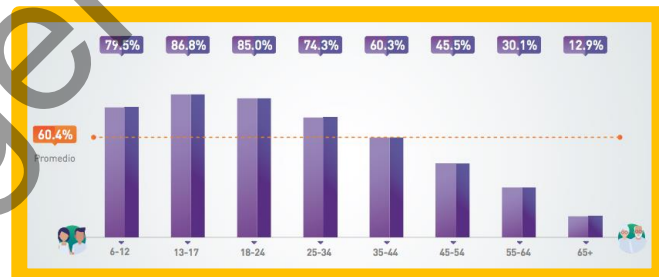


USO Y ABUSO DE LAS REDES SOCIALES Y SU RELACIÓN CON LA SEGURIDAD INFORMÁTICA.¹

Ángel Salvador López Vásquez²
angel.vasquez@zicatela.umar.mx

Abril 2019

Un tema que hasta este momento parece sencillo, pero conforme te vas adentrando te das cuenta de lo inmenso que es el mundo “virtual”, al día de hoy todos sabemos que las redes sociales prácticamente han inundado nuestras vidas, al grado que le hemos permitido cambiar nuestros hábitos. En palabras de Boyd (2010), las redes sociales son un punto de intersección entre la representación personal y la comunidad, que les permiten la representación del individuo en el espacio virtual, estas experiencias repercuten indiscutiblemente en el desarrollo. La función de las redes sociales no es otra cosa que mantenernos en contacto de manera permanente con familiares, amigos, conocidos o simplemente con personas con las que se comparten determinados intereses, esta última práctica se convierte en un tema de seguridad, dado que existen personas que generan perfiles falsos para lograr compaginar con alguien, al grado de convertirse en su “amigo virtual”, esto último es preocupante, piensa en los más pequeños, se ha visto considerablemente una gran cantidad de niños de 6 a 12 años usando el celular o tabletas con acceso a internet, representando el 79.5% de los usuarios que usan las TIC en México, lo anterior de acuerdo a las estimaciones del IFT³ con datos de la ENDUTIH⁴ 2016, como se muestre en la gráfica 1.



Gráfica 1. Estimaciones del IFT, con datos de la ENDUTIH 2016.

Pero, ¿cuál es la razón por la que se les brinda acceso a internet a los niños?, la respuesta es clara, la finalidad es entretener al niño para que no sea inoportuno en determinados horarios y deje a sus padres trabajar, limpiar, asistir a reuniones o simplemente ver la televisión, pero esto abre una ventana de tiempo para que personas con conocimientos mínimos logren enganchar a estos pequeños a juegos o videos “divertidos” que en muchos casos terminan manipulando al niño o enviandolos a enlaces no apto para menores mediante la publicidad engañosa de muchos sitios, pero no sólo queda ahí, también la información que muchas veces suele publicarse sin fines de maldad, pueden terminar en manos de delincuentes que se especializan en tráfico de

¹ El presente resumen es un producto final del seminario brindado en la Universidad del Mar Campus Puerto Escondido con fecha 24 de abril de 2019.

² Profesor-Investigador adscrito a la Lic. En Informática, de la Universidad del Mar Campus Puerto Escondido.

³ Instituto Federal de Telecomunicaciones – Es un órgano autónomo, su objetivo primordial es el desarrollo eficiente de la radiodifusión y las telecomunicaciones en México con apego a lo establecido en la Constitución.

⁴ Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de Información en los Hogares.

personas, prostitución, etc., es importante comenzar a generar y a transmitir una cultura de acceso seguro a internet, vigilar los sitios que visitan los niños y establecer horarios, sobre todo con el manejo de las redes sociales, ya que la información que publican o comparten puede llegar a manos equivocadas, por tanto al igual que se le enseña a los menores a no aceptar regalos de desconocidos y a no irse con personas extrañas, hay que transmitirles ese sentimiento de desconfianza a entablar conversación con desconocidos, sobre todo a facilitar datos personales aunque se hayan mantenido algunas conversaciones virtuales con anterioridad.

Al final no sólo queda ahí, las redes sociales han traído grandes beneficios, entre los cuales destacan las siguientes: Disponer de todo tipo de información clara y oportuna esto no quiere decir que sean 100% reales ya que también se publican infinidad de “fake news” o noticias falsas, otra es que ponen al alcance de forma innovadora el conocimiento científico actual, ofrecen gran cantidad de ocio y entretenimiento, además de facilitar las maneras de poder relacionarse o comunicarse con los demás, pero como dice el dicho, no todo lo que brilla es oro, dado que también existen riesgos muy latentes que muchas personas omiten, como son el robo de información y suplantación de identidad, los menores pueden acceder a contenidos inapropiados, riesgo de aislamiento o contacto con desconocidos, acoso o pérdida de intimidad, y uno de los puntos importantes es la pérdida en la noción del tiempo. Sin embargo los últimos años también se ha generado en la sociedad un impacto muy grande respecto a los riesgos que se tiene en las redes sociales como son el ciberacoso o más conocido como cyberbullying, grooming o engaño pederasta, doxing la cual proviene de dox que quiere decir abreviación de documentos que para las redes sociales es la práctica en internet para investigar y publicar información privada de un individuo, y por último el también muy sonado “sexting” la cual involucra el envío de mensajes sexuales por medio de las redes sociales. Los riesgos por el uso de las redes sociales son latentes, por lo que cada uno tendrá que ser responsable de la seguridad de su información, si has leído hasta este punto te invito a que aumentes la seguridad de tus redes sociales, evita compartir tus datos personales mediante el internet, no guardes contraseñas en tu cartera y celular, y sobre todo has un análisis de las personas que actualmente tienes agregada a tu red social, ya que seguramente puedes tener “espías” que sólo quieren hacerte daño, termino este escrito con las palabras del famoso hacker Kevin D. Mitnick, dónde nos hace ver que, *“el eslabón más débil de la seguridad informática eres tú.”*