NUESTROS SERVICIOS MÓVILES, ESTAMOS TRANSFORMANDO EL MUNDO DE LA TECNOLOGÍA FINANCIERA PARA BENEFICIO DE LOS CLIENTES.

Martínez Ramírez Julie Andrea
andreamar12@hotmail.com
Universidad Piloto de Colombia

***Abstract*— The Mobile Financial Services have marked a major revolution in society with the new system on-line transactions, the new service has also implicated financial institutions, traders implement security policies to prevent fraudulent movements such as theft information in order to carry out checks to avoid comply with the policies which were defined to carry out the principles of security such as confidentiality, availability, integrity.**

So that the world of technology as it progresses we find major changes that society has learned over time and understand the different vulnerabilities that can be performed when a service is provided as mentioned below document and what are the different ways that you can carry out a leak or theft of confidential information

***Keywords*— Security, Mobile Banking, Mobile**

Financial Services.

***Resumen*— Los Servicios Financieros Móviles han marcado una gran revolución en la sociedad con el nuevo sistema de transacciones on-line, este nuevo servicio también ha implicado a que las entidades financieras, comercializadoras implementen políticas de seguridad para evitar movimientos fraudulentos, como es el robo de información confidencial con el fin de llevar a cabo controles para evitar que se incumplan con las políticas de seguridad tales como la confidencial, disponibilidad, integridad.**

De tal manera que el mundo de la tecnología a medida que avanza nos encontramos con grandes cambios que la sociedad ha tenido que aprender con el tiempo y conocer las diferentes vulnerabilidades que se puede llevar a cabo cuando se presta un servicio tal como se menciona a continuación del documento y cuáles son las diferentes maneras en que se puede llevar a cabo una filtración o robo de la información confidencial.

***Índice de Términos*— Riesgo, sociedad, seguridad, Banca móvil, servicios financieros móviles.**

I. INTRODUCCIÓN

Los servicios financieros han marcado un cambio tan importante en la sociedad en la manera de que se usa el dinero, permitiendo a cualquier usuario acceder desde su dispositivo móvil con el fin de realizar transacciones, consultas, compras en línea. Esta lista no solo involucra a los usuarios sino a también al gobierno y a las entidades que hacen parte de las operaciones con solo tener acceso a Internet.

En medio del cambio se ha venido involucrando un 90% de la sociedad en el uso de dispositivos móviles, sino también el servicio de voz como una herramienta de trabajo, socialización o quizás diversión. Sin embargo existe un gran obstáculo para que los procesos bancarios se simplifiquen, por esta razón existen temores sobre los aspectos de seguridad y complejidad para llevar a cabo cada uno de los controles en el proceso que se presta a cada uno de los clientes que tienen dicho servicio.

II. SERVICIOS FINANCIEROS MÓVILES

A. Banca Móvil:

Es un medio por el cual se podrá recibir información bancaria y realizar transacciones financieras en línea a través del teléfono celular, de manera fácil, segura y confiable sin la necesidad de tener la tarjeta plástica. Quizás las herramientas que nos prestan este servicio pueden ser adulteradas por Hackers, no suele ser solo un experto el que realice una violación de la seguridad ya que los Smartphone no cuentan con antivirus que sea totalmente confiable y efectivo para detectar que la aplicación no cuenta con las políticas de seguridad.

B. Dinero Móvil:

Es un servicio que se facilita a quienes envían dinero a quienes desean, para ser retirado en cajeros automáticos, este será recibiendo un mensaje de texto con la clave de retiro y un código de seguridad, un servicio fácil y óptimo.

C. Pagos Móviles:

Es un servicio que permite realizar transacciones en línea, con este servicio se busca transformar los medios de pago de forma más fácil y rápida desde el celular.

Los usuarios con solo agregar el número de tarjeta pueden realizar el pago de alguno de los productos y servicios, compras online y transferencia de dinero. El pago móvil es un método de pago sin contacto, del cual la tecnología NFC también forma parte.[1]

D. Nfc Móvil:

Plataforma abierta al público para dispositivos móviles con una capacidad de tasa de transferencia de 424 Kbits para comunicaciones instantáneas, es decir valida su identificación y el equipo desde donde el usuario está ingresando. El alcance de esta tecnología es muy corta debido a que solo tiene un alcance de 20cm. La ventaja es la gran capacidad de enviar y recibir información al mismo tiempo.

