Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-27

DIAGNÓSTICO ACTUAL DEL CIBERDELITO CONTRA USUARIOS DE BANCA EN LÍNEA EN EL SECTOR BANCARIO COLOMBIANO

Jairo Alejandro Rincon Castañeda

Jorge Alberto Chavarría Martínez

Viviana Garcia Garcia

Ingeniería de Sistemas

Director: Gabriel Taborda

INSTITUTO TECNOLÓGICO METROPOLITANO

30 de octubre de 2015

RESUMEN

El presente trabajo tiene como objeto presentar una aproximación a las cifras de fraude electrónico a usuarios de banca en línea en Medellín, sus tipologías, los hábitos de seguridad que los usuarios practican para poder, posteriormente, presentar un plan de recomendaciones de seguridad informática a estos usuarios.

La información se recolectó mediante una encuesta dirigida a usuarios de banca en línea, residentes en Medellín, desarrollada mediante la herramienta Formularios de Google Drive, la cual obtuvo un total de 266 encuestados. Las estadísticas se obtuvieron mediante tabulación, tablas dinámicas y gráficas realizadas en Microsoft Office Excel 2013.

Se encontró un alto índice de fraudes e intentos de éstos, (23% de los encuestados ha sido víctima, mientras que el 42% afirma que le han intentado hacer un fraude electrónico); además que la mayoría se hacían a través de correos electrónicos y accediendo a páginas web fraudulentas (Phishing), con más del 50% entre fraudes exitosos e intentos de éstos. Se observó igualmente que, la mayoría de usuarios de móviles y tablets no utilizan ni antivirus ni herramientas de seguridad informática, (sólo el 54% afirma hacerlo siempre o frecuentemente) lo cual facilita el obrar delictivo. La mayoría de las personas que pudieron evitar un fraude, fue porque ellos mismos sospecharon de la plataforma (64%), lo que quiere decir, que poseen un nivel básico de conocimiento de herramientas informáticas. Y sólo algunos se preocupan por acceder a estas web digitando la dirección, (40%). Se concluye que existe poca cultura y educación sobre los riesgos y medidas de seguridad que se deben adoptar para usar los bancos virtualmente. Tampoco existe una cultura de denuncia de este tipo de fraudes.

*Palabras clave***:** ciberdelito, delitos informáticos, sistemas financieros, banca en línea.

RECONOCIMIENTOS

Agradecemos a todas nuestras familias por el acompañamiento y apoyo incondicional para poder cumplir con nuestro sueño de ser profesionales en Ingeniería de Sistemas. Además, agradecemos al Docente Gabriel Taborda, por hacer posible este trabajo de grado y en general, a todos nuestros profesores en el ITM. Así mismo, queremos agradecer al grupo de investigación de Seguridad de los Sistemas de Información (SISSI) por hacer parte de este informe.

ACRÓNIMOS

ADPIC Acuerdo sobre los aspectos de los derechos de propiedad intelectual.

APT Amenazas Avanzadas Persistentes

BotNet o Bot Ataque que reparte la carga en varios computadores; generalmente mediante IRC. Actualmente se está implementando a través de Http lo que significa que es mucho más sencillo el manejo.

DDoS: ataque distribuido de denegación de servicios (Distributed Denial-of-Service).

CCIT Cámara Colombiana de Informática y Telecomunicaciones.

COMPUTADORES ZOMBIES: computadores de personas particulares que son utilizados por un tercero para realizar acciones malintencionadas sin que el propietario se percate.

CONPES Coordinación Nacional para la Planeación de la Educación Superior.

DNNS Denegación de servicio de nombres de domino.

HTTP Protocolo de Transferencia de Hipertexto.

IRC Internet Relay Chat

TI o TIC tecnologías de la información y la comunicación.

TABLA DE CONTENIDO

LISTA DE GRÁFICAS

LISTA DE TABLAS

INTRODUCCIÓN

Debido a la alta incidencia de delitos electrónicos en el sector financiero en Colombia, se hace necesario realizar una aproximación a la situación actual del tema, con el fin de alertar a la comunidad académica interesada, a las entidades bancarias y a las autoridades para que se implementen medidas de prevención y solución de los diferentes tipos de ataques que se presentan frecuentemente en el país; ya que estos crímenes, en Colombia, son cada vez más frecuentes, siendo el sector financiero uno de los preferidos por este tipo de delincuentes y es la sociedad civil usuaria de banca en línea la más afectada.

Por lo anterior, el objetivo general de este proyecto es diagnosticar el estado actual del ciberdelito contra usuarios de banca en línea en el sector bancario colombiano, el cual se propuso lograr mediante los siguientes objetivos específicos:

- Identificar la incidencia de cibercrímenes y tipologías más usadas contra usuarios de banca en línea.
- Reconocer los hábitos de seguridad adoptados por los usuarios de banca en línea.
- Comparar los resultados de las encuestas con los estudios publicados sobre el tema en Colombia.
- Proponer estrategias de prevención para el usuario, las entidades bancarias y las autoridades que sirvan para mitigar el riesgo de estos delitos.

En el presente documento se encontrará el desarrollo y resultados de esta investigación; inicialmente, se encuentra el Marco Teórico, donde el lector encontrará información que lo contextualizará sobre qué son los delitos informáticos, sus principales clasificaciones, los tipos de victimarios que existen y una breve reseña de cifras y datos del

comportamiento de estos delitos en Colombia. A continuación se encuentra la Metodología donde encontrará la información necesaria para comprender detalladamente cómo se realizó el proyecto, cuál es su confiabilidad y sus limitaciones; posteriormente, se presentan las tablas estadísticas de los resultados de las encuestas con su respectivo análisis y comparación con resultados previos realizados por otros autores, seguido por las estrategias de prevención sobre fraude electrónico bancario desde el punto de vista teórico presentadas a usuarios de banca en línea, entidades bancarias y autoridades. Finalmente, se encontrarán las conclusiones más relevantes identificadas en los resultados, recomendaciones y propuestas para futuros trabajos.

1. MARCO TEÓRICO

1.1.Delitos informáticos o ciberdelitos

Los delitos informáticos, también conocidos como ciberdelitos o criminalidad informática, hacen referencia a toda actividad, o conjunto de actividades, que es considerada antijurídica y que se ejecuta utilizando cualquier medio informático o que tiene como objetivo dañar algún tipo de sistema informático, ya sea ordenadores, redes de internet, medios o dispositivos electrónicos, (Cuervo, 2008). Según el autor, el cibercrimen puede clasificarse en dos grandes categorías: una instrumental y la otra de objetivo o fin. Respectivamente:

1. La informática es el medio por el cual se realiza el delito. (instrumental)
2. La acción del cibercrimen tiene por objeto hacer daños, generar pérdidas, o impedir el uso de sistemas informáticos. (de objetivo)

La primera de estas categorías, incluye delitos como sabotaje informático, piratería informática, hackeo, crackeo y DNNS (Denegación de Servicio de Nombres de Domino). Mientras que en la segunda categoría se encuentran delitos como falsificación de documento electrónico, cajeros automáticos y tarjetas de crédito, robo de identidad, phreaking, fraudes electrónicos y pornografía infantil, (Cuervo, 2008).

Según Salellas (2013), los delitos informáticos son todas aquellas conductas ilícitas que se hacen por medio de cualquier medio informático. Dichas conductas se han caracterizado en las figuras típicas de delito, por lo que pueden ser sancionadas por el derecho penal. Sin embargo, con la rápida evolución de los sistemas informáticos y la aparición de nuevas herramientas tecnológicas, es necesario que el estado regule las conductas delictivas de forma específica para garantizar el uso adecuado y seguro de tales herramientas.

1.2. Historia de los delitos informáticos

De acuerdo con Guzmán (2009) junto con las innovaciones y la masificación de las TIC, la guerra, violencia y delincuencia también se ha transformado, pues estos medios han facilitado el acceso a varios tipos de información y concuerda con que, los primeros delitos de este tipo se dieron a inicios de la década de los noventa cuando el internet y la computación llegaron al alcance de los hogares y empresas.

Tal es el caso de Latinoamérica, según lo indica Prandini (2011), donde se ha crecido tecnológicamente a la par de otras regiones más desarrolladas y paralelamente ha crecido la necesidad de implementar sistemas de seguridad de la información.

Por su parte, Temperini (s.f.) asegura que este tipo de delitos son los de mayor crecimiento en los últimos años a través de todo el mundo y con una proyección anual cada vez mayor. Según el mismo autor, este tipo de delitos crecen debido al fácil acceso a las herramientas tecnológicas que tienen las empresas privadas y públicas, los usuarios y por supuesto los delincuentes. Para los últimos, su actuar delictivo se facilita principalmente porque no hay suficiente información sobre prácticas de seguridad informática, no hay suficientes políticas públicas y programas de seguridad eficientes y además por el persistente mercado negro de información. Según el autor, uno de los delitos informáticos más comunes es el robo de información personal o empresarial para ser usada con fines de lucro.

Según Guzmán (2009), también se hace cada vez más frecuente el daño de información, el robo de datos, fraudes electrónicos al sistema financiero y a la seguridad de los estados, así como el robo de información de bases tributarias y expedientes.

1.3. Tipos de delitos informáticos

Los delitos informáticos abarcan una gran variedad de clasificaciones, según el tipo de ataque utilizado, el objetivo, el criminal, la víctima y el daño que genera.

Según Pecoy (2012), pueden clasificarse de la siguiente manera:

1.3.1. Sabotaje informático:

El delincuente o autor pretende destruir el centro de cómputo, es decir, las máquinas, software o la información que éstos poseen. Es una de las tipologías más comunes y graves de los crímenes informáticos.

1.3.2. Piratería informática:

Es la violación ilegal de derechos de autor; es decir, toda mercancía o comercio que afecta el derecho de autor, según lo describe el ADPIC, citado por el autor.

La piratería, generalmente, se presenta de dos formas: a través del robo temporal de la máquina, es decir, acceso a un dispositivo de cómputo sin autorización en un tiempo definido, con el fin de sabotear información o sacar provecho personal de ello; la segunda modalidad es, la apropiación o hurto de software y/o datos, a través del acceso al dispositivo de un tercero.

1.3.3. Cajeros automáticos y tarjetas de crédito:

Toda actividad que permite extrae dinero de cajeros automáticos, a través de tarjetas magnéticas robadas o información personal de acceso a una cuenta bancaria con fondos.

1.3.4. Robo de identidad:

Es el delito que se da después de que el criminal obtiene información de datos personales ajenos y la usa para su propio beneficio, se puede incurrir en el delito de estafa y en el caso que, el criminal haya obtenido la información por el empleo que ejerce, se viola entonces el secreto profesional.

1.3.5. Phreaking:

Es la tipología más antigua de ciberdelitos, es la acción de acceder al sistema de telecomunicaciones para realizar llamadas telefónicas a larga distancia utilizando una cuenta ajena. Se afirma que es una forma primitiva del hacking.

Por su parte, Acurio del P. (s.f.) los clasifica en dos tipos principales de delitos: delincuencia informática y abuso informático: quien según Gómez, citado por el autor, lo define como: "conjunto de comportamientos dignos de amonestación penal que tienen por objeto a los sistemas o elementos de técnica informática o que están en relación significativa con ésta, pudiendo presentar múltiples formas de lesión de variados bienes jurídicos", (p. 9); y criminalidad informática, definida por Baón, citado por el autor, que lo define así: "la realización de un tipo de actividades que, reuniendo los requisitos que delimitan el concepto de delito, sean llevadas a cabo utilizando un elemento informático o vulnerando los derechos del titular de un elemento informático ya sea hardware o software, (p. 10).

1.3.6. Ataques DDoS y/o denegación del servicio

Los ataques DDoS (Ataque Distribuido de Denegación de Servicios) son de los más usados en los últimos años. Se les denomina ataque por consistir en una ofensiva dirigida en contra de un sitio web; el fraude puede activarse desde un clic que actualice la página, hasta un sofisticado software que automatiza el envío de paquetes de red hacia el enemigo, (Lazalde, 2013).

Además, según el autor, se convierte en una denegación de servicio; pues, como consecuencia del ataque, el sitio web deja de conceder sus servicios de forma normal; esto puede generar entonces pérdidas millonarias. La duración del ataque puede ir de algunos minutos a varias semanas, según la pericia de los administradores del sitio web para detenerlo. Otra característica de este tipo de ataques es que son distribuidos; pues hay una multitud de atacantes repartidos por toda la red, donde la suma de fuerzas puede colapsar el acceso al sitio web del enemigo en turno. Este tipo de ataques suelen ser por causas políticas, (Koike, 2015).

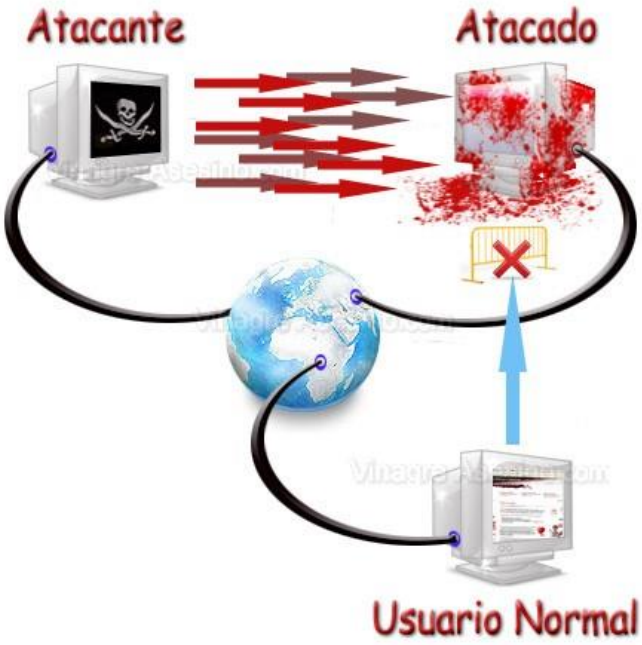
Por su parte, los ataques de denegación de servicio se dan cuando se satura la máquina que está prestando un servicio, para que ésta no pueda seguirlo prestando.

Las dos formas más comunes de saturar una máquina son:

• Generar un alto número de falsos requerimientos de servicio para que la máquina no tenga recursos suficientes para atender los verdaderos requerimientos de servicio.

• Generar peticiones con paquetes mal formados que generen fallas en el protocolo y este se bloquee o se reinicie para recuperar su funcionalidad.

Gráfica I. Ataques de denegación del servicio



Fuente: (Pando, 2008).

Como se muestra en la gráfica anterior, en los ataques de denegación de servicio, el objetivo principal es imposibilitar el ingreso y/o acceso a los recursos y servicios de la compañía a lo largo de un tiempo indefinido, estos ataques están redirigidos normalmente a los servidores que administran las plataformas para que con ello no se pueda acceder.

1.3.7. Amenazas Avanzadas Persistentes

Este tipo de amenazas, suelen considerarse más dañinas que otros tipos de ataques; pues, son capaces de perdurar en el tiempo en una máquina infectada, pasan desapercibidas ya que pueden realizar ataques a través de vulnerabilidades poco conocidas y generalmente se dirigen a un objetivo muy específico; por ejemplo, suelen ser espionajes a organizaciones, gobiernos y objetivos militares, (INTECO, s.f.).

Este tipo de delito se caracteriza por ser prolongado y el delincuente debe de ser paciente y poseer una meta específica; éste, generalmente, utiliza técnicas de ingeniería social, (persuasión o engaño) para poder infectar algún dispositivo; posteriormente, el delincuente procede a realizar varias acciones, como son el acceso a información, activación de cámara, lectura de los comandos del teclado, entre otros. Generalmente, una vez infectado un equipo, se procede a infectar otros intercomunicados.

Se le denomina **amenaza** sólo aquellos ataques que persiguen un objetivo importante; **persistente** cuando se hace un estudio previo al ataque, mas no si el ataque es duradero en el tiempo; y **avanzada** se le denomina cuando el tipo de ataque es innovador y específico para su objetivo.

