CLONACIÓN DE TARJETAS DE CREDITO

Trabajo realizado por:

LUISA MARÍA ROLDAN

LINA MARÍA RINCÓN

DUVAN ARLEY TABORDA

TECNOLÓGICO DE ANTIOQUIA INSTITUCIÓN UNIVERSITARIA

FACULTAD DE CIENCIAS ADMINISTRATIVAS Y ECONÓMICAS

PRÁCTICA ADMINISTRATIVA

MEDELLÍN

2017

CLONACIÓN DE TARJETAS DE CREDITO

Por:

LUISA MARÍA ROLDAN

LINA MARÍA RINCÓN

DUVAN ARLEY TABORDA

Asesor

NAIRO DURANGO RODRIGUEZ

TECNOLÓGICO DE ANTIOQUIA INSTITUCIÓN UNIVERSITARIA

FACULTAD DE CIENCIAS ADMINISTRATIVAS Y ECONÓMICAS

PRACTICA ADMINISTRATIVA

MEDELLÍN

2017

Tabla de Contenido

Introducción

Este trabajo se constituye como un compendio de elementos teóricos que se dirigen todos ellos, a la investigación y comprensión de los diversos problemas de fraude presentados a nivel nacional, como una realidad inherente en nuestra sociedad y que trae consigo consecuencias a las personas, la importancia de este trabajo es realizar una investigación acerca de este tipo de acontecimientos presentados en el ámbito bancario.

Su objetivo principal es dar a conocer y analizar la problemática actual en materia de fraudes por clonación de tarjetas ya que en la actualidad es un problemática de interés nacional que afecta a gran cantidad de persona que utiliza los medios electrónicos.

La investigación de esta problemática se realizó por el interés de los integrantes del grupo, en conocer las maneras de realizar fraude y la desinformación de las personas con respecto a este tema y así tener una proyección enfocada al proceso de seguridad llevado por los bancos para minimizar este tipo de sucesos.

En este trabajo se visualiza una realidad que se vive en nuestra ciudad y todo nuestro país con respecto a los fraudes realizados directamente como clonación de las tarjetas de entidades bancarias y afectan directamente la economía de los colombianos por las pérdidas de dinero como consecuencia de este hecho lamentable.

La característica principal de este tipo hechos es que se puede realizar de la manera más simple sin que la persona lo note, en ocasiones por tener un exceso de confianza la cual tiene mucho que ver con nuestra cultura o por desconocimiento de este tipo de practicas

Clonación de Tarjetas de Crédito

1.Identificación del proyecto

1.1. Tema general de la investigación

Clonación de tarjetas de crédito en el sector financiero.

1.2. Tema específico de la investigación

Se enfoca dentro del sector financiero en los bancos (Bancolombia y Banco de Bogotá) para generar unas alertas que puedan ser útiles frente al riesgo de las tarjetas de crédito.

1.3. Definición del problema de investigación

Se puede establecer que los impactos generados por temas de clonación de tarjetas de créditorepercuten en la economía Nacional e Internacional. El fraude es conocido a nivel mundial y mucho más en el sector bancario, la clonación es un método utilizado por medio del cual a la persona le realizan compras o pagos personas no autorizadas o sin tener la tarjeta física original; solo basta con pasar la tarjeta por tarjeta de banda magnética por un dispositivo el cual realiza un registro de la información y puede ser usada otra tarjeta que tiene la persona que realiza el fraude, esto ocurre en situaciones de la vida diaria como compras en centros comerciales, hoteles, restaurantes, etc. Muchas veces con la ayuda del empleado del lugar o en ocasiones por inocencia o por exceso de confianza al revelar las claves.

En el 2015 los bancos colombianos por concepto de riesgo de su operación perdieron $122.000.000 del cual un 70% corresponde a operaciones que el cliente desconoce siendo un posible fraude y el banco decide reconocer.

(El Tiempo, 2016)

En La actualidad este fenómeno tiende a aumentar ya que aún hay vulnerabilidades en las operaciones virtuales. Los bancos tratan de combatir con mecanismos biométricos y toquen que facilitan el proceso de autenticación de forma más segura.

El problema es de carácter nacional e internacional debido a falta de control y seguridad por parte de los bancos y otras por falta de conocimiento, exceso de confianza e inocencia del victimario.

1.4 Definición del espacio de investigación

El uso de las tarjetas de crédito ha adquirido valor y relevancia con el paso del tiempo, a futuro será el principal medio de pago, desplazando de una manera considerable al dinero en efectivo.

El uso de las tarjetas de crédito no está exento de tener problemas, casos comunes que podemos ver a simple vista como los fraudes, hurto, pérdida o delitos virtuales.

La seguridad de las tarjetas de crédito no solo hace referencia a una seguridad física asumiendo que si porto la tarjeta conmigo no tendría inconvenientes, se debe ir mas allá y conocer que existe la posibilidad de captación de datos, alteración de operaciones y demás formas de realizar un proceso indebido con este dinero plástico.

Las entidades bancarias deben buscar resultados efectivos a corto y largo plazo con medidas de seguridad que permita disminuir los actos de clonación de tarjeta y fraudes electrónicos, objetivos comunes que deberían aplicar no uno sino una unión de bancos buscando siempre proteger a las personas que hacen uso de sus tarjetas y sobre los cuales se debe velar por una seguridad sobre sus productos.

El gobierno es un aliado de las entidades bancarias para este tipo de delitos informáticos sobre los cuales existen leyes que permiten castigar a los responsables, de ahí la importancia de la ley que adiciona al Código Penal colombiano el Título VII BIS denominado "De la Protección de la información y de los datos" buscando una disminución de este tipo de abuso.

1.5. Población

La población en general es el sector financiero colombiano incluyendo personas naturales y jurídicas. La muestra se toma de los usuarios y/o consumidores de tarjetas de crédito en los bancos, banco de Bogota y Bancolombia.

