Usuarios y hackers, un riesgo en la transmisión de datos financieros en Colombia.

Usuarios y hackers, un riesgo en la transmisión de datos financieros en Colombia.[1]

Users and Hackers, a Risk in the transmission of Financial Data in Colombia.

John Freddy Quintero Tamayo[2]
[1]Corporación Universitaria de Investigación y Desarrollo, Colombia.

Artículo recibido en el mes de Octubre de 2013; artículo aceptado en el mes de Noviembre de 2013

Citación del artículo: Quintero, J. F. (2013). Usuarios y hackers, un riesgo en la transmisión de datos financieros en Colombia. *I+D Revista de Investigaciones*, 2(2), 89-98.

Resumen

En este documento se reflexiona sobre el tema de los riesgos y vulnerabilidades de los datos de los usuarios y el uso de dispositivos móviles en diversas entidades financieras de Colombia. Se analizan en detalle las vulnerabilidades existentes y mediante demostraciones, se ilustran mecanismos como la estafa mediante clonadores de tarjetas, y robo de información por hurto de dispositivos móviles. La ingeniería social puede alcanzar a penetrar cualquier sistema de seguridad, sin llegar a manipular virus informáticos; todo radica en la astucia del atacante, puesto que se valen de muchos métodos fraudulentos para robar identidades o datos clasificados como confidenciales.

Palabras clave: Sniffing, Spoofing, MITM, Trashing, Riesgo, Ingeniería Social**.**

Abstract.

This paper a reflection lays out the user´s data risks and vulnerabilities when using of mobile devices and do financial transactions in entities by web in Colombia. By means of demostrations some security problems are ascertained, such as: credit card cloner swindle and stealed mobile devices information hacking. Social Engineering deciphers any security system without informatic virus tampering, only with attacker´s tricks, which use many fraudulent methods to steal identities and confidential classified data.

[1]Artículo de reflexión, de enfoque cualitativo, resultado de un proyecto de investigación, desarrollado en el grupo de investigación GIDSAW de la Corporación Universitaria de Investigación y Desarrollo (UDI) (Colombia). Dirección: Calle 9 # 23-55, PBX. 6352525.

[2]Ingeniero de Sistemas, Universitaria de Investigación y Desarrollo (UDI) de Bucaramanga (Colombia). Especialista en Seguridad Informática. Universitaria de Investigación y Desarrollo (UDI) de la ciudad de Bucaramanga. Docente-investigador del grupo GIDSAW. Corporación Universitaria de Investigación y Desarrollo (UDI) Bucaramanga (Colombia): Dirección: Calle 9 # 23-55.PBX: 6352525. Correo-e: john.quintero@udi.edu.co

Keywords: Sniffing, Spoofing, MITM, Trashing, Risk, Vulnerability, Social Engineering**.**

Introducción

La banca móvil se basa en servicios para usuarios con dispositivos móviles que tengan acceso a internet para realizar transacciones, consultas del estado de sus cuentas, bloqueos preventivos, entre otros. Dentro de las responsabilidades delegadas en una entidad bancaria, se encuentra la transmisión de la información por medio de canales seguros. Algunas de estas entidades asumen este rol con profesionalismo y teniendo en cuenta métricas de seguridad mínimas como las expuestas en la norma externa 052 de 2007 de la Superintendencia Financiera de Colombia (SFC). En cuanto a ataques basados en la intercepción de datos, se encuentran: "Man in the Middle", "Hombre en el Medio"; "Man in the Middle Mobile", "Hombre en el Medio Móvil", los cuales tienen la capacidad y las herramientas suficientes para llevar a cabo un ataque, vulnerando la confidencialidad de los datos. Estos ataques se ejecutan con sistemas operativos *GNU/Linux*, además de su facilidad para ser controlados y dirigidos tanto a redes locales, como a dispositivos móviles de usuarios que desconocen temas de seguridad. Dentro del gran círculo de riesgos, encontramos la ingeniería social, métodos o pasos aplicables a vulnerar la confidencialidad de los datos de usuarios en las entidades financieras de Colombia, sin necesidad de utilizar algún medio digital. La ingeniería social, al igual que la intercepción de datos confidenciales de muchos usuarios financieros en Colombia y el mundo, no son tomados con la rigidez y el cuidado que ello conlleva, omitiendo detalles mínimos como el trashing, técnica basada en la *recolección de datos analizando la basura*.

