TÍTULO DEL TRABAJO DE GRADO

Estrategias para implementar el correcto manejo de la seguridad bancaria en los usuarios del sistema financiero para realizar transacciones a través de plataformas virtuales

AUTORES

Katherine Paola Pico Silvera Cc. 1.098.769.918

John Sebastián Mantilla Calderón Cc. 1.095.823.170

UNIDADES TECNOLÓGICAS DE SANTANDER

FACULTA DE CIENCIAS SOCIOECONOMICAS Y EMPRESARIALES

TECNOLOGIA EN BANCA Y FINANZAS

BUCARAMANGA

FECHA DE PRESENTACIÓN 18-03-2019

TÍTULO DEL TRABAJO DE GRADO

Estrategias para implementar el correcto manejo de la seguridad bancaria en los usuarios del sistema financiero para realizar transacciones a través de plataformas virtuales

AUTORES

Katherine Paola Pico Silvera Cc. 1.098.769.918
John Sebastián Mantilla Calderón Cc. 1.095.823.170

Trabajo de Grado para optar al título de

Estrategias para implementar el correcto manejo de la seguridad bancaria para realizar transacciones a través de plataformas virtuales

DIRECTOR

Juan Carlos Ruiz Sarmiento

I&D FINANCIERO

UNIDADES TECNOLÓGICAS DE SANTANDER
FACULTAD DE CIENCIAS SOCIOECONOMICAS Y EMPRESARIALES
TECNOLOGIA EN BANCA Y FINANZAS
BUCARAMANGA
FECHA DE PRESENTACIÓN 18-03-2019

Nota de Aceptación

_____

_____

_____

_____

_____
Firma del jurado

_____
Firma del Jurado

DEDICATORIA

Dedicamos este trabajo de grado a nuestros compañeros uteistas para que puedan acceder a estos conocimientos que son de gran importancia para su vida personal y laboral.

A nuestros queridos docentes que son la fuente de sabiduría y que nos transmitieron sus conocimientos para lograr esta meta.

A nuestros familiares que son la base de nuestras vidas y que participaron indirectamente en nuestro proyecto.

AGRADECIMIENTOS

Queremos agradecer a Dios por ser la guía y quien nos ha brindado la oportunidad de llevar a término final esta carrera que con mucho esfuerzo hemos construido.

Agradecemos a nuestros distinguidos docentes en especial al profesor Juan Carlos Ruiz Sarmiento que con su apoyo y dedicación vertieron en nosotros su sabiduría y se han convertido en la base y refuerzo para lograr y cumplir con nuestros deberes institucionales.

A nuestros padres Juan Pico, Jacqueline Silvera y Reinaldo Mantilla, Martha Calderón ya que ellos nos han brindado su apoyo y amor incondicional, nos han inculcado valores y nos han motivado a seguir y alcanzar nuestros sueños.

Por último nuestros agradecimientos al comité de trabajo de grado que nos ha brindado la oportunidad de consultar, desarrollar, complementar y culminar los propósitos de está nuestra monografía con la certeza de que sus mecanismos aportados formarían base para culminar con éxito nuestro propósito.

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

RESUMEN EJECUTIVO

En este presente trabajo daremos a conocer los riesgos más comunes que viven los usuarios del sistema financiero al realizar sus transacciones virtuales en los diferentes medios ya que por el mal uso de la seguridad bancaria y la falta de cultura y conocimientos, muchos usuarios se han visto afectados y han sido víctimas por los diferentes fraudes en las plataformas virtuales lo que ha conllevado a que los consumidores tengan un mal concepto de la banca móvil y la banca online.

Según las entidades financieras los usuarios aun no tienen una buena cultura para usar adecuadamente las plataformas y aplicaciones de las entidades bancarias, además se presenta una gran desconfianza al uso de la red por motivos de la seguridad y la privacidad. Por tal razon analizaremos, evaluaremos y corregiremos la percepción negativa que tiene los usuarios acerca de las transacciones virtuales permitiendo que se maximice la seguridad, facilidad y la confianza de ellos hacia las transacciones en la banca movil y en línea.

Para lograr estos objetivos propondremos estrategias de seguridad bancaria que le permitan a los usuarios del sistema financiero poder tener unos conocimientos y una orientacion para que eviten y minimicen los riesgos que trae el uso incorrecto de los mecanismos virtuales afectando la seguridad informática y esto se hará por medio de recomendaciones puntuales elaboradas por los bancos. Para ello se utilizará mecanismos de divulgación para que los usuarios puedan conocer e implementar estas estrategias y se pueda crear una cultura de seguridad bancaria.

PALABRAS CLAVE. Análisis, Banca, Estrategias, Propuestas, Seguridad

INTRODUCCIÓN

En el siguiente trabajo los lectores encontraran las razones por las cuales se pretenden dar a conocer las estrategias de seguridad para un manejo adecuado de las plataformas virtuales al hacer transacciones bancarias, ya que gracias a la popularización de la banca móvil y en línea son muchos los usuarios del sistema financiero que han empezado a implementarlo en el país lo que conlleva a que un gran número de clientes tengan acceso a los diferentes productos y servicios de la instituciones financieras permitiéndoles realizar transacciones por medio de un dispositivo móvil o computadora de manera ágil, segura y sin hacer largas filas. En Colombia desde hace 10 años se viene trabajando el tema de la seguridad informática sin embargo éstos conocimientos e implementación aún no han sido apropiados por parte de los clientes lo que ha provocado grandes problemas y dolores de cabeza para las entidades financieras afectando la seguridad bancaria y a los usuarios del sistema financiero. (MINTIC, s.f.)

Unas de las amenazas que enfrentan los usuarios de la banca móvil y en línea son el Phishing (mensajes falsos para robar información), Pharming (redirige a los usuarios a otros sitios webs falsos), Smishing (técnica a base de ingeniería social que hace estafas por medio de SMS), estas técnicas entre otras han permitido vulnerar la seguridad bancaria afectando los datos personales y el bolsillo de los usuarios logrando una percepción negativa hacia la banca móvil y en línea. Según un estudio realizado por la multilatina Digiware en Colombia son generados 542.465 ataques informáticos diarios de los cuales 39,56 % pertenecen al sector financiero (Portafolio, 2017)

Por las razones mencionadas anteriormente nace el interés de realizar este trabajo ya que se pretende dar a conocer en un contexto más profundo acerca de la seguridad bancaria y el manejo adecuado de las plataformas virtuales para poder realizar transacciones con seguridad y confianza devolviendo la tranquilidad a los usuarios del sistema financiero Colombiano, para esto se requiere y se plantea conocer los medios de uso más comunes para hacer transacciones en las plataformas virtuales, sus riesgos, estrategias que permitan a los usuarios poder realizar sus transacciones de manera segura y confiada y por último los medios para divulgar dichas estrategias.

La metodología, entendida como el procedimiento empleado para el logro de un objetivo, se desarrolló en el presente trabajo, mediante el Marco Lógico, estudiando información obtenida, para después proceder a darle una estructuración lógica, con el fin de poder establecer un orden de tal manera que fuera posible diagnosticar el contenido, dando como resultado las conclusiones sobre el tema propuesto.

1. DESCRIPCIÓN DEL TRABAJO DE INVESTIGACIÓN

1.1. PLANTEAMIENTO DEL PROBLEMA

El presente trabajo de grado se realiza por la necesidad de proponer y dar a conocer estrategias que le permitan al usuario del sistema financiero poder realizar sus transacciones de manera segura y confiada en la banca móvil y en línea.