1.6. Revisión de antecedentes

Para poder hablar de la clonación de tarjetas de crédito es necesario inevitablemente conocer la historia y su evolución a través del tiempo donde los avances tecnológicos día a día encaminan a utilizar este medio de pago como el de más uso por encima de otros medios de pago.

En el año 1958 Nace la primera tarjeta, denominada Bank Americard, que fue emitida por el Bank of América. En 1969 Nace la primera tarjeta de crédito en Colombia, cuando el Banco de Bogotá inició negociaciones con el Bank of América. Esta asociación iniciaría operaciones formalmente en 1970, después de esto, en 1971, con el fin de optimizar la administración y coordinar las funciones de tarjetas de crédito, se creó la asociación bancaria Credibanco.

(credibanco, SF)

En 1976 Credibanco adoptaría la denominación del nombre universal de la tarjeta de crédito, designándose en ese entonces como Credibanco Visa para Colombia, organización que une esfuerzos con los cinco bancos más importantes del momento: Banco de Colombia, Banco de Bogotá, Banco Cafetero, Banco Ganadero y Bancoquia . Esta unión fortaleció la presencia de las tarjetas Visa en Colombia, y garantizó, de entrada, un gran respaldo para su tarjeta Visa Clásica, primer producto puesto en el mercado comercial nacional.

1984: hacen su aparición los primeros datafonos en Colombia, dando nacimiento a la red de P.O.S. de Credibanco. Estos causaron revolución por su innovación tecnológica, y estaban exclusivamente para uso con tarjetas Visa. Estos datafonos simplemente autorizaban la transacción. En principio la red de datafonos fue llamada Credibanco Veloz, luego Servicio Electrónico hasta llegar a su nombre actual Credibanco es su Red, con el lema "Acepto Todas"

El primer datafono fue instalado en el restaurante O Sole Mío en Bogotá, y esa misma noche fue puesto a prueba. Un italiano fue quien por primera vez pasó su tarjeta a través de la novedosa tecnología que se estrenaba en Colombia.

Las primeras autorizaciones eran recibidas vía telefónica por un grupo de 30 operarias instaladas en un gran salón. Cada una de ellas transcribía la autorización a mano y la pasaba al

banco, que la enviaba al exterior a través del télex y el autotélex, tardándose hasta 5 días en obtener respuesta, tiempo que el usuario tenía que esperar para reclamar su compra. En la actualidad la misma operación tarda apenas 5 segundos.

2. Análisis del problema de investigación

2.1 Planteamiento o descripción del problema

Dentro del sector financiero las Tarjetas de Crédito son un producto de mayor impacto para los usuarios y/o consumidores, ya que es una modalidad de dinero plástico y cuenta con varias ventajas a la hora del manejo y el riesgo ante el fraude o robo de las mismas, sin embargo se han venido presentado diferentes casos de corrupción o problemáticas en la clonación de estos productos, en los bancos Bancolombia y Banco de Bogotá realizan estudios y desarrollan diferentes alternativas sobres estos riesgos, debido a que en su razón de ser esta fundamentalmente el cuidado y protección de la información financiera de todos y cada uno de sus usuarios.

¿Qué resultado puede obtenerse al realizar una relación entre, la cantidad de usuarios y/o consumidores afectados por este fenómeno de clonación de tarjetas de crédito y las diferentes alternativas de los bancos?

¿Qué contribución han hecho los diferentes entes financieros, frente a la latente de las clonaciones en las tarjetas de crédito vinculadas a los mismos?

2.2 Preguntas orientadas al proceso investigativo

2.2.1. Pregunta general

¿Cuál es la responsabilidad que tienen los bancos, sus soluciones y respaldo frente un cliente es víctima de fraude por clonación?

2.2.2.Preguntas específicas

¿De las personas que fueron objeto de fraude en que porcentaje el banco dio favorabilidad y le respondió al cliente por su dinero?

¿Por qué las tarjetas de crédito son los productos con mayor adquisición y de mejor productividad para estas dos entidades financieras?

¿Cuál ha sido el crecimiento de esta modalidad de dinero plástico, en las entidades financieras Bancolombia y Banco de Bogotá con referencia al fraude que se presenta en las mismas?

3. Objetivos

3.1 Objetivo general

Establecer las principales técnicas para evitar vulnerar los usuarios de tarjetas de crédito en el sistema financiero, brindar estrategias para evitar ser víctimas del delito de clonación.

3.2 Objetivos específicos

- Ofrecer a los usuarios de Bancolombia y Banco de Bogotá unas prácticas permanentes que deban seguir para evitar este delito.

- Identificar los equipos con los que se pueden realizar clonaciones de una tarjeta de crédito.

- Determinar los principales métodos para la clonación de una tarjeta de crédito.

- Proponer a Bancolombia y banco de Bogotá la realización de campañas para evitar clonación de tarjetas de crédito.

- Identificar la reacción de los usuarios que han sufrido la clonación de tarjetas de crédito.

4. Justificación

Con este proyecto se desea investigar y analizar los diferentes comportamientos y afectaciones que se presentan en un delito informático como lo es la clonación de tarjetas de crédito. Desde allí identificar como pueden estos percances afectar a los ciudadanos, que en general enfrentan una inexperiencia con relación a aspectos económicos que impactan en la sociedad, donde el conocimiento es básico en temas de fraude y así poder evitar de cierta manera este fenómeno mundial.

La finalidad principal es tener conocimientos de cómo funciona este delito y recomendaciones para evitar ser víctima de este hecho económico que golpea la sociedad, el entendimiento de los delitos informáticos y formas de contrarrestar la situación permitirá a los

usuarios ser menos vulnerables a estar circunstancias negativas presentadas en la parte bancaria y el uso del dinero plástico, entender los procedimientos a seguir en caso de ser estafados y la ley que nos cobija en una circunstancia como esta.