Tal como lo afirma García (s.f.), en la literatura, se pueden encontrar tres clases principales de delitos según su forma de operación a través de los tiempos:

1.3.8. Primera generación: ataques físicos

Encontramos aquí ataques que se centran en componentes electrónicos, como podrían ser los propios ordenadores, los cables o los dispositivos de red. El objetivo de los protocolos distribuidos y de la redundancia es la tolerancia frente a un punto único de fallo. Actualmente se conocen soluciones para estos ataques, utilizando protocolos distribuidos y de redundancia para conseguir una tolerancia a fallos aceptable.

1.3.9. Segunda generación: ataques sintácticos

Se trata de ataques contra la lógica operativa de los ordenadores y las redes, que quieren explotar vulnerabilidades existentes en el software, algoritmos de cifrado y en protocolos, así como permitir la denegación del servicio prestado. Aunque no existen soluciones globales para contrarrestar de forma eficiente estos ataques, podemos encontrar soluciones cada vez más eficaces.

1.3.10. Tercera generación: ataques semánticos

Finalmente, podemos hablar de aquellos ataques que se aprovechan de la confianza de los usuarios en la información. Este tipo de ataques pueden ir desde información falsa en boletines informativos y correos electrónicos hasta la modificación del contenido de los datos en servicios de confianza, como, por ejemplo, la manipulación de bases de datos con información pública, sistemas de información bursátil, sistemas de control de tráfico aéreo, etc.

Se basan en la manera en que los humanos asocian significado a un contenido. El inicio de este tipo de ataques surgió con la colocación de información falsa en boletines informativos o e-mails, por ejemplo, para beneficiarse de las inversiones dentro de la bolsa financiera. También pueden llevarse a cabo modificando información caduca.

Esta generación de ataques se lleva a su extremo si se modifica el contenido de los datos de los programas de ordenador, que son incapaces de cotejar o sospechar de su veracidad. Su solución pasará no sólo por el análisis matemático y técnico, sino también por el humano.

1.4. Tipos de victimarios informáticos

Acurio del P. (s.f.) identifica dos actores principales en el delito:

1.4.1. Sujeto activo:

Es quien ejecuta el delito haciendo uso de una herramienta o instrumento informático.

1.4.2. Sujeto pasivo:

Sujeto sobre quien recae el delito, generalmente es el titular del elemento informático utilizado para delinquir por lo cual, se considera victimario, en caso de desconocer el hecho, se convierte igualmente en víctima y en ocasiones, es la víctima final.

1.5. Delitos informáticos en el sector bancario en Colombia

En una publicación realizada en Colombia INN, por Dueñas (2015), se afirma que cualquier persona o dispositivo informático es vulnerable a los delincuentes y que éstos buscan cualquier tipo de información para revenderla en el mercado negro como pueden ser hasta historiales médicos para cobrar dinero para devolverlos, (extorsión), también roban datos de clientes para vender en cadenas minoristas, sin embargo, para la información de gobiernos no existen todavía clientes. Se afirma igualmente que la población civil es la más afectada.

Aunque se reconocen esfuerzos y preocupaciones por parte del gobierno y las empresas, aún queda mucho por corregir y perfeccionar para minimizar este tipo de actos delictivos y según lo expresa David Agudelo, Director de la unidad virtual de la Universidad Católica de Manizales, para Caracol Radio (2012), hacen falta políticas públicas claras y eficientes y además, que los bancos no publican la información de este tipo de actividades delictivas para no afectar su buen nombre y que no basta con fiarse de un antivirus y un anti-spam. En concordancia con lo anterior, Héctor Tamayo coordinador de tecnología del CCIT (Cámara Colombiana de Informática y Telecomunicaciones), durante una entrevista realizada por Santa María (s.f.) para Topcomm, aseguró que en Colombia no hay ninguna

ley que obligue a las corporaciones a hacer públicos los hechos de pérdida de información, por lo que es difícil saber el verdadero impacto de estos delitos.

En la misma entrevista también se habla del mercado negro de información que existe en Colombia, de casos de extorsión para devolverla y se asegura que, los correos electrónicos son los principales medios utilizados para llegar a la víctima, siendo las víctimas preferidas los usuarios de banca en línea.

Como lo evidencia Guzmán (2009), los delitos electrónicos han adquirido un carácter transnacional, por lo cual, ha generado cambios en las regulaciones jurídicas de los países; y según lo indica Acurio del P (s.f.), en el contexto legal, estos delitos han tenido una amplia confusión, debido a la variedad de tipos de crímenes y de bienes jurídicos afectados.

El carácter transnacional se evidencia en un ejemplo citado en un documento CONPES (2011), donde para el caso de afectación colombiano, el primer evento importante ocurrió en el año 2010, desde España, a través de un ataque dirigido a 190 países mediante "computadores zombis" con "BotNet Mariposa". Colombia ocupó el puesto número 5 de los países más afectados, con un 4.94% de afectación.

Guzmán (2009) evidencia igualmente que, en Colombia, desde la aparición de este tipo de medios de información se han implementado algunas medidas por parte del gobierno y que aún existen unas limitaciones debido a la falta de conocimiento para actuar, ya que debe implementar acciones de control y a su vez, respetar el acceso a la información y los derechos fundamentales; así mismo, Mazón y Pereira (s.f.) afirman que, llevar a cabo la legislación es un tema complicado debido a la falta de claridad de términos específicos de los bienes jurídicos, de las leyes que se violan a través de estos delitos y de la culpabilidad que tiene un titular de un dispositivo informático.

Sin embargo, la medida tomada más recientemente es la Ley 1273 de 2009, la cual genera un nuevo bien jurídico denominado "de la protección de la información y de los datos" (Temperini, s.f.) Por la cual se reglamentan: atentados contra la confidencialidad, integridad y disponibilidad de datos y de sistemas informáticos, y atentados informáticos y otros. Ley

que modificó el Código Penal y genera penas económicas y jurídicas para los siguientes actos: acceso abusivo a un sistema informático, obstaculización ilegítima del sistema informático o red de telecomunicación, interceptación de datos informáticos, daño informático, uso de software malicioso, violación de datos personales, hurto por medios informáticos y transferencia no consentida de activos. (Ley 1273, 2009).

Temperini (s.f.) afirma que, dicha normativa busca preservar integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones. A través de esta incorporación, el capítulo I de la Ley 1273 de 2009, titulado "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos", a partir del cual regula una serie de artículos penales que van desde el artículo 269A hasta el artículo 269J. Adicionalmente se incorpora el artículo 58, considerando como agravante general "si la realización de alguna de las conductas punibles, se realicen utilizando medios informáticos, electrónicos o telemáticos", tal como lo indican las leyes 1273 de 2009 y Ley 1366 de 2009.

Así mismo, Guzmán (2009) identifica las principales limitantes de esta Ley: la falta de conocimiento entre lo legal o ilegal por parte de los usuarios de medios informáticos y la falta de información y datos de los nuevos bienes tutelados.

Según el estudio comparativo de las regulaciones para este tipo de delitos en Latinoamérica realizado por Temperini (s.f.), Colombia posee un 75% de nivel de sanción penal de delitos informáticos, lo cual lo posiciona como el séptimo país del subcontinente. El abuso de los dispositivos y la falsedad informática no fueron encontrados en la legislación de Colombia y son los delitos menos reglamentados en América Latina. Igualmente, el autor asegura que, por el carácter transnacional, este tipo de delitos debería ser reglamentado en coherencia con los demás países de la región y del mundo, sin embargo, no existe armonización legal de estos delitos en el continente.

Es imposible conocer la verdadera magnitud de los delitos informáticos debido a la falta de denuncias y falta de investigación de autoridades responsables. Igualmente, en Colombia, faltan leyes de protección a víctimas y es escasa la preparación de las autoridades

para comprender, investigar y aplicar el tratamiento jurídico adecuado, lo cual lleva a los escasos estudios realizados a una "cifra oculta" o "cifra negra" ya que las empresas no denuncian este tipo de ataques para no perder prestigio. (Acurio del P., s.f.) Y para el sector bancario, este tipo de cifras publicadas, significa una amenaza debido a que este sector se soporta en la confianza, tal como lo afirma Fortinet, en la publicación de Colombia Digital (2015).

> Aun así, existen algunas cifras de diferentes entidades y organizaciones, donde, por ejemplo, un estudio realizado por Symantec en el año 2010, citado por Prandini (2011), se puede posicionar a Colombia en el cuarto puesto de América latina en cuanto a su vulnerabilidad de seguridad informática, siendo los ataques tipo Bot los de mayor representación. Igualmente, un estudio de ESET en el 2011, citado por la autora, se posiciona al país en el segundo puesto en tener computadores infectados con troyanos bancarios, y respecto a la generación de spam, el país ocupa el décimo puesto en el mundo y el segundo en el subcontinente según Symantec en el año 2010. El phishing en la región es existente aunque no muy frecuente, el más afectado es México y finalmente, se indica que, Colombia ocupaba en el año 2010, el puesto número 8 de América Latina y el 36 en el mundo en cantidad de computadores infectados por Bots. (Prandini, 2011).

Para el sector financiero los resultados no son diferentes: los ataques son cada vez más frecuentes, las modalidades cambian tan rápido como la tecnología, no existen estudios representativos por parte de las autoridades o las mismas entidades financieras, debido a la posible generación de paranoia que se puede dar en los consumidores financieros, tal como lo asegura Ricardo Villadiego, directos ejecutivo de Easy Solutions en una entrevista realizada por Dueñas (2015): "el fraude electrónico crece y cambia rápidamente y las precauciones permanecen estáticas. La ley sola no soluciona el problema. Las legislaciones tardan tiempo en aprobación y estudio, pero los ataques evolucionan rápidamente".

Así mismo lo indican Ojeda-Pérez et al. (2010) quienes aseguran que uno de los medios informáticos más vulnerados es el financiero; y que, si bien las entidades financieras

reconocen la importancia de la planificación de la seguridad informática, no son coherentes con las técnicas, herramientas y procedimientos aplicados y menos con la preparación del talento humano para garantizarla ni con la inversión destinada para ello. Afirman que la seguridad igualmente es un reto colectivo, y debe hacerse junto con la participación del estado y la ciudadanía. También lo afirma la Certicámara (2014), cuando afirma que, el sector financiero, el comercio electrónico y la tecnología es donde los delincuentes hacen más actos y son los sectores que más crecen anualmente. Afirma igualmente, que, se pierden anualmente aproximadamente 464 millones de dólares en el país por ciberataques y cobra 6 millones de víctimas por año.

Además, Villadiego afirma que, el Skimming, (manipulación de cajeros electrónicos) ha afectado a América Latina desde la década de los 90 y por eso se cambiaron las tarjetas de banda por chip, caso contrario a lo que sucede en Estados Unidos, donde ni siquiera se ha planteado la necesidad de implementar esta tecnología. (Dueñas, 2015). El mismo autor afirma que, en Colombia, los fraudes bancarios, la clonación de tarjetas y el robo de credenciales son las tipologías de crímenes más comunes y que estima que por cada $10.000 pesos del sistema bancario se pierden $20 pesos.

Según un informe generado por Colombia Digital (2015), los métodos más usados para robar en el sistema financiero son:

1.5.1. Phishing:

Se ha convertido en la modalidad más común. Se trata de la generación de páginas falsas que se envían generalmente por correo electrónico o a través del acceso a portales web, lo que facilita el robo de datos personales como nombres de usuarios, contraseñas, tarjetas y pin. Estas informaciones también se pueden obtener fraudulentamente a través del skimming para robar en cajeros y portales web.

Gráfica II. Ejemplo de página falsa

Fuente: (Aitor, 2015).

Como se evidencia en la Gráfica II, el ataque tipo phishing muestra páginas iguales o similares a la original; generalmente, se detectan porque no poseen firma o marca de seguridad en el enlace, tal como se muestra en la flecha de la imagen.

1.5.2. Skimming:

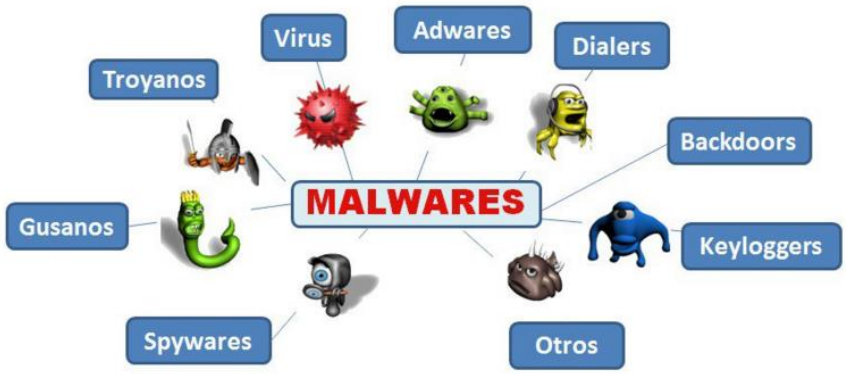
Se trata de elementos electrónicos que obtienen información de las bandas magnéticas de las tarjetas de crédito, débito y son capaces de captar contraseñas.

1.5.3. Malware:

Otra modalidad común de fraude financiero, el cual consiste en un software que se infiltra y afecta un sistema informático, troyano bancario, el cual busca información, hace transacciones, y genera accesos remotos.

Como se muestra en la siguiente gráfica, existen diversos tipos de Malware, los cuales se clasifican por su forma de funcionamiento o por su finalidad.

Gráfica III. Tipos de Malware



Fuente: (Taringa, 2013).

Sin embargo, la delincuencia va muchas más allá de estos tres métodos, pues, se sabe que existe un mercado negro de estos tipos de datos; los fraudes y robos inician con la obtención ilegítima de información a través de Phishing, hacking o malware y luego se vende a otras personas para que estas hagan los movimientos fraudulentos, espionaje industrial o APT; estas últimas se realizan a través de herramientas y procesos dirigidos a naciones y organizaciones, y los ataques puede durar meses y años en el mismo objetivo sin ser detectados.

Lo anterior está en concordancia con una publicación del diario El País, del 24 de diciembre del 2014, donde se informa una nueva modalidad de Phishing para realizar fraudes electrónicos y consiste en obtener datos a través de llamadas fraudulentas, (Phreaking) e informa igualmente que, los delincuentes, en menos de una hora pueden realizar varias extracciones de hasta $500.000.000 de una sola cuenta, dato proporcionado por un investigador del CTI para el diario.

1.6. Cifras e impacto del ciberdelito al sistema financiero colombiano

Respecto al impacto que generan estos delitos, se encuentran sólo algunos datos aislados; respecto a las denuncias, se encuentra que, en el año 2011, se reportaron 1000 denuncias para este tipo de delitos según un informe de Colombia Digital, presentado por Rodríguez (2012), siendo los de mayor frecuencia el acceso abusivo y hurto, interceptación, violación datos privados, transferencias no consentidas de activos, suplantación de sitios web, daño informático, matoneo y obstaculización ilegítima y para el sector bancario el más común fue la clonación de tarjetas, principalmente en las ciudades de: Bogotá Cúcuta, Cartagena, Medellín y Cali, por lo que se puede apreciar que no es un fenómeno aislado; así mismo, en el año 2012, se reportaron en promedio 187 denuncias mensuales por el delito de fraude electrónico, según afirma Caracol Radio (2012).

Así mismo, Serna (2011) afirma que, durante ese año, las denuncias aumentaron en un 30% respecto al año anterior, haciendo uso de la Ley 1273 de 2009 y se realizaron 87 capturas. También afirma que, la clonación de tarjetas fue el delito más frecuente, y se realiza en establecimientos comerciales, valiéndose de un Skimmer; esta modalidad se utiliza con frecuencia en las tarjetas débito. Sin embargo, aclara también que, con la implementación de chips y eliminación de bandas, el delito ha disminuido. El autor señala también que, según el defensor del consumidor financiero, se estima una pérdida para el sector financiero, entre el año 2007 al año 2011 de 20 mil millones de pesos a causa de estos delitos. Serna, (2011) también afirma que ni Asobancaria ni la Súper Intendencia Financiera de Colombia han realizados estudios o diagnósticos de este tipo de delitos informáticos, donde se hace urgente conocer las cifras de ocurrencia de clonación de tarjetas, robos de identidad, tráfico de bases de datos, entre otros.

