ES SEGURO EL USO DEL SOFTWARE EN EL INTERCAMBIO DE INFORMACION BANCARIA

GLORIA ELIZABETH RODRIGUEZ ROBAYO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA- UNAD –
ESPECIALIZACION EN SEGURIDAD INFORMATICA
BOGOTÁ D.C.
2018

ES SEGURO EL USO DEL SOFTWARE EN EL INTERCAMBIO DE INFORMACION BANCARIA

GLORIA ELIZABETH RODRIGUEZ ROBAYO

MONOGRAFÍA DE GRADO PARA OPTAR AL TÍTULO DE ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Director Proyecto:
Ingeniero Martin Camilo Cancelado Ruiz

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA- UNAD-
ESPECIALIZACION EN SEGURIDAD INFORMATICA II
BOGOTÁ D.C.
2018

Nombre de Aceptación

_____

_____

_____

_____

Firma del presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Bogotá D.C., 30 de octubre de 2018

CONTENIDO

pág.

LISTA DE TABLAS

Pág.

TABLA DE FIGURAS

pág.

INTRODUCCIÓN

La evolución tecnológica aplicada a los Sistemas informáticos crece y se desarrolla de forma continua, en donde los bancos son líderes en la implementación de software bancario con el objeto de facilitar la gestión de movimientos para sus clientes y de esta manera enfrentar con nuevos servicios a un mercado de alta competencia, en el cual el uso e implementación de nuevos sistemas informáticos o software bancarios no se excluyen del Derecho.

Es así como la información hace parte del proceso de bienes que llegan a ser universalmente reconocidos y como tales deben ser jurídicamente protegidos, junto a las herramientas que facilitan su manejo, lo cual se integra en el concepto de informática.

El manejo y operación de información con bases informáticas, en uso de Software y hardware a través de los diferentes dispositivos a los que hoy se tiene acceso; presentan alto riesgo, pues dicha información se encuentra expuesta a pasar por un número indeterminado de personas, lo que implica la posibilidad latente de que surjan errores técnicos y generar inseguridad en el uso de la información almacenada en el Sistema Informático. Entre otros aspectos porque esta información puede ser copiada de forma exacta e indistinguible del original, y no siempre se respeta la coherencia del sistema. Situación que posibilita los fraudes y la problemática de una Inseguridad Informática. Cuando se accede al conocimiento del sistema o se cuenta con acceso al mismo permitiendo la intervención en la información, establecer modificaciones y transformar el estado original, en ocasiones de forma indistinguible, lo que constituye un delito.

El acceso y la modificación de información en los Software bancarios a través

de la violación de los mecanismos de protección de las transacciones bancarias tanto patrimoniales del autor como otras defraudaciones y amenazas, pueden proceder de programas dañinos que son instalados en la computadora del usuario, como son los virus, igualmente pueden llegar por vía desusada en donde los delincuentes se conectan a Internet e ingresan a distintos sistemas con motivos fútiles. La presente investigación se basa en la necesidad fundamental de saber qué recursos se necesitan para controlar ese acceso y las medidas del Estado Social de derecho en cuanto a regulación y protección a los derechos de los usuarios con relación a la información almacenada en el sistema informático bancario.

1. **TÍTULO DE LA MONOGRAFIA**

ES SEGURO EL USO DEL SOFTWARE EN EL INTERCAMBIO DE LA INFORMACIÓN BANCARIA

2. PLANTEAMIENTO DEL PROBLEMA

2.1. DESCRIPCION DEL PROBLEMA

En Colombia, los Software bancarios para el intercambio de información con el usuario requiere altos niveles de protección al consumidor debido a la gran incertidumbre del manejo que se otorga en la operación misma del quehacer diario de la función bancaria, tales como transferencias de fondos, compras, pagos de recibos, entre otras y cuya información final puede llegar a ser manipulada por personas no sólo a través del deterioro patrimonial y eventual enriquecimiento, sino también para documentar elementos relevantes de los clientes del banco para facilitar la ejecución de otros delitos, tales como secuestros, chantajes, favorecimientos en beneficios, entre otros. El sistema informático es susceptible de la manipulación, el manejo, la copia de información y resulta vulnerable a la ejecución de maniobras fraudulentas que no respetan la coherencia del sistema, el derecho al buen nombre, a la honra, a la confidencialidad y a la seguridad de los clientes. El delito se facilita cuando se adquiere el conocimiento del sistema o se obtiene el acceso al software y por ende a su información, dando la oportunidad de que intervengan manos criminales para modificar de forma indistinguible el estado original del sistema e incurrir en el manejo del software para crear un fraude

Figura 1.Elementos que afectan la seguridad bancaria

Fuente: El autor

2.2. FORMULACIÓN DEL PROBLEMA

¿Qué tan seguro es el uso de datos en el intercambio de información bancaria en Colombia en cumplimiento a la Ley 1480 de 2011?

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Determinar los principales elementos que afectan la seguridad del software bancario implementado a través del uso de internet para transacciones e intercambio de información entre la entidad y sus cuentas habientes en la ciudad de Bogotá.

3.2 OBJETIVOS ESPECÍFICOS

- Evaluar el impacto de los delitos informáticos bancarios y la aplicación de la Ley 1480 de 2011.
- Identificar los avances tecnológicos que se han convertido en nuevas amenazas para la seguridad informática a nivel mundial.
- Describir los controles de los bancos y los mecanismos de protección para los usuarios de la banca electrónica
- Realizar un informe sobre los reportes de vulnerabilidad informática que se presentan para transacciones bancarias

4. JUSTIFICACIÓN

Los sitios web son susceptibles de inseguridad ya que el software puede ser manipulado y copiado de forma exacta e indistinguible de un original. En el inicio de usos de redes en los años noventa se tenía un uso reservado; sin embargo la globalización permitió que el acceso a la información y a las redes se hiciera más común así como la oportunidad de navegación en los sitios web, correos electrónicos, Facebook y otras redes, convirtiéndose en un canal con grandes condiciones de vulnerabilidad a su seguridad y generando un intercambio constante de información que incluye también un riesgo de intromisión o simulación, facilitando delitos como por ejemplo el hurto por suplantación de tarjetas débito o crédito bancarias haciendo un mal uso de la web.

En otras palabras la seguridad de los software bancarios por tener relación directa con el patrimonio de los Colombianos, es una problemática que requiere especial atención ya que Colombia no ha sido ajena a las dificultades que se han generado a nivel mundial por el mal uso de dicha información y que ha facilitado la ejecución de delitos tanto contra el patrimonio como contra la seguridad y buen nombre de los clientes y sus familias, inclusive las Instituciones tanto privadas como púbicas también han sido afectadas por constantes delitos o fuga de información.

La seguridad digital de cualquier usuario está en riesgo pues este puede ser engañado o forzado a descargar programas en su ordenador y sometido a intenciones dañinas, generalmente a través de software que se presenta de diferentes formas como por ejemplo los virus, troyanos, spyware o gusanos que son amenazas al manipular el uso de distintos servicios.

La Superintendencia Financiera de Colombia, cuenta con Funciones

Jurisdiccionales bajo la perspectiva del régimen de protección al consumidor, diseñó e implementó un sistema de información para el manejo del flujo electrónico de documentos e información y al hacer seguimiento como ente de vigilancia encontró reclamaciones con argumentos de modalidad del fraude de "PHISHING" El estafador, conocido como phisher, el cual se vale de técnicas de ingeniería social, haciéndose pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo general un correo electrónico, o algún sistema de mensajería instantánea, redes sociales SMS/MMS, a raíz de un malware o incluso utilizando también llamadas telefónicas[1].

El informe presentado para el año 2014 de La organización de los Estados americanos, una de las prioridades de la Organización de los Estados Americanos (OEA) es respaldar los esfuerzos e iniciativas de nuestros Estados Miembros destinados a fortalecer las capacidades necesarias para que el dominio informático sea más seguro, estable y productivo. Representa el esfuerzo de múltiples actores, con el aporte de Symantec, AMERIPOL, Microsoft, LACNIC, ICANN, y el Grupo de Trabajo Anti-Phishing (APWG). El informe también brinda un panorama integral de la Seguridad cibernética en América, con el aporte de 30 de los 32 países de América Latina y el Caribe[2].

[1] MOYA R., RAÚL. Delitos informáticos: Estudio concreto sobre Fraudes y Phishing. Escuela Politécnica Superior de Jaéan, 2013, p. 3.

[2] ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. Tendencias de seguridad Cibernética en América Latina y el Caribe. Symantec, 2014. Extraible en: https://www.sites.oas.org/cyber/Documents/2014%20-%20Tendencias%20de%20Seguridad%20Cibern%C3%A9tica%20en%20Am%C3%A9rica%20Latina%20y%20el%20Caribe.pdf

5. ALCANCE Y DELIMITACIÓN DEL PROYECTO

5.1. ALCANCE

Este proyecto tiene como alcance el identificar qué elementos contribuyen para que se implementen las propuestas en las políticas de seguridad informática, identificando qué impacto hay en cuanto al uso o ejecución de la informática del Software bancario, con criterios de seguridad y calidad al adoptar medidas que permitan prestar un servicio seguro y acceso a un software; sea la ausencia o deficiencia de los controles informáticos que permiten el acceso no autorizado a los canales de distribución a los sistemas informáticos de la entidad bancaria, el uso de datos del usuario al transmitir o ser suplantado en los canales de distribución de los servicios financieros, con respecto a la Ley de protección al usuario la Ley 1480 de 2011 y el Software útil que pueden escalar en delitos como el terrorismo informático.

El acceso brindado por las entidades vigiladas a sus clientes para la realización de operaciones mediante el uso de aplicaciones personalizadas, utilizando generalmente enlaces dedicados acorde a que toda persona natural o jurídica con la cual la entidad establece y mantiene una relación contractual o legal para el suministro de cualquier producto o servicio propio de su actividad y de la interacción de las entidades sometidas a inspección y vigilancia de la Superintendencia Financiera de Colombia, con sus clientes y usuarios para el desarrollo de su objeto social.

Atendiendo lo dispuesto en el artículo 15 de la Carta Política y demás regulación, normas aplicables sobre la materia, considerar que tan confidencial es toda aquella información amparada por la reserva bancaria, el contar con controles y alarmas que informen sobre el estado de los canales, y además permitan identificar, corregir las falencias de manera segura y oportuna. Todo haciendo posible el objetivo de dar mayor seguridad a los

datos y al manejo de información en la comunicación de datos entre un usuario y una entidad bancaria.

5.2. DELIMITACIÓN DEL PROYECTO

Los Sistemas informáticos son una disciplina que maneja conceptos con alto nivel de abstracción y un vasto mundo que obedece a diferentes circunstancias, el objeto de estudio para el presente proyecto se centra entonces en analizar los Sistemas Informáticos del sector bancario en cuanto a su integridad e inviolabilidad en la ciudad de Bogotá

Las organizaciones bancarias según los expertos en seguridad informática realizan actividades investigativas orientadas a conocer el estado de los sistemas y trazar hasta su origen cualquier eventualidad o intrusión, al observar el periodo de 2016 a 2017 se determina que con el intercambio de información en el uso del sistema bancario, el cliente puede ser engañado o forzado al acceder al sistema y como resultado pueden aparecer de distintas formas de software, como son los virus, troyanos, spyware o gusanos, los cuales representan verdaderas amenaza pues manipulan la información y deja a las personas expuestas robos en torno a la tecnología.

6. METODOLOGÍA

Este proyecto de investigación lleva a cabo un método inductivo, proceso de razonamiento y análisis de la revisión jurídica, observando los hechos que manifiesten el objeto del problema, se emplea el carácter descriptivo, encaminado a determinar en Colombia como se ha reglamentado el uso del software para transacciones bancarias, para lo cual se utilizará un análisis cualitativo.

En correspondencia con el objetivo, el tipo es descriptivo analítico logrando así una triangulación metodológica de la investigación, así mismo, se revisará el material al cual se tenga acceso y que contenga información sobre las situaciones encontradas en los diferentes aplicativos de software bancario, de tal forma que permita realizar una diferenciación entre la utilización que aporta al bienestar del usuario y la manipulación de extraños de esta información, suplantando datos.

Se utilizará un análisis de derecho comparado netamente documental e información jurídica, para observar una muestra de la legislación, referentes a la vigilancia del software informático bancario y del usuario para encontrar la forma adecuada de seguridad informática que ayudará a inferir el modelo que seguirá Colombia.

Se hace necesario la recolección de base de datos que reflejen el problema, para desarrollar una forma descriptiva de casos, por otro lado, esta investigación no solo se quedará en el plano documental, sino que para el buen desarrollo de la misma se realizará también identificación de posibles daños o vulneración de derechos entre sujetos pasivos y activos.

Las fuentes de recolección de información que se utilizan son de tipo primario en cuanto a las entrevistas e información directa, igualmente se

utilizaran fuentes secundarias como son los documentales, noticias de medios de comunicación, reportajes periodísticos, análisis investigativos entre otros.

6.1. MUESTRA.

La muestra es la que puede determinar la problemática para el ejercicio de la investigación ya que es capaz de generar los datos con los cuales se identifican las fallas dentro del proceso.[3]

El grupo de individuos que se toma para dar curso a esta investigación es la población que tiene acceso a un Banco de Colombia, que usan un sistema informático, Software, para hacer sus transacciones. Se trata de estudiar un fenómeno estadístico en cuanto al conocimiento que tienen los usuarios sobre la inseguridad en el manejo del Software.