5. Marco referencial

5.1Marco teórico

La clonación de tarjeta también conocida como "skimming" es un tipo de fraude por medio del cual se duplican tarjetas y así realizar transacciones y retiros sin la autorización del titular de la cuenta. Esta modalidad de delitoocurre tanto en cajeros automáticos como en establecimientos comerciales o restaurantes. Los delincuentes pueden cargar consigo un dispositivo conocido como 'skimmer', que les permite leer la banda magnética tan solo con deslizarla por una ranura.

Otra modalidad conocida de clonación se da por medio de la instalación de ese dispositivo sobre el lector del cajero automático, con el cual crean un lector falso para robar sus datos. Una vez consiguen la información, la graban en una tarjeta nueva y obtienen su contraseña por medio de cámaras que instalan en los cajeros o por una persona que simula ser un cliente del cajero y observa cuando la víctima digita la clave.(El tiempo, 2016)

Este tipo de fraude es un método inmediato; en un segundo la información de la banda magnética de la tarjeta es copiada, lo que hace que las personas no se enteren hasta que realizan otra transacción en su cuenta

El duplicado de la información se puede presentar en cualquier establecimiento donde los malhechores manipulan los dispositivos simulando la ranura en la cual se introduce la tarjeta.

Según el gremio representativo del sector financiero colombiano, Asobancaria, esto lo hacen gracias a la manipulación de los datafonos y cajeros, en muchas ocasiones con la complicidad del empleado del lugar donde pasan la tarjeta que puede ser un dispositivo diminuto que permite el copiado de la información de la víctima.

Como usuario bancario y víctima de este fraude usted cuenta con dos vías inmediatas, según Juan Fernando Celi, defensor del consumidor financiero del grupo Bancolombia: la primera es acudir con urgencia a la entidad bancaria a la cual se encuentra afiliado y la segunda, consultar directamente con la Superintendencia Financiera en el departamento de protección al consumidor financiero, para que esas entidades empiecen con la investigación pertinente. Luego, es aconsejable que el usuario se dirija a la Policía Nacional para poner la denuncia (con la documentación que le proporcionó el banco) y así empezar una investigación paralela que puede ser dispendiosa y demorada.

La entidad bancaria después de conocer el caso por parte de sus clientes comienza la respectiva investigación donde determinan la culpabilidad del usuario como (descuido de su clave, ayuda de terceros en la transacción) o si por el contrario fue víctima de fraude. Dependiendo del resultado de esta indagación los bancos reconocen parcial o totalmente el valor hurtado.

Los bancos pueden utilizar toda la tecnología que tienen disponible para la seguridad de sus clientes pero si los usuarios no están enterados de estos tipos de robos y presentan descuido con sus claves no tendrían derecho a reclamación alguna.

Para que exista un fraude en la clonación de tarjeta es necesario que se duplique la información de la banda magnética y que se obtenga la clave, con estos datos se realiza el defalco en la cuenta de la víctima.

Existen 2 tipos de tarjetas, las tarjetas débito y las tarjetas de crédito en ambos casos el delincuente lo que busca es la clave o pin bien sea para realizar pagos en establecimientos, compras a través de internet o avances en efectivo

Como da a conocer el portal Finanzas Personales, "en Colombia 4,3 millones de personas están expuestas a este delito gracias al uso de la banca online".

En Colombia no existe una norma que obligue a los bancos a tener un seguro contra este tipo de delito, esto se debe a que el fraude no se realiza propiamente al banco sino a la persona portadora de la tarjeta y el uso que se le dé es responsabilidad exclusiva del cliente.

A pesar de esto tanto Bancolombia como el banco de Bogota tiene un seguro todo riesgo donde cubren el uso indebido o utilización fraudulenta de la tarjeta generada por una tercera persona no autorizada, las personas por lo general no tienen conocimiento de este seguro y el uso que pueden darle en caso de ser víctimas de este delito aunque para que el banco asuma el seguro deben hacer la investigación correspondiente dentro de los plazos estipulados y con la documentación requerida para este tipo de trámite.

Asobancaria, señala que durante los últimos años se han realizado inversiones cuantiosas para la banca en cuanto a la instrumentación de medidas constantes que ayudan a mitigar el riesgo de fraude a través de tarjetas débito o crédito. Se estima que este valor se aproxima a más de 150'000.000 de dólares que se invierten en mecanismos para realizar las transacciones de manera más segura.

Particularmente, en cuanto a la clonación, los bancos han desarrollados medidas como:

1) Emisión de algunos tipos de tarjetas con tecnología EMV (conocida como tarjeta chip)

2) Instalación de dispositivos antiskimming en los cajeros (o ATM)

3) Instalación de cámaras en cajeros asociados con cada transacción.

4) Información en línea (a través de mensaje de texto o correo electrónico) sobre las transacciones realizadas.

5) Capacitaciones a establecimientos comerciales para el debido uso de las tarjetas en los datafonos.

6) Campañas comunicacionales a los clientes para que tomen las debidas precauciones en el momento de realizar sus transacciones.(Semana, 2012)

Si se tienen varias denuncias sobre un cajero en específico o algún establecimiento público donde informen un posible fraude los bancos abren una investigación para identificar cual es el método utilizado en dicho suceso y tomar los correctivos necesarios para evitar esta fuga de información.

Al final con los resultados obtenidos en la investigación se da a conocer sobre quien recae la responsabilidad y cuáles son las medidas a tomar para reestablecer lo perdido a los usuarios.

Por parte de la policía Nacional también se realizan ciertas recomendaciones para evitar ser víctima de este tipo de fraudes el cual se presenta en diferentes situaciones y modalidades. (Centro Cibernetico Policial, S.F.)

