

DISPOSITIVOS MÓVILES, REDES SOCIALES Y LA SEGURIDAD DE LA INFORMACIÓN

Atuesta Quitian Vladimir.
Universidad Piloto de Colombia
Vladimir.atuesta@gmail.com

Resumen—Este artículo presenta una introducción a los peligros y riesgos derivados de la constante utilización y masificación de los dispositivos móviles y la utilización de redes sociales en las actividades diarias.

La razón para escribir acerca de este tema es la falta de conciencia, medidas de seguridad y abuso de parte de los proveedores de servicio de datos y de las aplicaciones utilizadas para la gestión de las redes sociales.

Índice de Términos— Datos personales, Dispositivo Móvil, Red Social, Smartphone, Tablet, Wi-Fi.

I. INTRODUCCIÓN.

Debido al exponencial incremento en la compra y utilización de dispositivos móviles a nivel mundial y el acceso a internet a través de conexiones de datos móviles, la información manejada en los dispositivos, y las aplicaciones utilizadas en estos, es vulnerable a distintos tipos de ataques para la recolección, divulgación, robo por acceso y/o a través de aplicaciones basadas en el requerimiento de permisos por parte de los usuarios, con los que logran controlar los mismos y controlar en su totalidad el dispositivo de las víctimas. El auge que ha tomado el valor de los datos personales para beneficio propio, el incremento de conexiones a internet y la inadecuada utilización de los dispositivos y servicios son el motivo principal para que la información personal y en general la

almacenada y accedida desde los dispositivos móviles y las redes sociales sean blanco de los ataques y sea el principal objetivo a nivel mundial de los delincuentes informáticos, de las empresas dueñas de las redes sociales y en general de personas que tengan el conocimiento para saber el valor de la información y el uso que se le puede dar en la actualidad.

Hoy en día la información revelada por la población sin control alguno, y la tecnología en las organizaciones actuales y la criticidad de la fidelidad, integridad, disponibilidad y confidencialidad de la información, han surgido y evolucionado técnicas que permiten acceder a dicha información de manera ilegítima o por simple aceptación del usuario, en el primer caso por medio de la explotación de vulnerabilidades o debilidades de las plataformas tecnológicas, y en el segundo por la falta de conciencia, ignorancia o simplemente por necesidad para tener acceso a algún recurso o información.

II. INTERNET MÓVILES Y SU INCREMENTO EN EL MUNDO

A. Definición.

Esta tecnología permite obtener internet en cualquier lugar y momento, siempre que se disponga de cobertura móvil por parte del proveedor del servicio, La UIT (Unión Internacional de Telecomunicaciones) es el organismo especializado de las Naciones Unidas para las tecnologías de la información y la comunicación – TIC [01], [01] es la encargada de atribuir el espectro radioeléctrico y las órbitas de satélite a escala mundial, esta organización realiza

informes estadísticos de las conexiones, accesos y otros factores que ayudan con la visión global para analizar lo plateado en este artículo.

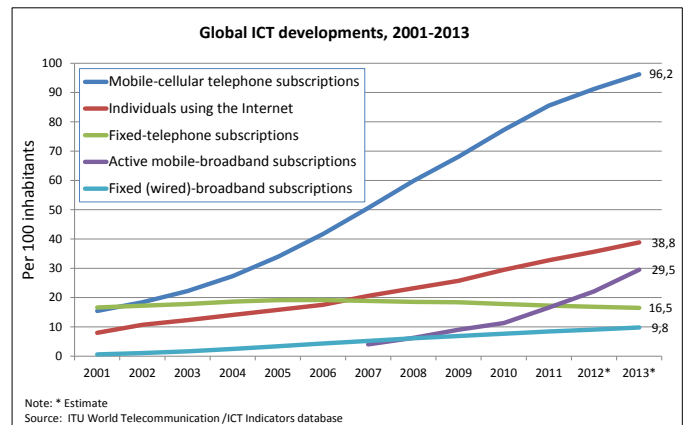
El internet móvil en el mundo ha tenido una evolución significativa y creciente año tras año, en febrero de 2013 una publicación de [1] indica que “La banda ancha móvil es el mercado más dinámico, con 2 100 millones de abonados en todo el mundo”, la tabla I muestra el aumento de las suscripciones de telefonía celular en tres (3) países del mundo, en Colombia el aumento de las suscripciones a la telefonía móvil celular desde el año 2000 hasta el año 2012 ha sido del 2174%, lo cual indica que existen más suscripciones en el país que habitantes en Colombia, según datos del Departamento Administrativo Nacional de Estadística DANE[2] para el año 2014 (47.433.662).

