SEGURIDAD INFORMÁTICA PARA NIÑOS Y ADOLESCENTES

Mauricio Martínez Tibaduiza
Universidad Piloto de Colombia
Bogotá, Colombia
maomartinez@yahoo.com

***Abstract*—Against the use of Internet, children and teenagers currently unknown threats that are on the internet and therefore may potentially affect the devices that they use to have Internet access, or worse get to publish confidential information from them themselves, their parents or relatives. Parents play an important role towards education of their children; Why not implement best practices for Internet use? This document puts into context and gives the reader different tools that allow you to start having good practice to use the internet service**

***Índice de términos*—adolescentes, amenazas, antivirus, celulares, computadores, concientizar, confidencial, correo, educar, espías, internet, música, niños, padres, redes sociales, seguridad informática, tabletas, videojuegos, virus.**

***Resumen*— Actualmente los niños y adolescentes usuarios de internet, desconocen las amenazas que se encuentran en internet y que por ende podrían llegar a afectar los dispositivos por medio de los cuales tienen acceso a Internet, o peor aún, llegar a publicar información confidencial de ellos mismos, sus padres o familiares. Los padres desempeñan un papel importante frente a la educación de sus hijos, ¿porque no se deberían tener buenas prácticas para el uso del servicio de Internet? Este documento pone en contexto al lector y le entrega una serie de herramientas que le permiten empezar a tener buenas prácticas de uso del servicio de internet para ser aplicado a niños y adolescentes.**

I. INTRODUCCIÓN

Este documento relaciona los diferentes aspectos de la cotidianidad a la que se enfrentan niños y adolescentes en el constante uso de las tecnologías informáticas; y menciono constante uso, porque tanto se tiene acceso a un computador desde el colegio, como también a nivel personal para la gran mayoría de casos, o en un café internet, o se tiene acceso a otros dispositivos que hoy día encontramos en el mercado y que permiten interconexión a internet, como lo son teléfonos móviles inteligentes, tabletas, televisores inteligentes, relojes inteligentes, o dispositivos blue-ray; como por mencionar algunos. Cada uno de los anteriores dispositivos le permite al usuario tener acceso a internet y aplicaciones por medio de las cuales podrá acceder a información pública, sitios de entretenimiento, redes sociales, e incluso le permitirá compartir información;

¿Hasta qué punto los niños y adolescentes tienen conciencia de lo que se debe acceder vía web, o de lo que se debe y no se debe compartir en internet? ¿Conciencia de lo que se puede o no se puede descargar de internet?

Este documento relaciona puntos a tener en cuenta frente al buen uso que debería darse al acceso a internet, teniendo en cuenta reglas básicas de seguridad informática aplicadas a un entorno que es muy vulnerable, y que por la falta de conocimiento frente a las amenazas cibernéticas que se encuentran en constante crecimiento podrían llegar a comprometer un dispositivo usado por un niño o adolecente para luego ser usado como herramienta para afectar otros dispositivos o sistemas.

Es importante conocer a que riesgos se encuentran expuestos los usuarios de internet, y que riesgos puede llegar a enfrentar en su día a día frente al uso de los dispositivos que dispone el mercado de hoy día a disposición, para que todos estemos interconectados o en línea.

II. AMENAZAS CIBERNÉTICAS

Cuando nos referimos al ciber-espacio, estamos haciendo referencia a Internet, y así como en nuestra vida cotidiana hacemos referencias a amenazas biológicas que llegan a afectar nuestro estado de salud como por ejemplo puede ser el virus de la gripa, virus de sarampión o actualmente el virus que causa la fiebre del chicunguña; en internet existen amenazas cibernéticas que pueden llegar a afectar o

“enfermar” los dispositivos por medio de los cuales accedemos a la red Internet; esto significa que deberíamos saber o conocer ciertos parámetros que nos podrían indicar si existe riesgo de infectar un dispositivo cuando navegamos en internet, y deberíamos plantear una posición para ejecutar acciones preventivas en pro de minimizar dichos riesgos, e incluso darle un adecuado uso a los dispositivos que usamos para interconectarnos; y por qué no, pensar en alargar la vida útil de estos.

