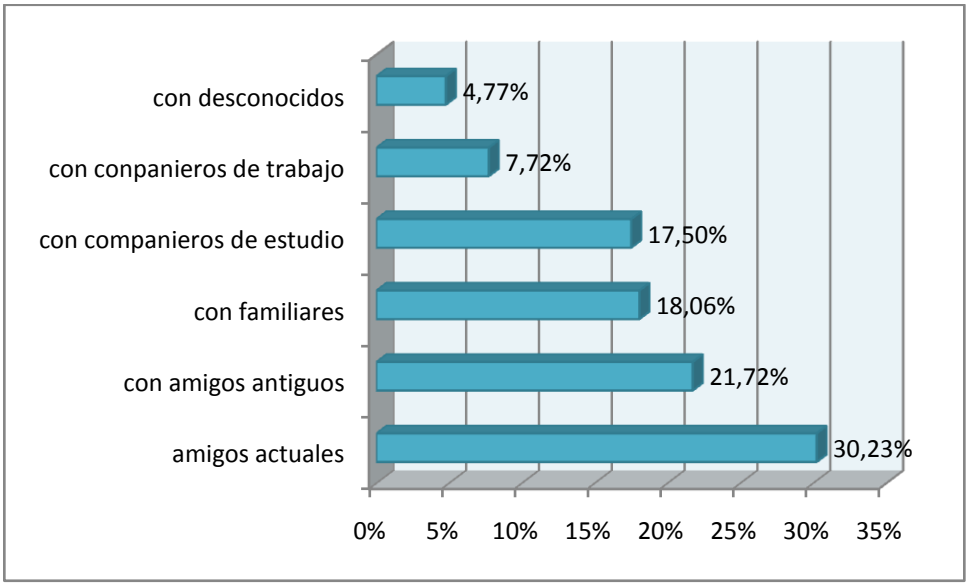

Figura 29. Con quien se Relaciona en Redes Sociales

❖ Lo más agradable de las Redes Sociales

Los encuestados aseguran que lo que más les gusta de las redes sociales es: estar en contacto con amigos o familia el 30.98%, conocer gente el 17.93%, ver y comentar fotos de amigos el19.57%, la comunicación el 16.13% y reencontrarse con amigos o familia el 15.13%

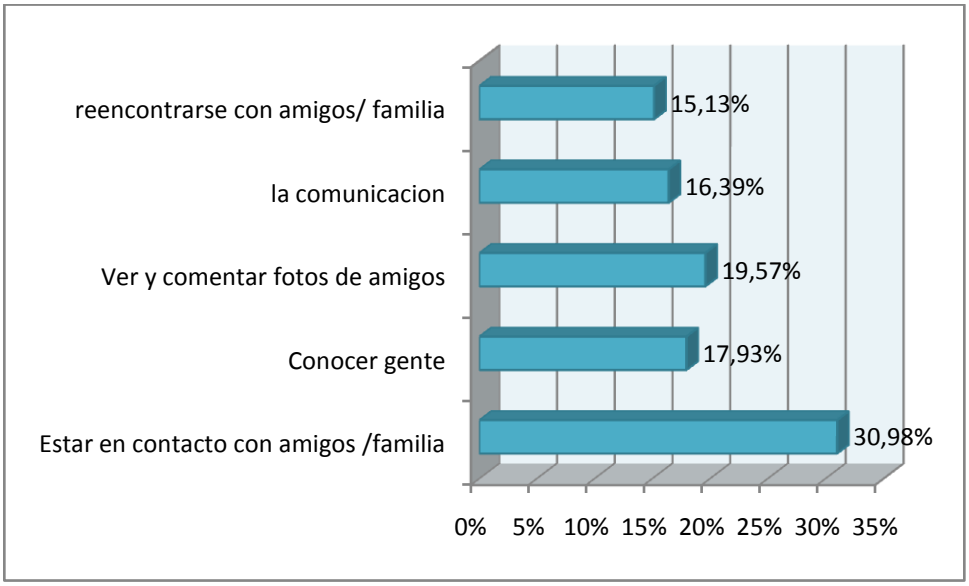

Figura 30. Lo más agradable de las redes sociales

❖ Lo que preocupa a los usuarios

Los encuestados aseguran que lo que menos les gusta de las redes sociales es: falta de privacidad el 38.49%, uso inmoral de datos el 23.97% y la publicidad el 28.55%. Mientras que el 8.99%, aseguran que todo les gusta.

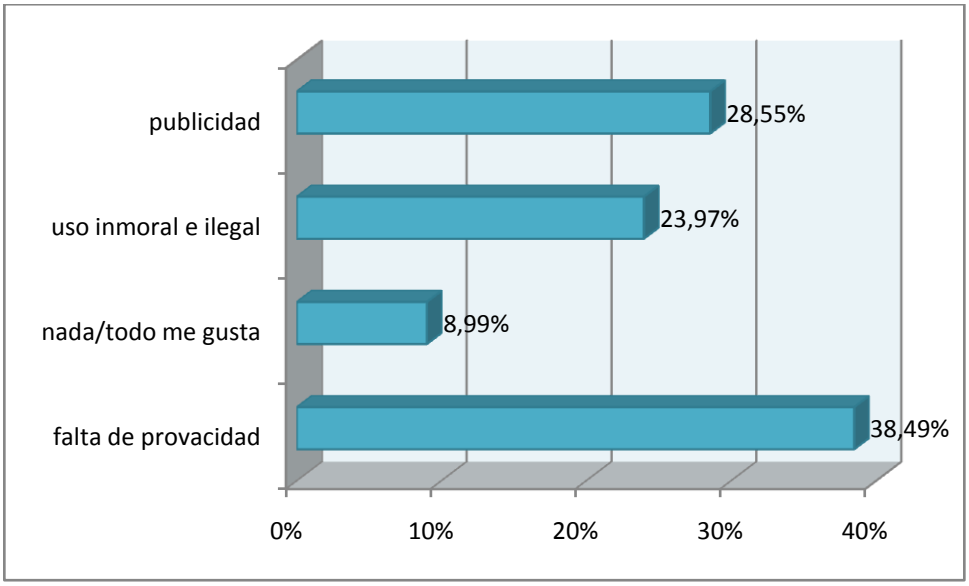

Figura 31. Lo que preocupa a los usuarios

2.6 Análisis de Resultados

Una vez obtenido el resultado de las encuestas, se ha llegado a la siguiente conclusión:

- El 76.20% de los encuestados asegura usar alguna de las redes sociales.
- Las redes sociales más usadas son: Hi5 (50.41%), Facebook (44.72%), Sonico (2.44%).
- En cuanto al tamaño de las redes sociales, la mayoría de usuarios (34.25%) poseen en su red social de uno a 100 amigos,
- La mayoría de los encuestados (73.18%) afirma ser parte del alguna comunidad o grupo de amigos.
- De los usuarios que pertenecen a una red social el 35.29% se conectan a la misma varias veces a la semana.
- Semanalmente el 53.18% accede menos de una hora a las Redes Sociales.

- La mayoría de los usuarios (31.76%) observa fotos y videos, el (21.83%) sube fotos y (18.43%) envía mensajes.

- Al momento de usar las redes sociales la mayoría (34.74%) acceden desde un Ciber Café, mientras que el (34.59%) lo realizan desde su casa.

- Al momento de relacionarse con otras personas a través de su red social, el (30.23%) lo realiza con amigos actuales, mientras que el (21.72%) con amigos antiguos y el (18.06%) se relaciona con sus familiares.

- El (30.98%) de los usuarios asegura que lo que más les gusta de las redes sociales es estar en contacto con amigos y familia. En cambio el (38.49%) le preocupa la falta de privacidad de las redes sociales y el (23.97%) le preocupa el uso inmoral de datos.

3. SEGURIDAD DE REDES SOCIALES

La popularidad que han alcanzado las redes sociales, y de la que ya hemos hablado en capítulos anteriores, convierte a estos sitios en uno de los principales objetivos de los hackers. Si bien, posiblemente no se pueda atacar a Hi5 o Facebook como tal, pero si pueden atacar al elemento más valioso y vulnerable a la vez que tienen las redes sociales, que son los usuarios, si estos demuestran poco interés en la privacidad de su información personal; de nada sirven las barreras implementadas en los servidores de estos sitios.

En el presente capitulo se analiza las políticas de privacidad, parámetros configurables de privacidad, las condiciones de uso y todos los aspectos relacionados con la estructura de las seguridad y privacidad de las redes sociales con mayor incidencia en nuestro entorno.

3.1 Estructura de Seguridad de Redes Sociales

Las redes sociales, con el objetivo de salvaguardar la información de sus usuarios, han implementado parámetros configurables de seguridad y privacidad. Estos parámetros deben estar configurados acorde a las necesidades de privacidad de cada usuario, y precisamente esa es la idea central, que cada usuario establezca hasta que punto va a compartir su vida en la red social.

A continuación se analizan el esquema de seguridad de las redes sociales que en el Capítulo II, se identificaron como las de mayor incidencia en la Ciudad de Loja. El Análisis se enfoca en parámetros configurables de privacidad y aspectos relacionados con la privacidad de las redes sociales analizadas.

			
Exposición de información (por defecto)			
Perfil	Todos	Todos	Amigos
Inf. de contacto	Todos	Amigos	Amigos
Lista de amigos	Todos	Todos	Amigos
Contenidos	Todos	Todos	Amigos
Estados	Amigos	Todos	Amigos
Búsqueda	No Aplica	Todos	SI
Información Obligatoria			
Email	x	x	x
Nombre	x	x	x
Apellido	x	x	x
Genero	x	x	x
F. Nacimiento	x	x	(Se puede ocultar)
País			x
Ciudad			x
Configuración de privacidad			
	- Perfil - Correo - Fotos - Actualizaciones - Estados en línea *Ver Anexo B*	- Inf. de perfil - Inf. de contacto - Aplicaciones - Búsquedas - Lista de Bloqueados *Ver Anexo C*	- Mi perfil - Mensajes - Búsquedas - Sonico Chat - Notificaciones *Ver Anexo D*

Tabla 3. Resumen de Información publicada en Redes Sociales

3.1.1 Privacidad en Hi5

Hi5 diferencia dos tipos de información:

"Información personal" es información sobre el usuario que lo identifica personalmente, por ejemplo, su nombre, dirección, dirección de correo electrónico, número telefónico.

"Información anónima" es aquella que no está asociada o vinculada a su información personal; la información anónima no permite la identificación de personas individuales.

Hay que tener en cuenta que toda la información tanto personal como anónima es recolectada y almacenada por Hi5 y puede ser utilizada para sus propios propósitos internos, como lo establece Hi5 en su política de privacidad (25).

La privacidad de la información personal esta cargo del usuario para ello Hi5 al igual de muchas de las redes sociales ha puesto a disposición de sus usuario algunas opciones configurables de privacidad (Anexo B), ya que por defecto esta red social proporciona una cuenta totalmente abierta, donde, las fotos, comentarios, estados e información personal, puede ser vista por cualquier usuario e incluso por personas que no se han registrado. A continuación, se detalla algunas de las configuraciones más relevantes:

- ***Perfil****:* Muestra toda la información ingresada voluntariamente por el usuario. En *Ajustes de Perfil* el usuario es quien decide si todos los usuarios o solo sus contactos pueden ver su perfil, de igual manera puede determinar si todos lo usuario o ningún usuarios pueden "*ver que visite su perfil* ".

- ***Fotos****:* Todas las fotos que se han subido a Hi5 se encuentran organizadas por Álbumes, las fotos pueden ser etiquetadas y comentadas por cualquier usuario. En *Ajustes de Fotos* el usuarios puede configurar si desea o no recibir comentarios en las fotos, si decide recibir comentarios en las fotos, es necesario

activar la opción de *No acepto automáticamente en fotos* de tal manera que el propietario del perfil es quien decide lo que se publica.

- ***Estado****: Las actualizaciones de los estados en línea son mensajes cortos que los usuarios publican, los estados por defecto aparecen en la parte izquierda de la página de inicio de hi5 de todos los amigos de Red. Hi5 permite restringir la publicación de los estados, en Ajustes de Estados en Línea* activando la opción ¨Ningún usuario puede ver mi estado en línea¨

- Quien visito mi perfil*:* Hi5 Permite ver quién visitó nuestro perfil durante el día y muestra las visitas que has tenido a lo largo del tiempo, desde el momento de activación de la cuenta. El usuario puede permitir o no que los demás usuarios vean que "*visite su perfil*" en *Ajustes de Perfil*.

- ***Fives****:* Los Fives son una especie de emoticones permanentes con los cuales se puede dedicar como gratificación, recuerdo, diversión o conmemoración. Del mismo modo que con los comentarios, el usuario decide si desea recibir Fives de todos los usuarios, solo de sus amigos o desea no recibir Fives.

- ***Notificaciones****:* Las Redes Sociales por lo general envía notificaciones al correo electrónico de todas las actividades que se desarrollan en la misma. Esto suele ser un poco molesto y se presta para confusiones con enlaces malintencionados.

- **Búsquedas**: A diferencia de las demás Redes Sociales analizadas, Hi5 no permite restringir la visualización de nuestro perfil en las búsquedas que cualquier usuario realicen.

3.1.2 Privacidad en Facebook

Facebook ofrece un panel de configuración de privacidad, cuando está bien configurado en cierta manera asegura un control de la imagen pública del usuario.

En Facebook, hay tres niveles básicos de privacidad: **Amigos**, **Amigos de amigos** y **Todos**. Un extremo de apertura es "Todos", donde cualquiera puede acceder a esa información con sólo hacer una búsqueda en Facebook. El otro extremo, es personalizar uno a uno los usuarios que pueden ver o no la información.

Si el usuario ajusta un mayor nivel de privacidad, impedirá que en el futuro otros usuarios lo encuentren, limitando la socialización, por otro lado si se deja las opciones de privacidad establecidas por defecto, consiente el acceso de cualquier individuo a su información. De nada serviría establecer niveles máximos de privacidad si la intención es hacer amigos.

El perfil, por defecto, tiene marcada la opción de que toda su información sea pública y que se pueda publicar en buscadores. Si esto ocurre, una vez que la información haya salido de Facebook, este sitio no se responsabiliza por lo que puedan hacer con su información.

El propio Zuckerberg cree que la privacidad es una rémora del pasado. Según su visión, los usuarios de la red en los últimos años percibieron el valor de compartir en Internet conocimiento, temas personales, gustos, preferencias y contenidos (26).

En la Guía sobre la privacidad de Facebook (27), se detallan los parámetros configurables de privacidad están organizados en las siguientes secciones:

Información personal y publicaciones ofrece detalles personales, como tu cumpleaños e ideas políticas, junto con tu contenido y el que otros han publicado en tu muro. Controlas quién puede ver cada tipo de información.

Información de contacto ofrece los detalles de contacto, como tu dirección de correo electrónico y número de teléfono. Te recomendamos que sólo esté visible para tus amigos.

Amigos, etiquetas y conexiones ofrece la información y el contenido que habéis compartido tú y otras personas en Facebook. Esto incluye relaciones (compartidas entre tú y la persona con la que estés relacionada), intereses y fotos en las que te han etiquetado. Esta configuración te permite controlar quién ve la información en tu perfil real. Sin embargo, puede seguir estando visible en otros sitios a menos que la elimines del perfil. Por ejemplo, otros usuarios podrán ver que estás conectado a una página si están en esa página. Además, tus relaciones con otras personas pueden aparecer en sus perfiles.

Aplicación y sitios web ofrece la información que está disponible en las aplicaciones que usáis tú y tus amigos.

Buscar te permite controlar si se te crea un resultado público de búsqueda. También puedes controlar quién puede ver tu información en la búsqueda de Facebook.

Lista de bloqueados te permite identificar a determinadas personas a las que quieres impedir que interactúen contigo en Facebook.

3.1.3 Privacidad en Sonico

Sonico, dice que no es necesario publicar datos, como número de teléfono y dirección personal. Asegura que si los contactos quieren este tipo de información deben pedir mediante un mensaje personal, por ello, datos como orientación política o religiosa ni si quiera existe en el perfil, esto con la intención de evitar cualquier intento de agresión y por contrario fomentar el dialogo. Otros datos como número de celular está incluido opcionalmente sólo para aquellos que formen redes cerradas y controladas**.**

La diferencia de Sonico con las demás Redes Sociales se basa en dos aspectos, el primero es su sistema de *moderación manual proactiva de contenidos*, que consiste en un equipo dedicado exclusivamente a chequear cada perfil nuevo y el contenido subido al sitio, para verificar la autenticidad de los perfiles y evitar pornografía, pedofilia, abuso y discriminación. El segundo es la segmentación en

detalle (edad, sexo, geografía, por perfiles) (28). Sonico asegura que, "Esta combinación logra que las marcas se sientan más protegidas y seguras para participar y exponer sus productos, a la vez que les reporta excelentes resultados" (29).

En diciembre de 2009, Sonico lanzó un nuevo sistema de privacidad denominado **PPP**: *Privado, Público y Profesional*. Este sistema establece niveles de confianza, que permiten comportarse, comunicarse y segmentar la información que se comparte dependiendo de la confianza que se tenga con el otro usuario. Rodrigo Teijeiro, Desarrollador de Sonico, asevera que: "*hemos descubierto que en la vida real las personas se desenvuelven e interactúan en distintos ámbitos de manera diferente y de acuerdo a cada ámbito varía el tipo de información que se comparte*" (30). Este sistema en realidad son tres perfiles que permiten organizar la vida online de los usuarios.

El Perfil Privado, cuenta con la mayor cantidad de herramientas para compartir fotos, videos, comentarios, organizar eventos y relacionarse con personas de confianza.

El Perfil Publico, permite integrar herramientas externas como blogs, cuentas de Twitter y otros sitios, además de facilitarle a otras personas, la posibilidad de seguir nuestra actividad.

El Perfil Profesional, se centra en el Curriculum Vitae y experiencia laboral y sirve como punto de partida para relacionarnos con otros profesionales, establecer un punto de contacto y emprender o participar en búsquedas laborales.

Tus **amigos** podrán acceder a tu **perfil privado**
Tus **seguidores** podrán acceder a tu **perfil público**
Tus **contactos** podrán acceder a tu **perfil profesional**

3.1.4 Otras Condenaciones de Privacidad

Hay que tener en cuenta que las configuraciones internas de privacidad no son suficientes para que un usuario se sienta cien por ciento seguros en su red social. Existen otras consideraciones de seguridad que son desconocidas por los usuarios y que hay que tener en cuenta.

Cookies.- Sonico asegura que en ningún caso las cookies proporcionarán información de carácter personal de usuario, quien en relación a las mismas mantendrá pleno anonimato, aun frente a Sonico.com, dado que tampoco suministran información tendiente a la individualización del usuario. Por su parte, Hi5 puede usar tanto las cookies de sesión y las cookies persistentes. Las Cookies permiten identificarle a un individuo como un usuario concreto y permite guardar sus preferencias personales, así como información técnica como puedan ser vistas o páginas concretas que visite. Facebook también usa cookies para publicidad y proteger al usuario.

Indexación de contenidos.- Se refiere a la extracción de contenidos e información personal de las redes sociales por parte de los buscadores para ser presentado como resultado de sus búsquedas. En octubre de 2009, Microsoft anunció planes de incorporar los mensajes públicos de Facebook en sus resultados de motor de búsqueda, aunque el servicio aún no está disponible. Google anunció recientemente planes para incorporar cierta información de Facebook en su nuevo producto de búsqueda a tiempo real, pero la información se limitará a los perfiles especiales de las páginas de Facebook creadas por famosos y empresas (31). Además, las actualizaciones de las páginas de fans de Facebook comenzarán a aparecerá en los resultados de búsquedas en tiempo real de Google (32).

Web Beacons.- Son gráficos ocultos en las páginas web, que se usan generalmente para registrar varios datos sobre los visitantes de la página. Línea de código que utiliza un sitio web o un servidor publicitario de un tercero para realizar el seguimiento de la actividad de un usuario (33). Las redes sociales pueden albergar también web beacons, se utilizan de una forma similar a las

cookies. Además, suelen utilizarse para medir el tráfico de usuarios que visitan una página web y poder sacar un patrón de los usuarios de un sitio.

El Programa Facebook Beacon (faro), contempla la colaboración entre Facebook y distintas marcas comerciales. Es un programa controversial, porque requiere que Facebook siga los movimientos de sus usuarios en los sitios web de las empresas que pagan por participar en el mismo (34).

4. RIESGOS POTENCIALES

Cada día, millones de personas alrededor del mundo acceden a su red social, pero no todos lo hacen con la intención de socializar; un grupo considerable y creciente de usuarios acceden a estos sitios con el objetivo de obtener algún beneficio y es que estos sitios no son totalmente seguros, aparte de las técnicas conocidas de ciberdelincuencia, los usuarios están expuestos al envío de mensajes amenazantes, inserción de contenidos lesivos contra el honor, la usurpación de identidad con fines fraudulentos, uso de contenidos delictivos, entre otras, que constituyen un abanico de técnicas y conductas que son utilizadas por los ciberdelincuentes.

Los usuarios no solamente exponen sus datos de contacto y fotos en las que aparecen, sino que también publican fotos de su familia, amigos y de sus propiedades, además publican sus vivencias, viajes, ideología política, pensamiento, contenidos en general y están pendientes de compartir con sus “Amigos” todas las actividades que realizan en el día, pero entre sus “Amigos” pueden haber personas que están a la espera del momento oportuno para atacar. Aunque en nuestro medio no se han reportado casos de ciberdelincuencia en redes sociales hay que considerar seriamente los riesgos que conlleva la utilización de estas comunidades.

En el presente capitulo se analizan los riesgos potenciales y las técnicas usadas por los ciberdelincuentes en las redes sociales, muchas de las técnicas de ciberdelincuencia tradicional han sido adaptadas para ser usadas en redes sociales y otras que surgieron específicamente para estos sitios.

4.1 Principales Riesgos de Participar en Redes Sociales

“Las redes sociales hoy en día son muy comunes y es normal que una gran cantidad de usuarios de Internet participen de las mismas, y es por eso, que los atacantes comenzaron a dirigirse hacia ellas como nuevo foco de ataque”, explicó Cristian Borghello, Technical & Educational Manager de Eset para Latinoamérica (35). Y es que las redes sociales han superado la función fundamental para las que fueron creadas, que es de interrelacionar a personas. Ahora que las empresas han visto en estas

comunidades un nuevo canal para llegar directamente a los clientes potenciales, los ataques son más frecuentes. Sophos en su estudio denominado Security Threat 2010, afirma que existe un incremento en los ataques de spam y malware, en el último año el 57% de los usuarios recibió correo basura a través de redes sociales y esto representa un incremento del 70.6% comparado con el año anterior. Además el número de infectados y propagadores de malware registro un crecimiento del 69.8% (36)**.**

"Los sitios de redes sociales como MySpace y Facebook ya han tomado la posta como basureros virtuales de spam, troyanos y spyware" (37). A continuación se detallas los principales riesgos de participar en las Redes sociales.

4.2 Ingeniería Social

Es un conjunto de técnicas, usadas para engañar o manipular a las personas para que revelen voluntariamente información confidencial sin que ellos se den cuenta y para que hagan cosas que normalmente no lo harían. La Ingeniería Social usa principalmente las redes sociales, pero puede valerse de cualquier medio para obtener información de las personas, no solo está asociado de las acciones ejecutadas en línea y se aprovecha principalmente de la credulidad de las personas.

Para los Ingenieros Sociales no existen barreras, se puede tener la mejor tecnología, firewalls, sistemas de detección de ataques, dispositivos biométricos, etc. Lo único que se necesita es un llamado a un empleado desprevenido, aplicar una de sus técnicas y obtener acceso total al sistema (38).

4.3 Exposición de la Información

Una revisión aleatoria de perfiles de usuario en Hi5, Facebook y Sonico permitió descubrir que muchos usuarios publican fotos de viajes, fiestas, amigos, familia, etc.. Además combinan estas redes sociales con otros servicios de video como Youtube que hacen de estos perfiles un verdadero resumen de nuestras vidas. La exposición de la información puede causar:

Robo de información	El robo de información través de las redes sociales ocurre de forma constante, la extrema confianza de los usuarios, tras el descuido en la configuración de privacidad da paso a una peligrosa exposición de su vida online. La información personal así como publicaciones y fotos pueden ser usadas de manera fraudulenta.
Deducción de Contraseñas	Muchos de los usuarios usan como contraseña o como parte de su contraseña cierta información personal como nombres, apellidos, fecha de nacimiento, número de identificación personal o números de teléfono, así como también gustos, preferencias o cualquier otra información que puede ser deducida a través de las publicaciones de su perfil. En la actualidad existen programas que funcionan como adivinador de contraseñas que tiene un alto grado de efectividad esto principalmente porque los usuarios no crean contraseñas fuertes.
Usurpación De Identidad	Las personas que de una u otra manera logran descubrir nuestras credenciales de acceso a nuestra red social, pueden usurpar nuestra identidad para realizar acciones amenazantes y publicaciones de contenidos lesivos contra el honor de otros usuarios, que pueden crear conflictos y llevar al enfrentamiento de personas inocentes.
Falsa Identidad	Los usuarios malintencionadamente suelen crear perfiles con identidades falsas de personas o empresas tomando en ocasiones información real, pero con fines fraudulentos. Se calcula que hasta un 40% de los

	nuevos perfiles en Facebook son falsos (39). Un estudio desarrollado por Bit Defender demuestra que los perfiles falsos más exitosos son aquellos más cuidados y que imitan a los reales, al incluir, por ejemplo, muchas fotos e información. En este estudio se crearon tres perfiles, el primero de ellos, sin ninguna foto y sin apenas información del usuario ganó 23 amigos; otro con una foto y algo de información, 47; y el tercero, con muchos datos y muchas fotos, 53 (40).
Crímenes Contra el Honor	Las redes sociales y sus innumerables perfiles falsos dan paso a la divulgación de comentarios malintencionados, rumores, calumnias e injurias acerca de otros usuarios. Por lo general, esta información es propagada a través de las actualizaciones de estado y a través de mensajes que en ocasiones incluyen fotomontajes.

Tabla 4. Riesgos de la exposición de la Información (creación propia)

4.4 Secuestro

Ahora que las redes sociales son fácilmente accedidas a través teléfonos celulares, es muy común ver que nuestros amigos publican en sus estados su ubicación especifica, si están viajando publican la ruta que están tomando, el destino y más información que permitirá ubicar físicamente al usuario de la red social. Toda esta información ingresada a través de nuestros estados, más la información del perfil crea la posibilidad de un secuestro, y es que, para un secuestrador, en lugar de vigilar a sus víctimas, solo observan sus publicaciones ya que ellos se encargan exhibirse ante cualquier persona y generalmente, como quieren relacionarse, se exhiben como más poderosos y ricos de lo que son. Eso los hace terriblemente vulnerables (41). Un

ejemplo de ello es lo que sucedió con Francisco Grassi, estudiante universitario guatemalteco quien fue secuestrado tras ser engañado a través del chat de Hi5 (42).

4.5 Odio y Violencia

Un informe de Simon Wiesenthal Center reveló que en 2009 el uso de Internet por parte de grupos milicianos y violentos, a través de redes sociales como Facebook, Twitter y YouTube, aumentó un 20%, habiéndose creado en ese período 1.500 nuevos sitios que promueven la violencia, el antisemitismo, la homofobia, la música de odio y el terrorismo (43).

El caso más conocido y cercano a nuestro medio de violencia en redes sociales es el suscitado en Colombia, donde un grupo de Facebook titulado *"Me comprometo a matar a Jerónimo Alberto Uribe, hijo de Álvaro Uribe"*, incitada a agredir al hijo del Presidente de Colombia, este delito fue catalogado y sancionado como terrorismo (44).

Figura 32. Violencia y odio en Redes Sociales (44)

Una revisión aleatoria de los grupos a los que pertenecen mis amigos en mi Red Social, permitió descubrir que algunos de ellos están vinculados a grupos como "*No*

soporto Jorge Ortiz" (45), "*Ecuador declara persona no grata a Jaime Nebot*" (46) y "*Odio las Cadenas Nacionales del Presidente*" (47), con 10.791, 5.043 y 27.776 seguidores respectivamente. Estos grupos evidentemente están promoviendo cierto tipo de odio o violencia en contra de estos personajes.