TABLA 1.
SUSCRIPCIONES TELEFONÍA MÓVIL [1]

<i>Mobile-cellular telephone subscriptions</i>			
<i>Año</i>	<i>Colombia</i>	<i>United States</i>	<i>Russia</i>
2000	2'256'801	109'478'031	3'263'200
2001	3'265'261	128'500'000	7'750'499
2002	4'596'594	141'800'000	17'608'756
2003	6'186'206	160'637'000	36'135'135
2004	10'400'578	184'819'000	73'722'222
2005	21'849'993	203'700'000	120'000'000
2006	29'762'715	229'600'000	150'674'000
2007	33'941'118	249'300'000	171'200'000
2008	41'364'753	261'300'000	199'522'340
2009	42'159'613	274'283'000	230'050'000
2010	44'477'653	285'118'000	237'689'224
2011	46'200'421	298'281'000	256'116'581
2012	49'066'359	303'052'000	261'887'751

Estos datos indican el exponencial crecimiento en la suscripción al servicio de telefonía móvil y la importancia que tiene este tipo de comunicación para el desarrollo de las actividades de las personas en todo el mundo. En la siguiente imagen se muestra un estadístico realizado por [1] a nivel mundial de las conexiones por cada 100 habitantes por tipo de conexión.

Figura 1.
EVOLUCIÓN MUNDIAL POR TIPO DE CONEXIÓN [3]



III. DISPOSITIVOS MÓVILES Y REDES SOCIALES EN LA EMPRESA

La necesidad de compartir la información por parte de los usuarios, ha crecido al tiempo que la tecnología. Como lo ha sido el uso de las redes sociales en las actividades diarias, ya sea para facilitar, acelerar o por distracción en un momento del día.

Pero este aumento de uso de las redes sociales, es debido a la creciente utilización de los dispositivos móviles en los usuarios y la cantidad de conexiones móviles como ya vimos anteriormente. Es esta la gran preocupación de las empresas al momento de garantizar la seguridad de la información.

Normalmente el envío o intercambio de información de la empresa, se realiza mediante dispositivos móviles, como lo son, computadores portátiles, Smartphone, tablets ya sean personales o de la institución. Lo que preocupa es que esta información que se intercambia no es eliminada de los dispositivos personales, de esta forma puede ser robada, ya que los controles de seguridad en estos dispositivos no es igual a los que pertenecen a las empresa.

Esto se debe la mayoría de veces a los empleados, los cuales muchas veces por desconocimiento o falta de capacitación, entre otras malas prácticas en la navegación la seguridad de la información se ve expuesta.

Es por esto que las empresas deben educar a sus empleados en el uso de los dispositivos móviles y redes sociales, generando conciencia en lo vulnerables que son y las pérdidas que pueden generar para la empresa. Como también creando políticas de uso (definir qué clase de información puede manipular los empleados a través de que dispositivos) y compromisos por parte de ellos. Esto debido a que el uso de estos cada día va ser mayor y cada vez más difícil de frenar o evitar.

IV. AUMENTO DE LA TASA DE PENETRACIÓN DE LAS CONEXIONES MÓVILES

Según la base de datos de la reglamentación mundial de las telecomunicaciones/TIC, el crecimiento de uso de banda de ancha en conexiones móviles cada vez va ser mayor.