En cajeros electrónicos

- validar que no exista ningún aparato instalado en la ranura de ingreso de la tarjeta de crédito.
- Al realizar un pago con debito no perder de vista la tarjeta en ningún momento y validar que si sea la tarjeta con los datos propios.
- Nunca aceptar ayuda de extraños
- No confiar en la amabilidad de un desconocido al realizar una transacción
- En lo posible oculte la clave al digitarla
- Si detecta alguna anomalía informar a la entidad correspondiente o a la policía nacional

En restaurantes o estaciones de gasolina

- Realizar la operación de manera personal y no permitir que la realice un tercero
- Cubra el teclado del dispositivo al momento de digitar la clave
- Este alerta de que su tarjeta solo sea deslizada una vez por el dispositivo y verifique cuando la devuelvan que si sea la suya
- No arroje a la basura los comprobantes de pago donde estén registrados los datos personales.

5.2 Marco legal

Protección al Consumidor

Los Bancos Bancolombia y Banco de Bogotá cuentan con mecanismos que dan tranquilidad y seguridad a todos sus clientes. Entre estos se encuentra.

La Ley de protección: Ley 1328 de 2009 que es el régimen de protección al consumidor financiero.(Banco de Bogota, S.F.)

El presente régimen tiene por objeto establecer los principios y reglas que rigen la protección de los consumidores financieros en las relaciones entre éstos y las entidades vigiladas por la Superintendencia Financiera de Colombia, sin perjuicio de otras disposiciones que contemplen medidas e instrumentos especiales de protección.

Funciones de esta ley.

A) Atender de manera oportuna y efectiva a los consumidores financieros de las entidades correspondientes.

b) Conocer y resolver en forma objetiva y gratuita para los consumidores, las quejas que estos le presenten, dentro de los términos y el procedimiento que se establezca para tal fin, relativas a un posible incumplimiento de la entidad vigilada de las normas legales, contractuales o procedimientos internos que rigen la ejecución de los servicios o productos que ofrecen o prestan, o respecto de la calidad de los mismos.

c) Actuar como conciliador entre los consumidores financieros y la respectiva entidad vigilada en los términos indicados en la Ley 640 de 2001, su reglamentación, o en las normas que la modifiquen o sustituyan. Para el efecto, el consumidor financiero y la entidad vigilada

podrán poner el asunto en conocimiento del respectivo Defensor, indicando de manera explícita su deseo de que el caso sea atendido en desarrollo de la función de conciliación. Para el ejercicio de esta función, el Defensor deberá estar certificado como conciliador de conformidad con las normas vigentes.

El documento en el cual conste la conciliación realizada entre la entidad vigilada y el consumidor financiero deberá estar suscrito por ellos y el Defensor del Consumidor Financiero en señal de que se realizó en su presencia, prestará mérito ejecutivo y tendrá efectos de cosa juzgada, sin que requiera depositarlo en Centro de Conciliación. El incumplimiento del mismo dará la facultad a la parte cumplida de hacerlo exigible por las vías legales respectivas.

d) Ser vocero de los consumidores financieros ante la respectiva entidad vigilada.

e) Efectuar recomendaciones a la entidad vigilada relacionadas con los servicios y la atención al consumidor financiero, y en general en materias enmarcadas en el ámbito de su actividad.

f) Proponer a las autoridades competentes las modificaciones normativas que resulten convenientes para la mejor protección de los derechos de los consumidores financieros.

g) Las demás que le asigne el Gobierno Nacional y que tengan como propósito el adecuado desarrollo del SAC.

También cuentan con más leyes que los adoptan para la penalización de dichos fraudes.

La Ley 1273 de 2009 creó nuevos tipos penales relacionados con delitos informáticos y la protección de la información y de los datos con penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes

El 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 “Por medio del 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”.

Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que las empresas se blinden jurídicamente para evitar incurrir en alguno de estos tipos penales.

No hay que olvidar que los avances tecnológicos y el empleo de los mismos para apropiarse ilícitamente del patrimonio de terceros a través de clonación de tarjetas bancarias, vulneración y alteración de los sistemas de cómputo para recibir servicios y transferencias electrónicas de fondos mediante manipulación de programas y afectación de los cajeros automáticos, entre otras, son conductas cada vez más usuales en todas partes del mundo. Según la Revista Cara y Sello, durante el 2007 en Colombia las empresas perdieron más de 6.6 billones de pesos a raíz de delitos informáticos.

De ahí la importancia de esta ley, que adiciona al Código Penal colombiano el Título VII BIS denominado "De la Protección de la información y de los datos" que divide en dos capítulos, a saber: “De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos” y “De los atentados informáticos y otras infracciones”.

- Artículo 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático

protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269C: INTERCEPTACIÓN DE DATOS INFORMÁTICOS. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

- Artículo 269F: VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Al respecto es importante aclarar que la Ley 1266 de 2008 definió el término dato personal como "cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica". Dicho artículo obliga a las empresas un especial cuidado en el manejo de los datos personales de sus empleados, toda vez que la ley obliga a quien "sustraiga" e "intercepte" dichos datos a pedir autorización al titular de los mismos.

- Artículo 269I: HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239[3] manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 del Código Penal[4], es decir, penas de prisión de tres (3) a ocho (8) años.

Así mismo, la Ley 1273 agrega como circunstancia de mayor punibilidad en el artículo 58 del Código Penal el hecho de realizar las conductas punibles utilizando medios informáticos, electrónicos ó telemáticos.

Como se puede apreciar, la Ley 1273 es un paso importante en la lucha contra los delitos informáticos en Colombia, por lo que es necesario que se esté preparado legalmente para enfrentar los retos que plantea.

