PRINCIPALES CARACTERÍSTICAS, MODOS DE PERPETRACIÓN Y VULNERACIÓN DE LA SEGURIDAD INFORMÁTICA A TRAVÉS DE LA MODALIDAD CARDING.

JONATHAN DURAN PAMPLONA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA "UNAD"
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C, COLOMBIA
2020

PRINCIPALES CARACTERÍSTICAS, MODOS DE PERPETRACIÓN Y VULNERACIÓN DE LA SEGURIDAD INFORMÁTICA A TRAVÉS DE LA MODALIDAD CARDING.

JONATHAN DURAN PAMPLONA

MONOGRAFÍA

Proyecto de Grado para optar al título de:
Especialista en Seguridad Informática

Director de proyecto
MBA, Esp. CHRISTIAN ANGULO RIVERA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA "UNAD"
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C, COLOMBIA
2020

Nota de aceptación:

_____

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Bogotá D.C, Mayo 2020

A mi querida madre Patricia Eugenia quien con su apoyo y orientación logró encaminar mi futuro a lo que es hoy, a mi esposa Dayana Irene y a mi pequeña Ariana Sofía quienes se han convertido en el motor de vida y cada día inspiran mi razón de ser en el mundo, son ellas la gran motivación a seguir adelante en mi trasegar académico.

Jonathan Duran Pamplona

AGRADECIMIENTOS

Agradezco a Dios todo poderoso quien siempre ha permitido el cumplimiento de mis objetivos personales y laborales. A los ingenieros Luis Fernando Zambrano y Especialista Cristhian Angulo Rivera por su guía en todo el proceso formativo, por ese constante empuje para la realización del presente trabajo.

TABLA DE CONTENIDO

LISTA DE FIGURAS

pág.

GLOSARIO

BOTNET: Dicho término está conformado por dos palabras del idioma ingles La "robot" y "network". Generalmente un delincuente digital usa para la comisión de su objetivo un virus de tipo troyano con el único fin de vulnerar la seguridad no solo de uno sino de varios ordenadores, una vez infectados toma el control de cada uno de ellos para administrarlo de manera remota desde una red de “bots”.[1]

CIBERDELITO: Acción antijurídica y culpable a través de vías informáticas o que tiene como objetivo destruir y dañar por medios electrónicos y redes de Internet. Existen conductas criminales por vías informáticas que no pueden considerarse como delito, según la: "Teoría del delito", por lo cual se definen como abusos informáticos y parte de la criminalidad informática. La criminalidad informática consiste en la realización de un tipo de actividades que, reuniendo los requisitos que delimitan el concepto de delito, sean llevados a cabo utilizando un elemento informático

DELITO: Acción realizada de forma voluntaria o por imprudencia que va en contra de la Ley, por ejemplo, el homicidio, el robo o la estafa son los delitos más comunes. Implica, por consiguiente, ir en contra de lo que está establecido como una ley.[2]

HACKER: Se considera hacker a todo aquel individuo con habilidades sobresalientes en el ámbito informático, se caracteriza por su capacidad de manipular o direccionar los sistemas o redes informáticos, aunque el concepto es siempre asociado a aspectos maliciosos o negativos, no todos los catalogados hacker usan su pericia para tal fin, en la actualidad se conocen los denominados

[1] KASPERSKY, ¿Qué es un botnet? - Definición [En línea]. [Consultado: 14 de febrero de 2018] Disponible en internet: https://latam.kaspersky.com/resource-center/threats/botnet-attacks
[2] COLOMBIA LEGAL CORPORATION, Edición, ¿Qué se considera un delito? [en línea]. Asesores legales especialistas, [Consultado: 15 de enero de 2019]. Disponible en Internet: https://colombialegalcorp.com/se-considera-delito/.

"White hat hacker" quienes permiten a las organizaciones detectar fallos en su seguridad para promover la mejora de sus herramientas de seguridad.

HACKING: Es una forma de delincuencia por la que se accede a información personal o confidencial almacenada en la base de datos de sistemas pertenecientes a cualquier persona u organización desde una ubicación remota. El dueño real puede no ser consciente de que su información confidencial está siendo accesible a otra persona. Para ello, los delincuentes utilizan software especial.

MONOGRAFÍA: Documento descriptivo no seriado, impreso o no, que registra información sobre un tema específico estructurado en una sola parte o previsto para que se complementen en un número limitado de partes separadas. [3]

PHISHING: Es una de las principales formas de ciberdelincuencia y las personas más afectadas por este ciberdelito son aquellas que utilizan internet como medio para sus transacciones en efectivo y otros servicios relacionados con la banca. El criminal intenta adquirir información sensible como nombres de usuario, contraseñas y detalles de tarjetas de crédito y/o cuentas bancarias para retirar dinero o para comprar productos en línea ilícitamente.

SKIMMER: Herramienta más utilizada por los delincuentes para clonar las tarjetas. Esta herramienta permite almacenar entre 15 y 20 claves de tarjetas.[4]

VISHING: Es una práctica criminal fraudulenta en donde se hace uso del Protocolo Voz sobre IP (VoIP) y la ingeniería social para engañar a personas y obtener

[3] COLOMBIA. Instituto Colombiano de Normas Técnicas y Certificación, NTC 5613, Referencias bibliográficas. Contenido, forma y desarrollo [en línea]. Bogotá: 2008 33 p. [Consultado: agosto 12 de 2017]. Disponible en Internet: https://www.politecnicojic.edu.co/images/downloads/biblioteca/guias/NTC5613.pdf

[4] LOBOS, Elkjaer, El temido "skimmer" [en línea]. 24 horas. (3 de agosto de 2012), [Consultado: 06 de noviembre de 2018]. Disponible en Internet: https://www.24horas.cl/nacional/conoce-el-skimmer-lo-mas-utilizado-para-clonar-tarjetas-250832.

información delicada como puede ser información financiera o información útil para el robo de identidad.

TARJETA EMV: El sistema EMV es una parte más de la evolución de la seguridad en las tarjetas, en este caso, basada en la incorporación del chip a la tarjeta, algo ya común y extendido en la actualidad.

RESUMEN

Cada día es creciente el número de las transacciones bancarias, por ello, la investigación en torno a la mutación y adaptación de las distintas conductas delictivas es fundamental para la seguridad informática. Con base en lo anterior, es posible determinar que además de las modalidades delictivas como el hurto simple, actualmente, existen otros como el *Carding* que se dan en la Internet y que dicha modalidad, puede ocurrir entre personas que están a kilómetros de distancia. Basta con tener los conocimientos y la tecnología adecuada para la comisión de la conducta delictiva. El objetivo de esta investigación consiste en describir las distintas modalidades de *Carding* presentes en nuestro entorno. Con una recopilación y organización de la información se pueden obtener los elementos necesarios para realizar una descripción detallada de los principales elementos de seguridad informática que se ven vulnerados en la mencionada modalidad. Los diferentes conceptos que surjan serán definitivos para comprender el modo de actuación de los cibercriminales y las posibles maneras en las que se pueden anticipar las formas de crimen. Los medios de comunicación y la tecnología han hecho que se adopte un idioma universal basado en redes sociales y tecnologías de la información, haciendo que las afectaciones sean comunes a todos los usuarios sin distinción étnica, social o cultural. Es por ello por lo que es propicio hacer énfasis en las modalidades de ciberdelitos y las formas de llegar a ellos, en este caso particular lo que refiere a fraude con tarjetas de crédito o también "*Carding*".

ABSTRACT

Every day is increasing the number of banking transactions, therefore, research around the mutation and adaptation of the different criminal behaviors is fundamental for computer security. Based on the above, it is possible to determine that in addition to criminal methods such as simple theft, currently, there are others such as Carding that occur on the Internet and that this modality can occur between people who are miles away. It is enough to have the right knowledge and technology to commit criminal behavior. The objective of this research is to describe the different Carding modalities present in our environment. With a collection and organization of information you can obtain the necessary elements to make a detailed description of the main elements of computer security that are violated in the mentioned modality. The different concepts that emerge will be definitive to understand the mode of action of cybercriminals and the possible ways in which the forms of crime can be anticipated. The means of communication and technology have led to the adoption of a universal language based on social networks and information technologies, making the effects common to all users without ethnic, social or cultural distinctions. That is why it is propitious to emphasize the forms of cybercrime and the ways to reach them, in this particular case what refers to fraud with credit cards or also "Carding".

INTRODUCCIÓN

Es indiscutible que en el siglo XXl impera lo digital y que dicho mundo ha logrado potencializarse a través de la aparición de las redes informáticas, los teléfonos inteligentes y evolución de la tecnología que permite una comunicación ubicua. Dicho contexto ha permitido una revolución a todos los niveles de la cultura humana, quienes desarrollan y los que la usan se han visto beneficiados. Lo anterior también ha derivado en que la falta de conocimiento técnico y la falta de prevención, permita a ciertos usuarios sacar ventaja para aprovechar la vulnerabilidad de los sistemas informáticos para adulterar, suplantar o violar la seguridad de los datos en beneficio propio.

Por su parte, en el contexto mundial, en los últimos años ataques de gran magnitud en organizaciones de renombre mundial han causado pérdidas millonarias. Los fraudes con el uso de una tarjeta bancaria son cosa de noticia mundial debido a la vulnerabilidad que causa en la confianza del público para el uso de estos dispositivos. En muchas de las ocasiones estos fraudes los han realizado Hackers que quieren hacer fama entre su comunidad, pero si se consolidaran la cantidad de fraudes realizados por personas comunes con algún nivel de conocimiento en seguridad informática, quizás, el valor por las pérdidas acaecidas por el detrimento en la confianza y la seguridad de la Red sería mucho mayor.

La problemática es tan grande que ya hay algunos intentos de las organizaciones bancarias y las instituciones del estado para crear información de interés e inclusive cursos de acción formativa que permitan tener a los usuarios, transacciones más seguras en el entorno digital de la modernidad.

Con base en dichos aspectos se hace propicio indagar desde un contexto internacional y local sobre las principales modalidades de cibercrimen existente en

nuestro país asociadas con el Carding, que se asocia con los delitos bancarios que implican fraude con tarjetas débito o crédito.

Para la presente investigación ese es el eje de indagación que se considera como problemático ya que en la actualidad se viene promoviendo el uso del dinero electrónico de manera extendida en el país. De acuerdo con los breves elementos de contextualización, se realizará el proceso de problematización en torno a la siguiente pregunta de investigación.

1 DEFINICIÓN DEL PROBLEMA

1.1 PLANTEAMIENTO

Usualmente y ceñidos a la modernización digital los usuarios personales y empresariales, realizan a diario sin número de transacciones electrónicas financieras a través de distintos canales establecidos por las entidades de comercio. A pesar que en la actualidad se cuentan con diferentes herramientas para el control y mitigación de transacciones fraudulentas, el desconocimiento de las modalidades delictivas se convierte en el principal aliado de los ciberdelincuentes para la comisión de sus objetivos, ya que mediante diferentes técnicas que, aunque pueden parecer de poca planificación trascienden de manera relevante en la economía del usuario en general, ante esto es importante responder ciertos interrogantes.

1.2 FORMULACION

¿Cuáles son las principales características, modos perpetración y vulneración de la seguridad informática a través de la modalidad delictiva Carding?

2 JUSTIFICACIÓN

Teniendo en cuenta la constante evolución del mundo digital, se hace imprescindible conocer las diferentes modalidades empleadas por algunos usuarios con dudosas intenciones que buscan adquirir algún provecho de la Red de manera ilícita. Con la presente investigación se busca hacer énfasis en lo que refiere al fraude de tarjetas crédito y débito o también conocido como *Carding*.