4.6 Dating

Muchos usuarios de las redes sociales utilizan sus servicios para encontrar pareja. Lamentablemente esto es un peligro inminente, ya que conduce a la creación de múltiples cuentas de usuario, con mucha información, fotografías y que por lo general no tienen ninguna restricción de acceso. Lo recomendable es no organizar encuentros con desconocidos que se contactan a través de la red social. Pero, en caso de hacerlo, se debería elegir lugares públicos y concurridos, ya que los usuarios pueden ser objeto de algún tipo de delincuencia tradicional. En este sentido, en Sonico fue removida la opción "Interesado en" de los perfiles para minimizar ese riesgo. Además, todo usuario que sea encontrado haciendo lo popularmente llamado dating, sufrirá la eliminación de su cuenta (48).

4.7 Propagación de Malware

Eset Latinoamérica informa sobre la utilización de las redes sociales para propagar malware, se trata de perfiles falsos de MySpace procedentes de China; los enlaces hacia estos perfiles son enviados al correo electrónico y cuando el usuario ingresa sus credenciales de acceso automáticamente se descarga un troyano llamado "*downloader"* para que este descargue otros malware en equipo ya infectado. La URL creada por el atacante es similar a las verdaderas de los perfiles de usuarios de MySpace, pero el dominio apunta (en este caso) a sitios chinos creados para alojar malware

4.8 Virus

Koobface es probablemente el virus de redes sociales más conocido, apareció en 2009 atacando principalmente a MySpace, Facebook, LinkedIn y Twitter. Kookface

envía mensajes a los contactos de una cuenta infectada provocando que los demás usuarios bajen el virus e infecten sus cuentas (49). La infección se consigue a través de la ingeniería social, ya que los usuarios son en su mayoría engañados para hacer clic en enlaces maliciosos integrados en mensajes personales haciéndose pasar por un amigo (50). La técnica de infección era muy simple pero resulto ser muy eficiente, ya que el gusano usaba las cuentas ya comprometidas para atraer amigos para atraer a los amigos del usuario e invitarlos a del clic en enlaces malicioso (51). Luego de una infección exitosa Koobface intenta obtener información confidencial de las víctimas.

Otros gusanos más complejos usan manipulaciones avanzadas de URL para un ataque CSRF (Cross-Site Request Forgery) o Falsificación de petición en sitios cruzados en español. La URL maliciosa creada por los gusanos es publicada en los perfiles de los usuarios a fin de propagarse infectado los contactos.

4.9 Social Phishing

Consiste en capturar información personal y financiera de las victimas con el objetivo robar dinero, suplantar a personas, entre otras. Se comete mediante un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta. El estafador conocido como Phisher envía un correo simulando ser una invitación a pertenecer a una red social, o simulando que algún contacto ha realizado un comentario de tu estado, publicación o foto, con enlaces hacia el supuesto sitio web. Sin embargo, cuando el usuario da clic en el enlace disponible ingresa a un sitio idéntico al real, pero falso, donde se piden nombres de usuario y contraseñas. Una vez que el usuario haya ingresado sus credenciales de acceso, el atacante los recibirá de manera automática y podría utilizarlos para cometer algún delito. De igual forma, tendría acceso a información personal de la víctima y datos privados de los contactos. La información recolectada en las Redes Sociales puede ser usada maliciosamente de distintas maneras, según un informe de Eset Latinoamérica (35).

Los ciberdelincuentes están al asecho y los momentos de mayor riesgo son cuando hay noticias sobre personajes muy populares en la red, o tras alguna hazaña deportiva

de importancia mundial, durante la celebración de eventos de importancia global e incluso se inventan la muerte de algún famoso para llamar la atención. Algunos experimentos han otorgado una tasa de éxito de un 90% en ataques Phishing en redes sociales (54). Otro estudio realizado en junio de 2004 en los Estados Unidos con los cadetes de West Point, revelo que el 80% de los 500 cadetes a los que se les envió un e-mail falso fueron engañados y procedieron a dar información personal (55).

Según un informe de MessageLabs Intelligence 2008, una táctica popular de los ciberdelincuentes incluyó el uso de cuentas ficticias en sitios de Redes Sociales para activar enlaces maliciosos que conducían usualmente a sitios de Phishing (56). Además revela que los ciberdelincuentes explotan la información del estafado de tal manera que obtienen las credenciales de acceso a las redes sociales con el objetivo de subir comentarios, correo basura y enlaces a estafas Phishing en los perfiles de los amigos del estafado, proporcionando cierto nivel de confianza a estos enlaces. En este mismo sentido, el 45% de los españoles encuetados por RSA ha sufrido algún ataque de Phishing en Facebook y Tuienti, y por ello el 81% se muestran preocupados con la seguridad de sus datos personales (57). En Latinoamérica, Según ItEcuador, hubo un incremento de 135% en el número de fraudes en línea y 80% de los casos de fraude del 2008 fueron mediante Phishing (58).

4.10 Spam 2.0

Con la llegada de la Web 2.0 y el auge de las redes sociales, los spammers han vistos en estas comunidades una gran oportunidad para inundarlas de correo basura, principalmente publicada y noticias, con el objeto de hacer daño a los usuarios, ya sea con enlaces a estafas Phishing, Malware u otra técnica de ciberdelincuencia. “El componente viral que poseen las redes sociales hace al spam interesante. En teoría si etiquetó a 20 personas en una foto, y cada uno cuenta con 150 amigos en promedio, tendríamos un alcance de 3.000 personas. Eso es en teoría, ya que el abundante flujo de información hace que se diluya fácilmente”, señala Alfredo Velazco, de Incom (59).

Según un estudio realizado por la empresa Brightmail, aproximadamente un 14% del spam a lo largo del 2004 está asociado a fraudes, y un 80% a la oferta de servicios o

compra de productos (60). En el Informe de Security Report 2010 de Sophos, evidencia que: El 57% de los usuarios reconoce haber sufrido ataques de spam a través de sitios de redes sociales durante 2009, lo que supone un aumento del 70,6% con respecto al año pasado (36).

4.11 Aplicaciones

En las redes sociales como Facebook, aún los usuarios más cuidadosos pueden entregar información personal a extraños sin que se den cuenta, al usar una aplicación diseñada por terceros y que incluyen juegos, testes, competencias, concursos de conocimientos entre otros, estamos permitiendo que estos accedan a nuestra información. Adrienne Fell, de la Universidad de Virginia, que recientemente estudió la seguridad de Facebook. Examinó más de 150 de las aplicaciones más populares para ver cuánta información podría ella acumular. Afirma que el 90% de las aplicaciones tienen un acceso innecesario a datos privados. "Una vez que la información llega al servidor de un tercero, Facebook no puede hacer nada" (61).

4.12 Juegos Sociales

Redes sociales como Hi5 han apostado por los juegos sociales. Los juegos sociales requieren que los usuarios agreguen a mas usuarios para jugar el mismo juego y alcanzar las más altas puntuaciones, en este sentido los usuarios agregan a personas desconocidas, los ciberdelincuentes aprovechan esto para crear perfiles falsos, los mismos que mediante bots, que son programas automatizados publican spam y enlaces maliciosos en grupos y perfiles de los contactos. "Los usuarios son más propensos a aceptar los spammers en su lista de amigos cuando están en una red social que en cualquier otro entorno online," señala el responsable de Marketing de BitDefender en España, Raúl García, "sobre todo, si necesitan un grupo muy grande para mejorar su puntuación o su situación en un juego" (40). Cuando el spam se produce en canales relacionados con estos juegos sociales, la facilidad para que un usuario acepte como amigo a un desconocido es mayor, puesto que le interesa aumentar el número de colaboradores de su equipo. Esto hace casi imposible detectar

automáticamente a los spammers, puesto que los propios usuarios tienden a darles credibilidad.

4.13 URL's Abreviadas

Hay muchos sitios que ofrecen el servicio gratuito a abreviación de URL's, esto con el objetivo de ahorrar espacio en sus publicaciones en las redes sociales, especialmente en Facebook y Twitter. La mayoría de las URL's publicadas en las redes sociales son enmascaradas con pequeñas URL's, esto favorece a los ciberdelincuentes ya que el usuario no sabe dónde irá a parar en el momento que haga clic en ellas. Estos servicios están siendo aprovechados por los ciberdelincuentes para redirecciones a los usuarios a páginas web maliciosas y que, por lo tanto, no muestran el nombre de la página a la que dirigen. Para evitar el peligro de las URL's abreviadas, existen servicios que permiten ver que webs se esconden detrás del enlace acortado, de modo que el usuario pueda saber si esta URL es maliciosa antes de dar clic sobre ella (62).

4.14 Las Redes Sociales y las Empresas

Las redes sociales aglomeran a cientos de millones de usuarios o potenciales clientes, solamente considerando los usuarios de las redes sociales analizadas en el presente estudio, es decir, de Hi5, Facebook y Sonico, la sumatoria alcanza alrededor de 515 millones de usuarios. La mayoría de las empresas tienen perfil en alguna red social, donde publican todo tipo de contenidos, de tal manera que promueven su empresa a través de sus publicaciones. Los medios de publicidad tradicionales ahora están compartiendo protagonismo con las redes sociales, hoy en día ya se habla de Marketing en las redes sociales, pero las empresas como cualquier otro usuario están propensas a ser víctima de algún ataque. La firma de seguridad computacional Check Point advierte de las fallas y virus en la web; el 80% de la fuga de datos empresariales se da por medio de negligencias ante sitios no seguros (63). Datos recientes de Manpower Professional revelan que el 75% de los empleados afirman que sus empresas no cuentan con una política formal sobre el uso de las redes sociales en el trabajo. Esto sugiere que una amplia mayoría de las empresas están adoptando la

postura de “esperar a ver qué sucede” antes de desarrollar sus propias políticas formales sobre el uso de las redes sociales (64).

Un estudio desarrollado por Deloitte revela que, El 15% de los trabajadores afirma que estaría dispuesto a comentar sus problemas laborales y sus desacuerdos con “el jefe”, en las redes sociales en las que participa. Además que, - El 49% de los trabajadores no cambiaría su conducta, ni su permanencia, y ni siquiera su frecuencia de participación en las redes sociales, por mucho que lo especifiquen las políticas o las normas de su empresa (64). Aparte de los riesgos antes mencionado, las empresas deben considerar los riesgos potenciales que se detallan a continuación:

Deterioro de la Imagen Corporativa	Las empresas pueden manejar adecuadamente su perfil empresarial, pero el deterioro de la imagen corporativa se da principalmente por las actividades publicaciones y contenidos de los empleados en las redes sociales y aun mas grave cuando los empleados publican información sensible o confidencial relacionado a las labores desarrolladas en la empresa. Sitios como Facebook tienen campos opcionales para especificar el nombre de la empresa donde trabaja, el cargo que ocupa, entre otras, que permiten determinar la situación laboral del usuario. Según un estudio desarrollado por Sophos denominado Security Reporte 2010, revela que el 72% de los encuestados afirma sentirse preocupados ante el comportamiento que sus empleados puedan adaptar en las redes sociales. Este mismo informe señala que el 49% de las empresas permite a todos sus empleados un acceso sin restricciones a Facebook, lo que supone un aumento de más del 13% con respecto al año anterior (36). Por otro lado, en una encuesta relazada a 1400

	empresas con más de 100 empleados de los Estados Unidos, revela que el 54% de las empresas a prohibido totalmente la utilización de redes sociales, y que el 19% las utiliza con fines comerciales (66).
Pérdida de Productividad	Los empleados suelen pasar gran cantidad de tiempo conectado a su red social, realizando labores propias de la red social y que en muchas de las veces no tienen nada que ver con sus labores. En el Reino Unido se estima que la pérdida de productividad debida al uso de portales de redes sociales como Facebook durante la jornada laboral, cuesta a las empresas más de 8.000 M€ (66).
Consumo de ancho de banda	El ancho de banda en las empresas puede ser consumido por publicaciones de contenidos y utilización de aplicaciones en redes sociales, que, por lo general no están relacionadas con las actividades laborales, lo más preocupante de esto es que las comunicaciones críticas de la empresa pueden salir afectadas. En el Reino Unido se estima que el 20% del ancho d banda de la red se consume por la utilización de redes sociales (66).

Tabla 5. Riesgos de Redes Sociales en Empresas (creación propia)

4.15 Los Menores en las Redes Sociales

Según el estudio “Seguridad infantil y costumbres de los menores en Internet”, realizado por Acción Contra la Pornografía Infantil (ACPI) y la Asociación Protégeles,

el 54,5 por ciento de los menores no ha recibido información alguna sobre las normas básicas de seguridad a la hora de utilizar Internet. Éste desconocimiento se traduce en situaciones preocupantes: el 30% de los encuestados que utiliza Internet ha facilitado su número de teléfono en alguna ocasión; un 16 %, su dirección, y un 15 % ha concertado una cita con un desconocido a través de la Red (67).

4.16 Delincuencia Tradicional y las Redes Sociales

Muchos de los usuarios de redes sociales publican mensajes donde relatan todas las actividades realizadas y a realizar durante el día; esto toma mayor importancia ahora que las redes sociales son accesibles desde teléfonos celulares y los usuarios no necesariamente están sentados frente a computador, sino que realizan sus publicaciones desde cualquier lugar y en cualquier momento, esto facilita el trabajo de los delincuentes. Ya que estas publicaciones pueden contener información útil para la delincuencia tradicional. Algunos usuarios con el afán de compartir su vida con sus "Amigos" publican acerca de sus bienes muebles o inmuebles y confirman estas aseveraciones con fotos, direcciones e información sensible en general.

5. ANÁLISIS DE PRIVACIDAD DE REDES SOCIALES EN LOJA

La privacidad que brindan las redes sociales no proporciona total seguridad para información de los usuarios, como se vio en capítulos anteriores, los ciberdelincuentes hacen uso de avanzadas técnica de hacking con la finalidad de acceder a la información sensible de los usuarios. Pero los propios usuarios son los que se encargan de facilitarles el trabajo a los ciberdelincuentes, a través de sus publicaciones y por el descuido en las configuraciones de privacidad. Por ello, es imprescindible analizar todos los aspectos relacionados con la privacidad, es decir, la exposición de la información y parámetros configurables, de tal manera que se pueda evaluar el nivel de conocimiento y de protección de la información personal de los usuarios de redes sociales en la Ciudad de Loja.

5.1 Problemática

De acuerdo con la investigación desarrollada, no se han identificado estudios a nivel local y nacional que permitan identificar nivel de exposición e incidencia en la privacidad de la información personal de los usuarios de redes sociales.

5.2 Universo

El Universo tomado para la presente encuesta corresponde al número total de personas que en la encuesta sobre la incidencia en nuestro entorno, afirmaron usar Redes Sociales. Es decir, que el Universo para esta encuesta corresponde 441 personas de ambos sexos de entornos educativos secundarios y universitarios.

5.3 Muestra

Para determinar la muestra se aplico la formula $n = P/\left(1+\left(e^2 xP\right)\right)$, siendo la más adecuada para los casos de poblaciones grandes. En la encuesta aplicada se estableció un porcentaje de 4% (0.04) de error de muestreo debido a que por ser la población grande se necesita un nivel de significancia menos, obteniendo una muestra que nos de seguridad en los resultados.

$n = P/(1+(e^2 * P))$ Donde:

n = tamaño de la muestra ?

P = población 441

e = nivel de error 0.04%

$N = 441/(1+(0{,}04^2 * 441))$

$N = 441/(1+(0.7056))$

$N = 441/(1.7056)$

$N = 258$

5.4 Aplicación de Encuesta

Para realizar un análisis comparativo de los datos obtenidos en los Entornos Educativos Secundarios (en adelante EES) y Entornos Educativos Universitarios (en adelante EEU), se aplicó el mismo número de encuestas en ambos entornos, es decir, en la Universidad Técnica Particular de Loja y Universidad Internacional Sede Loja (EEU) y Instituto Técnico Superior "Daniel Álvarez Burneo" y el Colegio "Juan Montalvo" (EES)

5.5 Tabulación de Resultados

- **Exposición de la Información**

En EEU 89,53% de los encuestados aseguran que la información publicada en su Red Social es real, esta información corresponde a nombres, apellidos, dirección de correo electrónico, número de celular, fotos propias y fotos de terceros, ciudad de origen, ubicación actual, nombre de universidad, nombre del trabajo y cargo.

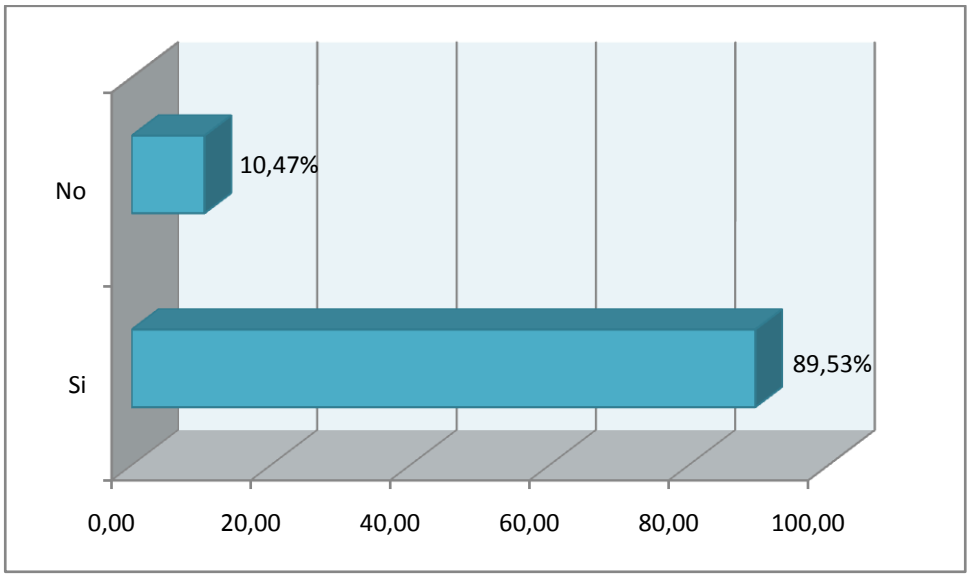

Figura 33. Información real publicada en redes Sociales en EEU

Por su parte en EES el 90,70% de los encuestados aseguran publicar información real en su red social.

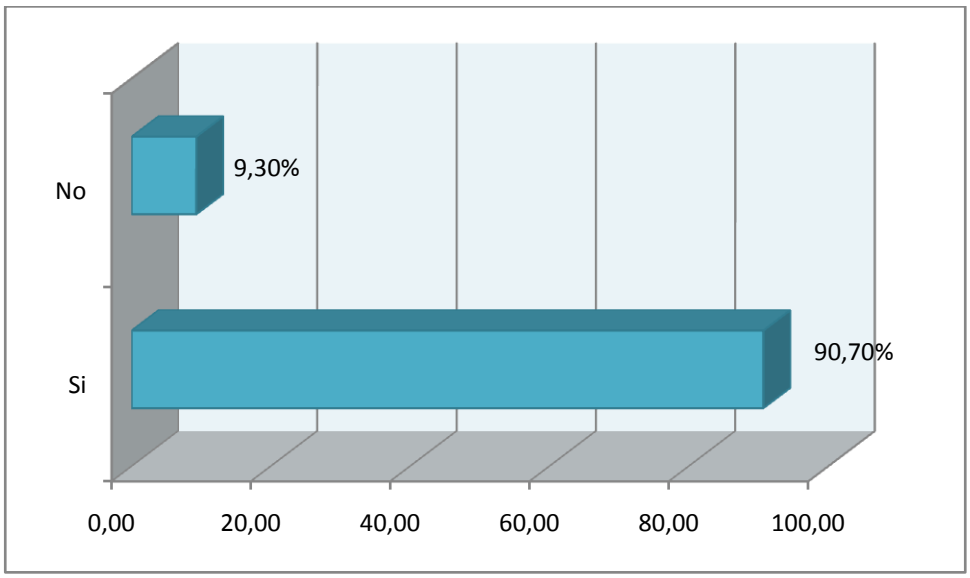

Figura 34. Información real publicada en Redes Sociales en EES

Las redes sociales permiten publicar todo tipo de información personal, como se observa en la Figura 31, en EEU, se ha determinado que el 99,61% y el 87,21% han publicado su nombre y apellido respectivamente, otros datos sensibles como lugar de trabajo 22,48%, cargo 18,22%, ubicación actual 41,86% y número de celular 15,12%

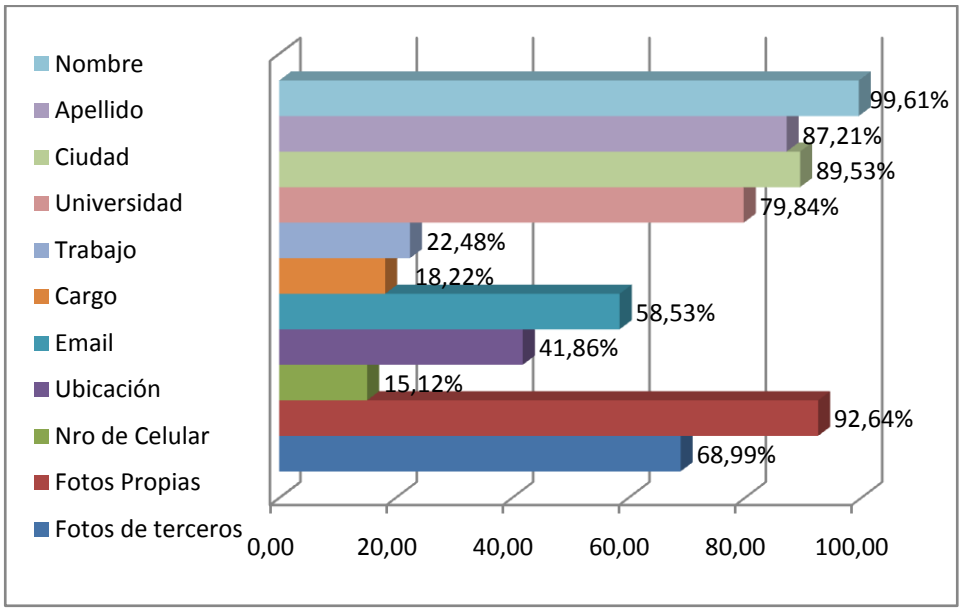

Figura 35. Información del Perfil de Usuario en EEU

En cambio, en EES, el 100 % han publicado su nombre, el 61,63% han publicado apellido, otros datos como email 38,76%, ubicación actual 62,02% y número de celular 39,15%.

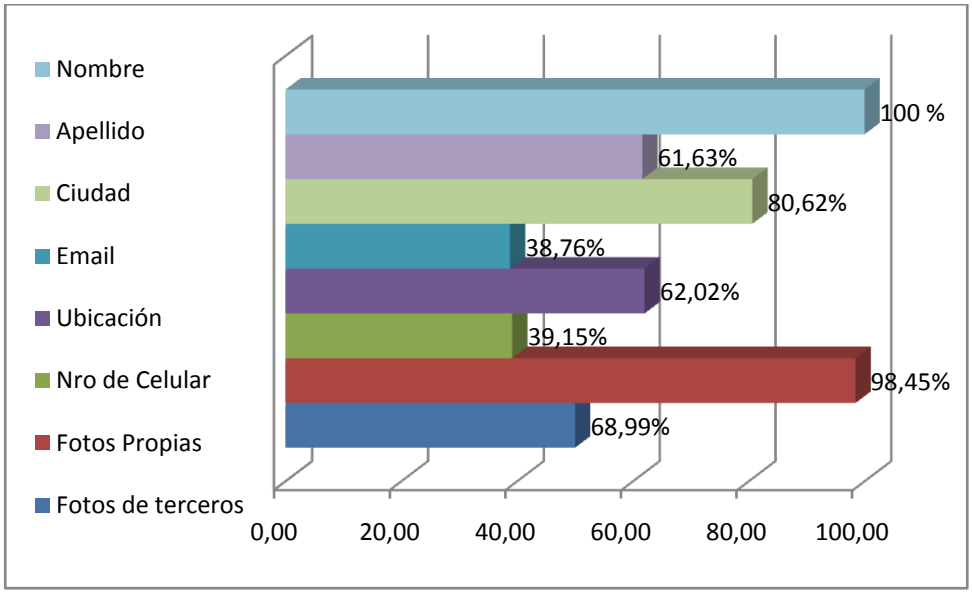

Figura 36. Información de Perfil de Usuario en EES

❖ **Privacidad que brindan las Redes Sociales**

En EEU el 59,30% de los usuarios teme por la seguridad de sus datos en la red social

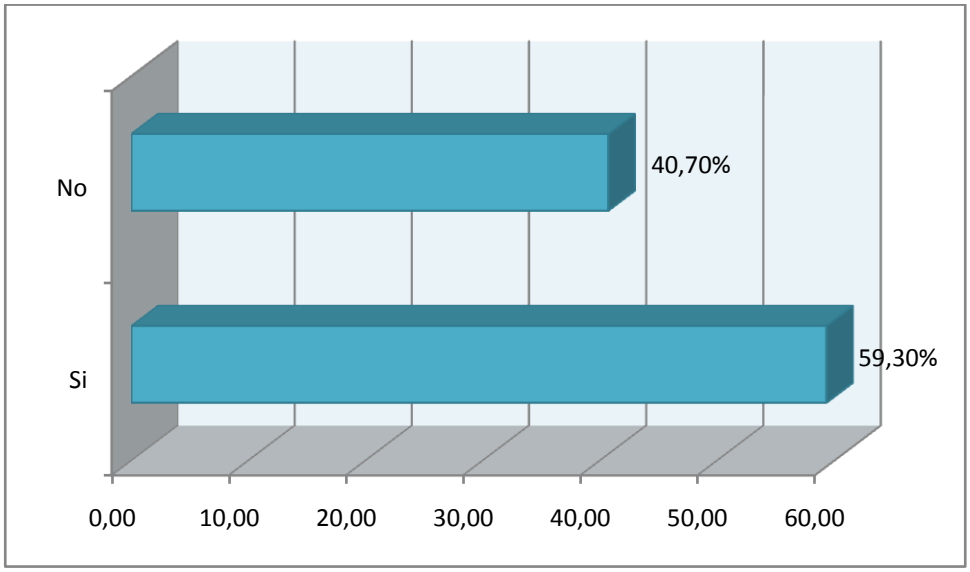

Figura 37. Seguridad de la Información personal en EEU

En cambio, en EES solamente el 26,74% de los usuarios teme por seguridad de sus datos en la red social, es decir que el 73,26% restante, no les preocupa la seguridad de su información y se exponen de tal manera que están propensos a sufrir algún ataque.