Así como se presentan sintomatologías por un virus bilógico en una persona, nuestros dispositivos presentan síntomas y dolencias cuando nos infecta un virus informático, entonces observamos que éstos se tornan más lentos cuando se ejecutan tareas o se abren aplicaciones, se bloquean, o cuando se inician, generan errores que nunca antes habíamos visto, cuando accedemos a internet desde un pc, nos aparecen íconos nuevos o diferentes a los comúnmente conocidos, aparecen mensajes de un momento a otro sin solicitarlos, o aparecen íconos en nuestro escritorio de computador que nunca antes habíamos visto; o se desconfiguran nuestras carpetas y documentos donde almacenamos datos e información; y éstos como por dar un ejemplo al respecto.

Entonces, un virus informático no es más que un programa informático creado con el propósito de afectar un dispositivo, o sus aplicaciones, programas o incluso su sistema operativo, tal como los que conocemos hoy día: Windows, MAC, Linux, Android, iOS, entre otros.

Hay un tipo de virus informático que por ejemplo ha sido creado y diseñado para robar datos confidenciales del usuario, como por ejemplo las claves del usuario, la información referente a sus preferencias de navegación en internet; estos programas espías son conocidos en el mundo informático como “spyware”.

Otra forma de obtener datos confidenciales es cuando el usuario los introduce de forma manual e intencional en una página web que es de su entera confianza pero que ha sido falsificada, donde muy seguramente ha accedido a ella por medio de un vínculo o “link” recibido por correo; por ejemplo “*la actualización de datos para la cuenta bancaria*”; muchos casos se han visto frente a que las entidades bancarias supuestamente solicitan actualización de datos a través de correo electrónico, y el vínculo o link puesto en el mensaje recibido envía al usuario a una página falsa creada inclusive con los logos corporativos de dicha entidad; siendo así una forma muy eficiente de capturar información confidencial de un usuario, esta manera de obtener información es conocido como “phishing” en el ambiente informático.

Ahora estamos enfrentados a una amenaza que está tomando fuerza la cual es conocida a nivel informático como “ransomware”. Esta amenaza se basa en que cuando afecta el dispositivo de la víctima lo que hace es “secuestrar” los datos o información importante del usuario solicitando a la víctima realizar un pago a través de internet, para que pueda volver a tener acceso a dicha información; por ejemplo bloquea el acceso a los documentos almacenados por el usuario, en el dispositivo, como pueden ser fotos, imágenes, videos, música, documentos y archivos personales en general. Lamentablemente las víctimas que han pagado no han recibido a cambio la solución para volver a tener acceso a dicha información.

Los anteriores son unos ejemplos sencillos de las amenazas que se encuentran disponibles y en crecimiento continuo en internet, sin embargo, es importante resaltar que adicionalmente a estas existen muchísimas más, lo cual implica un riesgo demasiado alto de posible infección para los usuarios que accedemos a internet.

Para muchas de las amenazas informáticas existentes, hay una forma muy sencilla de detenerlas, y es a través de otro programa que haya sido creado con la capacidad de detectarlas y eliminarlas, estos programas de detección de virus informáticos son conocidos como antivirus, y son aplicativos que se pueden instalar en equipos de cómputo, teléfonos inteligentes o tabletas; y le brindan al usuario final una capa de seguridad frente a las amenazas cibernéticas como por ejemplo las descritas anteriormente.

Cabe señalar que debido a que el antivirus informático es un aplicativo desarrollado por una compañía orientada a seguridad informática, se debe pagar por su uso y su licencia, tal como se paga por ejemplo por un sistema operativo como Windows o Mac, por dar un ejemplo. Hoy día los fabricantes dan la facilidad de poder comprar este programa o

aplicativo por internet, sin necesidad de ir a una tienda o almacén en específico.

III. Amenazas en los Dispositivos

Existen muchas formas bajo las cuales un dispositivo que tiene acceso a internet, puede llegar a infectarse, y si hacemos referencia al dispositivo de uso clásico para acceder a la red de Internet, como lo es el computador, encontramos, que un virus puede llegar a afectar nuestro pc de diferentes formas; como por ejemplo al descargar música, películas, o videojuegos gratis; que promueven muchos sitios en internet. En principio muchos de los sitios que ofrecen música libre, están atentando contra los derechos de autor; bien conocemos que los derechos de autor están atados a que los consumidores debemos pagar para tener acceso a su obras o creaciones, y los sitios que ofrecen música, o películas, o videojuegos de forma gratuita, le están entregando al usuario dicha información, pero a cambio instalan programas maliciosos como virus o spyware, sin que el usuario se entere.