La importancia del estudio aquí planteado, se sustenta en la creciente tendencia en las transacciones electrónicas que a diario se procesan. Hay oportunidad para los riegos de seguridad y las posibles amenazas deben revisarse. Por otra parte, los usuarios no cuentan con los conocimientos mínimos adecuados que sirvan como medios de prevención a la hora de enfrentar el fraude. Se requieren acciones contingentes que orienten al usuario al estar en presencia de una simple técnica de ingeniería social y nos ser conscientes de ello.

En el país el comercio electrónico toma impulso a través de la publicidad conforme transcurren los años, por lo que se hace propicio aumentar las técnicas de prevención frente a la comisión de delitos, especialmente, para impactar en la comunidad en general que desconoce las connotaciones a la hora de realizar comprar o usar los diferentes métodos de pago que se ofrecen en la red para las transacciones y que son crecientes conforme avanza la tecnología.

2.1 ALCANCE

Con el desarrollo de la presente investigación se pretende resolver interrogantes propuestos en la formulación de la misma, con dicha conceptualización clara se pueden generar cursos de ilustración, prevención y acción que sirvan para hacer frente a la modalidad, trascendiendo como medio de orientación al público en general, comunidad académica y demás miembros de la sociedad en la cual se pueda presentar la conducta delictiva.

3 OBJETIVOS DEL PROYECTO

3.1 OBJETIVO GENERAL

Describir las principales características, modos de perpetración y vulneración de la seguridad informática a través de la modalidad delictiva *Carding*.

3.2 OBJETIVOS ESPECÍFICOS

Conocer las generalidades y principales características relacionadas con el *Carding*.

Delimitar las formas más recurrentes de vulneración de la seguridad mediante el *Carding*.

Describir las principales afectaciones de seguridad informática tanto en Colombia como a nivel personal y/o organizacional como consecuencia del *Carding*.

4 MARCO DE REFERENCIA

4.1 MARCO TEÓRICO

El siglo XXl es el de la revolución digital, lo que a veces ni tiene un significado muy preciso para la mayoría de las personas, sin embargo, para los expertos en computación e informática significa que hay cambios que contradicen los paradigmas de la tecnología que antes eran ampliamente conocidos. Con la aparición de la red Internet el mundo ha logrado potencializarse a través de la aparición de las redes informáticas, los teléfonos inteligentes y evolución de la tecnología que permite una comunicación ubicua.

La Red ha permitido un acelerado cambio en las costumbres humanas, particularmente, en lo que se refiere a hábitos diarios de la vida pública. Por ejemplo, ir al banco o también realizar todo tipo de transacciones para pagar los servicios que utiliza frecuentemente.

En el contexto mundial, en los veinte últimos años el avance de las redes y los servicios para los teléfonos inteligentes han facilitado el paulatino avance de la comunicación y en particular el surgimiento de comunidades que atacan y hacen evidente la fragilidad de la red. Por ejemplo, múltiples organizaciones de USA y el resto del mundo han sufrido ciberataques en la búsqueda de la información vital de las empresas lo que ha derivado en pérdidas millonarias.

Una modalidad apenas creciente en el contexto colombiano pero que se relaciona con las prácticas delictivas que se pueden realizar en la Red, es el *Carding*, es decir, el fraude en que se ven implicados los datos de una tarjeta bancaria. El *Carding* es un fenómeno mundial que basa su éxito en la vulnerabilidad de la Internet y que causa la desconfianza del público para realizar sus transacciones a través de la red.

Como también ya se planteó en la problematización, en muchas ocasiones estos fraudes los han realizado Hackers que quieren hacer fama entre su comunidad de expertos tecnológicos, pero estos han hecho tan evidente la vulnerabilidad de la red y de los sistemas que otros han aprovechado esto para iniciar su carrera delictiva en línea. Lo anterior también ha derivado en que la falta de conocimiento técnico y la falta de prevención, permita a los servicios bancarios y a los usuarios en general generar contingencias adecuadas para prevenir, perfilar y combatir a quienes poseen alguna experticia con la que puedan sacar ventaja para aprovechar la vulnerabilidad de los sistemas informáticos, es decir, para adulterar, suplantar o violar la seguridad de la infraestructura de Internet en su propio beneficio.

Es conocido que el delito avanza porque hace parte de un problema humano, social y cultural, manifestándose de diversas maneras de cibercrimen en el siglo actual. Algunas formas de actuar delictivo en la red se asocian con delitos sexuales, la suplantación de la identidad, otros como el robo de datos bancarios a partir de diversas modalidades dentro de las cuales se encuentra el *Carding*.

Es importante conocer las diferentes actuaciones delictivas del *Carding* que pueden existir en la actualidad en Colombia. Este marco teórico busca relacionar las características más recurrentes de esta modalidad, así como recoger y describir los diferentes conceptos que se pueden generar en torno a esta problemática, para que sean conducentes a las interpretaciones más adecuadas que permitan describir cómo opera la modalidad del *Carding* y delimitando las conductas de mayor repetición actualmente.

4.2 MARCO CONCEPTUAL

AUTENTICACIÓN: Verificar que un documento ha sido elaborado (o pertenece) a quien el documento dice. Aplicado a la verificación de la identidad de un usuario en informática, cuando el usuario puede aportar algún modo que permita verificar que es quien dice ser, suele realizar mediante un usuario *login* y una contraseña *password*.

CONFIDENCIALIDAD: Cualidad de un mensaje, comunicación o datos, para que solo se entiendan de manera comprensible o sean leídos, por la persona o sistema que esté autorizado. Comprende por tanto la privacidad o protección de dicho mensaje y datos que contiene[5]

DELITO INFORMÁTICO: Conducta establecida dentro de la normatividad como típica, antijuridica y culpable, cometida mediante medios digitales o informáticos y que por su connotación permita la alteración, vulneración, modificación o destrucción de datos u ordenadores. Teniendo en cuenta que el mundo digital avanza de una manera extremadamente rápida hay ciertas conductas que podrían quedarse fuera de la jurisdicción exístente ya que su aparición se genera posterior a la creación a la norma, por tanto, dichas actuaciones o conductas se consideran como abusos informáticos.

DISPONIBILIDAD: Capacidad de un servicio, de unos datos o de un sistema, a ser accesible y utilizable por los usuarios (o procesos) autorizados cuando estos lo requieran. Supone que la información pueda ser recuperada en el momento que se necesite, evitando su pérdida o bloqueo.[6]

[5] COSTAS, Jesus. Seguridad y alta disponibilidad. Madrid: RA-MA Editorial, 2014. 227 p.
[6] Ibid. COSTAS, J.

INTEGRIDAD: Cualidad de mensajes, comunicación o datos, que permite comprobar que no se ha producido manipulación alguna en el original, es decir no ha sido alterado.[7]

HACKER: Se considera hacker a todo aquel individuo con habilidades sobresalientes en el ámbito informático, se caracteriza por su capacidad de manipular o direccionar los sistemas o redes informáticos, aunque el concepto es siempre asociado a aspectos maliciosos o negativos, no todos los catalogados hacker usan su pericia para tal fin, en la actualidad se conocen los denominados *"White hat hacker"* quienes permiten a las organizaciones detectar fallos en su seguridad para promover la mejora de sus herramientas de seguridad.[8]

RIESGO INFORMÁTICO: El concepto de riesgo hace referencia en su carácter general a todo aquello presente en el entorno que puede desencadenar en un evento si no se presta la administración o gestión correspondiente. Aplicado al ámbito que nos atañe para la presente investigación se cataloga como todas aquellas amenazas presentes en el campo informático que pueden generar afectación de datos y ordenadores si no son tomadas las medidas correspondientes de mitigación y control.

TARJETAHABIENTE: Usuario de una tarjeta plástica utilizada como medio de pago, puede ser crédito o débito.

VULNERABILIDAD: Son aquellos elementos de carácter tangible o intangible que bien aprovechados pueden proporcionar a un atacante una representativa ventaja para la comisión de un actuar delictivo. Dentro del ambiente informático se puede decir que hallamos seis tipos de vulnerabilidades representadas en físicas,

[7] Ibid. COSTAS, J.
[8] AVAST, Hacker. [En línea]. [Consultado: 14 de febrero de 2018] Disponible en internet: https://www.avast.com/es-es/c-hacker.

naturales, factores humanos, de hardware, de software y red, los cuales fuera de una correcta gestión pueden trascender notablemente en el correcto desarrollo y seguro de las operaciones personales y de la organización.

4.3. MARCO LEGAL

Constitución política de Colombia 1991: Articulo 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

Proyecto de Ley 71, de 4 de septiembre de 2002, del Senado de la República, por la cual se reglamentan los bancos de datos financieros o de solvencia patrimonial y crediticia y se dictan otras disposiciones.

Proyecto de Ley 05/2006 Senado “Por el cual se reglamenta el Habeas Data y el Derecho de Petición ante Entidades Financieras, Bancarias y Centrales o Banco de Datos”. Acumulado Proyecto de Ley nº 27/2006 Senado “Por la cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera y crediticia, y se dictan otras disposiciones”. Aprobado por la comisión el día 12 de octubre de 2006. Ley 1273 de 2009 del 5 de enero 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":

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 p 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.

Ley 1341 de 30 de julio de 2009, sobre principios y conceptos sobre la Sociedad de la Información y la Organización de las Tecnologías de la Información y las Comunicaciones (Diario Oficial nº 47426 de 30 de julio de 2009).

5 GENERALIDADES Y CARACTERISTICAS DE LA CONDUCTA

5.1 GENERALIDADES

Cuando se habla de modalidades delictivas enfocadas al cibercrimen, un usuario no informado podría pensar que se trata de un tema innovador el cual genera curiosidad. Es acertado decir que llame la atención por la connotación de la conducta, pero el resto de la afirmación no es del todo cierta, ya que el auge de la comunicación y las tecnologías de la información han permitido que hasta ahora sea de conocimiento público su existencia. La comisión de conductas antijurídicas en el espacio de la Internet apareció y ha mutado desde mucho antes de lo que nosotros creemos. Por ejemplo, en el año de 1990 en Estados Unidos se realizó una operación anti-hacker sin precedentes, denominada “Operación Diablo del Sol”. Allí se incautaron más de 30.000 ordenadores en todo el territorio norteamericano, los cuales fueron enviados al laboratorio de Investigaciones Informáticas del Servicio Secreto para su análisis.[9]

Es notorio por el ejemplo que dichas operaciones datan de finales del siglo XX y si hacemos el mismo conteo a la aparición de Redes Sociales, se evidencia que estas dan su gran salto en 2004 con la creación de Facebook, es decir, hace 13 años, tiempo en el que tanto la complejidad de la comunicación como el mundo digital han tomado mayor vigor en desarrollo de la humanidad. Cuando se trasciende del contexto internacional y se revisa un concepto como el de *Carding* que se refiere al fraude con tarjetas de crédito y débito. “El *Carding* consiste en comprar usando la cuenta bancaria o la tarjeta crédito de otro, esto se consigue con un poco de ingeniería social y mucha perseverancia; con una correcta vigilancia de la víctima”.[10]

[9] ARTEAGA, Sahnya. Delito: Crimen Electrónico citado por MORANTES, Ceudiel, Fraude electrónico financiero en Colombia, Bogota 2010, 20p, Trabajo de grado para optar al título de Especialista en Administración de la Seguridad, UMNG, Facultad de relaciones internacionales, estrategia y seguridad, Cundinamarca.

[10] RAMIREZ, “Carding: conoce cómo roban las tarjetas de crédito: mdz. {En línea}. [Consultado: 05 de noviembre de 2017]. Disponible en internet: http://www.mdzol.com/nota/514175-carding-conoce-como-roban-las-tarjetas-de-credito/.