En este sentido y desde un punto de vista empresarial, la nueva ley pone de presente la necesidad para los empleadores de crear mecanismos idóneos para la protección de uno de sus activos más valiosos como lo es la información. (Gandini, Isaza, & Delgado, s.f.)

6. Sistema de hipótesis y variables

6.1 Hipótesis de trabajo

Los señores Juan Fernando Celi Munera, y Alejandro de Jesús Gómez Montoya defensores del consumidor financiero del grupo Bancolombia y Banco de Bogotá nos presentan la siguiente información

La primera es acudir con urgencia a la entidad bancaria a la cual se encuentra afiliada.

La segunda es consultar directamente con la superintendencia financiera en el departamento de protección al consumidor financiero, para q esas entidades empiecen con la investigación pertinente.

Luego es aconsejable que el usuario se dirija a la Policía Nacional para poner la denuncia (Con la documentación que le proporciono el banco) y así empezar una investigación paralela que puede ser dispendiosa y demorada.

Después de dar a conocer el caso, la entidad bancaria inicia la investigación correspondiente para determinar si el cliente fue víctima del copiado de banda o perdió la confidencialidad de sus datos (por ejemplo al descuidar su clave). Los tiempos de respuesta al cliente afectado varían de acuerdo con la investigación del caso, y dependiendo de los resultados de la pesquisa se determina si hay lugar o no a reclamaciones y así a un reintegro total o parcial del dinero.

Según Asobancaria, si se tienen constantes denuncias de algún cajero o sitio comercial en específico tachado por ese tipo de fraude, generalmente se abre un proceso de investigación con el fin de identificar el medio de fuga de la información.

Se debe tener en cuenta que este fraude es más común de lo que usted se imagina y no existe norma que obligue al banco a responder por su dinero.

6.2 Variables utilizadas

Definición conceptual

Clonaciones de tarjetas de crédito: Esta variable se refiere al porcentaje de usuarios que han sido víctimas de clonaciones de las tarjetas de crédito.

Tipos de clonaciones de tarjetas de crédito

- Clonación – online y física
- Robo de identidad
- Phis Hing - (engaño informático)
- Hacking - (persona de robo de información)
- Smishing (estafa informática)

Importancia de la tarjeta de crédito

Esta variable consiste en determinar la importancia que los usuarios dan a la tarjeta de crédito en función de las ventajas y beneficios que esta ofrece.

7. Diseño metodológico

7.1 Método de investigación utilizado

La presente investigación tiene un enfoque Analítico, enfocado en un manejo descriptivo de las situaciones presentadas en casos de clonación de tarjetas, se desglosan los diferentes factores que intervienen en este delito, se pueden encontrar causas, naturaleza de la problemática presentada y por supuesto los efectos que tiene dicho indicador en la economía nacional.

7.2 Tipo de investigación

La investigación desarrollada es de tipo descriptivo, ya que, nuestro estudio realizado pretende conducir a la comprensión de un fenómeno como la clonación y el impacto generado en Colombia, se busca encontrar las causas que lo generan orientados y la identificación y el análisis de variables independientes y sus resultados, tratando de llegar a hechos verificables en nuestra investigación.

7.3 Fuentes de investigación

Las fuentes principales de información se basaron en la web, documentales de diferentes periodistas y las páginas de los bancos de Bogota y Bancolombia

7.4 Instrumento de aplicación

El instrumento de búsqueda utilizado fueron principalmente las bases de datos de Asobancaria, artículos de diferentes revistas y periódicos a través de estos mecanismos de búsqueda nos apoyamos de un abogado con amplia trayectoria en el sector financiero y actual Defensor del Consumidor Financiero del Grupo Bancolombia.

8. Tabulación y análisis de la información recopilada

Ilustración 1 Tiene o ha tenido productos financieros?

Se segmentó en personas que hayan tenido algún producto financiero ya que son los los más propensos a sufrir este tipo de delitos por tener o haber tenido algún producto, se puede constatar que el 100% de los encuestados han obtenido algún servicio financiero.

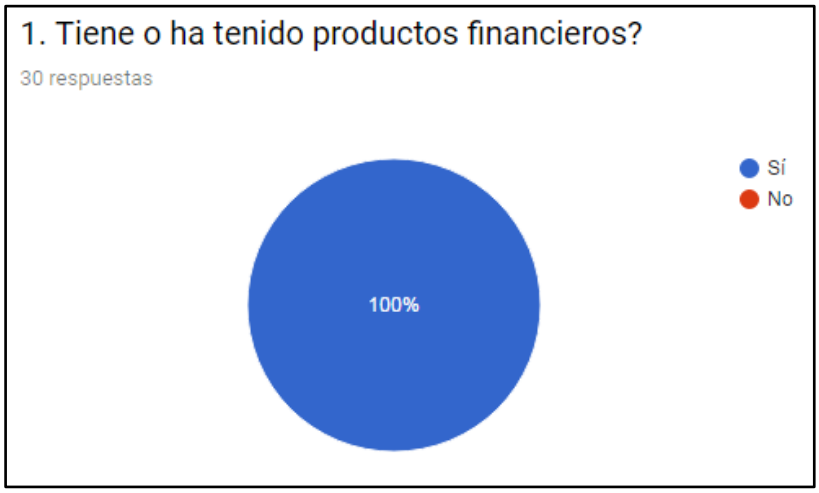


Ilustración 2 En que estrato vive usted?