Para llevar a cabo esta reflexión sobre el tema de la seguridad informática, se utilizaron algunas demostraciones directas bajo las posibilidades previstas por las leyes vigentes en Colombia, en particular por la ley 1273 de 2009 (Congreso de Colombia, 2009). Las primeras demostraciones o testing que se realizaron, fueron las de transmisión de información de banca móvil, generada con dispositivos móviles Samsung® "Android®", Iphone® "IoS®"; paralelamente a ello, también se realizaron demostraciones de interceptación de información en los dos tipos de dispositivos utilizados para las pruebas, lo cual será analizado en detalle en este artículo, en el cual se defiende la tesis de que no existe sistema informático seguro, pero algo aún más peligroso que un virus informático, es la seguridad perimetral de los sistemas de transmisión de datos bancarios, pues sus vulnerabilidades se hallan encapsuladas como para no ser detectadas por una simple inspección.

Ingeniería social y ataques informáticos de interceptación de información en dispositivos móviles.

Los usuarios de la banca móvil se definen como sujetos en riesgo, porque muchos de ellos almacenan su información financiera en dispositivos móviles o cuentas de correo electrónico, los cuales son interceptables en la medida en que no se signan por parte de las entidades bancarias, las métricas de seguridad estipuladas. En Colombia se desconocen los ataques informáticos dirigidos a dispositivos

móviles, pero algunas estadísticas, por ejemplo, muestran que la clonación de tarjetas de crédito es un ataque informático muy frecuente, tal como la Unidad de Delitos Informáticos de la Policía Nacional seccional Huila lo señala en su record de denuncias recibidas en el año 2012 (Diario del Huila, 2012) (ver tabla).

Tabla1. *Modalidades de robo bancario demandadas*.

Lugar	Modalidad	Año 2011	Año 2012
Neiva	Por servilínea	1	
Neiva	Tarjeta crédito Clonada	8	4
Pitalito	Tarjeta crédito Clonada	1	
La Plata	Tarjeta crédito Clonada	1	
Total		**10**	**5**

Fuente: http://www.diariodelhuila.com

En esta modalidad se observa que la mayoría de delincuentes informáticos utilizan métodos antiguos y muy conocidos; esto crea en los usuarios bancarios un punto de ignorancia ante la eventualidad de los ataques a dispositivos móviles, llegando a ignorar los parámetros mínimos de seguridad en un dispositivo móvil.

Tipos de ataques

Con respecto a los ataques, siempre se encontrará un segundo actor, el cual llamaremos hacker, quien aprovecha las vulnerabilidades y el poco conocimiento de informática de los usuarios financieros, para, en pocos segundos, vulnerar las mínimas métricas o parámetros de seguridad que se tengan en los dispositivos móviles. Algunos métodos de interceptación de información, son los siguientes:

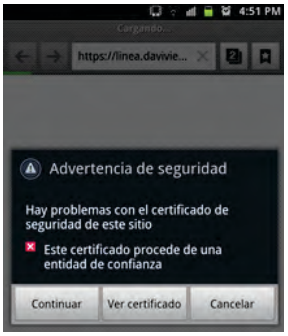
(a) MITMO: "Man In The Middle Mobile"

Es un método de interceptación de información por medio de una computadora, dirigido hacia un dispositivo móvil y su aplicabilidad, inicia debido al famoso malware de dispositivos móviles *Zeus/zbot* (ABC.es, 2011). El ataque se ejecuta entre diversos sistemas operativos móviles tales como: Android®, iOS®, Symbian®, Blackberry®. Para hacer uso de este ataque, es necesario contar con sistemas operativos que de una forma u otra contribuyan a capturar información; un ejemplo claro de estos sistemas operativos es *Linux Backtrack 5*® (Vivek, 2011), el cual contiene herramientas necesarias para lograr ejecutar un ataque sniffing a un dispositivo móvil, para obtener toda su información transmitida por medio de una red WiFi.