En los últimos años ha sido notoria la vulneración de páginas web empresariales por parte de delincuentes informáticos, quienes tienen como objetivo sustraer listados de grandes cantidades de tarjetas de crédito. El experto en crimen organizado y seguridad de la información Misha Glenny, expone que el acceso masivo a números de cuentas ha superado con grandes distancias al hurto diario de tarjetas de crédito de forma personal. Con este ejemplo se evidencia que la modalidad de *Carding* puede marcar hito no solo en la seguridad personal, sino que puede ser notable en un porcentaje mayor en las organizaciones que se afectan causando pérdidas millonarias en la economía.[11]

Para evidenciar parte de la problemática se proporciona un ejemplo bastante ilustrativo que puede abarcar algunas de las características de la modalidad *Carding*: A finales de 2012 un grupo de hackers, hasta ahora prófugos, entraron -se asume que desde Ucrania- en un sistema de procesado de tarjetas de crédito utilizado por el Banco de Muscat, una importante entidad de Medio Oriente.

Los hackers lograron descubrir los números de tarjetas de prepago emitidas por el banco, retiraron el límite de crédito en las tarjetas y cambiaron los códigos “pin” de las mismas. Después, sabiendo los números que normalmente aparecen en la línea magnética en la parte de atrás de las tarjetas, los hackers visitaron en Internet varias páginas Web dedicadas a la actividad criminal.

Al igual que cuando se trata de empleos legales, los hackers utilizaron los servicios de estas páginas para reclutar equipos de criminales de bajo perfil a nivel local, contrabandistas y blanqueadores de dinero. Formaron un gran equipo internacional para este proyecto particular. Estos sitios Web funcionan como cualquier otra página web que ofrece servicios de trabajadores independientes o *freelancers*: la gente

[11] BBC mundo, “Los secretos del cibercrimen organizado para robar tarjetas de crédito”. {En línea} [Consultado: 05 de noviembre de 2017]. Disponible en internet:(http://www.bbc.com/mundo/noticias/2014/11/141110_tecnologia_crimen_organizado_cibercrimen_tarjetas_credito_ig).

recibe críticas y evaluaciones por sus trabajos y su reputación crece o mengua según cómo ejecuten los planes criminales.

Así, tras tener equipos organizados en todo el mundo, los hackers procedieron a enviarles información sobre la franja magnética de las tarjetas.[12] Generalmente los datos proporcionados por un ciberdelincuente a la hora de usar la modalidad de *carding* son totalmente falsos lo que permite que la entrega material sea realizada con total tranquilidad y con la comodidad como si fuera en su hogar.

La ideología de los *Carders* (quienes se dedican a delitos usando tarjetas bancarias) se basa en que existe mucha gente que tiene grandes cantidades de dinero y no sabe qué hacer con él; que no está nada mal utilizar algo de ese dinero para comprar algunas comodidades con ese «préstamo involuntario», ya que posiblemente el dueño de la tarjeta ni se dé cuenta de que él no hizo esta compra. Una bifurcación del exceso de consumo.[13]

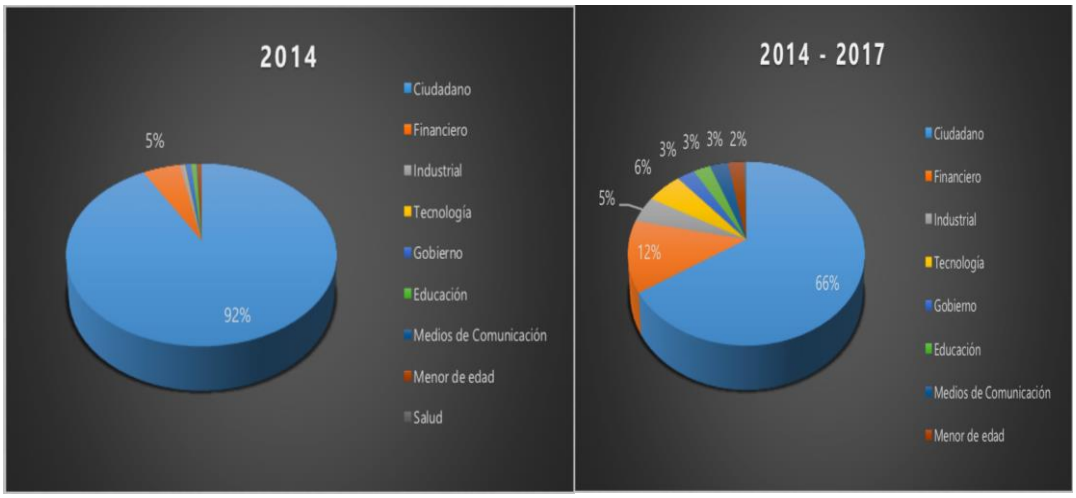
Con la presentación de diferentes casos a nivel mundial y nacional, es posible generar un concepto amplio frente al actuar delictivo y entender de manera más amplía su perpetración, siendo claro que no está orientada a una sola víctima, por el contrario, podemos evidenciar que puede estar dirigido tanto a personas como a organizaciones sin importar su tamaño o actividad económica.

Prueba de la evolución y caracterización de delitos informáticos en nuestro país es evidenciada en el informe presentado por la Policía Nacional de los colombianos, ver figura 1. En esta grafica se puede observar que para el año 2014 el porcentaje de afectación para los ciudadanos en general por ciberdelitos era del 92% y un 5% repercutía en el sector financiero. Lo impactante de dicha estadística se hace notoria

[12] Ibid., BBC mundo.
[13] RAMIREZ, “Carding: conoce cómo roban las tarjetas de crédito: mdz. {En línea}. [Consultado: 05 de noviembre de 2017]. Disponible en internet: http://www.mdzol.com/nota/514175-carding-conoce-como-roban-las-tarjetas-de-credito/.

en cuanto que en tan solo en 3 años el porcentaje de afectación adquirido un carácter de incremento de áreas como la tecnología, gobierno, educación, medios de comunicación y el ya afectado financiero que paso del 5% al 12%. Lo que deja ver la importancia de prevenir y redoblar esfuerzos para mitigar dicha problemática delincuencial.

Figura 1 Comparativo de población afectada por ciberdelitos en Colombia



FUENTE: POLICÍA NACIONAL, Dirección de Investigación criminal e interpol, Caracterización del cibercrimen. [Diagrama]**.** Amenazas del cibercrimen en Colombia 2016-2017. Marzo 2017. Colombia. [Consultado: 16 de septiembrede2018]. Disponible en internet: https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-2017.pdf.

Aunque el tema es demasiado amplio es necesario delimitar las conductas de mayor repetición para ampliar sus connotaciones y que el usuario final identifique el modo de operación y pueda identificar fácilmente al momento de verse enfrentado a una de estas modalidades. Teniendo en cuenta lo anterior, las conductas elegidas para tal profundización serán el denominado phishing e ingeniería social.

Siendo así, es propicio realizar una breve mención sobre otras formas de ejecución que, aunque no serán profundizadas, es relevante tenerlas en cuenta como noción general frente al tema.

Los puntos de conexión Wi-Fi son comunes en estos días, pero los estafadores pueden crear un punto de acceso wifi gratuito sin contraseña: si se conecta a uno y accede a su tarjeta de crédito en línea, pueden robar sus datos de acceso y posiblemente la información de su tarjeta de crédito si realiza una compra. También pueden falsificar tarjetas de crédito obteniendo la información de su tarjeta de crédito con un skimmer, que a menudo no son detectados por los consumidores. Una vez que tienen la información personal, los estafadores pueden hacer todo, desde llamar a la compañía de tarjetas de crédito o al banco que se hace pasar por el usuario y reclamar la pérdida o el robo de la tarjeta, hasta completar solicitudes de tarjetas de crédito fraudulentas (una forma de robo de identidad) y realizar compras por internet.[14]

5.2 CARACTERISTICAS

Conocidos aspectos de interés general es oportuno mencionar características de las partes involucradas en la conducta, en este entendido se puede decir que en primer lugar se halla el victimario quien es el perpetrador de la acción, para poder entender un poco mejor su forma de actuar es meritorio ampliar los rasgos que definen a un delincuente informático y las motivaciones que sustentan su accionar.

Para entender la forma de pensar y actuar de un delincuente común o este caso informático, es relevante tener presente distinto ámbitos que marcan la conducta y que se catalogan como motivaciones para el actuar ilícito, en cuanto al factor

[14] HOFFOWER, Hillary. There's a good chance you're a victim of credit card scams and you don't even know it — here's what to do [en línea]. [Consultado: 18 de septiembre de 2018]. Disponible en Internet: https://www.businessinsider.com/credit-card-fraud-scam-what-to-do-2018-8

psicológico se haya el delito como elección propia; en este aspecto es posible afirmar que la persona nace con la determinación de cometer conductas catalogadas en la sociedad actual como ilegales, el individuo no busca ningún beneficio económico, ni suplir ningún tipo de necesidad material, ni mucho menos por un impulso de momento, lo hace como forma de obtener placer , es su forma de satisfacer la búsqueda de nuevas experiencias y vivencias en su día a día.

Como segundo factor se plantea la que quizá en la actualidad sea la de mayor repetición, y es aquella que se da por la influencia social, dicho postulado se sustenta en la ideología del mundo contemporáneo en el que las apariencias trascienden de una manera notable debido al acceso a las tecnologías de la información, y el “dinero fácil”, el cual motiva la actuación de personas que en muchas ocasiones justifican su actuar con falta de oportunidades y surgimiento. Hoy en día dicha problemática trasciende especialmente en países considerados como subdesarrollados, donde la cultura y jurisdicción permite que el delito sea repetitivo y las medidas para mitigarlo son flexibles o inoperantes.

Por último, se hallan las condiciones agresivas por las cuales pudo haber atravesado el individuo a lo largo de su existencia, dicho factor puede repercutir significativamente en el delincuente, quien halla en su actuar ilegal una forma de cambio en las condiciones de vida, sin valorar que su conducta afecta también negativamente la sociedad.

Cuando se traslada el enfoque a el delincuente informático, es posible evidenciar ciertas divergencias en la justificación del obrar, soportándose en la investigación y la exploración. Un delincuente informático generalmente cuenta con gran capacidad intelectual y hábitos no muy comunes por la sociedad, su pasión está centrada en navegar en la red y equipos informáticos, sus motivaciones son de carácter personal (ocio, diversión, económicos) o en porcentaje por presiones impuestas por otro tipo

de delincuentes quienes buscan la forma de infundir terror para que este trabaje o haga lo que necesita.[15]

Como segundo interviniente en la conducta se halla la víctima, quien se podría decir que es cualquier miembro de la sociedad en general o ente comercial, pero ante esta afirmación se debe controvertir el hecho que, para poder verse afectado por tal modalidad la condición esencial es ser tarjetahabiente. Cumpliendo dicha condición de forma inmediata se hará parte del entorno vulnerable en la conducta de Carding. Aunque puede generar alerta el anterior postulado, el conocimiento de las diferentes divergencias y características que rodean el ilícito pueden orientar de una mejor manera a todos los usuarios y empresas que actualmente basan su economía en las transacciones bancarias y dinero digital.

Revisados los aspectos generales y hechos el recorrido histórico frente a la conducta relacionada al fraude en tarjetas de crédito, a continuación, se platea una descripción y profundización de las modalidades delimitadas como base de estudio.

[15] LUNA, Cesar. Perfil criminológico de un delincuente informático. [en línea]. [Consultado: 13 de febrero de 2019]. Disponible en Internet: http://www.derecho.usmp.edu.pe/centro_inv_criminologica/revista/articulos_revista/2013/Articulo_Prof_Cesar_Ramirez_Luna.pdf.

6 PRINCIPALES MODALIDADES DE PERPETRACIÓN Y VULNERACIÓN

Conocidas las generalidades de la conducta, es importante hacer un recorrido por las modalidades más relevantes y conocidas de la misma. En primer lugar, es propicio saber que para perpetrar la conducta existen maneras digitales y físicas, las cuales dependiendo la determinación de la víctima serán usados por el delincuente. Para comprender esta divergencia iniciaremos con analizar las consideradas del ámbito digital, para esto se ha seleccionado la conducta conocida como “ingeniería social”.