Figura 2

AUMENTO DE TASA DE PENETRACIÓN SEGÚN UIT [01].

Recuadro 1: Aumento de la tasa de penetración de las conexiones móviles de banda ancha en países con una tasa elevada de penetración de las conexiones fijas de banda ancha, 2009-2011

En el Cuadro que figura a continuación se observa la evolución de la tasa de penetración de las conexiones fijas y móviles de banda ancha en ciertos países que han tenido en 2009 la tasa de penetración de las conexiones fijas de banda ancha más elevada. Estas cifras indican que, incluso en países con servicios fijos de banda ancha bien afianzados, y un grado de aceptación elevado, las conexiones móviles de banda ancha aumentan de forma espectacular, registrándose tasas medias de crecimiento de alrededor del 26% entre 2010 y 2011, en comparación con un crecimiento del 3% en la tasa de penetración de las conexiones fijas de banda ancha durante el mismo periodo. En promedio, en esos países, hay 56,7 conexiones móviles y 34 conexiones fijas de banda ancha por cada 100 habitantes.

País	Conexiones fijas de banda ancha por cada 100 habitantes		Crecimiento 2010-11	Conexiones móviles de banda ancha por cada 100 habitantes		Crecimiento 2010-11
	2009	2011		2009	2011	
Países Bajos	37.01	38.74	2%	N/A	49.19	29%
Dinamarca	36.94	38.21	1%	29.61	80.24	26%
Suiza	35.94	39.20	3%	25.32	36.07	17%
Noruega	34.52	36.55	4%	11.12	24.37	26%
República de Corea	34.08	36.91	3%	88.93	105.05	7%
Francia	31.87	36.12	6%	30.44	43.96	20%
Suecia	31.59	31.77	0%	69.91	91.55	10%
Luxemburgo	31.37	32.90	-1%	N/A	66.67	9%
Canadá	30.51	32.02	7%	N/A	32.91	8%
Alemania	30.21	32.47	2%	23.06	34.81	35%
Reino Unido	29.56	32.74	6%	36.98	62.27	44%
Bélgica	29.40	32.95	5%	5.77	19.35	99%
Hong Kong	28.95	31.54	5%	33.89	51.84	33%
China						
Finlandia	28.71	29.50	1%	71.29	87.10	3%
Estados Unidos	25.69	28.75	4%	39.81	65.48	24%

Fuente: UIT, Base de datos de la reglamentación mundial de las telecomunicaciones/TIC, www.itu.int/icteye

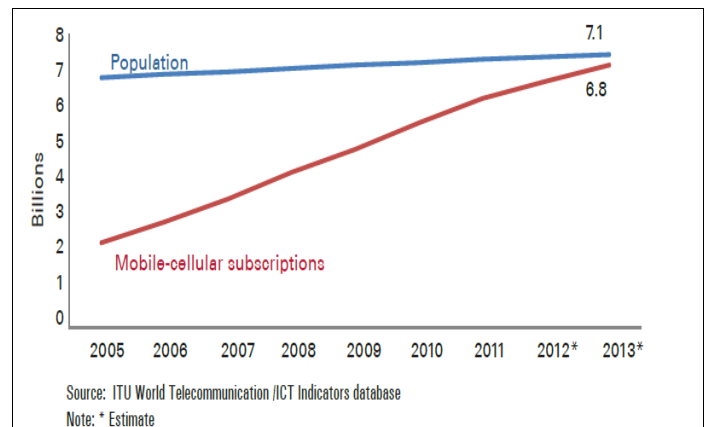
- La banda ancha móvil es el mercado más dinámico, con 2 100 millones de abonados en todo el mundo [3].

De acuerdo el informe de la UIT The World in 2013: ICT Facts and Figures, pronto existirá tecnología móvil celular como habitantes tiene el planeta, y se prevé que la cifra rebasará los siete mil millones a principios de 2014. La mayoría residen en Asia, región que sigue siendo el motor de crecimiento del mercado. A finales de 2013 el índice de penetración móvil global habrá alcanzado el 96% en todo el mundo, 128% en el mundo desarrollado y el 89% en los países en desarrollo.