6.2. POBLACIÓN

La localidad de Santafé tiene un promedio de habitantes de 110.053. [4]

La población es un conjunto de individuos de la misma clase, limitada por el estudio. Según Tamayo “La población se define como la totalidad del fenómeno a estudiar donde las unidades de población poseen una característica común la cual se estudia y da origen a los datos de la investigación”.[5]

[3] TAMAYO & TAMAYO. MARIO. El Proceso de la Investigación científica. México: Editorial Limusa S.A. 1997. p. 38

[4] SECRETARIA DE PLANEACIÓN. Portal. 2017. (en línea) Disponible en: http://www.sdp.gov.co/portal/page/portal/PortalSDP/InformacionTomaDecisiones/Estadisticas/RelojDePoblacion

[5] Ibidem. p.114

6.3. ENTREVISTA ESTRUCTURADA.

Una herramienta que permite el desarrollo de la investigación al aplicarla al Gerente del Banco, como a usuarios o personas del Banco, con el fin de recolectar la información concreta de personal y medios alternativos para lograr actualización y mayor eficiencia y desarrollo del objetivo de este proyecto.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA- UNAD - ESCUELA CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA BOGOTÁ D.C. – 2017 Qué tan seguro es el uso de datos en el intercambio o suplantación de información Bancaria

6.4. ENCUESTA.

La siguiente encuesta es realizada con fines académicos, como trabajo de grado para estudiantes de Especialización en Seguridad Informática de la UNAD. Hace parte de una investigación de ¿Qué tan seguro es el uso de datos en el intercambio o suplantación de información bancaria en Colombia en cumplimiento a la Ley 1480 de 2011?
Por favor responda las siguientes preguntas de selección Múltiple marcando la respuesta que se acomode mejor a su elección.
1 ¿Con que frecuencia visita usted un medio informático (Web...) para hacer transacciones bancarias?:
a) Una vez por semana
b) De dos a tres veces por semana
c) Más tres veces por semana
d) Rara vez
e) Nunca

2.- ¿Sabe usar un medio informático para hacer operaciones bancarias?:
Si
No
3.- Alguna vez ha presentado un inconveniente al realizar una transacción a través de un aplicativo?
Si
No
Cual:
4.-Considera usted que existe algún nivel de riesgo al realizar transacciones electrónicas o suministrar información electrónica? Cual:
5. Cómo calificaría la seguridad informática en Colombia: Muy insegura ,
Insegura,
Medianamente segura,
Segura
Muy segura
6. Ha recibido correos, informándole que tiene bloqueada su cuenta
Si
No
Una vez
Varias veces
6. Tiene alguna recomendación para el sector bancario para garantizar la seguridad de su información?
Cual
¡MUCHAS GRACIAS POR SUS RESPUESTAS!

6.5. FUENTES SECUNDARIAS:

- Biblioteca Luis Ángel Arango - Bogotá
- Repositorio, base de datos UNAD –Bogotá.
- Superintendencia Financiera de Colombia.
- Bancos de Colombia - Bogotá

7. MARCO REFERENCIAL

La recopilación breve y escueta de conceptos, teorías y regulación que se relaciona directamente con el desarrollo de la situación problemática identificada y del problema de investigación que pueden contribuir al desarrollo del mismo subdividido en Marco conceptual, Marco Histórico, Marco teórico, y Marco normativo o legal.

7.1. MARCO CONCEPTUAL

Es importante tener algunos conceptos claros que dinamicen y unifiquen con el fin de comprender a lo largo del desarrollo de este trabajo en el dinamismo de la tecnología y que se entiende por seguridad informática empleada en operaciones bancarias.

- **Estaciones de Red.** En informática es una estación de trabajo (en inglés Workstation) es un computador de altas prestaciones destinado para trabajo técnico o científico[6].

- **Red de Computadoras.** Es un ordenador que proporciona a los usuarios el acceso a los servidores y periféricos de la red. A diferencia de una computadora aislada, tiene una tarjeta de red y está físicamente conectada por medio de cables u otros medios no guiados con los servidores. Los componentes para servidores y estaciones de trabajo alcanzan nuevos niveles de rendimiento informático, al tiempo que ofrecen fiabilidad, compatibilidad, escalabilidad y arquitectura avanzada ideales para entornos multiproceso[7].

[6] ENDERLE, GUNTER K. & KANSY G. PFAFF. Computer Graphics Programming. Gks – The Graphis Standars. Second Edition. London Paris Tokio. Springer – Verlag, 1987.
[7] TANEMBAUN, ANDREW S. Redes de Computadoras. Pearson Educación, México. 2003

- **Ciberespacio.** Término inglés cyberspace, [8] llegó al castellano como ciberespacio. Así se denomina al entorno artificial que se desarrolla mediante herramientas informáticas. Así se denomina al entorno artificial que se desarrolla mediante herramientas informáticas. Es una realidad virtual. No se trata de un ámbito físico, que puede ser tocado, sino que es una construcción digital desarrollada con computadoras (ordenadores)

- **Malware.** Programa maligno. Malicious Software. Engloba todos aquellos programas diseñados para causar daños al hardware, software, redes, como los virus, troyanos, gusanos, nukes. Término común que se utiliza al referirse a cualquier programa malicioso. (Código malicioso). Es un software que tiene como objetivo infiltrarse en o dañar una computadora sin el conocimiento de su dueño y con finalidades muy diversas ya que en esta categoría encontramos desde un troyano hasta un spyware[9].

- **Phishing.** Consiste en el robo de información personal y/o financiera del usuario, a través de la falsificación de un ente de confianza. De esta forma, el usuario cree ingresar los datos en un sitio de confianza cuando, en realidad, estos son enviados directamente al atacante[10].

- **Servidor.** Es una computadora que, formando parte de una red, provee servicios a otras computadoras denominadas clientes.

- **El spyware.** Denominado Software espía, una aplicación que recopila

---

Libro digital. ISBN: 970-26-0162-2. Área Universitaria.
https://books.google.com.co/books?id=WWD-4oF9hjEC&printsec=frontcover&dq=redes+de+computadoras&hl=es&sa=X&ved=0ahUKEwjEn6uanI_UAhUF4yYKHYsZA2cQ6AEIIjAA#v=onepage&q=redes%20de%20computadoras&f=false

[8] GUTIERREZ C, OSCAR. Glosario terminológico sobre internet y contenidos multimedia. Universidad Autónoma de Barcelona. 2014 Extraíble en: https://ddd.uab.cat/pub/tfg/2014/123526/TFG_oscargutierrez.pdf

[9] CCM. Diferentes tipos de programas maliciosos. Extraíble en: http://es.ccm.net/faq/2809-diferentes-tipos-de-programas-maliciosos

[10] Ibíd.

información sobre una persona u organización sin su conocimiento ni consentimiento.

- **Seguridad informática.** Se refiere a las tipologías, al conjunto de elementos, condiciones de sistema informático de procesamiento, dispositivos, y herramientas encargadas de los datos, métodos y técnicas, y su almacenamiento, orientados a proveer condiciones seguridad y confianza, disponibilidad y privacidad[11].

- **Sistema de Gerencia Integral de Riesgos.** Según PDVSA, es una herramienta para la administración integral de los riesgos a la salud y seguridad de los trabajadores, a la integridad de las instalaciones y al ambiente[12].

7.2. MARCO TEÓRICO

7.2.1 Teoría del control

Se presenta en este proyecto, el modelo que podría contribuir al desarrollo del mismo. Toda organización entre las que se encuentra el sistema bancario debe estar a la vanguardia de los procesos de cambio donde disponer de información continua, confiable y en tiempo, se reconoce como seguridad informática.

El objetivo del control en los Sistemas de Información debe ser el de preservar la confiabilidad, privacidad y certificar que esta información es

[11] CERVIGÓN, H. ALFONSO, G. & ALEGRE, R. MARÍA DEL PILAR. Seguridad Informática. Extraíble en: https://books.google.com.co/books?id=c8kni5g2Yv8C&printsec=frontcover&dq=concepto+de+seguridad+informatica&hl=es&sa=X&ved=0ahUKEwijgf39lY_UAhVILyYKHYPgABUQ6AEIJjAB#v=onepage&q=concepto%20de%20seguridad%20informatica&f=false

[12] OOCITIES. Parte II: Soporte conceptual. Extraíble en: http://www.oocities.org/es/aryelitvelardes/Aryelit/parteii.htm

accesible sólo a las personas acreditadas para consultar la información y evitar accesos inobservados o divulgaciones no autorizados. La falta de confidencialidad puede darse por imprudencias directas o indirectas con cualquier tipo de soporte y su no protección puede generar consecuencias como responsabilidad civil, administrativa, cualitativa, deontológica, credibilidad, prestigio, imagen, amenazas lógicas, físicas e informáticas.

Los esquemas de control de los Sistemas Informáticos se desarrollan para proteger y conservar el equilibrio. Actúan sobre ellos dos fuerzas: (i) una que trata de impedir los cambios bruscos y(ii) otra que impulsa al sistema a cambiar, de forma lenta y evolutiva.

Todo el sistema de retroalimentación constituye lo que se ha denominado sistemas de control; consta de las siguientes variables: (i) Un elemento que se desea controlar; (ii) Mecanismos sensores: que son sensibles para medir las variaciones o los cambios de la variable; (iii) Medios Motores: a través de los cuales se pueden desarrollar las acciones correctivas. (iv) Fuente de Energía: que entrega la energía necesaria para cualquier tipo de actividad. (v) Retroalimentación: mediante la cual se logra llevar a cabo acciones correctivas; Establecidos en la retroalimentación negativa, que es cuando se modifica la conducta del sistema y se deja constante los objetivos; los sistemas tienden a mantener una conducta relativamente estable, ya que este mecanismo está constantemente vigilando el comportamiento del sistema y tomando las medidas necesarias para que se mantenga dentro de los límites deseados (Moreno, cita a Bertoglio, 1998, p.10)

7.2.2. Interface fácil. Predicciones de Joseph Carl Robert Licklider.

Unos de los primeros que previó la computación interactiva moderna, en campos de gráficos para la computación y su aplicación a toda clase de actividades, librerías digitales, comercio electrónico, banca; fue pionero de

Internet, con una visión temprana de una red de ordenadores mundial mucho antes de que fuera construida. Se interesó por la tecnología de la información, y se trasladó al MIT en 1950 como profesor asociado, donde ocupó el cargo en un comité que estableció el Laboratorio Lincoln del MIT y estableció un programa de psicología para estudiantes de ingeniería. En octubre de 1962, Licklider fue nombrado jefe de la Oficina de Técnicas de Procesamiento de la Información (IPTO) en ARPA, en la Agencia de Investigación de Proyectos Avanzados de Defensa de Estados Unidos. Jack Ruina, director de ARPA, ofrecido a Lick ponerse a la cabeza de dos departamentos de ARPA; para hacer realidad mediante su financiación para la investigación, Licklider desempeñó un papel similar en la concepción y la financiación temprana de redes de investigación, sobre todo ARPA NET. Él formuló las primeras ideas de una red informática mundial en agosto de 1962 en BBN, en una serie de notas que discuten el concepto de "Red de ordenadores intergalácticas". Estas ideas contenidas en casi todo lo que Internet es hoy en día, incluyéndola computación en nube. Incluyendo la interfaz gráfica de usuario, **ARPANET, y el predecesor directo de Internet. Johnson, Lyndon B[13].**

Plantó las semillas de la informática en la era digital, en el campo de la psicoacústica, Licklider es más recordado por su teoría de la percepción del tono Dúplex en 1951, presentada en un artículo[14]; escribió un libro titulado “Librerías del futuro” fue reproducido en un libro de 1979 y formó la base para los modelos modernos de la percepción de la altura[15].

7.2.3. ARPANET- Paul Baran.

Desarrollo e impulsor de las redes de conmutación de paquetes Para la estrategia de defensa estadounidense era importante el desarrollo de una red de comunicaciones que sobreviviese a un ataque nuclear. Como solución al problema, Baran ideó los fundamentos de las redes de conmutación de

[13] BARZANALLANA, RAFAEL. Bibliografía de Joseph Carl Robnett Licklider. Departamento Informática y Sistemas. Universidad de Murcia. 2016. Extraído en: http://www.um.es/docencia/barzana/BIOGRAFIAS/Biografia-JCR-Licklidder.php
[14] Ibid..
[15] Ibíd.

paquetes. Es el desarrollo previo de una red de nodos que actuarían como conmutadores de ruta de paquetes desde un nodo a otro su destino final. Los nodos usarían una estrategia llamada “encaminamiento de la patata caliente” cuando un nodo recibe un paquete, lo almacena, determina la mejor ruta para su destino y lo envía al siguiente nodo de la ruta. En cuanto las computadoras deberían ser usada las estadísticas u actualizadas constantemente en la red[16].

7.3. MARCO CONTEXTUAL

7.3.1. Criterio de Uso y Calidad de la Información

Se trata de definir criterios de seguridad y calidad de información, uso de Software e informes de establecimientos bancarios.

En uso del sistema informático haciendo uso de pago crédito y débito adoptadas por todas las entidades sometidas a la inspección y vigilancia de la Superintendencia Financiera de Colombia (SFC), para los año 2016-2017, casos de fraude y suplantación de identidad a la hora de manipular y usar vía internet el sistema bancario algunos ejemplos que dieron vía libre a la implementación biométrica y hechos que hace nuevos demandantes de productos financieros y hacia potenciales riesgos de inseguridad informática en la banca de Colombia.