En los últimos tiempos vemos por noticias y por diferentes medios de comunicación como los consumidores de productos y servicios financieros son víctimas de la inseguridad bancaria como lo son el Phishing que también es conocido como suplantación de identidad por medio de correos electrónicos, el Pharming en la cual los usuarios son re-direccionados a una página web fraudulenta y el Smishing en la cual se envían mensajes pidiendo información, lo que ha conllevado a que los clientes de las entidades financieras desconfíen de realizar transacciones en las diferentes plataformas virtuales y aplicaciones que ofrecen permitiendo crear una percepción negativa de la banca móvil.

Esto en cierta parte también se debe a la falta de educación financiera de la población, a la carencia de una cultura de seguridad bancaria y que las personas no tienen una orientación y unos conocimientos para que puedan implementar y aplicar en su vida permitiendo mejorar su seguridad en las transacciones virtuales. Estos problemas pueden conllevar a que los delitos cibernéticos aumenten y a que un gran porcentaje de usuarios colombianos disminuyan el uso de la banca móvil. Por tal razón nos hacemos esta pregunta ¿Qué estrategias se pueden implementar para aumentar la seguridad bancaria y corregir la mala percepción de la banca móvil en los usuarios del sistema financiero colombiano?

Para esto se vió la necesidad de conocer más a fondo qué es la banca móvil, los riesgos y fraudes de los ciberdelincuentes y las estrategias a implementar para la seguridad bancaria

1.2. JUSTIFICACIÓN

Con la evolución y crecimiento de la tecnología las entidades financieras han optado por expandir sus productos y servicios financieros a través de las plataformas de servicios virtuales y aplicaciones que les permiten a los usuarios poder hacer sus transacciones ya sea por medio de un ordenador o por un dispositivo móvil desde cualquier lugar, lo que ha conllevado a la bancarización y a la inclusión social del sistema financiero.

Por tal razón se ve la necesidad de desarrollar un manual de estrategias que permita aumentar la seguridad bancaria en los usuarios del sistema financiero Colombiano para que se pueda mejorar el manejo de la seguridad informática debido a las técnicas de los ciberdelincuentes por vulnerar dicha seguridad permitiéndoles conocer dichas estrategias para mejorar y dar un adecuado uso a los servicios del sistema financiero.

1.3. OBJETIVOS

1.3.1 OBJETIVO GENERAL

Desarrollar un Manual de estrategias que permita aumentar la seguridad bancaria y mejorar la percepción de la banca móvil y en línea, en los usuarios del sistema financiero Colombiano, que permita mejorar su nivel de aceptación en cuanto al manejo de la seguridad informática y el correcto uso de los servicios financieros a fin de minimizar el riesgo de los mismos.

1.3.2 OBJETIVOS ESPECÍFICOS

a. Identificar los medios de uso más comunes para hacer transacciones virtuales.
b. Identificar los riesgos en las transacciones virtuales que afectan la seguridad informática y la protección de datos personales.
c. Proponer estrategias de seguridad bancaria por medio de recomendaciones realizadas por bancos y entidades financieras para que los usuarios puedan realizar sus transacciones virtuales de manera segura, confiada y fácil.
d. Utilizar Mecanismos de divulgación para que los usuarios conozcan estas estrategias propuestas.

2. MARCO REFERENCIAL

2.1.1 Marco Teórico

la globalización ha permitido que las nuevas tecnologías evolucionen para realizar y facilitar las tareas del día a día, además con dicha evolución el acceso a la información bancaria por medio de estas plataformas tecnológicas se ha vuelto masiva y una necesidad para los usurios y clientes del sistema financiero, lamentablemente en la última decada se han encontrado puntos de acceso con ciertas vulnerabilidades en estas plataformas bancarias, la cual puede ser entre spyware de contraseñas y la ingenieria social utilizada por muchos ciberdelincuentes entre otros métodos.

Hablar sobre la seguridad es importante y de la informática mas revelante aun, mezclando juntos estos términos tenemos que destacar el porqué ésta area de las TICS, está evolucionando tan constantemente ya que practicamente se esta accediendo a la mayoria de los servicios de manera digital y escasamente se acude ahora a un punto fisico.

La seguridad informática se ve vulnerada por cibercriminales que gracias a las diferentes herramientas y métodos de robo informático, hurtan tanto información de personas para utilizarlas en su contra como el dinero de los clientes de las entidades bancarias permitiendo que esto sea un atractivo para la formalizacion de bandas criminales.

Consecuencia de esto unos de los avances que han permitido el fortalecimiento de la seguridad informática ha sido la creación de softwares como antivirus potenciales que han detectado a tiempo diferentes malwares, la huella digital al ingreso de las aplicaciones móviles para la verificación lo cual lo hace muy seguro, en los nuevos smartphone se

implementa tambien la verificación facial y lo mas importante las diferentes campañas de sensibilización que realizan dichas entidades para que los usuarios sean consientes del manejo de su información personal.

Hoy en día para nadie es un secreto que los ataques a las grandes organizaciones y personas que poseen alguna información importante, va a ser un objeto atractivo y puede verse vulnerada dicha información por los ciberdelincuentes o hackers, ahora bien, depende de los usuarios darle un buen uso a los datos personales y evitar de suministrar información que puedan usar de manera ilícita.

En la actualidad para los usuarios de las entidades bancarias hay un sistema muy interactivo el cual cada retiro, avance, consignación, automáticamente llegará a su dispositivo celular un aviso, también se le avisa acerca de la información bancaria de su interés y los diferentes mantenimientos de la sucursal bancaria virtual, además de ello cuenta con un soporte y atención las 24 horas del día los 7 días de la semana el cual estará pendiente de cualquier inconveniente que pueda ocurrir en algún momento inesperado.

Constantemente son muchas las personas que requieren y usan la banca móvil y la banca en linea para realizar transacciones, consultas bancarias, acceso token para retiro de dinero a través del móvil, pagar sus recibos de servicios públicos e impuestos del estado todo esto gracias a la seguridad informática que se implementa y que se actualiza constantemente para dar confidencialidad, facilidad y confianza al realizar estas transacciones.

2.1.2 Marco Conceptual

Uno de los grandes desafíos para américa latina y Colombia es mejorar su seguridad en temas informáticos ya que se estima que el 70% de las empresas consideran que su información esta en grave peligro de ser descifrada, y proveer estas bases de datos como actividad ilícita, todo esto mediante una serie de códigos maliciosos. Respecto a la seguridad informática se realizaron varios estudios, la mayoría han tenido un resultado cercano al 35% que las empresas han sido atacadas durante el último año. Ahora las prácticas mas comunes que se realizan son la toma de información de empresas para venderlas como bases de datos o el fraude. ¿Ahora cómo podemos tener mas control sobre la seguridad informática en cualquier empresa?

- Un equipo de seguridad: cada empresa debe tener un ingeniero de sistemas y un equipo de seguridad y también saber por quien esta constituido nuestro equipo de seguridad informática.
- Analizar respuesta: cómo podemos responder rápidamente a un ataque que requiera una prioridad.
- Periocidad: Se deben establecer ideas lógicas de cual serán los ataques recibidos y como se puede responder lo más eficaz, así lograr identificar y solucionarlo también de la manera más adecuada

Todas las empresas tienen o tendrá al menos un incidente de seguridad informática, teniendo en cuenta esto se debe tener acciones para tener la seguridad de sus clientes , y su participación continua en la entindad bancaria sin riesgos. A continuación se evidencian

varias vulnerabilidades en ciertas páginas bancaria que necesitan ser verificadas y corregidas para el correcto fucionamiento.