A pesar de que cuenta con un corto alcance a la misma que opera, también podemos hablar de si cuenta con seguridad como el impacto en la copia de los códigos del chip con usos fraudulentos. No es solo robar información confidencial del usuario sino también la modificación en la misma. Por esta razón la seguridad se opta a través de las transacciones como SSL

Figura II. Descripción modelo NFC
Ref:http://www.xataka.com/moviles/nfc-que-es-y-para-que-sirve

La seguridad es y va a ser de gran importancia cuando se manejan cuentas bancarias, transacciones, compras online desde un teléfono móvil. Es por esto que toda transacción debe ser avalada por el mismo usuario realizando respectivamente la autenticación tales como PIN o clave personal.

Actualmente se ha venido implementando grandes cambios en las organizaciones financieras implementando las tarjetas SIM con el fin de resguardar toda la información (Claves). Una gran forma de llevar a cabo un resguardo de la información en caso de que sea robado el teléfono móvil asociada la cuenta y el acceso son inmediatamente bloqueados remotamente. [2]

II. NOVEDADES

Con el tiempo se ha incrementado este sistema donde los usuarios optan por la facilidad del uso de las transacciones en línea, es como se ha implementado en conjunto con los diferentes operadores tales como: Claro y el Banco Popular un servicio que facilitará la forma de realizar transacciones bancarias pero en el momento de anunciar este nuevo producto no han dado conciencia en las implicaciones de llevar a cabo este nuevo proyecto debido a que se debe anunciar que con solo tener una mejor infraestructura tecnológica también implica a varios riesgos que pueden implicar a la entrega de datos sensibles más de una vez a personas no confiables que desean en conocer dicha información.

Así como también se ha venido conociendo desde el 17 de Septiembre del presente año el lanzamiento por parte del Bancolombia el servicio de Billetera Móvil para realizar compras desde el celular. Para que todos los usuarios puedan adquirir este servicio es solo contar con la instalación de la aplicación App store realizando el proceso de validación del código de seguridad, este proceso debe ser revisado previamente con la entidad bancaria ya que sin tener el consentimiento de que el servicio y la aplicación es la correcta no dispondría el cliente de este servicio.

El banco a su vez debe realizar el proceso de activación del servicio, con el fin de realizar la configuración en caso de alertas, notificaciones al Banco. Estos grandes avances de tecnología han venido trabajando en conjunto con la entidad MasterCard ya que cuentan con la tecnología suficiente para la implementación del servicio Billetera [3].

III. COMPORTAMIENTO DEL MERCADO EN COLOMBIA DE PAGOS MÓVILES

A pesar de convertirse en una de las mejores industrias de crecimiento alcanzando un gran porcentaje de usuarios que optan este medio de pagos móviles. De acuerdo a un estudio realizado a algunas de las entidades tales como InternetMedia Services y COM Score se conocieron algunas de las cifras (%) de las cuales es importante conocer los grandes avances que ha llegado la tecnología en convertirse en un fuerte para las empresas y marcas de dispositivos móviles para implementación de fuertes aplicaciones con fuentes de seguridad óptimos , esto con el fin de velar los ítems que involucra la seguridad informática como la disponibilidad, integridad y confidencialidad.

%	***Observación***
99%	*Los usuarios tienen instalado diferentes aplicaciones en los dispositivos Móviles.*
35%	*Usuarios Smartphone.*
39%	*Tablets*
22%	*Usuarios con dispositivos móviles que cuentan con más de 20 aplicaciones instaladas.*
60%	*Usuarios utilizan aplicaciones de redes sociales tales como Spotify, likened y Waze.*

TABLA I
Estadísticas de la investigación del mercado móvil
http://www.colombiadigital.net/actualidad/noticias/item/8158-usuarios- moviles-un-mercado-creciente-en-latam.html

Dentro de la investigación realizada por la entidad Aso Bancaria, los pagos por online se incrementó a un 33% que en el recorrido del año se ha presentado recomendaciones de seguridad a las personas que realizan este tipo de procesos que implican tales como la información confidencial, respecto a dos cosas importantes a la hora de realizar transacciones online como cambiar la clave frecuentemente. [4]

IV. RIESGOS Y VENTAJAS DE LAS TRANSACCIONES ONLINE EN DISPOSITIVOS MÓVILES

Dentro del proceso de realizar, las diferentes transacciones, consultas, compras online, existen diferentes sistemas. De los cuales se encuentran ventajas y desventajas como el incremento porcentual de malware afectando los dispositivos móviles con un alce del 58%, lo que consiguió este virus fue el robo de información confidencial como correos electrónicos, números telefónicos.