Otra forma de afectar un equipo es dando clic en la opción de "Aceptar" para las ventanas emergentes que aparecen cuanto estamos navegando, muchos usuarios de internet no se detienen a leer la información mostrada en el mensaje, sino por el contrario hacen clic en aceptar, muy pocos se toman la molestia de leer para conocer el contenido de dichos mensajes, o de cerrar dicha ventana. Fácilmente se puede cerrar la ventana emergente se ya sea con el mouse, o con el teclado usando Alt+F4 en Windows, o tecla "Command" + W para MAC.

Un ejemplo clásico de estas ventanas emergentes es aquella que se muestra al usuario de internet, mostrando un mensaje donde hace referencia a que el equipo donde se encuentra navegando se ha infectado o se le ha detectado un virus, y que para poder eliminar dicha amenaza es necesario hacer clic sobre tal ventana.

Este tipo de alertas inducen al usuario a realizar compras de supuestas aplicaciones de antivirus, pero muchas de ellas no lo son.

Otra forma de infectar nuestro sistema de cómputo es cuando traemos una USB del exterior a nuestro pc personal y la conectamos, como por ejemplo, descargar información desde un sitio público como un café internet, y llevar la USB a nuestro equipo, desconociendo si en dicho sitio los equipos están protegidos con un antivirus, o cuando compartimos nuestro equipo personal con otras personas que a su vez traen dispositivos de almacenamiento USB del exterior desconociendo si fueron usadas en equipos protegidos o no.

Cuando se reciben correos electrónicos no deseados o no requeridos, como aquellos que muchas veces llegan en inglés con información de promociones para compra, promociones de acceso a juegos en línea, o videojuegos para computador, u otro tipo de información; son mensajes de tipo basura, conocidos en informática como spam.

En este tipo de mensaje muchas veces se encuentra un vínculo o acceso que direcciona al usuario a un sitio web en especial, en su mayoría dichos vínculos contenidos en el mensaje tienen como objetivo descargar amenazas en el dispositivo, que pueden ser del tipo virus, para afectar el sistema u aplicaciones, o de tipo espía, para capturar datos o información del usuario.

Otra problemática a la cual se enfrentan los niños y adolescentes usuarios de internet, y que es considerado como una debilidad que puede ser aprovechada por una amenaza, es el hecho de compartir y publicar información personal de ellos mismos, de sus contactos, amigos, o familiares, sin saber quién puede estar observando o adquiriendo dicha información; el riesgo se aumenta cuando se publica demasiada información, o más información de la que tradicionalmente debería publicarse; ahora no solamente por falta de conocimiento se pueden comprometer los dispositivos usados por niños y adolescentes, sino también se está comprometiendo su información personal y de sus allegados.

Otro de los problemas que se generan a través de internet que pueden afectar a niños y adolescentes y que es una amenaza creciente que ha empezado a materializarse, es el denominado ciber-bullying, el cual es una forma de matoneo virtual, principalmente usado a través de las redes sociales y que se encuentra en auge y crecimiento; lo que llama la atención sobre la afectación de quien es víctima del ciber-bullying, es la velocidad con la que se propaga y se multiplica la información a través de internet.

IV. ESTADÍSTICAS DE LAS CIBERAMENAZAS

Para tener un acercamiento de cómo han crecido las amenazas cibernéticas, vamos a hacer un acercamiento de cómo se encuentran hoy; y para ello revisaremos la información de estado y comportamiento de dichas amenazas respecto de las compañías que se dedican a seguridad informática o ciberseguridad.

No es una amenaza olvidar o dejar un dispositivo con datos personales olvidado en un sitio, esto es considerado como una debilidad, la amenaza ocurre cuando se manipulan los datos encontrados allí de manera fraudulenta. Kaspersky una compañía dedicada a la creación de soluciones de seguridad informática como lo es el nombrado antivirus Kaspersky, indica que solamente en Estados Unidos Durante el año 2012 fueron olvidados en los aeropuertos alrededor de 12000 equipos portátiles[1]; la cuestión es, ¿en dónde habrá terminado la información contenida en dichos dispositivos? Alguien podría crear un falso perfil en una red social a partir de las fotos o videos encontrados en un computador portátil olvidado.