Santiago Hernández (2017) Afirma “La seguridad de la información bancaria es un aspecto vital de los bancos y compañías financieras”. A continuación se les compartirá el artículo realizado por el Consultor en Seguridad de la Información Santiago Hernández, donde muestra algunos puntos claves en seguridad de la información en el sector bancario como sus riesgos.(P.1)

EVIDENCIAS

1. Davivienda

Vulnerabilidades encontradas:

- Cifrados inseguros
- Firma de certificado insegura
- Poodle

2. Banco de Bogotá

Vulnerabilidades encontradas:

- Poodle
- Firma de certificado insegura
- No soporta FS
- Cifrados inseguros
- Protocolos modernos no habilitados

3. Banco de Occidente

Vulnerabilidades encontradas:

- Protocolos modernos no habilitados
- Poodle
- No soporta FS
- Cifrados inseguros
- Firma de certificado insegura

4. Banco Popular

Vulnerabilidades encontradas:

- Poodle
- Cifrados inseguros
- Protocolos modernos no habilitados
- No soporta FS

5. Bancolombia

Vulnerabilidades encontradas:

- SSLv3
- Cifrados inseguros

- No soporta FS

Santiago Hernández, (2017) afirma "También teniendo en cuenta que estas son las vulnerabilidades de las plataformas, pero también existen programas o archivos maliciosos que también pueden exponer la información"(P.5)

ATAQUES SIMULTANEOS ATRAVEZ DE MENSAJES

Un ataque de servicio distribuido es aquél en el que una multitud de sistemas (que previamente han sido comprometidos), se ayudan para sacar un beneficio común, dinero , claves información personal.

Son muchos los usuarios que usan alguna aplicación de la banca móvil y que usan la banca en línea para realizar sus transacciones lo cual puede verse como un blanco para los ciberdelincuentes, lo que ha conllevado a que éstos tengan como objetivo crear artimañas y métodos que les permita de alguna u otra forma vulnerar la seguridad y la privacidad para obtener dicha información personal y bancaria para así sacar provecho de ello. Lo métodos que frecuentemente se usan son:

La fuerza bruta: El ataque de fuerza bruta consiste en intentar descifrar una contraseña mediante el uso de contraseñas que lo asocien a algo familiar o personal, número de la cédula, año en que nació nombre y su año de nacimiento, intentando varias combinaciones que pueden terminar accediendo. Los hackers prueban distintas combinaciones al azar, conjugando nombres, letras y números, hasta que dan con el patrón correcto. Números, fechas de nacimiento, nombres de mascotas y nombres de actores y actrices son las contraseñas más utilizadas por los usuarios.

Diccionario del hacking: Este método también se podría considerar como la anterior, de fuerza pero con la diferencia que se hace el trabajo automáticamente pero, en este caso, un software se encarga automáticamente de descifrar la contraseña. Empiezan por palabras simples y luego más complejas. Este tipo de programas pueden hacer hasta 50 intentonas por minutos en algunos casos y, según un informe, más del 50% de las contraseñas robadas se obtuvieron de esta forma.

Phishing: Se ha convertido en una de las herramientas más utilizadas por los hackers para robar contraseñas y nombres de usuario. Consiste en engañar a la víctima para que rellene un formulario falso con sus credenciales de inicio de sesión. Se crea un correo falso el cual pide información bancaria ya sea de sus tarjetas de créditos y sus claves con la razón de ser un mantenimiento o por seguridad, pero al enviar esta información se llevaran la sorpresa de que le han vaciado su cuenta, por este método cae mucha gente anualmente ya que tienen una apariencia muy similar, y se hacen pasar por dicho banco.

El Spidering o Araña web: Es un bot que inspecciona automáticamente las páginas web. Una de sus aplicaciones más comunes es realizar una copia de todos los sites para crear sistemas de búsquedas más rápidos. Normalmente se usa en grandes empresas con bases de datos amplias para sacar mayor beneficio.

Ataque key logger: Este procedimiento es similar al phishing o suplantación de identidad, actúa atreves de un formulario en el cual al enviarlo este servidor tiene acceso a esa información para usar a su disposición en cualquier momento.

Rainbow table: Es unas tablas programas para ocultar la información de tal manera esta estará expuesta al ser trasmitida por un servidor.

Está en nosotros implementar seguridad informática en nuestras vidas así evitando incidentes de estos, y también usando la red y las aplicaciones bancarias de manera adecuada.

3. DESARROLLO DEL TRABAJO DE GRADO

3.1. Pasos para el desarrollo del proyecto bajo la Metodología del Marco lógico.

Análisis de la situación {
- Matriz de Involucrados
- Árbol del problema
- Árbol de objetivos
- Alternativas de solución
- Matriz de marco lógico
- Documento técnico
- Hilo conductor

3.1.1 Matriz de Involucrados.

Tabla 1. Matriz de involucrados

GRUPO DE INVOLUCRADOS	INTERESES	PROBLEMAS	RECURSOS Y MANDATOS
Usuarios	Conocer acerca de la banca móvil y en línea, conocer estrategias de seguridad bancaria y tener plena seguridad y confianza para realizar transacciones en las plataformas virtuales	Carencia de conocimiento acerca de la banca móvil y en línea, desconocimiento de estrategias de la seguridad bancaria e inseguridad y desconfianza en realizar transacciones por estos medios	Acceso al Manual de estrategias para la seguridad bancaria
Entidades Financieras	Acceder a una mayor base de clientes por medio de la banca móvil y en línea, mayor expansión de los productos y servicios financieros, percepción positiva de la banca móvil y en línea	Crecimiento lento de bancarización en la población, poca expansión de los productos y servicios financieros, percepción negativa de la banca móvil y en línea debido al cibercrimen	Publicidad por medio de volantes a las personas que frecuenten las entidades bancarias y en Redes sociales como Facebook e Instagram
Estudiantes	Aplicación del conocimiento adquirido en el correcto manejo de la seguridad bancaria para realizar transacciones virtuales	Poco interés por aplicar e implementar las estrategias de seguridad bancaria	Acceso al Manual de estrategias para la seguridad bancaria
Docentes	Complementar los conocimientos determinados de una	Falta de sentido de aprendizaje por parte de los estudiantes en la	Estatuto Docente- Octubre 16 de 2016, UTS.

	temática al estudiante desde un nivel básico.	búsqueda y ampliación de nuevos saberes para la formación de un plus profesional.	
Programa	Liderar a nivel regional y departamental la implementación de la seguridad bancaria para realizar transacciones virtuales	Poca integración por parte de los estudiantes graduados al entrar en la educación superior en el programa académico de Banca y finanzas	Divulgación Recurso Humano

3.1.2 Árbol de problemas.

Tabla 2. Árbol de problemas

EFECTO FINAL
Problemas y atrasos en captación de dinero por parte de las entidades bancarias.

EFECTO INDIRECTO	EFECTO INDIRECTO	EFECTO INDIRECTO
Disminución del flujo de dinero para las entidades financieras	Creciente atraso tecnológico y financiero	Crecimiento del desinterés en los usuarios para usar la banca móvil y en línea
EFECTO DIRECTO	**EFECTO DIRECTO**	**EFECTO DIRECTO**
Disminución de las transacciones en las plataformas virtuales por mal manejo de las mismas	Alto nivel de desconfianza e insatisfacción por los usuarios	Aumento de la inseguridad y crecimiento de nuevos cibercriminales

PROBLEMA CENTRAL
Poca aceptación por parte de los usuarios de la Banca móvil y en línea

CAUSA DIRECTA	CAUSA DIRECTA	CAUSA DIRECTA
Escaso conocimiento de la seguridad bancaria en las plataformas virtuales	Alto índice de cibercrimen	Escasas estrategias para aumentar la seguridad bancaria en la banca móvil y en línea
CAUSA INDIRECTA	**CAUSA INDIRECTA**	**CAUSA INDIRECTA**
Alta Ignorancia de las ventajas de usar la banca móvil y en línea como herramienta de la vida diaria	Alto miedo por parte de los usuarios para salir de la zona de confort para usar las plataformas virtuales	Bajas propuestas para aumentar el uso de la banca móvil y en línea

3.1.3 Árbol de objetivos.