Además el uso del internet, se estimó que en el 2013 alcanzó los 2 700 millones de usuarios, es decir, el 39% de la población mundial. Aunque, el acceso a Internet seguirá siendo limitado en el mundo en desarrollo. Según las previsiones, sólo el 31% de la población estará en línea en 2013, comparado con el 77% en el mundo desarrollado. Europa seguirá siendo la región del mundo más conectada, con una penetración del 75%, superando ampliamente las regiones de Asia y el Pacífico (32%) y África (16%). Como lo muestra en la Figura 3, estudio realizado por el director ITU Brahim Sanou.

Figura 3

PARALELO POBLACIÓN Y TELÉFONOS CELULARES [1]



Y publica las cifras más recientes sobre el desarrollo tecnológico a nivel mundial:

- La penetración móvil supera el 100% en cuatro de las seis regiones del mundo
- El número de abonados a la tecnología móvil celular se acerca a los 7 000 millones

Hay casi tantas suscripciones de teléfonos celulares como personas en el mundo.

Figura 4

IMPACTO DE LA TELEFONÍA CELULAR 2005-2013 [3]

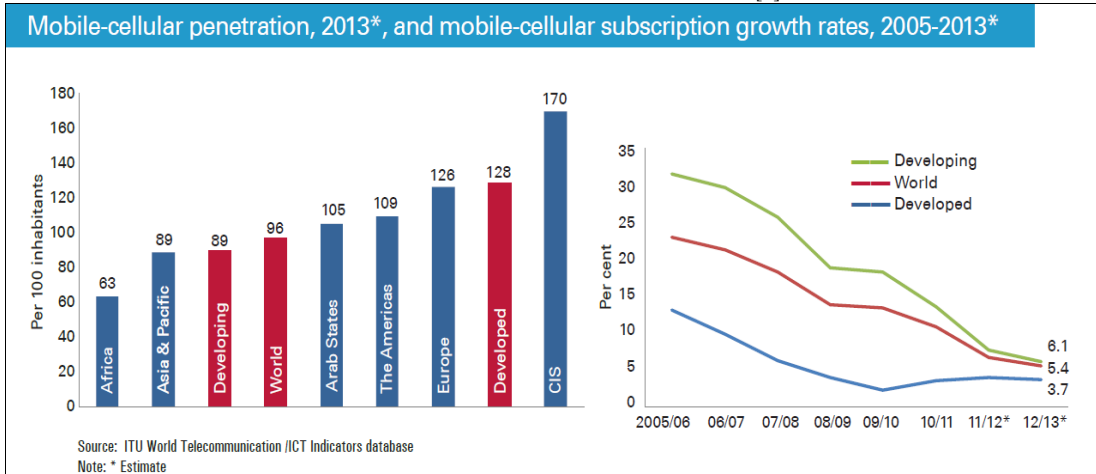
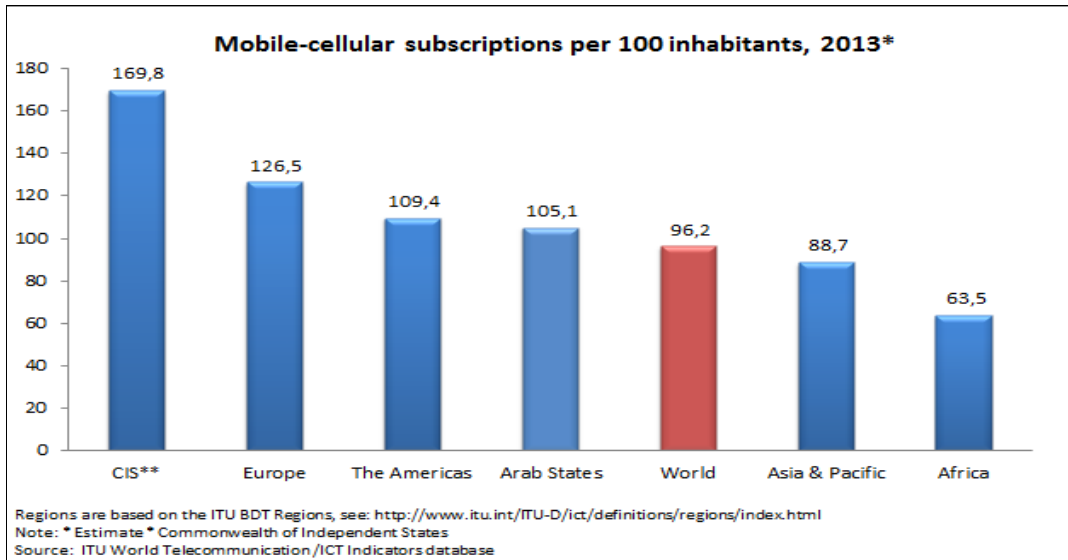