[16] SWEEZY, M. PAUL LEO. HABERMAS: PAUL A. BARAN, Collective Portrait. Press. Digitalized. Universidad California. 2008. 1965.

7.3.2. Sistema de Gestión de Seguridad de La Información

7.3.2.1 ISO 27000.ES

Con el objetivo de garantizar que las organizaciones realizan una correcta gestión de la seguridad de la información de acuerdo a las cláusulas del estándar NTC-ISO/IEC 27001:201310, según la reorganización de las publicaciones ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, que permite el desarrollo del proceso sistemático conocido y adoptado por toda organización, apoyado desde el punto de vista de gestión de riesgos asociado a la seguridad que identifica amenazas que constituye un Sistema de Gestión de Seguridad de la Información que permite a una estructura organizacional, responsabilidad, política, procedimiento, proceso, recursos que gestione de modo apropiado la seguridad de la información. El adecuar la filosofía de las normas ISO, provee un instrumento a las organizaciones desarrollar el objetivo del negocio, con el propósito de poder mantener el riesgo por debajo del nivel definido por la organización[17].

Es así, que la serie 27000 sirve de apoyo a las organizaciones en cuanto a la implementación de ISO/IEC 27001, como pauta importante, única certificable dentro de esta serie. Con la implementación de este Sistema de Gestión de Seguridad de la Información, le provee a las organizaciones un proceso de mejora continua, debida y continua gestión de los riesgos de seguridad que permite la intervención activa de toda la organización con relación a la planeación, definición, identificación e implementación de controles y medidas orientadas a salvaguardar la seguridad de los activos de

[17] Normas ISO27000.es - El portal de ISO 27001 en español. Extraído en: http://www.iso27000.es/iso27000.html

información de la organización.[18]

7.3.2.2. Seguridad Informática

Es necesaria y de uso pragmático de cualquier sistema, el identificar la existencia de peligros, daños o riesgos, malos usos, peligros que pueden afectar el buen funcionamiento de un determinado sistema o de los resultados que de él se alcanzan. Aunque la realidad demuestra que ningún sistema puede ofrecer un cien por ciento - 100% de seguridad, los existentes pueden ser para disminuir los posibles riesgos presentados a nivel de información.[19]

[18] Ibidem.
[19] ESCRIVA, G. GEMA & ROMERO S. ROSA. Seguridad Informática. M. Macmillan Iberia, S.A. Libro en español electrónico ISBN 9788415991410. 2013. Extraído en: http://site.ebrary.com.sibulgem.unilibre.edu.co:2048/lib/bibliounilibresp/detail.action?docID=10820963&p00=seguridad+informatica

7.4. MARCO LEGAL

Siempre que se desea implementar un Sistema de seguridad, toda organización debe obligatoriamente cumplir con todas las leyes, normas, decretos, etc. En Colombia son aplicables en el desarrollo de estas actividades. De forma general brevemente se mencionan en el tema la regulación legal y marco reglamentario de seguridad informática.

Tabla 1**.** Actualización propia marco legal de seguridad informática

Ley – Decreto -Resolución	Descripción
Ley 44 de 1993	Modifica a la Ley 23/1982
Ley 527 de 1999	Validez jurídica y probatoria de la información electrónica;
Ley 545 de 1999	Por medio de la cual se aprueba el "Tratado de la OMPI -Organización Mundial de la Propiedad Intelectual- sobre Interpretación o Ejecución y Fonogramas (WPPT)", adoptado en Ginebra el veinte|(20) de diciembre de mil novecientos noventa y seis (1996
Ley 594 de 2000	Ley General de Archivos – Criterios de Seguridad;
Ley 565 de 2000	por medio de la cual se aprueba el "Tratado de la OMPI –Organización Mundial de la Propiedad Intelectual– sobre Derechos de Autor (WCT)", adoptado en Ginebra, el veinte (20) de diciembre de mil novecientos noventa y seis (1996).
Ley 603 de 2000	Se modifica el informe gestión de la Ley 222 de 1995.
Ley 679 de 2001	Pornografía Infantil – Responsabilidad ISPs;
Ley 719 de 2001	Comercio Electrónico y Firmas Digitales
Ley 962 de 2005	Simplificación y Racionalización de Trámite. Atributos de seguridad en la información electrónica de entidades públicas;
Ley 1150 de 2007 –	Seguridad de la información electrónica en contratación en línea;
Ley 1266 de 2008 –	Habeas data financiera, y seguridad en datos

Ley – Decreto -Resolución	Descripción
	personales.
Ley 1273 de 2008 -5 de enero de 2009	Delitos Informáticos y protección del bien jurídico tutelado que es la información; (añade dos nuevos capítulos al Código Penal Colombiano) Capitulo Primero: De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos; Capitulo Segundo: De los atentados informáticos y otras infracciones. Como se puede ver en el primer capítulo, esta Ley está muy ligada a la ISO27000, lo cual coloca al País a la vanguardia en legislación de seguridad de la información, abriendo así la posibilidad de nuevas entradas con este tema.
Ley 1341 de 2009 –	Tecnologías de la Información y aplicación de seguridad.
Ley 1437 de 2011	Procedimiento Administrativo y aplicación de criterios de seguridad.
Ley 1480 de 2011	Protección al consumidor por medios electrónicos. Seguridad en transacciones electrónicas.
Ley 1581 de 2012	Ley estatutaria de Protección de datos personales.
Ley 1623 de 2013	Ley de Inteligencia – Criterios de seguridad.
Ley 1712 de 2014	Transparencia en el acceso a la información pública.
Decreto 460 de 1995	Por el cual se reglamenta el Registro Nacional del Derecho de Autor y se regula el Depósito Legal.
Decreto 162 de 1996	Se reglamenta la Decisión Andina 351de 1993 y la Ley 44 de 1993, en relación con las Sociedades de Gestión Colectiva de Derecho de Autor o de Derechos Conexos.
Decreto 1360 de 1989	Por el cual se reglamenta la inscripción de soporte lógico (software) en el Registro Nacional del Derecho de Autor.

Ley – Decreto -Resolución	Descripción
Decreto 1747 de 2000	El cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales.
Decreto 19 de 2012	Racionalización de trámites a través de medios electrónicos. Criterio de seguridad.
Decreto 2184 de 2012	"Por el cual se corrigen yerros en la Ley 1480 del 12 de octubre de 2011"
Decreto 2364 de 2012	Firma electrónica
Decreto 2609 de 2012	Expediente electrónico
Decreto 2693 de 2012	Gobierno electrónico
Decreto 1377 de 2013	Protección de datos personales
Decreto 1510 de 2013	Contratación Pública electrónica
Decreto 333 de 2014	Entidades de certificación digital
Resolución 26930 de 2000	Por la cual se fijan los estándares para la autorización y funcionamiento de las entidades de certificación y sus auditores.

Fuente: El autor

Los fraudes informáticos en el amplio sentido de la información como se observa se implementan y surgen cada día normativa a la velocidad de la misma dinámica de la tecnología y globalización.

8. RESULTADOS ESPERADOS

Se espera obtener como resultado académico información sistematizada de la lista de entidades bancarias que reporten la vulnerabilidad informática de un Software con criterios de seguridad de la Superintendencia Financiera de Colombia.

Buscar los mecanismos que permitan llevar a la práctica en la Banca de Colombia, los resultados de la investigación para demostrar la realidad y efectividad del uso de datos en el intercambio o suplantación de la información bancaria en cumplimiento de la Ley 1480 de 2001, promover en la inclusión académica para manejar esta base investigativa en la carrera de seguridad informática.

8.1. RECURSOS NECESARIOS PARA EL DESARROLLO

8.1.1. Recursos Humanos y Técnicos:

En cuanto a tiempo un promedio de 4 Meses, respaldado por una certificación de ser estudiante de la UNAD, que permiten desarrollar el objetivo de esta investigación.
Es así como existe un acercamiento a los Indicadores de la Superintendencia Financiera por intermedio de la plataforma, en la cual se tiene acceso a consultar la base de datos por web.

8.2. PLANIFICACIÓN PARA REALIZAR

Para la planificación de este proyecto se describe las actividades que se van a desarrollar.

- Documentación de impacto en el sistema informático bancario en la suplantación de datos e identidad.

- Documentación acerca de la Ley 1480 de 2011.

- Protocolo de criterios de calidad y seguridad de la información.

- Recolección de datos de protección de datos.

- Recolección de datos del ente disciplinario que abre procesos de conductas fraudulentas del cibercriminal denominado “phiser”.

- Lista de entidades bancarias reporten la vulnerabilidad informática de un Software con criterios de seguridad por la Superintendencia Financiera de Colombia.

- Recolección de información de canales de distribución a los sistemas informáticos de la entidad bancaria, con respecto a la Ley de protección al usuario la Ley 1480 de 2011.

- Identificar cómo controlar la navegación de los usuarios sin mecanismos de seguridad informática en el uso de información e intercambio bancario.

- Establecer políticas que regulen el uso de aplicaciones del sistema informático e interactuado con el sistema bancario.

- Identificar y alimentar información documental de los resultados de prevención de ataques de suplantación y fraudes en el uso de la información.

- Sensibilizar a los usuarios de los problemas que surgen con la seguridad informática.

- Documentar qué seguridad tiene una entidad bancaria para proteger la información del usuario que accede a la información personal de transacción o interacción bancaria.

- Capacitación e información de protección de datos e implementación, realización de recomendaciones.

8.2.1. Recursos económicos: Costos y Presupuesto

Metodológicamente este tipo de investigación en su realización del mismo, con el objeto de examinar un problema de investigación es poco estudiada o que no ha sido abordado antes ha de servir para el estudio de los resultados.

Los aportes monetarios no monetarios como:

Tabla 2. Costos – Presupuestos.

Descripción	Unidad	Costo
Material Fungible:		450.000
Uso de computador.	100.000	
Horas de investigación,	100.000	
Uso de infraestructura Equipos de cómputo Internet e impresora. Tinta Argollado Transcripción de datos. Impresiones Fotocopias	250.000	
Gastos Varios		700.000
Pasajes – Desplazamiento a: Institución Superintendencia Financiera de Colombia Biblioteca	15.000 x 20 días	
Almuerzo -	200.000	
Imprevistos (10 %) proyecto		115.000
Total, del Proyecto:		1.265.000

Fuente: El autor

9. CRONOGRAMA DE ACTIVIDADES

Tabla 3. Cronograma

No.	Actividades para el desarrollo de de la Monografía	Julio				Agosto				Septiembre				Octubre				Noviembre				Diciembre			
1	Presentación del Proyecto al Comité para su Aprobación																								
2	Revisar el documento que cumpla con la norma NTC 1486																								
3	Recolección Información Documental																								
4	Desarrollo Inicial del Problema de Investigación																								
5	Identificación Ley 1480 de 2011																								
6	Desarrollo de los Objetivos de la Investigación																								
7	Protocolo de seguridad de la información																								
8	Desarrollo Fuentes Secundarias de la Investigación																								
9	Construcción de la Investigación																								
10	Sustentación de Investigación																								
11	Últimos ajustes por solicitud del jurado																								
12	Resultados obtenidos																								
13	Entrega Final y Aprobación																								
14	Entrega Final y Aprobación de la Monografía																								

Fuente: El autor

10. EL IMPACTO DE LOS DELITOS INFORMÁTICOS BANCARIOS Y LA APLICACIÓN DE LA LEY 1480 DE 2011

La gran falta de conocimiento de los usuarios del sector financiero bancario sobre sus derechos hace que en ocasiones se tomen decisiones que implican un alto riesgo de afectar su patrimonio: “Un gran porcentaje de la población carece de los conocimientos para analizar la información financiera disponible, hacer uso efectivo de los mecanismos de protección, y tomar decisiones informadas y responsables” (Asobancaria, 2011, p.1). Este hecho que resulta bastante frecuente permite concluir que existe un alto desconocimiento tanto de las normas como los derechos, y por tal razón es el mismo Sistema financiero el llamado a buscar estrategias que permitan la protección de sus clientes, en especial haciendo énfasis en la importancia de proveer información clara y oportuna, mantener un buen nivel de eficiencia en el manejo de derechos y deberes que se encuentran establecidos en la Ley 1480 de protección al consumidor, tanto a nivel del consumidor como de las entidades que prestan el servicio. De igual forma resulta relevante desarrollar conocimientos y actitudes de los usuarios para tomar adecuadas decisiones con relación a la protección de su patrimonio, que hoy resulta vulnerable por el frecuente uso de Sistemas Informáticos, que si bien es cierto son generadores de grandes soluciones para mejorar la calidad de vida, el aprovechamiento del tiempo y los costos, también es cierto que los mismos Sistemas Informáticos pueden dejar expuesta la información y la confidencialidad de dicha información financiera.

La verdad es que la Ley 1480 deja sin evidenciar los casos de uso de la norma para el Sector financiero, lo que implica que su aplicación esté sujeta a múltiples interpretaciones, por tal motivo a continuación se revisa el concepto 2013008465-008 del 8 de julio del 2013 de La Superintendencia Financiera sobre la aplicación de la Ley en este sector.