Se conserva una relación directamente proporcional entre el estrato socioeconómico y el uso de tarjetas de credito

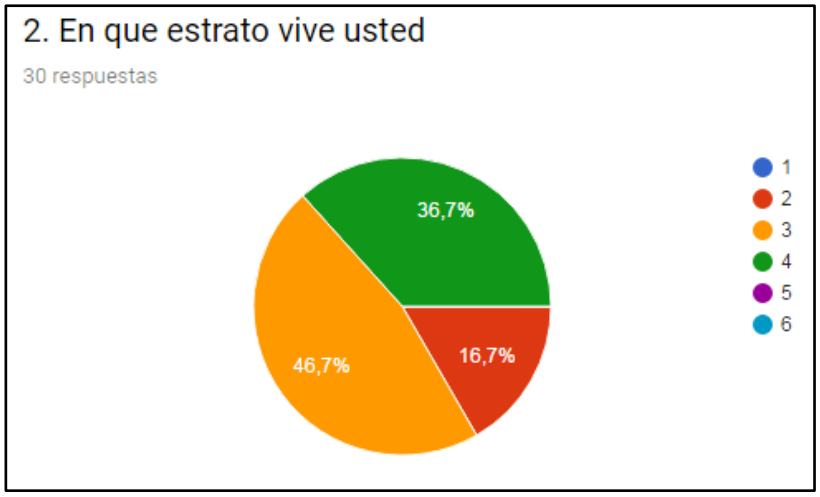


Ilustración 3 Tiene o ha tenido tarjetas de crédito?

El 100% de las personas que tiene un producto financiero ha tenido una tarjeta de crédito con alguna entidad.

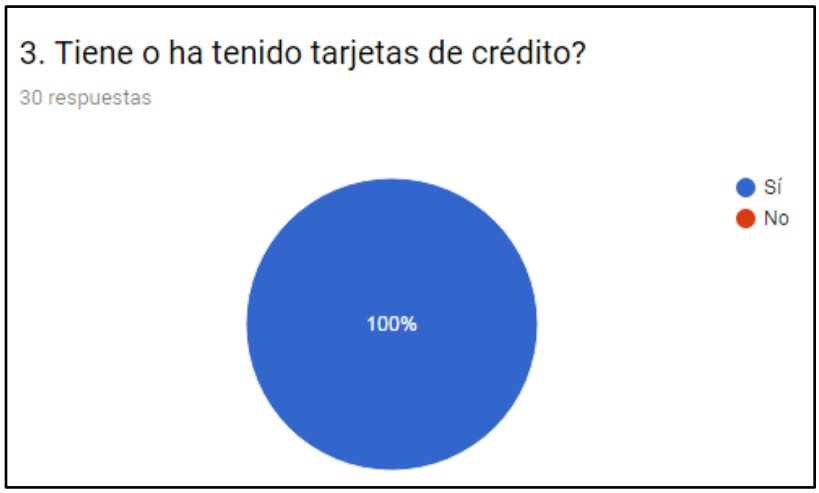


Ilustración 4 Con que entidad tiene o tuvo tarjeta de crédito?

Bancolombia es el que más aporta personas que han tenido o tiene tarjetas de crédito con un 63.3% Seguido de Davivienda con un 13.3% y banco de Bogotá con el 10%

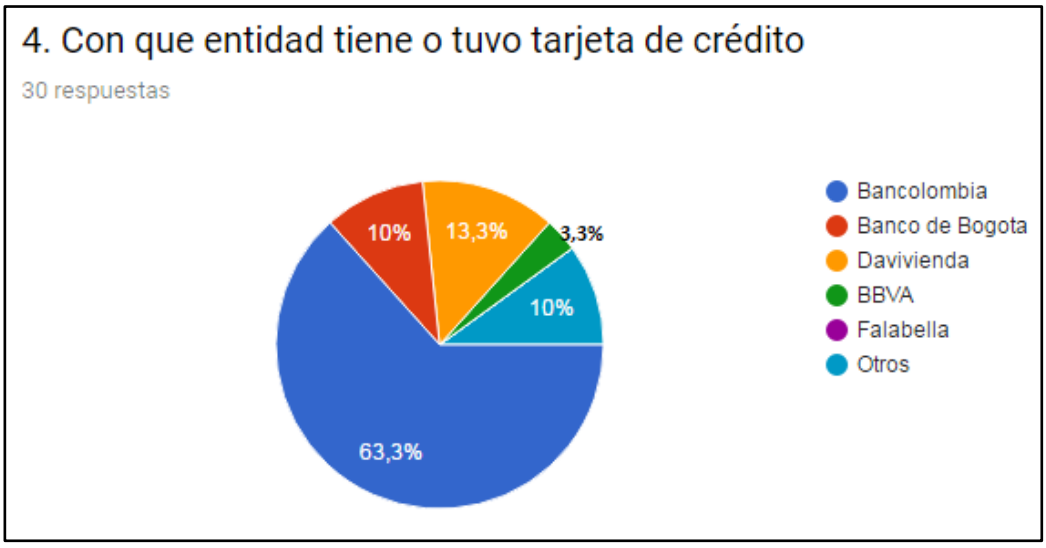


Ilustración 5 Conoce alguna de estas modalidades de fraude en tarjetas de crédito?

El mayor porcentaje de personas con un 40% conoce la clonación de tarjetas pero hay un 16% el cual no tiene conocimiento de ningún tipo de fraude y podría ser vulnerable a este delito.