América latina y Colombia han sido pioneras en modalidades de fraude electrónico, como sucedió durante el año 2014, donde un ex policía de la Dijín, quien trabajaba para el Banco BBVA, realizó un millonario robo que dejó 1.024 millones desaparecidos, los cuales

extrajo de los cajeros, a los cuales les instaló un software que podía robar la información, eliminar el rastro de la transacción y el límite de extracción. (Laverde, 2014). Así mismo, el ingeniero de Mc Afee, Juan Pablo Páez, afirma que durante un ataque masivo a dispositivos móviles, un grupo de delincuentes se robó 3.800 millones de pesos, en marzo del 2013. (Mayorga, 2014).

Una aproximación a la magnitud del problema en el país, se puede observar en un estudio realizado por KPMG, (2013) donde se asegura que 7 de 10 empresas en Colombia sufrieron un fraude en el año 2012. Así mismo, se habla de pérdidas que ascienden los 3.600 millones de dólares y que el 70% de los crímenes económicos han sido por los mimos empleados, de igual forma se señala que, el 51% de las pérdidas fue el fraude económico. (p. 10).

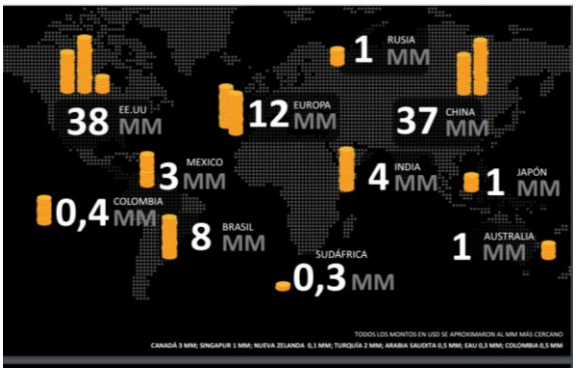
Se encontró que, el cibercrimen causó un daño económico aproximado de 550 millones de dólares en el año 2012 en Colombia. (p. 32) y que el 23% de estos crímenes se debe a la deslealtad de los empleados, mientras que el 20% a fallas de seguridad y 17% por el robo del dispositivo móvil, (p. 33).

Así pues, como se puede evidenciar, estos ataques están en constante aumento y transformación, genera grandes pérdidas económicas y afecta a casi todos los sectores productivos, a la Nación y a la sociedad civil, por lo que se hace necesario implementar mejores medidas de seguridad mientras la Ley empieza a actuar de manera más eficiente. Así como lo afirman Ernst & Young (2011), en la importancia de generar un sistema de seguridad integrado que sea predictivo, que ayude a identificar los riesgos reales: adelantarse a las amenazas. Proteger lo más importante: detectar y monitorear. Equilibrar los fundamentos: invertir en TI y hacer un buen uso de ellas; también afirman que el programa de seguridad debe ir más allá del cumplimiento y las innovaciones tecnológicas no deben ser prohibidas, sino por el contrario, deben aprovecharse para el beneficio de las compañías. Lo anterior está de acuerdo a la perspectiva generada por Websense (2008), quien dice que las compañías deben replantear sus sistemas de seguridad y enfocarlas a la información ya que esta es la clave de todo. Así mismo, debe integrar los canales de comunicación y las

aplicaciones por medio de las cuales recibe y envía información para minimizar los riesgos de fuga de datos.

Según un estudio realizado por Cisco (2008) las mayores pérdidas de información sensible de las empresas se dan por culpa de los mismos empleados de las compañías, porque no respetan las normas de seguridad (acceden a páginas indebidas, correos electrónicos personales desde dispositivos empresariales, comparten contraseñas, envían información empresarial a dispositivos personales, entre otros. Por lo cual, se afirma que en la cultura de seguridad empresarial, se deben enfocar en educar sobre este tipo de actividades que vulneran la información.

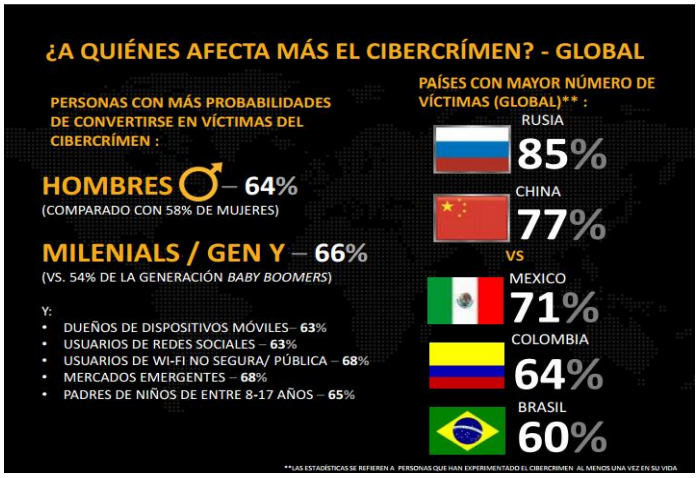
Gráfica VII. Costo mundial del cibercrimen al consumidor



Fuente: (Norton, 2013)

Como se aprecia en la imagen anterior, en cuanto a costo, el cibercrimen afecta principalmente a los habitantes de Estados Unidos, seguido por China y luego toda Europa; Colombia y Sudáfrica se encuentran en los últimos puestos, sin embargo, se evidencia que existe un alto costo por este tipo de delitos. Vale aclarar que, las cifras están expresadas en dólares americanos.

Gráfica VII. Países con mayor número de víctimas del cibercrimen



Fuente: (Norton, 2013).

En la imagen anterior se puede observar que Colombia ocupa el cuarto puesto en el mundo con mayor número de víctimas de cualquier tipo de ciberdelito con un 64%, comparado con Rusia quien es el primero con un 85%. México, Brasil y Colombia, 3 países americanos que están en la lista de los primeros 5 más afectados, lo cual es preocupante. Se aclara que los datos son del reporte proporcionado por Norton en el año 2013 y que las cifras se toman de individuos que han sido víctimas de ciberdelito al menos una vez.

Gráfica IX. Porcentaje de sanción legal contra ciberdelitos en Centro y Suramérica

perjuicio para un tercero. Algunos países como Argentina, exigen que el sistema o dato sea de acceso restringido. Otros como Chile, no lo mencionan. Colombia, expresa en su redacción que el sistema puede ser o no de acceso restringido. Costa Rica comienza afirmando que será delito si hay peligro para la intimidad o privacidad de un tercero. Y otra larga lista de características especiales, que como el lector podrá observar, un análisis técnico-jurídico riguroso sobre ellos es realmente interesante, pero cuya extensión excede los límites del presente trabajo. No obstante, dicho análisis será realizado a futuro.

Finalmente, una aclaración importante. No sería correcto considerar que los resultados expuestos en la Tabla N° 2 permitan concluir que técnicamente un país determinado se encuentra o no en cumplimiento de las disposiciones materiales en materia penal que dispone la Convención de Cibercriminalidad de Budapest. Dicha afirmación encuentra fundamento en que, las figuras penales consideradas, si bien han sido tomadas de la citada Convención, ello no implica que se ha hecho un análisis pormenorizado de todos los requisitos que se establecen en cada artículo material penal de la misma. Los delitos informáticos considerados para el estudio sólo han sido tomados a modo de referencia, sin contrastar los requisitos técnicos legales que la Convención exige para considerarlos como correctamente tipificados.

En el primer grupo, identificado desde un punto de vista cuantitativo, es posible concluir con la realización de un ranking de países de acuerdo al nivel de protección penal en relación a los delitos informáticos analizados (a través de la reorganización de los datos arrojados por la Tabla N° 4).

N°	País	%
1	Puerto Rico	100%
2	República Dominicana	100%
3	Venezuela	100%
4	Argentina	88%
5	Costa Rica	88%
6	Panamá	88%
7	Paraguay	88%
8	Colombia	75%
9	México	75%
10	Brasil	63%
11	Chile	63%
12	Ecuador	63%
13	El Salvador	63%
14	Perú	63%
15	Uruguay	63%
16	Bolivia	50%
17	Guatemala	50%
18	Honduras	50%
19	Cuba	0%
20	Haití	0%
21	Nicaragua	0%

Tabla Nro 5. Ranking de países con más sanción penal para los delitos informáticos considerados.

Por otro lado, esta vez a partir de la reorganización ascendente de los datos de la Tabla N° 3, es posible determinar un ranking de los delitos informáticos con

Fuente: (Temperini, s.f.).

Como se aprecia en la imagen anterior, Puerto Rico, República Dominicana y Venezuela son los únicos países de la región mencionada que cumplen a cabalidad con normatividad vigente en contra de ciberdelitos y protección de datos. Colombia, siendo una de las principales víctimas, ocupa el puesto número 8 de 21 con un cumplimiento del 75%, al igual que Brasil y México; por lo que estos países ocupan los puestos 8, 9 y 10 siendo muy similares. Por su parte, Nicaragua, Haití y Cuba tienen un nulo cumplimiento (0%). Estos datos se calcularon según las leyes y penalidades existentes de acuerdo a diferentes tipos de ataques y modalidades de cibercrímenes.

1.7. La banca en línea y la seguridad en Internet

1.7.1 Seguridad informática

Aunque existen muchas definiciones de seguridad, tal vez la más resumida y aceptada es "Característica que indica que un sistema está libre de todo peligro, daño o riesgo", (Mifsud, 2012). Por lo tanto, este concepto puede aplicarse a la seguridad informática, campo donde tiene especial énfasis la protección de la información como tal.

Según la autora, la seguridad informática es entonces un conjunto de medidas técnicas, organizativas y legales que permiten a una organización o persona asegurar la confidencialidad, integridad y disponibilidad de su sistema de información. Estos tres aspectos son la base de todo sistema de seguridad de información y deben ser controlados constantemente:

- **Confidencialidad:** hace referencia a mantener oculta o secreta determinada información, con el fin de protegerla para que no exista divulgación o autorizada de esto. Una de las técnicas más empleadas para asegurar la confidencialidad es la criptografía.

- **Integridad**: se refiere a una información correcta, veraz y fiable; es decir, que ésta no esté tergiversada o incompleta. Su objetivo es entonces evitar modificaciones no autorizadas a la información.

  Existen dos tipos de integridad:

  - ***Integridad de los datos:*** volumen y calidad de la información.
  - ***Integridad del origen:*** la fuente de información debe de ser veraz y fiable, (autenticación).

- **Disponibilidad:** hace referencia a que se puede o debe de disponer libremente de la información, o en su lugar, que está lista y puede usarse. Por lo tanto, la información debe permanecer disponible para los elementos o personas autorizadas. Es entonces su finalidad la de prevenir interrupciones no autorizadas o controladas de los recursos informáticos.

  Por lo anterior, puede resumirse entonces que, la seguridad informática consiste en mantener en equilibrio estos tres aspectos fundamentales; dependiendo del entorno, alguna de estas características es más importante que otras; para el caso que compete en este estudio, en la seguridad informática bancaria es primordial la integridad; pues es preferible que alguien pueda ver el saldo de otro antes de que pueda modificarlo.

El gran crecimiento del uso de compras en línea y banca en línea ha creado la necesidad de implementar nuevos y mejores sistemas de seguridad por parte de las compañías prestadoras de estos servicios; puesto que se ven en la obligación de proteger a los usuarios con el fin de prestar un servicio seguro y de alta calidad.

La confianza, según Isfahani y Mircholi (2013) es uno de los factores más importantes para las empresas financieras y los servicios de compra; esta variable o factor puede verse afectado (positiva o negativamente) por diversos motivos, entre los que se destacan: eficiencia, accesibilidad, privacidad, calidad de servicio, requerimientos para prestar el servicio. Sin embargo, como afirman los autores, en los países en vías de desarrollo, los bancos, en su afán por acaparar el mercado electrónico, no se han detenido lo suficiente a vigilar la privacidad y seguridad de los usuarios, por lo que genera bajos índices de satisfacción y confianza por parte de los usuarios.

Según Buch I Tarrats y Jordán (2011) la mayoría de transacciones bancarias se realizan sobre redes de conmutación de paquetes X.25; las cuales, se consideran seguras por estar controladas por operadores autorizados, pero no por presentar medidas de seguridad basadas en técnicas criptográficas, autentificación segura o integridad de la información.

El internet puede considerarse de protección blanda, pues, es una red pública donde la autenticación de usuario es un identificador y una clave secreta que sólo éste conoce (usuario y contraseña). Sin embargo, esta red posee problemas de autenticidad, integridad, confidencialidad y repudio, lo cual, afecta la seguridad de la banca en línea de las siguientes formas:

- **Robo de información:** mediante escuchas de red, permite obtener información del usuario como números de cuentas o de tarjetas de crédito, balances de cuentas o información de facturación.
- **Suplantación de identidad:** permite al atacante realizar operaciones en nombre de otro.
- **"Sniffers":** son herramientas informáticas que permiten la obtención la lectura de la información que se transmite por la red (claves de paso o información de operaciones).
- **Modificación de información:** permite alterar el contenido de ciertas transacciones como el pago, la cantidad o incluso la propia orden de compra.
- **Repudio:** el rechazo o negación de una operación por una de las partes puede causar problemas a los sistemas de pago. Si una parte rechaza un previo acuerdo con la respectiva, ésta deberá soportar unos costos adicionales de facturación.
- **Denegación del servicio:** un ataque de denegación de servicio inhabilita al sistema para que éste pueda operar en su normalidad, por lo tanto imposibilita a las partes la posibilidad de realización de operaciones transaccionales. Éstos son de extrema sencillez y la identificación del atacante puede llegar a ser imposible.

Explican los autores que, en los servicios de banca virtual, los usuarios realizan las operaciones bancarias de forma remota. El sistema se implanta sobre redes TCP/IP (Internet), WAP (comunicaciones móviles) o propietaria (por ejemplo, cajeros automáticos).

A continuación se presenta una tabla donde se sintetizan los tipos de ataques más comunes y la vulnerabilidad informática que representan.

ATAQUE	VULNERABILIDAD
Sabotaje informático	Integridad y disponibilidad de la información.
Piratería informática	Autenticidad y confidencialidad de la información.
Suplantación de identidad	Autenticidad y confidencialidad
Phreaking	Autenticidad, confidencialidad, integridad.
Ataques DDoS	Autenticidad, confidencialidad, integridad, no repudio, disponibilidad.
Amenazas avanzadas persistentes	Autenticidad, confidencialidad, integridad, no repudio, disponibilidad.

Fuente: elaboración propia.

Ya descritos los tipos de ataques y sus consecuencias, se procederá en este documento a profundizar en las medidas y sistemas de seguridad.

1.7.2 Protocolos e infraestructuras de seguridad

El sistema de banca virtual debidamente acreditado discrimina efectivamente la autentificación del usuario, respalda con pautas de seguridad la autorización de transacciones, en este sentido la plataforma electrónica está rigurosamente diseñada para el acceso a los servicios y posibilitar que los usuarios firmen digitalmente los datos (Buch I Tarrats y Jordán, 2011). En este sentido Jordi Buch i Tarrats y Francisco Jordán afirman que:

> Para la acreditación fuerte a través de internet, se recomienda el protocolo SSL (o TLS) de forma que el usuario que dispone de un certificado digital de operación bancaria pueda acreditarse al sistema, mientras que éste se acredita al usuario con su respectivo certificado de servidor. El mismo protocolo garantizará la confidencialidad e integridad de los datos. Si el usuario opera desde un teléfono móvil, se usará el protocolo WTLS. El sistema bancario virtual deberá guardar las órdenes de transacciones generadas por los usuarios, para los que éstos deberán firmarlas digitalmente con su clave de firma digital. Los estándares usados son el PKCS#7 definido por RSA y S/MIME si el sistema de basa en mensajería segura. (p. 39).