- En primer lugar, la Superintendencia Financiera aclara que existe prelación de los elementos considerados en la Ley 1328 del 2009 (Reforma Financiera que incluyó el Estatuto del Consumidor Financiero) por considerarse un régimen especial para el consumidor financiero y por tal motivo una Ley preferente.
- Aplicación de la Ley 1480 de 2011 frente al Régimen de Protección al Consumidor Financiero en materia de fraude electrónico:
    - *La ley 1328 de 2009 es un régimen especial de protección al consumidor financiero y aun cuando la Ley 1480 buscar la protección del consumidor en términos generales para todo bien o servicio, la misma deja claro en su artículo 1 que tiene por objeto establecer los principios y reglas que rigen la protección de los consumidores financieros en las relaciones entre éstos y las entidades vigiladas por la Superintendencia Financiera de Colombia, sin perjuicio de otras disposiciones que contemplan medidas e instrumentos especiales de protección; así mismo el artículo 2º manifiesta que aplica en todos los sectores de la economía, pero aclara economía "*respecto de los cuales no exista regulación especial, evento en el cual aplicará la regulación especial y suplementariamente las normas establecidas en esta ley*".*
    - *Ante esta situación implica que antes de aplicar la Ley 1480 será siempre necesario verificar que el delito o la violación a la norma no se encuentre en la Ley 1328 del 2009 en el Estatuto del Consumidor Financiero.*
    - *En cuanto a lo que se refiere a información mínima que se suministra al consumidor, el artículo 23 de la Ley 1480 de 2011, manifiesta que debe ser clara, veraz, suficiente, oportuna, verificable, comprensible, precisa e idónea y hace responsable a la empresa proveedora del bien o servicio del daño que se cause por información inadecuada. Para este caso la ley 1328 en su capítulo IV (información al consumidor financiero) genera iguales conceptos, pero nombra la Superintendencia Financiera*

para precisar las normas a sus vigiladas. (Contenidas en el capítulo Sexto de la circular básica jurídica CBJ)

- *Frente a fraudes en los Sistemas Informáticos financieros, las entidades financieras deben responder por los riesgos a los que se exponen los usuarios como consecuencia del desarrollo de su actividad, en especial porque una institución financiera se considera una institución de benefició público y por tal motivo no puede faltar a la confianza depositada por el consumidor financiero; sin embargo toda situación debe generar investigación para garantizar que no se trate de una situación de una situación imputable al cliente. En esta época bastante frecuente que por agilidad y facilidad se entreguen claves, se realicen operaciones en sitios no seguros, y no se tenga en cuenta lo protocolos de seguridad informática de la entidad prestadora del servicio, en cuyo caso el Consumidor financiero es el directo responsable. Así entonces, el ejercicio de la actividad bancaria conlleva implícitamente que la entidad financiera cumpla con los deberes especiales que le son exigibles y asuma los riesgos inherentes de los diferentes canales –Internet, banca móvil, cajero automático, etc.- que pone a disposición de sus clientes para el manejo de los productos y servicios ofrecidos.*

Para todos los casos el Defensor del Consumidor Financiero (DFC) es el encargado de dar solución a las quejas y tramites solicitados por los consumidores, y en todos los casos no es suficiente con canalizar una comunicación y otorgar la respectiva respuesta en copia literal, sino que debe propender por la generación de soluciones. Especialmente en asuntos de fraudes financieros originados en los Software y Sistemas informáticos o fraudes a través de medios electrónicos. el caso de fraudes electrónicos, se realiza la verificación de estándares de calidad o requerimientos mínimos de seguridad y perfil transaccional del cliente, cumplimiento de procedimientos

en el Sistema de Atención al Consumidor Financiero SAC (información, seguridad y calidad en los canales), aspectos estos que se encuentran debidamente desarrollados en circulares de esta Superintendencia.

Tabla 4. Artículos Ley 1480 de 2011

Art	**Descripción**	**Impacto**
3	Derecho a la seguridad e indemnidad: Derecho a que los productos no causen daño en condiciones normales de uso y a la protección contra las consecuencias nocivas para la salud, la vida o la integridad de los consumidores.	La seguridad es vida cuando de temas financieros se trata. No sólo es patrimonio. La falta de mecanismos de seguridad y confidencialidad puede costar literalmente vidas de personas y usuarios.
3	Derecho a la reclamación: Reclamar directamente ante el productor, proveedor o prestador y obtener reparación integral, oportuna y adecuada de todos los daños sufridos, así como tener acceso a las autoridades judiciales o administrativas para el mismo propósito, en los términos de la presente ley. Las reclamaciones podrán efectuarse personalmente o mediante representante o apoderado.	Derecho que con frecuencia es ignorado por el sector financiero, pues ante las dificultades esporádicas o frecuentes, se toman un tiempo para dar solución a los requerimientos y reclamaciones de los usuarios y no responden a las afectaciones financieras, sociales, de honra, entre otros que puede originar la no solución inmediata ante una dificultad.
6	Todo productor debe asegurar la idoneidad y seguridad de los bienes y servicios que ofrezca o ponga en el mercado, así como la calidad ofrecida. En ningún caso estas podrán ser inferiores o contravenir lo previsto en reglamentos técnicos y medidas sanitarias o fitosanitarias. Responsabilidad solidaria, administrativa y por daños	El crecimiento acelerado y constante del sector financiero y su requerimiento permanente de actualización en los Software para la búsqueda de protección al consumidor, conlleva también a permanentes cambios y ajustes que en ocasiones no son lo suficientemente divulgados; de igual forma originan fallas en el flujo de la información y la

Art	Descripción	Impacto
		disponibilidad de los recursos del cliente. Pero lejos está la posibilidad de que el usuario pueda evidenciar su situación y que la entidad financiera asuma sus responsabilidades descritas en la Ley por no estar explicitas en la misma para dificultades presentadas en este sector.
27	El consumidor tiene derecho a exigir a costa del productor o proveedor constancia de toda operación de consumo que realice. La factura o su equivalente, expedida por cualquier medio físico, electrónico o similares podrá hacer las veces de constancia. Su presentación no será condición para hacer valer los derechos contenidos en esta ley	La oportunidad de un fraude en el sector financiero es latente y casi imperceptible para miles de usuarios, en cuanto existen costos financieros aplicados a las cuentas habientes que por ser mínima cuantía pueden pasar desapercibidos, y el banco si bien reporta el movimiento, no se genera una información acumulada anual que permita la validación de dichos valores y una eventual reclamación.

Fuente: Ley 1480 de 2011 – Consulta de la norma

11. **AVANCES TECNOLÓGICOS QUE SE HAN DERIVADO EN NUEVAS AMENAZAS QUE SE IMPONEN A NIVEL MUNDIAL EN LA SEGURIDAD INFORMÁTICA**

Sus inicios son del año de 1982, debido a su evolución se conoce como un medio de extorsión.

11.1. **RANSOMWARE**

Es un tipo de programa dañino que restringe el acceso a determinadas partes o archivos del sistema infectado[20], y pide un rescate a cambio de quitar esta restricción algunos tipos de ransomware cifran los archivos del sistema operativo inutilizando el dispositivo y coaccionando al usuario a pagar el rescate.

Aunque los ataques se han hecho populares desde mediados de la década del 2010, el primer ataque conocido sucedió a finales de los '80s por parte del Dr. Joseph Popp.[21] Su uso creció internacionalmente en junio del 2013. La empresa McAfee señaló que solamente en el primer trimestre del 2013, había detectado más de 250 000 tipos de ransomware únicos[22]

11.1.2. Funcionamiento

El atacante camufla el código malicioso dentro de otro archivo o programa apetecible para el usuario que invite a hacer *clic.* Algunos ejemplos de estos camuflajes serían:

- Archivos adjuntos en correos electrónicos.

[20] «Virus: Ransomware bitcoins y móviles». definición. Consultado el 31 de octubre de 2017.
[21] «A History of Ransomware Attacks: The Biggest and Worst Ransomware Attacks of All Time». *Digital Guardian*. Consultado el 3 de octubre de 2017.
[22] «McAfee: Cyber criminals using Android malware and ransomware the most». Info World. Consultado el 16 de octubre de 2017>>

- Vídeos de páginas de dudoso origen.
- Actualizaciones de sistemas.
- Programas, en principio, fiables como Windows o Adobe Flash.

Figura 2.Como actúa Ramsoware

Fuente: Pagina de onemagazine.es

Luego, que ha penetrado en el ordenador, el ransomware se activa y provoca el bloqueo de todo el sistema operativo, lanza el mensaje de advertencia con la amenaza y el importe del rescate que se ha de pagar para recuperar toda la información. Además, en ocasiones incluyen en la amenaza la dirección IP, la compañía proveedora de Internet y hasta una fotografía captada desde la cámara web.[23]

11.2.3. Como protegerse

Se puede evitar si se siguen unas buenas prácticas

[23] IIEMD, Instituto Internacional Español de Marketing Digital (15 de noviembre de 2016). «Qué es Ransomware y cómo Microsoft lo combatirá». *https://iiemd.com/marketingdigital/*. Consultado el 1 de noviembre de 2017.

Figura 3. Como protegerse de Ransoware

Fuente: El autor

11.2. TIPOS DE RAMSOWARE

Figura 4 Tipos de Ransoware

Fuente: Pagina de Protetco

11.2.1 Maktub

El ataque se realiza al comprimir los archivos antes de cifrarlos**.**

El proceso se realiza a través de correos spam, en archivos adjuntos en PDF o de editor de texto. Cuando el usuario lo abre, en segundo plano se instala en el equipo, se comprimen los archivos y los cifra.

11.2.2. Doublelocker

Es un malware que funciona en dos etapas. Primero trata de vaciar la cuenta bancaria o de PayPal y luego bloquea el dispositivo e información para solicitar el pago del rescate, para Android. Además de cifrar la información, es capaz de bloquear el dispositivo. Se distribuye a través de una versión falsa de Adobe Flash Player, el cual es subido a sitios web.

DoubleLocker puede cambiar el PIN del dispositivo, evitar que las víctimas accedan al mismo y también cifrar la información que encuentra en él; una combinación que no se ha visto hasta la fecha en el ecosistema Android.

11.2.3 Wannacry

Apareció el 12 de mayo de 2017, con origen en Estados Unidos, de malware Vault [24]revelado por Wikileaks, el código ataca a sistemas Windows que no estén actualizados de una manera adecuada.

Este virus provocó el cifrado de datos en más de 75 mil ordenadores por todo el mundo afectando, entre otros, a:

- Rusia: afecto a la red de semáforos, metro e incluso el Ministerio del Interior;
- Reino Unido: afecto a los centros hospitalarios;
- Estados Unidos;
- España: afecto a empresas como: Telefónica, Gas Natural e Iberdrola.

[24] Vault 7 es una serie de documentos que WikiLeaks comenzó a lanzar el 7 de marzo de 2017 que detalla actividades de la Agencia Central de Inteligencia (CIA) para ejercer vigilancia electrónica y guerra informática.

. Los sistemas operativos más vulnerables ante el *ransomware* son: Windows Vista, Windows 7, Windows Server 2012, Windows 10 y Windows Server 2016.

El ordenador infectado que se conecte a una red puede contagiar el *ransomware* a otros dispositivos conectados a la misma red, infectando a dispositivos móviles, si no tienen el parche de seguridad instalado.

11.2.4. Petya

Petya se descubrió en marzo de 2016.

Cómo funciona el malware infecta el registro de inicio, que encripta las tablas de archivos del sistema de archivos NTFS al volver a iniciar se inicia el sistema infectado, bloqueando el sistema para que arranque en Windows, hasta que se pague.

11.2.5. **Troyano Remtasu**

Este código malicioso, roba la información por medio de la captura de datos generados en el teclado, los almacena en un archivo dentro de la máquina y luego los envía a un equipo remoto utilizando protocolo FTP.

Remtasu, pasa a formar parte de una botnet[25] controlada por el atacante.

En Colombia el código malicioso llamado Remtasu, se instala y empieza a robar información del dispositivo, parecido al sistema de copiar y pegar texto: tiene la posibilidad de ser un keylogger, “es un programa diseñado para registrar lo que el usuario teclea para después enviar estos datos al servidor del atacante”.

Se ha incrementado en un 30% el virus, en los últimos meses, el 82% de los archivos detectados correspondían a campañas de propagación asociadas a correos electrónicos de servicios relacionados con usuarios en Colombia. El restante porcentaje se reparte en direcciones asociadas con usuarios de países como Argentina, Chile, Brasil, Costa Rica, Ecuador, Venezuela y México, pero en menor medida:

Remtasu no estaba buscando como blancos empresas, sino usuarios en general. este tipo de código utiliza son correos electrónicos, que llevan un archivo adjunto, y que dicen venir de una entidad bancaria, o instituciones como la Dian, para así engañar al usuario, quien termina descargando un archivo ejecutable (usualmente con la extensión .exe)

Dentro de algunos nombres, se encuentra la DIAN[26], Avianca[27], Falabe**l**la[28] o títulos que hacen referencia a cobros jurídicos o pagos sin realizar. Si bien los íconos utilizados corresponden con aplicaciones o tipos de archivos como videos, fotos o documentos, la extensión de los mismos es la de un archivo ejecutable, lo cual ya es una señal de alerta para considerar el archivo como sospechoso.