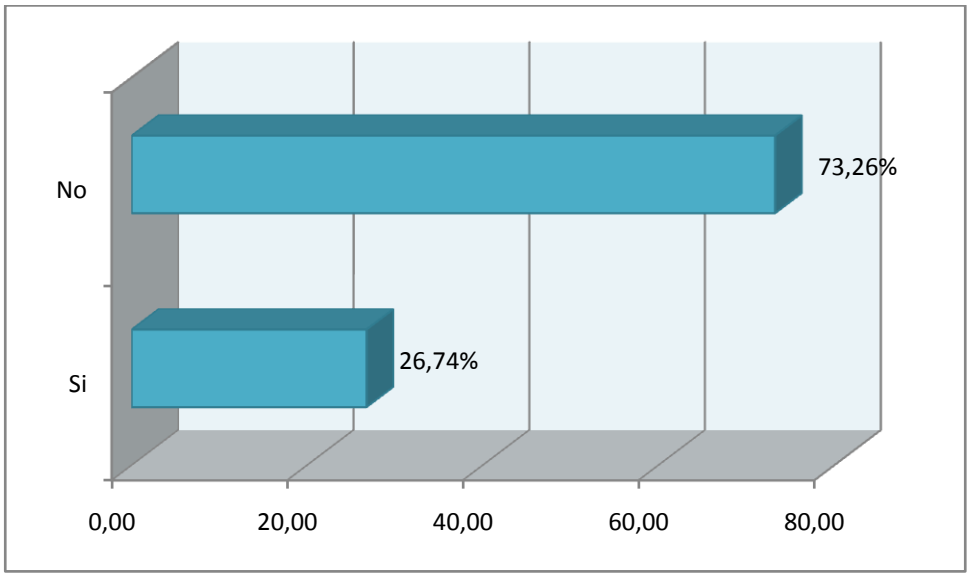

Figura 38. Seguridad de la Información personal en EES

Al ser preguntados si confían en la seguridad que brindan las redes sociales, el 44,96% (en EEU) confía en la redes sociales, mientras que la confianza es mayor en EES llegando al 67,44%

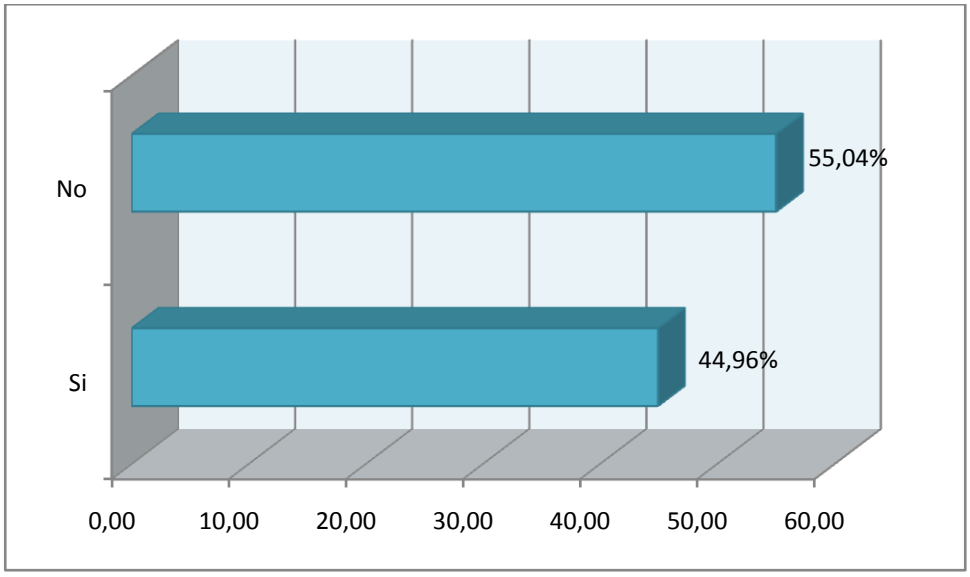

Figura 39. Confianza en la seguridad que brindan las Redes Sociales en EEU

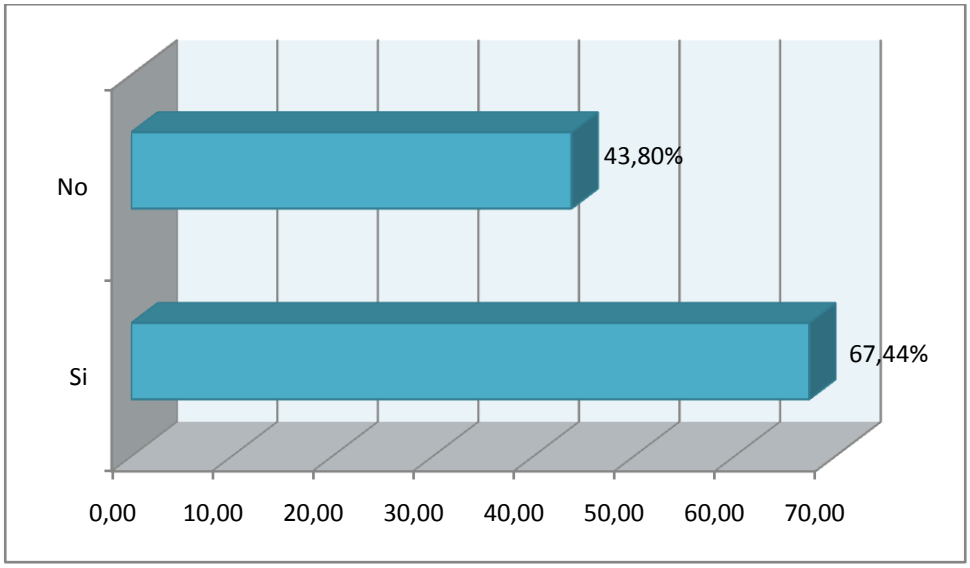

Figura 40. Confianza en la seguridad que brindan las Redes Sociales en EES

De acuerdo con la investigación desarrollada en capítulos anteriores, se ha determinado que la exposición de la información personal puede poner en riegos su integridad física. En el presente estudio, al ser preguntados si están consientes de aquello, el 67,83% en EEU y 16,67% en EES afirmaron ser consientes de los riesgos que conlleva la exposición de la información.

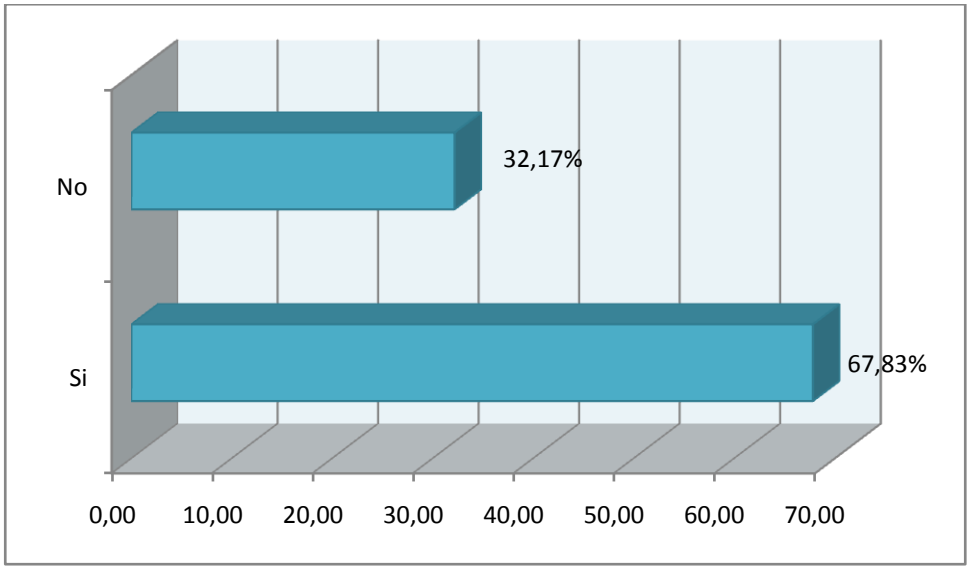

Figura 41. Riesgos de publicar la información personal en EEU

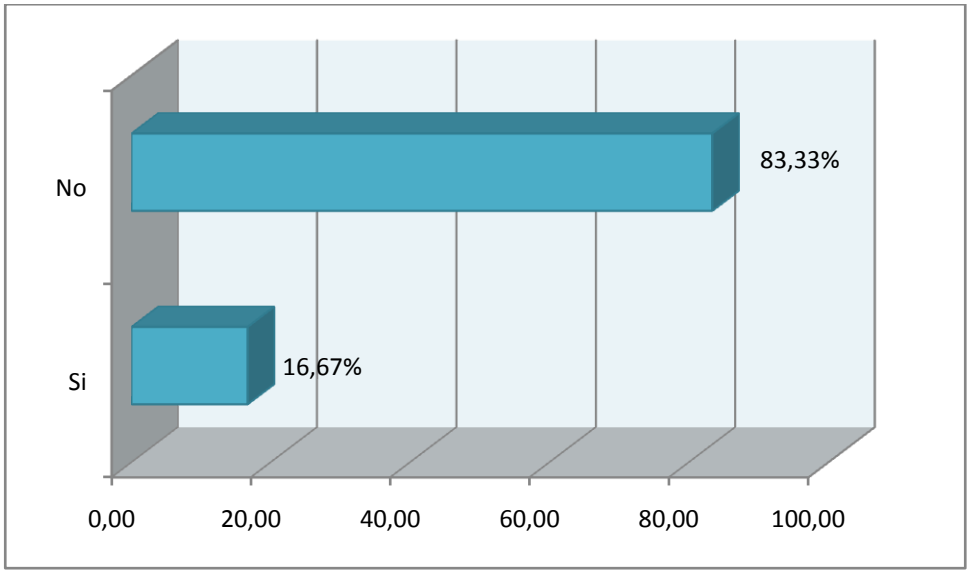

Figura 42. Riesgos de publicar la información personal en EES

Redes sociales como Facebook permiten que terceros desarrollen aplicaciones para ser usadas por sus usuarios, los desarrolladores a cambio reciben toda la información personal de los usuarios que han accedido a la aplicación, en el presente estudio, el 32,17% de los encuestados en EEU y el 56,59% en EES usan frecuentemente aplicaciones en sus redes sociales, al ser preguntados si están consientes que al usar dichas aplicaciones permiten traspaso de su información

personal, el 39,92% en EEU y el 12,79% en EES afirman ser consciente de aquello, como se muestra en las Figuras 45 y 46.

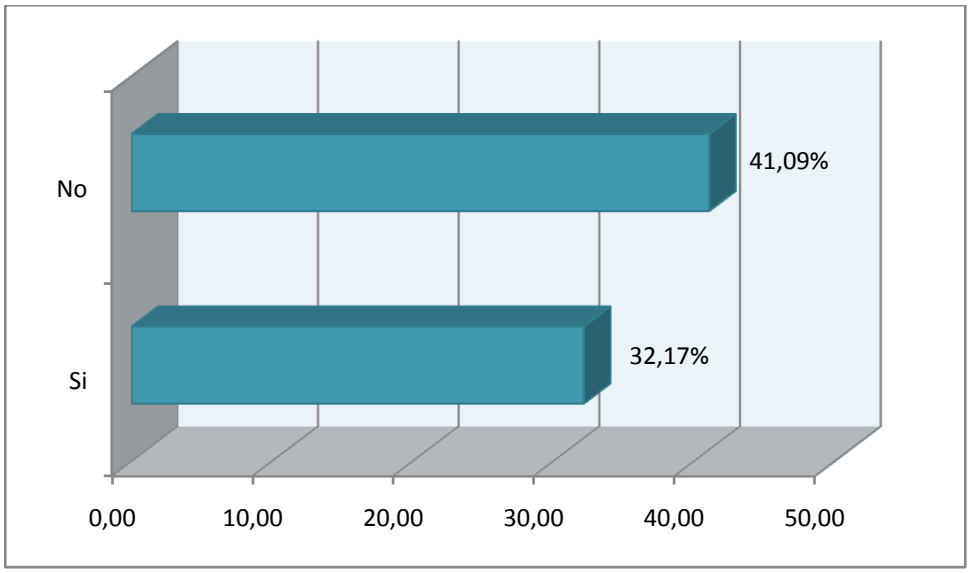

Figura 43. Utilización de Aplicaciones en EEU

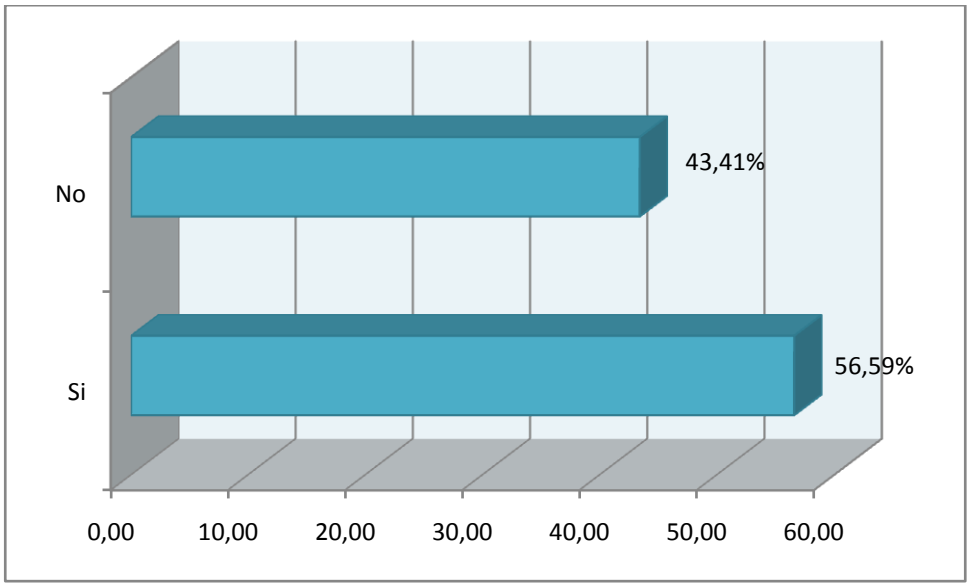

Figura 44. Utilización de aplicaciones en EES

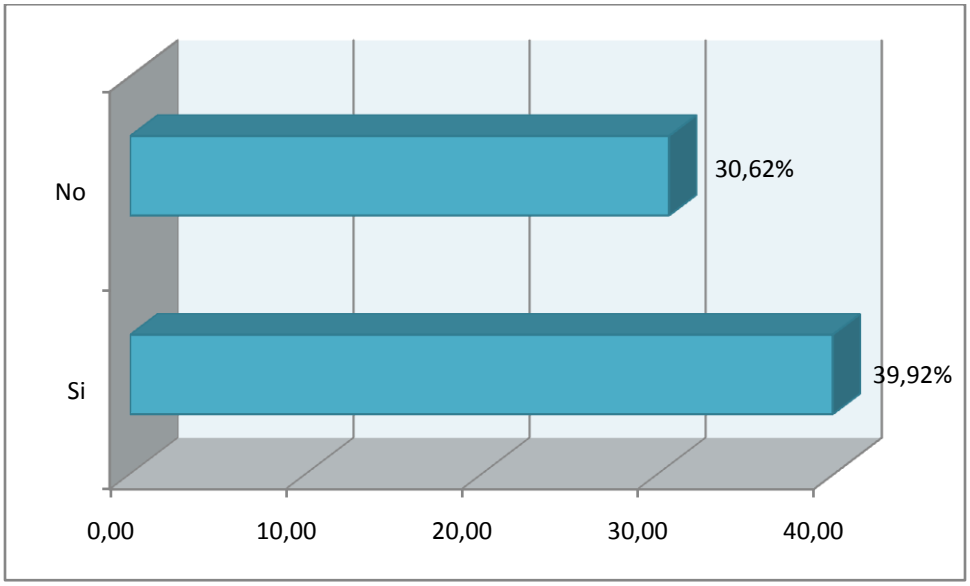

Figura 45. Conocimiento del riesgo que implica la utilización de aplicaciones en EEU

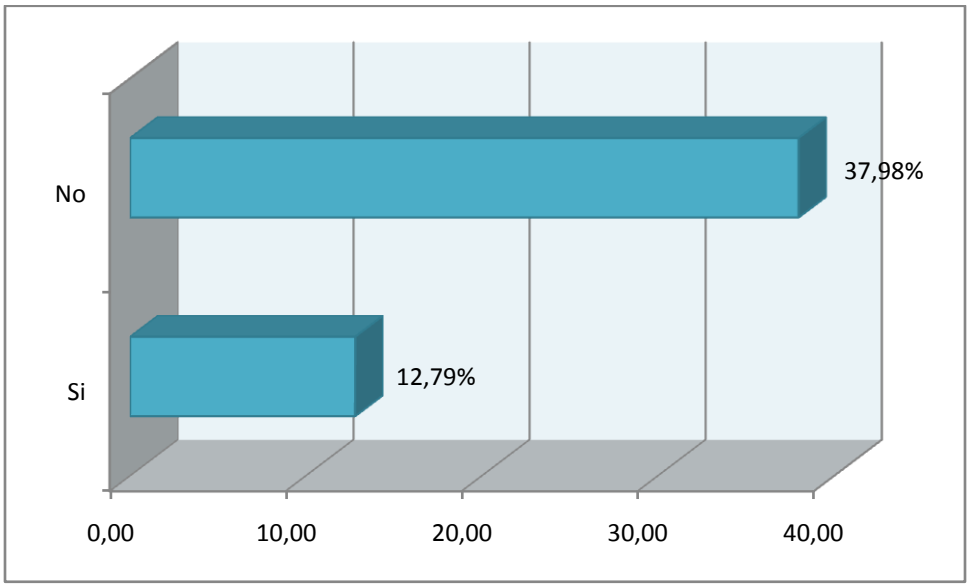

Figura 46. Conocimiento del riesgo que implica la utilización de aplicaciones en EES

Las redes sociales están siendo usadas para agredir verbalmente a los usuarios, en el presente estudio, el 8,53% de los encuestados en EEU y el 12,02% de los encuestados en EES afirman haber sido amenazado o insultados a través de su red social.

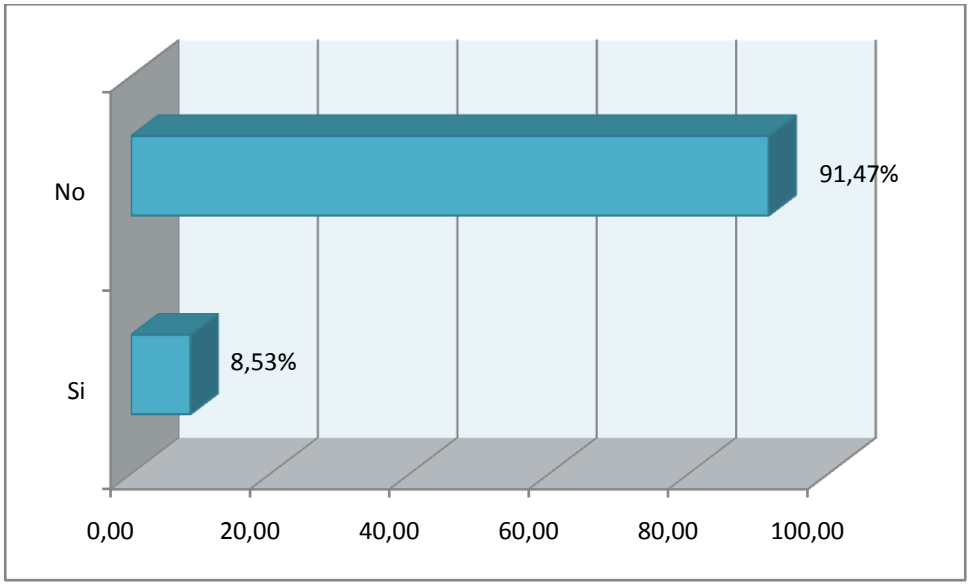

Figura 47. Agresión a través de Redes Sociales en EEU

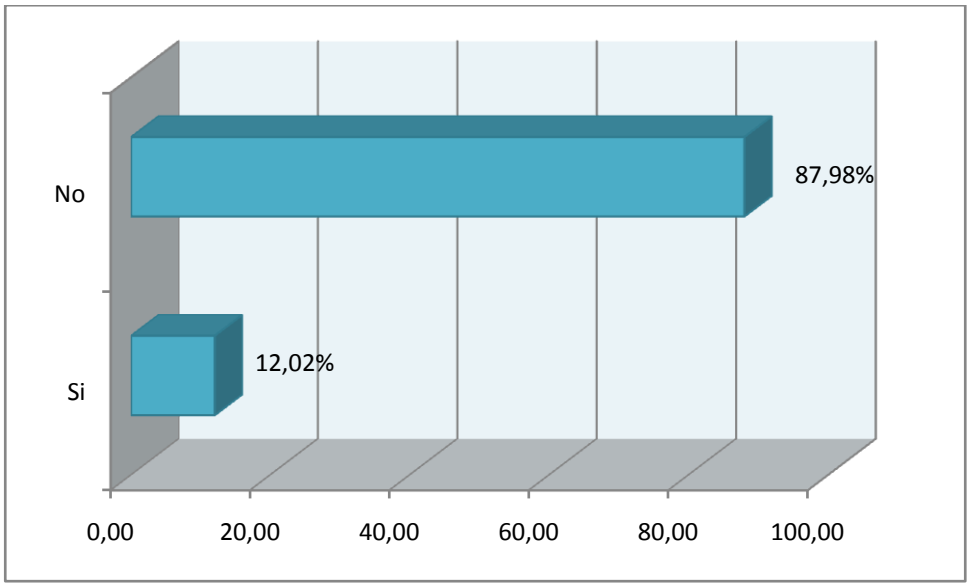

Figura 48. Agresión a través de Redes Sociales en EES

- **Seguridad de la Contraseña de Usuario**

Al hablar de la seguridad de redes sociales, es inevitable analizar la seguridad que brinda la contraseña de usuario, en la actualidad existen programas dedicados a descifrar contraseñas, además, estas pueden ser deducidas a través de la información publicada por los mismos usuarios en su red social, en el presente

estudio, tomando como referencia que una contraseña segura es aquella que tiene mínimo 8 caracteres mayúsculas, minúsculas e incluye números y símbolos, la pregunta formulada a los encuestados es que si consideran que su contraseña es segura, donde, el 73,26% en EEU y el considera que su contraseña es segura, estos datos contrastan con los obtenidos en EES donde solo el 23,64% de los encuestados afirman que se contraseña es segura.

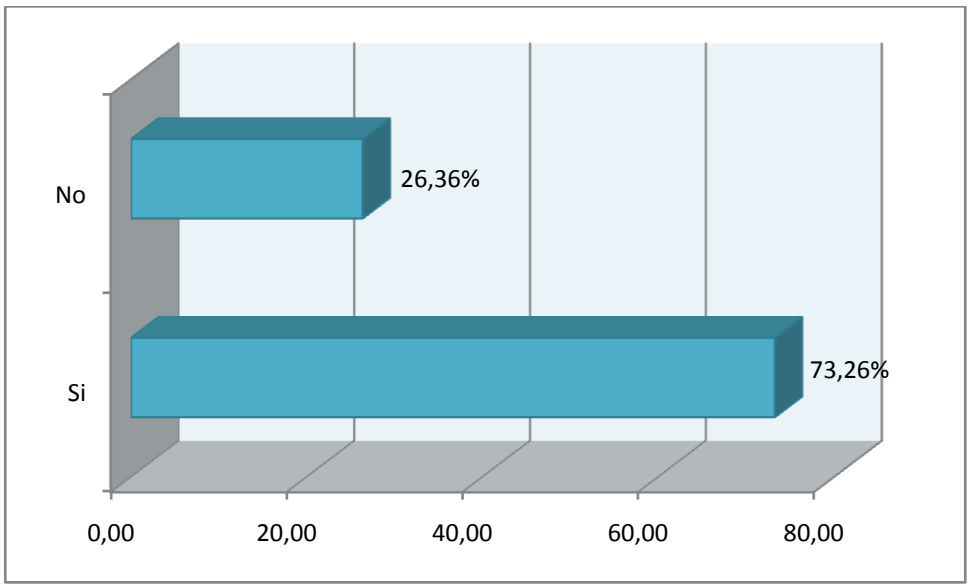

Figura 49. Seguridad de Contraseñas en EEU

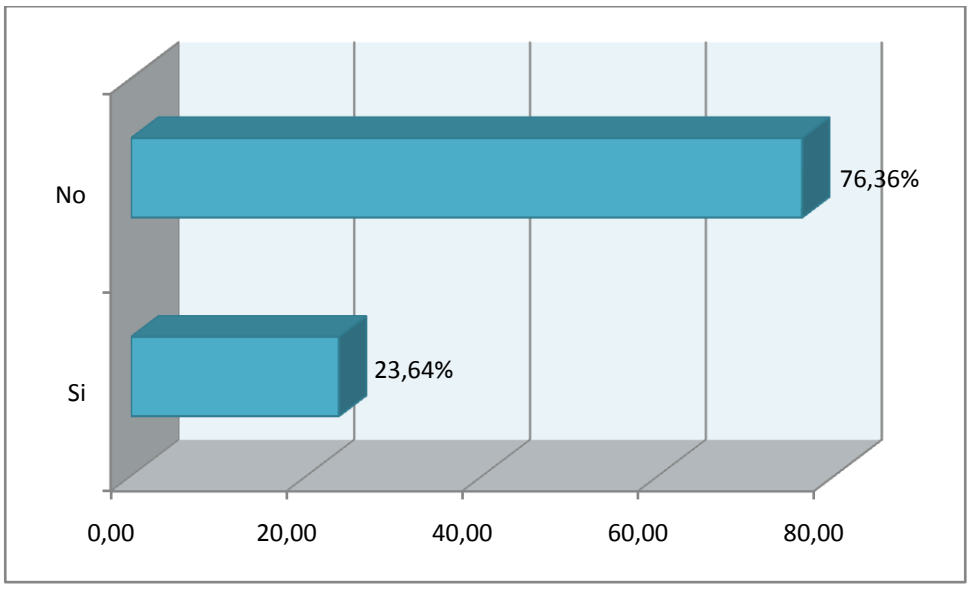

Figura 50. Seguridad de Contraseñas en EES

Otro aspecto considerado en la encuesta, es la frecuencia con que los usuarios cambian su contraseña, donde, el 41,47% (en EEU) y el 84,95% (en EES) aseguran que nunca ha cambiado su contraseña, el 25,19% (en EEU) y el 11,24% (en EES) la cambia anualmente y el restante 33,33% (en EEU) y el 5,81% (en EES) semestralmente.

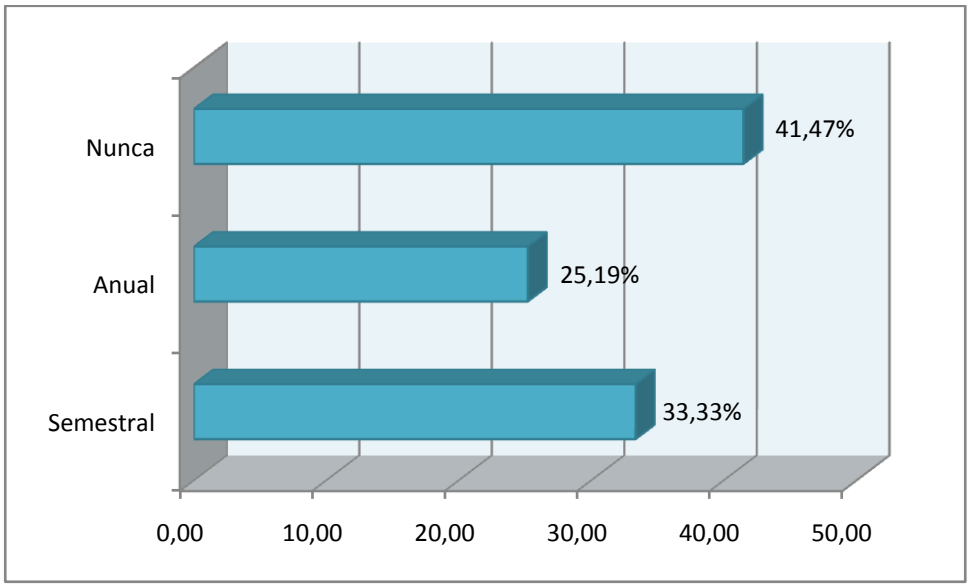

Figura 51. Frecuencia de cambio de contraseña en EEU

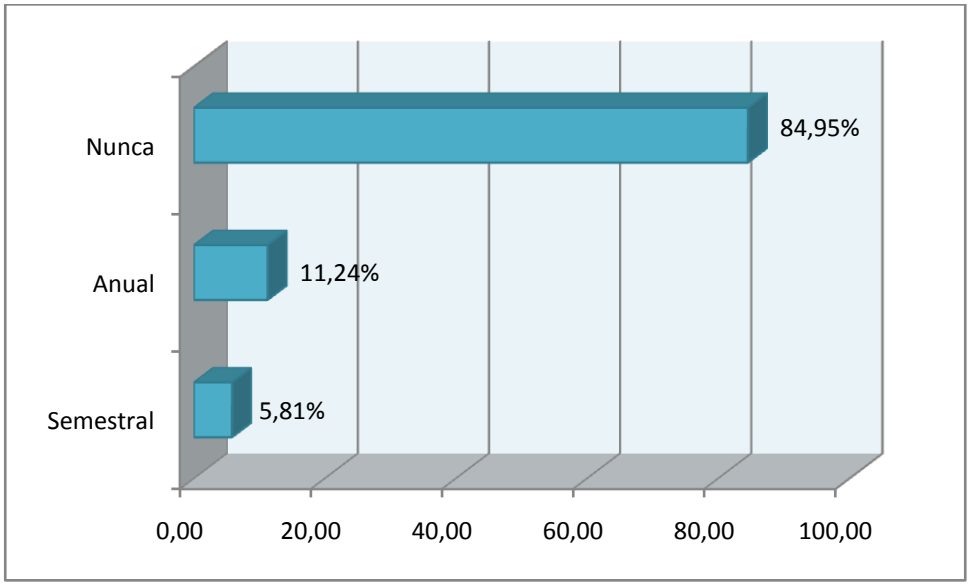

Figura 52. Frecuencia de cambio de contraseña en EES

❖ **Configuraciones de Privacidad**

La exposición de la información se da principalmente por el descuido en la configuración de privacidad del perfil, en el presente estudio, se ha determinado que el 75,58% de los encuestados en EEU aseguran haber configurado la privacidad de su perfil, en cambio en EES solamente el 36,82% de los encuestados asegura haber configurado su privacidad.