Tabla 3. Árbol de objetivos

	EFECTO FINAL	
	Aceptación y uso de las aplicaciones móviles. Así todo el contenido de la banca desde su dispositivo.	
FIN INDIRECTO	**FIN INDIRECTO**	**FIN INDIRECTO**
Acertamiento y competitividad ante la globalización en las TICS, motivando el uso de estas plataformas digitales.	Competitividad en el conocimiento acerca de los sistemas virtuales, electrónico, móvil, entre otros.	Mejoría y asesoría online para dudas e inquietudes de la banca, también teniendo sus beneficios y características por usarla
EFECTO DIRECTO	**EFECTO DIRECTO**	**EFECTO DIRECTO**
Habilidad para obtener información integrada del portafolio digital de medios de pago online.	Mayor captación de clientes, e información de transacciones por medio de este uso online	Aumenta aceptación de clientes y variedad de portafolios para interactuar desde la aplicación móvil
	OBJETIVO CENTRAL	
	Crear un manual de estrategias, y motivar el uso adecuado de las Apps Bancarias móviles.	
FIN DIRECTO	**FIN DIRECTO**	**FIN DIRECTO**
Socializar y dar a conocer el portafolio de la aplicación en el proceso de transacciones bancarias,	definir los mecanismos de divulgación sobre el correcto uso y beneficios	Promueve la eficiencia y transfiere conocimiento a más personas para que utilicen este medio
FIN INDIRECTO	**FIN INDIRECTO**	**FIN INDIRECTO**
confort sin salir de su oficina para realizar las debidas transacciones y pagos virtuales,	Mejora la utilización de manera personal, profesional y empresarial	Mayor participación en el país en transacciones y uso de las aplicaciones bancarias.

3.1.4 Matriz de marco lógico.

Tabla 4. Matriz de Marco Lógico

Nivel	Resumen Narrativo de Objetivos	Indicadores	Medios de Verificación	Supuestos
Fin	Implementar el uso de las aplicaciones bancarias móviles, en Usuarios que no la utilicen y la desconozcan así Enseñando e informando la importancia en la comunidad del correcto manejo de estas, también descongestionando las sucursales bancarias, así obteniendo más flujo en el sector financiero	N° de personas que realizan un pago presencialmente, sobre N° de personas que hacen uso de la banca móvil.	Software. Y uso de bitácoras en transacciones bancarias frecuentes.	Mayor número de personas con el uso correcto de las aplicaciones móviles de la banca.
Propósito	Aumentar conciencia y el beneficio que trae usar aplicaciones móviles para las actividades financieras	Tasa de personas que no tienen conocimiento de aplicaciones móviles y por qué motivo no la han adquirido.	Informe detallado de los estudiantes y personas naturales enterados e interesados en descargar la aplicación móvil	Disminuir el número de personas que desconozcan el manejo y uso del producto.
Componente	Ofrecer charlas, conferencias, del debido uso e implementación de las aplicaciones móviles para el uso transaccional, diario con el fin de optimizar tiempo y dinero.	Porcentaje de personas que están interesados en estas charlas, y orientación de manejo de aplicaciones		Facilidad en la ejecución de transacciones por medio de esta herramienta,
Actividades	Aumentar el interés, y el uso de toda transacción que desee realizar por el medio bancario de la App.	Porcentaje significativo de personas con el uso de aplicaciones para ahorrar tiempo significativo y dinero.	Software del número de personas participantes tanto al inicio y como al final del proyecto. Registro y control de las personas que tomen información del correcto uso de la banca móvil	Habilidad para obtener información Las dificultades del uso de la herramienta móvil , así enfocándonos en solucionar

				estas problemáticas

Fuente: (Ortegón, Pacheco, & Prieto, 2005)

3.1.5 Documento Técnico.

INTRODUCCIÓN DEL MANUAL

Hoy en día es muy frecuente utilizar la banca en línea y la banca móvil para realizar transacciones virtuales, ya que estas herramientas ofrecidas por las entidades financieras han permitido mejorar la calidad de vida de los usuarios logrando reducir el tiempo, costos y permitiendo expandir la bancarización lo cual ha sido un logro muy significativo para el sector financiero.

Son muchos los usuarios que han dejado de hacer largas filas en los bancos y se han sumado a realizar sus transacciones virtualmente, no obstante el cibercrimen ha aumentado lo que ha conllevado a que los usuarios tengan inseguridad y desconfianza de realizar estas operaciones bancarias por estos medios que por lo general es causado por el mal uso de la seguridad bancaria y mal uso de los datos personales para realizar estas transacciones.

Ha continuación se dará a conocer en el presente manual los medios más comunes para acceder a la banca móvil y a la banca en línea, los riesgos que se presentan a diario al momento de hacer transacciones virtuales y las estrategias de seguridad bancaria que permitirán mejorar la percepción de la banca móvil y en línea creando una cultura de seguridad informática para disminuir el riesgo de ser atacados por ciberdelincuentes.

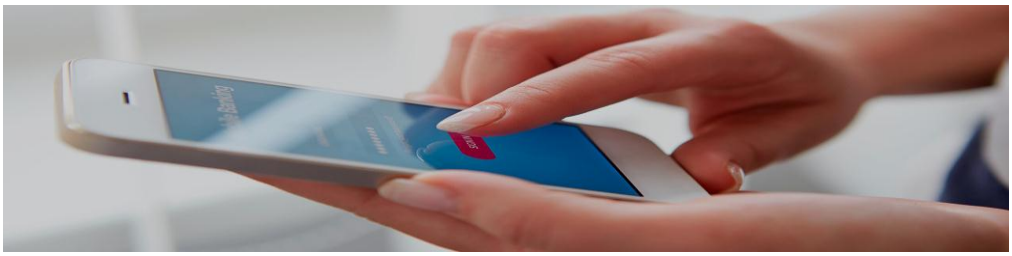


Figura 1. Tomado de: Asobancaria

MEDIOS DE USO MÁS COMUNES PARA HACER TRANSACCIONES VIRTUALES

La tendencia del siglo XXI está abriendo nuevos campos para las transacciones bancarias entre ellas se clasifican de acuerdo a su uso en frecuentemente y regularmente, también se diferencian, en qué tipo de dispositivo se usa para acceder a ellas. Con estas tenemos varias ventajas.

CLASIFICACIÓN DE ACUERDO A SU USO

Uso regular

La banca en línea: Se le conoce también con el nombre de banca electrónica, banca virtual o e-banking, ésta es la banca en la que se accede por medio del internet, básicamente es la página oficial del banco y en éste se encuentran todas las herramientas, para que puedan realizar las operaciones bancarias. Para ser más específicos acerca de los términos la banca electrónica hace referencia a que se accede por medios electrónicos para realizar dichas operaciones, la banca virtual hace referencia a que no se requiere presencia física para realizar transacciones y la banca en línea hace referencia al portal web que ofrece el banco para realizar las transacciones a través del internet.

¿Cómo se ingresa? Si es por internet sólo es necesario digitar la URL de la página de su banco y acceder con su número de cédula y clave. Ejemplo:

https://www.bancodecolombia.com

Figura 2. Tomado de: Alamy

¿Cuáles son los beneficios de la banca en línea?