Figura 4

ESTADÍSTICAS POR SUSCRIPCIÓN A TELÉFONOS CELULARES POR HABITANTES POR REGIONES [3]



Estas cifras son alarmantes en la medida que nuestros datos están en la red y pueden ser accedidos por más personas en el mundo, las conexiones móviles generan un acceso ilimitado a las publicaciones en internet cuando no se tiene un control prudente sobre lo que se publica y se almacena en internet.

I. REDES SOCIALES

Los entes reguladores de todo el mundo requieren una estrategia, para el crecimiento de usuarios en las redes sociales, lo que representa una parte crítica en las plataformas sociales.

Facebook, Twitter y LinkedIn y Google Plus, que fue inaugurada en junio de 2011, ha crecido numerosamente en la cantidad de usuarios activos:

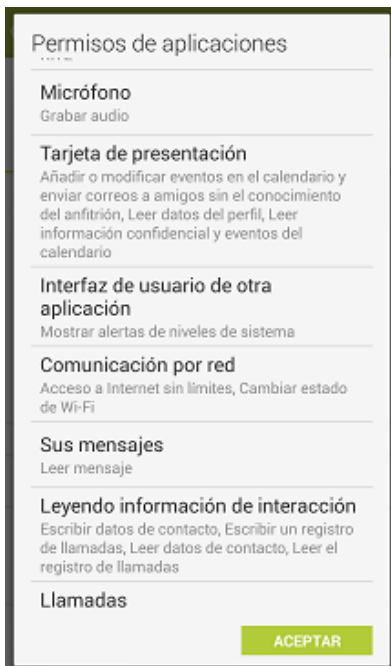
- **Facebook**

Ha crecido hasta llegar a más de 750 millones de usuarios activos, el usuario promedio de Facebook cuenta con 130 amigos, está conectado a 80 páginas, grupos y eventos comunitarios, e introduce 90 diferentes contenidos por mes. Más de 30.000 millones de contenidos se intercambian cada mes, y más de 250 usuarios activos acceden a Facebook a través de dispositivos móviles como los teléfonos inteligentes.

Muchos empresarios y promotores de más de 190 países trabajan con la plataforma de Facebook, y los usuarios de la red instalan 20 millones de aplicaciones por día. Más de 2,5 millones de sitios web están integrados con la plataforma de Facebook, incluidos más de la mitad de los 100 principales sitios web mundiales, según ComScore. [4].

Esta red social genera una gran acogida a nivel mundial según las estadísticas ya mencionadas, pero la gran incógnita es ¿Que hace Facebook con nuestros datos? Al momento de instalar la aplicación esta solicita una serie de permisos para poder ser instalada, entre los que se encuentran acceso a cámara, ID de llamadas, almacenamiento, comunicación de red sin restricción entre muchas otras, la siguiente imagen muestran algunas de las solicitudes que se autorizan a Facebook al momento de realizar la instalación en el dispositivo móvil y en caso tal de no estar de acuerdo con estos permisos esta no puede ser instalada.