6.1 INGENIERÍA SOCIAL

Es un método no-técnico de los piratas informáticos y que depende en gran medida de la interacción humana. Es una de las mayores amenazas que enfrentan las organizaciones hoy en día, los creadores de virus utilizan tácticas de ingeniería social para convencer a la gente a ejecutar virus en archivos adjuntos de correo electrónico, o simplemente de compartir su información mediante archivos o falsas webs de empresas u proveedores de servicios o productos, otros utilizan la ingeniería social para convencer a la gente a revelar información sensible, etc.[16]

La técnica anterior se podría catalogar como la de mayor repetición cuando a la hora de efectuar un fraude a la información de una tarjeta o información financiera, por lo que no se puede decir que cada una actúa por sí sola, muchas veces una técnica de ingeniería social puede lanzarse en conjunto con *phishing*, esto se puede evidenciar cuando se recibe una llamada telefónica de alguien que se hace pasar por funcionario de cierta entidad financiera a fin de ofrecer productos o diciendo que alguien intentó violentar la tarjeta y por tanto requiere una verificación de datos para

[16] Finanzas personales, “Los tipos de robos que hacen a través de las tarjetas”. [En línea]. [Consultado: 05 de noviembre de 2017]. Disponible en Internet: (http://www.finanzaspersonales.co/credito/articulo/los-robos-pueden-hacer-tarjetas/53157).

corroborar que habla con el titular del producto. De esta forma se pueden obtener fácilmente los datos sensibles no solo de la tarjeta, sino también la información personal necesaria para complementar el hecho delictivo.

Con el pasar de los años y la constante evolución tecnológica, las redes sociales han pasado a cumplir un rol demasiado importante en la sociedad actual, lo que hace llegar a pensar que muchas personas desgastan bastante tiempo de su vida en querer aparentar ante los demás mediante publicaciones lo interesante de su vida y su nivel actual, esto trasciende al hecho de compartir demasiada información sensible en cada una de estas redes, situación que es fácilmente aprovechada por delincuentes informáticos para la comisión de las conductas ilegales.

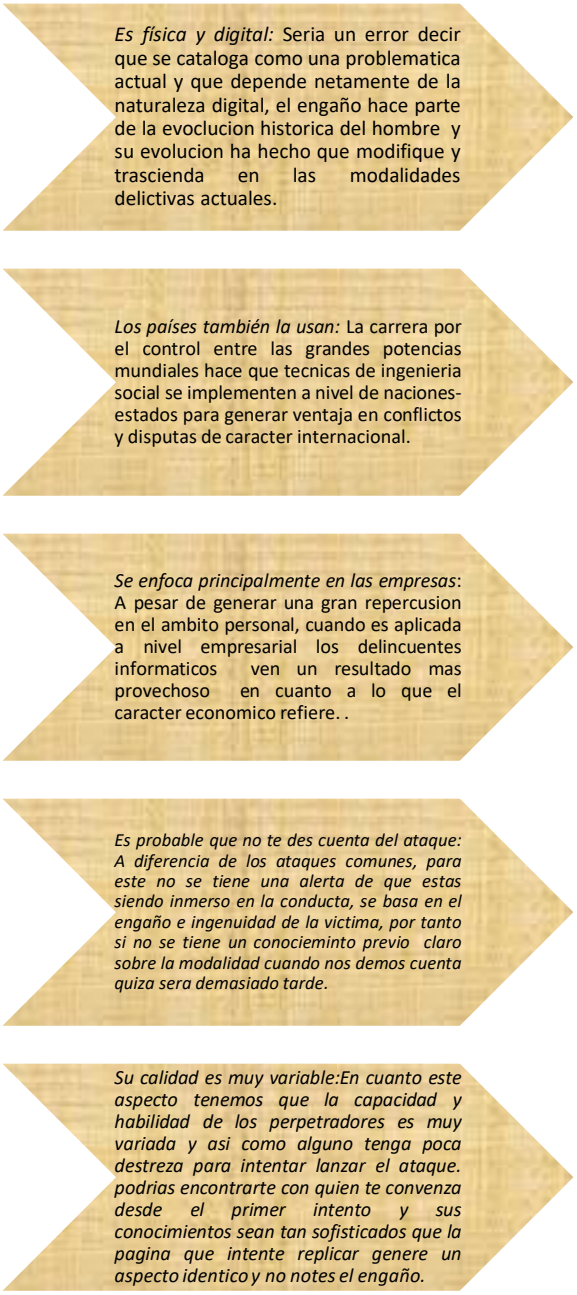
La famosa compañía de seguridad informática ESET plantea en su sitio web cinco premisas a tener en cuenta cuando se habla de ingeniería social (ver figura 2), su revisión supone la introducción más apropiada al contexto de esta modalidad, permitiendo aclarar y sentar precedentes para el desarrollo de la temática.

Así mismo es importante conocer el perfil y connotaciones de un ingeniero social, esto con el fin de generar un correcto enfoque y entender mejor las modalidades que de allí se desprenden. Brad Sagarin, doctor en psicología social y autor de un estudio de la persuasión, describe las armas con que cuenta un ingeniero social así:

"No hay nada mágico en la ingeniería social, el ingeniero social emplea las mismas técnicas de persuasión que utilizamos todos los demás a diario. Adquirimos normas, intentamos ganar credibilidad,exigimos obligaciones recíprocas. Pero el ingeniero social aplica estas técnicas de una forma manipuladora, engañosa y muy poco ética, a menudo con efectos devastadores".[17]

[17] MITNICK, Kevin y SIMON, William. El arte de la intrusión: la a verdadera historia de las hazañas de hackers, intrusos e impostores. 1 ed. Madrid: RA-MA Editorial, 2007. p. 313.

Figura 2. Aspectos relevantes de la ingeniería social



FUENTE: DURAN, Jonathan. Características relevante ingeniería social. [Diagrama]. Bogotá D.C. 2018.

Los rasgos de un rol; en los ataques de ingeniería social quien se encarga de ejecutar la acción primero genera un estudio para adoptar el rol especifico que más se ajuste para lograr su cometido, como ya pudimos observar anteriormente es posible perpetrar la conducta de manera física y digital por eso en ciertos casos de ingeniería el delincuente hace parte de la organización y se caracteriza de acuerdo a como mejor pueda completar su objetivo, pasando por cliente, técnico o alguien de influencia en la empresa.

Completado dicho aspecto es importante ganar la credibilidad como garantía para el siguiente paso el cual causa que el objetivo adopte un rol que se ajuste a los intereses del atacante.

Como ya se planteará más adelante, la información en el ser humano tiene dos maneras de asimilarse, y es importante para el atacante desviar la atención del pensamiento sistemático dejando todo en mano de las emociones las cuales serán propicias para manipular. La forma de avanzar con base en lo anterior se sustenta en que al iniciar peticiones pueden parecer inofensivas, incrementando de manera progresiva la agresividad de las mismas, dichas solicitudes pueden ir acompañadas del aprovechamiento de que el ser humano alivia su corazón al servir y prestar ayuda a los demás, este factor es usado por los ingenieros sociales.

Otro aspecto a tener en cuenta se basa en el sentir humano, de entender los gustos y la simpatía hacia cosas y personas por parte de la víctima, esto hará poco complejo llegar a él, adoptando el perfil o rol que sea necesario para completar el proceso, esta táctica incluye gran cantidad de herramientas a usar partiendo desde investigar su entorno social hasta generar halagos y mencionar nombres de familiares y amigos. Un aspecto totalmente contrario se orienta al miedo haciendo creer a su objetivo que algo muy malo puede pasar sino se ciñe a las indicaciones que se están dando por parte del victimario.

La ingeniería social puede ser empleada a gusto y ajuste del perpetrador, y con el pasar de los años y avances tecnológicos ha podido adoptar distintas divergencias para lograr su cometido. A continuación, se podrá profundizar en las modalidades tomadas para el estudio y las cuales representan mayor repetición en la sociedad actual.

6.1.1 Phishing

Dentro de las formas de perpetuar la modalidad se halla el denominado *Phishing* cuyo origen etimológico del inglés es pesca. El *phishing* es una estafa por correo electrónico que intenta engañar a la víctima para que revele los números de sus tarjetas y códigos de identificación personal (PIN), contraseñas de cuentas bancarias u otra información privada.[18] Su metodología es muy sencilla y basta con efectuarse en la persona indicada para arrojar los resultados deseados, de allí la importancia de generar la prevención adecuada en la sociedad en general, ya que actualmente es común la utilización de tarjetas especialmente las de crédito para realizar compras y transacciones por internet.

Se puede catalogar el Phishing como una de las modalidades que más afectan en Colombia, debido a las falsas ofertas publicadas en portales web e incluso reconocidas tiendas de comercio electrónico como mercadolibre.com, OLX.com, tucarro.com, etc. Estas estafas se originan por el incumplimiento de algunas de las partes, bien sea en el envío o recibo de productos vendidos o comprados en las plataformas, o en el cambio de las condiciones y calidad de los mismos.[19]

[18] Marisol, "Qué es la ingeniería social y cómo protegerse de ello", Tarjetas de crédito hoy. {En línea}. disponible en (https://tarjetasdecreditohoy.com/que-es-la-ingenieria-social-y-como-protegerse-de-ello-a-sus-tarjetas/).

[19] POLICÍA NACIONAL, Dirección de Investigación criminal e interpol, Caracterización del cibercrimen. [diagrama]**.** Amenazas del cibercrimen en Colombia 2016-2017. Marzo 2017. Colombia. [Consultado: 16 de septiembrede2018]. Disponibleeninternet:
https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-2017.pdf.

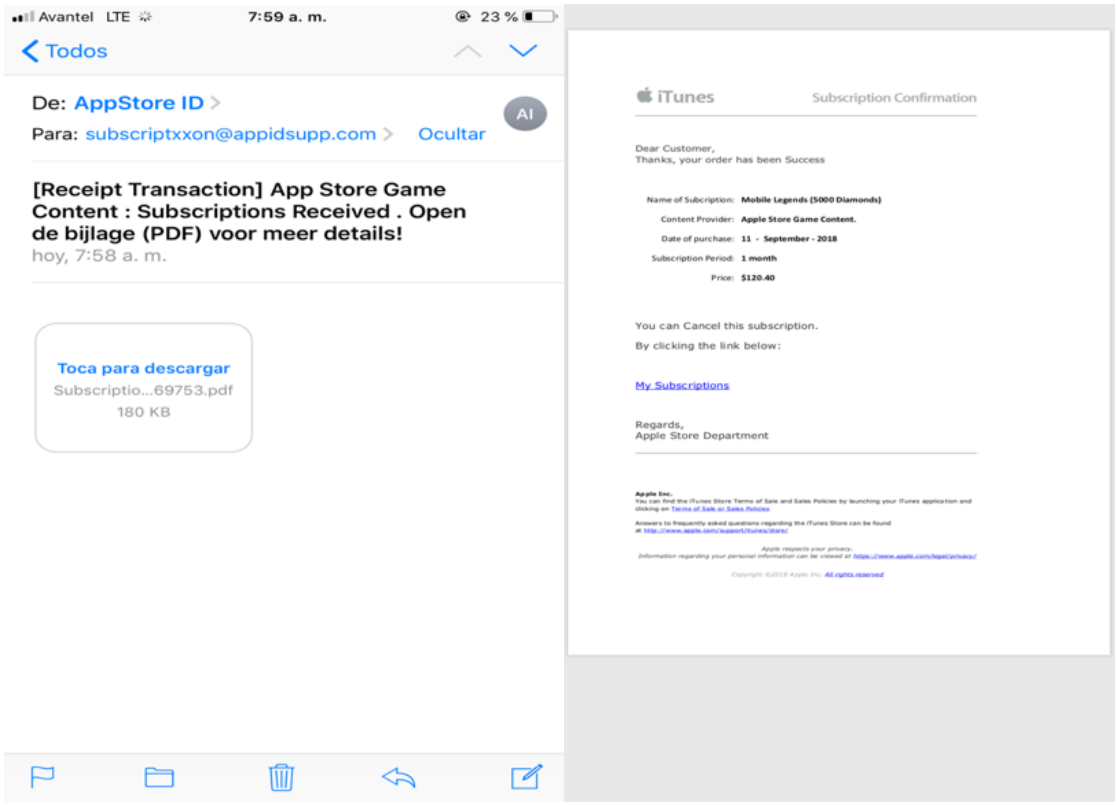
Como método ilustrativo se presenta a continuación un ejemplo de la forma en que los delincuentes a diario generan miles de intentos para acceder a información de las tarjetas de crédito.