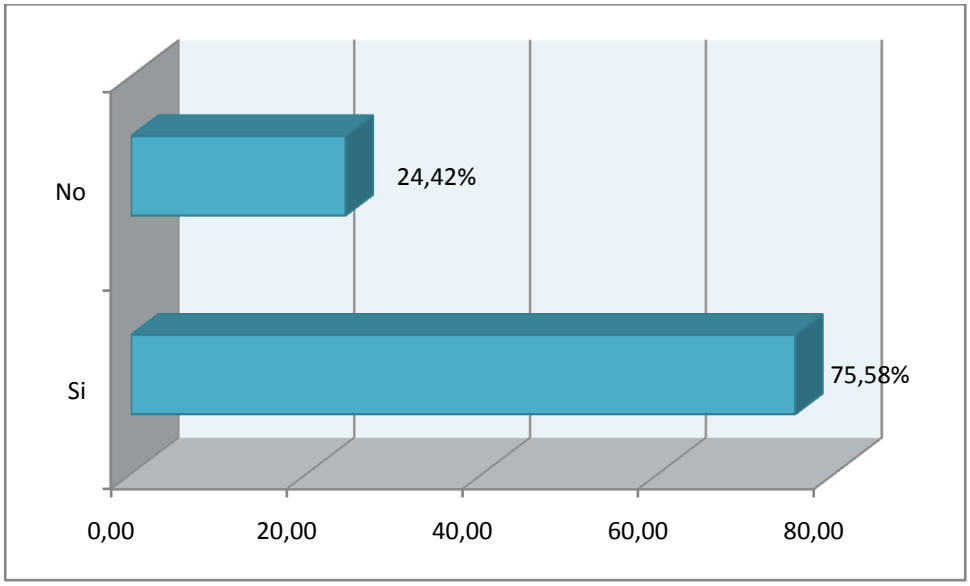

Figura 53. Configuración de privacidad en EEU

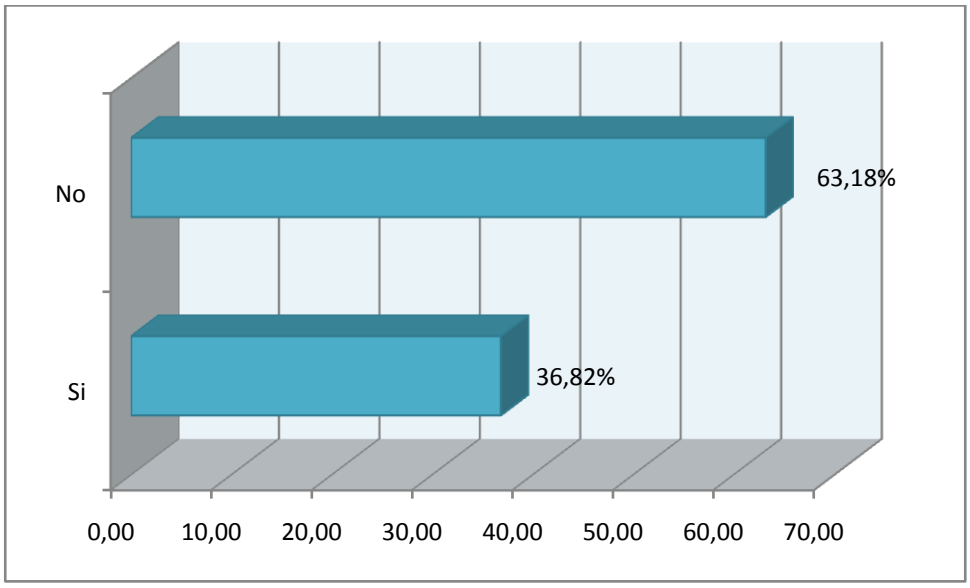

Figura 54. Configuración de privacidad en EES

La configuración de privacidad en las diferentes redes sociales varía dependiendo del enfoque que cada una de ellas tiene sobre la privacidad, pero hay parámetros comunes entre las configuraciones de las redes sociales analizadas en el presente estudio.

El aspecto más relevante de la configuración de la privacidad es la restricción del acceso al perfil de usuario, los niveles de confianza establecidos para el presente estudio son: solo amigos, algunos amigos y todos los usuarios.

En EEU el 61,35% de los encuestados, asegura haber configurado la privacidad, de tal manera, que solo sus amigos puedan ver su perfil, el 14,98% permite que solo alguno de sus amigos accedan a su perfil y solo el 23,67% han dejado las configuraciones por defecto de privacidad.

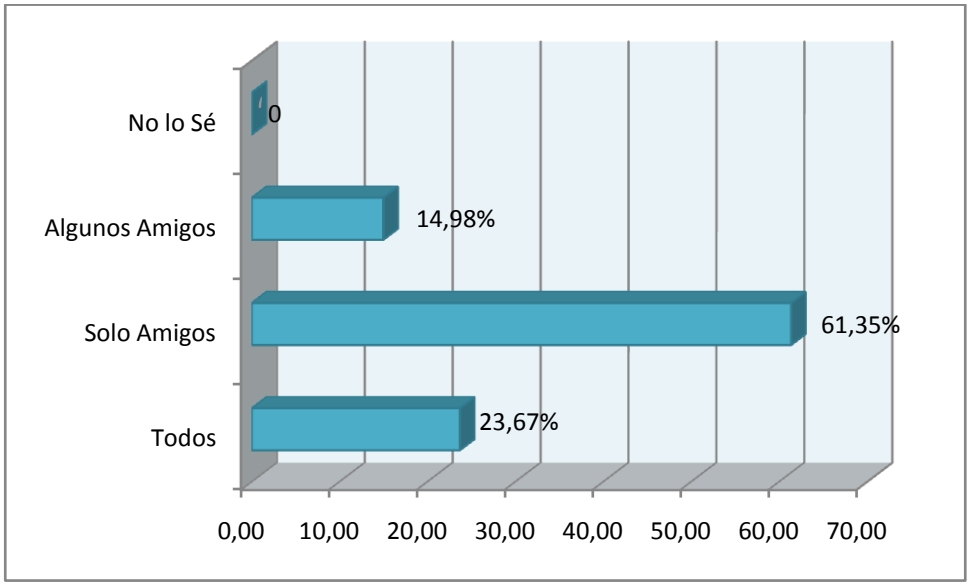

Figura 55. Restricciones en la privacidad de perfil en EEU

En cambio, en EES el 23,16% de los encuestados, asegura haber configurado la privacidad, de tal manera, que solo sus amigos puedan ver su perfil, el 7,37% permite que algunos de sus amigos accedan a su perfil y el 69,47% han dejado las configuraciones por defecto de privacidad.

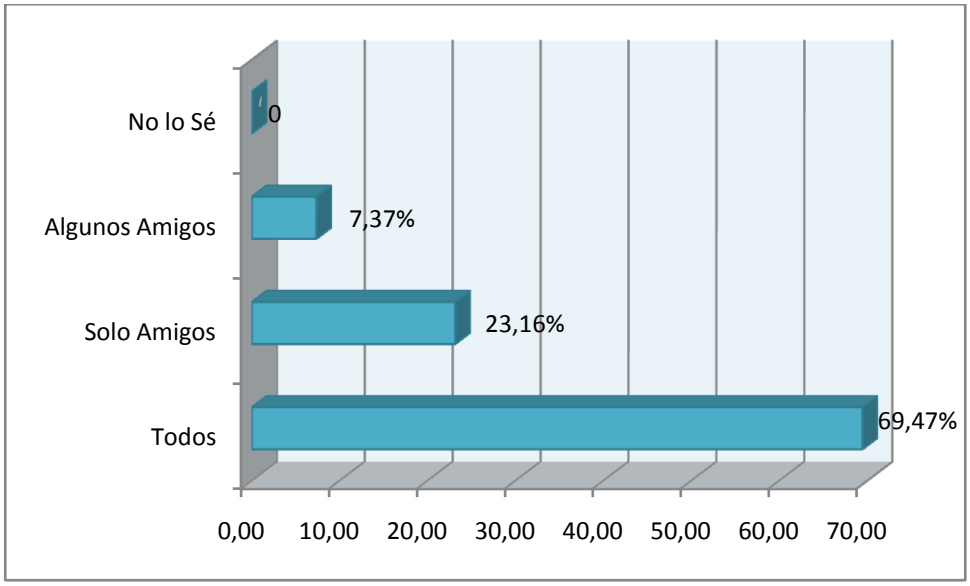

Figura 56. Restricciones en la privacidad del perfil en EES

Las redes sociales, permiten que los usuarios bloqueen a otros usuarios para que no puedan tener acceso a su información, esto principalmente porque ciertos usuarios pueden representar peligro. En el presente estudio, el 50,39% (En EEU) y el 51,16% (En EES) aseguran haber bloqueado algún usuario.

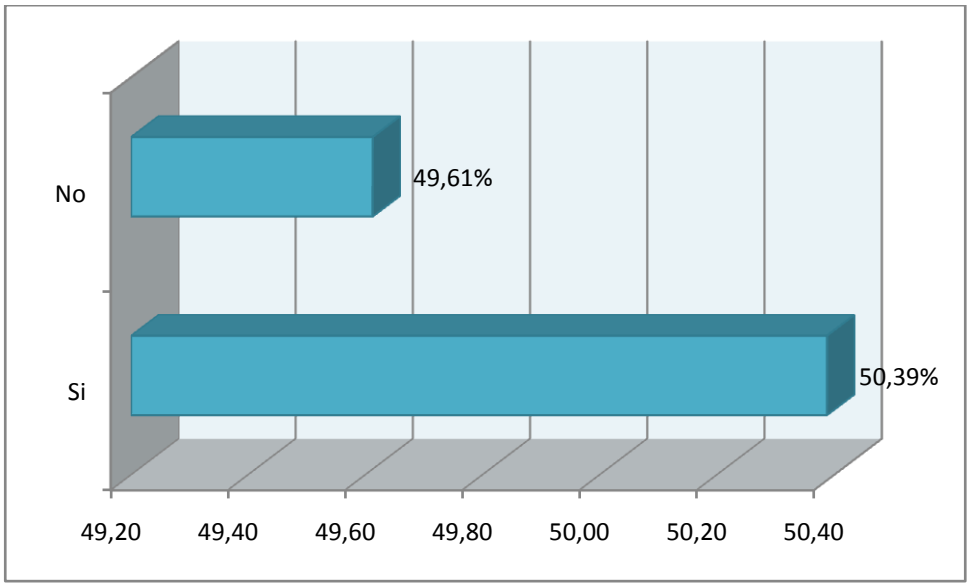

Figura 57. Bloqueo de usuario en EEU

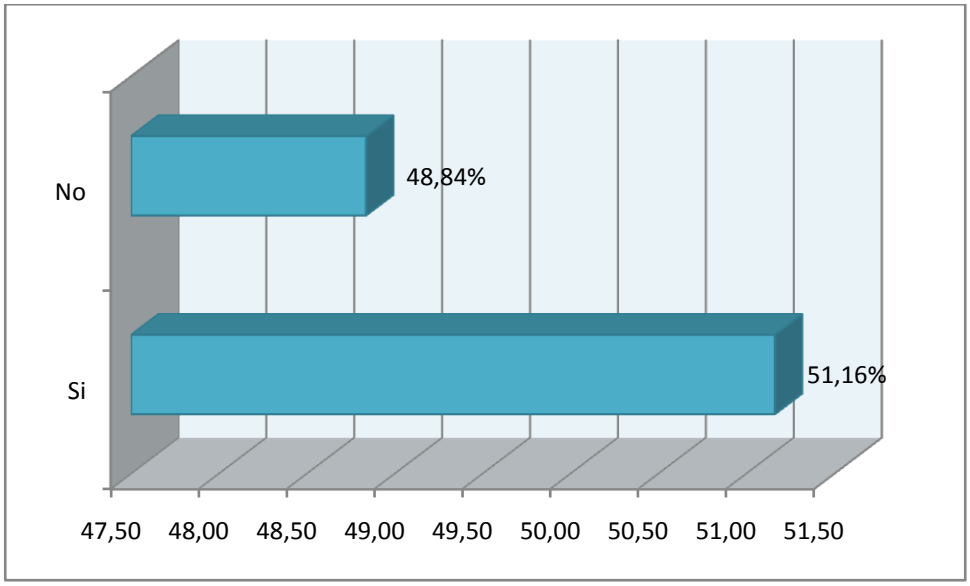

Figura 58. Bloqueo de usuarios en EES

- **Usabilidad**

De lo investigado en capítulos anteriores, los usuarios principalmente emplean las redes sociales para hacer amigos, esto implica la admisión de desconocidos, en el presente estudio, se ha determinado que el porcentaje de usuarios que admiten desconocidos en su red social es de 48,06% en EEU, estos datos contrastan con los obtenidos en EES, donde la cifra llega a 72,48%.

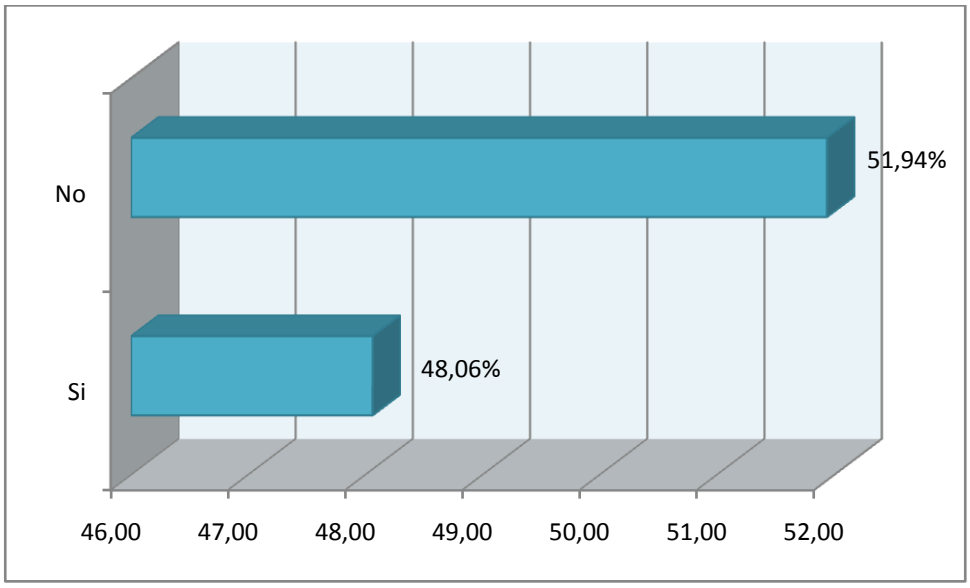

Figura 59. Admisión de desconocidos en EEU

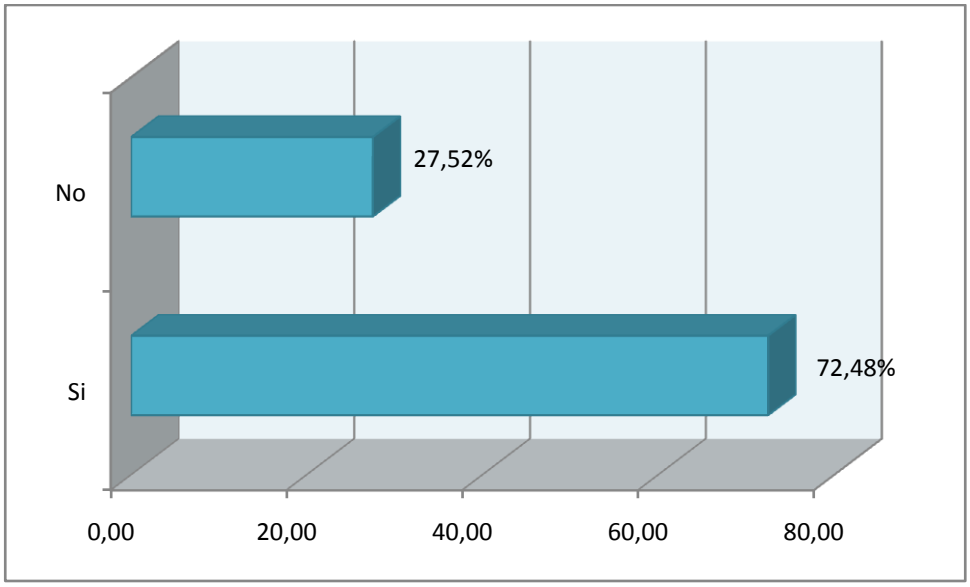

Figura 60. Admisión de desconocidos en EES

Muchos de los usuarios ponen en riesgos su integridad al encontrase con personas que han conocido en a través de las redes sociales, en EEU el 7,75 % de los usuarios se han citados con desconocidos, mientras que en EES la cifra alcanza el 28,29%.

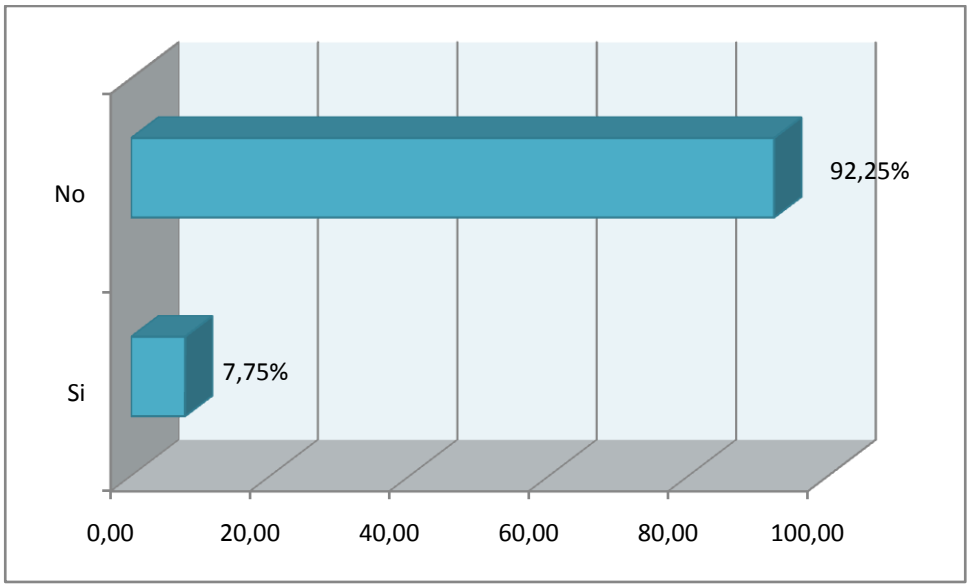

Figura 61. Dating en EEU

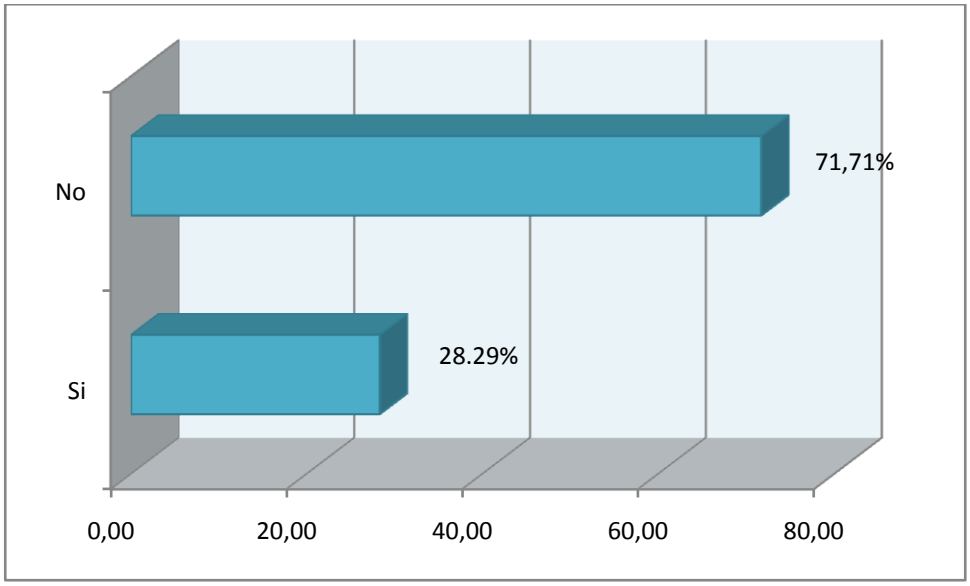

Figura 62. Dating en EES

Por otro lado, el 27,52% (en EEU) y el 46,12% (en EES) aseguran haber encontrado fotos suyas publicados por terceros y sin su permiso.

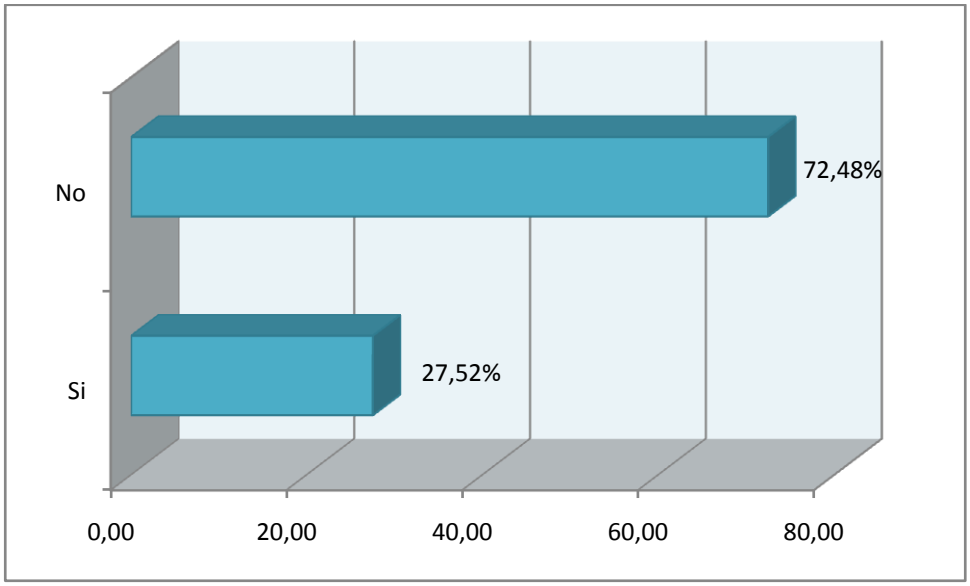

Figura 63. Fotos publicados por terceros en EEU

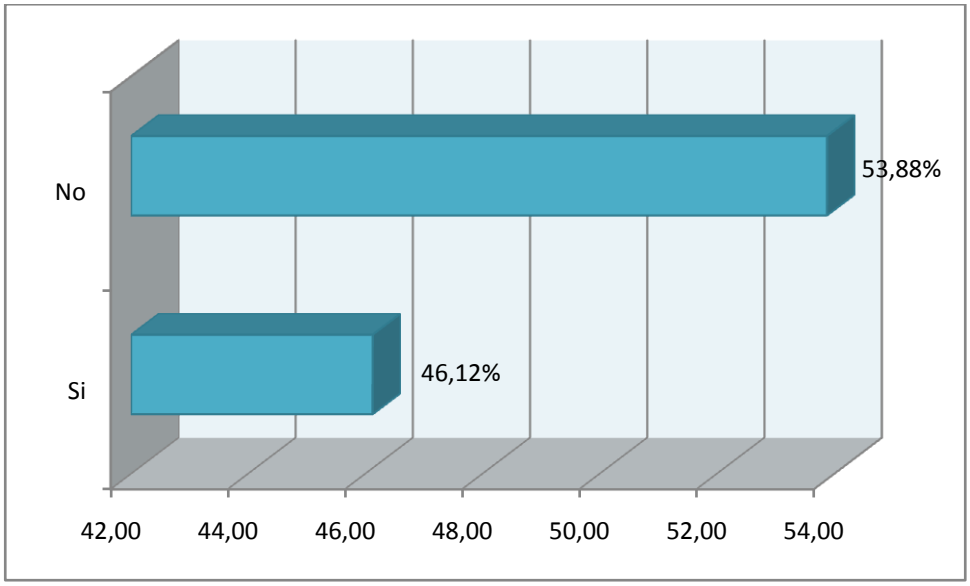

Figura 64. Fotos publicadas por terceros en EES

Finalmente la opinión de los encuestados en EEU relacionada a la seguridad de su información personal es: el 3,09% no le interesa la seguridad de su información, el 72,48% de los encuestados analiza la información (datos, fotos, contenidos, etc.) que sube a su red social y el 25,48% asegura sentirse preocupado por la seguridad de su información. Por su parte en los EES, el 37,45% no le interesa, el 32,17% de los encuestados analiza la información que sube a su red social, y el 30,12% asegura sentirse preocupado por la seguridad de la información

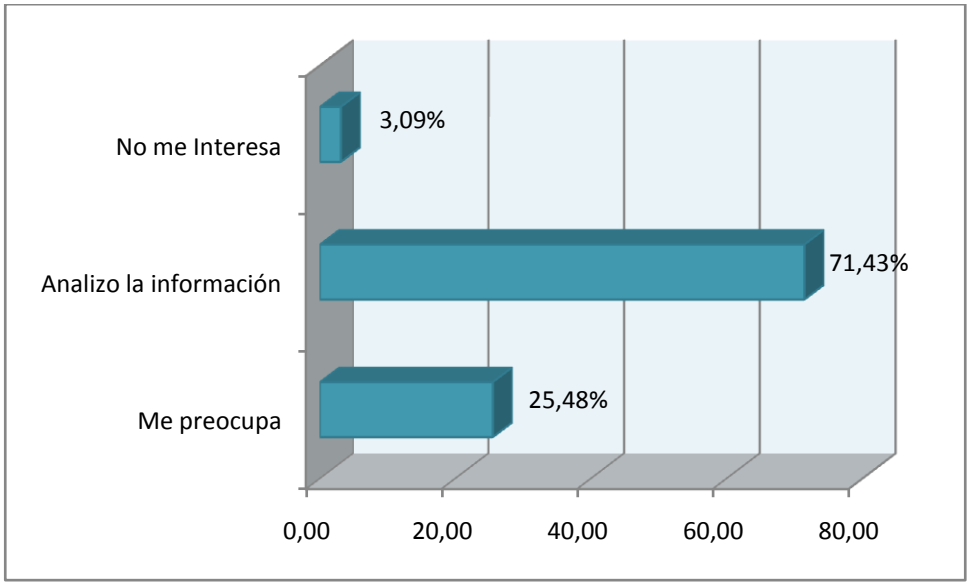

Figura 65. Opinión del usuario sobre la seguridad de la Información en EEU

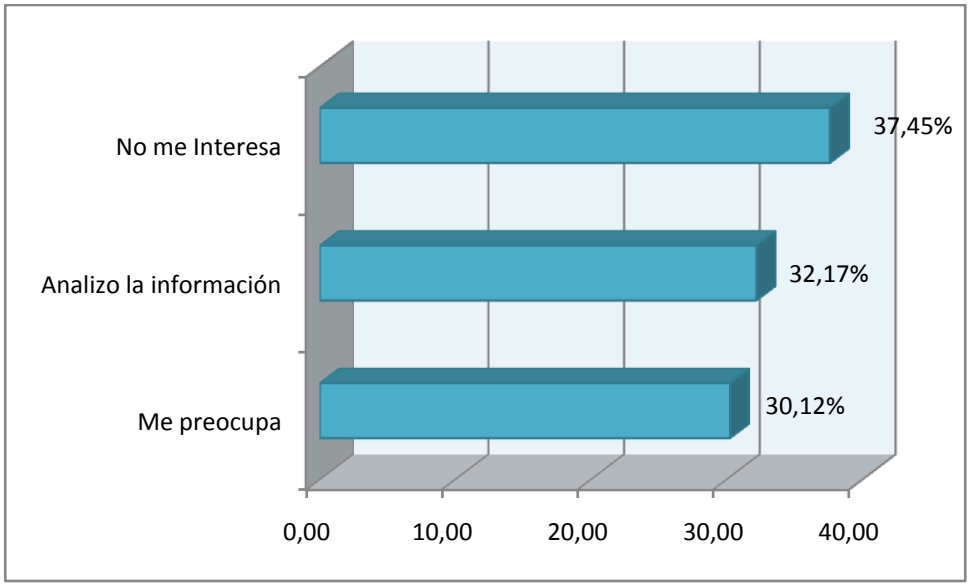

Figura 66. Opinión del usuario sobre la seguridad de la información en EES

5.6 Análisis de Resultados

Un vez que se desarrollado la tabulación de los datos se observan grandes diferencias entre los grupos definidos para la presente investigación. Las estadísticas generadas en Entornos Educativos Universitarios (EEU), reflejan mayor nivel de conocimiento y precaución con la seguridad de información personal, a diferencia de las estadísticas generadas en Entornos Educativos Secundarios (EES) donde se puede apreciar cierta despreocupación por la seguridad de su información y los riesgos que trae consigo la exposición de la información personal, los aspectos más relevantes se detallan a continuación:

- Los usuarios de las redes sociales tanto de EES y EEU están exponiendo su información personal en las redes sociales, ya que el 90,70% (en EES) aseguran que los datos publicados son reales, esto, frente a 89,53% (en EEU). Además, el 59,60% de los usuarios en EEU están consientes de los riesgos y temen por la seguridad de su información, mientras que en EES solamente el 26,74% teme por la seguridad de su información. Sin embargo, el 44,96% en EEU confían en la

seguridad que proporcionan las redes sociales, frente al 67,44% de los usuarios en EES.