Figura 4.
PERMISOS DE APLICACIÓN FACEBOOK



- **Twitter**

Ha captado más de 200 millones de usuarios desde su lanzamiento en julio de 2006, y añade diariamente otros 460.000. Los usuarios envían más

de 200 millones de tuits por día. Y este aumento se debe a que la mayoría accede por sus teléfonos móviles [4].

Twitter está revolucionando la industria social ya que su método de 140 caracteres para publicar en la red ha tenido gran acogida por la facilidad de utilización y la sencillez de su interfaz. Además está siendo utilizado para estar informado en tiempo real de los acontecimientos a nivel mundial debido a que los canales de noticias, grandes personalidades y en general una persona en el momento justo publican contenidos con información que en ocasiones es útil para estar actualizado con los acontecimientos locales, nacionales o mundiales según sean las preferencias de seguidores en la red.

Pero esta Red Social tiene el inconveniente que tienen todas, la recolección de datos personales por la autorización del usuario al momento de instalar la aplicación, y surge la misma pregunta que con Facebook y que todas las redes sociales. ¿Son seguros y confidenciales nuestros datos en las redes sociales?

- **LinkedIn**

Cuenta con unos 120 millones de usuarios, la mitad de ellos residentes de los Estados Unidos. Entre los países que cuentan con muchos usuarios LinkedIn figuran Brasil y el Reino Unido. Actualmente, el mayor crecimiento de esta red es en América Latina y África [4].

Esta red social está dedicada a compartir los perfiles profesionales de las personas y de las empresas, se puede decir que es una red profesional pero que cuenta con datos muy importantes de cada uno de sus miembros, profesión, trabajo, dirección, experiencia, una hoja de vida en la web pública para quien quiera observarla.

Las redes sociales y su acogida por parte de un alto porcentaje de la población mundial pueden llegar a manipular a la población con el contenido de sus cuentas ya que no existe una regulación expresa que proteja al consumidor de estos servicios. Debido esto es necesario que un ente regulador vigile la información que en las redes sociales está siendo

socializada o publicada y que los datos personales no sean divulgados y/o utilizados para otros fines, como lo es la venta a empresas según su *timeline* y perfil de publicaciones en estas redes. Cabe la pregunta ¿Porque en ocasiones llega publicidad de lugares, objetos, ropa y otra serie de cosas en las que nunca se ha tenido contacto, pero que están relacionadas el perfil?

II. RECOMENDACIONES DE SEGURIDAD PARA EL USO DE DISPOSITIVOS MÓVILES

- Establecer una contraseña de bloqueo o patrón

Esto hace más difícil el acceso a su información en caso de robo o pérdida. Definir si es posible una contraseña o patrón no visible y que el dispositivo se bloquee de forma automática cuando lleve un tiempo inactivo.

- Desactivar opciones no utilizadas como Bluetooth o GPS

De esta manera, se evita la propagación de códigos maliciosos (malware) y el consumo innecesario de la batería. [5]

- Desactivar que las aplicaciones puedan utilizar mi información de ubicación.

Con esto evita que violada su privacidad. Y sea utilizada esta información para fines maliciosos.

- Utilizar un software para cifrar las llamadas y la mensajería instantánea
- Utilizar siempre que sea posible un software para cifrar las conversaciones de voz y la mensajería instantánea, esto evitará que ninguna persona excepto los interlocutores pueda escuchar la conversación o leer el intercambio de mensajes de texto [5].

- Instalar sólo aplicaciones provenientes de fuentes de confianza

Utilizar software legítimo proveniente de fuentes confianza ayuda a minimizar la posibilidad de convertirse en una víctima de códigos maliciosos [5].

- Actualizar el sistema operativo y las aplicaciones del dispositivo móvil

Al igual que con los ordenadores, actualizar tanto el sistema operativo como los programas es necesario para obtener la mayor seguridad y las nuevas funcionalidades [5].