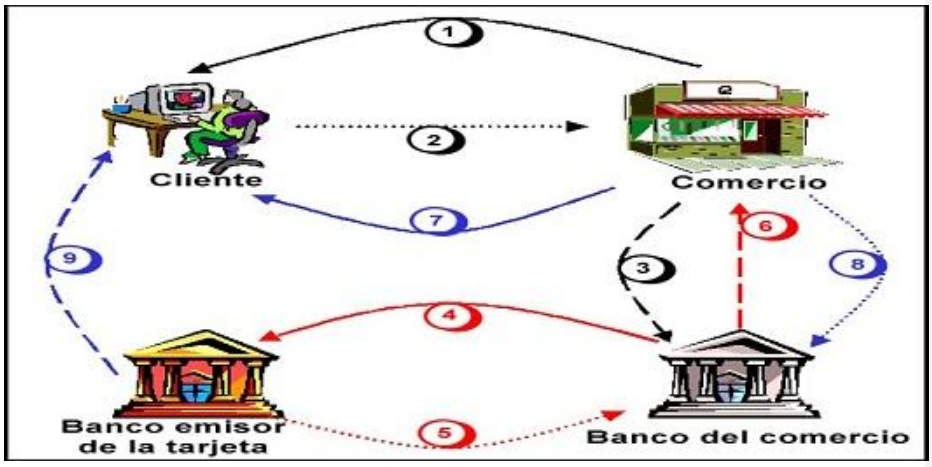
La autentificación consiste en que el usuario entrega al servidor un desafío-respuesta firmado digitalmente con su clave privada y el servidor verificará que el certificado se ha emitido por una Autoridad Reconocida y que éste no haya expirado ni revocado.

En el procedimiento de autorización de transacciones, el usuario devuelve la orden firmada digitalmente y el servidor, una vez validada mediante el mismo procedimiento anterior, la guardará para asegurar el no repudio de ésta. La orden de transferencia no se procesará hasta que se hayan realizado los pasos anteriores, como explican Buch I Tarrats y Jordán (2011).

1.7.2.1 Protocolo SET

SET (Secure Electronic Transaction) es un protocolo que emula de forma electrónica, mediante el uso de certificados y firmas digitales, el pago de bienes y/o servicios mediante tarjeta de crédito; sin embargo, posteriormente también se ha introducido el uso de tarjeta de débito con uso de PIN por Internet. Este sistema utiliza las últimas tecnologías de firma digital y certificación para llevar a cabo la protección de los datos a través de Internet. La seguridad de las transacciones bancarias en internet deben de ser identificadas previamente y proveerles de un certificado para que puedan funcionar dentro del sistema que generalmente son operadas por instituciones financieras capaces de emitir tarjetas (emisores) o instituciones asociadas, como bancos, que solicitan la emisión de tarjetas; los certificados de todas las entidades sólo son válidos para una marca determinada siendo imposible utilizarlo en otro, (Buch I Tarrats y Jordán, 2011).

Gráfica IV. Protocolo SET



Fuente: (InternetLab, 2013).

Como se aprecia en la imagen anterior, el funcionamiento del protocolo SET consta de 9 etapas:

1. Arranque de la cartera: el servidor del comerciante envía una descripción del pedido que activa la aplicación cartera del cliente.

2. Transmisión cifrada de la orden de pago: el cliente comprueba el pedido y transmite una orden de pago de vuelta al comerciante. La aplicación cartera crea dos mensajes que envía al comerciante. El primero, la información del pedido, contiene los datos del pedido, mientras que el segundo contiene las instrucciones de pago del cliente. En este momento, el software cartera del cliente genera un firma dual, que permite juntar en un solo mensaje la información del pedido y las instrucciones de pago, de manera que el comerciante puede acceder a la información del pedido, pero no a las instrucciones de pago, mientras que el banco puede acceder a las instrucciones de pago, pero no a la información del pedido. Este mecanismo reduce el riesgo de fraude y abuso, ya que ni el comerciante llega a conocer el número de tarjeta de crédito empleado por el comprador, ni el banco se entera de los hábitos de compra de su cliente.

3. Envío de la petición de pago al banco del comerciante: crea una petición de autorización que envía a la pasarela de pagos, incluyendo el importe a ser autorizado, el identificador de la transacción, todo ello convenientemente cifrado y firmado. Entonces se envían al banco adquiriente la petición de autorización junto con las instrucciones de pago.

4. Validación del cliente y del comerciante por el banco adquiriente: el banco del comerciante descifra y verifica la petición de autorización. Si el proceso tiene éxito, obtiene las instrucciones de pago del cliente, que verifica a su vez, para asegurarse de la identidad del titular de la tarjeta y de la integridad de los datos. Se comprueban los identificadores de la transacción en curso y, si todo es correcto, se formatea y envía una petición de autorización al banco emisor del cliente a través de la red de medios de pago convencional.

5. El emisor de la tarjeta autoriza la transacción: se autoriza el pago por el banco emisor del cliente. El banco emisor verifica todos los datos de la petición y si todo está en orden y el titular de la tarjeta posee crédito, autoriza la transacción.

6. Envío al comerciante de un testigo de transferencia de fondos: cuando el banco del comerciante recibe una respuesta de autorización del banco emisor, genera y firma digitalmente un mensaje de respuesta de autorización que envía a la pasarela de pagos, convenientemente cifrada, la cual se la hace llegar al comerciante.

7. El servidor del comerciante completa la transacción: se envía un recibo a la cartera del cliente. Cuando el comerciante recibe la respuesta de autorización de su banco, verifica las firmas digitales y la información para asegurarse de que todo está en orden. El software del servidor almacena la autorización y el testigo de transferencia de fondos. A continuación completa el procesamiento del pedido del titular de la tarjeta, enviando la mercancía o suministrando los servicios pagados. Además, se le entrega a la aplicación cartera del cliente un recibo de la compra para su propio control de gastos y como justificante de compra.

8. Entrega del testigo de transferencia de fondos para cobrar el importe de la transacción: luego de haber completado el procesamiento del pedido del titular de la tarjeta, el software del comerciante genera una petición de transferencia a su banco, confirmando la realización con éxito de la venta. Como consecuencia, se produce el abono en la cuenta del comerciante.

9. El banco emisor de la tarjeta de pago envía el aviso de crédito al cliente: se produce el cargo en la cuenta del cliente. A su debido tiempo, la transacción se hace efectiva sobre la cuenta del cliente, (InterLab, 2013).

1.7.1.2 Protocolo SSL

La mayoría de los sistemas transaccionales actuales se basan en soluciones basadas en SSL. Se le conoce de forma genérica como punto de venta virtual (TPV virtual). La principal carencia de los pagos SSL es la imposibilidad de firmar digitalmente la orden de transacción que emite el comprador eliminando de esta forma el requisito que éste posea un certificado digital. Esto se soluciona situando el TPV virtual en la pasarela de pagos (que se encuentra en la entidad financiera), y solicitando éste la autentificación al comerciante, a diferencia del protocolo SET, donde es el comerciante quien traslada la orden que de compra a la pasarela. Por lo anterior, se han tarjetas virtuales caracterizadas por disponer de un saldo fijo que se agota, siendo necesaria su recarga posterior, (Buch I Tarrats y Jordán, 2011).

Gráfica V. Protocolo SSL

Fuente: (Unad, 2011).

En la gráfica V se puede apreciar el proceso de funcionamiento del protocolo SSL, donde el usuario solicita un inicio de sesión, por lo que se requiere conexión con el servidor; posteriormente la solicitud es validada por un certificado que devuelve la señal al dispositivo del usuario y ésta a su vez se dirige de nuevo al servidor por medio de la llave encriptada; finalmente se termina el proceso de inicio de sesión entre el usuario y el servidor.

1.7.2.3 PKI (Infraestructura de clave pública)

Según Buch I Tarrats y Jordán (2011) el PKI o Infraestructura de clave pública, son estándares y servicios que facilitan el uso de la criptografía y los certificados en un entorno de red.

Mediante el establecimiento de una infraestructura de clave pública se permite garantizar diversos requerimientos de seguridad.

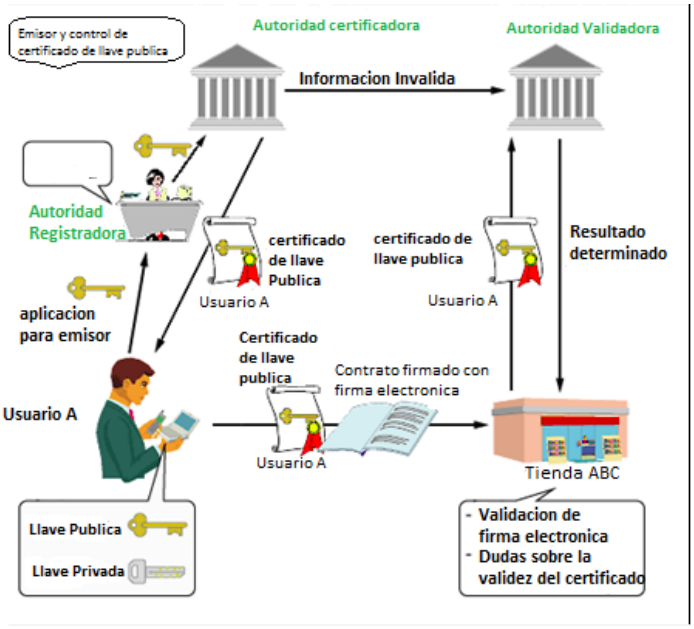
La confidencialidad se garantiza cifrando los datos que viajarán por la red; a través del uso de firmas digitales, lo que garantiza la autenticidad, la integridad y el no repudio de los datos. Sin embargo, se requiere:

- **Autoridad de Certificación (CA):** emite certificados para las partes que intervienen, mantiene las listas de revocación de certificados para resolver los casos de robo, pérdida o suspensión de claves privadas. Un problema de seguridad que afecte a la CA puede afectar a toda la infraestructura existente.
- **Directorio:** es la base de datos donde se publican los certificados; además se guardan otros datos las listas de revocación.
- **Sistema de revocación de certificados:** aunque sea un servicio asociado a la autoridad de certificación, éste puede suministrarse por otra entidad.

- **Actualización, históricos y copias de claves:** componentes que permiten la renovación del certificado y el uso de claves antiguas.
- **Soporte para el no repudio:** la protección de las claves privadas puede ser crítica para el no repudio de las firmas digitales realizadas. Los sistemas basados en tarjetas criptográficas son los que ofrecen las mayores garantías. Estos componentes deben existir y pueden estar gestionados por la propia entidad bancaria, un consorcio u otra entidad externa.

A continuación, en la gráfica VI se muestra el proceso de funcionamiento del PKI.

Gráfica VI. Funcionamiento PKI



Fuente: (Ziv, 2012).

1.7.3 La imagen de seguridad de la banca virtual

Muchas entidades financieras utilizan una imagen de seguridad para acceder a la banca virtual, para lo cual, cuando el usuario se registra por primera vez elige una imagen de su gusto y se le advierte que no ingrese sus datos financieros si la imagen no corresponde a la que eligió. Esta estrategia se implementó con el fin de evitar ataques de *Phishing*, (Lee, Bauer y Mazurek, 2015).

Sin embargo, su eficiencia para evitar este tipo de ataques no se conoce con certeza. Incluso, en un estudio citado por los autores, el 92% de los usuarios de banca en línea, afirmaron acceder a sus cuentas cuando no se mostraba la imagen de seguridad. En el estudio realizado por ellos, demostraron que, el 73 de los usuarios acceden a su cuenta sin fijarse en la imagen de seguridad y sólo el 27% se abstiene de acceder cuando esta no se presenta o es errónea; esto demuestra que los usuarios no poseen este hábito de seguridad; además, los autores afirman que la imagen de seguridad puede utilizarse igualmente en un ataque de *Phishing*, por lo que este método de seguridad no es muy efectivo, más, si se compara con otros; por ejemplo, utilizar dos factores de autenticación del usuario. Por lo anterior, los autores sugieren que los bancos deben implementar mejores sistemas de seguridad para acceder a banca en línea, pues no ´solo favorece la conciencia de los usuarios, sino que complica el actuar delictivo.

1.8 Una mirada hacia el futuro

Los criminales, durante años, han infiltrado personas pertenecientes a organizaciones para cometer con mayor facilidad los delitos financieros. Es decir, se unen o le pagan a un empleado para que este extraiga información, ponga elementos de captura de información en cajeros o datáfonos, entre otros. (Villadiego, 2015).

Por lo anterior, es de esperar que estos criminales sigan usando esta técnica para crear mejores técnicas de fraude, más económicas y efectivas. Actualmente, por ejemplo, los delincuentes están haciendo uso de Raspberry Pi para realizar ataques de tipo Man in the middle. Esta tecnología novedosa posee características muy llamativas para los delincuentes, no sólo por el hardware sino que pertenece a una comunidad realmente activa que constantemente realiza actualizaciones y mejoras; además, su uso es extremadamente sencillo.

Los delincuentes se están aprovechando de que esta nueva tecnología se está usando en diversas organizaciones con fines legítimos, sin embargo, estas personas no se preocupan por la seguridad, por lo que el delincuente busca cualquier vulnerabilidad del sistema para sacar provecho de ello. Por lo anterior, se hace necesario que las empresas, al igual que los delincuentes, se mantengan informados e inviertan en investigación de seguridad, minimizando de esta forma las vulnerabilidades y prevenir ataques sumamente riesgosos para las compañías; ya que, esta nueva modalidad de ataque se ve venir en un futuro cercano. (Villadiego, 2015).

2. METODOLOGÍA

Inicialmente, se realizó una búsqueda y selección de literatura referente al tema del cibercrimen en el mundo y Colombia, además de antecedentes de estudios sobre este tipo de delitos en el sistema financiero colombiano con el fin de contextualizar al lector y hallar los problemas reales que se presentan en el país referentes al ciberdelito bancario; se hizo uso de internet, bases de datos académicas; se encontró que se reporta inexistencia de estudios oficiales y cifras relevantes y específicas, por lo que se vio la necesidad de implementar un cuestionario, dirigido a usuarios de banca en línea residentes en la ciudad de Medellín, la cual se realizó a través de la herramienta Formularios de Google Drive, los cuales fueron contactados mediante correo y los encuestados son contactos de diferentes cuentas de correo. Esto se realizó con el fin de establecer un diagnóstico de la situación actual de los ciberdelitos contra usuarios de banca en línea; la encuesta permitió conocer los hábitos de seguridad de estos usuarios, la incidencia y tipología de fraudes bancarios electrónicos; la encuesta tuvo un resultado de 266 respuestas, las cuales fueron tabuladas en Microsoft Office Excel 2013, para poder obtener las tablas dinámicas y así interpretar los resultados obtenidos. Posteriormente, se procedió a comparar y discutir la información reportada y determinar un porcentaje de incidentes relacionados con cibercrímenes, identificar los principales medios usados para delinquir y conocer los hábitos de seguridad de los usuarios. Finalmente, se expone una lista de las prácticas básicas que deben adoptar los usuarios de banca en línea y consumidores electrónicos para evitar ser víctimas de este tipo de delitos.

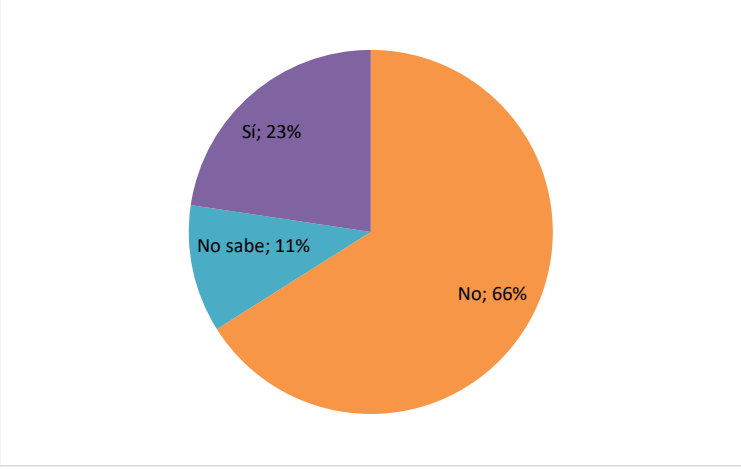
3. RESULTADOS Y DISCUSIÓN

3.1. Resultados de la encuesta sobre el fraude electrónico a usuarios de banca en línea en Medellín

A la encuesta se le estima un porcentaje de error de aproximadamente 5%. El total de población encuestada fue de n= 266, los usuarios elegidos para dicha encuesta son residentes en la ciudad de Medellín, los cuales fueron contactados mediante correo electrónico, por lo que los datos obtenidos sólo dan una información parcial; sin embargo, los resultados demuestran las tendencias de los hábitos de seguridad que conocen o adoptan los usuarios de banca en línea; igualmente, se evidencia el índice de ocurrencia de fraudes e intentos de fraude electrónico al sistema bancario. Al ser la encuesta sólo a personas de Medellín, es de esperarse que la mayoría reporte a Bancolombia como el ente financiero objeto del fraude.