De igual manera, las entidades bancarias no comunican a sus clientes los riesgos que pueden impactar la reputación de la organización si no son usadas correctamente. La falta de noticias ante las amenazas de banca móviles los atacantes puede ingresar en cualquier momento con el fin de atacar a cualquier consumidor desde cualquier dispositivo móvil, tabletas o hasta llegar a la entidad bancaria y llevar a cabo una denegación de servicio con el fin de ingresar al sistema y vulnerar sus servicios.

Por esta razón se han venido incrementando procesos de concientización a los consumidores que llevan a cabo el uso desde sus dispositivos móviles para realizar transacciones online, del buen uso de ellos y además no aceptar link, emails que soliciten datos personales tales como número de tarjeta, usuario, password, sin que sea propiamente de las entidades bancarias las únicas que son autorizadas en solicitar dicha información.

V. RIESGOS TECNOLÓGICOS

Es importante que los datos y servicios se encuentren siempre disponibles para acceder a ella. Existen varias formas que puede afectar la disponibilidad tales como desastres naturales, actos maliciosos y también ataques de denegación de servicios. Por esta razón, es importante conocer los riesgos que implican que la seguridad en dispositivos móviles no sea tan óptima como parece, de tal manera que se conocerá ampliamente cada uno de los principios de la seguridad informática, tales como:

A. *Confidencialidad:*

Es importante llevar a cabo un proceso donde los datos sean cifrados y no estar disponible para personal proveedor del servicio. Es por esto, que no se debe romper este gran principio que se transmite toda la información en redes públicas es decir redes celulares. A pesar de llevar a cabo controles como de acceso y establecer cortafuegos, sistema detección de intrusos es importante para llevar a cabo la protección de los datos e confidencialidad.

B. *Integridad:*

Es importante que toda la información sea precisa, y confiable para validar la integridad de todos los datos durante la transmisión ya que se puede detectar la interceptación e manipulación de los datos.

C. *Disponibilidad:*

Es importante que los datos y servicios se encuentren siempre disponibles para acceder a ella. Existen varias formas que puede afectar la disponibilidad tales como desastres naturales, actos maliciosos y también ataques de denegación de servicios.

D. *Autenticación:*

Es relacionado con la autenticación del usuario y contraseña, es por esto, que implica a los proveedores que prestan este tipo de servicio que se involucren más dentro del proceso de seguridad para que este principio no se rompa.

La gestión de riesgos tiene un proceso importante, para llevar a cabo los controles necesarios con el fin de minimizarlos, lo que implica en realizar las transacciones Online desde dispositivos móviles.

En cuanto a la evaluación de Riesgos permite analizar con profundidad las principales amenazas, se deben llevar a cabo ciertas preguntas con el fin de determinar la viabilidad de la amenaza, incidentes y las diferentes actividades que hay que llevar a cabo para la evaluación de riesgos tales como:

- Mejores prácticas para contrarrestar las amenazas.
- Preparación de los proveedores de servicio.
- Análisis de riesgos.
- Monitoreo.

Lugar del riesgo (elemento de la red)	Amenaza	Principio que se infringe	Riesgo probable	Controles de seguridad recomendados
Aplicación de la red móvil	• Revelación • Interceptación	Confidencialidad	Se ha leído información crítica enviada vía SMS	• Los números de cuenta del cliente se cifran cuando se transmiten • Los NIPs del cliente se cifran cuando se muestran y transmiten
Teléfono del usuario final	• Modificación	• Integridad • Autenticación	Infección causada por software malicioso móvil	• Las políticas de información por el lado de la red pueden descargarse en los teléfonos • Uso de antivirus específico para teléfonos inteligentes
Centro SMS, aplicación de SFM, red bancaria	• Interrupción	• Disponibilidad • Irrefutabilidad	Ataques de denegación de servicio	• Implementar un sistema que restrinja el tiempo de respuesta del paquete • Requerir que los SFM establezcan un entorno de red de alta seguridad, al adaptar las normas de mejores prácticas de seguridad como la ISO9001
Teléfono del usuario final	• Fabricación	• Autenticación • Irrefutabilidad	Ataques de suplantación de identidad *(phishing)*	• Solicitar una campaña activa de concienciación de los clientes, para instruir a los consumidores acerca de mensajes maliciosos • Exhortar a los consumidores/ víctimas a que reporten el número de los atacantes maliciosos a los proveedores de servicios de telecomunicaciones, para que puedan enviarse mensajes de advertencia y bloquear el número celular en forma permanente