- Evitar utilizar redes Wi-Fi públicas

No utilizar este tipo de redes públicas para servicios que requieran de información sensible, como transacciones bancarias, compras, etc. Preferentemente se utilizarán redes 3G [5].

- Activar la verificación de instalación de aplicaciones.

Bloquea y advierte la instalación de aplicaciones maliciosas.

- Realizar copias de seguridad de la información almacenada

Es recomendable realizar periódicamente copias de seguridad de la información almacenada en el dispositivo. También se debe evitar escribir información sensible como contraseñas en forma de recordatorios o mensajes de texto [5].

- Configurar adecuadamente las redes sociales

No compartir información de forma pública y limitar la cantidad de amigos [5].

- No abrir hipervínculos sospechosos de correos, mensajes o sitios web

Tampoco escanear cualquier código QR, estos se pueden reemplazar por otros que no lo son, para dirigir al usuario a un sitio que descarga alguna clase de código malicioso [5].

- Ser cuidadoso con el dispositivo para evitar su robo o pérdida

No dejar el dispositivo móvil sin vigilar ni utilizar la funcionalidad manos libres en lugares concurridos [5].

- Ajuste de seguridad en las redes sociales.

No comparta la ubicación en tiempo real o fotografías en las redes sociales, esta información puede ser utilizado en ingeniería social.

- Utilizar herramientas de bloqueo de localización remota.

En caso de robo o pérdida la localización remota, bloqueo e incluso limpiar el contenido para prevenir que alguien tenga acceso a la información personal.

- Cifrar el teléfono

Habilitar la función de cifrado del teléfono, si está disponible, para contar con un nivel adicional de protección de sus datos.

Estas son algunas de las recomendaciones más comunes para el uso de dispositivos móviles, las cuales pueden ayudar a disminuir el robo o fuga de información que puede ser utilizada para fines comerciales, fraudes, ingeniería social y otra serie de utilidades que pueden llegar a darle a nuestra información en el mundo globalizado de internet.

Con la redacción de este artículo se pretende generar conciencia de la utilización de las redes sociales y los dispositivos móviles conectas a internet, conciencia que estamos en un mundo evolucionado que gira entorno a la tecnología y a estar conectado en todo momento por diversión,

trabajo, estudio, conocimiento u otros motivos que pueden poner en riesgo nuestra información que para la industria tiene un valor muy significativo aunque no le estemos dando la importancia que se merece.

Queda destacar la seguridad de la información para la niñez en el mundo, las regulaciones que deben existir para la protección de esta población ya que según un informa de la ITU “Utilización de los teléfonos móviles por los niños” realizado en 4 países del mundo comenta que la propiedad de teléfonos móviles por parte de niños entre ocho y 18 años es alta: casi del 70% en los cuatro países en que realizaron la investigación [6]. Estos datos revelados demuestran que la niñez en el mundo debe tener un control más estricto en las conexiones y en la protección de sus datos.

REFERENCIAS

- [1] (2014) ITU Statistics “**International Telecommunication Union**” Disponible en: <http://www.itu.int/es/about/Pages/default.aspx>
- [2] (2014) DANE “**Departamento Administrativo Nacional de Estadística**” Disponible en: http://www.dane.gov.co/reloj/reloj_animado.php
- [3] Brahima Sanou (2013) ITU Disponible en internet: <http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013-s.pdf>
- [4] Michael Geist “Confronting The Social Media Regulatory Challenge” Disponible en <https://itunews.itu.int/Es/1867-Medios-de-comunicacion-social.note.aspx>
- [5] (2012) 10 recomendaciones de seguridad para el uso de dispositivos móviles Disponible en: <http://www.cellcrypt.es/recomendaciones.html>
- [6] (2013) ITU Disponible en internet: <http://www.itu.int/osg/csd/cybersecurity/gca/cop/Reports/Childrens%20Report%202011%20EXEC%20SUM%20Spanish%20Final.pdf>