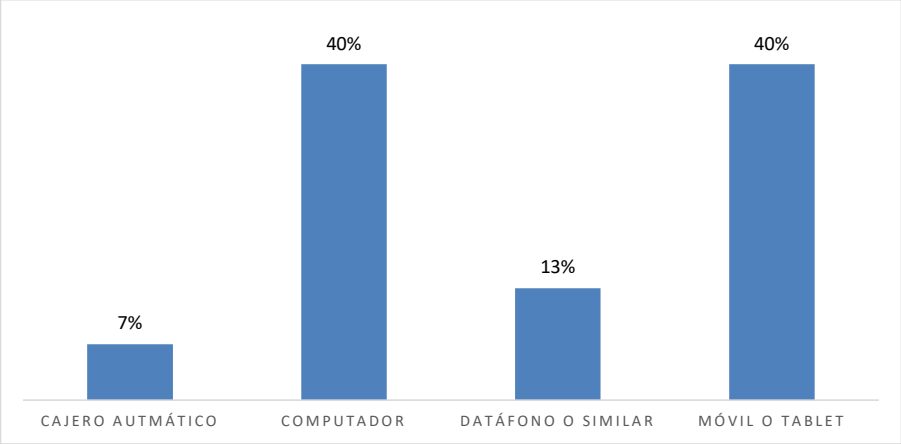
3.1.1. Índices de ocurrencia de fraude electrónico bancario

Tabla 1. ¿Ha sido usted víctima de algún fraude electrónico bancario



El 66% de los encuestados afirmó nunca haber sido víctima de un fraude electrónico bancario, sin embargo, el 11% no tiene la certeza, mientras que el 23% de la muestra poblacional confirma haber sido víctima de este delito. Se evidencia que es alta la población que desconoce sí ha sido víctima de fraude electrónico bancario o no; además, el resultado de 23% de víctimas concuerda con las afirmaciones de Acurio del P. (s.f), Temperini (s.f), Guzmán (2009) y Certicámara (2014), los cuales afirman que estos delitos no son casos aislados y que se mantienen en continuo crecimiento, aunque no existen cifras oficiales de incidencia.

Tabla 2. ¿A través de cuál medio se realizó el fraude?

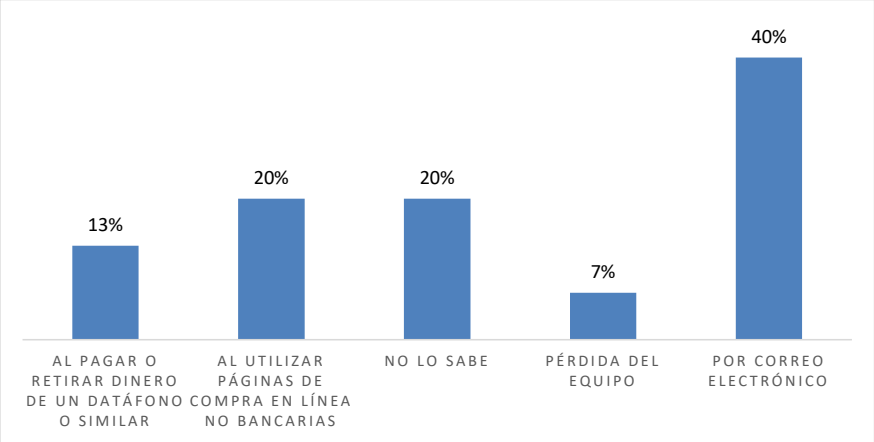


A las personas que afirmaron haber sido víctimas se les ha realizado la pregunta previa que se ilustra en la gráfica, encontrándose así que el 40% fue a través del uso del computador al igual que los celulares o tablets, seguido por datáfonos o similares con un 13%, mientras que el 7% afirmó haber sido víctima a través de cajeros automáticos. Esta información concuerda con las afirmaciones de Colombia Digital (2015) respecto a las modalidades más comunes utilizadas en el país para el fraude electrónico bancario: Phishing

Comentado [JMDV1]: datáfonos

y Malware, así mismo como el Skimming, el cual se evidencia con un 13% de incidencia en los encuestados.

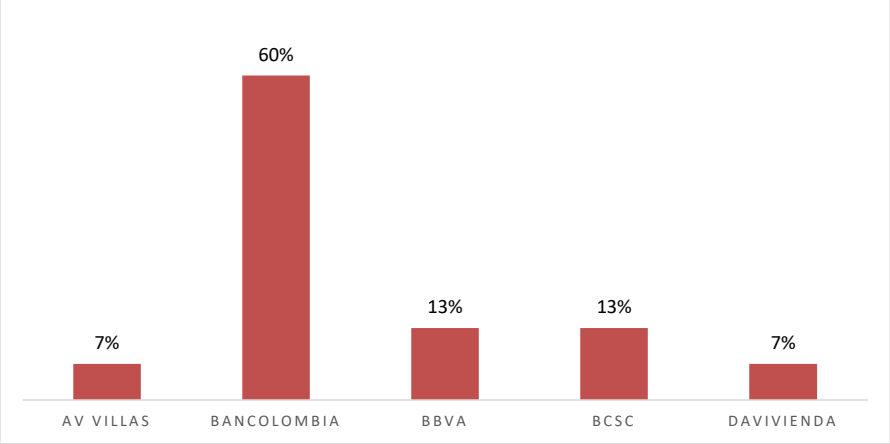
Tabla 3. ¿Cómo sucedió el fraude?



El 40% de las víctimas fueron atacadas a través del correo electrónico, seguidas por las páginas de compra en línea no bancarias con un 20%, el mismo porcentaje asegura no saber cómo ocurrió el fraude. El 13% afirma haber sido víctima al pagar o retirar dinero en datáfono o cajeros y el 7% por pérdida o robo del dispositivo electrónico.

Es alarmante que el 20% de las víctimas no supieran a través de cuál medio fue el fraude, mientras que la mayoría afirmó haber sido por correo electrónico, lo cual demuestra las afirmaciones hechas por Certicámara (2014), KPMG (2013) y Colombia Digital (2015), quienes aseguran que es la modalidad más común de hacer los fraudes bancarios y el robo de información financiera.

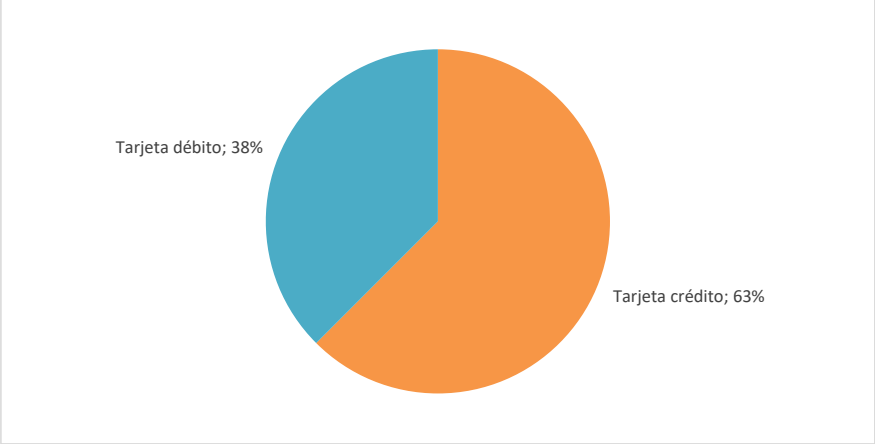
Tabla 4. ¿A cuál banco pertenecía el producto objeto del fraude?



La mayoría de los encuestados, con un 60% afirma que el producto objeto del fraude electrónico pertenecía a Bancolombia, lo cual era de esperarse por ser todos los encuestados habitantes de Medellín, ciudad en la que Bancolombia es el banco principal con más usuarios activos respecto a los demás entidades bancarias. Le siguen a éste, con igual porcentaje, los bancos BBVA y BCSC con un 13% y por último, con 7%, cada uno, los bancos AV Villas y Davivienda.

Sin embargo, las estadísticas concuerdan con el informe de quejas presentado por la Superintendencia Financiera de Colombia en el año 2014, pues Bancolombia fue la entidad en recibir el mayor número de quejas.

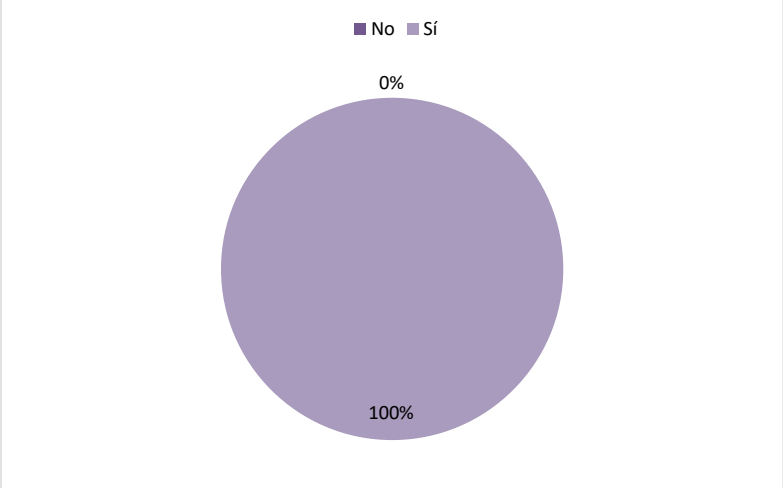
Tabla 5. ¿Qué tipo de producto fue el objeto del fraude?



El 63% de los fraudes ocurrieron a tarjetas de crédito, mientras que el 38% pertenecían a tarjetas débito.

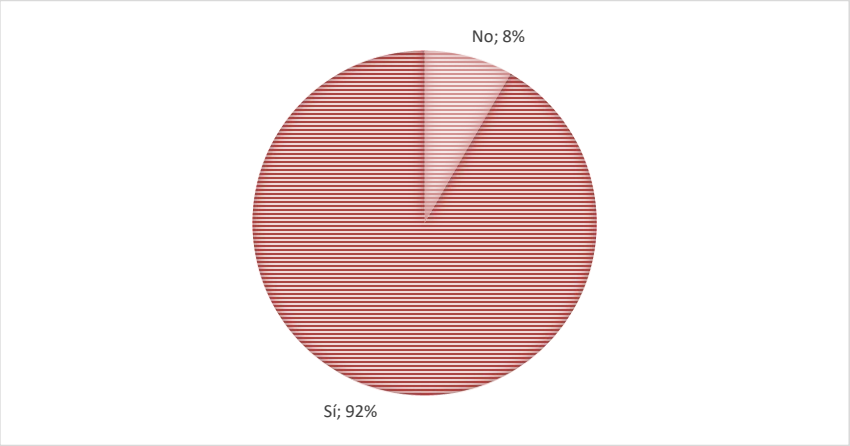
Esta cifra concuerda con las afirmaciones de Dueñas (2015), pues, al ser la tarjeta de crédito la más utilizada en compras en línea y en datafonos, es más propensa a su clonación o robo de contraseñas. Sin embargo, los fraudes en tarjetas débito son también altos.

Tabla 6. Al momento del fraude, ¿utilizaba un dispositivo electrónico personal?



El 100% de los encuestados que afirmaron haber sido víctimas a través de computadores, tablets o móviles aseguraron haber utilizado un dispositivo propio en el momento del fraude. Esta cifra es alarmante, pues evidencia la inseguridad existente en los dispositivos personales y la alta incidencia de acceso remoto, tal como lo mencionó Colombia Digital (2015) y el Diario El País (2014).

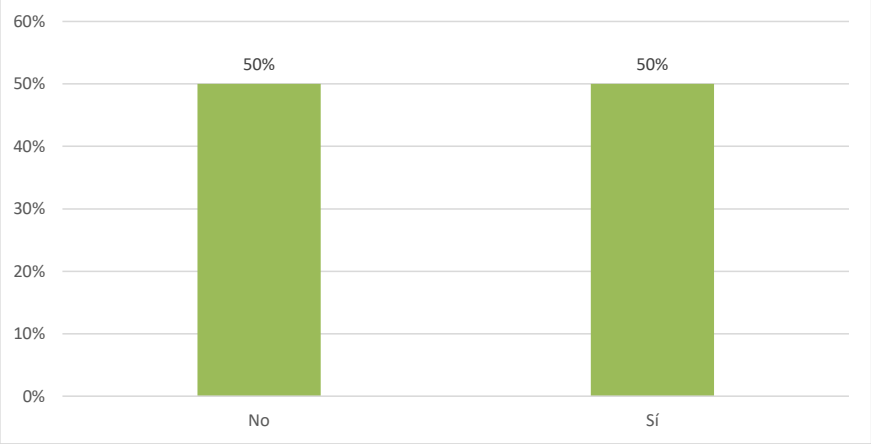
Tabla 7. Al momento del fraude, ¿estaba conectado a una red personal o segura?



El 92% de los encuestados que afirmaron haber sido víctimas a través de celulares, tablets o móviles aseguraron haber utilizado una red privada y segura en el momento del fraude, mientras que el 8% estaba utilizando una red pública o sin seguridad.

Al igual que las cifras sobre el uso de dispositivo personal, se demuestra la capacidad de los delincuentes para acceder de manera remota, ya que la gran mayoría estaba conectado a una red privada y segura.

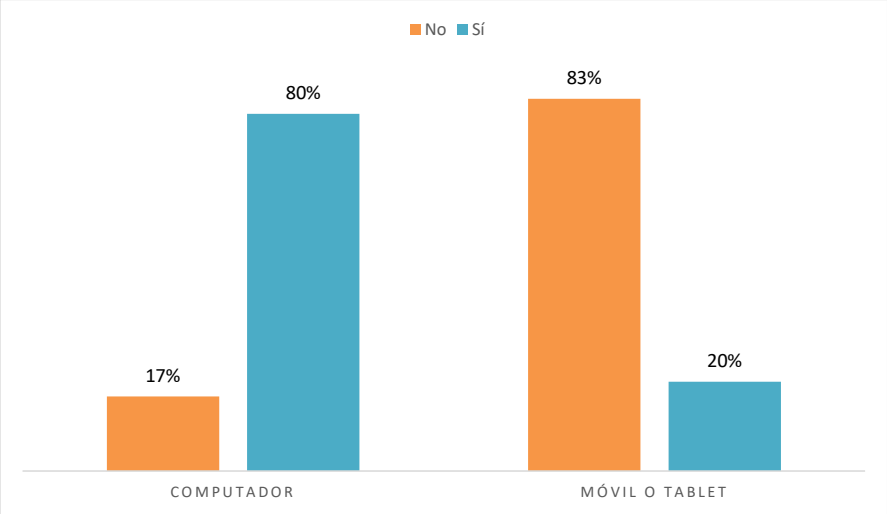
Tabla 8. Al momento del fraude, ¿utilizaba antivirus o alguna herramienta de seguridad?



El 50% de las víctimas aseguró no haber utilizado un antivirus o herramienta de seguridad electrónica en el momento del fraude.

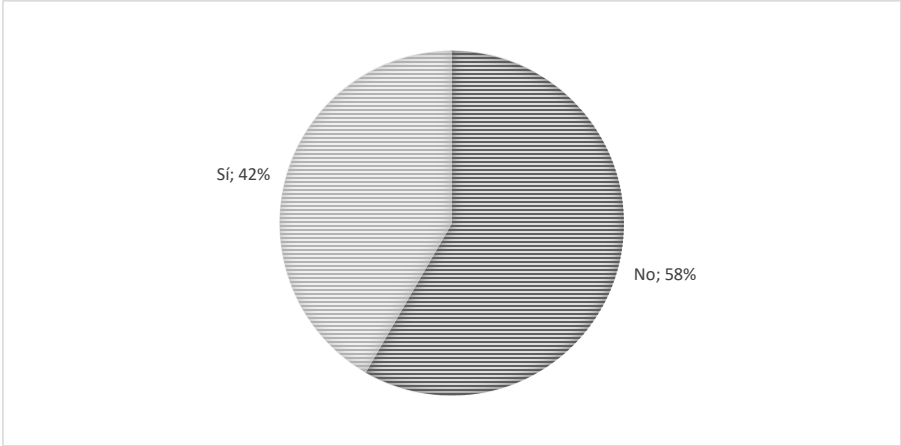
El hecho de que sólo la mitad de las víctimas encuestadas estuviesen utilizando un antivirus actualizado y confiable, explica la facilidad de acceder fraudulentamente a sus datos privados. Sin embargo, el 50% que sí lo utilizaba confirma la afirmación de David Agudelo, al afirmar que "no basta con tener un antivirus y un antispam" (Caracol Radio, 2012).