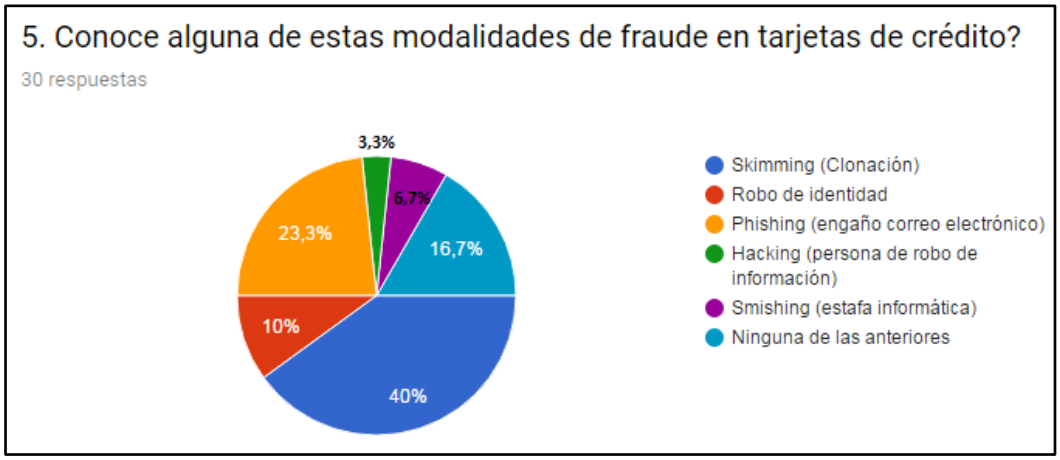


Ilustración 6 Usted tiene conocimiento de algún método para clonar una tarjeta de crédito?

A pesar de que la mayoría de personas conocen la clonación de tarjetas de crédito podemos validar que un alto porcentaje 63,3% no tiene conocimiento de cómo realizan la clonación siendo un punto crítico para los delincuentes realizar el fraude

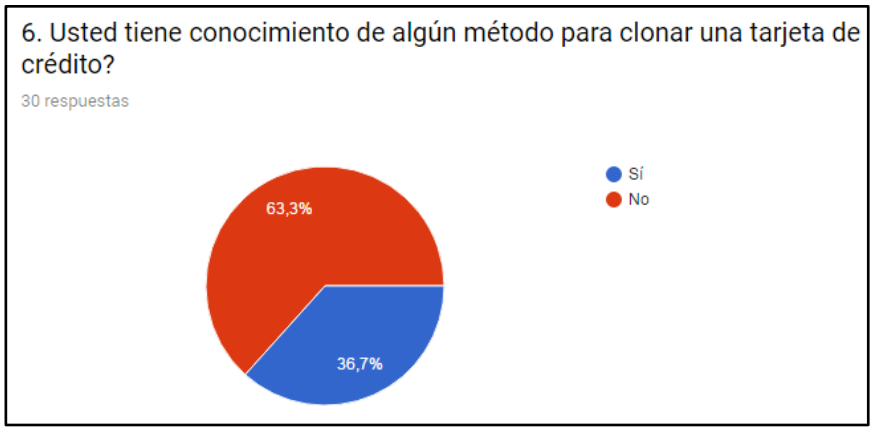


Ilustración 7 Algunas vez le han hecho un fraude en su tarjeta de crédito?

De las 30 encuestas realizadas solo 1 persona ha sido objeto de fraude en tarjetas de crédito con un 3,4%

Ilustración 8 Sabe que existen seguros especializados en fraudes financieros?

Más de la mitad de los encuestados con un 53,3% no conocen los seguros que ofrecen las entidades financieras para proteger su dinero en caso de un fraude, la cultura colombiana no muestra un poder adquisitivo con respecto a los seguros.

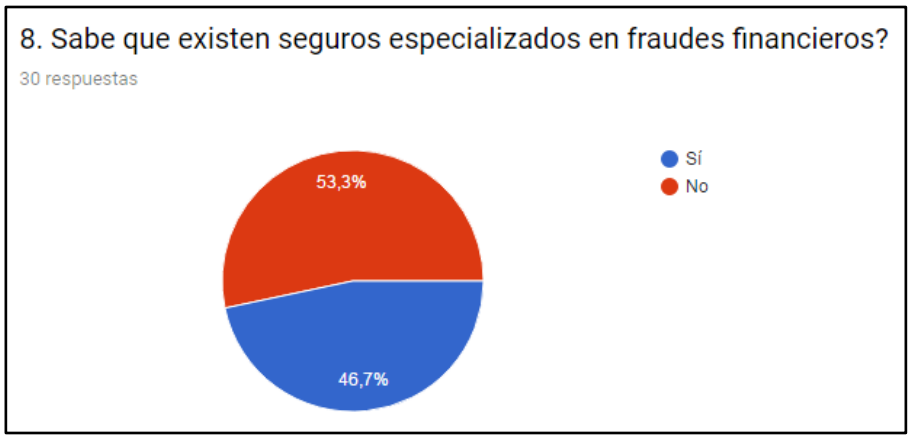


Ilustración 9 Qué tipo de precauciones tiene usted para evitar un fraude?

Las personas toman sus precauciones pero no todas las necesarias para evitar el fraude y aún falta concientizar ese 6,7% a ser precavido al momento de realizar estas transacciones para así disminuir las posibilidades de ser víctimas de este delito