✓ Reduce el tiempo: Se puede realizar transacciones de manera inmediata sin la necesidad de hacer largas filas en los bancos

✓ Realizar trámites donde quieras: Con la banca en línea se puede realizar transacciones desde el hogar, el trabajo, la universidad, el parque etc. sin la presencia física del banco

✓ Realizar varias transacciones al mismo tiempo: Se puede hacer movimientos bancarios como consulta de saldo, pagos de tarjeta de crédito, pagos de servicios, recargas y consignaciones

✓ Control y registro de cómo se mueve el dinero: Se podrá ver y revisar lo que se paga y lo que se recibe en la cuenta bancaria para así tener mayor información de los gastos mensuales y como poder ahorrar mas

✓ Seguridad en las transacciones: Por medio de un usuario y clave se podrá realizar transacciones de manera segura, además se tendrá plena seguridad ya que generalmente cada

banco permite la opción de ser notificado al correo electrónico o al número de celular por medio de un mensaje de texto al momento de realizar cualquier transacción bancaria

Figura 3. Tomado de: Negocenter

Dispositivos para la banca en línea

- ✓ Computador de escritorio
- ✓ Portátil
- ✓ Dispositivo móvil (solo ingresando al portal web del banco)

Uso frecuente

La APP Banca móvil: La banca móvil es proporcionada por los bancos a través de aplicaciones para poder realizar transacciones en las 24 horas del día. Se puede usar desde cualquier celular independientemente del operador que se tenga. La banca móvil actualmente es la opción más fácil para acceder a la información de las cuentas bancarias.

¿Cómo se ingresa? Cualquier persona con un dispositivo Smartphone puede acceder solo ingresando al market place o play store, descargando la aplicación del banco e ingresando su cédula y clave, con esto ya podrá usar los beneficios de esta entidad bancaria y con un acceso ilimitado.

¿Cuáles son los beneficios de la banca móvil?

- ✓ Disponibilidad las 24 horas, los 7 días de la semana: Se podrá ingresar a la aplicación del banco en cualquier momento y en cualquier lugar de acuerdo a la necesidad para realizar la transacción o para realizar la consulta
- ✓ Realizar varias transacciones : Se podrá consultar saldos, pagar la tarjeta crédito, pagar servicios públicos, transferir saldo y hacer recargas
- ✓ Permite mayor flexibilidad : Esto se debe a que no requiere el uso de un ordenador para realizar las transacciones
- ✓ Permite el proceso de bancarización: Para las poblaciones rurales y de bajos recursos es de gran ayuda ya que les permite el acceso a los servicios y portafolio bancario de manera fácil y cómoda
- ✓ Seguridad y confiabilidad: la banca móvil permite a los usuarios realizar sus transacciones de manera tranquila y confiable ya que previene fraudes y evita cargar con el dinero en efectivo

Figura 4. Tomado de: Bellbank

Dispositivos para la banca móvil

- ✓ Celular Smartphone
- ✓ Tablet

RIESGOS MÁS COMUNES EN LAS TRANSACCIONES VIRTUALES

Una de las razones por las cuales los usuarios temen al realizar sus transacciones bancarias en línea es el miedo a los fraudes realizados por ciberdelincuentes en la cual obtienen los datos personales provocando una gran debilidad en las cuentas bancarias para así hurtar el dinero de las personas, no obstante los bancos tienen implementados medidas cautelares para realizar las transacciones de manera segura, sin embargo la mayoría de los fraudes cometidos en la banca en línea se debe principalmente a errores cometidos por los usuarios en temas de seguridad bancaria, por lo tanto es necesario aclarar los riesgos más comunes que se presentan tanto en la banca en línea como en la banca móvil para que los usuarios puedan estar precavidos a la hora de realizar sus transacciones bancarias.

RIESGOS DE LA BANCA EN LÍNEA

Phishing (Pesca)

Es la suplantación de identidad en la cual el estafador se hace pasar por una persona o una entidad financiera en una comunicación electrónica por medio de correo electrónico en la cual el ciberdelincuente invita al usuario a dar click en un enlace el cual supuestamente lo direccionará a una página falsa del banco. Al final el usuario engañado ingresa a la página falsa del banco e ingresa sus datos personales y es así cómo los ciberdelincuentes obtienen la información personal para cometer los fraudes.

Figura 5. Tomado de: datamovil

Smishing (SMS – Phishing)

Es una variable de Phishing en la cual el ciberdelincuente usa los mensajes de texto de celular y la ingeniería social para engañar a los usuarios y así obtener tanto su información personal como financiera. En éste tipo de fraude el ciberdelincuente le envía un mensaje de texto por celular a la víctima en la cual lo invita a ingresar a una dirección de una página falsa de una entidad financiera en el cual cuando el usuario ingrese a dicha dirección de la página falsa del banco e ingrese los datos personales éste delincuente obtendrá tanto la información personal como la información financiera del usuario. Otra forma de Smishing es cuando el ciberdelincuente envía un mensaje de texto al número celular del usuario con un número de teléfono falso aparentando ser del Call center de una entidad financiera con el fin de que el usuario llame y poder obtener su información.

Figura 6. Tomado de: Securelist

Pharming

Consiste en vulnerar los software de los servidores DNS (Domain Name System) o de los equipos de los mismos usuarios, en el cual el ciberdelincuente redirige un nombre de dominio a un dispositivo electrónico, de esta manera cuando el usuario introduce el nombre del dominio será re direccionado a una página web falsa.

Figura 7. Tomado de: Seguridad movil

Software espía

En esta modalidad el ciberdelincuente instala un programa espía en el computador del usuario sin su autorización en el cual éste puede monitorear desde otros computador todas las actividades que realiza el usuario como visualizar las páginas webs que visita y la información que llega al correo electrónico para así obtener la información personal.

Figura 8. Tomado de: Locura informática digital

Keylogger

En esta modalidad el ciberdelincuente obtiene la información del usuario utilizando herramientas tanto software como hardware. En la modalidad de software el key logger captura todo lo que digita el usuario y lo envía a un correo electrónico que él mismo creó. Este es un software que se instala y funciona de forma invisible. En la modalidad del

hardware el ciberdelincuente instala un dispositivo al computador para que todo lo que digite el usuario en el teclado quede grabado en una memoria.

Figura 9. Tomado de: Locura informática digital

RIESGOS DE LA BANCA MÓVIL

Redes wi-fi públicas

Las redes wi-fi gratuitas como la de los parques, universidades, hoteles, aeropuertos etc. son poco seguras ya que éstas pueden ser manipuladas por los ciberdelincuentes para así llegar hasta los dispositivos móviles y obtener la información personal del usuario.

Figura 10. Tomado de: Seguridad móvil

Dejar la aplicación abierta

Esto permitirá el acceso a terceros a ingresar a la información de las cuentas bancarias y hacer fraudes. Aunque en la mayoría de las aplicaciones de los bancos después de un momento de inactividad la sesión se cerrará automáticamente solicitando nuevamente la cédula y clave del usuario para el nuevo ingreso a la APP.