- La falta de información en los EES sobre la seguridad de los datos e importancia de mantener una contraseña segura, ha determinado que el 76,36% de los encuestados mantengan contraseñas débiles, mientras que en EEU solamente el 26,36% consideran que su contraseña no es segura. Otro aspecto importante es la frecuencia de cambio de contraseña, donde el 41,47% de los encuestados en EEU aseguran que nunca han cambiado su contraseña y en EES la cifra llega al 84,95%

- En cuanto a la configuración de privacidad en EEU el 75,58% ha configurado la privacidad pero en EES solo el 36,82%. Tomando como referencia solo a los usuarios que han configurado la privacidad. En EEU 23,67% ha dejado las configuraciones por defecto y el 61,35% permite que solo sus amigos accedan a su perfil. En cambio en EES 7,37% han dejado las configuraciones por defecto y el 23,16% permite que solo sus amigos puedan acceder a su perfil. Hay que destacar que estas configuraciones solo hacen referencia a la visibilidad del perfil.

- Finalmente, En EEU el 71,34% analiza la información que sube a la red y solo al 3,09% no le interesan, en cambio en EES el 32,07% analiza la información que sube y la mayor parte es decir el 37,45% no le interesa la seguridad de su información.

5.7 Correlación de Datos

Para la correlación de los datos obtenidos en la encuesta de privacidad de Redes Sociales se han analizado las variables:

- ¿Publica datos reales en Redes Sociales?
- ¿Acepta invitaciones de amistad de desconocidos?
- ¿Usa aplicaciones en Redes Sociales?
- ¿Es consciente de los riesgos que implica la utilización de aplicaciones en Redes Sociales?
- ¿Teme por la seguridad de su información en Redes Sociales?

- ¿Ha configurado la privacidad del perfil de usuario?

Se han seleccionado estas variables que son fundamentales en la presente investigación y su análisis permitirá obtener más información acerca de la privacidad de Redes Sociales en la localidad. A continuación se desarrollan la correlación entre las variables mencionadas.

¿Cuántos de los usuarios que han publicado sus datos reales en las redes sociales, aceptan invitaciones de amistad de desconocidos?

En la Figura 67, claramente se observa que la tendencia es que los usuarios publiquen información real y acepten desconocidos; y los usuarios que no publican información real pero no aceptan invitaciones de desconocidos con un 89,2% del total.

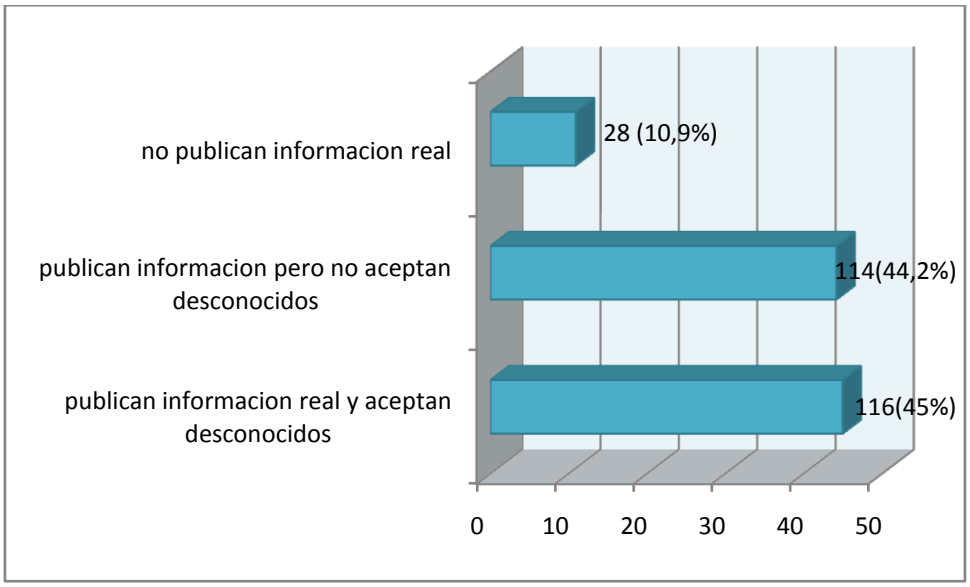

Figura 67. Correlación de datos entre ¿Publica información real? Y ¿Acepta invitación de amistad de desconocidos?

¿Cuántos de los usuarios que usan aplicaciones en redes sociales conocen los riesgos que implica su utilización?

Como se observa en la Figura 68 el 41,9% de los encuestados no usa aplicaciones el restante 58,1% usa aplicaciones y conoce los riesgos que esto implica; y usa aplicaciones y desconoce los riesgos.

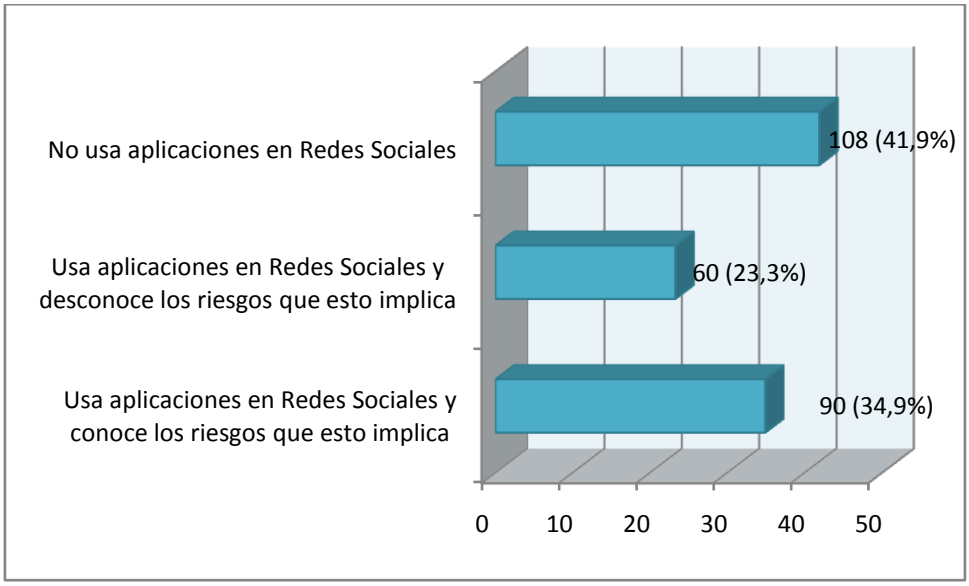

Figura 68. Correlación de datos entre ¿Usa aplicaciones? y ¿En consiente de los riegos que implica la utilización de aplicaciones en Redes Sociales?

¿Cuántos de los usuarios que temen por la seguridad de sus datos en sus redes sociales, han configurado la privacidad de su perfil?

En la Figura 69 se observa que la mayor parte de los encuestados teme por seguridad de su información y ha configurado la privacidad del perfil con un 49,2% y el restante 50,8% teme por la seguridad de su información pero no ha configurado; y no teme por la seguridad de su información.

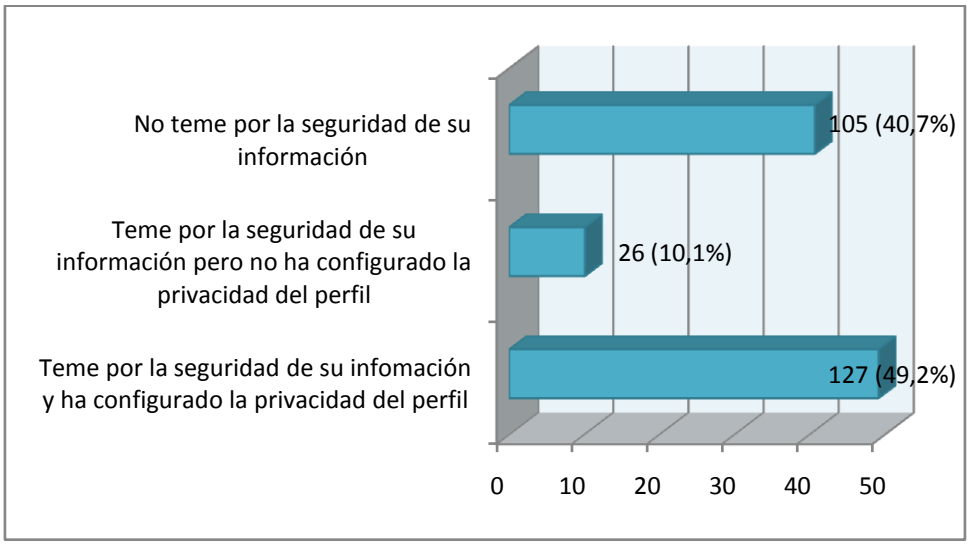

Figura 69. Correlación de datos entre ¿Teme por la seguridad de su información? y ¿Ha configurado la privacidad de su perfil?

6. POLITICAS DE BUEN USO PARA GESTIONAR LA PRIVACIDAD DE LA INFORMACION Y SEGURIDAD EN REDES SOCIALES

En el presente capitulo se describe una propuesta de políticas de buen uso destinadas a gestionar la privacidad de la información personal y contenidos en las redes sociales con mayor incidencia en nuestro entorno, que son, Hi5, Facebook y Sonico, esto, con la finalidad de ofrecer un marco para el uso seguro y responsable de las Redes Sociales. A través de estas pautas, se establecen los comportamientos seguros y responsables de los usuarios, además, las configuraciones y procedimientos para proteger nuestros datos e informar sobre contenidos inapropiados.

6.1 Política General

Objetivo.- Establecer los principios generales para la seguridad y privacidad de la información en las Redes Sociales.

Responsables del cumplimiento.- Los usuarios que frecuentemente están interactuando y socializando a través de su Red, son responsables de cumplir con las políticas definidas en el presente capitulo.

Definición.- A través de las políticas de buen uso, definidas para el presente capitulo, se pretende orientar a los usuarios, de tal manera que puedan gestionar la privacidad de información personal. Para tal efecto, se han establecido un conjunto de controles estructurados a través de:

- **Normas:** Definiciones concretas sobre cada uno de los temas de seguridad que luego serán adaptadas para asegurar la seguridad y privacidad en Redes Sociales.

- **Procedimientos:** Detalle de cursos de acción y tareas que deben realizar los usuarios para hacer cumplir las definiciones de las Políticas

- **Estándares Técnicos:** Conjunto de parámetros específicos de seguridad para las Redes Sociales analizadas.

Por ello, es política de la Universidad

- Asegurar que sea procesada toda la información necesaria y suficiente para la marcha de la Universidad únicamente en los sistemas informáticos y procesos transaccionales (Integridad).

- Garantizar que todos los medios de procesamiento y/o conservación de información cuenten con medidas de protección física que eviten el acceso y/o utilización indebida por personal no autorizado, así como permitan la continuidad de las operaciones. (Protección Física).

- Garantizar que todos los accesos a datos y/o transacciones cumplan con los niveles de autorización correspondientes para su utilización y divulgación (Autorización).

Estos principios se garantizarán a través del cumplimiento de una o varias de las normas que a continuación se proponen.

6.2 Norma 1 | Participación en Redes Sociales

a. Objetivo

Definir pautas generales para asegurar una adecuada comprensión de aspectos relacionados con la utilización de redes sociales.

b. Consideraciones Generales

i. El usuario debe plantear el objetivo que se quiere alcanzar con el uso de la red social, a partir de aquí, todas las actividades que se desarrollan

dentro de estas plataformas deben estar encaminadas a la consolidación de su identidad.

ii. Leer atentamente las Políticas de Privacidad y las Condiciones de Usos de las redes sociales, centrándose en el tratamiento que esto sitios efectúa con los datos personales del usuario.

iii. Analizar cuál de las redes sociales se ajusta a sus necesidades y darse de baja de las que no use, de tal manera que se evite dejar rastro de su información personal por la red (ver procedimiento PRO1NO1 | Desactivación de Cuentas)

6.3 Norma 2 | Configuración de la Privacidad del Perfil

a. Objetivos

Definir pautas generales para la configuración de la privacidad del perfil de usuario.

b. Consideraciones Generales

i. Todas las redes sociales disponen de parámetros de configurables de privacidad, cada una de estas redes sociales tiene un enfoque diferente en cuanto a la privacidad, pero todas fueron creadas con objetivo de mantener la privacidad del usuario.

ii. El usuario deberá configurar la privacidad de su perfil (ver procedimiento PRO1NO2 | Configuración de Privacidad del perfil)

iii. El usuario deberá bloquear a los usuarios que representen algún tipo de peligro o con quienes no desea tener ningún tipo de contacto (ver procedimiento PRO4NO2 | Bloqueo de Usuarios)

iv. El usuario no deberá aceptar invitaciones de desconocidos, lo ideal es asegurarse de saber de quién se trata antes de aceptar la invitación

6.4 Norma 3 | Tratamiento de la Información del Perfil de Usuario

a. Objetivo

Guiar el establecimiento de restricciones a la información de carácter personal.

b. Consideraciones Generales

i. Suministrar solo la información necesaria para que sus amigos lo reconozcan, el resto de información, como detalles acerca de su familia, domicilio, lugar de trabajo, propiedades, viajes, horarios y actividades cotidianas deben obviarse.

ii. La información de contacto como números de teléfonos o direcciones de correo electrónico, no deben ser publicadas, ya que si algún usuario requiere esta información la puede pedir a través del servicio de mensajería que ofrecen las redes sociales.

6.5 Norma 4 | Reporte de Abusos o Denuncias

a. Objetivos

Establecer las condiciones en las que se debe usar el Reporte de Abuso o Denuncia en las redes sociales

b. Consideraciones Generales

i. El usuario deberá reportar el abuso o denunciar cuando sus fotos estén siendo usadas por terceras personas (ver procedimiento PRO1NO4 | Reporte de abuso).

ii. El usuario deberá reportar el abuso o denunciar, cuando su información personal está siendo usada por terceras personas en perfiles falsos (ver procedimiento PRO1NO4 | Reporte de abuso).

6.6 Norma 5 | Publicaciones y Contenidos

a. Objetivos

Establecer pautas para orientar la divulgación de publicaciones y contenidos

b. Consideraciones Generales

i. Las publicaciones que realicen los usuarios no deben contener información de carácter personal ni información de contacto.

ii. En las publicaciones no se deben detallar las actividades que los usuarios van a realizar en su vida offline.

iii. Evitar realizar comentarios negativos o discriminatorios respecto a un usuario o grupos de usuarios, por religiones, filiaciones políticas, orientación sexual. etc.

iv. No publicar fotografías o videos de propiedades muebles o inmuebles.

v. No publicar fotos o videos que puedan atentar contra la dignidad de terceros.

6.7 Norma 6 | Credenciales de Acceso (Contraseña)

a. Objetivo

Gestionar de manera adecuada las contraseñas de usuario en las redes sociales

b. Consideraciones Generales

i. Se deberá crear la contraseña tomando en consideraciones establecidas en el presente capitulo (ver estándar técnico ET1NO1: Creación de Contraseñas)

ii. Cambiar periódicamente la contraseña, algunos sitios de banca en línea aplican esta política, precisamente por la criticidad de la información que contiene, puede que la información almacenada en las redes sociales no sea tan trascendental como las de la banca en línea pero esta política puede marcar a diferencia entre la privacidad o no.

iii. No usar la misma contraseña para todos los sitios en los que se ha registrado, es probable que no se pueda tener una contraseña para cada sitio, pero, lo ideal es contar con tres contraseñas: de bajo, medio y alto nivel de seguridad, para ser usada en los diferentes sitios dependiendo de la criticidad de la información.

6.8 Norma 7 | Navegación

a. Objetivo

Establecer conductas para una adecuada navegación.

b. Consideraciones Generales

i. No almacenar los nombres de usuario contraseñas en los navegadores de los equipos cuando acceden a las redes sociales.

ii. Cerrar la sesión de su red social una vez que haya realizado todas las actividades, esto principalmente si accede desde algún lugar público como Ciber Café.

6.9 Estándar Técnico

6.9.1 ET1NO1 | Creación de Contraseñas

TITULO	Estándar Técnico : Creación de Contraseñas
VERSION	1.0
AUTOR	Jorge Omar Sisalima
ESTADO	Aprobado

- La contraseña debe tener una longitud mínima de 8 (ocho) caracteres
- La contraseña debe tener una combinación de letras mayúsculas, minúsculas, números y caracteres especiales
- La contraseña no debe estar conformada por el nombre del usuario o cualquier otra información como: cumpleaños, nombre de hijos, etc.
- Tampoco utilizar letras adyacentes del teclado como *asdfgh*, o numero consecutivos como *123456*
- Palabras de algún idioma en particular como "*cuaderno*", ya que existen programas dedicados a descifrar las contraseñas comprándolas con cada una de las palabras del diccionario.
- Las contraseñas no deben poder deducirse de la información personal, información de otras personas o de información relacionada con gustos, preferencias, aficiones, ni nada que se pueda llegar a obtener o deducir con su información o la de otros, incluso si esta información no está en línea.

6.10 Procedimientos

6.10.1 PRO1NO1 | Desactivación de Cuentas

TITULO	Procedimiento : Desactivación de Cuentas
VERSION	1.0
AUTOR	Jorge Omar Sisalima
ESTADO	Aprobado

a. Hi5

Paso 1: vez que ha ingresado en su perfil de usuario, se debe acceder a “mi cuenta” que se encuentra en la parte superior derecha de la pantalla como se muestra en la Figura 70

Figura 70. Perfil de Usuario Hi5

Paso 2: Ir a “Cancelar mi cuenta”

Figura 71. Mi Cuenta

Paso 3: Se muestra una advertencia que Hi5 hace respecto a la cancelación de su cuenta, para completar el proceso de cancelación se debe ingresar el correo electrónico, su contraseña y dar clic en “Cancelar mi cuenta”

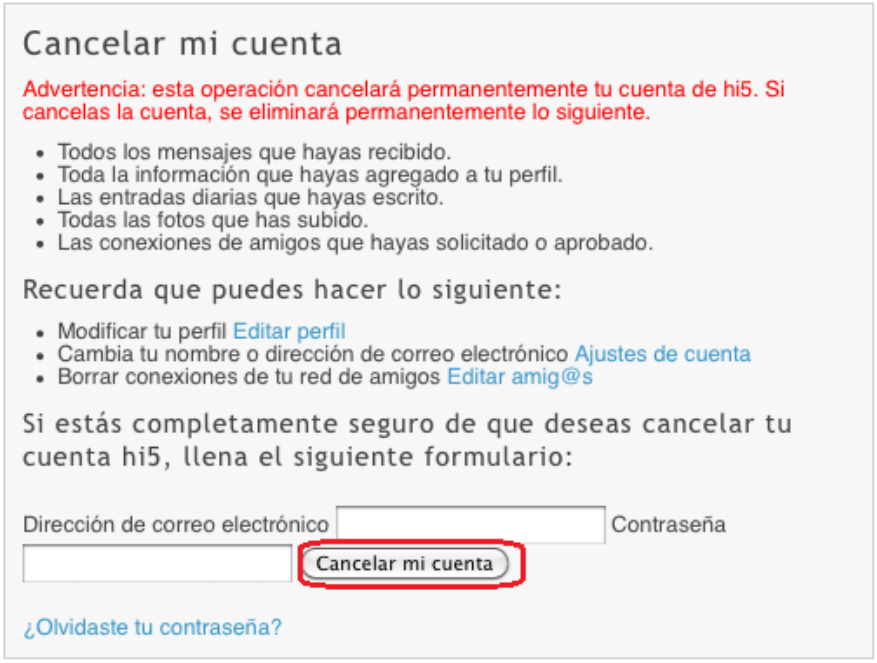

Figura 72. Formulario para cancelar cuenta de hi5

b. Facebook

Paso 1: Una vez que se han ingresado su usuario y dar clic en Cuenta y luego ir a "Configuración de la cuenta"

Figura 73. Menú de opciones de configuración de la cuenta de Facebook

Paso 2: Ir a "Desactivar la cuenta", que se encuentra en la parte inferior.

Figura 74. Configuración de la Cuenta

Paso 3: Seleccionar un motivo por el que se quiere desactivar la cuenta, detallar el motivo de desactivación y dar clic en Confirmar

Figura 75. Formulario para desactivar cuenta de Facebook

Paso 4: Ingresar su contraseña

Figura 76. Confirmación de Contraseña

Paso 5: Escribir la palabras que aleatoriamente se muestran como parte del control de seguridad de Facebook. Finalmente aparecerá un mensaje donde se notifica que la cuenta ha sido desactivada.

Figura 77. Control de Seguridad

c. Sonico

Paso 1: En la Figura 78 se muestra la página que por defecto se abre cuando iniciamos sesión en Sonico. Para cerrar la cuenta de Sonico, se debe acceder a “Mi cuenta”, cuyo enlace se encuentra en la parte superior derecha de la pantalla.

Figura 78. Página principal de Sonico

Paso 2: Acceder a “Quiero cerrar mi cuenta”, cuyo enlace se encuentra en la parte inferior de la pestaña Configuración Básica.

Figura 79. Configuraciones básicas de Sonico

Paso 3: Seleccionar un motivo de suspensión y dar clic en el botón "Desactivar mi cuenta", luego aparecer una notificación de que la cuenta ha sido desactivada.

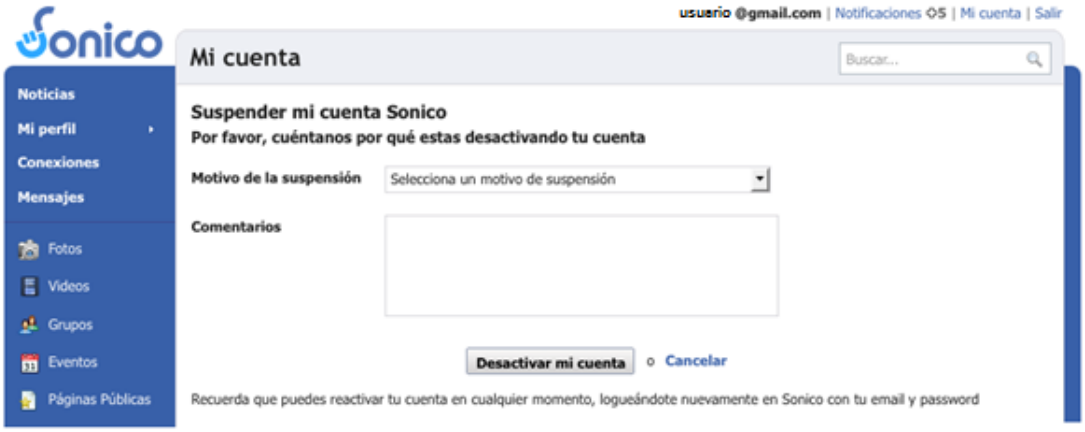

Figura 80. Formulario para desactivación de cuenta en Sonico

6.10.2 PRO1NO1 | Configuración de Privacidad del perfil

TITULO	Procedimiento : Configuración de Privacidad de Perfil
VERSION	1.0
AUTOR	Jorge Omar Sisalima
ESTADO	Aprobado

a. Hi5

Paso 1: Para la configuración de la privacidad del perfil de usuario en Hi5, el usuario debe ir a "mi cuenta"

Figura 81. Perfil de Usuario Hi5

PASO 2: Dar clic en la pestaña “Seguridad”

Figura 82. Mi Cuenta Hi5

PASO 3: Personalizar cada uno de los ajustes de privacidad. Ver ANEXO B

b. Facebook

Paso 1: Para la configuración de la privacidad del perfil de usuario en Facebook, el usuario debe ir a “Cuenta”, luego dar clic en “Configuración de la privacidad”

Figura 83. Menú de opciones de configuraciones de Facebook

Paso 2: Ir a “Personalizar la configuración”, que se encuentra en la parte inferior de la pantalla.

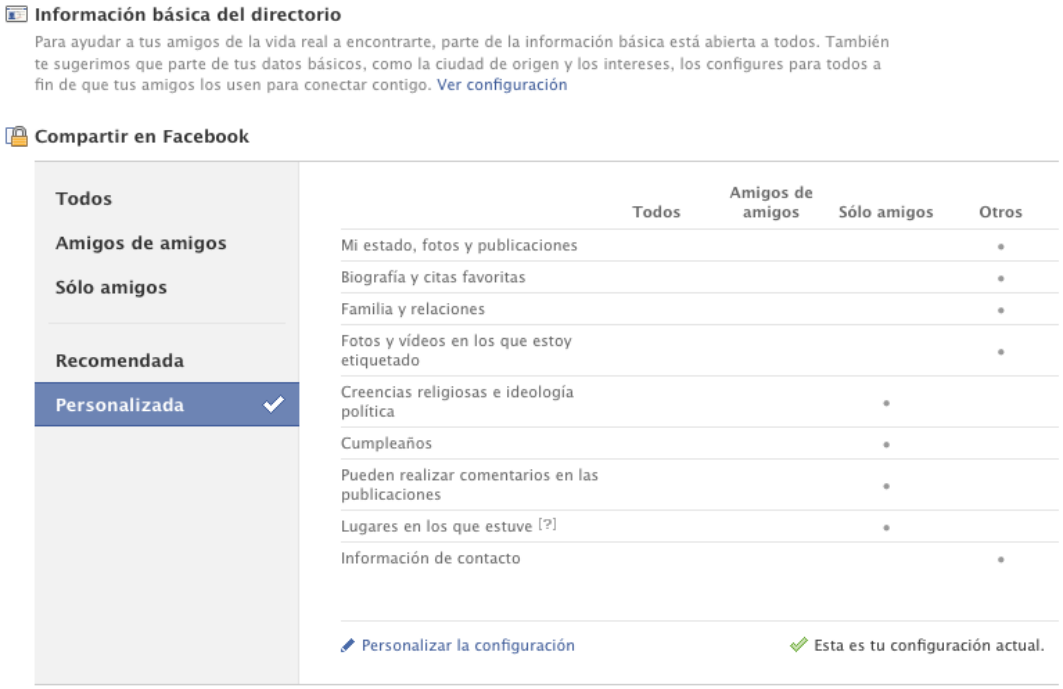

Figura 84. Personalizar configuración

Paso 3: Personalizar cada uno de los parámetros de privacidad. Ver ANEXO C

c. Sonico

Paso 1: Para la configuración de la privacidad del perfil de usuario en Sonico, el usuario debe ir a “Mi cuenta”

Figura 85. Página principal de Sonico

Paso 2: En la pestaña "Privacidad" se despliega el listado de los parámetros, lo cuales deben ser personalizados por los usuarios. Ver ANEXO D

6.10.3 PRO4NO2 | Bloqueo de Usuarios

TITULO	Procedimiento : Bloqueo de usuarios
VERSION	1.0
AUTOR	Jorge Omar Sisalima
ESTADO	Aprobado

a. Hi5

Paso 1: Para bloquear a un usuario, se debe acceder al perfil de usuario de la persona a quien se quiere bloquear, dar clic en bloquear, cuyo enlace se encuentra bajo la foto del usuario.