La demostración realizada para argumentar este aspecto, implicó contar con la herramienta *ettercap,* en la que se realizó la fase inicial con la ejecución de la herramienta para interceptar datos desde un sistema operativo Linux Bactrack 5®, el cual se utiliza previamente configurado. Esta herramienta es manipulada como un sniffing para capturar tramas de información que viajan dentro de una red. Luego, en la fase de análisis, una vez configurada y puesta en marcha la aplicación Ettercap®, hay que conocer algunos parámetros como lo son: La puerta de enlace del router, ip del dispositivo móvil; esta información se puede obtener por medio de aplicaciones como *Nmap*®, que son capaces de efectuar un diagrama de red, en el cual se podrá

obtener información como: sistemas operativos de los dispositivos conectados a la red, y puertos abiertos. Cada una de las aplicaciones mencionadas se complementan para ir descifrando cada uno de los interrogantes que se generen en el camino del atacante o hacker. En la fase de ejecución, se espera hasta que la víctima proceda a abrir su explorador de internet desde su dispositivo móvil, y una vez que la víctima realice esta acción, se emitirá un mensaje de alerta de seguridad desde su dispositivo móvil, la cual hará alusión al siguiente mensaje: *"hay problemas con el certificado de seguridad de este sitio"*, este mensaje se podrá apreciar en la figura 1 de esta demostración. Cuando el usuario es víctima y no comprende los mensajes de alerta emitidos desde su dispositivo móvil, es un trabajo sin mayores contratiempos para el atacante; una vez culminado el ataque, el delincuente informático obtendrá información desde su aplicación de Ettercap®; tal información es confidencial y sensible, dentro del rango de datos capturados pueden existir: contraseñas, nombres de usuario, número de tarjetas de crédito, o cualquier otro tipo de información que sea enviada entre la web como formularios; este tipo de ataque es común en redes inalámbricas públicas.

Figura1. Mensaje de alerta de seguridad



Fuente: El autor.

Dentro del ataque *Man in the middle mobile* se genera un *arp spoofing*: es la acción de disfrazar la ip del atacante con la ip del router o ap (McClure, Scambray, Kurtz, 2012); ésto obtendrá como resultado la interceptación de datos sensibles y confidenciales de cualquier usuario, sin levantar sospecha alguna. En los dispositivos móviles es difícil llegar a detectar un ataque de spoofing, porque no se cuenta con aplicaciones que ayuden a detectarlas ó que hagan un escaneo progresivo a los protocolos arp para señalar las duplicidades de las direcciones ip. Actualmente es una forma fácil de pescar víctimas, porque todo usuario es feliz navegando en redes WiFi que no tengan ningún tipo de seguridad, internet gratis a cambio de la información confidencial; una vez el atacante tenga en sus manos la información, visualizará en su pantalla la aplicación de Ettercap®, tal como se muestra en la figura 2, la demostración que se llevó a cabo.

Figura. 2. Pantalla de resultados de un ataque *MITMO*

Fuente: El autor.

El ataque demostrado anteriormente es un ejemplo sencillo y eficaz, en el cual se demuestra que la información en dispositivos móviles es

insegura; a lo mejor la mayoría de usuarios imaginan que los riegos desde sus dispositivos móviles son pocos, o de hecho piensan que no hay riesgo alguno; el peligro de este ataque radica en la cantidad de personas que almacenan información bancaria, corporativa, ya sea en la nube de Google "Google Drive©", ó en la nube de Microsoft© "Sky Drive©"; la pregunta que se genera es: ¿por qué es peligroso almacenar información bancaria en la nube?, Por el hecho de que es más fácil vulnerar una cuenta de correo electrónico que un sistema de banca móvil, porque los datos de los correos electrónicos enviados desde el formulario del navegador hacia el router, no viajan encriptados, esto conlleva a la intercepción de información confidencial como el password de las cuentas de correo, y su respectivo nombre de usuario. Al igual que las cuentas de correo, incluso las redes sociales son víctimas de este ataque, pero sólo el delincuente informático podrá analizar la información que allí se almacena; como ejemplo exhaustivo son las conversaciones de la red social *Facebook*©, esta red social cuenta con un sistema de almacenamiento de todas las conversaciones realizadas desde una cuenta, sin opción de eliminarlas; desde la perspectiva del delincuente informático, esto es muy atractivo porque si en algún momento se realizaron conversaciones en las cuales se mencionan: nombre de bancos, números de cuentas bancarias, números de tarjetas de crédito, datos personales, y fechas de tarjetas de crédito, todo esto reunido, será un festín de datos confidenciales para cualquier hacker.