La empresa de diseño y producción de tecnología Apple, es reconocida por la comercialización de su producto insignia “el iPhone”, para completar su experiencia tecnológica en dicho dispositivo es necesario crear una cuenta de acceso denominada Id de Apple, al momento de crear dicha cuenta se solicitan diferentes datos personales y como requisito adicional se solicita información financiera para realizar compras en su tienda de aplicaciones y música (si es de interés del usuario).

Dicha situación es aprovechada por los delincuentes para intentar perpetrar la modalidad de phishing, esto es posible de una manera muy sencilla ya que a diario suministramos nuestra dirección electrónica de correo en diferentes páginas de registro, siendo esta una base de datos provechosa para el perpetrador, quien en primer lugar accede a esta información y genera una dirección falsa de correo (de carácter similar a la original de Apple, modificando ciertos campos y símbolos), con esto inicia su “pesca”, enviando mensajes de correo a las direcciones ya antes adquiridas y en donde informa que la cuenta presenta inconvenientes o detalla la realización de compras desconocidas por el usuario y/o víctima.

En las imágenes (ver fig. 3), se puede observar un correo electrónico recibido en un día cualquiera, el usuario remitente se disfraza como AppStoreID, y el asunto supone la adquisición a una suscripción de un juego en la tienda online, así mismo carga un documento adjunto en formato pdf con logos de Apple en donde se plasman los datos de confirmación de la compra.

Figura 3 Comunicación de correo electrónica tipo “phishing”



FUENTE: DURAN, Jonathan. Comunicación de correo electrónico tipo “phishing”. [Fotografía]. Bogotá D.C. 2018. Evidencia del inicio de la modalidad.

La estafa se desarrolla al invitar a la víctima a descartar la transacción si es desconocida para él, mediante un link suministrado para efectuar los pasos correspondientes a la cancelación.

Basta con dar clic al vínculo y de inmediato procede a dar paso a la siguiente parte del proceso de obtención de datos.

Figura 4 Presentación de la página donde es remitido el usuario

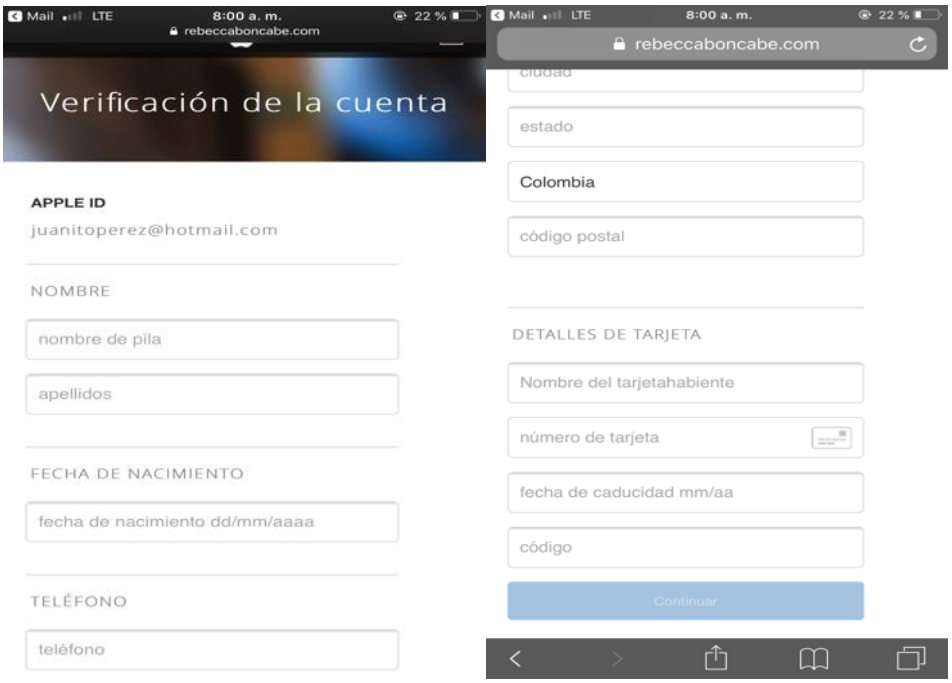
FUENTE: DURAN, Jonathan. Presentación de la página donde es remitido el usuario. [Fotografía]. Bogotá D.C. 2018. Suministro de datos para inicio de sesión.

Como se evidencia en la imagen (ver fig. 4), la página falsa aparenta ser la oficial de Apple por sus logos y diseño, solicita autenticación para poder realizar las respectivas modificaciones y cancelar la supuesta suscripción adquirida, como es de notarse se puede digitar cualquier correo y contraseña para el inicio de sesión, sin importar cual sean los datos suministrados siempre dará acceso al siguiente paso, generando de a poco confianza al usuario para que continúe con el suministro de datos necesarios para completar la estafa.

Inmediatamente nos pedirá comprobar cierta información como “garantía” para iniciar la cancelación (ver fig. 5), esto incluye una casilla especial para digitar la información financiera registrada en la cuenta original incluyendo código de verificación de la tarjeta de crédito, parte fundamental de la estafa.

Al completar el registro y dar la confirmación el delincuente recibirá de la manera más sencilla lo suficiente para vulnerar la seguridad de la tarjeta y realizar compras por internet que usualmente es lo que hace al obtener este tipo de datos.

Figura 5 Solicitud de información personal y financiera



DURAN, Jonathan. Solicitud de información personal y financiera. [Fotografía]. Bogotá D.C. 2018. Incluye solicitud de información sensible de la víctima, incluyendo la de su tarjeta de crédito.

Aunque es una situación propia, medios informativos de nuestro país han venido alertando sobre esta metodología desde hace años atrás, prueba de ello se puede ver reflejado en el artículo publicado el 15 de enero de 2018 por la empresa de seguridad ESET, allí se plantea que en países como Argentina y Colombia se

observa gran afectación por campañas de este tipo, sin contar con una cifra oficial sobre su repetición. “El sistema operativo iOS de Apple tiene el 12 por ciento del mercado mundial y se halla en constante crecimiento en América Latina en lo que usuarios refiere, esto hace que se convierta en un atractivo para los delincuentes informáticos según lo expone el especialista en seguridad informática de ESET Maximiliano Cantis. Además, asegura que los ciberdelincuentes usan como método diferentes formatos de mensajes con características similares, dentro de ellos se destacan correos con archivos adjuntos en formatos PDF que dan información sobre supuestas compras realizadas por el usuario y requieren verificación de identidad. También es posible hallar links que redireccionan al usuario a paginas externas con el fin de verificar la informacional personal y financiera exponiendo plazos de 24 horas para no generar bloqueo de sus cuentas.[20]

Aunque parezca un método poco significativo, y puedan existir muchos factores que permitan identificarlo como estafa desde el inicio del proceso, especialmente si no es un usuario que cuente con una cuenta de este tipo, lastimosamente a diario cantidad de usuarios caen y se ven afectados notablemente en sus finanzas por desconocimiento de tal modalidad.

Al analizar el ejemplo anterior, el lector puede decir que no se verá afectado por pertenecer a otra línea de cuentas o sistema operativo y que al recibirlo lo descartara, pero frente a esto es oportuno mencionar que tan solo es un ejemplo de infinidad de correos que suponen ser de una empresa determinada y que la desatención o desconocimiento pueden llevar a la víctima a suministrar los datos solicitado de la forma deseada por el perpetrador.

[20] EL TIEMPO, Tecnología. Ojo con correo falso de Apple que roba sus datos bancarios. . [En línea]. (05 de enero de 2018), [Consultado: 10 de marzo de 2019]. Disponible en Internet: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/correo-falso-de-apple-roba-sus-datos-bancarios-171332

Como forma más sofisticada se halla el denominado “spear phishing” el cual es una estafa de correo electrónico u otro tipo de comunicación dirigida a personas o empresas de manera específica. En un porcentaje mayoritario se busca la obtención de datos con fines ilícitos o maliciosos, pero también puede sustentarse en instalar algún tipo de malware del ordenador de la víctima.

La reconocida empresa de seguridad informática Kaspersky Lab plantea la forma como opera la modalidad; en un escenario cualquiera llega a la bandeja de correo una comunicación de una procedencia aparentemente de confianza, al abrir dirige al usuario a una página de apariencia confiable, pero con gran cantidad de malware. Una táctica para captar la atención de la víctima se sustenta en el contenido que generalmente promueven, la procedencia de sitios de interés o de población vulnerable.

En gran cantidad de ocasiones, los ataques son perpetrados por hackers que trabajan de manera independiente, pero siempre no suele ser así, cibercriminales tienen la intención de obtener información con el fin de revenderla a gobiernos o empresas privadas para los fines que estos estimen pertinentes.

A menudo las medidas de seguridad tradicionales no bastan para detener estos ataques porque están personalizados de forma muy inteligente. En consecuencia, se están volviendo más difíciles de detectar. El descuido de un empleado común puede repercutir de manera significativa en el general de la empresa o gobiernos, incluso en organizaciones sin ánimo de lucro.

Con el robo de información y datos un delincuente cibernético puede generar diversas consecuencias, que van desde manipular precios de acciones en el mercado o secuestrar computadores en gigantescas redes (botnets) , por eso es importante concientizar a la dirección y el general de la organización sobre las posibles amenazas y el curso de acción a seguir a la hora de recibir comunicaciones

electrónicas desde direcciones sospechosas o de dudosa procedencia, adicional a esto es prioritario adoptar herramientas tecnológicas que permitan su mitigación.[21]

Conocida la metodología, se puede decir que existe una técnica de carácter similar, pero es catalogada con la denominación de smishing. El smishing. Es una forma de phishing mediante la cual alguien intenta obtener información privada a través de un mensaje de texto o SMS, es una amenaza emergente y en crecimiento en el mundo de la seguridad en línea.[22]

6.1.2 Smishing

Para un entendimiento efectivo y sencillo, se puede decir que es una forma de hacer phishing) en la cual se ven inmersos las víctimas al recibir un mensaje de texto en un equipo celular. Trasciende y genera alerta ya que en la actualidad las personas confían plenamente en este tipo de comunicación, y aunque se es consciente de los riesgos que pueden presentarse al momento de dirigirse a enlaces que vienen en correos electrónicos, los niveles de confianza aumentan cuando se trata de un sms, llevándolos a caer de manera ingenua en tal modalidad.

La ingeniería social se encuentra presente en todo momento de perpetración de la conducta en el entendido que siempre se recopila información personal de la víctima para llegar al objetivo. Los atacantes se encargan de recopilar todo tipo de información valida sobre la víctima (seguridad social, tarjetas de crédito, etc.), esto valiéndose de registros en línea.

Como otra forma de vulnerabilidad se halla lo referido al SMS que recibe con el enunciado alertando que al no seguir los pasos de registro requeridos se iniciara

[21] KASPERSKY, Lab. ¿Qué es el spear phishing? [En línea]. [Consultado: 14 de febrero de 2018] Disponible en internet: https://latam.kaspersky.com/resource-center/definitions/spear-phishing.