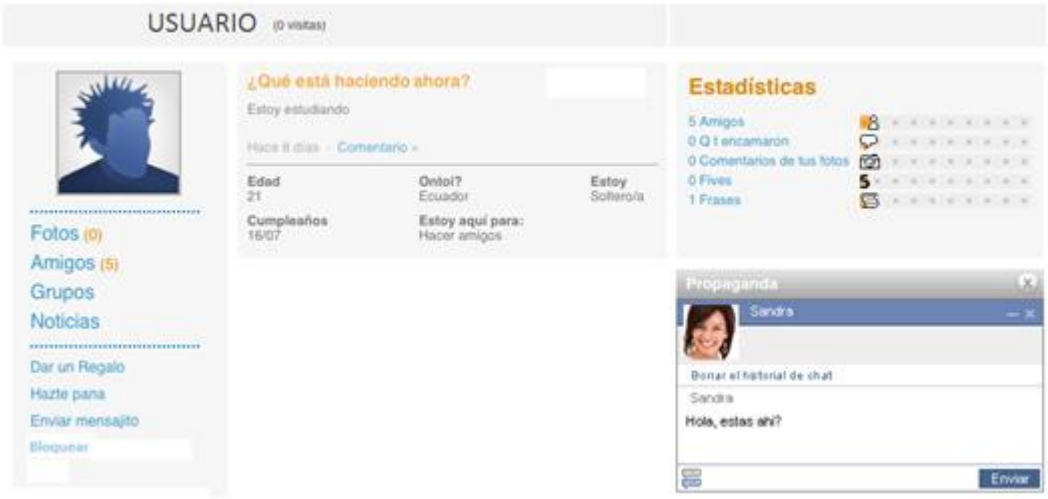

Figura 86. Perfil de Usuario Hi5

Paso 2: Hi5 muestra una advertencia sobre el bloqueo del usuario y el parte inferior pregunta se esta seguro que desea bloquear a dicho usuario, para lo cual, se debe dar clic en “Si”

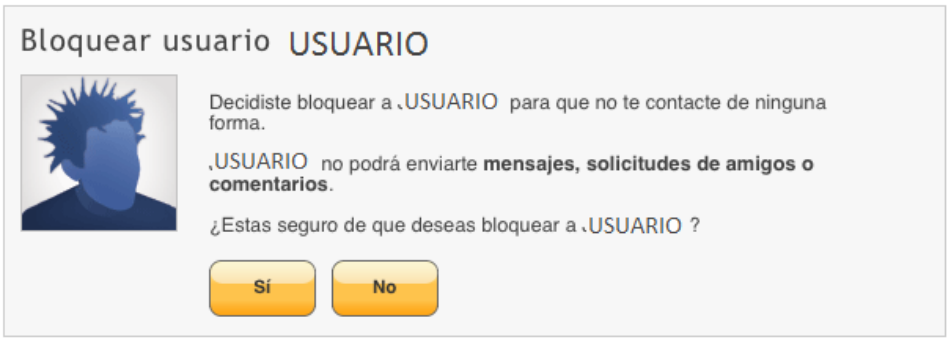

Figura 87. Confirmación de bloqueo de usuarios

b. Facebook

Paso 1: Para bloquear a un usuario, se debe acceder al perfil de usuario de la persona a quien se quiere bloquear, dar clic en “Denunciar/bloquear a esta persona”, cuyo enlace se encuentra en la parte inferior izquierda del perfil de usuario.

c. Sonico

Paso 1: Para bloquear a un usuario, se debe acceder al perfil de usuario de la persona a quien se quiere bloquear, dar clic en el botón “Denunciar”, que se encuentra en la parte inferior derecha del perfil de usuario.

Figura 88. Perfil de Usuario de Sonico

6.10.4 PRO4NO2 | Reporte de Abuso o Denuncia

TITULO	Procedimiento : Reporte de Abuso o Denuncia
VERSION	1.0
AUTOR	Jorge Omar Sisalima
ESTADO	Aprobado

a. Hi5

Paso 1: Para reportar abuso o denunciar, se debe acceder a la foto o contenido que se dese reportar, luego ir a “Denunciar” que se encuentra en la parte superior.

Figura 89. Denuncia o Reporte de Abuso en Hi5

b. Facebook

Paso 1: Para reportar abuso o denunciar, se debe acceder a la foto o contenido que se dese reportar, luego ir a "Denunciar esta foto" que se encuentra en la parte inferior del recurso.

Figura 90. Denuncia o Reporte de Abuso en Facebook

7. LEGISLACION DE REDES SOCIALES

Los usuarios con el afán de socializar y compartir su vida con sus amigos, están exponiendo su información personal y dejando al descubierto su intimidad y actividades cotidianas. Como ya se vió en los capítulos anteriores, existen muchos riesgos a los que los usuarios están propensos. Por este motivo en algunos países se están dando los primeros pasos para la legislar las Redes Sociales.

Esta legislación debe estar orientada a mantener la privacidad de la información personal, asegurar el derecho a la intimidad, honor e imagen. Hasta el momento no se ha concretado una ley que hable explícitamente de redes sociales, pero en algunos países de la región como México y Chile se han realizado propuestas para legislar las redes sociales. En un contexto más amplio la Unión Europea desde alguien tiempo atrás se está preocupando de proteger la privacidad de la información personal en estas comunidades.

7.1 Problemática

Las redes sociales se han consolidado como un referente de la comunicación, interacción social e intercambio de información en tiempo real. La utilización de las redes sociales puede plantear riesgos para la privacidad de los usuarios. Ya que, la información de carácter personal incluyendo fotografías y videos, están siendo accedidos de forma púbica y global de una manera y en cantidades sin precedentes, con objetivos diferentes al de la socialización. Por ello, es imprescindible crear un marco jurídico que permita regular y establecer sanciones a las actividades licitas e inapropiadas en las redes sociales. En este, sentido se deben tomar en cuenta algunas implicaciones jurídicas como:

- Protección de los derechos del honor, intimidad y propia imagen.
- Protección de Datos de Carácter Personal.
- Protección de menores.

7.2 Implicaciones Jurídicas de las Redes Sociales

La mayoría de las redes sociales se han preocupado más de los aspectos técnicos que de los aspectos jurídicos. Obviamente existen cuestiones tan importantes que deben ser tomadas en cuentas por las redes sociales y que se detallan a continuación.

- **Derecho al Honor, Intimidad y Propia Imagen**

  El derecho al honor es aquel que tiene toda persona a su buena imagen, nombre y reputación, de tal forma que todos pueden exigir que se respete su esfera personal, con independencia de las circunstancias particulares, siendo un derecho irrenunciable (68). *El derecho a la propia imagen* pretende salvaguardar un ámbito propio y reservado del individuo, aunque no íntimo, frente a la acción y conocimiento de los demás (68). *El derecho a la intimidad* tiene por objeto la protección de la esfera más íntima de la persona, y se encuentra íntimamente ligado a la protección de la dignidad del individuo.

- **Protección de datos de carácter personal**

  Vivimos en una sociedad basada en la información, el impulso que en estos últimos tiempos han tenido las nuevas tecnologías y específicamente las redes sociales, han supuesto un tratamiento masivo a la información de carácter personal ya que la naturaleza de las redes sociales es hacer públicos sus datos en sus perfiles de usuario para socializar.

- **Protección a la propiedad intelectual**

  A través de las redes sociales cada día se usan, comparten y difunden contenidos protegidos por el derecho de propiedad intelectual, esta normativa hace referencia a la protección de los derechos de los autores de las obras artísticas científicas y literarias de su propia creación. La naturaleza de las redes

sociales ha permitido que contenidos como fotografías y videos sean publicados por terceros sin ningún tipo de autorización de autor de estos contenidos.

- **Protección a los menores**

Los menores son el grupo más vulnerable dentro de las redes sociales, principalmente por el desconocimiento de los riesgos a los que conlleva la participación en redes sociales y la excesiva confianza de estos usuarios para compartir su información y contenidos.

7.3 Legislando Redes Sociales

7.3.1 En la Unión Europea

La Comisión Europea está tomando los primeros pasos en cuanto a la regulación de redes sociales. El pasado 09 de febrero de 2010 según una publicación de elmundo.es, la Unión Europea ha exigido a las redes sociales cumplir con la normativa de protección de datos, haciendo énfasis en la protección de sus usuarios menores de edad y les insistan en aplicar mejores medidas, especialmente en no permitir que publiquen por defecto los datos de estos usuarios. "Los perfiles de los menores deben ser 'privados' por defecto y las preguntas o denuncias de abusos deben ser respondidas con rapidez y de forma adecuada", exigió la comisaria en su declaración (69).

7.3.2 En Latinoamérica

En México en febrero del 2010, el diputado del PRD Nazario Norberto Sánchez presentó una iniciativa de ley para controlar el contenido de las redes sociales. Según este diputado la razón por la que se pretende regular las redes sociales, es para evitar que los usuarios usen estas redes para evadir los controles policiales y ubicar a personas por delincuentes.

El 15 de junio de 2010, la Asamblea General del Distrito Federal ALDF (México) informó su preocupación e iniciativa de incluir el delito de usurpación de identidad y de personalidad en redes sociales, lo cual sería un precedente para la legislación de estas comunidades (70).

En Chile, la cámara legislativa está tramitando un proyecto de ley que habla expresamente de las redes sociales (ver ANEXO E), La reforma chilena, atendiendo a la experiencia de este grupo, lo que pretende es dotar de una legislación adecuada a los usos en las redes sociales de las personas físicas y proteger cuando terceros usan esos instrumentos fuera de ese objetivo (71).

7.3.3 En el Ecuador

Según la Asambleísta María Paula Romo, al momento no existe ninguna ley, ni siquiera una propuesta de ley encaminada a la protección de los usuarios de las redes sociales (70).

El estudio de Redes Sociales, privacidad y sus implicaciones jurídicas, no está tan alejada de la realidad, vemos que en Europa y algunos países de Latinoamérica se están dando los primeros pasos para la regularización de redes sociales. El grupo más vulnerable dentro de estas plataformas son los menores, debido al desconocimiento de los riegos y excesiva confianza de estos usuarios. Por ello se están usando estas redes con plataformas de captación de victimas para realización de ilícitos.

Los derechos de los usuarios, como al honor, intimidad y buen nombre; están siendo violentados dentro de las redes sociales, pero no existe un marco jurídico que sancione estas actividades dentro de las redes sociales.

En base a lo expuesto se ha visto la necesidad de desarrollar la siguiente propuesta, cabe recalcar que la misma fue desarrollada con asesoría con los abogados del departamento de Gestión Legal de la Universidad Técnica Particular de Loja.

PROPUESTA DE INCORPORACION AL SISTEMA LEGAL PENAL DE UNA NORMATIVA QUE SANCIONE LOS DELITOS A TRAVES DE LAS REDES SOCIALES

MOTIVOS

Las redes sociales se han convertido en un fenómeno social sin precedentes en la historia de la humanidad, vemos que, redes sociales como Facebook han alcanzado los 500 millones de usuarios y cada día se unen más personas. Estas plataformas ofrecen grandes posibilidades de comunicación e intercambio de información en tiempo real, permitiendo la propagación de ideas, participación ciudadana, negocios, diversión e integración social, ya que son sistemas globales que maximizan las estructuras sociales de la vida off line.

Las redes sociales se han convertido en poderosos canales de comunicación e interacción y su acelerado crecimiento genera un gran riesgo debido al acceso de la información de carácter personal, la cual posee gran valor como tal, constituye un poder en sí mismo, que puede ser utilizado para delinquir, presionar, chantajear, dirigir, manipular, o controlar, además han sido objeto de una indiscriminada comercialización, mediante el cual pocas personas se han enriquecido y aprovechado económicamente.

En algunos países de la región se consagra constitucionalmente el derecho a la protección de datos en internet, pero en ninguno de ellos se habla explícitamente de la protección de datos de carácter personal en las redes sociales.

En el Ecuador, no existe una ley que proteja a los usuarios de redes sociales frente a los riegos de tratamiento y utilización de datos personales con fines comerciales e ilícitos, usurpación de identidad, creación de perfiles falsos o reproducción de dichos datos en cualquier otro lugar. Pero se cuenta con la Ley de Comercio Electrónico, Firmas Electrónicas, y Mensajes de Datos, Ley Orgánica de Defensa del Consumidor, Ley de

Telecomunicaciones y Ley de Sistema Nacional de Datos, que abordan temas relacionados a la protección de datos y delitos informáticos, pero no es suficiente, ya que, en asuntos legales, las cosas deben ser claras y precisas para evitar mal interpretaciones.

CONSIDERANDO

Que: La Constitución de la República, en el artículo 1, establece: que el Ecuador es un Estado Constitucional de derechos y justicia social, democrática, soberana, independiente, unitaria, intercultural, plurinacional y laico;

Que: El artículo 66, garantiza, el derecho a la integridad personal, la cual incluye, la integridad física, psíquica, moral y sexual; así como el derecho a guardar reserva sobre sus convicciones;

Que: El numeral 19, del artículo 66, en forma expresa garantiza, el derecho a la protección de datos de carácter personal, el cual incluye el acceso y la decisión sobre información y datos de ese carácter, así como la correspondiente protección;

Que: Es necesario generar un marco regulatorio adecuado y eficaz para evitar que el acceso a los datos de carácter personal y contenidos publicados en redes sociales se transformen en un riesgos para los usuarios;

Por estas razones, se ha desarrollado la siguiente:

PROPUESTA DE INCORPORACION AL SISTEMA LEGAL PENAL DE UNA NORMATIVA QUE SANCIONE LOS DELITOS A TRAVES DE LAS REDES SOCIALES

CAPITULO I

GENERALIDADES

Art. 1. *Objetivo.* Garantizar que los contenidos y datos de carácter personal en las redes sociales estén adecuadamente protegidos evitando un uso inadecuado e indiscriminado para garantizar el honor y el derecho a la intimidad que cualquier persona tiene.

Art. 2. *Alcance.* La presente ley se limita a protección de la información de carácter personal, protección de menores, regularización de contenidos en las redes sociales

Art. 3. *Glosario de Términos.* Para los fines de la presente ley entiéndase por:

Titular de datos*:* Persona propietario de los datos

Información personal: Los datos que se refieren a toda aquella información relativa al individuo que lo identifica o lo hace identificable. Entre otras cosas, le dan identidad, lo describen, precisan su origen, edad, lugar de residencia, actividades que realiza, trayectoria académica, laboral o profesional. Además aspectos más sensibles como es el caso de su forma de pensar, estado de salud, sus características físicas, ideología o vida sexual, entre otros.

Intimidad*:* Es la parte interior de la persona que solamente cada uno conoce de sí mismo.

Terceros: Persona o personas distinto del titular de los datos.

Usuario: Persona natural o jurídica que se han registrado en la red social y que tiene un perfil de usuario y comparte información.

Amigos: Usuarios de la red social que han sido agregados a la lista de contactos del perfil de usuario.

Perfil de Usuario: Pagina principal de una red social, donde se muestra la información personal del usuario.

Grupos de amigos o Comunidades: Usuarios agrupados dentro de la red social que tienen intereses en común y comparten información relacionada a estos intereses.

Cyberbulliyng o ciberacoso: escolar, es el asedio u hostigamiento entre menores, principalmente entre compañeros de escuela o colegio.

Contenidos: Información adicional publicada en los perfiles de usuario como: fotografías, enlaces, archivos, videos, etc.

Art. 4. *Ámbito.* La presente ley se aplicara a los datos personales y contenidos registrados en las redes sociales, susceptibles de tratamiento y a toda forma de uso posterior por terceros. El o los responsables del tratamiento radicados fuera del territorio nacional, se sujetará a las normas de Derechos Internacional.

CAPITULO II

PROTECCION DE LA INFORMACIÓN PERSONAL

Art. 5. La información personal que el empleador recabe de sus trabajadores en una red social, no podrá ser usada para despedir sus empleados.

Art. 6. La información relacionada con ideología política, orientación sexual, estado de salud, no podrá ser usada para discriminar al titular de los datos.

Art. 7. La información de carácter personal no podrá ser usada para usurpar o suplantar la identidad de los usuarios con fines ilícitos o para agredir o difundir mensajes o contenidos lesivos al honor de las personas u otros fines que no sea el de socializar.

Art. 8. La información de carácter personal, relacionada con gustos, preferencias o aficiones no podrá ser usada por terceras personas para propagar spam.

Art. 9. Los grupos, páginas o comunidades de las redes sociales, no podrán ser usadas para promover la violencia y odio contra otras personas.

Art. 10. Los grupos, páginas o comunidades de las redes sociales, no podrán ser usadas para realizar actos ilícitos.

CAPITULO III

CONTENIDOS

Art. 11. Los Contenidos fotográficos publicados en redes sociales no podrán ser usados en fotomontajes o subidos en otros perfiles sin autorización del titular o usados con otros fines ilícitos.

Art. 12. Las redes sociales no podrán ser usadas para publicar contenidos racistas, discriminatorios o atentatorios al honor de los usuarios.

CAPITULO IV

MENORES

Art. 13. Las redes sociales no podrán ser usadas para acosar o incitar a los menores a realizar actos pornográficos u otros ilícitos.

Art. 14. Las redes sociales no podrán ser usadas para el acoso entre menores (Cyberbullying)

CAPITULO V

SANCIONES

Art. 15. Usurpación y Suplantación de identidad.- La apropiación de la identidad de los usuarios de redes sociales, será sancionado con la pena de 10 salarios mínimos y 3 meses de prisión.

Art. 16. El uso doloso de la información publicada en redes sociales, por parte del empleador será sancionada con la pena de 20 salarios mínimos y 6 meses de prisión.

Art. 17. La publicación de contenidos que inciten a la violencia y odio será sancionado con la pena de 20 salarios mínimos y 6 meses de prisión.

Art. 18. La publicación de contenidos o comentarios que lesiones la dignidad de las personas, menoscabando su imagen o atentando con su propia estima, será sancionado con 20 salarios mínimos y 6 meses de prisión.

Art. 19. La alteración o modificación de fotografías sin autorización del titular será sancionado con 20 salarios mínimos y tres meses de presión.

Art. 20. El incitar a los menores a través de redes sociales a realizar actos pornográficos o el uso de imágenes de carácter pornográfico donde se incluya menores, será sancionado con la pena de 20 salarios mínimos y 2 años de prisión.

Art. 21. La intimación y maltrato psicológico deliberado a través de redes sociales, hacia un menor por parte de otro u otros menores de su mismo entorno escolar, será sancionado por primera vez con una multa de 20 salarios mínimos a los padres del acosador, y con una multa de 50 salarios mínimos en caso de reincidencia.

DISPOSICIÓN DEROGATORIA

En virtud de la vigencia de la presente Ley, quedan derogadas las normas y disposiciones que se opongan a la misma.

DISPOSICIÓN FINAL

La presente ley, entrará en vigencia, a partir de la fecha de su publicación en el Registro Oficial.

8. DISCUSIÓN Y ANÁLISIS DE RESULTADOS

Contrariamente a los que se piensa, las redes sociales no son un invento actual, ya que siempre han existido, debido a que una Red Social es básicamente un grupo de personas, ya sean estos amigos, compañeros, vecinos, etc., que se relacionan a través de sus ideas, pensamientos, creencias, aficiones en común, etc.. Pero, con el aparecimiento de la Web 2.0 en general y particularmente de las plataformas que ofrecen el servicio de redes sociales, este concepto toma mayor importancia revolucionando la manera en cómo el mundo se comunica ya que se han consolidado como un poderoso canal de comunicación e interacción social.

Cada día, millones de personas alrededor del mundo acceden a su red social, pero no todos lo hacen con la intención de socializar; un grupo considerable y creciente de usuarios acceden a estos sitios con el objetivo de obtener algún beneficio y es que estos sitios no son totalmente seguros, aparte de las técnicas conocidas de ciberdelincuencia, los usuarios están expuestos al envío de mensajes amenazantes, inserción de contenidos lesivos contra el honor, la usurpación de identidad con fines fraudulentos, uso de contenidos delictivos, entre otras, que constituyen un abanico de técnicas y conductas que son utilizadas por los ciberdelincuentes. Por su parte la delincuencia tradicional tiene en las redes sociales una plataforma de captación de victimas, ya que para ellos es más fácil revisar el Facebook de su víctima, a que tener que seguirlo físicamente, para encontrar el momento adecuado para atacar.

Todas las Redes Sociales disponen de un conjunto de parámetro configurables de privacidad, pero, son los usuarios quienes deben gestionar la privacidad de su información personal, todos están expuestos a ser víctimas de ataques de los ciberdelincuentes y el principal riesgos es la exposición, que puede traer graves consecuencias a los usuarios llegando incluso a afectar su integridad física. Pero se puede minimizar el riesgo, personalizando dichas configuraciones ya que por defecto estas no tienen ninguna restricción, y esto potencia la exposición de los individuos a un entorno desconocido, lleno de gente que está a la espera de un descuido de los usuarios para aprovecharse. Ahora la meta de nuestra sociedad es crear nuevos servicios utilizando las tecnologías de la información y comunicación, que nos lleven a

consolidar la sociedad de la información pero sin dejar de lado la seguridad y privacidad de los usuarios.

En el Ecuador, no existen estudios previos que demuestren como se han desarrollado las redes sociales, pero de acuerdo a los reportes de audiencias de estos sitios, se ha podido determinado que la mayoría de los usuarios se concentran en Quito y Guayaquil, y las audiencias minoritarias son Loja, Cuenca y Manta. En Loja, de acuerdo con la información obtenida en la encuesta de "*Incidencia de Redes Sociales en Loja*", se pudo determinar que, estas son mayormente usadas por estudiantes universitarios y secundarios, en comparación con profesionales en las instituciones de gobierno encuetadas. De igual manera, con la información obtenida en la encuesta de "*Privacidad de Redes Sociales en Loja*", se ha determinado, entre otras cosas que, los usuarios de Redes Sociales de Entornos Educativos Secundarios son más vulnerables frente a los usuarios de Entornos Educativos Universitarios principalmente por el desconocimiento de los riegos, exposición de la información personal y dejadez en la configuración de la privacidad.

Las redes sociales son el único medio de comunicación masivo que puede ser usado ilícitamente debido a que no existe ninguna ley o normativa que regule y sanciones las actividades desarrolladas por los usuarios en esto sitios. Ya que, algunos derechos Humanos como al honor, buen nombre, propia imagen e intimidad están siendo vulnerados, debido a las actividades que inconsciente o mal intencionadamente desarrollan los usuarios, acerca de si mismo y de los demás.

En el Ecuador se consagra constitucionalmente la protección de datos de carácter personal, pero hasta el momento no existe ningún cuerpo jurídico que garantice dicha protección de datos en ningún ámbito, cabe recalcar que existen leyes como, La Ley de Comercio Electrónico, Firmas Electrónicas, y Mensajes de Datos, Ley Orgánica de defensa del Consumidor, ley de Sistema Nacional de Datos Públicos, que tratan temas relacionados a la protección de datos pero no lo abordan explícitamente. Es por ello que la propuesta de incorporación al sistema legal penal de una normativa que sanciones los delitos a través de redes sociales desarrollada en el presente estudio se convierte en un precedente para la protección de datos en el país. Esta propuesta está orientada a garantizar que los contenidos y datos de carácter personal en redes sociales estén

adecuadamente protegidos, evitando el uso inadecuado e indiscriminado para garantizar el honor y el derecho a la intimidad que cualquier persona posee

9. CONCLUSIONES

- Hi5 fue una de las primeras redes sociales en llegar a Latinoamérica, por ello, se consolido como uno de los sitios más visitados en la mayoría de los países de la región, pero, actualmente Facebook está acaparando la mayoría parte de la audiencia latinoamericana y cuenta con 515'617,460 usuarios alrededor del mundo. En el Ecuador, Hi5 tiende a la baja desde Octubre de 2008, cuando alcanzo su nivel más alto de actividad en el país, llegando aproximadamente a 150,000 visitas diarias. Mientras que Facebook, desde Junio de 2007, ha mantenido un incremento constante, alcanzando 1'549,680 usuarios en Septiembre de 2010 y consolidando como una de las audiencias de mayor crecimiento en la Región.

- La utilización de redes sociales en entornos educativos y entidades de gobierno en la ciudad de Loja, llega al 76.20%, siendo Hi5, Facebook y Sonico las redes más usadas con 50.41%, 44.72% y 2.44% respectivamente.

- Las redes sociales son mayormente utilizadas por los usuarios de Entornos Educativos secundarios y universitarios llegando al 84,28% frente a los usuarios de las entidades de gobierno encuestadas, donde solo 25,10% utiliza redes sociales.

- Los usuarios de Entornos Educativos Secundarios EES son más vulnerables que los usuarios de Entornos Educativos Universitario EEU, principalmente por:

    - El desconocimiento de los riesgos ya que solo el 16,67% en EES es consciente de los riegos frente al 67,83% en EEU.

    - El 73,26% de los usuarios de EEU aseguran tener una contraseña segura frente al 23,64% de EES.

    - En cuanto a las configuraciones de privacidad, solo el 36,82% en EES ha personalizado la privacidad de su perfil, frente al 75,58% en EEU.

- Tomando como referencia solo a los usuarios que han configurado la privacidad. En EEU 23,67% ha dejado las configuraciones por defecto y el 61,35% permite que solo sus amigos accedan a su perfil. En cambio en EES 7,37% han dejado las configuraciones por defecto y el 23,16% permite que solo sus amigos puedan acceder a su perfil. Hay que destacar que estas configuraciones solo hacen referencia a la visibilidad del perfil.

❖ Las redes sociales superaron la función para la que fueron creadas y se consolida como el único medio de comunicación masiva que puede ser usado ilícitamente ya que no existe legislación alguna alrededor del mundo que regule las actividades en las redes sociales. Pero, en algunos países de la región como México y Chile se están dando los primeros pasos para legislar las redes sociales. En el Ecuador no existe alguna ley que aborde explícitamente estos temas, pero, la propuesta de ley desarrollada en el presente estudio se consolida como precedente para una futura implementación en la legislación ecuatoriana.

10. TRABAJOS FUTUROS

- Tomando como línea base el presente estudio, se debería continuar con el análisis de la Seguridad de Redes Sociales en la Ciudad de Loja y ampliando el alcance a nivel nacional, de tal manera que permita llevar un registro del desarrollo de las redes sociales en el Ecuador y sus implicaciones políticas y jurídicas.

- Las empresas han visto en las redes sociales un poderoso canal de comunicación e interacción directa con sus potenciales clientes, siendo este entorno, uno de los que mejor aprovecha los beneficios de las redes sociales. Por ello, se debería desarrollar un estudio de incidencia y Seguridad de las Rede Sociales en las PYMES

- Los avances tecnológicos y fundamentalmente las redes sociales han generado un ritmo acelerado de cambio en el marketing, tanto en la oferta de productos como en los canales de comunicación, por ello es importante desarrollar un estudio de las redes sociales como herramienta de marketing para las empresas y como la privacidad y seguridad de la información en estas plataformas puede influir en la reputación de marcar y empresas.