Tabla 9. Comparación del uso de antivirus entre usuarios de móviles y tablets Vs computadores



Se evidencia que la cultura del uso de antivirus es escaso en los usuarios de móviles o tablets, ya que sólo el 20% de los que fueron víctimas aseguraron haber utilizado uno para acceder a sus servicios financieros, lo cual es proporcionalmente inverso a los usuarios de computador, ya que el 80% de ellos, afirmaron haber utilizado un antivirus en el momento de acceder a sus servicios financieros en línea. Esto concuerda con la preocupación de Villadiego, al afirmar que las personas creen que las tablets y los móviles no pueden ser infectados con virus o malware y por ello no lo hacen, además que, los delincuentes se aprovechan de esta creencia para acceder más fácilmente. (Dueñas, 2015)

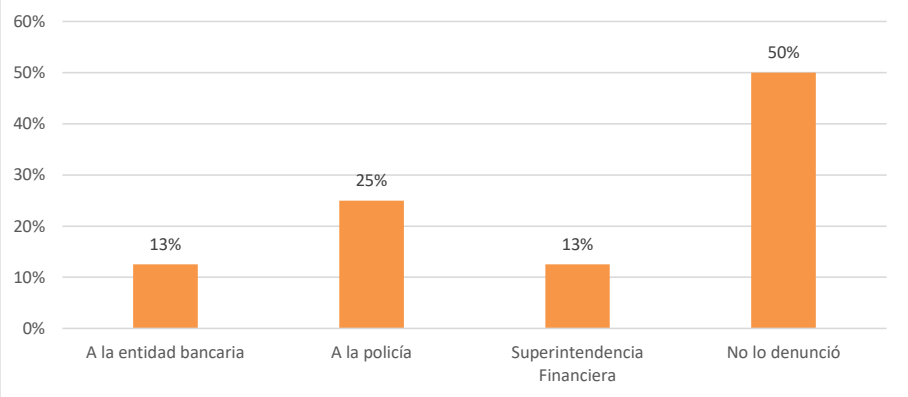
Tabla 10. ¿Considera que pudo haber evitado el fraude?



El 58% de las víctimas encuestadas, aseguró haber podido evitar el fraude, mientras que el 42% no lo cree así.

Aunque es evidente que la mayoría cree haber podido evitar el fraude, (adoptando medidas básicas de seguridad antes de acceder al sistema financiero en línea), es alto el porcentaje que cree que fue imposible evitarlo. Esto concuerda con los estudios de KPMG (2013), al descubrir que la mayoría de los usuarios no consideran que el uso de la tecnología es riesgoso y no se confían en que las medidas de precaución y prevención de seguridad informática realmente funcionen.

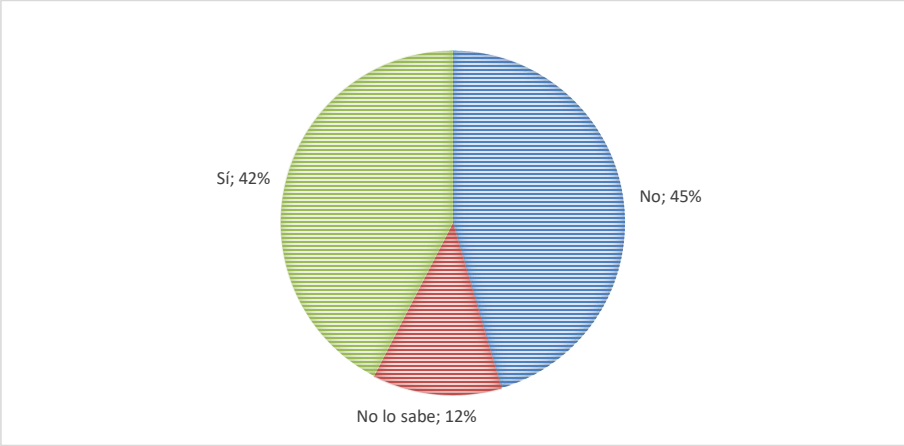
Tabla 11. ¿Denunció el fraude y a quién?



Es evidente que, la cultura de denuncia de este tipo de delitos es muy bajo, ya que el 50% de las víctimas afirmó no haberlo reportado a ninguna entidad. Las personas que sí lo denunciaron, en su mayoría, lo hicieron a la Policía Nacional, con un 25%, mientras que el 13% lo realizó a la Superintendencia Financiera y el mismo porcentaje lo hizo a la entidad bancaria. Estas cifras concuerdan con las afirmaciones de Acurio del P (s.f.) al decir que las personas no denuncian este tipo de delitos y por lo cual, es difícil establecer cifras confiables de incidencia.

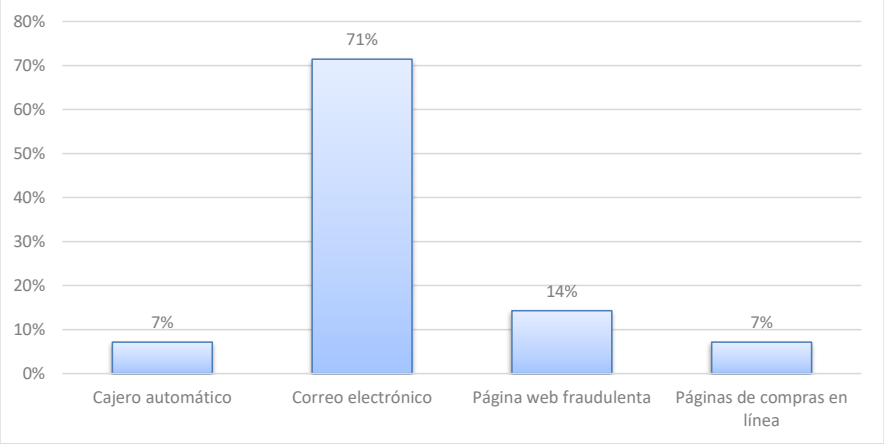
3.1.2. Índices de ocurrencia de intentos de fraude electrónico bancario

Tabla 12. ¿Le han intentado robar información a través de medios electrónicos?



De las personas que afirmaron no haber sido víctimas de fraudes bancarios electrónicos, el 42% de ellas asegura que sí le han intentado robar información financiera sin éxito, el 12% de ellos no está segura y el 45% de ellos asegura que nunca le han intentado robar este tipo de información a través de medios electrónicos. Estas cifras demuestran que la incidencia de este tipo de delitos es realmente alta, pues aunque estas personas evitaron el robo, se evidencia la presencia de personas dedicadas a este tipo de criminalidad, en concordancia con las afirmaciones de Acurio del P. (s.f.), Temperini (s.f.), Guzmán (2009) y Certicámara (2014).

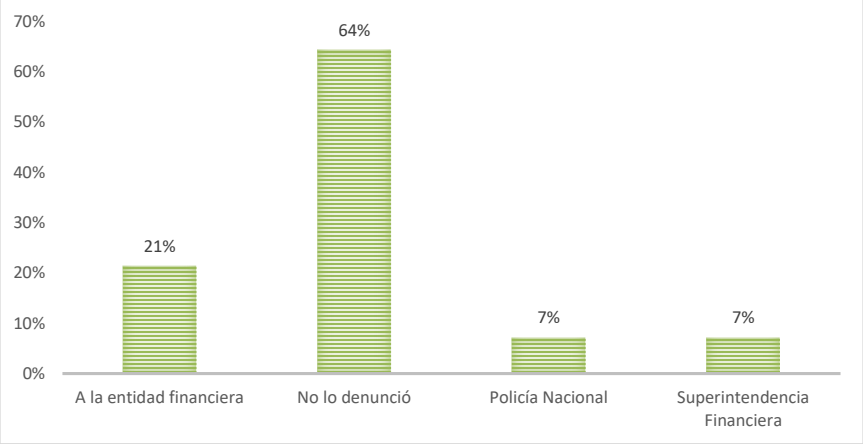
Tabla 13. ¿A través de cuál medio le intentaron robar la información?



De los encuestados que aseguraron haber sido víctimas de intentos de fraude sin éxito, el 71% afirmó que fue a través del correo electrónico, seguido por un 14% a través de páginas webs fraudulentas y por último, con 7% cada uno, fueron a través de cajeros automáticos y páginas de compras en línea.

Una vez más se demuestra que la mayor incidencia de estos crímenes es a través del correo electrónico y el Phishing, como ya se ha afirmado y comprobado con los datos proporcionados por Acurio del P, (s.f.).

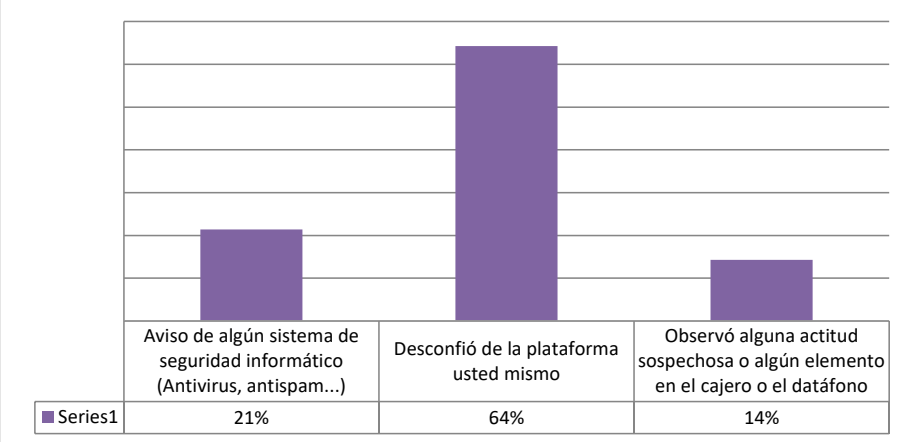
Tabla 14. ¿Denunció el intento de fraude y a quién?



El 64% de los encuestados, aseguró no haber denunciado a ninguna entidad el intento de fraude, mientras que el 21% lo hizo a la Entidad Financiera y por últimos, con un 7% cada uno, se reportaron a la Policía Nacional de Colombia y a la Superintendencia Financiera de Colombia.

El porcentaje de denunciantes en intento de robo fue 14% menor al caso de fraudes con éxito, lo cual era predecible debido a la falta de cultura de denuncia de este tipo de crímenes. La mayoría de los que denuncio, prefirió hacerlo a la entidad financiera, por lo cual, es de esperarse que estas cifras no se reporten públicamente como lo afirma Colombia Digital (2015).

Tabla 15. ¿Cómo evitó el fraude?



El 64% de los encuestados que evitaron ser víctimas de fraudes electrónicos financieros aseguró que lo habían evitado por desconfianza de la plataforma, mientras que al 21% de ellos los alertó el antivirus o el antispam y el 14% de ellos, lo evitó a través de la observación de actitudes sospechosas o elementos extraños en los dispositivos.

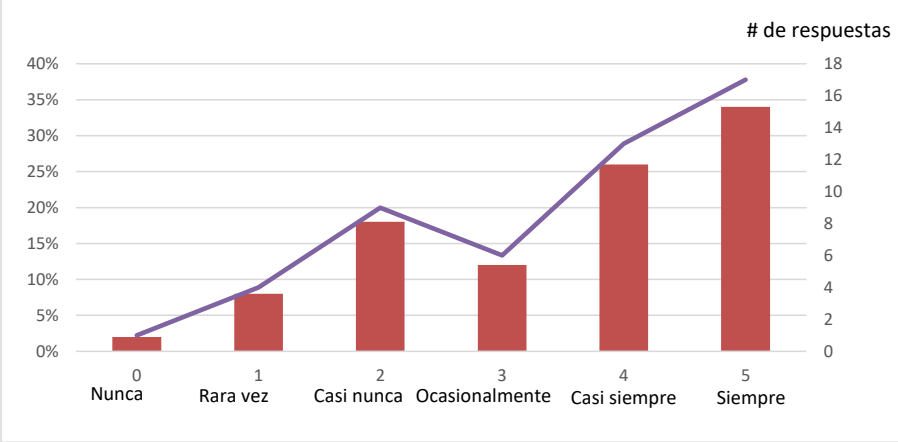
Esto demuestra que, la mayoría de personas que han evitado ser víctimas de fraudes electrónicos, lo han logrado por la precaución y cultura de seguridad informática que poseen y en menor medida, por el uso de herramientas de seguridad electrónica, lo cual corrobora las afirmaciones de Temperini (s.f.) y KPMG (2013) al decir que es necesario generar educación y hábitos de seguridad informática y que esto es uno de los pilares claves para combatir este tipo de delincuencia.

. Medios más usados contra usuarios de banca en línea	. Cajero automático . Computador . Datafono o similar . Móvil o Tablet
. Formas más frecuentes de fraude	. Al pagar o retirar dinero de un datafono o similar . Compras en online . Pérdida o robo de equipo de computo . Vía mail
. Tipo de productos al momento del fraude	. Tarjeta Debito . Tarjeta de Crédito

3.1.3. Hábitos de seguridad informática de los usuarios de banca en línea encuestados

El siguiente bloque de preguntas corresponde a una evaluación cuantitativa siguiendo una escala Likert que abarca calificaciones de 0 a 5, siendo 0, nunca; 1, rara vez; 2, casi nunca; 3, ocasionalmente; 4, casi siempre y 5, siempre.

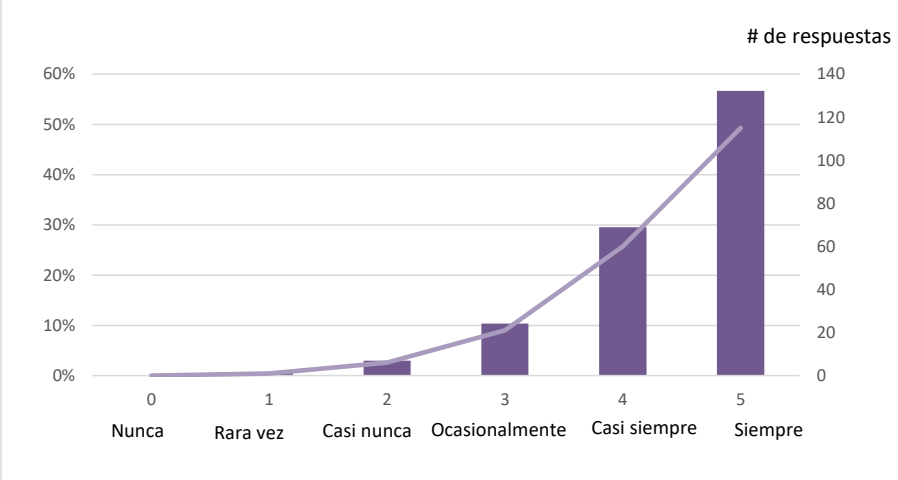
Tabla 16. Conexión a redes privadas y seguras



Se les ha preguntado a los encuestados sobre el uso de redes seguras al momento acceder a los servicios financieros en línea, y los resultados, tras el análisis de la gráfica, son los siguientes: El 34% afirma usar redes seguras siempre (calificación:5), el 26% afirma usarlas casi siempre (calificación:4), el 18% asegura que casi nunca usa redes seguras (calificación: 2), le sigue el 12% indicando que el uso de redes seguras sólo se hace ocasionalmente, mientras que en el extremo está el 8% y el 2% indicando, respectivamente que usan las redes seguras rara vez (calificación: 1) o que nunca usan una red segura (calificación: 0).