[22] NORTON, security, ¿Qué es el smishing? Norton by Symantec. [en línea]. [Consultado: 22 de octubre de 2018] Disponible en internet: https://co.norton.com/internetsecurity-emerging-threats-what-is-smishing.html.

cobro diario de tarifas por usar el servicio de cierto producto o suscripción, es allí donde los conocimientos adquiridos mediante este documento serán más que efectivos, ya que el mensaje se deberá omitir y si por alguna razón se viera reflejado algún tipo de cobro en su tarjeta de crédito se deberá elevar una petición a la entidad financiera para solucionar el inconveniente.

Para lograr identificar si estamos siendo víctima de esta modalidad es fundamental no generar respuesta a mensajes de usuarios desconocidos y más si el número de teléfono presenta algún tipo de diferencia al que usualmente conocemos.

Por ejemplo, si en el remitente se observa el numero 5000 es una señal clara que el SMS ha sido enviado de una dirección de correo electrónico directamente al número celular. Es prudente también instalar aplicaciones desde la tienda oficial de la plataforma de la que se accede ya que las allí provistas están sujetas a verificación y evaluación antes de salir al mercado. Siempre será optimo adoptar demasiadas precauciones que no contar con ninguna, si desconoce el destinatario la mejor manera de evitar el riesgo es ignorar su contenido.

La forma más apropiada para evitar este tipo de engaños es obviando dar clic en anuncios y enlaces recibidos de direcciones de correo desconocidas para el usuario, y verificando que los diferentes portales que se visitan cuenten con los protocolos seguros HTTPS (protocolo seguro de hipertexto), además es recomendable revisar de manera constante los movimientos efectuados por nuestros productos financieros, hacer comprar en sitios web reconocidos y con buena reputación, así como hacer caso omiso a llamadas y mensajes que nos generen sospecha.[23]

[23] POLICÍA NACIONAL, Dirección de Investigación criminal e interpol, Caracterización del cibercrimen. [diagrama]**.** Amenazas del cibercrimen en Colombia 2016-2017. Marzo 2017. Colombia. [Consultado: 16 de septiembrede2018]. Disponibleeninternet: https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-2017.p.4.

Otra técnica que podría catalogarse como similar por sus connotaciones es la conocida como “vishing” la cual por sus características hace que sea un tema también de especial atención.

6.1.3 Vishing

Es una estafa que pretende suplantar la identidad del afectado a través de VoIP (Voice over IP), recreando una voz automatizada semejante a la de las entidades bancarias. El término proviene de la unión de dos palabras: voice y phishing.[24]

Teniendo claro lo que a phishing refiere, es posible comprender de manera adecuada la modalidad de vishing, reafirmando la composición entre estos dos términos, la divergencia ocurre en el sentido que el vishing no usa un correo para obtener la información, sino que se basa en una llamada telefónica a la víctima con la intención de acreditar sus datos financieros para el cumplimiento de su objetivo.

Si lo que se pretende es mostrar y esclarecer dudas frente a la modalidad, es preciso dar a conocer que puede perpetrarse de varias maneras; La primera de ellas consiste en enviar un mensaje de texto (donde aplica su relación con el tema ya mencionado de smishing) a la víctima informando que se ha realizado cierta transacción con su tarjeta y que si desconoce de esta debe comunicarse con la entidad financiera para cancelar el movimiento, el valor agregado está en que dentro del mensaje se incluye el número de contacto al cual deberá llamar para solucionar el inconveniente (siendo este el del delincuente), la victima sin realizar ningún otro tipo de verificación inmediatamente atiende y realiza dicho llamado, y es allí donde remitido a una persona o contestadora muy eficiente quien luego de confirmar y adicionar datos personales y financieros, manifiesta haber cancelado a satisfacción

[24] BBVA, Seguridad, ¿Qué es el vishing? [en línea]. BBVA página oficial. (25 de noviembre de 2015), [Consultado: 08 de octubre de 2018]. Disponible en Internet: https://www.bbva.com/es/vishing-la-imaginacion-los-estafadores-no-limites/.

la supuesta transacción fraudulenta, sin saber que el fraude se consolidara con el procedimiento acabado de realizar.

Como otra forma de intentar concluir la estafa se halla la perpetrada por el delincuente que toma contacto con la víctima, pero esta vez no por mensaje de texto, sino de manera directa ya sea igualmente con una voz digital (tipo bancaria) o con mucha destreza usando la propia, en esta comunicación se da a conocer que la tarjeta que posee presenta problemas de autenticación o cualquier otro tipo de anomalía, a lo que la victima de manera progresiva ira suministrando datos sensibles personales y financieros.

Cabe anotar que en muchos casos el delincuente no obtiene la información en una sola comunicación y puede ser paciente realizando varios llamados hasta completar su objetivo, la destreza y poder de convencimiento del mismo, juegan un rol importante ya que pueden llegar a convencer a la víctima que en realidad se encuentran hablando con un funcionario de una entidad financiera. Lo fundamental y a tener en cuenta es nunca suministrar datos por ningún medio telefónico o de internet que no sea de procedencia confiable y al momento de evidenciar un rasgo mínimo de falta de veracidad se debe desistir del tipo de transacción o comunicación.

Es pertinente destacar nuevamente, que mucha información tomada por delincuentes informáticos es fácilmente adquirida por suministro dado por el mismo usuario o víctima en las distintas actividades que se realizan diariamente en el ámbito digital, esto mediante registros, suscripciones, redes sociales, entre otros. Brindamos buena cantidad de información personal que es de gran utilidad para iniciar un modelo determinado de estafa.

Es importante delimitar la cantidad de datos que estamos dispuestos a compartir en la red para así prevenir la comisión efectiva de varias conductas. La difusión de

casos presentados es una excelente vitrina para dar a conocer como un ciber criminal puede vulnerar la seguridad informática en pequeñas y grandes escalas.

Aunque las formas existentes de ingeniería social en cualquiera de sus modalidades podrían ser fáciles de identificar para una persona del común, es relevante conocer cierta connotación del pensamiento humano de donde se puede destacar lo siguiente: Dentro de la psicología social se hallan dos modelos presentes en la humanidad para procesar la información, la sistemática y la heurística. "Cuando procesamos la información sistemáticamente, pensamos con detenimiento y de forma racional una petición antes de tomar una decisión. Por el contrario, si la procesamos heurísticamente, tomamos atajos mentales para tomar las decisiones.

Por ejemplo, podemos acceder a una petición en función de quién afirma ser el que hace la petición, en lugar de fijarnos en la confidencialidad de la información que ha solicitado. Intentamos funcionar en el modo sistemático cuando el tema es importante para nosotros. Pero la presión del tiempo, la distracción o una emoción fuerte nos hace cambiar al modo heurístico".[25]

Del entendido de este supuesto psicológico es posible afirmar que, sin importar la capacidad mental y conocimientos, es posible verse inmerso como víctima de dicha conducta, para el victimario basta con conocer entender el pensamiento humano para hallar las herramientas adecuadas para llegar al cumplimiento de su fin.

Algo más ceñido a la habilidad delincuencial se hallan las modalidades que han sido catalogadas como físicas, aunque son de mayor complejidad para identificar que las propuestas en ingeniería social, es posible mitigarlas si se tienen los conocimientos y se realizan las prevenciones previas.

[25] MITNICK, Kevin y SIMON, William. El arte de la intrusión: la a verdadera historia de las hazañas de hackers, intrusos e impostores. 1 ed. Madrid: RA-MA Editorial, 2007. p. 316.

Aunque los postulados han sido enfocados a las modalidades con el objetivo de obtener información de tarjetahabientes, es oportuno mencionar que la modalidad tiene infinidad de propósitos de carácter económico. La Policía Nacional de Colombia pone en evidencia mediante boletines informativos hechos de la vida real en donde se demuestra cómo actúan los delincuentes para obtener beneficio.

El ejemplo relata lo siguiente: *"Buenas tardes, mi nombre es Kassandra y les comparto mi historia para que, así como yo, usted también pueda evitar una estafa por el "Sobrino retenido": El día 06-02-2016 siendo las 5:16 p.m. recibí una llamada a mi celular, donde un hombre quien afirmó ser mi sobrino, como no logré identificarlo, é/ me dijo: ¿Quién crees que soy? Lamentablemente, tenía tonos parecidos a uno de mis sobrinos, y como pensé que era una broma, le dije: eres Leonardo o Santi; a lo cual el delincuente respondió: soy Leonardo, ya ni mi voz reconoces. Cuando é/ me dijo que había sido retenido por la policía porque en su carro llevaba un arma, y que necesitaba 2 millones de pesos para que no lo judicializaran, inmediatamente mi sentido común me hizo saber que era para robarme; entonces, empecé a hacerle preguntas, tantas que el tipo se enredó y no sabía ni qué responder.*

Seguidamente, como mi mami estaba allí escuchando, no soportó oír todas las mentiras del delincuente, ni el que yo intentara averiguar más datos sobre él, por lo cual decidió agredirlo verbalmente por el teléfono, dando por terminada la llamada. Luego me comuniqué con e/ @CaiVirtual, indiqué toda la información relacionada con el caso y ellos me brindaron toda la orientación y atención frente a la situación que me había ocurrido. Espero que mi historia sirva como medida preventiva para

que muchos ciudadanos que sean objetivo de estos bandidos, logren evitar ser víctimas del fraude antes mencionado".[26]

A pesar que actualmente son muchos los cuidados que se toman por parte de las entidades bancarias para evitar que sus cajeros sean vulnerados por delincuentes, los fraudes siguen presentándose en las diferentes modalidades y se convierten en amenazas latentes para las personas. La imaginación de la delincuencia no tiene límites y las tácticas para su cometido van desde lectores de bandas magnéticas, hasta teclados y cámaras de diminuto tamaño.

6.2 SKIMMING

Sacar dinero en cajeros automáticos sigue siendo una de las operaciones más comunes al utilizar nuestras tarjetas bancarias y, por lo tanto, una de las ocasiones más propicias para los fraudes. El *skimming* se ubica entre los fraudes más comunes en cajeros automáticos.[27]

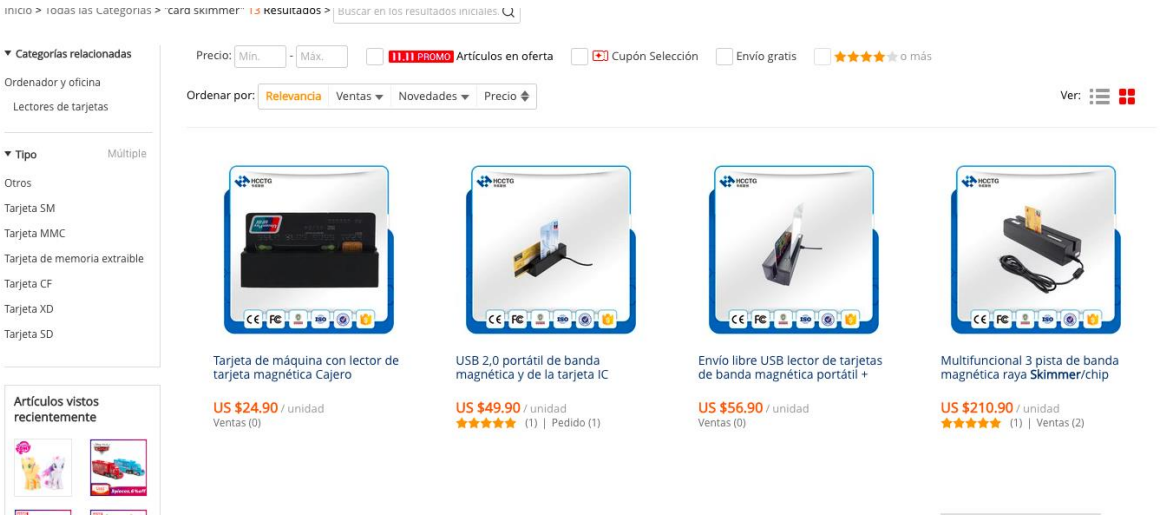
Es una modalidad de fraude que consiste en hurtar información de tarjetas débito y crédito mediante dispositivos que toman la información de la banda magnética de las mismas, una vez cumplido el objetivo se procede a realizar transacciones y retiros a nombre del titular. Trasciende en complejidad ya que puede ser usada por el delincuente pasada cantidad notable de tiempo después de efectuada la maniobra, haciendo más difícil el seguimiento a la conducta delictiva.