Check Point es otra compañía dedicada a la fabricación y comercialización de tecnologías enfocadas a la seguridad; esta compañía indica en su informe anual de amenazas correspondiente al año 2015 [2] indica aspectos muy importantes a tener en cuenta, de todo lo que ocurre en un día de trabajo en una empresa:

- Cada 24 segundos un computador accede a un sitio web malicioso.
- Cada 34 segundos un virus desconocido por los antivirus es descargado
- Cada 5 minutos una aplicación de alto riesgo es usada.
- Cada 6 minutos un virus conocido es descargado
- Cada hora se producen 106 descargas de virus desconocidos
- Un porcentaje del 86% de las compañías analizadas accedieron a sitios malicioso
- Un 96% de las compañías al menos usaron una aplicación de alto riesgo.

Frente a la anterior problemática de amenazas crecientes y emergentes en internet, ahora debemos analizar ¿cada cuánto se conectan los niños y adolescentes a internet durante un día?; ¿cuáles son los sitios de internet de donde ellos descargan datos, información, juegos, música etc?. Muchos de los padres y madres cuya herramienta de trabajo es un computador, un teléfono inteligente, o una tableta, llevan estos dispositivos a sus hogares; ¿cuántos de ellos prestan estos dispositivos a sus hijos o familiares para que puedan acceder a internet?; ¿cuantos conectan su teléfono o tableta al portátil corporativo para cargar su batería?; en esta conexión ¿cómo se garantiza que un virus no se trasmita al dispositivo móvil?; ¿cuántos usuarios de este tipo no conectan vía wifi su dispositivo corporativo en la misma red de la casa para tener acceso a internet, donde dicho wifi es el mismo donde toda la familia conecta sus dispositivos para poder navegar?

Finalmente Check Point indica en su informe que en el año 2014 los virus informáticos aumentaron en un 71% respecto al año 2013, llegando a 142 millones.

Symantec, otra compañía dedicada a la creación y comercialización de soluciones de seguridad informática en su volumen 20 del "Internet Security Threat Report" [3] indica que en el 2014, el 17% (casi 1 millón) de aplicaciones creadas para el sistema operativo de teléfonos inteligentes y tabletas Android, eran virus disfrazados de aplicaciones.

Symantec identifica que un 60% de los mensajes de correo electrónico son spam; así mismo el 60% de todos los ataques dirigidos con malware o virus, afectaron las pequeñas y medianas empresas, durante el año 2014.

Los ataques de secuestro de información contenida en equipos y dispositivos móviles, creció en un 113% para el año 2014.

Frente a los dispositivos móviles según el informe de Symantec, se encontró el sistema operativo con mayor número de debilidades que permitiría a un hacker atacar el dispositivo o a un virus, poderlo infectar y afectarlo, en primer lugar para 2014 fue iOS, segundo lugar Android, tercer lugar BlackBerry OS, cuarto y último lugar Windows Phone; frente a esta problemática debemos tener en cuenta que los dispositivos con mayor venta en el mundo tienen sistema operativo Android y iOS.

Frente a las aplicaciones usadas para navegar en internet, durante el año 2014, en orden de mayor a menor respecto a las debilidades que podrían ser aprovechadas por un hacker o un virus, encontramos en primer lugar el navegador Opera, en segundo lugar Mozilla Firefox, en tercer lugar Microsoft Internet Explorer en cuarto lugar Google Chrome y en último lugar y con menos debilidades que podrían ser aprovechadas por un hacker o un virus informático esta Apple Safari; sin embargo vale aclarar que el navegador de Apple, también podría ser vulnerado por una amenaza cibernética, o ser víctima de un ataque de hacking.

Ahora preguntémonos, ¿cuantos correo de tipo basura recibimos a la semana, o diariamente en nuestro buzón de mensajería personal? ¿Cuál es el sistema operativo que tienen nuestros dispositivos móviles? ¿Cuál es el navegador comúnmente usado para navegar en internet?

Los anteriores son unos sencillos ejemplos de cómo se encuentran en estado de riesgo los aplicativos y dispositivos comúnmente usados por niños y jóvenes; para mayor información al respecto en las referencias del presente documento se relacionan los sitios web de donde se puede descargar la información que relaciona cada fabricante de seguridad, para tener una visibilidad mucho más completa frente a la problemática de estas amenazas que se encuentran latentes y en crecimiento en Internet.