11. RECOMENDACIONES

- Difusión y promoción del uso de las políticas para gestionar la privacidad de la información y seguridad de redes sociales.

- Fortalecimiento de la propuesta de ley e impulso para la implementación en la legislación ecuatoriana.

- Capacitación a los usuarios acerca de las configuraciones de privacidad de las Redes Sociales con mayor incidencia en nuestro entorno.

- Análisis el desarrollo de grupos temáticos especializados y de investigación dentro de las redes sociales y su influencia en la gestión de conocimiento para la Educación Superior en Latinoamérica y el Ecuador.

12. REFERENCIAS

1. **ESV, English Standar Version of Bible.** Mapping New Testament Social Networks. [En línea] [Citado el: 12 de Noviembre de 2009.] http://www.esv.org/blog/2007/01/mapping-nt-social-networks/.

2. **FERNANDEZ BURGUEÑO, Pablo.** Redes Sociales en la Administración Pública Local. [En línea] [Citado el: 2009 de Noviembre de 12.] http://www.pabloburgueno.com/wp-content/uploads/2009/12/Redessociales-en-la-Adm-P%C3%BAblica-Local.pdf.

3. **VALENZUELA, Jaime y VALERIO, GAbriel.** primeros pasos para el e-learning 2.0, Virtual Educa, Tecnológico de Monterrey (México). [En línea] [Citado el: 2009 de Noviembre de 13.] http://www.virtualeduca.info/ponencias/446/Ponencia%20-%2009-09-09.doc.

4. **WIKIPEDIA;.** Eciclopedia Libre, Concepto de Red Social. [En línea] [Citado el: 2010 de Noviembre de 13.] http://es.wikipedia.org/wiki/Red_social.

5. **FABERNOVEL Consulting.** Social Network Werbsites: best practices from leading services. [En línea] 2007. [Citado el: 2009 de Noviembre de 15.] www.fabernovel.com/socialnetworks.pdf.

6. **Digizen;.** Social Networks Overview. [En línea] [Citado el: 2009 de Noviembre de 15.] http://www.digizen.org/socialnetworking/.

7. **FERNÁNDEZ BURGUEÑO, Pablo.** Clasificación de Redes Sociales, 2009. [En línea] [Citado el: 2009 de Noviembre de 15.] http://www.pabloburgueno.com/2009/03/clasi_cacion-de-redes-sociales/.

8. **WIKIPEDIA.** Enciclopedia Libre en Español, Flickr. [En línea] [Citado el: 2009 de Noviembre de 15.] http://es.wikipedia.org/wiki/Flickr.

9. **WIKIPEDIA;.** Enciclopedia Libre en Español, YouTube. [En línea] [Citado el: 2009 de Noviembre de 15.] http://es.wikipedia.org/wiki/YouTube.

10. —. Enciclopedia Libre en Español, Shelfari. [En línea] [Citado el: 2009 de Noviembre de 15.] http://es.wikipedia.org/wiki/Shelfari.

11. **WIKIPEDIA.** Enciclopedia Libre en Español, Lastfm. [En línea] [Citado el: 2009 de Noviembre de 15.] http://es.wikipedia.org/wiki/Lastfm.

12. —. Enciclopedia Libre en Español, Ning. [En línea] [Citado el: 2009 de Noviembre de 15.] http://es.wikipedia.org/wiki/Ning.

13. **TOP TEN REVIEW;.** Ranking de Redes Sociales. [En línea] [Citado el: 2009 de Noviembre de 16.] http://social-networkingwebsites-review.toptenreviews.com/.

14. **WIKIPEDIA;.** Enciclopedia Libre en Español, Red Social Hi5. [En línea] [Citado el: 2009 de Noviembre de 20.] http://es.wikipedia.org/wiki/Hi5.

15. —. Enciclopedia Libre en Español, Red Social Facebook. [En línea] [Citado el: 2009 de Noviembre de 21.] http://es.wikipedia.org/wiki/Facebook.

16. **WIKIPEDIA.** Enciclopedia Libre en Español, Red Social Orkut. [En línea] [Citado el: 2009 de Noviembre de 21.] http://es.wikipedia.org/wiki/Orkut.

17. **ALEXA;.** rankings. Retrieved July 17, 2006 from:. [En línea] 2006. [Citado el: 2009 de Noviembre de 16.] http://alexa.com.

18. **TENDENCIAS DIGITALES;.** Investigación y Análisis de Mercados en Internet - Redes Sociales . [En línea] [Citado el: 2009 de Noviembre de 17.] www.tendenciasdigitales.com.

19. **ENLACE DIGITAL;.** Crecimiento de usuarios de Facebook en Argentina. [En línea] [Citado el: 2009 de Noviembre de 17.] http://enlacedigital.com.ar/i/la-comunidad-facebook-argentina-paso-los-6-millones.

20. **FACEBOOK, INSIDE.** Colombia supera los 5 millones de usuarios en Facebook. [En línea] [Citado el: 2009 de Noviembre de 17.] http://es.insidefacebook.com/2009/05/08/colombia-supera-los-5-millonesde-usuarios-en-facebook/.

21. **FASTRACKMEDIA;.** Estadisticas de Redes Sociales online en América Latina 2009. [En línea] [Citado el: 2009 de Noviembre de 17.] http://spanish.fastrackmedia.com/blog/post/estadisticas-de-redessociales-online-en-america-latina-2009/.

22. **WSI;.** Social Media Threndes Report 2009. [En línea] [Citado el: 2009 de Diciembre de 4.] http://s3.amazonaws.com/ppt-download/wsisocialmediatrendsreport20091-12614106186407-phpapp02.pdf?Signature=JT7FwmAVe1zMHAFgIst%2BiOo1aV4%3D&Expires=1284066885&AWSAccessKeyId=AKIAJLJT267DEGKZDHEQ.

23. **GERENCIAL FORMACIÓN;.** Estadísticas de Facebook en Ecuador. [En línea] [Citado el: 2009 de Noviembre de 24.] http://blog.formaciongerencial.com/tag/facebook-ecuador/.

24. **INCOM;.** Estadisticas de Audiencia de Facebook en Ecuador. [En línea] [Citado el: 2009 de Noviembre de 17.] http://incom.ec.

25. **HI5;.** Política de Privacidad. [En línea] [Citado el: 2009 de Noviembre de 19.] http://www.hi5.com/friend/displayPrivacy.do.

26. **KIRKPATRICK, Marshall.** Facebook's Zuckerberg Says The Age of Privacy is Over. [En línea] [Citado el: 2009 de Noviembre de 27.]

http://www.readwriteweb.com/archives/facebooks_zuckerberg_says_the_age_of_privacy_is_ov.php.

27. **FACEBOOK;.** Guía Sobre la Privacidad de Facebook. [En línea] [Citado el: 2009 de Noviembre de 29.] http://www.facebook.com/privacy/explanation.php.

28. **SONICO;.** El mercado de Internet en Latam. [En línea] [Citado el: 2009 de Noviembre de 30.] http://www.iab.com.uy/imagenes/ul/arch/presentacinsocialmedia.pdf.

29. **SONICO, CORPORACIÓN.** Acerca de Sonico. [En línea] [Citado el: 2009 de Diciembre de 2.] http://corporate.sonico.com/evento12_12_2008/acerca_de_sonico.pdf.

30. **SONICO;.** Privado Público Profesional. [En línea] [Citado el: 2009 de Diciembre de 3.] http://es.blog.sonico.com/desarrollo/privado-publico-profesional/.

31. **HOY TECNOLOGÍA;.** Facebook publica por defecto toda la información del usuario en Google y Bing. [En línea] [Citado el: 2009 de Diciembre de 4.] http://www.hoytecnologia.com/noticias/Facebook-publica-defecto-toda/145102.

32. **MELANSON, Mike.** Google Takes First Shot at Facebook Search Results. [En línea] [Citado el: 2009 de Diciembre de 4.] http://www.readwriteweb.com/archives/google_takes_first_shot_at_facebook_search_results.php.

33. **SANTO TOMAS, Escuela superior de Comercio y Administración.** Web Beacons, México D. F. Julio 2008. [En línea] [Citado el: 2009 de Diciembre de 4.] http://itzamna.bnct.ipn.mx:8080/dspace/bitstream/123456789/2812/1/LRC2008G633m.pdf.

34. **ARMELANI, Guillermo y VILLANUEVA, Julian.** En las Redes Sociales, el Anuncio eres tu. Universidad de navarra. [En línea] [Citado el: 2009 de Diciembre de 4.] http://www.iese.edu/es/files/Art_Villanueva_Armelini_Facebook_redes_sociales_Esp_tcm5-7158.pdf.

35. **BORGHELLO, Cristian.** Technical & Educational Manager, Eset LAtinoamérica, Phishing en Redes Sociales, Facebook y Hi5. [En línea] [Citado el: 2009 de Diciembre de 10.] http://www.eset-la.com/company/1773-phishing-redes-sociales-facebook-hi5.

36. **SOPHOS;.** Security Threat Report: 2010. [En línea] [Citado el: 2009 de Diciembre de 17.] http://www.sophos.com/sophos/docs/eng/papers/sophos-security-threat-report-jan-2010-wpna.pdf.

37. **WATCHGUARD;.** Las 10 principales amenazas a la seguridad de los datos de las PyMEs. [En línea] [Citado el: 2009 de Diciembre de 20.] http://www.watchguard.com/infocenter/whitepapers/top10threats.asp.

38. **MITNICK, Kevin;.** Ingeniería Social. [En línea] [Citado el: 2009 de Diciembre de 26.] http://www.kevinmitnick.com/.

39. **SPAMFIGHTER;.** Facebook has a Deluge of Malicious Profiles. [En línea] [Citado el: 2009 de Diciembre de 21.] http://www.spamfighter.com/News-11092-Facebook-has-a-Deluge-of-Malicious-Profiles.htm.

40. **PETRE, George Lucian ;.** Facebook – Another breach in the wall. [En línea] [Citado el: 2009 de Diciembre de 22.] http://download.bitdefender.com/resources/files/Main/file/fb-another_breach_in_the_wall.pdf.

41. **EL SEMANARIO;.** Secuestro a través de Redes Sociales. [En línea] [Citado el: 2009 de Diciembre de 23.] http://www.elsemanario.com.mx/news/news_display.php?story_id=9679.

42. **RAMIREZ SARAS, Jose Andres.** Resporte de secuestro a trvés de engaños por Hi5. [En línea] [Citado el: 2009 de Diciembre de 23.] http://ja-jp.facebook.com/topic.php?uid=82174001269&topic=10114.

43. **WIESENTHAL;.** Ataques a traves de Redes Sociales. [En línea] [Citado el: 2010 de Enero de 2.] http://www.wiesenthal.com/atf/cf/%7B54d385e6-f1b9-4e9f-8e94-890c3e6dd277%7D/NY-RELEASE.PDF.

44. **EL INFORMADOR.** Amenazan de muerte por facebook a hijo de Álvaro Uribe. [En línea] [Citado el: 2009 de Enero de 3.] http://www.informador.com.mx/internacional/2009/119192/6/amenazan-de-muerte-por-facebook-a-hijo-de-alvaro-uribe.htm.

45. **FACEBOOK.** Página de Facebook: No soporto a Jorge Ortiz. [En línea] [Citado el: 2010 de Enero de 4.] http://www.facebook.com/pages/No-soporto-a-Jorge-Ortiz/141422812542?ref=sgm.

46. **FACEBOOK;.** Página de Facebook: Ecuador declara persona no grata a Jaime Nebot. [En línea] [Citado el: 2010 de Enero de 16.] http://www.facebook.com/pages/Ecuador-declara-PERSONA-NO-GRATA-a-Jaime-NEBOT/302271179008?ref=sgm.

47. **FACEBOOK.** Página de Facebook: Odio las cadenas nacionales del Presidente. [En línea] [Citado el: 2010 de Enero de 12.] http://www.facebook.com/pages/ODIO-LAS-CADENAS-NACIONALES-DEL-PRESIDENTE/187502920786?ref=sgm.

48. **SONICO.** Dating. [En línea] [Citado el: 2009 de Enero de 19.] www.sonico.com.

49. **F-SECURE;.** Informe de virsus a traves de Redes Sociales. [En línea] [Citado el: 2010 de Enero de 27.] http://www.f-secure.com/weblog/archives/00001555.html.

50. **RSA, The Security Division of EMC.** Global Online Consumer Security Survey. http://www.rsa.com/products/consumer/whitepapers/10665_CSV_WP_1209_Global.pdf visitado

2010, 26 de Abril. [En línea] 2010. [Citado el: 2010 de Enero de 28.] http://latinamerica.rsa.com/press_release.aspx?id=10678.

51. **HERNANDEZ, Ma. Angeles y Fernandez, Ma. Solano.** Ciberbullying un problema de acosos escolar, Universidad de Murcia - España. [En línea] [Citado el: 2010 de Febrero de 12.] http://www.utpl.edu.ec/ried/images/pdfs/ciberbullyng.pdf.

52. **JAKOBSSO, Markus, JOHUNSON, Nathan y JAGATIC, Tom.** Social Phishing. A publicarse en Communications of the ACM. 3 de junio del 2006. [En línea] [Citado el: 2010 de Marzo de 3.] http://www.indiana.edu/%7Ephishing/social-network-experiment/phishing-preprint.pdf.

53. **BANK, David.** "'Spear Phishing' Tests Educate People About Online Scams", The Wall Street Journal, 17 de agosto de 2005. [En línea] [Citado el: 2009 de Marzo de 9.] http://online.wsj.com/public/article/0,,SB112424042313615131-z_8jLB2WkfcVtgdAWf6LRh733sg_20060817,00.html?mod=blogs/.

54. **SYMANTEC.** MessageLabs Intelligence, 2008 Anual Security Report visitado 2010, 26 de Abril. [En línea] [Citado el: 2010 de Marzo de 17.] http://www.messagelabs.com/download.get?filename=MLIReport_Annual_2008_FINAL.pdf.

55. **RSA, The Security Division of EMC.** Global Online Consumer Security Survey 2010. http://www.rsa.com/products/consumer/whitepapers/10665_CSV_WP_1209_Global.pdf visitado 2010, 26 de Abril. [En línea] [Citado el: 2010 de Marzo de 23.] http://latinamerica.rsa.com/press_release.aspx?id=10678.

56. **ITECUADOR.** Informacion sober tecnologia en el Ecuador y el mundo, Ciberdelincuencia en Ecuador, avanza sin parar. [En línea] [Citado el: 2010 de Marzo de 26.] http://www.itecuador.com/2009/09/ciberdelincuencia-en-ecuador-avanza-sin-parar/.

57. **VELAZCO, Alfredo.** INCOM. [En línea] [Citado el: 2010 de Marzo de 28.] www.incom.ec.

58. **FERNANDEZ SANGUINO, Javier.** Spam, Spam, Spam: Cómo evitarlo y combatirlo, Germinus XXI, Madrid, España. [En línea] [Citado el: 2010 de Marzo de 23.] https://webmail.unizar.es/desarrollo/Spamspam.pdf.

59. **EL MERCURIO.** Seguridad en Redes Sociales. [En línea] [Citado el: 2010 de Abril de 3.] http://diario.elmercurio.com/2008/06/16/ciencia_y_tecnologia/ciencia_y_tecnologia/noticias/D8E7C32B-02B9-42DA-9DDC-F586F07E852C.htm?id={D8E7C32B-02B9-42DA-9DDC-F586F07E852C}.

60. **DOMAINTOOL.** Whois ip. [En línea] [Citado el: 2010 de Abril de 23.] http://whois.domaintools.com/.

61. **FERGUSON, Isabel.** CnnExpansion, Como tu empresa puede aprovechar la web. [En línea] [Citado el: 2010 de Abril de 24.]

http://www.cnnexpansion.com/emprendedores/2010/02/03/como-tu-empresa-puede-aprovechar-la-web.

62. **PROFESIONAL, MANPOWER.** Redes sociales y empresa, Como aprovechar el poder de los medios sociales. [En línea] [Citado el: 2010 de Abril de 28.] https://candidate.manpower.com/wps/wcm/connect/5c540b00403efc13aa05bb662953cdfc/Social_Networking.pdf?MOD=AJPERES&CACHEID=5c540b00403efc13aa05bb662953cdfc.

63. **DELOITTE;.** us 2009 ethics workplace survey. [En línea] [Citado el: 2010 de Abril de 29.] http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/us_2009_ethics_workplace_survey_220509.pdf.

64. **BITDEFENDER.** El blindaje empresarial contra las amenazas tecnologicas. [En línea] [Citado el: 2010 de Abril de 30.] http://www.bitdefender.es/files/Main/file/Seguridad_Proactiva-El_blindaje_empresarial_contra_las_amenazas_tecnologicas.pdf.

65. **PROTEGELES.** Proteccion de Menores en la Red. [En línea] [Citado el: 2010 de Mayo de 2.] http://www.protegeles.com/es_que_hacemos2.asp.

66. **AEPD;.** Estudio sobre la Privacidad de los datos personales y la Seguridad en Redes Sociales en linea. [En línea] [Citado el: 2010 de Mayo de 12.] https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Estudios/est_inteco_redesso_022009.pdf.

67. **MUNDO, EL.** Protección de datos de caracter personal. [En línea] [Citado el: 2010 de Julio de 22.] http://www.madrid.org/cs/Satellite?c=CM_Noticia_FA&cid=1142581677939&esArticulo=true&idRevistaElegida=1142576007987&language=es&pag=1&pagename=RevistaDatosPersonales%2FPage%2Fhome_RDP&siteName=RevistaDatosPersonales.

68. **MEXICO, CNN.** Mexico podria ser elprimer pais en castigar el mal uso de las Redes Sociales. [En línea] [Citado el: 2010 de Junio de 15.] http://mexico.cnn.com/nacional/2010/06/15/mexico-podria-ser-el-primer-pais-en-castigar-el-mal-uso-de-redes-sociales México podría ser el primer país en castigar el mal uso de redes sociales.

69. **NAVARRO BRAIN, Alejandro.** Serandor de las Republica de Chile, Proyecto de ley que limita la utilización de Datos Personales “Sensibles” disponibles en las Redes Sociales Virtuales. [En línea] http://www.navarro.cl/?p=1628.

70. **ROMO, María Paula.** *Asambleista de la República del Ecuador paularomo@gmail.com http://www.facebook.com/pages/Maria-Paula-Romo/49013602595.* Quito : s.n., 2010.

73. **THREATINFO;.** KoobFaceMalware attack. [En línea] [Citado el: 2010 de Febrero de 23.] http://threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_KOOBFACE.DC.

74. **SOPHOS.** Stops new version of koobface worm. [En línea] [Citado el: 2010 de Febrero de 26.] http://www.sophos.com/blogs/gc/g/2009/03/02/sophos-stops-new-version-of-koobface-worm/.

13.GLOSARIO DE TÉRMINO

Usuario: Persona Natural o jurídica que se haya registrado a la Red Social,

Perfil de usuario.- Es el conjunto de datos, incluso de carácter personal, que los usuarios introducen en una Red Social.

Privacidad.- Derecho de los individuos a controlar e influir en el almacenamiento de datos relativos a ellos mismos.

Política de Privacidad.- Es una información en la que el prestador de servicios de la sociedad de la información da a conocer los procedimientos, medidas de seguridad, destino y finalidad de los datos de carácter personal que en su caso hayan sido aportados de forma voluntaria por el usuario.

Cookie.- Es un archivo de texto que los servidores web utilizan para identificar los usuarios que se conectan. Se almacena localmente en cada equipo, y cada vez que el usuario vuelve a visitar el sitio, esta vuelve a enviarse al servidor para identificarlo.

Microblogging – Es una forma simplificada de descubrir y compartir ideas con otros en la web 2.0. Se podría definir como una red mundial donde todos comparten ideas o frase cortas (140 carácteres máximo) de forma instantánea para su red de seguidores. Twitter.com fue el precursor y quien lo convirtió en un fenómeno.

Web 2.0 – Término que se refiere a la interacción del usuario con el contenido, siendo el usuario el generador principal de dicho contenido.

Correo electrónico.- (En inglés e-mail) Se basa en un sistema que permite enviar y recibir mensajes escritos a través de Internet a cualquier parte del mundo de forma instantánea, a uno ó más usuarios.

Contraseña.- (En inglés Password) Información confidencial, generalmente una cadena de caracteres que identifican a un usuario para su acceso a un sistema o a recursos de uso restringido.

E-learning.- es un sistema de educación electrónico o a distancia en el que se integra el uso de las tecnologías de la información y otros elementos pedagógicos (didácticos) para la formación, capacitación y enseñanza de los usuarios o estudiantes en línea.

Código malicioso.- (En inglés Malware) Software capaz de realizar un proceso no autorizado sobre un sistema con un deliberado propósito de ser perjudicial. Virus, gusanos, troyanos son algunos ejemplos de código malintencionado.

Hacker.- Persona que tiene unos conocimientos avanzados de la informática y redes; y que busca acceder por diversas vías a los sistemas informáticos pero con fines de protagonismo, aunque no necesariamente con malas intenciones.

Vulnerabilidad.- Fallos o huecos de seguridad detectados en algún programa o sistema informático, que los virus utilizan para propagarse e infectar.

Riesgo.- Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios.

Recurso.- Información que se encuentra en Internet.

Nombre de usuario.- (En inglés *Login Name*) Nombre que es requerido al acceder a una Red Social y que identifica al usuario.

Navegador.- (En inglés *Browser*) Es el programa que permite visualizar los contenidos de las páginas Web en Internet.

Ingeniería social.- Son técnicas basadas en engaños que se emplean para dirigir la conducta de una persona u obtener información sensible.

Offline.- Estado de un usuario cuando no está conectado a internet.

Dating.- Se refiere a cualquier actividad social realizada, por lo general, entre dos personas con el objeto de evaluar la idoneidad mutua como compañero o compañera en una relación íntima o de pareja

CSRF (Cross-Site Request Forgery).- es un fragmento de código malicioso de un sitio web en el que comandos no autorizados son transmitidos por un usuario en el cual el sitio web confía.

Koobface.- es un Gusano informático que ataca a usuarios de las redes sociales Facebook, MySpace, hi5, Bebo, Friendster y Twitter.

URL.- (Siglas en inglés *Uniform Resouce Locator*) Es una dirección que permite acceder a un archivo o recurso.

Tráfico.- Se refiere a la medida de la cantidad de usuarios que visitan un sitio y a la frecuencia de las visitas.

Ciberbullying.- Cuando un o una menor atormenta, amenaza, hostiga, humilla o molesta a otro/a mediante Internet, teléfonos móviles, consolas de juegos, Redes Sociales u otras tecnologías telemáticas.

Phishing.- Es la contracción de "password harvesting fishing" (cosecha y pesca de contraseñas). Consisten en el envío de correos electrónicos, con el objetivo de engañar al usuario y obtener información sensible.

Pornografía infantil.- Toda representación, por cualquier medio, de un niño dedicado a actividades sexuales explícitas, reales o simuladas, o toda representación de las partes genitales de un niño, con fines primordialmente sexuales

Correo basura.- (En inglés Spam) Todo tipo de comunicación no solicitada, realizada por vía electrónica, mediante mensajes no solicitados y que normalmente tiene el fin de ofertar, comercializar o tratar de despertar el interés respecto de un producto, servicio o empresa.

Spammer.- La persona o compañía que realiza el envío de Spam.

Términos de uso.- Condiciones que regulan las actividades desarrolladas en las redes sociales, establecidas por los prestadores del servicio.

Aplicaciones.- Programas instalados en las Redes Sociales

Indexación de contenidos.- Es el proceso que realizan los bots de los buscadores, por el cual extraen información relevante de las páginas a las que acceden, y la almacenan en la base de datos del buscador.

Bot - Programa encargado de rastrear e indexar contenidos en la web, utilizado por buscadores, por ejemplo, googlebot.

Audiencia.- El público que recibe mensajes a través de un medio de comunicación, como las Redes Sociales.

Información personal.- Se refiere a la información que puede usarse para identificar, contactar o localizar a una persona en concreto,

Contenidos.- Información general publicada en las Redes Sociales con diferentes formatos audio, video, enlaces.

14.ANEXOS

ANEXO A

Encuesta sobre incidencia de Redes Sociales en Loja

Encuesta sobre incidencia de las Redes Sociales en la ciudad de Loja
"SEGURIDAD DE REDES SOCIALES"

Edad……
Sexo Masculino ( ) Femenino ( )

¿Sabe lo que es una Red Social?
SI ( ) NO ( )

¿Utiliza Redes Sociales?
SI ( ) NO ( )

Marque las Redes Sociales en las que tiene cuenta
Hi5 ( )
Facebook ( )
MySpace ( )
Orkut ( )
Sonico ( )
Badoo ( )
Otro……..

Aproximadamente ¿Cuántos amigos tiene en su Red Social?
Menos de 100 ( )
De 100 a 200 ( )
De 200 a 300 ( )
Más de 300 ( )
Otro……..

¿Se ha unido a comunidades o grupos de amigos?
SI ( ) NO ( )

Con que Frecuencia utiliza las Redes Sociales
Cada día ( )
Varias veces por semana ( )
Al menos una vez a la semana ( )
Casi nunca ( )
Otro……..

¿Cuántas horas dedica a la semana a visitar las Redes Sociales?
Menos de 1 hora ( )
De 1 a 3 horas ( )
De 4 a 6 horas ( )
De 7 a 10 horas ( )
Más de 10 horas ( )

¿Qué actividades suele realizar en las Redes Sociales?
Ver fotos o videos ( )
Usar aplicaciones o juegos ( )
Subir fotos ( )
Enviar mensajes ( )
Relacionarte con amigos ( )
Buscar pareja ( )
Otro……..

Cuando usa las Redes Sociales ¿Desde dónde suele conectarse?
En casa ( )
En el trabajo ( )
Universidad/colegio ( )
Ciber Café ( )
Otro……

Cuando usa las Redes Sociales para relacionarse ¿Con quién se suele relacionar?
Amigos actuales ( )
Con amigos antiguos ( )
Con familiares ( )
Con compañeros de estudio ( )
Con compañeros de trabajo ( )
Con desconocidos ( )
Otro……..

¿Qué es lo que más le gusta de las Redes Sociales?
Estar en contacto con amigos/ familia ( )
Conocer gente ( )
Ver y comentar fotos de sus amigos ( )
La comunicación ( )
Reencontrarse con antiguos amigos/familia ( )
Otro……..

¿Qué es lo que menos le gusta de las Redes Sociales?
Falta de privacidad ( )
Nada/ todo me gusta ( )
Uso inmoral e ilegal de datos ( )
Publicidad ( )
Otro……..