[26] POLICÍA NACIONAL, Dirección de Investigación criminal e interpol, [En línea]. Boletín de Análisis en Ciberseguridad, El sobrino retenido-estafa VISHING. Colombia. (07 febrero de 2016) [Consultado: 01 de enero de 2019]. Disponible en internet: https://caivirtual.policia.gov.co/sites/default/files/bacib_007.pdf

[27] ECONOMIA, Digital, La silicona y el 'skimming': los fraudes más comunes en cajeros automáticos. [en línea]. (15 de marzo de 2018), [Consultado: 23 de octubre de 2018]. Disponible en Internet: https://www.economiadigital.es/finanzas-y-macro/silicona-skimming-fraudes-cajeros-automaticos_543278_102.html.

Como característica principal se destaca que puede cometerse tanto en cajeros automáticos como en establecimientos de comercio de cualquier tipo con complicidad de sus empleados. El perpetrador sustenta su accionar en un dispositivo denominado “skimmer”, que una vez en su posesión o instalado en el cajero automático permite leer la banda magnética de la tarjeta y copiar su información. Lo preocupante o sensible de dicha modalidad es lo fácil que puede resultar la adquisición del dispositivo por cualquier persona, con tan solo tener la intención se puede efectuar la compra en páginas de ventas por internet.

Figura 6 Resultado búsqueda “skimmer tarjeta” página Aliexpress



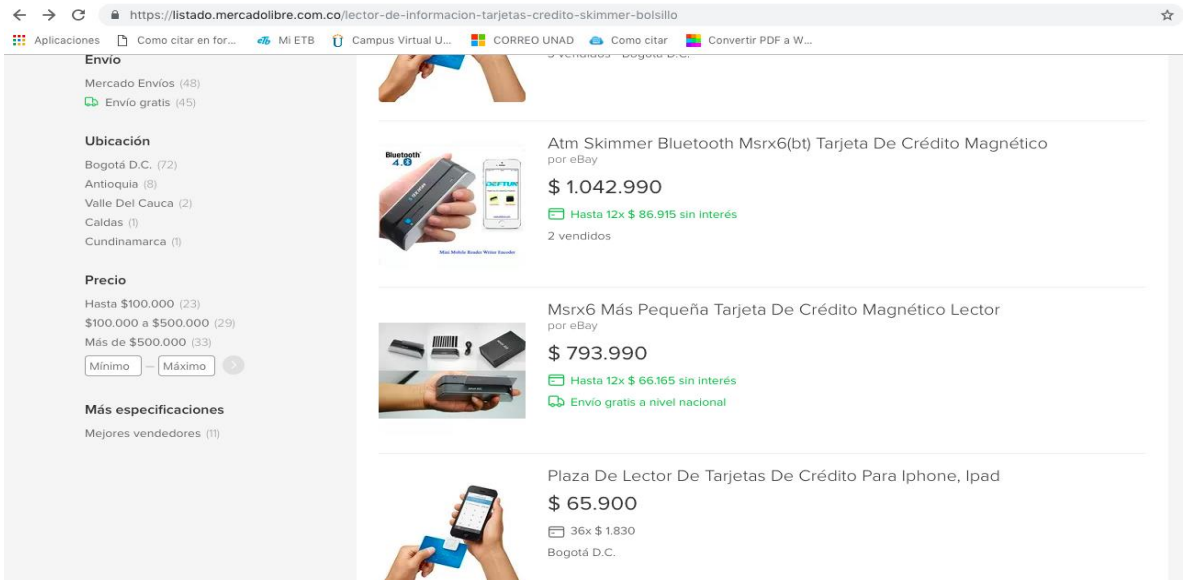
FUENTE: DURAN, Resultado búsqueda “skimmer tarjeta” página Aliexpress. [Fotografía]. Bogotá D.C. 2018. [Consultado: 01 de noviembre de 2018]. Disponible en Internet: https://es.aliexpress.com/af/cardskimmer.html?site=esp&SearchText=card+skimmer&g=y&origin=n&needQuery=n&spm=a219c.search0604.0.0.b806326dWzxiRb&jump=afs.

En las imágenes presentadas a (ver figura 6 y 7) es posible evidenciar el resultado de la búsqueda de dichos dispositivos en páginas de comercio tales como Aliexpress y Mercado Libre, en donde el costo puede oscilar desde los setenta y

cinco mil pesos hasta un millón de pesos moneda colombiana, dependiendo de las características y efectividad del dispositivo se presenta la variación en el precio.

Para que el delincuente logre perpetrar su conducta efectúa un sin número de maniobras que facilitan su actuar ilícito, entre ellas se destacan las siguientes:

Figura 7 Resultado búsqueda "skimmer tarjeta" Mercado Libre Colombia



FUENTE: DURAN, Resultado búsqueda "skimmer tarjeta" **Mercado Libre Colombia**. [Fotografía]. Bogotá D.C. 2018. [Consultado: 01 de noviembre de 2018]. Disponible en Internet: https://listado.mercadolibre.com.co/lector-de-informacion-tarjetas-credito-skimmer-bolsillo.

Cámara Estenopeica: Consiste en instalar una pequeña cámara sin lente muy cerca del cajero automático, es un método sofisticado el cual permite grabar en video mientras la victima ingresa su pin, la información recolectada es transmitida a un dispositivo ubicado a no más de cien metros de distancia.

Espiar o distraer a la víctima: Si el cajero donde se realiza la transacción permite algún tipo de oportunidad, un cómplice o el delincuente mismo puede tratar de observar por encima del hombro el PIN que digite el usuario. Aunque esto puede sonar demasiado ingenuo las habilidades de los delincuentes suelen ser amplias a

la hora de cometer ilícitos. Así mismo puede entablar algún tipo de conversación o generar distracción para de manera muy ágil generar la copia con un dispositivo de mano.

Teclado de PIN fraudulento: El perpetrador se encarga de ubicar un teclado de PIN falso sobre el original del cajero haciéndose pasar por un técnico.

El “Buen Samaritano”: El delincuente se encarga de bloquear la ranura de ingreso de la tarjeta con una banda metálica o de plástico, realizada la transacción y generar el error el delincuente lo observa y se acerca a la víctima con la supuesta intención de ayudar sugiriéndole que digite nuevamente la clave de PIN mientras él lo observa, el cajero retiene la tarjeta y el perpetrador la recupera después de que el usuario se marcha del lugar.

Ataques de Malware: Es una modalidad en incremento en la actualidad, consiste en instalar software malicioso a un cajero especifico el cual compromete el funcionamiento de la máquina, algunos de estos programas no solo se encargan de comprometer la seguridad del cajero, sino que también permiten realizar retiros por parte del delincuente y en la denominación deseada.

Aunque la modalidad ha logrado ser mitigada en gran porcentaje gracias a la implementación de tarjetas con chip, los delincuentes en su ingenio, a diario promueven la adaptación de nuevas técnicas que permitan llevar a cabo su objetivo, por lo que la clonación ha mutado a la recolección de la información de la tarjeta mediante el dispositivo ya mencionado complementando con la adaptación de una micro cámara en el cajero el cual permite observar la información faltante (por ejemplo el denominado CVV o código de seguridad) para ser transmitido luego o en tiempo real mediante una conexión wifi a un ordenador en donde se almacena la información.

La Policial Nacional de Colombia plantea ciertas recomendaciones estratégicas para evitar al máximo tal modalidad, ya que, aunque las entidades financieras promueven ciertas iniciativas y herramientas anti-skimming, la adopción de medidas personales siempre cumplirá un rol fundamental en la prevención;

Previo a la utilización de un cajero automático es importante verificar que no se encuentre presente ningún tipo de dispositivo o aparato extraño en todo el componente y especialmente en el sector de ingreso de la tarjeta o teclado numérico.

- Cuando realice pagos con su tarjeta nunca la pierda de vista y cuándo se la devuelvan, verifique que los datos en ella sean suyos.
- Nunca acepte ayuda de extraños al realizar transacciones en cajeros automáticos.
- Revise frecuentemente el saldo de sus cuentas bancarias.
- No confíe en la amabilidad de extraños al momento de realizar transacciones.
- En lo posible, trate de ocultar su clave mientras la digita, podría haber micro cámaras instaladas.
- Sí detecta alguna anomalía en el cajero, informe de inmediato a su entidad bancaria o a la línea de emergencias de la Policía Nacional.

En restaurantes o estaciones de gasolina:

- Realice la operación personalmente, no entregue su tarjeta a terceros.
- Cubra el teclado cuando digite la clave.
- Nunca olvide firmar el comprobante de pago.
- Cerciórese de que su tarjeta sea deslizada una sola vez y por un solo dispositivo; cuando se la devuelvan verifique que sea la suya. No arroje a la

basura los comprobantes de pago en los cuales estén registrados datos personales (firma, teléfono, número de tarjeta o número de cédula).[28]

[28] POLICIA NACIONAL DE COLOMBIA, ¿Sabe qué es el “skimming”?, Policía Nacional página Oficial (25 de Noviembre de 2015), [Consultado: 08 de Noviembrede 2018]. Disponible en Internet: https://www.policia.gov.co/noticia/%C2%BFsabe-qu%C3%A9-es-el-%E2%80%9Cskimming%E2%80%9D.

7 EL CARDING EN LA LEGISLACIÓN COLOMBIANA.

Conocidos los mencionados aspectos y ampliadas las formas de ejecución se hace importante distinguir la jurisdicción existente y planes de los estados para combatir de manera eficiente y eficaz a los cibercriminales que a diario idean y mejoran sus estrategias de ataque. De acuerdo con la última publicación hecha por la Policía Nacional sobre incidentes informáticos en Colombia publicado en el 2017, En Colombia se registran 15.565 en los últimos 3 años[29], cifra que representa un valor significativo si tenemos en cuenta que es una modalidad que poco se percibe en nuestro entorno financiero, por lo cual se sustenta la importancia de asignar un alto valor a su atención y precaución. Siendo conocedor de tal flagelo en Colombia se han venido adoptando medidas que promueven la seguridad de la información; para un mayor entendimiento de dicha jurisdicción se plantea la siguiente tabla:

Ley 1273 del 5 de enero de 2009	Documento CONPES 3701 de 2011
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	Política pública nacional propuesta que se establece con el fin de abordar las incertidumbres, los riesgos, las amenazas, las vulnerabilidades y los incidentes digitales. El Gobierno nacional expidió los lineamientos de política para ciberseguridad y ciberdefensa.
Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga,	Posterior a ella Esta política concentró los esfuerzos del país en contrarrestar el incremento de las amenazas informáticas que lo afectaban

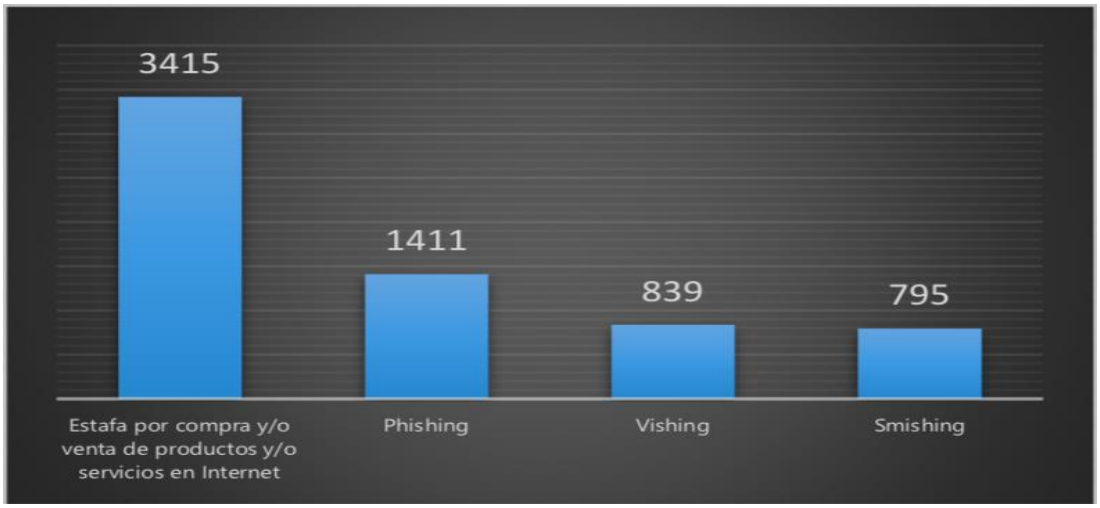
[29] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES, Impacto de los Incidentes de seguridad Digital, Colombia, 2017.