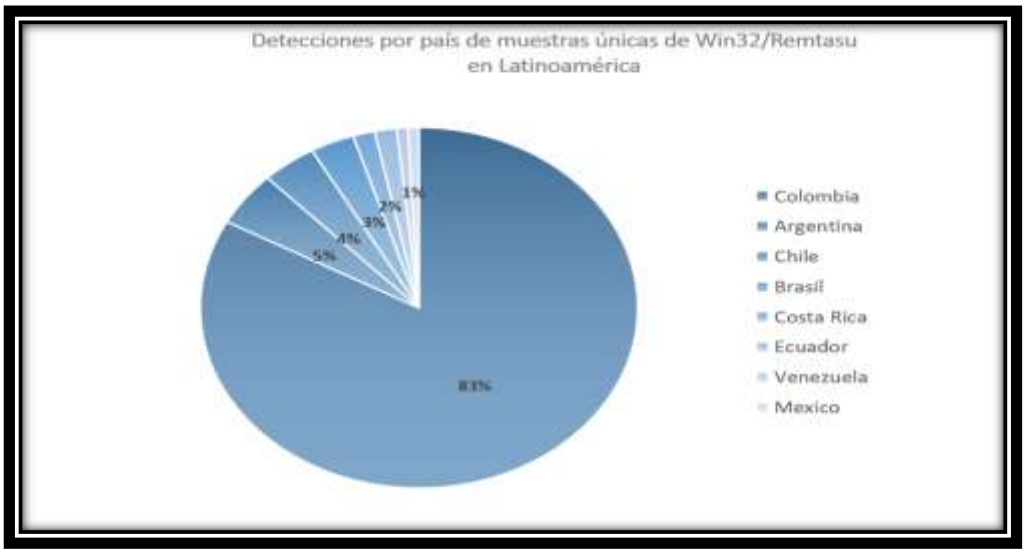
[25] El término “botnet” nace de dos palabras en inglés: “bot” por “robot”, mientras que “net” proviene de network o red en español. En resumen, se trata de un robot de red.

[26] La DIAN es la entidad encargada de garantizar el cumplimiento de las obligaciones tributarias, aduaneras y cambiarias en Colombia. Facilita las operaciones de comercio nacional e internacional. Se constituyó como Unidad Administrativa Especial, mediante Decreto 2117 de 1992

[27] AVIANCA S. A., es la aerolínea de bandera colombiana. Fue la primera fundada en América y es la segunda aerolínea más antigua del mundo, después de KLM, aunque KLM cesó operaciones durante la segunda ...

[28] Falabella es una tienda por departamento fundada en 1889 por una familia italiana radicada en Chile. Propiedad de S.A.C.I., Falabella cuenta con operaciones en Chile, Argentina, Perú, Colombia, Uruguay y Brasil

Tabla 5. Detenciones por países de Remtasu



Fuente: https://www.welivesecurity.com/la-es

12. DESCRIBIR LOS CONTROLES DE LOS BANCOS Y LOS MECANISMOS DE PROTECCIÓN PARA LOS USUARIOS DE LA BANCA ELECTRÓNICA

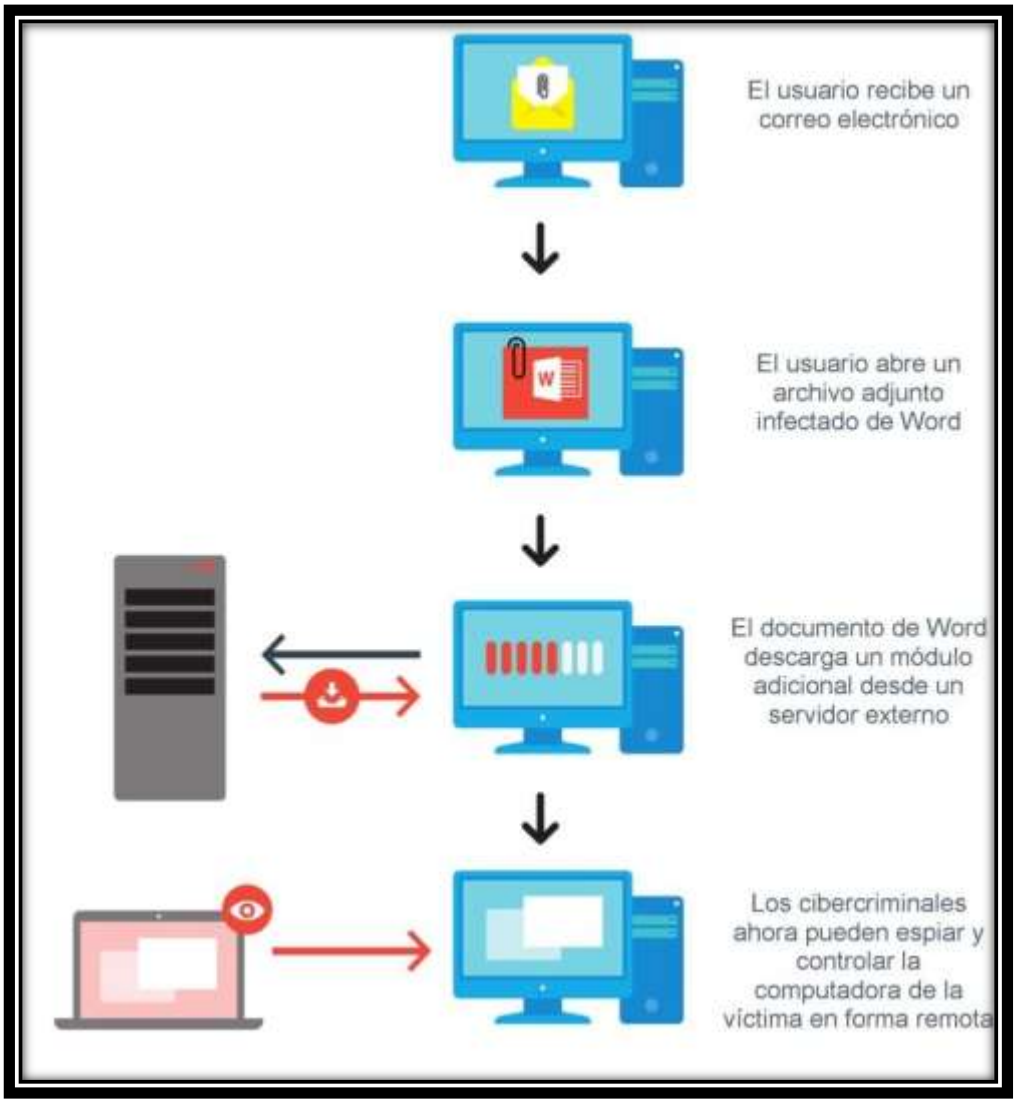
Figura 5.Estafas bancarias

Fuente: https://www.asociacionafectadosinternet.es/phishing-bancario/

En nuestro país la violación informática se realiza en el ciberespacio, y no se detiene. Se puede perpetrar desde cualquier lugar del país y contra cualquier usuario de ordenador del mundo, el uso indebido de las computadoras es lo que ha propiciado la necesidad de regulación por parte del derecho.

Cuando la víctima tiene conocimiento de que los delincuentes han accedido a sus cuentas bancarias y han efectuado transacciones o disposiciones de efectivo no consentidas ni autorizadas por éste, lo normal es que denuncie los hechos en la entidad bancaria y si la entidad no soluciona su caso debe radicar ante la superintendencia financiera su queja

Figura 6.Proceso de Acceso remoto



Fuente: https://www.welivesecurity.com

Siendo Internet una red pública de comunicaciones la seguridad de las operaciones bancarias se precisan soluciones tecnologías avanzadas que peritan minimizar las amenazas contra la autenticidad, la integridad y la confidencialidad de los datos que viajan a través de la Red así como el no repudio de las transacciones.

Las entidades prestadoras del servicio de banca online deben dotarse de medidas suficientes que garanticen al usuario la seguridad de las operaciones por lo que, en el supuesto de insuficiencia o mal funcionamiento

de las adoptadas, deben ser las entidades bancarias las que asuman las consecuencias derivadas de los fallos de seguridad del sistema. Aparte el uso de protocolos seguros de cifrado de información SSL (Secure Sockets Layer o capa de conexión segura) que permite establecer una conexión cifrada entre el usuario y la entidad de crédito impidiendo con ello el que terceras personas no autorizadas puedan acceder a la información confidencial que viaja a través de la Red, los sistemas de seguridad empleados por las entidades de crédito en sus operaciones electrónicas están basados en última instancia en infraestructuras de claves públicas (PKI) que garantizan la autentificación del usuario mediante el uso de claves de firma digital.

Las medidas establecidas por los bancos se articulan en varios niveles de seguridad complementarios y compatibles entre sí.

El primer paso, consiste en un código de usuario - contraseña o clave secreta privada que cada cliente podrá configurar para acceder a la oficina virtual.

Otro nivel de seguridad se sitúa la denominada tarjeta de coordenadas proporcionada por la entidad bancaria a cada usuario que consiste en un código de autorización de las operaciones único y personal para cada una de ellas. Estas claves se exigen al cliente para realizar cualquier operación que no sea una mera consulta de saldos como puede ser el movimiento de dinero entre cuentas, compras o transferencias.

Otra es la tarjeta de coordenadas que utiliza (BBVA) en su página virtual, lo constituye el empleo de claves aleatorias perecederas de un solo uso (“One time password”) que evitan el riesgo de copia, pérdida o robo de las claves de seguridad

Tabla 6.Tecnologías para la inclusión financiera

Tecnología	Definición	Solución de Inclusión Financiera
Big data	Manejo y administración de grandes cantidades de información.	El Big Data rompe barreras de asimetrías de información, pues la recolección de datos a través de fuentes alternas a las tradicionales brinda la posibilidad de conocer mejor al cliente e incluir dicha información en procesos de aprobación de créditos. Sin embargo, estos datos solo son útiles para la inclusión financiera si existe una capacidad mínima para analizar, procesar y convertirlos en mejores productos financieros.
Identificación biométrica	Sistemas de autenticación de identidad a través de medios fisiológicos como las huellas dactilares, lectura del iris, reconocimiento de voz o facial entre otros	En ocasiones, la ausencia de identificación es un desafío para los proveedores de servicios financieros, especialmente en zonas rurales, pobres o de bajos niveles de alfabetismo, en donde los procesos de registro de personas son complicados. Esta tecnología permite probar de forma clara, automática y confiable la identidad de posibles clientes.
Cloud computing	La computación en la nube busca tener todos los archivos e información en Internet.	La habilidad de tener el almacenamiento de datos y servicios en la nube, asegura el procesamiento rápido de transacciones y la completa conectividad entre el *front* y el *back* de los servicios financieros. Razón por la cual la implementación de esta herramienta en la prestación de servicios financieros ayudaría a mejorar los indicadores de uso de productos financieros, pues facilita la realización de transacciones garantizando seguridad y eficiencia.
Dispositivos móviles	Dispositivos inteligentes que ofrecen una amplia gama de funciones avanzadas, con conexión a redes de telecomunicaciones.	La alta penetración de teléfonos inteligentes y tabletas permite que los consumidores financieros puedan acceder a sus productos y servicios las 24 horas los 7 días de la semana, traduciéndose en mejores indicadores de calidad, bienestar y experiencia del cliente.
Internet	Conjunto descentralizado de redes de comunicación interconectadas.	Esta plataforma se convierte en un insumo fundamental de inclusión financiera pues permite la creación de canales como la banca móvil en donde cualquier consumidor puede acceder a información de productos adquiridos o a la oferta existente en el mercado para tomar decisiones informadas, que rompen barreras de asimetrías de información.

Fuente: http://www1.firstdirect.com/1/2/

Figura 7. Logo de Symantec

Fuente: https://www.symantec.com/

Symantec™ [29]es el distintivo de Seguridad en Internet más usado en el mundo, el escaneo de malware de sitio web y la prevención de phishing, son las estrategias que dan tranquilidad a los clientes y ayudan a reducir los riesgos de fraude.

[29] Symantec Endpoint Protection 14
La seguridad para endpoint de un solo agente más avanzada del mundo con prevención, detección y respuesta, engaño y adaptación.

13. INFORME SOBRE LOS REPORTES QUE SE PRESENTAN EN SEGURIDAD INFORMÁTICA PARA TRANSACCIONES BANCARIAS

De acuerdo con el Informe de Operaciones y Transacciones de la Superintendencia Financiera de Colombia, entre enero y diciembre 2017 se realizaron más de 5.400 millones de transacciones, de las cuales el 47% se hicieron a través de internet, cifra que en 2008 solo alcanzaba el 23%. Así en los últimos nueve años, las transacciones por ese canal han tenido un crecimiento superior a 25 puntos porcentuales.[30]

Por otro lado, a nivel de operaciones monetarias, el monto en el sistema financiero alcanzó los 7.214 billones de pesos durante 2017 de los cuales el 35% se efectuó por medio de internet ($ 2.550 billones de pesos, aproximadamente) mientras que solo de esas transacciones el 0.2% se realizó a través de telefonía móvil ($11 billones de pesos).

La puesta en marcha del CSIRT ubica al sector bancario y financiero a la vanguardia en la carrera por contrarrestar los ciberataques. Actualmente, la banca recibe el 39,6% del total de ataques del ciberespacio, lo que equivale en promedio a 214 mil por día.

Con la ejecución del proyecto de autenticación biométrica que lidera Asobancaria con apoyo de la Registraduría Nacional del Estado Civil y Certicámara S.A., el sector bancario y financiero ha venido avanzando a pasos agigantados en la transformación digital de sus servicios con documentos digitales de firma electrónica que cuentan con la misma validez jurídica que los documentos físicos.