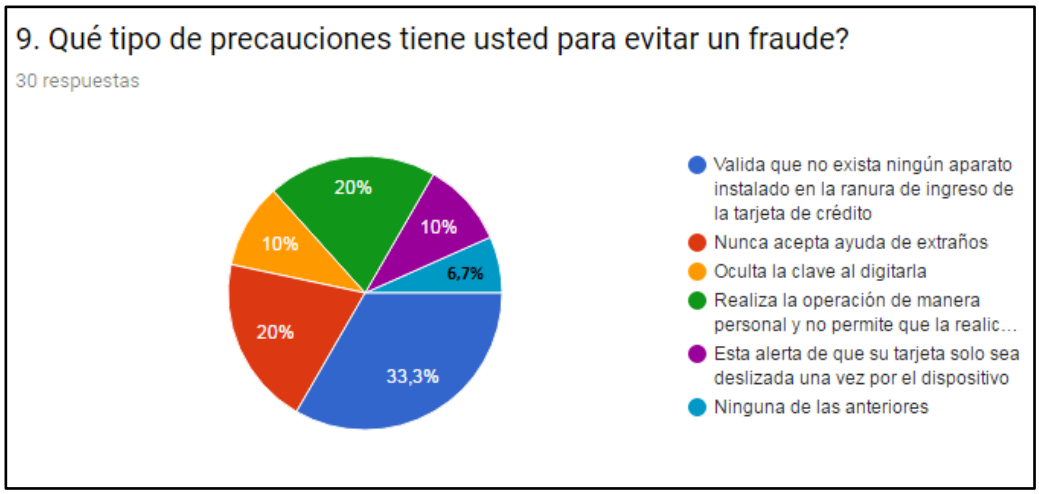
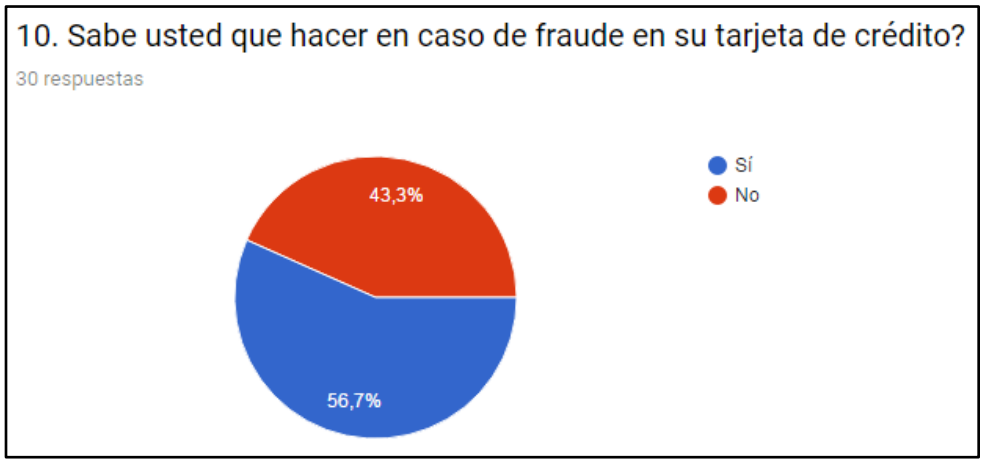


Ilustración 10 Sabe usted que hacer en caso de fraude en su tarjeta de crédito?

En un 43,3% las personas no saber qué proceso seguir si fueron víctimas de fraude, allí radica el hecho de que los bancos respondan por su dinero ya que como cliente debe seguir el debido proceso de reclamación correspondiente ante la entidad financiera.



9Conclusiones y recomendaciones

9.1 Conclusiones

Se puede concluir con esta investigación los posibles métodos utilizados para la clonación de tarjetas de crédito, como funciona este tipo de fraude y como podrían los usuarios disminuir este delito con algunas recomendaciones dado que es algo desconocido para muchos donde por exceso de confianza se puede llegar a caer en este desafortunado delito.

Se evidencia que los bancos en algunas ocasiones responden ante este tipo de situaciones no siempre son favorables para los clientes dado que como tal no se realiza directamente el

fraude al banco sino al portador de la tarjeta motivo por el cual la investigación se puede hacer algo extensa y difícil de probar.

Es claro la falta de información y sensibilización para que todas las personas estén enteradas de los métodos de clonación que existen y como prevenirlos, ya que actualmente las personas solo se interesan por el caso cuando les ocurre un suceso de estos o a algún familiar o persona de su entorno.

A pesar de que las entidades financieras invierten dinero en la seguridad de sus productos en este caso las tarjetas de crédito los delincuentes siguen burlando dicha seguridad de una u otra manera, es allí donde en conjunto con los demás bancos deben crear estrategias que permitan la disminución de las clonaciones.

9.2 Recomendaciones

Se le recomendaría a los bancos que realizaran campañas por medio de SMS masivos, volantes, en sus páginas web en la página principal, información visible las oficinas y difusión por medios televisivos donde se den recomendaciones acerca de cómo prevenir este delito.

Incentivar el cambio de la tarjeta por chip ya que es una tarjeta más segura que la de banda magnética y disminuiría el fraude por clonación además del envió del mensaje de texto al número celular del titular cada que se realice una operación así sea de un monto de poco valor para que así los usuarios estén enterados las 24 horas de los movimientos que se realizan con sus tarjetas y puedan realizar actuar proactivamente.

Bibliografía

Banco de Bogota. (S.F.). *Banco de Bogota*. Obtenido de https://www.bancodebogota.com/wps/portal/banco-de-bogota/bogota/atencion-al-cliente/proteccion-al-consumidor/ley-de-proteccion

Bancolombia. (S.F.). *Bancolombia.* Obtenido de https://www.grupobancolombia.com/wps/portal/personas/aprender-es-facil/seguridad/datafonos-cajeros-automaticos

Gandini, I., Isaza, A., & Delgado, A. (s.f.). *Delta asesores.* Obtenido de http://www.deltaasesores.com/articulos/autores-invitados/otros/3576-ley-de-delitos-informaticos-en-colombia#Ref1

Centro Cibernetico Policial. (S.F.). *Centro Cibernetico Policial*. Obtenido de https://caivirtual.policia.gov.co/

Semana (29 de mayo de 2016). ¿Quién responde por mi tarjeta clonada?. Semana. Recuperado de http://www.semana.com/noticias/articulo/quien-responde-tarjeta-clonada/258649-3

El tiempo (08 de marzo de 2016). Atento: así los delincuentes le pueden clonar sus tarjetas. El tiempo. Recuperado de http://www.eltiempo.com/archivo/documento/CMS-16531389

Credibanco. (S.F.). Credibanco. Obtenido de

https://www.credibanco.com/credibanco/historia

El tiempo (27 de abril de 2016). La banca y aseguradoras, en alerta por estafas con pagos por internet. El tiempo. Recuperado http://www.eltiempo.com/archivo/documento/CMS-16574145