En cuanto al servicio de banca móvil prestado por la mayoría de bancos en Colombia, se observó que es bastante seguro; se llega a esta afirmación por las demostraciones realizadas de los ataques de MITMO "Man In The Middle Mobile" realizado a estos sistemas; sus resultados fueron nulos ante este tipo de ataque especifico, como los datos que viajan desde el dispositivo móvil hacia el router están totalmente encriptados, además no permite realizar la consulta a la banca móvil, ó generan avisos de advertencia. Este tipo de alertas se pueden apreciar mejor en la demostración realizada, como se registra en la figura 3; las pruebas se ejecutaron en un banco en específico.

Figura 3. Servicio de consulta denegado a la banca móvil

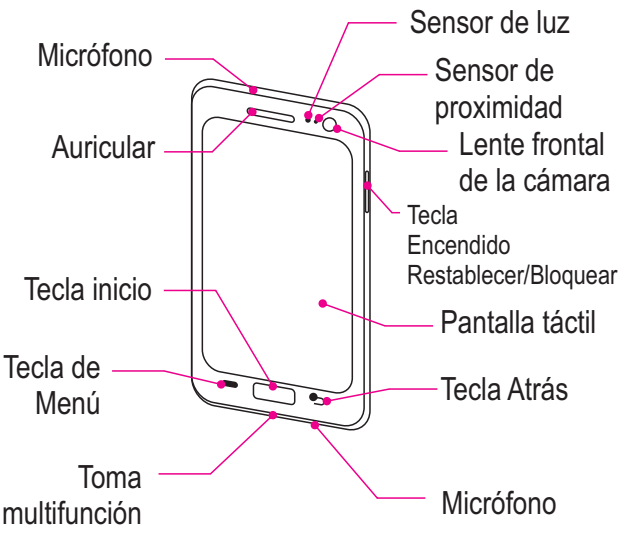
Fuente: El autor.

En algunos dispositivos móviles como el *Samsung Galaxy Note GT-N7000*, tienen una pequeña falla que al ser explotada por medio de un ataque MITMO "Man in the Middle Mobile", será todo un éxito, porque automáticamente

deshabilita todos los mensajes de alertas del dispositivo, de esta forma los mensajes de certificado de seguridad del sitio no serán emitidos, y los usuarios quedarán desprotegidos ante este ataque.

En los dispositivos Samsung Galaxy Note GT-N7000, con sistema operativo Android 2.36, se encuentra una opción que permite deshabilitar los mensajes de alerta de seguridad; esta opción se puede bautizar como un arma de doble filo, porque puede ser utilizada en el desarrollo de aplicaciones que generen riesgos por medio de la opción de configuración mencionada anteriormente; esta vulnerabilidad puede ser expandida de forma muy rápida; hay que recordar que los sistemas operativos móviles como Android poseen millones de apps gratuitas en su play store haciendo esto un atractivo de descargas a nivel mundial y una red de pesca para los delincuentes informáticos. Las grandes empresas como Samsung dejan a disposición de los usuarios la configuración de sus dispositivos móviles a un nivel avanzado, sin tener en cuenta que la poca experiencia de algunos otros usuarios pueden generar situaciones de riesgo a un fraude informático dirigido a sus dispositivos móviles. La tecnología crece cada día más y se enfoca en los Smartphone®; también se activan miles de servicios diariamente para simplificar los procesos que se tienen que hacer en la vida común de un usuario, pero es cierto que al existir miles de servicios, existirán mil formas de robar información y llegar al fraude electrónico. La ruta para verificar si está deshabilitada la opción mencionada anteriormente es: (a) abrir el navegador de internet desde el dispositivo móvil, una vez abierto el navegador se procede a oprimir la tecla menú, en vista que algunas personas desconocen dicha tecla, se puede observar en la figura 4, (b) una vez oprimida la tecla de Menú en el navegador de internet, seleccionar la opción ajustes, (c) se busca en las opciones: configuraciones de seguridad, y justo allí se encontrará la opción: mostrar advertencias de seguridad.

Figura 4. Servicio de consulta denegado a la banca móvil



Fuente: http://es.scribd.com/. Reproducida con autorización.

En esta opción se tiene que observar que esté seleccionada, dado que, si no se encuentra seleccionada, podrán sufrir cualquier tipo de ataque y el dispositivo móvil no se encontrará en la capacidad de emitir la alerta de seguridad; la opción se puede observar en la figura 5.