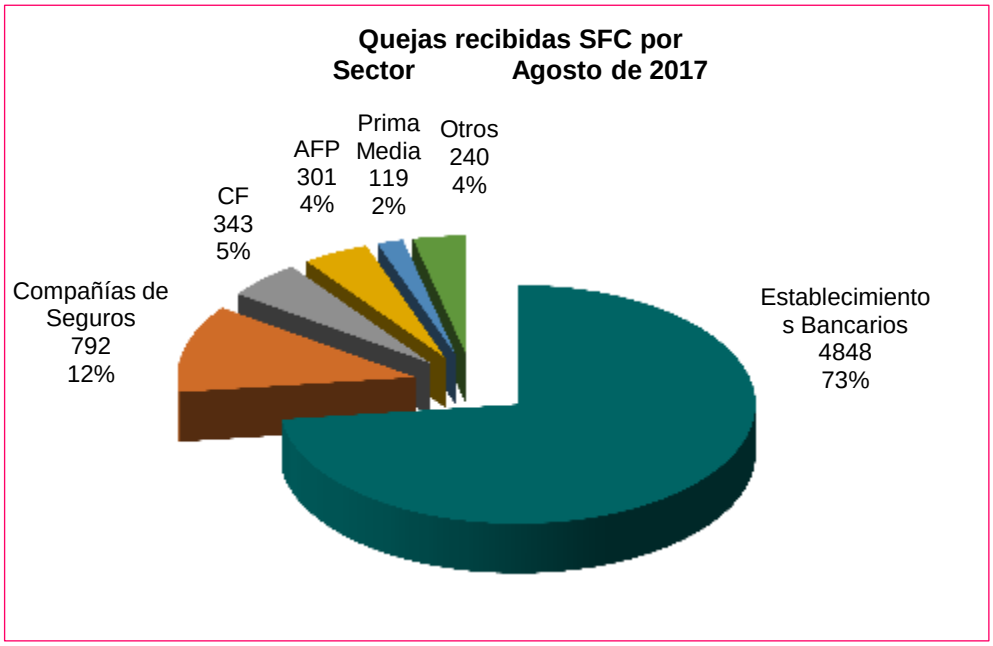
Gracias a este proyecto se ha mitigado el riesgo de suplantación y las transacciones han pasado de minutos a segundos, razón por la cual se espera que al finalizar este año todo el sector haga uso de esta herramienta y así facilitar el acceso de más personas al sistema bancario.[31]

[30] http://www.asobancaria.com/informe-mensual/
[31] http://www.asobancaria.com/informe-mensual/

Esta iniciativa ha sido catalogada como una de las más innovadoras en materia de seguridad convirtiéndose en referente para la región, por lo cual, diferentes países han manifestado su intención de replicarlo.

Para Certicámara S.A., operador biométrico del proyecto, la banca colombiana es ejemplo a nivel mundial en seguridad a través de esta iniciativa. Los retos venideros giran en torno a la biometría móvil, y el uso de dispositivos (tabletas y celulares) para la validación de identidad por huella y facial sin importar la ubicación geográfica. Este es uno de los pasos más importantes hacia el on-boarding digital que pueden ofrecer las entidades financieras

Figura 8. Quejas Radicadas del sector bancario



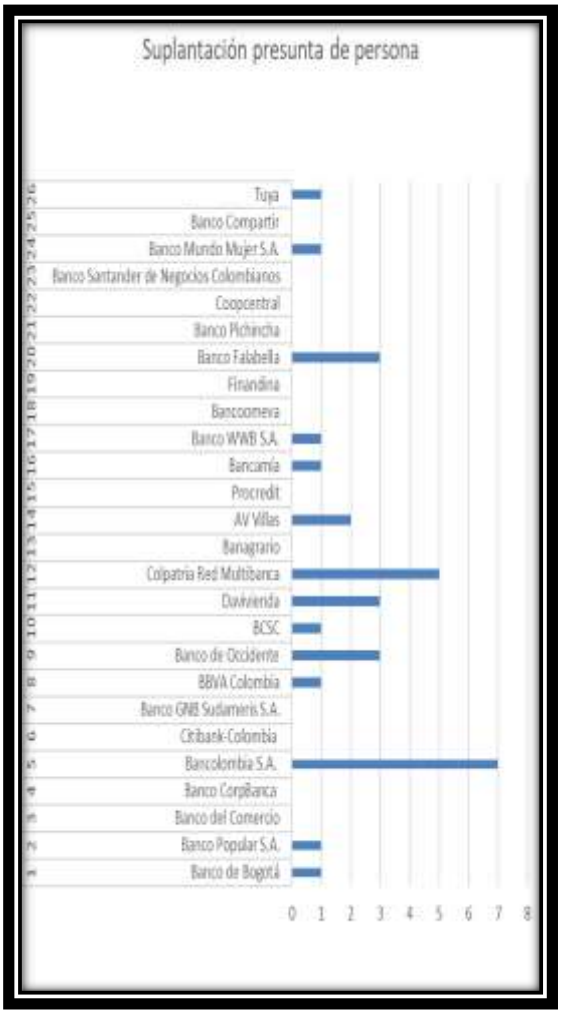
Fuente: Asobancaria

Figura 9.Entidades Bancarias

No.	Entidad Bancaria	Suplantación presunta de persona
1	Banco de Bogotá	1
2	Banco Popular S.A.	1
3	Banco del Comercio	0
4	Banco CorpBanca	0
5	Bancolombia S.A.	7
6	Citibank-Colombia	0
7	Banco GNB Sudameris S.A.	0
8	BBVA Colombia	1
9	Banco de Occidente	3
10	BCSC	1
11	Davivienda	3
12	Colpatria Red Multibanca	5
13	Banagrario	0
14	AV Villas	2
15	Procredit	0
16	Bancamia	1
17	Banco WWB S.A.	1
18	Bancoomeva	0
19	Finandina	0
20	Banco Falabella	3
21	Banco Pichincha	0
22	Coopcentral	0
23	Banco Santander de Negocios Colombianos	0
24	Banco Mundo Mujer S.A.	1
25	Banco Compartir	0
26	Tuya	1

Fuente: El autor

Figura 10. Gráfico de suplantación

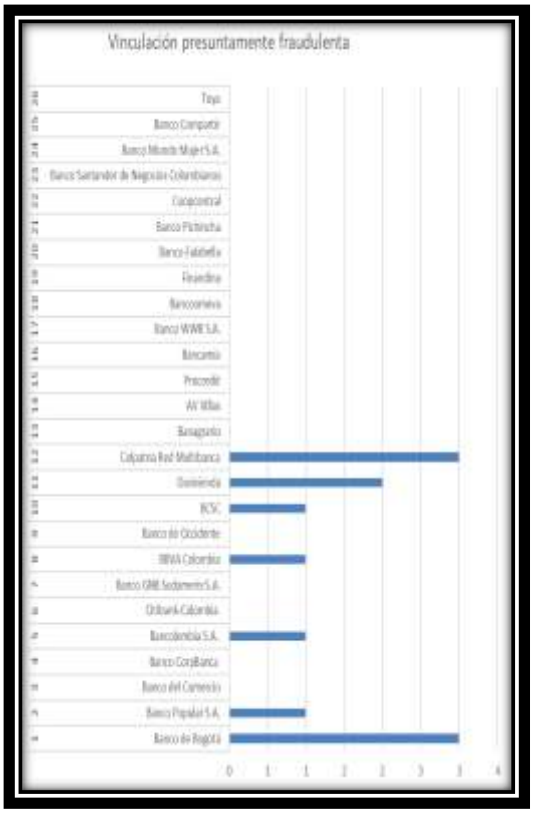


Fuente: El autor

La suplantación de identidad permite al atacante realizar operaciones en nombre de otro.

Según este reporte se puede observar que las entidades bancarias, mensualmente presentan problemas de seguridad en sus servicios y los usuarios tienen que levantar quejas por suplantación y vinculación fraudulenta, al registrar en sus cuentas compras que no han realizado y que les reportan que sus cuentas se encuentran bloqueadas.

Figura 11 . Vinculaciones fraudulentas en las entidades bancarias



No.	Entidad Bancaria	Vinculación presuntamente fraudulenta
1	Banco de Bogotá	3
2	Banco Popular S.A.	1
3	Banco del Comercio	0
4	Banco CorpBanca	0
5	Bancolombia S.A.	1
6	Citibank-Colombia	0
7	Banco GNB Sudameris S.A.	0
8	BBVA Colombia	1
9	Banco de Occidente	0
10	BCSC	1
11	Davivienda	2
12	Colpatria Red Multibanca	3
13	Banagrario	0
14	AV Villas	0
15	Procredit	0
16	Bancamía	0
17	Banco WWB S.A.	0
18	Bancoomeva	0
19	Finandina	0
20	Banco Falabella	0
21	Banco Pichincha	0
22	Coopcentral	0
23	Banco Santander de Negocios Colombianos	0
24	Banco Mundo Mujer S.A.	0
25	Banco Compartir	0
26	Tuya	0

Fuente: El autor

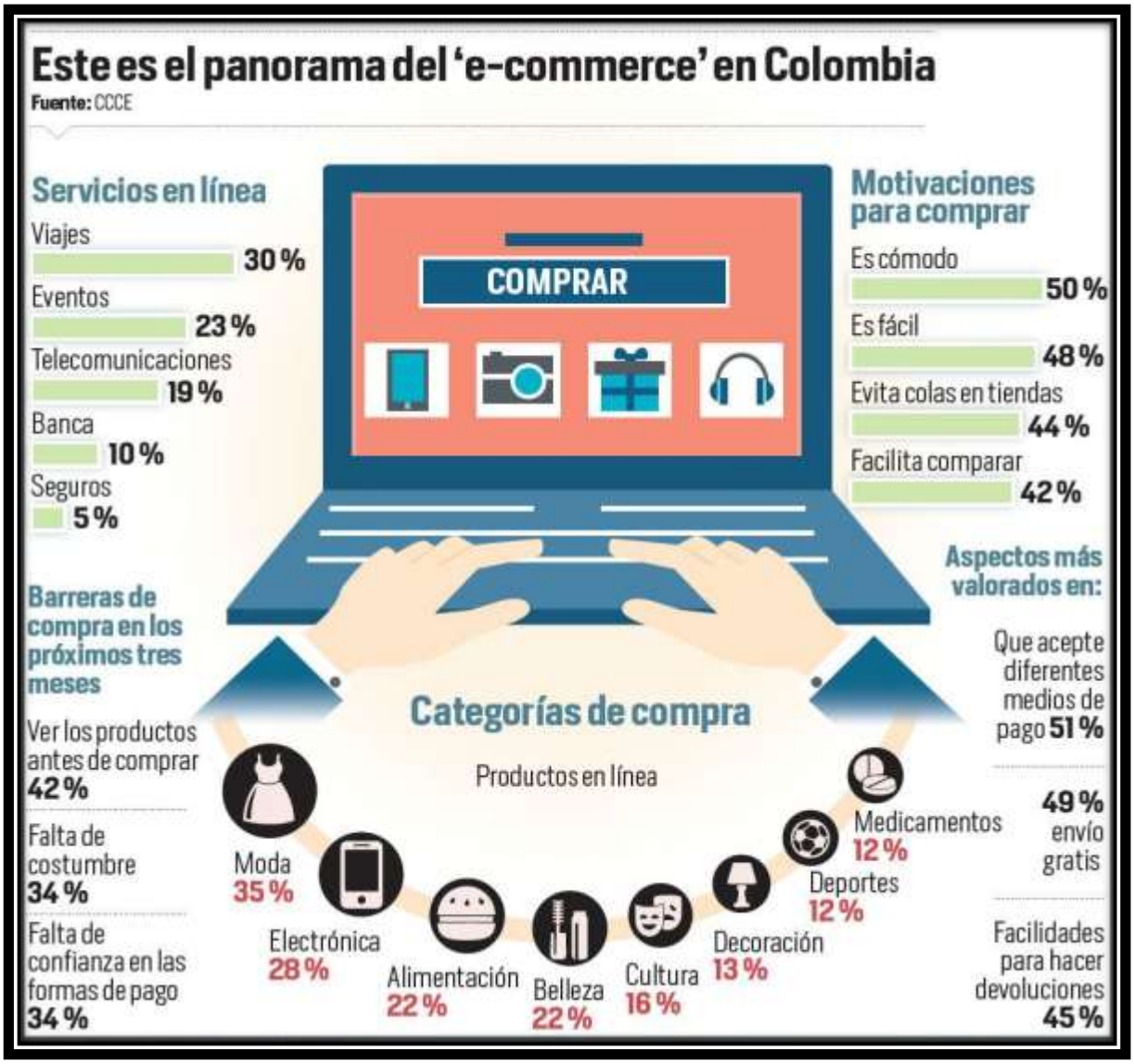
Figura 12. Fraudes Bancarios

Fuente. Condusef

Fraudes Bancarios: se refiere a la clonación de tarjeras, la cual utilizan para realizar compras y retirar el efectivo que tenga disponible la tarjeta

Las nuevas amenazas cibernéticas, han generado retos en materia de defensa y seguridad, que se ven enfrentados; empresas y personas en diversos ámbitos. es necesario definir y aplicar regulaciones que establezcan las bases para la protección del ciberespacio, así como fortalecer en la prevención, detección e investigación de ciberdelitos.