TABLA II
Clasificación de amenazas tecnológicas SFM
http://www.afi-global.org/sites/default/files/publications/mfswg_guideline_note_no_2_sp_final.pdf

VI. MEDIDAS DE SEGURIDAD

Para protegerse contra malware móvil se debe llevar a cabo recomendaciones que hoy en día hay una gran variedad de software de seguridad móvil que son gratuitos, también hay varias medidas de seguridad tales como:

- Nunca suministre información confidencial claves a terceros.
- Cerciorarse de no ser visto por terceros la información que se encuentra ingresando en el dispositivo móvil.
- Evitar realizar las transacciones en línea utilizando el altavoz.
- En caso de pérdida del dispositivo móvil se debe ingresar a la página del Banco para bloquear el servicio de Banca móvil.
- Tener presente que su dispositivo móvil es confidencial no prestarlo a terceras personas.
- Eliminar mensajes de texto que contenga información financiera.
- Si utiliza Wi-fi indicar que la red sea segura con el fin de conectarse a la aplicación móvil.
- Denunciar si existe cualquier otra aplicación bancaria que puede ser maliciosa.
- En caso de que se detecte algo sospechoso de la aplicación alertar a la entidad bancaria en caso de fraudes.
- No divulgar información confidencial o sensible como el Número de cedula y evitar llenar encuestas, formularios donde se vea involucrado la información confidencial.

Figura II. Seguridad para Smartphone
http://www.kaspersky.es/internet-security- center/internet-safety/Smartphone

La gestión de riesgos tiene un proceso importante para llevar a cabo los controles necesarios, con el fin de minimizar dichos riesgos que implican en realizar transacciones online desde dispositivos móviles. [5]

VII. FRAUDES CIBERNÉTICOS

Las mayores amenazas para todos los usuarios de Banca Móvil se encuentran como un punto débil frente a las diversas plataformas, contraseñas débiles, acceso a las redes inalámbricas o compartir información sensible, debido a esto son usadas por cibernéticos ante el robo de identidad.

Dentro de las investigaciones realizadas en la ciudad de México, se ha determinado que eso se debe a que la cultura de la prevención a todos los usuarios que hacen uso de la Banca móvil es muy frágil, ya que lo que puede el cibernético en primera instancia es realizar el proceso de ingeniería social con el fin de persuadir a los usuarios a la instalación de un certificado falso.

Se deduce que uno de cada dos usuarios llevan a cabo las precauciones de seguridad en referencia al uso de las contraseñas y de compartir información de sus dispositivos móviles, pero no todos los usuarios cuentan con un software de seguridad móvil tales como el antivirus, se debe a que un cierto porcentaje de personas acceden desde redes inalámbricas a la cuenta móvil.

El sistema operativo Android es el más usado en los dispositivos móviles pero este ha sido como blanco de amenazas móviles. Dentro de las investigaciones realizadas se ha encontrado aplicaciones maliciosas en el año 2013 alcanzado a 1.4000.000.

VIII. RECOMENDACIONES

Dentro de las recomendaciones que toda organización debe tener al momento de prestar un servicio como Banca Móvil es necesario contar con una infraestructura bien definida dentro del inicio de un proyecto que conlleva a manejar información sensible. Se debe contar con los requisitos de seguridad, el cual no impacte el buen servicio, disponibilidad e integridad de la información. Dentro de las recomendaciones se encuentran las siguientes:

- Conecta con tu banco a través de redes seguras, una de las mejores por la facilidad y precio es **Segure Wireless.**
- Usar la App oficial del Banco, no la versión Web.
- No almacenar datos bancarios en el teléfono, se recomienda usar app Safepad (Android) o Note Lock (Ios) que son block de notas protegidos con contraseñas.
- Instalar un antivirus para Android o Iphone.
- Realizar las actualizaciones periódicas de la apps y el sistema operativo del celular, a los hackers les gusta explotar los agujeros de seguridad contra las versiones antiguas de las apps, a través de esas vulnerabilidades pueden robar datos y dinero, de esta manera se evita que ingresen por la puerta trasera.
- Activación de antirrobo en el celular con la opción de borrado remoto.
- Asegurar que la contraseña contenga solo uno o más caracteres, prevenir el uso del usuario y contraseña para cuentas financieras.
- Considerar un bloqueo de pantalla o patrón en el dispositivo móvil.
- Tener precauciones sobre los mensajes que recibe desde un sitio web.