Figura 11. Tomado de: Androidpit

ESTRATEGIAS DE SEGURIDAD BANCARIA PARA REALIZAR TRANSACCIONES VIRTUALES

EN LA BANCA EN LÍNEA

- ✓ **Realizar transacciones desde ordenadores confiables y evitar conectarse a redes wi-fi públicas**

Esto es muy importante y básico ya que el realizar transacciones en ordenadores y redes públicas como salas de internet, universidades, parques y hoteles podría llevar a que terceros puedan acceder a la información con programas que guarden contraseñas vulnerando así la seguridad informática**.**

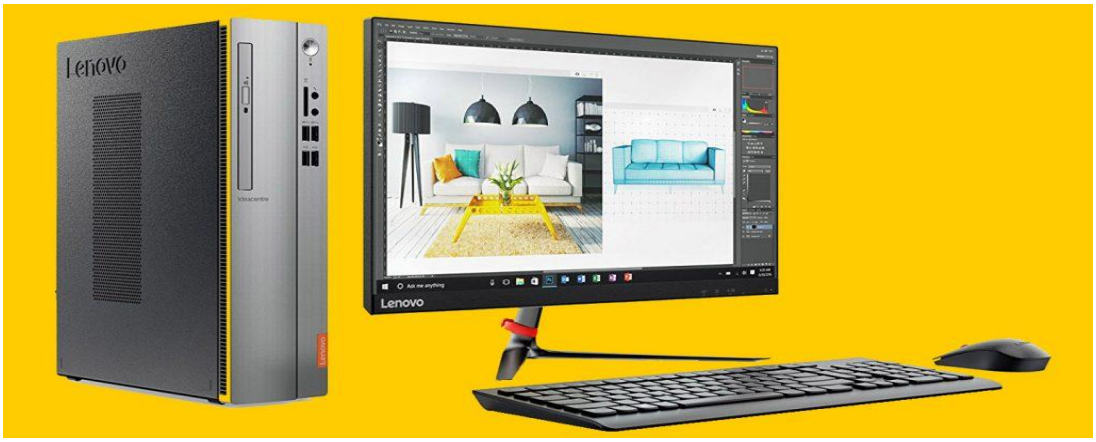


Figura 12. Tomado de: Androidpit

- ✓ **Instalar un antivirus y software de prevención anti-spyware y mantenerlos actualizados**

Esto permitirá una mayor seguridad previniendo los anuncios emergentes, amenazas de seguridad causadas por software no deseado y rendimiento lento.

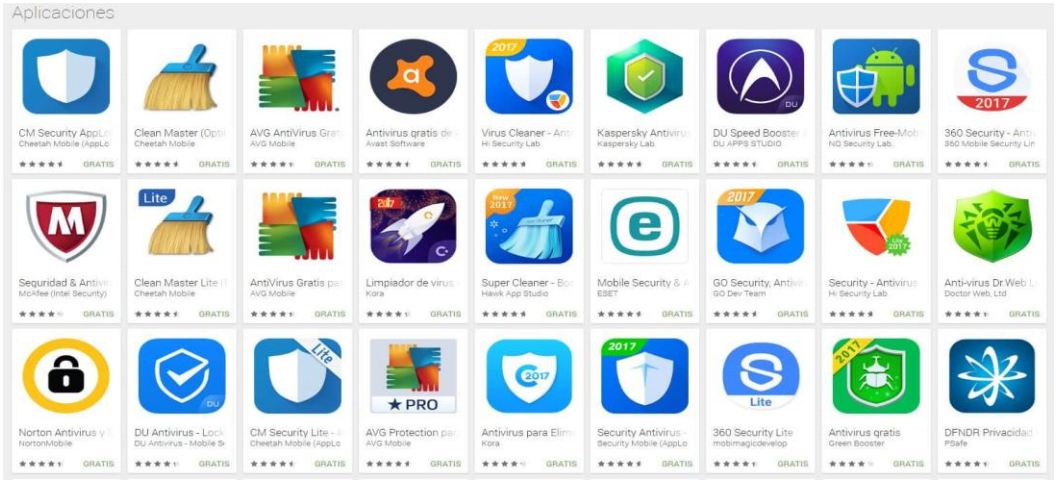


Figura 13. Tomado de: Pulso

- ✓ **Digitar siempre en la barra del navegador la dirección del Banco y verificar que esté seguida por https y un candado cerrado ya sea en la parte superior o inferior del navegador**

Es de vital importancia que los usuarios corroboren que la conexión esté segura mediante la observación de un icono en forma de candado que se encuentra en la parte superior izquierda del navegador de internet, llegado el caso de que el ícono del candado se encuentre abierto o de color rojo es importante abstenerse de continuar con la transacción.

Figura 14. Tomado de: Corpbanca

- ✓ **Cerrar siempre la sesión**

Cada vez que se ingrese al portal transaccional de una entidad financiera y se termine la operación se debe cerrar sesión de manera correcta y no en la "X" para cerrar el navegador.

Figura 15. Tomado de: Netrica

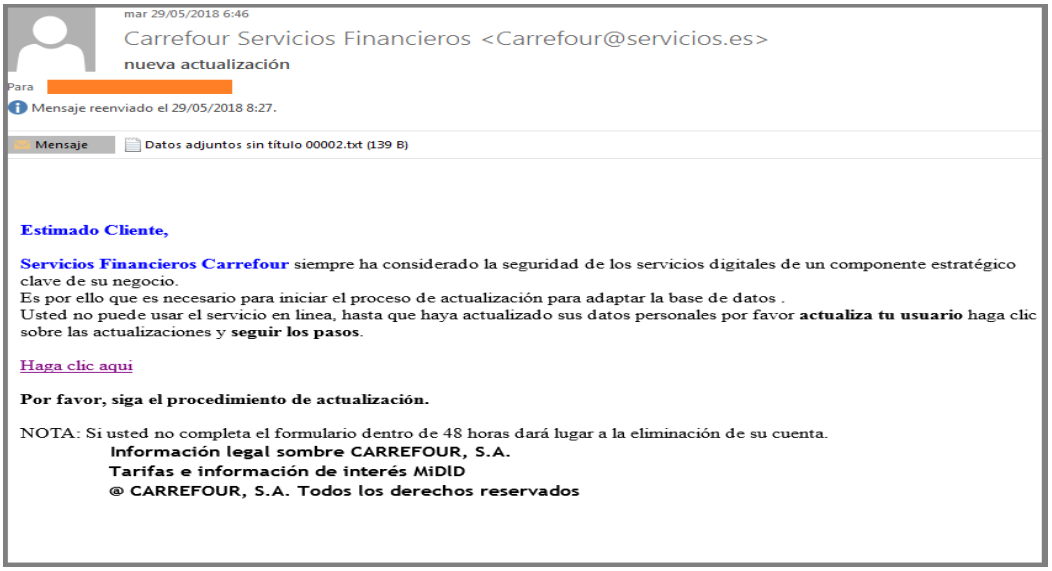
- ✓ **No ingresar contraseñas en las páginas webs a las que haya accedido por medio de un link enviado al correo electrónico**

Esto puede convertirse en Phishing, también cabe recordar de no dar la opción de guardar contraseña.

Figura 16. Tomado de: DiarioCrítico

- ✓ **No brinde información personal y financiera por medio de correos electrónicos**

Las entidades financieras nunca solicitan a sus clientes este tipo de información por este medio.



mar 29/05/2018 6:46

Carrefour Servicios Financieros <Carrefour@servicios.es>

nueva actualización

Para [redacted]

Mensaje reenviado el 29/05/2018 8:27.

Mensaje | Datos adjuntos sin título 00002.txt (139 B)

Estimado Cliente,

Servicios Financieros Carrefour siempre ha considerado la seguridad de los servicios digitales de un componente estratégico clave de su negocio.
Es por ello que es necesario para iniciar el proceso de actualización para adaptar la base de datos .
Usted no puede usar el servicio en línea, hasta que haya actualizado sus datos personales por favor **actualiza tu usuario** haga clic sobre las actualizaciones y **seguir los pasos**.

Haga clic aquí

Por favor, siga el procedimiento de actualización.

NOTA: Si usted no completa el formulario dentro de 48 horas dará lugar a la eliminación de su cuenta.

Información legal sombre CARREFOUR, S.A.
Tarifas e información de interés MiDID
@ CARREFOUR, S.A. Todos los derechos reservados

Figura 17. Tomado de: Oficina de Seguridad del Internauta

- ✓ **Mantener siempre el navegador del internet actualizado**

De esta manera la información que está encriptada será interpretada por los servidores correspondientes, además al estar actualizado se podrá verificar la autenticidad de la página web de la entidad financiera a la que se está ingresando.