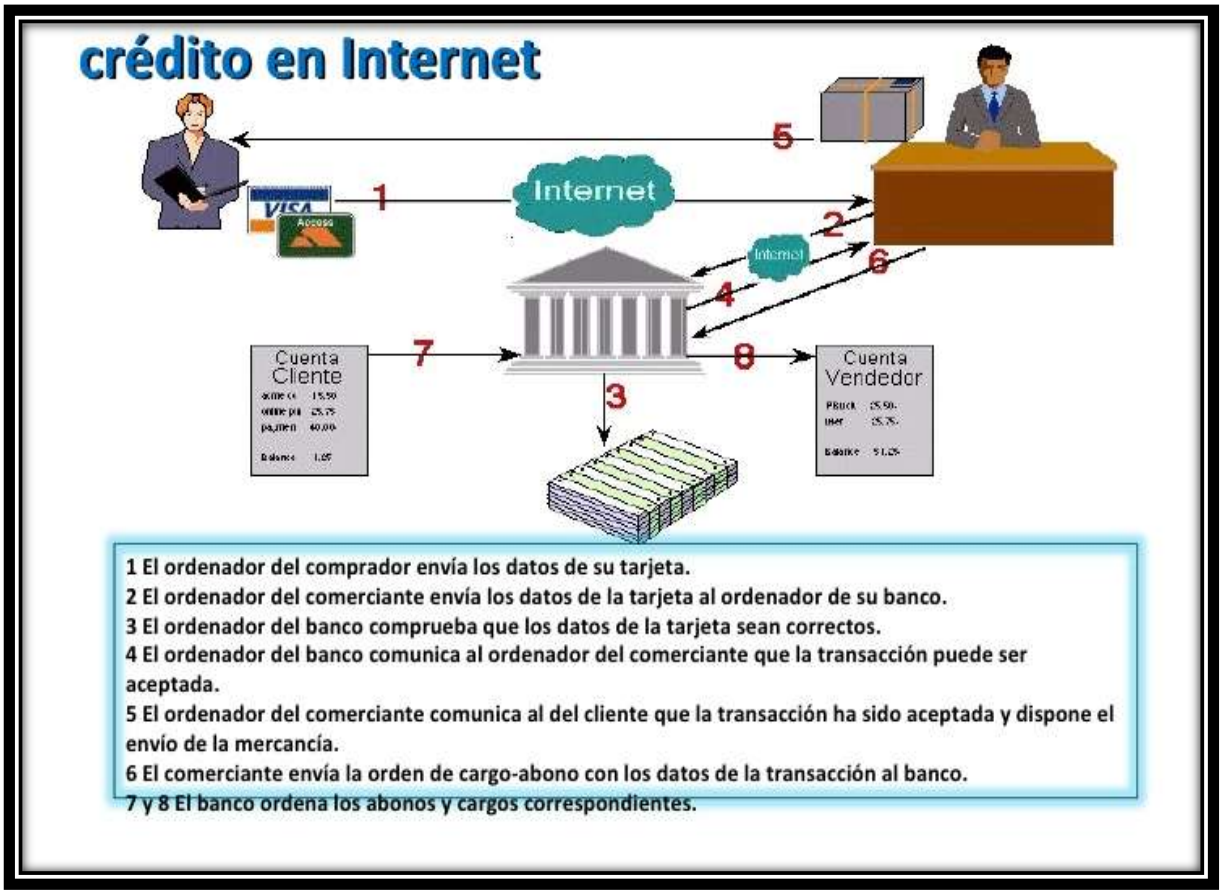
Figura 13. Comercio más utilizado en Colombia.



Fuente: CCCE

Modalidades de compras se busca garantizar la seguridad. Este es quizás el mayor problema para la gente interesada en realizar compras electrónicas.

Figura 14. Pasos a realizar pagos en internet



Fuente. https://es.slideshare.net/comerciop/comercio-electronico-3618401

El Comercio Electrónico es seguro siempre que se tomen las precauciones necesarias por parte del consumidor

Una página es segura, cuando aparece un candado en la parte inferior o superior de la página. Si aparece cerrado nos indica que la página es segura.

Se debe revisar la dirección URL de la página, debe aparecer https:// (la letra "s" confirma que se trata de un protocolo seguro).

Los navegadores indican los niveles de seguridad y alertan al usuario si son confiables realizar la transacción.

Alto: Es apropiada para recorrer los sitios menos seguros.

Mediano: Recomendado por Microsoft. Es seguro y funcional.

Medio bajo: Ideal para redes internas.

Bajo: sólo para sitios de plena confianza.

No es recomendable nunca, se sugiere no ingresar.

En el CONPES[32] No. 3854, que aborda el tema sobre "Política nacional de seguridad digital" de abril de 2016. Se relaciona con los lineamientos para las terminales de áreas financieras de entidades públicas, que pretenden que los dispositivos desde los cuales las entidades públicas realizan operaciones bancarias cuenten con unos requisitos mínimos de seguridad, tanto físicos como lógicos.

A pesar de las ventajas que pueda traer estas nuevas tecnologías, su beneficio se ve reflejado en muchos aspectos tales como (económicos, sociales y/o financieros), esto ayuda también a incrementar los riesgos de ataques informáticos.

Según el Informe Global de Seguridad 2015 de Trustwave, las amenazas informáticas siguen en aumento

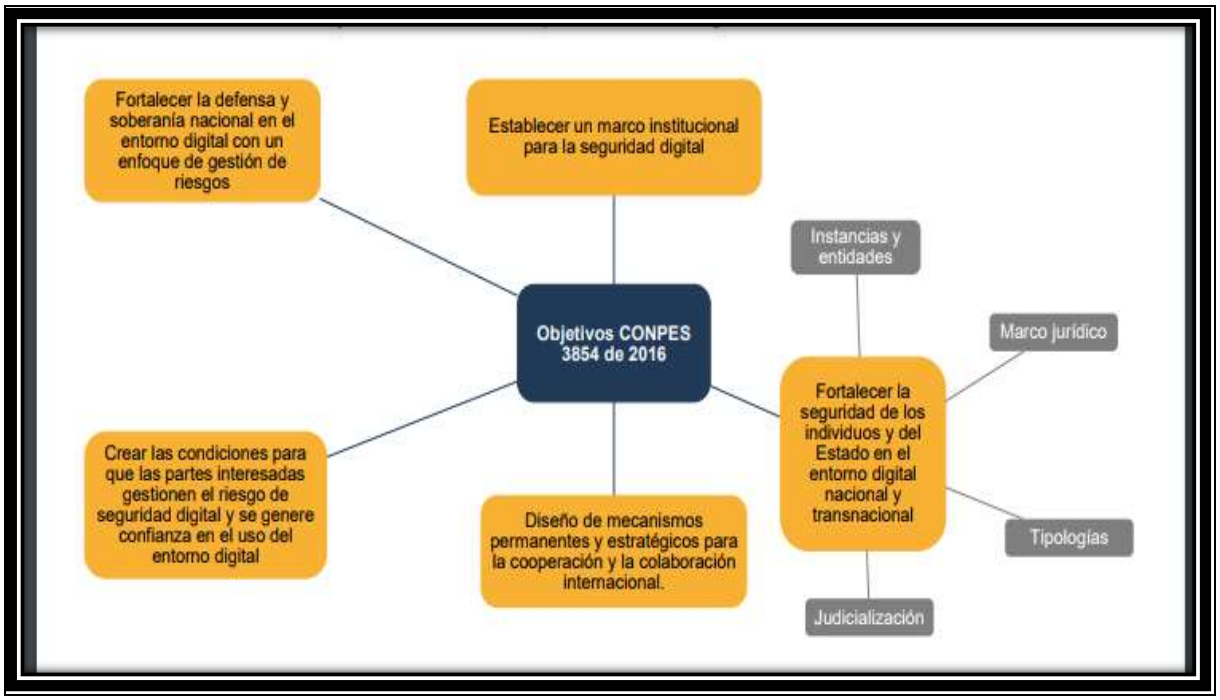
[32] Ésta es la máxima autoridad nacional de planeación y se desempeña como organismo asesor del Gobierno en todos los aspectos relacionados con el desarrollo económico y social del país.

Tabla 7 Estadísticas en materia de ciberdefensa y ciberseguridad

	Descripción
1.	Más de 169 millones de registros personales fueron expuestos en 2015 como producto de las 781 infracciones publicitadas por los sectores financieros, de negocios, educación, gobierno y salud (Reporte de brechas totales ITRC – *Identity Theft Resource Center*).
2.	El costo global promedio por cada registro perdido o robado que contiene datos confidenciales y sensibles fue de USD 154. (Costo de las brechas de información: Análisis Global | IBM / Ponemon).
3.	En 2015, se registró un 38% más de incidentes de seguridad detectados que en el 2014. ("Encuesta sobre el Estado Global de Seguridad de la Información 2016" | Price Waterhouse Cooper).
4.	En 2015, incluso un menor número de pequeñas y medianas empresas (29%) utilizaron herramientas estándar como la configuración y parches para evitar violaciones de la seguridad, en comparación con el 39% que lo hizo en 2014. ("Informe Anual de Seguridad 2016 " | Cisco).
5.	La mediana del número de días que los atacantes se quedan en estado latente dentro de una red antes de la detección es más de 200. ("Analíticas de las amenazas avanzadas " | Microsoft).
6.	Al menos el 52% de los encuestados consideró que un ataque cibernético exitoso contra su red se llevaría a cabo dentro del año. ("Informe de Defensa frente a Ciberamenazas 2015" | Grupo CyberEdge).
7.	El 70% de los ataques cibernéticos utilizan una combinación de técnicas de *phishing* y piratería e implican una víctima secundaria. ("Violación de datos Informe 2015 Investigaciones" | Verizon).
8.	El 74% de los directores de seguridad están preocupados por los empleados que roban información confidencial de la empresa. ("SANS 2015 Encuesta sobre Ejecutivas Amenazas" | SpectorSoft).
9.	Sólo el 38% de las organizaciones globales afirman que están preparadas para manejar un ciberataque sofisticado. ("Informe de situación sobre Ciberseguridad Global 2015" | ISACA Internacional).
10.	La mayoría de las víctimas de violación de datos encuestadas, el 81%, no cuentan con un sistema o servicio de seguridad para asegurarse de la detección de las violaciones de datos sino que confía en la notificación de un agente externo a pesar del hecho de que las violaciones 'autodetectadas' tardan sólo 14,5 días para contener un ataque a partir de la fecha de intrusión, mientras que las infracciones detectadas por un agente externo toman un promedio de 154 días. ("Informe Global de Seguridad 2015 de Trustwave" | Trustwave).

Fuente: Elaboración Asobancaria.

Tabla 8- Objetivos centrales de la política del CONPES



Fuente: CONPES 3854 de 2016. Elaboración Asobancaria

Se espera que con este informe del Conpes, sirva para contribuir con un entorno digital más seguro y reducir las prácticas inseguras de sus usuarios y sus posibilidades de ser víctimas de delitos.

Desde el sector financiero, cualquier esfuerzo que realicen en seguridad informática, es bien recibido ya que ayudan a promover un entorno digital más seguro

Teniendo en cuenta la meta establecida en el Plan Nacional de Desarrollo de lograr que en 2018 el 84% de la población adulta tenga al menos un producto financiero, se plantea el reto de incluir financieramente en 2 años y medio a más de 3,3 millones de adultos

Con el esquema propuesto en este documento se espera alcanzar el logro de esos objetivos, fortaleciendo las capacidades de todos los interesados en seguridad informática en el país.

14. RECOMENDACIONES

Se recomienda a las entidades bancarias que empleen las herramientas de comunicación que la tecnología ofrece, las plataformas que se manejan por Internet deben ofrecer a sus clientes un mejor servicio al cliente y le permitan obtener una atención igual o mejor que en cualquier sucursal bancaria.

También se deben realizar más campañas para informar a sus clientes sobre las medidas de seguridad que debe manejar y las aplicaciones o revisar las certificaciones que expida la página en la cual desea hacer alguna transacción o compra virtual.

15. DIVULGACION

El presente proyecto no posee ninguna restricción, la información desarrollada en el documento es completamente pública. La divulgación se puede realizar por la UNAD, la pueden consultar los estudiantes de la UNAD y el resto de los usuarios que ingresen a consultar el documento.

CONCLUSIONES

El impacto de los delitos informáticos bancarios va en aumento, y los avances tecnológicos permiten que exista un mayor riesgo al usar el sistema en el intercambio de información, los bancos deben adaptar medidas de seguridad para tener un mejor manejo de la confidencialidad de los datos de sus clientes y asegurar que sus transacciones se realicen apropiadamente en Internet. También deben, brindar seguridad al cliente que tienen un buen control y seguridad necesarios para infundir confianza entre los usuarios.

Los avances tecnológicos permiten que el sector financiero sea el que más use, las tecnologías, a nivel mundial, en la banca por Internet.

Para esta plataforma se ofrecen una cantidad de productos y/o servicios bancarios a los clientes: tanto a personas naturales o jurídicas, el cual permite una mayor rapidez en el proceso de servicios.

El incremento de usuarios de la banca virtual por medios de las Apps en sus celulares va en aumento. El uso de tecnologías ofrece servicios online, en todos los sectores de la economía. los cuales manejan unas ventajas competitivas que benefician al cliente.

Los bancos incentivan a sus clientes para utilizar la banca virtual, también ellos realizan inversiones para ofrecer un alto estándar de calidad, y las medidas de seguridad que requiera al realizar transacciones a través de la red, podemos observar que bancos como Bancolombia y BBVA, en sus plataformas de Aplicaciones App ya usan el sistema Touch Id, el cual permite el ingreso con huella dactilar lo que permite que su sistema de ingreso a la plataforma sea más seguro.