Como en gran parte existen también varias formas de realizar procesos online es parte de tráfico de mensajes SMS que tampoco cuenta con un proceso de cifrado seguro. De tal manera que es necesario que todos los datos viajen encriptados Punto a punto utilizando un modelo de seguridad por capas conjunto en proceso de integración NT.

Dentro de algunas de las recomendaciones que son clave para las entidades es la innovación y la educación un gran reto para los usuarios enfocada hacia el uso de Banca en línea que traen varios beneficios que son importantes tales como: Verificación de las transacciones en tiempo real, alertas en caso de fraude, recordatorios de pagos y las notificaciones en SMS. [6].

La interacción real con cada uno de los clientes es importante al prestar un servicio de banca móvil, al mismo tiempo se debe enfrentar a grandes retos de seguridad, es por esto que los clientes se preguntan si este servicio es 100% seguro, de ante mano es importante que se conozca las recomendaciones para los Cio, tales como:

- Innovación: Todas las instituciones deben llevar a cabo reuniones periódicas donde se defina un proceso de autenticación conocido como Fuera de Canal, en función a transacciones online, ya sea por medio de notificaciones Push o Sistemas biométricos.
- Educación: Llevar a cabo programas de concientización enfocada a que entiendan la importancia, verificando cada uno de los perfiles para validar si el proceso funciona correctamente.

Este servicio funciona cuando el usuario autoriza un login y/o transacciones mientras que el servicio Push puede ser insertada directamente desde los dispositivos móviles agregando beneficios de un canal que es totalmente protegido.

IX. ANALISIS REALIZADO DEL SERVICIO MÓVIL

Se calcula que en Colombia, uno de cada dos usuarios ya vienen utilizando este servicio con el fin de realizar transacciones, consultar saldos o transferir dinero a través del dispositivo móvil. De acuerdo a las investigaciones realizadas en el mercado los pagos electrónicos han ganado un gran alce frente al uso de dinero en efectivo.

Las entidades como la Superintendencia Financiera vieron el gran alcance que tiene las transacciones electrónicas en el país. También hay un estudio realizado enfocado al impacto de la Banca móvil tales como la seguridad, confidencialidad que representan a las personas que son reaseas frente al uso de los Smartphone en cuanto a realizar transacciones bancarias. Pero existen varias razones por las cuales las personas prefieren este servicio:

- Rapidez del 66% de los encuestados mencionaron que la conectividad permanente posicionan a los Smartphone como una de las alternativas que ligera el proceso y que brinda comodidad.
- Ahorro de tiempo del 60% la gente afirma que utilizan los dispositivos móviles para realizar operaciones de ahorro sustancial
- Flexibilidad del 59% la gente afirma que pueden realizar cualquiera de las operaciones desde cualquier lugar y en el momento que se desee. [7]

X. CONCLUSIONES

Hoy en día, no hace falta estar frente a un computador o tablet para la administración de las cuentas, también hay lugar desde un dispositivo móvil. Las aplicaciones bancarias permiten pagar facturas, transferencia de dinero que en gran manera no podemos definirlas en todo como seguras. A pesar que estas son limitadas de acuerdo a las condiciones de seguridad tales como el pin, user, password, muchas de las veces no se cuentan con programas de concientización a las personas que realizan este proceso, aunque es dispendioso, muchas de las veces no se conocen si se comprueba que la aplicación móvil del banco es validada y que cumplen con todos los requisitos de seguridad.

En términos generales, hay varias amenazas para los Smartphone como también los ordenadores, sin embargo hay aplicaciones androide que son maliciosas implicando un peligro tanto para la información confidencial que se está navegando dentro del celular. Por esta razón se recomienda que las entidades Bancarias o entre otras que se presta este servicio informen e indique cuál es su aplicación oficial y mencionen propiamente a todos las personas que utilicen este servicio, llevar a cabo programas de concientización por medio de comunicaciones de mercadeo (Marketing) ayudaría a que todas las personas conozcan que es un mejor servicio para manejar y que tipo de controles se deben llevar a cabo cuando impliquen a suministrar la información confidencial como el número de cedula , número de tarjeta de crédito.