Estas cifras demuestran que sólo un porcentaje de la población conoce la importancia del uso de redes privadas y seguras para acceder a servicios financieros con información personal, tal como lo ha afirmado KPMG (2013).

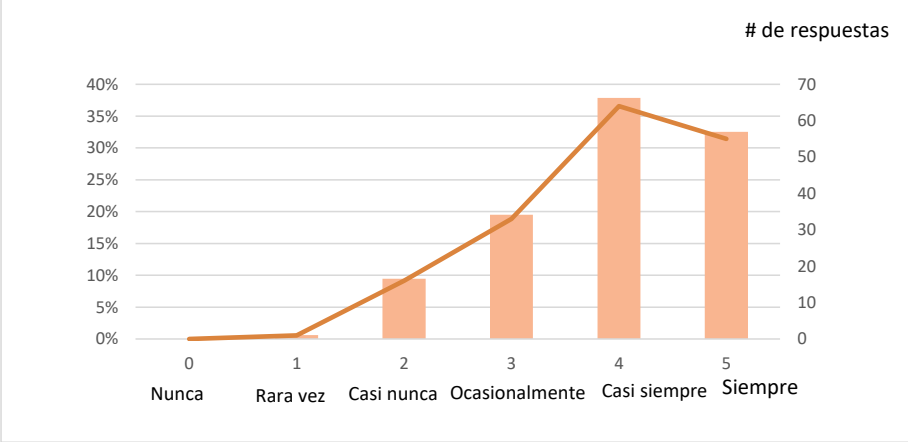
Tabla 17. Accede desde un dispositivo propio



Se les ha preguntado a los encuestados si acceden a sus servicios financieros desde un dispositivo propio. Como se aprecia en la gráfica el 57% del total de encuestados afirma, con una calificación de 5, que siempre accede a sus servicios electrónicos financieros desde un dispositivo propio, seguido con el 30% indicando que casi siempre (calificación de 4), el 10%, en cambio, afirma que sólo lo hace ocasionalmente, y tan sólo el 2% indica que rara vez lo hace (calificación de 1).

Estas cifras pueden interpretarse como el resultado de la masificación de dispositivos electrónicos de uso personal, como lo afirma Guzmán (2009); sin embargo, es un buen índice para la seguridad electrónica.

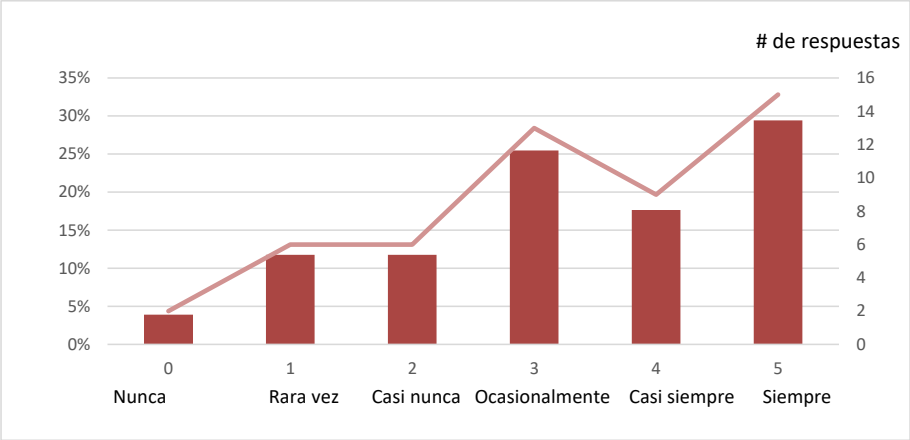
Tabla 18. Revisa que el cajero no posea dispositivos extraños



La mayoría de los encuestados demuestra ser precavido al utilizar el cajero, pues sólo el 9% aseguró no revisarlo nunca o casi nunca y el 71% afirmó hacerlo siempre o casi siempre.

Estas cifras pueden explicar por qué los cajeros no están en las primeras modalidades de robo y el alto índice de práctica de esta medida de seguridad, puede deberse a la gran cantidad de robos de este tipo en el pasado, lo que ha generado que la comunidad sea más precavida al usar este servicio.

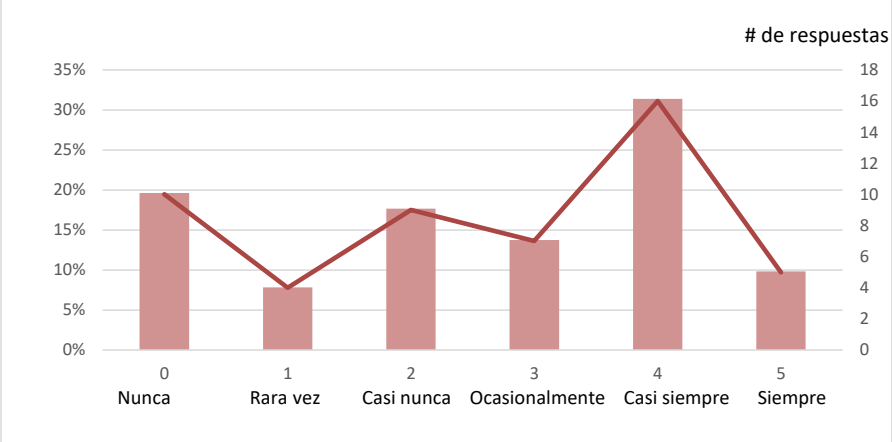
Tabla 19. Utiliza antivirus confiable y actualizado



Respecto al uso del antivirus confiable y actualizado, no se encuentran datos muy claros, pues el 29% asegura que siempre lo hace, (calificación de 5), mientras que el 25% de ellos dio una calificación de 3 u ocasionalmente, y en total, el 28% de ellos, dio una calificación entre 0 y 2, es decir, nunca o casi nunca utilizan un antivirus confiable.

Esto puede explicarse por la falta de cultura de uso de antivirus en dispositivos móviles o tablets, como se afirmó anteriormente, y demuestra además que, es relativamente fácil vulnerar la seguridad informática de estos usuarios.

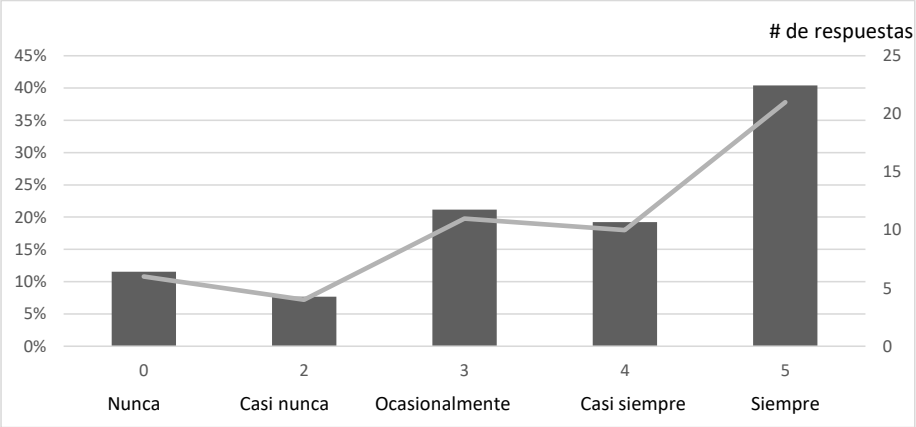
Tabla 20. Utiliza alguna herramienta de seguridad bancaria o antispam



El uso de herramientas de seguridad informática bancaria o antispam es escaso, pues, aunque el 41% afirmó usarlo siempre o casi siempre (calificaciones 4 y 5), el 28% dio una calificación de 0 y 1 y el 18% señala casi nunca usarlo (calificación 2).

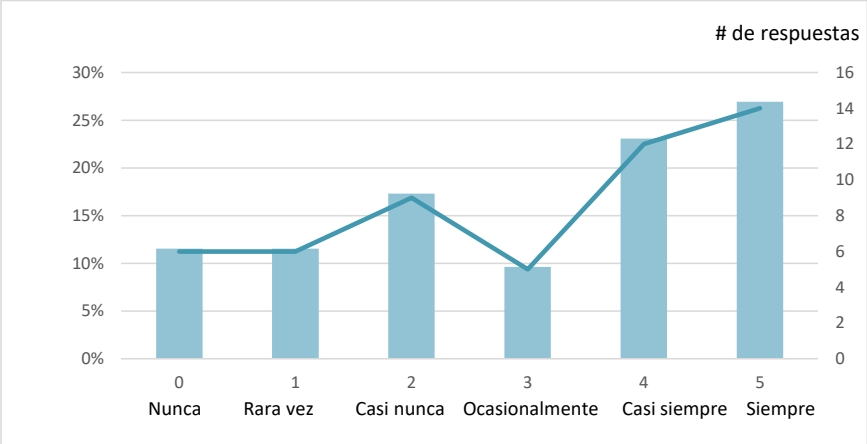
Es previsible que, los porcentajes de uso de este tipo de herramientas sean menores a los índices de uso de antivirus y además demuestra la falta de credibilidad o desconocimiento de los usuarios electrónicos sobre este tipo de herramientas, tal como lo dijo Dueñas, (2015).

Tabla 21. Digita la página web del banco en lugar de acceder por medio de enlaces o correos electrónicos



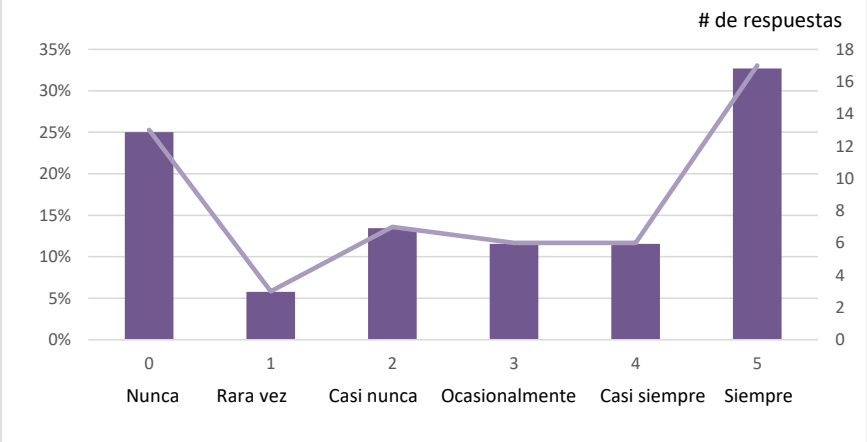
El 40% de los encuestados, afirma siempre escribir el enlace de la entidad bancaria para acceder a sus servicios, seguido por ocasionalmente, (calificación de 3) con un 21%. El 20% al parecer, no conoce la importancia de esta práctica preventiva pues dio calificaciones entre 0 y 2. Estas cifras concuerdan con la encuesta realizada por KPGM (2013), ya que sólo una parte de la población era consciente de la importancia de esta práctica.

Tabla 22. Verifica la marca de seguridad de la página antes de introducir sus datos personales (al inicio del enlace)



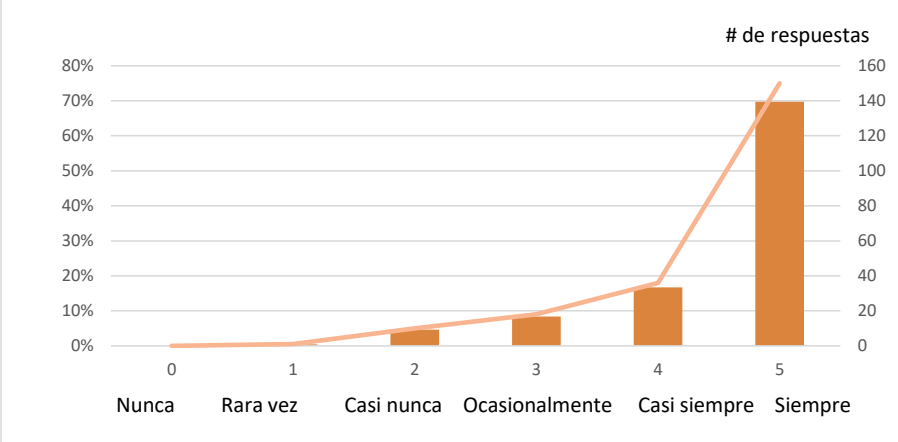
Como se demuestra en la tabla, son escasas las personas que reconocen la marca de seguridad de las páginas. En total, el 41% dio calificaciones entre 0 y 2, mientras que las calificaciones de 4 y 5 tuvieron un porcentaje del 50%. Por lo anterior, se demuestra, que quien sepa de esta marca lo adopta como una de las principales prácticas de prevención y seguridad informática, sin embargo, se evidencia que aún hay un alto desconocimiento de esto entre los usuarios de medios electrónicos.

Tabla 23. Informa a la entidad bancaria situaciones sospechosas



Del total de encuestados, sólo el 33% afirma informar siempre situaciones sospechosas a las entidades bancarias, seguido por un 25% de usuarios que afirmaron nunca hacerlo. Esto corrobora, como en los análisis anteriores de denuncias, es escasa esta cultura de informar, por lo cual es más complicado establecer cifras, evitar los fraudes, propicia el aumento de la cifra negra mencionada por Acurio del P (s.f.) y facilita la acción criminal.

Tabla 24. Reporta la pérdida de documentos o información personal financiera



La mayoría de personas encuestas afirman reportar la pérdida de documentos de información personal financiera, el 70% afirma hacerlo siempre, el 17% casi siempre, el 8% ocasionalmente y el 2% escasamente. Esas cifras demuestran que existe desconfianza en la gente cuando pierde sus tarjetas, contraseñas, extractos o saldos y al verse directamente afectados sí deciden comunicarlo.

En suma los habititos de seguridad informática adoptados por los usuarios de banca en línea son los siguientes: El acceso a servicios financieros desde dispositivos propios; la precaución y reserva con la que se utilizan los servicios del cajero electrónico, siempre revisando que no hayan dispositivos extraños en éste y, por último, el reporte de pérdida de documentos o información personal financiera. Los demás hábitos como el acceso a servicios financieros desde redes privadas y seguras; el uso de herramientas de antivirus actualizado y de seguridad bancaria son representativamente menos adoptados, por consiguiente se hace necesario proponer estrategias de prevención tal como se hará en el siguiente apartado.

3.2.Estrategias de prevención para los usuarios de banca en línea

A los usuarios de banca en línea y consumidores online se les recomienda que sigan las siguientes medidas de prevención para evitar un posible fraude:

A) Digitar siempre la página web del banco, pues el 41% de los encuestados no tiene esta práctica como un hábito de seguridad frecuente.

B) Verificar siempre la marca de seguridad del banco al inicio del enlace, que generalmente, está marcado con verde. Se sugiere debido a que se encontró que el 50% de los encuestados no poseen este hábito.

C) Utilizar un antivirus legal y actualizado, en conjunto con herramientas de seguridad bancarias como Safe-Money, algún anti-spam disponible gratuitamente en el centro de aplicaciones del explorador, así como bloqueadores de ventanas emergentes y publicidad que puede ser maliciosa como AdBlock. Esto es de suma importancia, y según los hallazgos obtenidos en el trabajo de campo, el 50% de los usuarios que fueron víctimas no estaban usando ningún tipo de antivirus, y respecto al hábito de su uso, sólo el 45,45% de los usuarios de tablets y/o móviles lo usan en su dispositivo.

D) Nunca acceder al banco o a la página del banco mediante enlaces de correo electrónico, ni rellenar formularios con datos personales en el mismo medio, pues es frecuente esta modalidad para el fraude bancario, como se demuestra en la Tabla 13.

E) Revisar siempre que el cajero no posea dispositivos extraños antes de introducir la tarjeta, de esta manera se evita el Skimming frecuentemente realizado, descrito en el marco teórico.

F) Denunciar a la policía, la entidad financiera, superintendencia financiera y al defensor del consumidor financiero cualquier fraude o actitudes sospechosas. Esta última afirmación se hace debido a que existe poca cultura de denuncia, como se puede apreciar en los resultados de las encuestas.

3.3.Estrategias de prevención para entidades bancarias y autoridades

Las entidades bancarias deben trabajar en conjunto con las autoridades y a continuación se presentan algunas medidas que pueden implementarse como estrategias de prevención de fraudes bancarias.