Figura 18. Tomado de: El Blog de Nerion

- ✓ **Cambiar con frecuencia la clave**

Es de vital importancia cambiar con frecuencia la clave segura, y no utilizar contraseñas creadas con información personal como la fecha de nacimiento, además las mejores contraseñas son aquellas que tienen la combinación de letras, números y caracteres.

Figura 19. Tomado de: Santander Rio

EN LA BANCA MÓVIL

- ✓ **Utilizar el móvil personal para acceder a la APP del banco**

No es seguro utilizar dispositivos móviles de terceros para acceder a la APP de su banco, por seguridad es recomendable solo acceder desde el móvil personal.

Figura 20. Tomado de: Davivienda movil

- ✓ **Configurar el nivel de seguridad en el dispositivo móvil**

Configurar el móvil para que se bloquee por inactividad con un tiempo alrededor de 10 segundos o menos, y poner una contraseña de desbloqueo fuerte como un PIN.

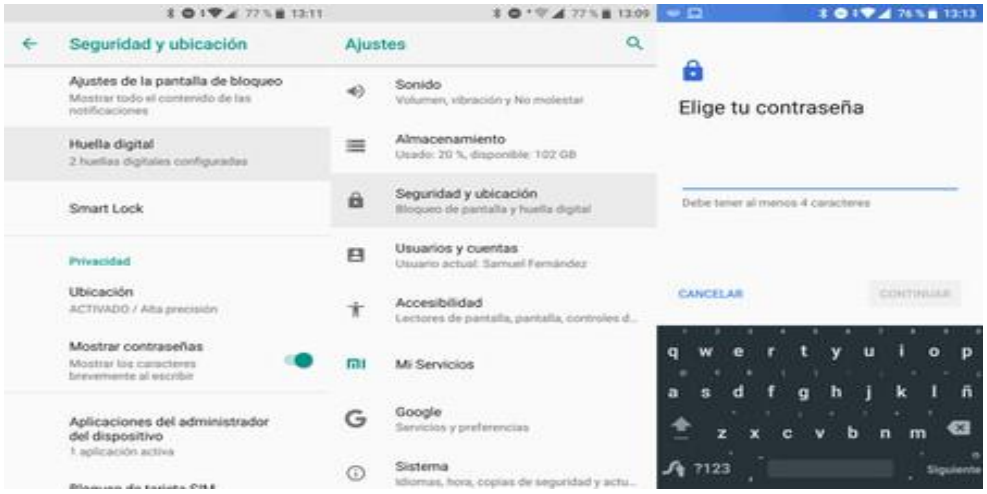


Figura 21. Tomado de: Xacata movil

- ✓ **No guardar la contraseña en la APP ni información de cuentas bancarias en el dispositivo móvil**

Esto permitirá prevenir que terceros puedan acceder a la información cuando se deja el móvil a disposición de otros.

Figura 22. Tomado de: Davivienda movil

- ✓ **Cambiar periódicamente la clave**

Además de cambiar la clave cierto periodo de tiempo es muy importante que se utilice claves diferentes para cada servicio de la entidad bancaria.

Figura 23. Tomado de: Davivienda

✓ **No conectarse a redes wi-fi públicas**

Ya que éstas pueden ser manipuladas para que los ciberdelincuentes obtengan la información personal del usuario, la mejor red privada son los datos móviles del teléfono.

Figura 24. Tomado de: Muy Sencillo

✓ **Cerrar sesión de manera correcta**

Cuando se esté dentro de la APP del banco se debe asegurar cerrar la sesión en la opción “Cerrar sesión” y no en la X.

Figura 25. Tomado de: Nequi

- ✓ **No hacer click en enlaces que dicen ser del banco cuando lleguen al correo electrónico o por mensajes de texto**

Para ello se puede ingresar al portal web del banco digitando la dirección URL propia sin que tenga el riesgo de acceder a una página falsa.

Figura 26. Tomado de: Banco de Bogota

- ✓ **Descargar la APP correcta**

Al momento de ingresar al Play Store ó APP Store descargar la aplicación correcta del banco del cual requiere.

Figura 27. Tomado de: Xacata movil

3.1.6 Métodos de divulgación.

✓ Semillero de la institución: Son una alternativa de investigación donde los espacios ideales que se realizan de manera extracurricular en la formación de la seguridad en aplicaciones bancarias, en los que participaran estudiantes bajo la orientación y el acompañamiento de nosotros aplicando la comunicación asertiva, para el fortalecimiento de las transacciones bancarias seguras y la implementación del manual de estrategias de seguridad bancaria, se realizara formulación de preguntas y respuestas abarcadas por nosotros los expertos, aplicación de métodos.

Los resultados derivados de este ejercicio formativo son divulgados mediante la publicación en revistas, en la página web de la formación académica de banca y finanzas, en revistas de la institución académica.

✓ Páginas web: Implementando el uso de las Tics, y de manera gratuita usando estos medios para dar a conocer la importancia del uso de las aplicaciones bancarias móviles, para el beneficio mutuo

✓ Panfletos en las clases extracurriculares: llevando a cabo la información del manual, de manera didáctica, muy visual, así dando a conocer la importancia de este como diario a vivir, y concientizando a la comunidad uteista.

Estos medios son más comunes para acceder a la banca móvil y a la banca en línea, los riesgos que se presentan a diario al momento de hacer transacciones virtuales y las estrategias de seguridad bancaria que permitirán mejorar la percepción de la banca móvil y en

línea creando una cultura de seguridad informática para disminuir el riesgo de ser atacados por ciberdelincuentes. De allí nace esta monografía para minimizar los riesgos y dar a conocer el amplio portafolio que pueden brindar una aplicación del banco en el dispositivo celular.

3.1.7 Hilo Conductor.

Tabla 5. Hilo conductor

ACTIVIDAD	TIEMPO(MESES)															
	1				2				3				4			
Etapa 1 : Recolección de información por medio de fuentes primarias y secundarias																
Se recolectará información y datos por paginas oficiales de entidades bancarias y por medio de entrevistas a contacto directo																
Etapa 2 : Organización y análisis de la información previamente recolectada																
Ordenamiento y análisis de la información y los resultados obtenidos																
Etapa 3 : Desarrollo del Manual de estrategias de seguridad bancaria																
Se creará y desarrollará el Manual de estrategias de seguridad bancaria																
Etapa 4 : Lanzamiento y divulgación del Manual de estrategias a la comunidad y usuarios en general																
Divulgación en los medios de socialización para el Manual ya elaborado																

Tabla 6. Cronograma de actividades del trabajo de investigación

ACTIVIDAD	TIEMPO (MESES)											
	1	2	3	4	5	6	7	8	9	10	11	12
Etapa 1 : Recolección de información por medio de fuentes primarias y secundarias												
Etapa 2 : Organización de la información previamente recolectada												
Etapa 3 : Desarrollo del Manual de estrategias de seguridad bancaria												
Etapa 4 : Lanzamiento y divulgación del Manual de estrategias a la comunidad y usuarios en general												

4. CONCLUSIONES

Teniendo en cuenta en el transcurso del proyecto se verifica los métodos más comunes que usan los ciberdelincuentes para vulnerar la seguridad bancaria y afectar a los usuarios del sistema financiero, además se pudo conocer los medios más comunes para hacer transacciones de la banca móvil y los beneficios que ofrece permitiendo a los colombianos realizar sus transacciones virtuales sin la necesidad de acercarse a una sucursal.