Dentro de los grandes avances que Colombia ha avanzado desde el año 2000 del servicio de tecnología financiera sigue siendo accesible gracias a los sistemas electrónicos y de las comunicaciones.

El mundo de la tecnología avanza rápidamente, puesto que es importante estar mejor actualizados, al ser más competitivos y usar la tecnología a favor de los grandes cambios. Sin lugar a duda, la estrategia móvil será importante para el futuro emisores de tarjetas y operadores. Teniendo en cuenta lo que hoy en día la posesión móvil se ha generalizado en todos los medios, comercio móvil o m-commerce como el factor de desarrollo de los pagos móviles. Estos avances han implicado a que todas las personas conozcan las políticas de seguridad que las entidades han optado.

Por esta razón el modelo de riesgos para la seguridad de la información aplicándolo correctamente dentro del proceso de banca móvil se puede llevar a cabo al cumplimiento de los objetivos, porque ofrece un planteamiento de las medidas de control que ayudan a que el proceso se lleve a cabo optimo y lograr afrontar un evento que puede romper el principio de la seguridad informática de las organizaciones que presten este servicio que en gran manera ha revolucionado el mundo de la tecnología bancaria o entre otras online.

De igual forma es importante que todos los miembros de la organización conozcan este servicio ya que en gran parte ayudaría a que se lleven a cabo programas de concientización,

estadísticas donde pueden implicar a mejoramiento del proceso que lleva a mejoramiento continuo o hasta llevar a una matriz de comunicaciones que puedan implicar a mejora muchos de los procesos.

Dentro de las ventajas que los usuarios encontramos de este servicio online en gran parte se reduce a las grandes filas, costos, seguridad, pago de servicios online, se despide del token, las compras son informadas. Es por esto la importancia de concientizarnos en saber controlar en cuanto a la divulgación de la información, en este medio donde la tecnología avanza con el tiempo implica a llevarse a cabo controles de buen funcionamiento para contrarrestar a que los hacker no intenten infiltrarse a los sistemas electrónicos, ya sea por malware u otro medio.

REFERENCIAS

[1] *CCM, "Qué es el pago móvil", [online], Disponible:* http://es.ccm.net/faq/11407-que-es-el-pago-movil.

[2] *Heraldo, Servicios financieros móviles, una realidad que transformó el uso del dinero", [online], Disponible: http://www.elheraldo.co/noticias/tecnologia/servicios-financieros-moviles-una-realidad-que-transformo-el-uso-del-dinero-7971*

[3] *Mobile Financial Services, Claro y Banco Popular presentan servicio efectivo Móvil,[online], Disponible: http://www.serviciosfinancierosmoviles.com/claro-y-banco-popular-presentan-servicio-e-fectivo-movil/#.VmciostdFD8*

Mobile Financial Services, Bancolombia lanzó su 'billetera móvil',[online],Disponible:http://www.serviciosfinancierosmoviles.com/bancolombia-lanzo-su-billetera-movil/#.VmcjD8tdFD8

[4] *Colombia Digital, "Usuarios móviles, un mercado creciente en LaTam",[online],Disponible: https://www.colombiadigital.net/actualidad/noticias/item/8158-%20usuarios-%20moviles-un-mercado-creciente-en-latam.html*

[5] *El país, "Así roban su dinero a través de fraudes electrónicos", [online], Disponible: http://www.elpais.com.co/elpais/judicial/noticias/asi-roban-su-dinero-traves-fraudes-electronicos*

[6] *CioPerú, "Recomendaciones de seguridad para la Banca Móvil", [online],Disponible:*http://cioperu.pe/articulo/16186/dos-recomendaciones-de-seguridad-para-la-banca-movil/

CioPerú, "7 consejos de seguridad para acceder a tu banco desde el teléfono", [online], Disponible: http://articulos.softonic.com/consejos-seguridad-banco-smartphone

[7] *Hsb Noticias, "Cinco razones para elegir las transacciones bancarias desde el celular", [online], Disponible: http://hsbnoticias.com/noticias/ciencia/tecnolog%C3%ADa/cinco-razones-para-elegir-las-transacciones-bancarias-desde-219008*