Figura 5. Servicio de consulta denegado a la banca móvil.

Fuente: El autor.

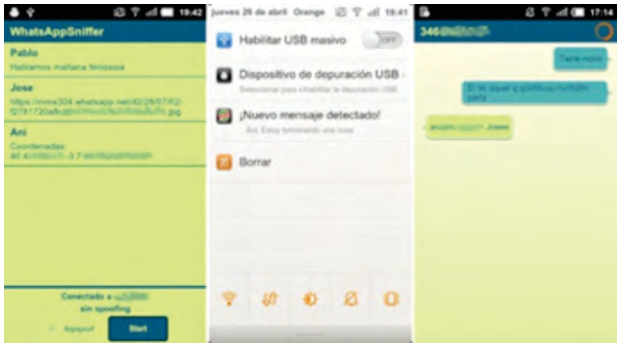
Concluyendo los resultados expuestos, se señala a los usuarios bancarios como un factor de peligro en la transmisión de datos bancarios o financieros, siendo los hackers el complemento a este peligro o riesgo; son dos factores que, unificados, generan inestabilidad en cualquier entidad bancaria o financiera del país. Una de las formas para mitigar estos riesgos, es la capacitación de usuarios o la divulgación de este tipo de ataques informáticos, ya que millones de usuarios capacitados o con algún tipo de conocimiento, serán un objetivo menos para un delincuente informático. Los conocimientos transferidos a los usuarios lograrán un impacto en el good will de las entidades en forma positiva; adjunto a ello, se logrará un descenso significativo de factor dinero en cuanto a demandas y asuntos relacionados con la degradación de los servicios seguros que brinden las entidades bancarias.

(b)WhatsApp Sniffer Free.

WhatsApp Messenger es una aplicación de mensajería multiplataforma que permite enviar y recibir mensajes sin pagar por SMS (http://www.whatsapp.com/). Esta plataforma es popular porque puede ser instalada en cualquier sistema operativo de diversos móviles; una de las ventajas que tiene esta plataforma, es que puede funcionar con una red GSM ó simplemente conectándose a una red inalámbrica (Chris, 2011) logrará tener el servicio activo, siendo la segunda opción la más utilizada por los usuarios, y la más insegura. Existen aplicaciones o apps desarrolladas por personas muy astutas en programación y con grandes dotes de ingenio; una de ellas es la aplicación *Whatsapp pwned free,* que permite interceptar los mensajes transmitidos desde cualquier whatsapp que se encuentre conectado a una red inalámbrica; este ataque es llamado comúnmente sniffing, aparte de interceptar mensajes, tiene la capacidad de interceptar imágenes ó vídeos. Para instalar este tipo de aplicaciones el dispositivo móvil debe estar en un modo de súper usuario ó más conocido como super root; el dispositivo debe estar en el modo súper usuario para permitir capturar las tramas de información que se transmiten desde el whatsapp, el delincuente informático podrá interceptar los mensajes de todos los usuarios whatsapp que estén conectados a una red inalámbrica no segura.

El escaso conocimiento de herramientas como Whatsapp pwned free, logra que los ataques sean más certeros, porque no se conocen medidas de seguridad para evitar y prevenir este tipo de ataque. A continuación se muestra en la figura 6 la interfaz de la aplicación Whatsapp pwned free.

Figura 6. Interfaz gráfica de la aplicación Whatsapp pwned free



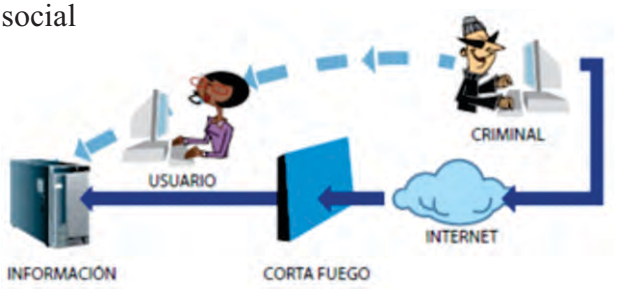
Fuente: http://www.hackplayers.com. Reproducida con autorización.

Se recomienda utilizar la aplicación *Whatsapp* conectada a una red GSM por motivo de seguridad, dado que las redes GSM (Harte, 2011) necesitan ataques más preparados y gente especializada para lograr un sniffing.