Finalmente otro de los fabricantes de tecnologías de seguridad reconocido en la industria: McAfee Intel Security, relaciona en una presentación de seguridad enfocada a padres de familia [4] importantes puntos a tener en cuenta:

- 27% de adolescentes tienen su computador de casa infectado con un virus informático.
- 48% de los padres creen que sus hijos les dicen la verdad acerca de su comportamiento en línea.
- El 71 % de los adolescentes dicen haber ocultado su comportamiento real "en línea".
- 20% de los adolescentes afirman haber terminado una amistad por causa de algo ocurrido a través de una red social.
- 31% de adolecentes reportan haber tenido acceso a películas y música pirata.
- 48% de adolecentes reportaron buscar respuestas en línea para sus exámenes.
- 46% de adolecentes reportan haber tenido acceso accidentalmente a páginas de pornografía.
- 32% reportan haber accedido de forma intencional a estas páginas
- Top 5 de las formas en que los adolescentes ocultan su comportamiento en internet:
    - 5. Usan un computador que sus padres no revisan: 23%.
    - 4. Mienten u omiten detalles de su comportamiento en línea: 23%.
    - 3. Ocultan o borran mensajes instantáneos o videos: 34%.
    - 2. Cierran o minimizan el navegador de internet cuando sus padres se acercan: 46%.
    - 1. Limpian o borran el historial de navegación del navegador: 53%.

V. ¿CÓMO HACER FRENTE A LAS CIBERAMENAZAS?

A continuación se presentan una serie de recomendaciones y de buenas prácticas con el fin de minimizar el riesgo de que nuestros dispositivos de uso diario se vean afectados por amenazas como lo puede ser captura ilegal de información, virus informáticos, programas espía, entre otros.

Nuestros dispositivos deben de tener como mínimo una capa de protección, la cual es un programa de antivirus. Hoy día muchos de los fabricantes permiten adquirir este programa o software a través de internet, y ofrecen promociones para adquirir su licencia a uno, dos o tres años para uso. Ahora bien si encontramos muchas soluciones posibles de antivirus, ¿cuál es la mejor?; Gartner (www.gartner.com) una compañía dedicada a consultoría recomienda a los siguientes fabricantes como los líderes en protección antivirus, según su reporte de análisis del mes de diciembre del año 2014 [5] : McAfee Intel Security, Kaspersky Lab, Trend Micro, Symantec y Sophos.

Muchos de los fabricantes de antivirus ofrecen como solución adicional al antivirus, el control de padres; por medio de esta aplicación se pueden

aplicar filtros de navegación en el computador para sitios no deseados como por ejemplo páginas web relacionadas con desnudos, sexo, pornografía, violencia, etc.

Vacunar o limpiar con el antivirus las unidades USB que se conecten al computador antes de usarlas, incluso las memorias de dispositivos móviles como tabletas o teléfonos inteligentes.

Evitar al máximo prestar los dispositivos que permiten el acceso a internet a terceros.

No abrir correos electrónicos que el usuario no esté esperando, o de los cuales se desconozca el remitente, igualmente si todas las transacciones de correo electrónico se hacen en español, lo más lógico sería eliminar sin abrir aquellos mensajes que ingresan al buzón en un idioma diferente.

Los bancos hacen referencia a que nunca solicitan actualización de datos a través de internet sino por otro medio como telefónico o de forma personal en sus oficinas; de lo contrario el usuario debería validar con su entidad bancaria la originalidad de dicho mensaje o de lo contrario debe eliminarlo. Igualmente esta recomendación aplica para cualquier otra entidad que solicite datos personales por correo electrónico.

Mantener los dispositivos en lugares seguros y bajo características de ambiente que eviten su perdida; por ejemplo tener cuidado con los dispositivos usados en un sitio público como un café, en un aeropuerto u hotel; así mismo evitar prestar a los niños los mismos para que ellos se entretengan en el centro comercial, mientras los padres realizan compras o diligencias personales; muchos dispositivos son extraviados por los menores porque ellos no tienen conciencia desarrollada a nivel de seguridad sobre el dispositivo e información contenida en ella.

Dialogo ante sus hijos frente al buen uso de redes sociales, por ejemplo, conocer la cantidad de contactos que los niños o adolescentes tienen; saber si sus hijos los conocen a todos; enseñarles a no aceptar a desconocidos como contacto en su red social; enseñarles que tipos de fotos podrían cargar, así mismo que tipo de información podría mostrar; y porque no, que los padres hagan parte de los contactos de sus hijos en estos sitios de redes sociales.

En los sitios web de juegos en línea, y redes sociales los niños y adolescentes deberían usar apodos no identificables [6].