ANEXO B

Configuraciones de Privacidad de Hi5

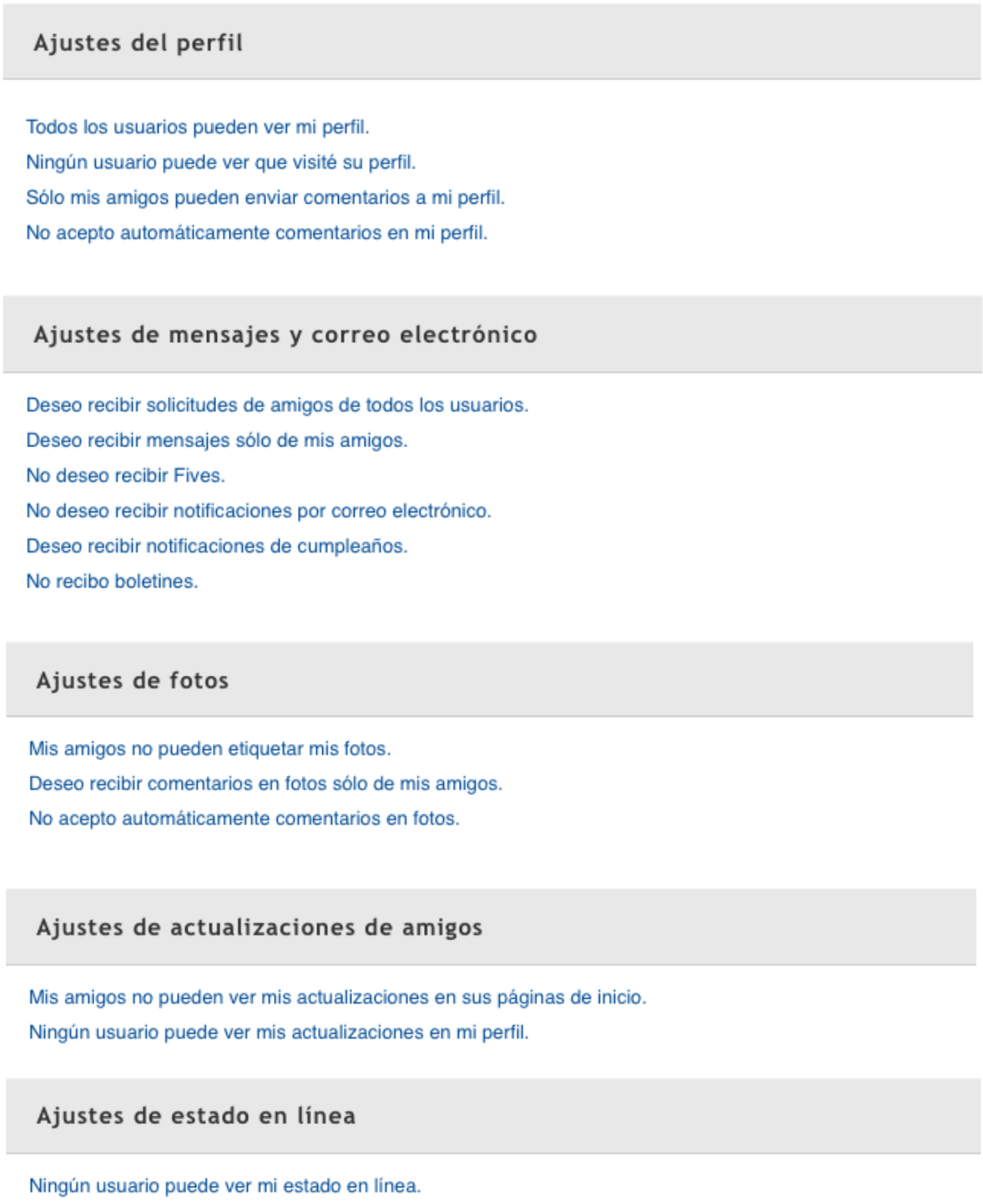

Figura 91. Configuraciones de Privacidad de Hi5

ANEXO C

Configuraciones de Privacidad de Facebook

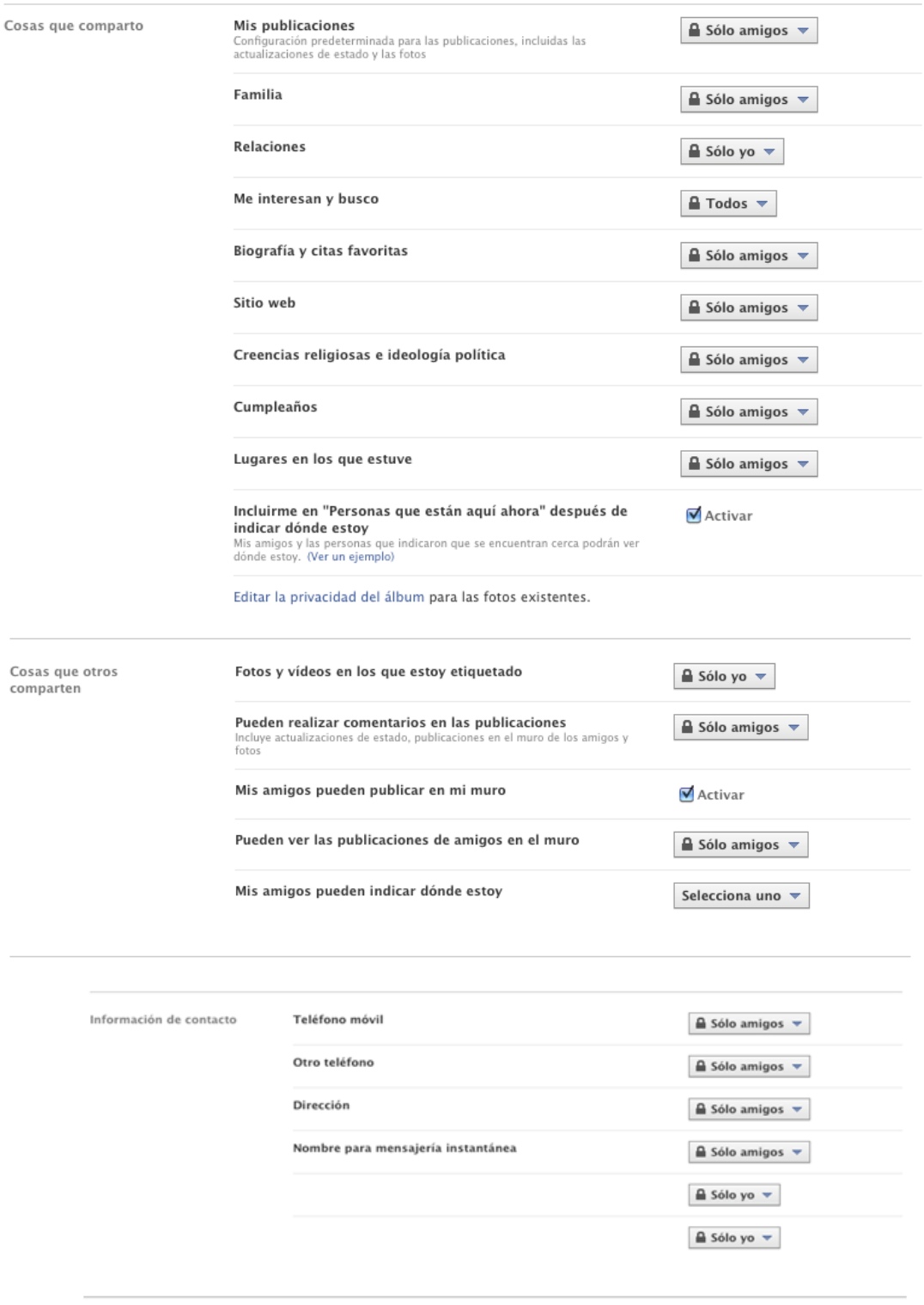

Figura 92. Configuraciones de Privacidad de Facebook

ANEXO D

Configuraciones de Privacidad de Sonico

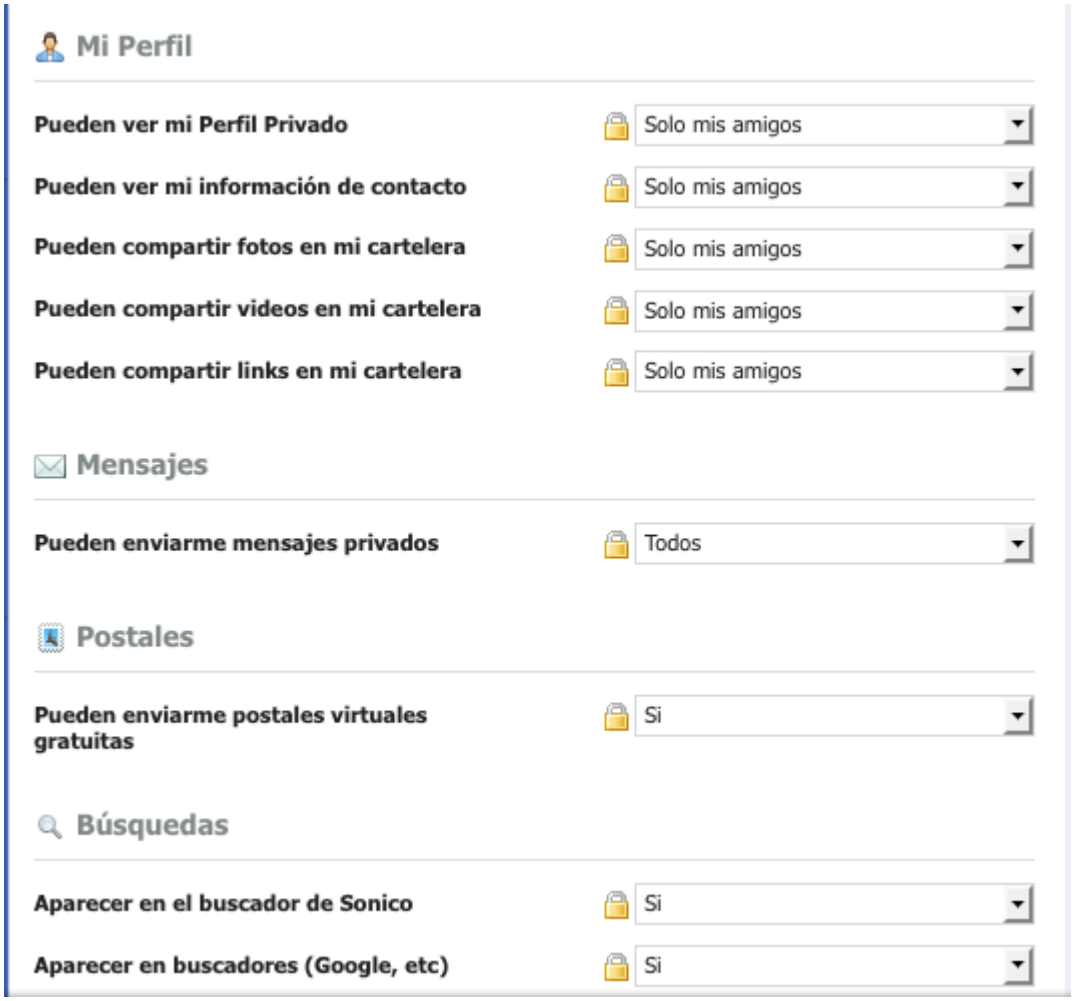

Figura 93. Configuraciones de Privacidad de Sonico

ANEXO E

Encuesta de Privacidad y Seguridad en Redes Sociales

Encuesta sobre Privacidad y Seguridad en Redes Sociales en la ciudad de Loja
"SEGURIDAD DE REDES SOCIALES"

Edad……

Sexo Masculino ( ) Femenino ( )

1. ¿Publicas datos reales en su Red Social?
SI ( ) NO ( )

¿Qué información muestra en su Perfil?
Nombre ( )
Apellido ( )
Ciudad ( )
Universidad ( )
Trabajo ( )
Cargo ( )
Email ( )
Ubicación Actual ( )
Nro. De celular ( )
Fotos suyas ( )
Fotos de amigos/familia ( )
Otro……..

2. ¿Teme por la seguridad de sus datos en su Red Social?
SI ( ) NO ( )

3. ¿Confía en la seguridad que proporciona su Red Social?
SI ( ) NO ( )

4. ¿**Sabía Ud. que al publicar su información en Redes Sociales puede poner en riesgo su integridad física?**
SI ( ) NO ( )

5. ¿Usa aplicaciones en su Red Social?
SI ( ) NO ( )

6. Si su respuesta es afirmativa, sabe Ud. que al usar aplicaciones en las Redes Sociales está proporcionando su información personal a los propietarios de la aplicación?
SI ( ) NO ( )

7. Una contraseña segura es aquella que tiene mínimo 8 caracteres mayúsculas, minúsculas e incluye números y símbolos ¿Considera que su contraseña es segura?
SI ( ) NO ( )

8. ¿Con que frecuencia acostumbra cambiar su contraseña?
Cada seis meses ( )
Al año ( )
Nunca ( )

9. ¿Ha sido amenazado o insultado a través de su Red Social?
SI ( ) NO ( )

10. ¿Ha configurado la privacidad de su perfil?
SI ( ) NO ( )

11. Si su respuesta es afirmativa. Qué tipo de configuración tiene aplicado respecto de su visibilidad
Mi perfil puede ser visto por cualquier usuario de la red social ( )

Mi perfil solo puede ser visto por mis amigos/contactos ( )

Mi perfil solo puede ser visto por algunos amigos/contactos ( )

No lo sé ( )

12. ¿Ha bloqueado algún usuario que Ud. cree que representa peligro?
SI ( ) NO ( )

13. ¿Ha aceptado invitaciones de amistad de desconocidos?
SI ( ) NO ( )

14. ¿Se ha citado con personas que ha conocido en su Red Social?
SI ( ) NO ( )

15. ¿Ha encontrado en su Red Social fotos suyas divulgadas sin su permiso?
SI ( ) NO ( )

16. Finalmente, ¿Qué opinión le merece la seguridad de su información personal?
Me preocupa ( )
Analizo la información que subo ( )
No me interesa ( )

ANEXO F

Propuesta de ley Chilena para legislación de Redes Sociales

PROYECTO DE LEY QUE LIMITA LA UTILIZACIÓN DE DATOS PERSONALES "SENSIBLES" DISPONIBLES EN LAS REDES SOCIALES VIRTUALES.

Fundamentos.

La creciente comunicación e interdependencia entre los distintos países y sus habitantes, como manifestación más irrefutable del fenómeno de la globalización, se produce a partir de las confluencias de una compleja serie de procesos sociales, políticos, económicos y culturales. Uno de esos fenómenos más trascendentes, es lo que se denomina "sociedad de la información". Los medios de generación de riqueza experimentaron sustanciales cambios a partir de las década de los ´70, eso es el trabajo ya no se dirigía exclusivamente a la producción de bienes corporales, sino que más bien, a la generación, recopilación almacenamiento y tratamiento de la información. Pero este nuevo fenómeno, no se agota y explica desde una perspectiva individual, ya que el manejo de la información también es necesario para el "bien común", pues todos somos los beneficiados con el aumento de conocimiento sobre el medio en que se desarrolla la comunidad.

A la luz de esta óptica, cobra mayor sentido indicar que, sólo en la medida en que la información esté al alcance de todos y no de unos pocos, más democrática será nuestra sociedad, pero surge una interrogante insoslayable, y viene dada si acaso ¿toda la información puede estar a disposición de todos?, y si acaso ¿cualquier persona puede llevar a cabo el tratamiento de cualquier dato personal, para los más diversos fines?, a la luz del constitucionalismo moderno y de la consagración de ciertas garantías constitucionales, ambas respuestas debieran ser negativas, por lo que la intervención del derecho se trona de imperiosa necesidad para venir a regular este tipo de materias a través de las "normas sobre protección de datos".

Esta nueva disciplina tiene un desarrollo histórico en Europa y Estados Unidos, los que no obstante tener sistemas de protección, doctrinariamente diferentes, ambas fuentes tratan con rigurosidad, sopesando la importancia de esta nueva proyección de la dignidad humana a través de la red: la nueva subjetividad virtual.

A diferencia de lo que ocurre con Colombia, Brasil, Uruguay, Argentina, entre otros países latinoamericanos, Chile no consagra constitucionalmente un derecho fundamental destinado a consagrar el derecho a la protección de datos. En efecto, la Constitución de Chile reconoce en su artículo 19, el derecho a la privacidad ("La Constitución asegura a todas las personas: (…) 4º.- El respeto y protección a la vida privada y a la honra de la persona y su familia;"). A diferencia de otros países de la región, no tiene una acción de Habeas Data, ni tampoco la garantía constitucional de libre acceso a los datos personales. Chile aprobó en 1999 la primera ley sobre protección de datos de un país latinoamericano, la Ley N º 19.628. Aunque inspirada en modelos europeos (en particular las leyes de Francia y España), la ley no prevé algunas instituciones que son esenciales en el modelo europeo de protección de datos. No cuenta, por ejemplo, con un registro central de bases de datos personales operativas, no prevé un órgano administrativo para su aplicación, no prevé el principio de finalidad y no establece procedimientos administrativos para que el titular de los datos haga valer sus derechos. Además de estas características que separan el sistema chileno de protección de datos del modelo europeo, e incluso de los últimos desarrollos en América Latina, como la legislación argentina, la ley uruguaya, e incluso el proyecto de ley de brasileño, su característica de ley general se ve ligeramente comprometida por su vocación de cubrir básicamente casos relacionados con el sector financiero. Recientemente se elaboró un proyecto de ley que introduce cambios en la Ley 19.628 y también en la Ley 20.285 (Ley de acceso a la información pública). En virtud de este proyecto, el Consejo de la Transparencia puede recibir atribuciones de autoridad de control, con el fin de velar por la aplicación de la ley.

Asimismo, la necesidad de reformar la ley Chilena se puede reagrupar en las siguientes razones:

1.- Inexistencia de un órgano de control, que obliga a los particulares a recurrir a Tribunales de Justicia, lo que significa necesariamente alto costo a los afectados.
2.- Dificultad de la responsabilidad por culpa, que pone de cargo del afectado la carga de la prueba de la culpa. Una misión casi imposible.
3.- Inexistencia de un registro de bases de datos privadas, lo que dificulta el ejercicio de los derechos.
4.- Multas y un catálogo sancionatorio ineficaz.

El principal cuerpo normativo en la materia en Chile está dado por la ley 19.628, frente a la cual podemos deslizar lagunas críticas; así, la ley referida no propende a un equilibrio entre la información que poseen lo actores en el tratamiento de datos personales, ya que sólo existe un registro de daros públicos y este ni siquiera es completo, lo que lleva a que los titulares de los datos personales desconozcan quien trata su información y cómo lo hace. Además el titular de los datos no participa en ninguna de las etapas del proceso de comunicación de sus datos a terceros distintos del responsable del registro (mercado secundario), lo que aumenta la asimetría de información, asimismo, no existe un reconocimiento que valide a los códigos deontológicos o de conducta como complemento de la legislación sobre protección de datos personales. No existe regulación respecto a la y transferencia transfronteriza de datos, lo que hace que nuestro país no cumpla en esta parte con los estándares internacionales. El régimen de sanciones es irrisorio frente a las infracciones a la norma, las que no incentivan a su cumplimiento. También la Ley 19628, mantiene el monopolio legal a favor de la CCS respecto de los datos patrimoniales.

Frente a este diagnóstico de falencia de nuestro ordenamiento jurídico en materia de protección de datos personales, debemos hacer frente a una especial manera de interacción social, en que fluyen miles de datos persona y que está dado por las nuevas redes sociales virtuales. Plataformas como Facebook, Youtube, Twitter, sirven para el intercambio de ideas, gustos, reflexiones, experiencia, es decir abren una nueva forma de socializar. Con todas las falencia de nuestra legislación , claramente no existe norma alguna referida a las redes sociales, las que día a día se utilizan para los más diversos fines, toda vez que por ellas circula información utilizable en materia política, religiosa, de salud y como no, laboral. A través de plataformas como Facebook, se puede tener acceso a datos sensibles, que permitan conocer perfiles de personas en sus más diversos aspectos, inclusive aquellos relacionados con la esfera íntima de cada sujeto, así , con la popularidad de la red Facebook, miles de personas, pueden tener información de otras miles de personas.

La realidad normativa europea nos señala que el Grupo de Trabajo del artículo 29 (GT29), órgano consultivo europeo independiente establecido en virtud de la Directiva 95/46/CE, adoptó el 12 de junio de 2009 la Opinión 5/2009, sobre las redes sociales en línea. Este documento se centra en cómo el funcionamiento de los servicios de redes sociales (SRS) puede satisfacer los requisitos de la legislación sobre protección de datos de la Unión

Europea. En particular, en el documento se destaca cómo muchos usuarios de las redes sociales se mueven dentro de una esfera puramente personal, poniéndose en contacto con gente como parte de la gestión de sus asuntos personales, familiar eso domésticos. Según destaca el GT29, la citada Directiva no impone las obligaciones de un responsable de datos a un individuo que procesa datos personales "en el transcurso de actividades estrictamente personales o Recordatorio: las opciones de restablecimiento de contraseña, unidas a una imprescindible concienciación conducían a otorgar un adecuado nivel de seguridad al acceso por parte de los usuarios. Principios básicos de la Protección de Datos 22domésticas". Siguiendo este precepto, el GT29 estima que, con carácter general, en la mayor parte de las actividades realizadas por los usuarios de un SRS debe aplicarse lo que denomina "exención doméstica", en lugar de la normativa de protección de datos.

Ahora bien, en la Opinión se especifican así mismo tres supuestos en los que tales actividades no estarían cubiertas por la "exención doméstica". **El primer supuesto se refiere a los casos en los que se utiliza el SRS como plataforma de colaboración para una asociación o una empresa. Si un usuario de SRS actúa en nombre de una sociedad o asociación, o utiliza el SRS principalmente como una plataforma para conseguir objetivos comerciales, políticos o benéficos, la exención no se aplica.** En este caso, el usuario asume todas las obligaciones de un responsable de datos que está revelando datos personales a otro responsable de datos (el SRS) y a terceros (otros usuarios del SRS o, potencialmente, otros responsables de datos con acceso a los mismos). En estas circunstancias, el usuario necesita el consentimiento de las personas concernidas o algún otro fundamento legítimo dispuesto en la Directiva de Protección de Datos. El GT29 expone que los prestadores del SRS deben garantizar la instauración de configuraciones por defecto gratuitas y que respeten la privacidad, restringiendo el acceso a los contactos seleccionados. En estas condiciones, cuando el acceso a la información del perfil se amplia hasta más allá de los contactos seleccionados, por ejemplo cuando se facilita el acceso al perfil a todos los miembros del SRS o cuando los datos son indexables por motores de búsqueda, el acceso desborda la esfera personal o doméstica. De igual manera, si un usuario toma una decisión informada de ampliar el acceso más allá de los "amigos" seleccionados, las responsabilidades inherentes a un responsable de datos se activan.

Efectivamente, se aplicará el mismo régimen legal que cuando cualquier persona utiliza otras plataformas tecnológicas para divulgar datos personales en Internet. En varios Estados Miembros, la falta de restricciones de acceso (y así el carácter público) significa que la Directiva de Protección de Datos se aplica en el sentido de que el usuario de internet adquiere responsabilidades de un responsable de datos. No obstante, el GT29 hace constar que, aunque la exención doméstica no se aplique, el usuario de SRS puede beneficiarse de otras exenciones como la exención con fines periodísticos o de expresión literaria o artística. En dichos casos, se ha de llegar aun equilibrio entre la libertad de expresión y el derecho a la privacidad

Finalmente, el GT29 aborda un tercer escenario en que la "exención doméstica" no sería aplicable. Se trata de aquellos supuestos en los que es preciso garantizar los derechos de terceros, particularmente en relación con datos sensibles. No obstante se hace constar que, aun cuando se aplique la "exención doméstica", un usuario podría ser responsable de acuerdo con las disposiciones generales de la legislación civil o penal nacional en cuestión (por ejemplo, por difamación, responsabilidad civil extracontractual por suplantación de personalidad, responsabilidad penal). **En la Opinión se aclara el concepto de "datos sensibles". Así, los datos que revelan el origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, la pertenencia a un sindicato o datos relativos a la salud o a la vida sexual se consideran sensibles. Los datos personales sensibles solo se pueden publicar en Internet con el consentimiento explícito del sujeto de datos o si el sujeto de datos ha hecho que los datos sean manifiestamente públicos él mismo**. El GT29 expone que en algunos Estados Miembros de la UE, las imágenes de los sujetos de datos consideran una categoría especial de datos personales, ya que se pueden utilizar para distinguir entre orígenes raciales/étnicos o pueden utilizarse para deducir las creencias religiosas o los datos sobre la salud. El GT29, en general, no considera que las imágenes en Internet sean datos sensibles, a menos que éstas se utilicen claramente para revelar datos sensibles acerca de los individuos.

En consecuencia, de conformidad con el criterio interpretativo mantenido por elGT29, es preciso que concurra alguno de los escenarios expuestos, en los que la "exención doméstica" no resulta de aplicación, para que sean aplicables los requisitos previstos en la LOPD.

De lo anterior se colige que si en Chile existiera una legislación adecuada, podría utilizarse libremente las redes sociales, pero con la seguridad de que cuando esos datos, dejan de ser “domésticos” y son utilizados con fines comerciales, o para tratar datos sensibles referidos a la salud, afiliación política, laboral etc, se aplicaría la norma sobre protección.

La red FACEBOOK que tiene más de 400 millones de usuarios, ha estado en tela de juicio en el último tiempo, por las débiles medidas de seguridad para resguardar la privacidad de los usuarios, así el mismo Mark Zuckerberg, admitiera que habían cometido errores en relación a los estatutos de privacidad, diciendo en una carta publicada en el Washington post que: "El mensaje que más hemos oído últimamente es que las personas quieren controlar sus datos más fácilmente. En pocas palabras, muchos de ustedes creían que nuestros controles eran demasiado complejos. Nuestra intención era ofreceros controles detallados (...). Nos equivocamos”

La preocupación generalizada surge tras la última política de privacidad dada a conocer por la empresa en abril 2010, donde los usuarios percibían que se estaban exponiendo muchos datos personales y que los controles para filtrarlos eran demasiado complejos.

Las pocas herramientas de privacidad ha dado lugar a prácticas como la de una **empresa francesa decidió terminar el contrato de funcionarios pues califican su conversación como "un acto que incita a la rebeldía".**

El caso se trató de tres empleados de la empresa francesa Alten que fueron despedidos después que un cuarto, también funcionario y contacto de uno de los involucrados, diera cuenta de una conversación donde hablaban mal de los jefes.

Los tres ex empleados de Alten conversaban por el muro de la red social, fuera del horario laboral, cuando a uno de ellos se le ocurrió referirse a sus jefes como el "club de los nefastos". Esta frase fue enarbolada por Alten como "un llamado a la rebeldía" dentro de sus instalaciones, por lo cual decidió terminar el contrato de los implicados. Uno de ellos llegó a un acuerdo económico contra la empresa, mientras que los otros dos

decidieron entablar un juicio laboral. Sus abogados argumentan que se trataba de una conversación privada entre amigos, y que ésta no causó ningún perjuicio a la empresa.

Chile es uno de los países con más usuarios de Facebook de América Latina, así lo reflejó un estudio realizado por la Universidad Bernardo O´Higgins en Mayo de 2010, titulada "Exposición electrónica de adolescentes en redes sociales Chile 2010", arrojó algunas cifras alarmantes; así un 93,33% de los usuarios permiten que cualquier persona la agregue como amigo, frente a un 3,67% que no lo hace, un 31,83% de los usuarios hace pública fotografías. Si coordinamos solamente los datos anteriores, significa que un altísimo porcentaje permite que lo agreguen como amigo, de modo que basta con confirmar esa solicitud y se tendrá acceso a las fotos e información personal de los usuarios.

El presente proyecto de ley tiene por objeto, contribuir a evitar la utilización arbitraria de datos personales presentes en redes sociales dentro de un contexto doméstico y privado, específicamente con una finalidad laboral perjudicial o persecutoria para el trabajador, que afecte la dignidad del trabajador, o con la finalidad de descontextualizar la utilización de datos sensibles de las personas, tales como sus datos de salud, afiliación política, o religiosa, racial, etc.

PROYECTO DE LEY

Artículo único: Incorpórese a la Ley 19.628 sobre protección de la vida privada el siguiente artículo 2 bis nuevo: "Los datos personales de carácter sensibles de una persona, según lo prescrito en la letra g) del artículo 2 de esta ley, disponibles en redes sociales en Internet, no podrán ser utilizados por terceras personas, para otros fines, más que para aquellos, que dentro del contexto doméstico o socializador de la red social, sean utilizados o estén disponibles, a menos que cuente con el consentimiento expreso del su titular según lo prescrito en el artículo 4 de la presente ley.

Así, los datos que un empleador recabe de sus trabajadores de una red social, no podrá utilizarlos como causal de despido, ni los datos sobre la salud de una persona ser utilizados para ofrecer planes de salud por parte de una empresa.

La inobservancia de lo dispuesto en este artículo hará aplicable las sanciones previstas, en el artículo V de esta ley.

ALEJANDRO NAVARRO BRAIN

SENADOR