(c) Trashing, técnica de ingeniería social

Indudablemente la ingeniería social fue un término popularizado por el ex - hacker Kevin Mitnick (2011). Este ex – hacker norteamericano, hizo uso de técnicas poco convencionales a la hora de robar datos e información confidencial, sin hacer uso de algún tipo de dispositivo electrónico, valiéndose de su personalidad y astucia; la ingeniería social se ha vuelto una herramienta esencial para los hackers debido a que no todo se puede saber mediante una computadora. En la figura 8 se describe de una mejor manera cómo interactúa un ataque con ingeniería social directamente con la víctima.

Figura 8. Interacción de un ataque de ingeniería social



Fuente: The GBM Journal. Reproducida con autorización.

La figura 8 deja en evidencia cómo un delincuente informático puede obtener información, aun teniendo un sistema simple de seguridad como lo es un firewall (Noonan & Dubrawsky, 2006), antivirus, debido que el delincuente interactúa directamente con la víctima obteniendo información muy certera y en menos tiempo que ejecutando un rootkit o malware (Adair, Hartstein & Richard, 2010).

En Colombia, a lo mejor se desconoce la técnica de *trashing* (recoger o buscar en la basura), esta técnica fue adoptada por el ya mencionado ex – hacker mediante lo que constituye la ingeniería social (Kevin, Simon & Steve, 2003). Muchas de las personas que poseen cuentas bancarias, líneas móviles, u otro servicio que genere facturación en su lugar de residencia, nunca tienen el cuidado al desechar este tipo de información impresa; esto tiene consecuencias graves, porque están arrojando a la basura información confidencial en extractos bancarios, recibos de las líneas móviles que contienen datos tan básicos que un delincuente informático logrará estudiar la identidad de cualquier víctima y posteriormente procederá a: suplantarlo ya sea por medios telefónicos o suplantarlo personalmente, aunque la segunda sea la más

difícil, pero quizá es la más eficaz para este tipo de ataques.

Este método de robar información puede generar problemas en las entidades bancarias de cualquier país, ya que es difícil controlar este tipo de eventos; unas de las formas es sensibilizar a los usuarios para que utilicen herramientas que le ayudarán a deshacer los medios impresos generados por cualquier empresa prestadora de servicios; posiblemente una de las formas más seguras de desechar este tipo de información es utilizando un triturador de papel y repartir los residuos del mismo en varias bolsas, esto evitará un robo de información.

Referencias

ABC.es Tecnología. Recuperado de http://www.abc.es/20110915/tecnologia/abci-malware-android-201109151722.html

Adair, S., Hartstein, B. Richard, M.(2010). *Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code.* Primera edición. United States of America: Wiley.

Chris, S. (2011). *Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems.* Segunda edición. United States of America: No Starch Press, 2011. 280 p. ISBN 978-1593272661.

Fraude electrónico, delito poco denunciado en el Huila. Recuperado de http://www.diariodelhuila.com/site/index.php/especiales/3161-fraude-electronico-delito-poco-denunciado-en-el-huila_noticia25474

Harte, L. (2011). *Introduction to GSM: Physical Channels, Logical Channels, Network Functions, and Operation*. Segunda edición. United States of America: Althos Publishing Inc.

Kevin, M. (2011). *Ghost in the wires my adventures as the world's most wanted hacker*. Primera edición. United States of America: Little, Brown and company.

Kevin, M., Simon, W & Steve, W. (2003). *The Art of Deception.* Primera edición. United States of America: Wiley.

Ley de la protección de la información y de los datos. No.1273. Congreso de la República de Colombia. Diario Oficial. Bogotá.2009.

McClure, S., Scambray, J. & Kurtz, J. (2012). *Hacking exposed: network security secrets and solutions.* Séptima edición. United States of America: Osborne/McGraw-Hill.

Noonan, W. & Dubrawsky, I. (2006). *Firewall Fundamentals*. Primera edición. United States of America: Cisco Press.

Requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios. Norma externa 052. Superintendencia Financiera de Colombia. Bogotá, D.C. 2007.

Vivek, R. (2011). *BackTrack 5 Wireless Penetration Testing Beginner's Guide*. Séptima edición. United Kingdom: Packt Publishing Ltd.

Whatsapp. Sistema de mensajería multiplataforma. Recuperado de http://www.whatsapp.com/