Asegúrese que todos los mensajes y perfiles de red social, estén configurados para que solo sus contactos lo puedan ver [6].

Las claves para el correo electrónico, redes sociales y otros portales de uso, deben ser complejas; por ejemplo, usar letras mayúsculas, minúsculas, números, signos como punto, coma, asterisco, interrogación, admiración, más, menos; y que mínimo sean de ocho (8) caracteres de longitud.

Realizar cambios de clave de forma continua, bajo los parámetros descritos anteriormente, y no las comparta.

Desactivar la opción de geo-etiquetado que permiten algunos dispositivos como celulares tabletas o cámaras [6].

Obtenga más información acerca de los juegos, aplicaciones, y redes sociales que sus hijos usan.

En internet todo es para siempre, se debe hacer énfasis en los niños y adolescentes que deben tener mucho cuidado con lo que se publica.

Debe de crear un ambiente de confianza con sus hijos, con el fin de que ellos le puedan manifestar si son víctimas de ciber-bullying. Así mismo hacer énfasis en que ellos no deben de participar en dichas actividades, bajo las premisas de “no lo reenvíes, no lo respondas” [6].

Recordemos que no hay nada gratis; incluir la palabra gratis en la búsqueda por ejemplo para tonos de celular implica un riesgo tres veces mayor para el resultado de sitios web, y que estos estén relacionados con amenazas cibernéticas [7].

La búsqueda de archivos por el nombre mp3 ya implica un riesgo de descargar malware, y lo aumenta mucho más cuando se combina con la palabra “gratis” [7].

Las páginas relacionadas con clubes de fans aumentan la cantidad de páginas relacionadas con amenazas maliciosas que son creadas de manera falsa para que los usuarios que buscan información al respecto puedan caer en ellas y así infectar sus dispositivos; un ejemplo de ello es la falsificación de un sitio tan popular para ver videos como lo es YouTube [7].

Absténgase de hacer clic sobre los vínculos mostrados o publicados de banners, de aquellos sitios que están relacionados con música, películas, y descargas en general, especialmente de las páginas web que no son oficiales [7].

VI. Conclusiones

La importancia de tener siempre presente que las amenazas informáticas nunca se acabarán es el pie para dar continuidad a la concientización de todos los usuarios de internet; la mejor estrategia de protección es no desconocer dichas amenazas, y por ende empezar a crear, compartir y porque no publicar buenas prácticas del uso del servicio de internet.

Para los niños y adolescentes es de vital importancia el acompañamiento de los padres en su proceso de crecimiento y adquisición de conocimiento a través de las herramientas informáticas.

Es importante adquirir soluciones tecnológicas para asegurar los dispositivos por medio de los cuales se accede a internet; existe una variedad de ellas en el mercado, y no se debe optar por un producto de adquisición gratuita.

Referencias

[1] WBMF News Ocubre de 2012. Informe de seguridad de Kaspersky disponible en: http://latam.kaspersky.com/productos-para-empresas/whitepapers/panorama-de-amenazas p 7

[2] Reporte de Seguridad de Checkpoint 2015, disponible en: http://www.checkpoint.com/resources/2015securityreport/index.html

[3] Reporte de seguridad de Symantec “Internet Security Threat Report” Volumen 20, disponible en: http://www.symantec.com/es/es/security_response/publications/threatreport.jsp?inid=es_ghp_hero1_istr-20

[4] Video ilustrativo de McAfee Intel Security Orientado a padres de familia, disponible en: http://link.brightcove.com/services/player/bcpid65694806001?&bctid=2625162189001&iframe=true&width=700&height=410

[5] Reporte de Gartner en plataformas de protección para equipos de cómputo y dispositivos; disponible en: http://www.gartner.com/technology/reprints.do?id=1-26F1285&ct=141223&st=sb

[6] [6] Tips para padres de familia, documento de McAfee, disponible en: http://www.mcafee.com/us/microsites/cybered/downloads/osk-parent-tips-resources-es.pdf

[7] Documento publicado por el fabricante McAfee, “Música y Películas: el Entretenimiento Frente al Riesgo en Internet” disponible en: http://promos.mcafee.com/es-ES/PDF/Digital_music_movies.pdf

Autor

Ingeniero de sistemas Mauricio Martínez Tibaduiza, con especialización en Seguridad Informática de la Universidad Piloto de Colombia, y quien actualmente se desempeña como Arquitecto de Seguridad para la compañía Multisoft S.A.S.