La implementación del Manual de estrategias de seguridad bancaria trae consigo la minimización de los riesgos de ciberataques ya que los usuarios tendrán más cuidado y crearan una cultura y una buena práctica de la seguridad informática al momento de realizar sus transacciones en la banca móvil y en línea permitiéndoles aprovechar al máximo los servicios financieros a fin de mejorar su calidad de vida.

El propósito principal del proyecto se contempla al uso global de la banca móvil y en línea en el sistema financiero, ya que brinda una mayor seguridad transaccional adicionando el plus de hacerlo a cualquier hora y desde cualquier lugar.

La globalización de la banca móvil y en línea, permitirá disminuir el riesgo de transacciones que se realizan presencialmente así aumentado la seguridad bancaria, aumentando las transacciones básicas diarias y de ésta manera moviendo la economía de manera progresiva permitiendo que un gran números de colombianos se unan para usar y disfrutar de los beneficios que trae estos servicios que ofrecen las entidades financieras.

Es de vital importancia que las personas puedan conocer e implementar este Manual de estrategias de seguridad bancaria, ya que son muchos los colombianos que van a requerir un

producto o servicio de alguna entidad bancaria y no está de más que se pueda adquirir una educación financiera acerca de los riesgos y las consecuencias de no manejar adecuadamente las plataformas virtuales.

Hay que crear una cultura de buenas prácticas para la seguridad y la protección de datos personales que permita minimizar dichos riesgos para lograr corregir la percepción negativa que se tiene de la banca móvil y en línea, esto conllevará a aumentar la tasa de transacciones bancarias diarias, ya que al realizarse desde la comodidad de su hogar y trabajo podrán realizarse en cualquier hora del día, así poniendo en súper habit la frecuencia transaccional.

5. RECOMENDACIONES

El proyecto de grado se enfoca en la seguridad bancaria para ello se debe haber un convenio con varias instituciones educativas preferiblemente universidades con los bancos , para tomar esta conciencia y dar jornadas de charlas de su uso debido de las aplicaciones bancarias así invirtiendo también en publicidad y capacitadores expertos, para que realicen este tipo de conferencias.

Logrando la aprobación y divulgación de este tema muy importante como lo es la seguridad bancaria, actuando desde la perspectiva preventiva, así culturizando cada vez más a las personas permitiéndoles llevar el mensaje de que no es necesario usar una sucursal bancaria para acceder a la banca o a la misma entidad financiera.

6. REFERENCIAS BIBLIOGRÁFICAS

Arbeláez , M., & Zuluaga, S. (2002). El sistema financiero colombiano de cara al siglo XXI. Bogotá.

Consejo Privado de Competitividad. (2010). Informe Nacional de Competitividad 2010-2011. Bogotá: Gráficas Gilpor Ltda.

Roca, G. A. (2017). Orígenes de la banca comercial en Colombia : la banca libre, 1870-1886. Obtenido de Banrepcultural: http://www.banrepcultural.org/biblioteca-virtual/credencial-historia/numero-135/origenes-de-la-banca-comercial-en-colombia

Juan Carballo (2016).Seis métodos que utilizan los hackers para robar contraseñas: https://computerhoy.com/noticias/software/seis-metodos-que-utilizan-hackers-robar-contrasenas-44062

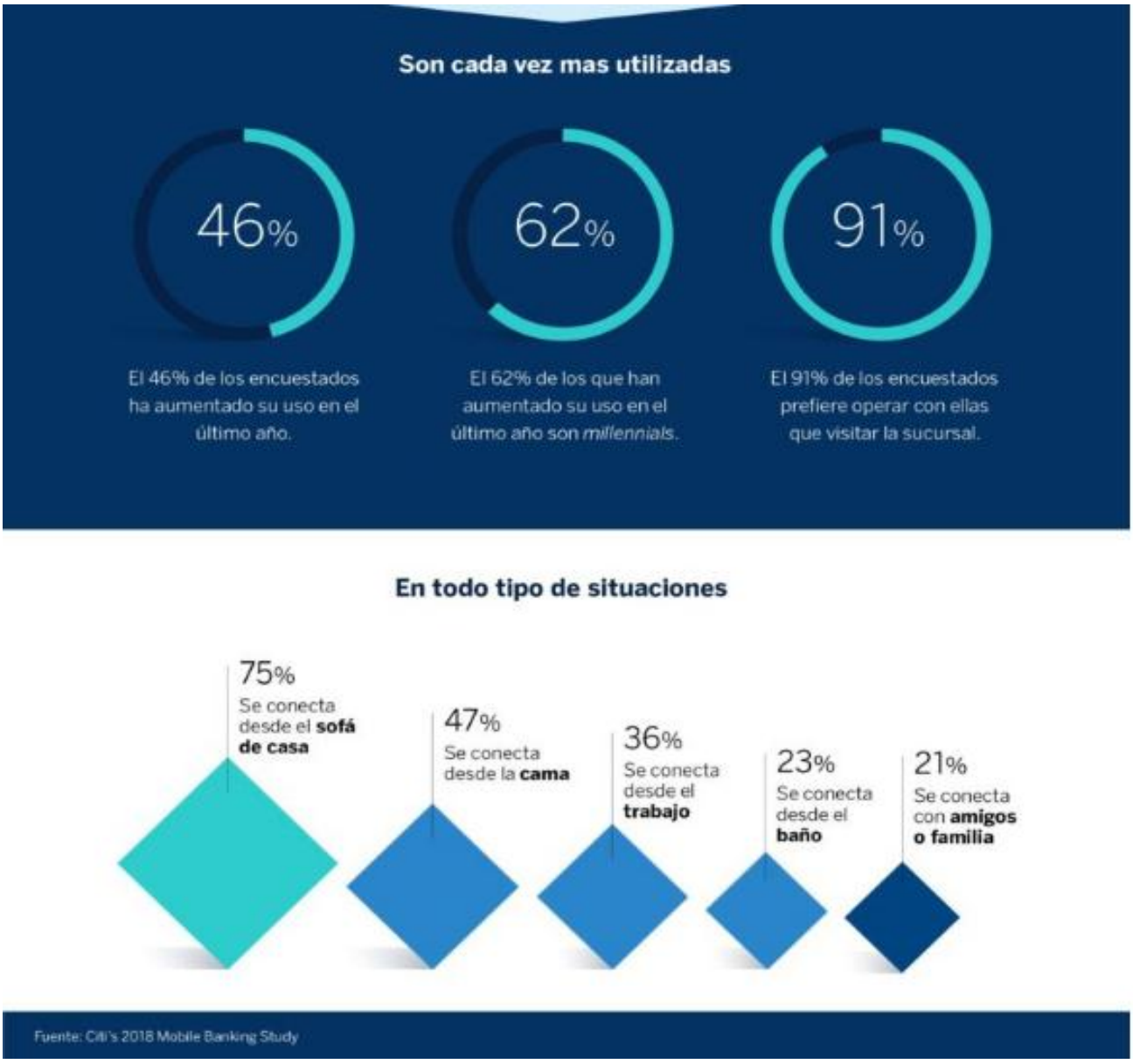
SANTIAGO HERNÁNDEZ (2017). Consultor de Seguridad de La Información: https://www.cloudseguro.co/seguridad-bancaria-en-colombia/

MINTIC. (s.f.). Fortalecimiento de la gestion TI en el Estado. Obtenido de https://www.mintic.gov.co/gestionti/615/w3-article-7083.html

Portafolio. (15 de Noviembre de 2017). Obtenido de https://www.portafolio.co/economia/finanzas/fraude-electronico-el-principal-problema-del-sistema-financiero-511655

7. ANEXOS

Frecuencia y la mejoría si se usa la Banca desde su dispositivo móvil



Tomado de: Citigroup.com