BIBLIOGRAFIA

BARZANALLANA, Rafael. Bibliografía de Joseph Carl Robnett Licklider. Departamento Informática y Sistemas. Universidad de Murcia. 2016. {En línea}. {Consultado el 20 de agosto de 2017} disponible en: http://www.um.es/docencia/barzana/BIOGRAFIAS/Biografia-JCR-Licklidder.php

BERTOGLIO, Oscar J. Introducción a la Teoría General de los Sistemas. México, D.F, Limusa.1982.

CCM. Diferentes tipos de programas maliciosos. Comunidad Informática. 2017.{En línea}. {Consultado el 1 de agosto de 2017} Disponible en: http://es.ccm.net/faq/2809-diferentes-tipos-de-programas malicioso

CERVIGÓN, H. Alfonso, G. & ALEGRE, R. María Del Pilar. Seguridad Informática.2017. Ediciones Paraninfo, S.A. 1Ed. España. {En línea}. {Consultado el 20 de Agosto de 2017} Libro digital Disponible en: https://books.google.com.co/books?id=c8kni5g2Yv8C&printsec=frontcover&dq=concepto+de+seguridad+informatica&hl=es&sa=X&ved=0ahUKEwijgf39lY_UAhVILyYKHYPgABUQ6AEIJjAB#v=onepage&q=concepto%20de%20seguridad%20informatica&f=false

Ciberdefensa y Ciberseguridad: de la política pública a las acciones concretas. De la Superintendencia Financiera. {En línea}. {Consultado el 30 de octubre de2017}Disponible en: https://cdn2.hubspot.net/hubfs/1756764/Asobancaria%20Eventos/Asobancaria%20-%20Semanas-Economicas/1062.pdf

Comercio Electrónico. {En línea}. {Consultado el 7 de diciembre de 2017} Disponible en: https://es.slideshare.net/comerciop/comercio-electronico-3618401

Concepto 2013008465-008 del 8 de julio de 2013 de La Superintendencia Financiera. {En línea}. {Consultado el 30 de septiembre de 2017} Disponible en: www.superfinanciera.gov.co/SFCant/Normativa/PrincipalesPublicaciones/boletinboletin4613/Proteccion%20Consumidor.html

¿Cuáles son los riesgos de permitir que las personas usen su teléfono inteligente en el banco? {En línea}. {Consultado el 30 de septiembre de 2017} Disponible en: https://www.welivesecurity.com/2017/08/23/smartphone-use-bank/

ESCRIVA, G. Gema & ROMERO S. Rosa. Seguridad Informática. M. Macmillan Iberia, S.A. 2017. En español. Libro electrónico ISBN 9788415991410. {En línea}. {Consultado el 1 de agosto de 2017} Disponible en: http://site.ebrary.com.sibulgem.unilibre.edu.co:2048/lib/bibliounilibresp/detail.actio?docID=10820963&p00=seguridad+informática

ENDERLE, Gunter K. & KANSY G. Pfaff. Computer Graphics Programming. GksThe Graphics Standars. Second Edition. London Paris Tokyo. Springer – Verlag.1987

Estas son las amenazas de seguridad informática de las que se debe cuidar. {Consultado el 30 de septiembre de 2017} Disponible en: https://www.elespectador.com/tecnologia/estas-son-amenazas-de-seguridad informatica-de-se-debe-articulo-611247

GUTIERREZ C, Oscar. Glosario terminológico sobre internet y contenidos multimedia. Universidad Autónoma de Barcelona. 2014 {En línea}. {Consultado el 24 de agosto de 2017} Disponible en: https://ddd.uab.cat/pub/tfg/2014/123526/TFG_oscargutierrez.pdf

Leyes desde 1992 - Vigencia expresa y control de constitucionalidad {En línea}. {Consultado el 24 de octubre de 2017} Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1480_2011.html

MORENO Bolívar. Indicadores de gestión de un sistema de quejas y reclamos de una entidad bancaria. 2009. En línea}. {Consultado el 5 de agosto de 2017}. Disponible en: http://www.bdigital.unal.edu.co/897/1/21788943_2009.pdf

MOYA R., Raúl. Delitos informáticos: Estudio concreto sobre Fraudes y Phishing. Escuela Politécnica Superior de Jaéan. 2013

Normas ISO27000.es - El portal de ISO 27001 en español. {En línea}. {Consultado el 24 de agosto de 2017} Disponible en: http://www.iso27000.es/iso27000.html

OOCITIES. Parte II: Soporte conceptual. {En línea}. {Consultado el 2 de agosto de 2017} Disponible en: http://www.oocities.org/es/aryelitvelardes/Aryelit/parteii.htm

Ojo con este virus informático, tal vez ha sido víctima del troyano Remtasu.

{En línea}. {Consultado el 30 de octubre de 2017} Disponible en: https://noticias.caracoltv.com/colombia/ojo-con-este-virus-informatico-tal-vez-hasido-victima-del-troyano-remtasu

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. Tendencias de seguridad Cibernética en América Latina y el Caribe. Symantec, 2014. {En línea}. {Consultado el 2 de agosto de 2017} Disponible en: https://www.sites.oas.org/cyber/Documents/2014%20%20Tendencias%20de%20Seguridad%20Cibern%C3%A9tica%20en%20Am%C3%A9rica%20Latina%20y%20el%20Caribe.pdf

¿Qué nos espera en términos de seguridad digital para el 2017? {En línea}. {Consultado el 20 de octubre de 2017} Disponible en: http://blogs.eltiempo.com/seguridad-digital/2017/01/25/que-nos-espera-en-terminos-de-seguridad-digital-para-el-2017/

Secretaria Distrital de Ambiente de Bogotá. 2017. Portal {En línea}. {Consultado el 20 de agosto de 2017} Disponible en: http://www.secretariadeambiente.gov.co

Secretaria de Planeación. Portal. {En línea}. {Consultado el 24 de agosto de 2017} Disponible en: http://www.sdp.gov.co/portal/page/portal/PortalSDP/InformacionTomaDecisiones

SWEEZY, M. Paul Leo. HABERMAS: Paul A. Baran, Collective Portrait. Press.Digitalizado. Universidad California - 2008. 1965.

Utilizan una web del gobierno polaco para propagar malware orientado al Sector Bancario. {En línea}. {Consultado el 24 de octubre de 2017} Disponible en: https://blogs.protegerse.com/2017/02/07/utilizan-una-web-del-gobierno-polaco-para-propagar-malware-orientado-al-sector-bancario/

RESUMEN ANALITICO ESPECIALIZADO-RAE

Tema:	Monografía- Seguridad Informática
Titulo	Es seguro el uso del Software en el intercambio de Información Bancaria
Autor	Gloria Elizabeth Rodríguez Robayo
Fuente Bibliográfica	Se referencian 24 fuentes bibliográficas, algunas están relacionadas con la temática a tratar Comercio Electrónico. {En línea}. {Consultado el 7 de diciembre de 2017} Disponible en: https://es.slideshare.net/comerciop/comercio-electronico-3618401 Concepto 2013008465-008 del 8 de julio de 2013 de La Superintendencia Financiera. {En línea}. {Consultado el 30 de septiembre de 2017} Disponible en: www.superfinanciera.gov.co/SFCant/Normativa/PrincipalesPublicaciones/bol etinboletin4613/Proteccion%20Consumidor.html
Año	2018
Resumen	Se presenta una imagen de proceso de evolución tecnológica, cuando se conocen fenómenos del sistema informático entre otros los bancarios; manejo, operación, de información con bases informáticas en uso de Software y Hardware en los diferentes dispositivos al que se tiene acceso; son susceptibles de ser expuestas a distintas manos, a errores de usuarios y técnicos frecuentes a los estados activos de inseguridad de una información almacenada en un sistema informático, este permite ser copiada de forma exacta e indistinguible del original, y no siempre se respete la coherencia del sistema, es utilizado para cometer fraudes, es aquí cuando se presenta la inseguridad informática y se crea un delito en el reflejo del hacer uso de la web y un banco, en transacciones bancarias de retiro y se es susceptible a engaño, violación de los mecanismos de protección tanto patrimoniales del autor como otras defraudaciones y otras amenazas que pueden proceder de programas dañinos que son instalados en la computadora del usuario. Es esencial saber que recursos se requieren para controlar ese acceso y protección Estatal del Estado Social de derecho en cuanto a regulación y protección a los derechos de los usuarios de un sistema informático.
Palabras Claves	Estaciones de red, malvare, phishing, servidor, spyware
Contenidos	Planteamiento del problema Descripción del problema Formulación del problema

RESUMEN ANALITICO ESPECIALIZADO-RAE

	Objetivos; General y específicos Justificación Alcance y delimitación del problema Alcance Delimitación del problema Metodología Muestra Población Entrevista estructurada Encuesta Fuentes secundarias Marco referencial Marco conceptual Marco teórico Marco contextual Marco legal Resultados Recomendaciones Conclusiones

2. Descripción del problema de Investigación

La evolución tecnológica aplicada a los Sistemas informáticos crece y se desarrolla de forma continua, en donde los bancos son líderes en la implementación de software bancario con el objeto de facilitar la gestión de movimientos para sus clientes y de esta manera enfrentar con nuevos servicios a un mercado de alta competencia, en el cual el uso e implementación de nuevos sistemas informáticos o software bancarios no se excluyen del Derecho.

El manejo y operación de información con bases informáticas, en uso de Software y hardware a través de los diferentes dispositivos a los que hoy se tiene acceso; presentan alto riesgo, pues dicha información se encuentra expuesta a pasar por un número indeterminado de personas, lo que implica la posibilidad latente de que surjan errores técnicos y generar inseguridad en el uso de la información almacenada en el Sistema Informático. Entre otros aspectos porque esta información puede ser copiada de forma exacta e indistinguible del original, y no siempre se respeta la coherencia del sistema. Situación que posibilita los fraudes y la problemática de una Inseguridad Informática. Cuando se accede al conocimiento del sistema o se cuenta con acceso al mismo permitiendo la intervención en la información, establecer modificaciones y transformar el estado original, en ocasiones de forma indistinguible, lo que constituye un delito.

3. Objetivos

RESUMEN ANALITICO ESPECIALIZADO-RAE

General

Determinar los principales elementos que afectan la seguridad del software bancario implementado a través del uso de internet para transacciones e intercambio de información entre la entidad y sus cuentas habientes en la ciudad de Bogotá.

Específicos

- Evaluar el impacto de los delitos informáticos bancarios y la aplicación de la Ley 1480 de 2011.
- Identificar los avances tecnológicos que se han convertido en nuevas amenazas para la seguridad informática a nivel mundial.
- Describir los controles de los bancos y los mecanismos de protección para los usuarios de la banca electrónica
- Realizar un informe sobre los reportes de vulnerabilidad informática que se presentan para transacciones bancarias

4. Metodología
Este proyecto de investigación lleva a cabo un método inductivo, proceso de razonamiento y análisis de la revisión jurídica, observando los hechos que manifiesten el objeto del problema, se emplea el carácter descriptivo, encaminado a determinar en Colombia como se ha reglamentado el uso del software para transacciones bancarias, para lo cual se utilizará un análisis cualitativo. En correspondencia con el objetivo, el tipo es descriptivo analítico logrando así una triangulación metodológica de la investigación, así mismo, se revisará el material al cual se tenga acceso y que contenga información sobre las situaciones encontradas en los diferentes aplicativos de software bancario, de tal forma que permita realizar una diferenciación entre la utilización que aporta al bienestar del usuario y la manipulación de extraños de esta información, suplantando datos. Se utilizará un análisis de derecho comparado netamente documental e información jurídica, para observar una muestra de la legislación, referentes a la vigilancia del software informático bancario y del usuario para encontrar la forma adecuada de seguridad informática que ayudará a inferir el modelo que seguirá Colombia.

5. Referentes teóricos
Se presenta en este proyecto, el modelo que podría contribuir al desarrollo del

sistema bancario, el cual debe estar a la vanguardia de los procesos de cambio donde disponer de información continua, confiable y en tiempo, se reconoce como seguridad informática.

6. Referentes conceptuales
Se reseña diferentes conocimientos que permiten un adecuado análisis para el desarrollo de este trabajo en el dinamismo de la tecnología y que se entiende por seguridad informática empleada en operaciones bancarias.

7. Resultados
Los principales elementos que afectan la seguridad del software bancario implementado a través del uso de internet para transacciones e intercambio de información entre la entidad y sus cuentas habientes en la ciudad de Bogotá.

8. Conclusiones
El impacto de los delitos informáticos bancarios va en aumento, y los avances tecnológicos permiten que exista un mayor riesgo al usar el sistema en el intercambio de información, los bancos deben adaptar medidas de seguridad para tener un mejor manejo de la confidencialidad de los datos de sus clientes y asegurar que sus transacciones se realicen apropiadamente en Internet. También deben, brindar seguridad al cliente que tienen un buen control y seguridad necesarios para infundir confianza entre los usuarios. Los avances tecnológicos permiten que el sector financiero sea el que más use, las tecnologías, a nivel mundial, en la banca por Internet. Para esta plataforma se ofrecen una cantidad de productos y/o servicios bancarios a los clientes: tanto a personas naturales o jurídicas, el cual permite una mayor rapidez en el proceso de servicios. El incremento de usuarios de la banca virtual por medios de las Apps en sus celulares va en aumento. El uso de tecnologías ofrece servicios online, en todos los sectores de la economía. los cuales manejan unas ventajas competitivas que benefician al cliente. .