A) Promover la cultura de prevención y seguridad electrónica a los clientes de banca en línea, mediante boletines en los bancos y cajeros, páginas web de la entidad y correos electrónicos de la base de datos de éstas. Esto con el fin de fortalecer los hábitos de seguridad de los usuarios, ya que se demostró que aún existe mucha confianza e ignorancia sobre prácticas sencillas y que garantizan una mejor seguridad.

B) Desarrollar y proporcionar a los clientes herramientas de seguridad electrónica específica para la entidad bancaria, para uso doméstico y/o empresarial. Esta práctica se hace necesaria no sólo por la importancia de confiabilidad que los usuarios depositan en las entidades bancarias, sino que a su vez permite mitigar la incidencia de crímenes, que según la literatura citada y la encuesta realizada es un fenómeno frecuente y no aislado.

C) Implementar medidas de identificación del titular de la cuenta diferentes a las claves de tarjeta al acceder a un servicio financiero virtual de la entidad, como preguntas secretas, datos personales anteriores u otros. Esta práctica podría disminuir considerablemente la suplantación de identidad.

D) Propiciar un enlace en la página web para reporte de anomalías, fuga de datos o elementos bancarios y fraudes electrónicos. En casos de emergencia, este tipo de medida puede evitar el robo de dinero de cuentahabientes con mayor rapidez, en caso de que el usuario se percate de algo extraño.

E) Implementar marcas de seguridad más visibles en sus portales web y darlo a conocer a sus usuarios; importante ya que aún el reconocimiento de la marca de seguridad no es muy habitual en todos los usuarios, igualmente garantizaría mayor confianza y seguridad.

F) Ofrecer capacitaciones a grupos empresariales o estudiantiles sobre los riesgos y medidas de prevención de fraudes bancarios electrónicos, lo cual fortalece la cultura de prevención y seguridad.

G) Implementar políticas públicas sobre el reporte de fugas de información de los sistemas bancarios así como la implementación de software diseñado para la seguridad de ésta. Esto con el fin de atacar con mayor eficiencia a los delincuentes.

4. CONCLUSIONES, RECOMENDACIONES Y TRABAJO FUTURO

- Es evidente que existe un alto índice de criminales que buscan víctimas entre los usuarios del sistema bancario, (23% de los encuestados ha sido víctima, mientras que el 42% afirma que le han intentado hacer un fraude electrónico), así como falta de conocimiento de este tipo de fraudes por parte de los usuarios, pues hay un alto porcentaje de personas que no saben si han sido víctimas de fraude electrónico o si han sufrido un intento de estos robos, (11% y 12% respectivamente).
- Se puede concluir que la tipología más común es a través de correos electrónicos y páginas falsas, Phishing, con más del 50% entre ataques exitosos e intentos y los medios más utilizados son los computadores, móviles y tablets. Además, hay una escasa cultura y educación de prevención en seguridad informática, ya que, en la mayoría de los casos, los usuarios no siguen las precauciones básicas para evitar los robos, como son: el uso de antivirus en tablets y móviles, verificación de la marca de seguridad y digitar la página financiera en lugar de acceder a través de enlaces o correos, lo cual, facilita a los criminales su accionar delictivo exitoso.
- Existe poca cultura de denuncia por parte de los usuarios ante estos incidentes, lo cual hace más difícil establecer cifras confiables y generar estrategias de prevención. También, es pertinente concluir que, la mayoría de las personas que han logrado evitar un fraude o robo de este tipo es por sus conocimientos en informática, ya que lo evitaron por desconfianza de la plataforma en mayor proporción que la ayuda de antivirus o herramientas de seguridad y así mismo, se demuestra que, no basta con tener un antivirus y un antispam para salvarse de estos fraudes.
- Se evidencia igualmente que, a medida que los delincuentes y su forma de delinquir es descubierta, los usuarios adoptan medidas de seguridad, como es el caso de la revisión de

elementos extraños en los cajeros. Es necesario tener en cuenta que, estos resultados poseen un margen de error del 5% aproximadamente y que la encuesta se realizó a 53 usuarios en total; aun así, los datos concuerdan con lo informado por investigaciones previas.

- La encuesta realizada a los usuarios de banca en línea da unos parámetros base para hallar la incidencia y tipología de fraudes bancarios electrónicos, así como para identificar los hábitos de seguridad y prevención que estos adoptan, sin embargo, estos datos sólo deben tomarse como una aproximación de referencia.
- Es posible, mediante las prácticas de prevención sugeridas, disminuir considerablemente este tipo de fraudes, las cuales son económicas, no requieren de mayor conocimiento en informática y están al alcance de cualquier usuario de este tipo de dispositivos. También, la cultura de denuncia puede lograr la identificación de estos criminales y su posterior proceso penal, así como generar un mayor conocimiento sobre el modus operandi de estos criminales.
- Es necesario seguir haciendo este tipo de estudios y no sólo sobre el sistema bancario, ya que las modalidades de crímenes son mucho más amplias e igualmente delicadas, como es el caso de extorsiones, acoso virtual, robo o suplantación de identidad, piratería, pornografía infantil, entre otros.
- Para futuros estudios sobre incidencia de fraudes electrónicos al sistema bancario, se recomienda ampliar la encuesta y especificar más en las formas del hurto, (modus operandi y tipologías). Sería muy provechoso para el país que la comunidad académica en conjunto con el estado y las entidades financieras desarrollaran un software de protección bancaria diseñada para el sistema financiero colombiano.
- Aunque este estudio proporcionó unas cifras coherentes, es necesario que en futuras investigaciones se encueste a un número mayor de usuarios, se evalúen los software de seguridad que utilizan los usuarios de banca en línea para compararlos y comprobar su efectividad, así como sistemas operativos utilizados, aplicaciones y extensiones informáticas; también debe determinarse una cantidad promedio de dinero extraviado por fraude y además, determinar el género de los encuestados, niveles de estudio y edades,

para establecer si estos factores sociales están relacionados con el uso seguro de las tecnologías y de esta forma hacer una tipología más acertada de las víctimas.

REFERENCIAS

- Acurio del P., Santiago. (s.f.). Delitos Informáticos: Generalidades. Recuperado de internet el 21/05/2015 en http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf
- Aitor. (2015). Phishing: Qué es y cómo protegerse. Disponible en: http://www.timos.info/phishing-que-es-y-como-protegerse/
- Buch I Tarrats, J. y Jordán, F. (2011). La seguridad de las transacciones bancarias en internet. Organización conganant. 11p.
- Caracol Radio. (2012). 187 denuncias mensuales por fraude electrónico en Colombia. 13 de marzo de 2012. Recuperado de internet el 07/08/2015 en http://www.caracol.com.co/noticias/tecnologia/en-promedio-187-denuncias-mensuales-por-fraude-electronico-se-registran-en-colombia/20120313/nota/1653843.aspx
- Certicámara. (2014).En Colombia el 42% de los usuarios de Internet ha sufrido un delito informático. Recuperado de internet el 21/05/2015 de https://www.ccb.org.co/content/download/4495/47693/version/1/file/Certic%C3%A1mara.pdf
- Cisco. (2008). Fuga de datos a nivel mundial: Riesgos y errores comunes de los empleados. Recuperado de internet el 21/05/2015 de http://www.cisco.com/web/offer/em/pdfs_innovators/LATAM/data_mist_sp.pdf
- Colombia Digital. (2015). ¿Cuáles son las amenazas de seguridad financiera más populares de Colombia? Publicado el 16 de junio de 2015. Recuperado de internet el 5/08/2015 en http://colombiadigital.net/actualidad/noticias/item/8365-cuales-son-los-amenazas-de-seguridad-financiera-mas-populares-en-colombia.html
- CONPES. (2011). Lineamientos de política para ciberseguridad y ciberdefensa. Ministerio de Interior y de Justicia Ministerio de Relaciones Exteriores Ministerio de Defensa Nacional Ministerio de Tecnologías de la Información y las Comunicaciones

Departamento Administrativo de Seguridad Departamento Nacional de Planeación-DJSG-DIFP-DIES-OI Fiscalía General. Recuperado de internet el 21/05/2015 en http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

- Cuervo, J. (2008). Informática Jurídica. Obtenido de Delitos informáticos: protección penal de la intimidad: http://www.informatica-jurídica.com/trabajos/delitos.asp
- Diario el País. (2014). Así roban su dinero a través de fraudes electrónicos. Publicado el 24 de diciembre de 2014. Recuperado de internet el 5/08/2015 en http://www.elpais.com.co/elpais/judicial/noticias/asi-roban-su-dinero-traves-fraudes-electronicos
- Dueñas C., M. (2015). Fraude electrónico crece y cambia de cara tan rápido como la tecnología. Bogotá. Recuperado de internet el 05/08/2015 en http://colombia-inn.com.co/fraude-electronico-crece-y-cambia-de-cara-tan-rapido-como-la-tecnologia/
- Ernst & Young. (2011). Seguridad de la información en un mundo sin fronteras Es momento de replantear el tema. Recuperado de internet el 21/05/2015 de http://www.ey.com/Publication/vwLUAssets/Seguridad_de_la_informacion_en_un_mundo_sin_fronteras/$FILE/Seguridad_de_la_informacion_en_un_mundo_sin_fronteras.pdf
- García, A., Joaquín. (s.f.). Ataques contra redes TCP/IP. Recuperado de internet el 21/05/2015 en http://ocw.uoc.edu/computer-science-technology-and-multimedia/advanced-aspects-of-network-security/advanced-aspects-of-network-security/P06_M2107_01769.pdf
- Guzmán A., Clara. (2009). Contextualización del cibercrimen en Colombia. Inventum No. 7 Facultad de Ingeniería Uniminuto. Recuperado de internet el 21/05/2015 de http://biblioteca.uniminuto.edu/ojs/index.php/Inventum/article/download/130/123
- INTECO. (s.f.). ¿Qué son los APT's?. Cuaderno de notas del observatorio. Madrid: 11p.

- InternetLab. (2013). Protocolo SET. El Protocolo de Seguridad en las transacciones electrónicas. Recuperado de internet el 21/03/2016 de http://www.internetlab.es/post/2640/protocolo-set/
- Isfahani, A. y Mircholi, A. (2013). A study of the effect of E-Bank service on E-trust: An E-security approach. Séptima conferencia internacional del comercio en línea en países en desarrollo con énfasis en la seguridad. 17(18). Irán: 10p.
- Koike, Y. (2015). An advanced electronic payment system to support enhanced service provision. NEC Technical Journal. 10(1). 42-45p.
- KPMG. (2013). Encuesta de fraude en Colombia 2013.
- Laverde Palma, J.D. (2014). El Millonario fraude al BBVA. El Espectador. Publicado el 24 de octubre. Recuperado de internet el 08/08/2015 en http://www.elespectador.com/noticias/judicial/el-millonario-fraude-al-bbva-articulo-524960
- Lee, J. Bauer, L. and Mazurek, M. (2015). The effectiveness of security images in internet banking. IEEE computer society. 1089-780I. 54-62p.
- Ley 1273 de 2009 Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. . Senado de la República de Colombia. Recuperado de internet el 21/05/2015 de http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html
- Mayorga, D. (2014). La vigencia del fraude bancario. El Espectador. Publicado el 8 de enero de 2014. Recuperado de internet el 09/08/2015 en http://www.elespectador.com/noticias/temadeldia/vigencia-del-fraude-bancario-articulo-467550
- Mazón, C., Cristina y Pereira P. (s. f.). Las tecnologías de Internet y las empresas: riesgos y oportunidades. Cuarto Congreso de Economía de Navarra. (s. f.). Recuperado de internet el 21/05/2015 de

http://www.navarra.es/NR/rdonlyres/A9E2F1DC-194F-42CE-A9F5-C8AF054D34AD/79802/cristina.pdf

- Mifsud, E. (2012). Introducción a la seguridad informática. Ministerio de educación, cultura y deporte. Madrid: España.
- Norton. (Octubre de 2013). Reporte Norton 2013. Symantec. 28p.
- Ojeda-Pérez, Jorge Eliécer, Rincón-Rodríguez, Fernando, Arias-Flórez, Miguel Eugenio, & Daza-Martínez, Libardo Alberto. (2010). Delitos informáticos y entorno jurídico vigente en Colombia. Cuadernos de Contabilidad, 11(28), 41-66. Recuperado de internet el 21/05/2015 de http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003&lng=en&tlng=es
- Pando M., Z. (2008). Ataques Ddos. Recuperado de internet el 21/03/2016 de http://es.kioskea.net/contents/attaques/dos.php3
- Pecoy, M. (2012). Delitos informáticos. Montevideo: universidad de Montevideo.
- Prandini Patricia y Maggiore Marcia.. (2011). Registro de Direcciones de Internet para Latinoamérica y el Caribe (LACNIC) Centro Internacional de Investigaciones para el Desarrollo (IDRC) Proyecto Amparo Panorama del ciberdelito en Latinoamérica. Recuperado de internet el 21/05/2015 de http://www.proyectoamparo.net/files/LACNIC-PanoramCiberd-VsFinal-20110701.pdf
- Rodríguez, A. (2012). Ahora la lucha es contra los ciberdelitos. Un informe de Colombia digital. 15 de febrero de 2012. Recuperado de internet el 08/08/2015 en http://colombiadigital.net/opinion/columnistas/cuestion-de-voltaje/item/1417-ahora-la-lucha-es-contra-los-ciberdelitos.html
- Salellas, L. (2013). Cabinas. Obtenido de Delitos informáticos - ciberterrorismo: http://www.cabinas.net/informatica/delitos_informaticos.asp

- Santa María, B., E. (s.f.) Delitos informáticos. CCIT. Recuperado de internet el 07/08/2015 en http://www.ccit.org.co/files/SEGURIDAD%20INFORMATICA/Delitos_Informaticos.pdf
- Serna, C.M. (2011). Clonación de tarjetas pone en jaque los bancos. El país S.A. Cali. Recuperado de internet el 09/08/2015 en http://www.elpais.com.co/elpais/judicial/clonacion-tarjetas-pone-en-jaque-bancos
- Taringa (2013). Tipos de Malwares. Recuperado de internet el 21/03/2016 de http://www.taringa.net/post/ciencia-educacion/17180999/Tipos-de-Malwares.html Lazalde, A. (2013). DDoS: qué es y cómo se ve este ataque informático. Diario Turing. Informática. España.
- Temperini, M., Gabriel. (s. f.). Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. 1ra. Parte. Doctorado en Derecho en la Facultad de Ciencias Jurídicas y Sociales de la Universidad Nacional del Litoral. Recuperado de internet el 21/05/2015 de http://conaiisi.frc.utn.edu.ar/PDFsParaPublicar/1/schedConfs/2/82-553-1-DR.pdf
- Universidad Nacional Abierta y a Distancia [UNAD]. (2011). Criptografía: lección 26: Características del protocolo SSL. Recuperado de internet el 21/03/2016 de http://datateca.unad.edu.co/contenidos/233011/233011Exe/leccin_26_caractersticas_del_protocolo_ssltls.html
- Villadiego, R. (2015). Mr. Robot Shows Art Imitating Life – And It's Not Sweet as Pi. Recuperado de internet el 18/04/2016 de http://newblog.easysol.net/mr-robot/
- Websense. (2008). Un libro blanco de Websense. Protección de la información esencial Garantizar la seguridad de los cimientos de su plataforma comercial en Internet. Recuperado de internet el 21/05/2015 de http://www.bltcolombia.com/pdf/DLP.pdf
- Ziv. (2012). What is PKI. Recuperado de internet el 21/05/2015 de http://software-engineer-tips-and-tricks.blogspot.com.co/2012/09/what-is-pki.html

FIRMA ESTUDIANTES _____

VIVIANA GARCIA

ALESSANDRO RINCON L.

FIRMA ASESOR _____ 25/10/2016

FECHA ENTREGA: _____

FIRMA COMITÉ TRABAJO DE GRADO DE LA FACULTAD _____

_____

RECHAZADO_____ ACEPTADO____ ACEPTADO CON MODIFICACIONES_____

ACTA NO._____

FECHA ENTREGA: _____

FIRMA CONSEJO DE FACULTAD_____

ACTA NO._____

FECHA ENTREGA: ____ _____