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.	significativamente, y en desarrollar un marco normativo e institucional para afrontar retos en aspectos de seguridad cibernética.
Artículo 269G: Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.	

A pesar de la jurisdicción existente y las sanciones descritas en la norma, la Policía Nacional de Colombia reporta en su informe de amenazas del cibercrimen 2016-2017 unas cifras contundentes en casos reportados sobre las distintas modalidades de carding en nuestro país (ver figura 8), tan solo en estafas por compra de y/o ventas de productos y/o servicios en internet se reportan un total de casos de 3415, en modalidad de Phishing 1411, en Vishing 839 y Smishing 795. Cabe anotar que

no es tenida en cuenta un gran número de casos que los usuarios dejan de reportar en algunas ocasiones por pena frente a lo que les ha ocurrido o simplemente por evitar ocupar su tiempo en la denuncia.

Figura 8 Reporte de casos en Colombia modalidades de Carding



FUENTE: POLICÍA NACIONAL, Dirección de Investigación criminal e interpol, Caracterización del cibercrimen. [Diagrama]**.** Amenazas del cibercrimen en Colombia 2016-2017. Marzo 2017. Colombia. [Consultado: 01 de noviembre de2018]. Disponible en internet: https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-2017.pdf.

Pero todo no es negativo es dichos aspectos, la efectividad de la estrategia y jurisprudencia en nuestro país es demostrable mediante los resultados operativos y casuística presente de la cual se puede destacar lo siguiente:

En septiembre de 2019 en el municipio de Málaga Santander la Policía de Santander capturó a un hombre de 49 años de edad cuando intentaba instalar un dispositivo electrónico al interior de un cajero automático, para acceder a las claves de las tarjetas de los usuarios de la entidad bancaria y hurtar el dinero de sus cuentas.

Según las investigaciones, por medio de la clonación de tarjetas de crédito y débito, el sujeto estafó a 500 personas en Santander, a quienes logró sacarles de sus cuentas bancarias la suma de $20 millones de pesos.
El coronel Jaime Escobar, comandante del departamento de Policía de Santander, indicó que el capturado no solo clonaba las tarjetas de las víctimas, sino se las bloqueaba para que éstas no pudieran usarlas más.

"Logrando estafar a estas personas con sistemas de bloqueo y clonación de tarjetas. Fue capturada la persona en el momento en el que estaba colocando uno de estos dispositivos electrónicos, de esta manera en Málaga logramos la captura de este sujeto, sacándolo de circulación", indicó el oficial.

Aseguró que, aunque el clonador de tarjetas hurtaba pequeñas cantidades de dinero a sus víctimas, si se suma la afectación a las 500 personas, se puede determinar que la cifra robada por el sujeto supera los 20 millones de pesos.

"Podríamos estar hablando de sumas que superan los 20 millones de pesos, estamos hablando de que, en cada transacción a pesar de ser pequeñas cantidades, si sumamos las 500 tarjetas afectadas es una gran suma de dinero y una estafa", explicó el coronel Jaime Escobar.

Las alertas electrónicas que lanzaban las entidades bancarias a sus usuarios, como el bloqueo de las tarjetas, permitió que las autoridades iniciaran un proceso investigativo en contra del capturado, quien realizaba hasta dos transacciones desde una misma cuenta, pero con diferente dispositivo electrónico para la clonación de tarjetas débito y crédito.[30]

[30] RCNRADIO, Blanco. S., Clonador de tarjetas estafó a 500 personas y robó más de $20 millones. [En línea]. (06 de septiembre de 2018), [Consultado: 23 de marzo de 2019]. Disponible en Internet:

Otro caso significativo ocurrió en mayo de 2017 donde la Fiscalía señala a cinco personas de integrar una banda delincuencial dedicada a suplantar a dueños de tarjetas de crédito para realizar millonarias compras en establecimientos comerciales.

De acuerdo con el ente acusador, tres hombres y dos mujeres eran los encargados de elaborar cédulas falsas con las fotografías de los suplantadores, pero con los datos de los dueños legítimos de esas identificaciones. Posteriormente, se comunicaban con la línea de servicio al cliente de los bancos en donde las víctimas tenían tarjetas de crédito y pedían que bloquearan las tarjetas, ya fuera por hurto o pérdida.

Luego, dice la Fiscalía, se dirigían a una oficina de atención al público y solicitaban, con el documento falso, la reexpedición de una tarjeta, “la cual utilizaban hasta llenar el cupo máximo de la misma con la compra de electrodomésticos, especialmente televisores de alta gama y teléfonos celulares”.

Otra modalidad era a través del denominado cambiazo. Llamaban a las víctimas y se hacían pasar como miembros de la entidad financiera. Les ofrecían beneficios, como el aumento del cupo de la tarjeta y un cobro inferior de la cuota fija mensual.

En el momento en que las víctimas aceptaban dichos beneficios, eran visitados por los suplantadores para hacer el cambio de tarjeta: les entregaban una falsa y se quedaban con la original para realizar compras de electrodomésticos que eran comercializados después en el centro sur de la capital.

---

https://www.rcnradio.com/colombia/santanderes/clonador-de-tarjetas-estafo-500-personas-y-robo-mas-de-20-millones.

De acuerdo con la investigación, el valor de las defraudaciones superó los $816 millones, entre diciembre de 2016 y marzo de 2017.

Según la Fiscalía, los procesados -señalados de integrar la banda Los Guajiros- deben responder por el delito de concierto para delinquir con fines de falsedad en documento público, ideológico y material con circunstancias de agravación punitiva por el uso, y por el punible de estafa en concurso homogéneo y sucesivo.[31]

7.1 CARDING EN EL ÁMBITO ORGANIZACIONAL

En el ámbito organizacional es preciso traer a colación como referencia el estudio realizado por parte del ministerio de las TICs en compañía de la OEA y el Banco Interamericano de Desarrollo el cual mide el impacto de los incidentes de seguridad digital para el año 2017 en Colombia, de él se puede destacar lo siguiente:

Cuando se pregunta a las organizaciones colombianas si creen que están preparadas para hacer frente a un incidente digital, un promedio simple del 37% de las empresas que participaron del estudio (empresas de los sectores Servicios, Industria y Comercio) cree que estaban preparadas para manejar un incidente digital. En cuanto al tamaño de estas empresas, el 70% de las grandes empresas se sienten muy preparadas o preparadas para gestionar un incidente digital, frente al 45% de las microempresas. Cuando se realiza la misma pregunta a las entidades públicas, uno de los resultados encontrados es que la mayoría de las entidades a nivel nacional se sienten preparadas. Los participantes del estudio en el nivel nacional indicaron que el 13% y el 48%, se sentían muy preparados o preparados, respectivamente. No obstante, cuando se compara con las entidades territoriales de

[31] EL ESPECTADOR, Bogotá. Así suplantaban a dueños de tarjetas de crédito en Bogotá. [En línea]. (05 de enero de 2018), [Consultado: 10 de marzo de 2019]. Disponible en Internet: https://www.elespectador.com/noticias/bogota/asi-suplantaban-duenos-de-tarjetas-de-credito-en-bogota-articulo-693714

orden municipal y departamental, los datos muestran que tan solo el 28%, a nivel municipal, y el 38%, a nivel departamental, se sintieron muy preparados o preparados para manejar un incidente.[32]

De acuerdo con lo anterior es posible generar un concepto sobre el nivel de preparación y conciencia con que cuentan las organizaciones actualmente en nuestro país, postulado importante a la hora plantear el conocimiento frente a los criterios de carding y sus modalidades. Aunque se ha realizado un recorrido importante por todo a lo que ella refiere es oportuno generar puntos de vista desde el ámbito organizacional.

Siendo así el estudio también género un interrogante que se alinea con lo desarrollado a través de todo el escrito; ¿Qué tipos de incidentes digitales, amenazas cibernéticas o ataques cibernéticos ha identificado su entidad/empresa durante el año 2016?, arrojando como resultado que el malware y el phishing se encontraban entre los tipos de incidentes más comunes. Se observó que, dentro del sector de Servicios, el 50% de los que respondieron notaron un aumento en los ataques de malware, 47% de phishing, 39% de ataques basados en web y 18% de ataques de denegación de servicio. En el sector Comercio, se hicieron observaciones similares con un 53% reportando un incremento en el malware, un 41% reportó un aumento en el phishing y un 21% notó un incremento tanto en ataques basados en web como en ataques de denegación de servicio. Curiosamente, sin embargo, hubo algunas variaciones dentro del sector Industria en esta observación, ya que el 67% reportó un incremento en la gravedad de los ataques basados en web y el malware y el 59% reportó un aumento en los ataques de phishing.[33]

[32] COLOMBIA, MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES, Impacto de los Incidentes de seguridad Digital, Colombia, 2017. 130pag.

[33] COLOMBIA, MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES, Impacto de los Incidentes de seguridad Digital, Colombia, 2017. 130pag.

Dichas estadísticas confirman e incremento anual que ha venido tomado la modalidad de phishing, no solo a nivel personal sino organizacional, resaltando la importancia de conocer ampliamente las connotaciones de la misma con el fin de mitigar la ocurrencia de la misma.

Conocidos tales postulados es propicio generar el siguiente interrogante; ¿Cómo ha afectado a las empresas el tema del carding en Colombia e internacionalmente?, para ello se presenta una recolección de casos empresarial que han trascendido en los últimos años:

Figura 9 Presentación Casos de referencia empresarial

Organización	Hechos y connotaciones
Equifax	En septiembre de 2017 la multinacional Estadounidense Equifax (agencia de informes de créditos al consumo) informo de un ciberataque que comprometió información de crédito sensible de un alto porcentaje de ciudadanos de ese país, el hackeo lo ejecutaron dos jóvenes bajo el nombre de PastHole Hacking Team, que gestaron el golpe entre mayo y junio de dicho año. El robo de datos se descubrió hasta finales de julio. Sin embargo, no fue hasta el 7 de septiembre cuando la empresa reconoció lo sucedido. Equifax alego que un agujero del servidor web Apache había sido el causante del ciberataque, pues el mismo se había solucionado a mediados de año, pero la empresa no había instalado el parche a tiempo. Allí pudo abrirse la puerta a los criminales para acceder a la información sensible. [34]

[34] EDECONOMIADIGITAL, Redacción. Así se gestó el hackeo financiero a la multinacional estadounidense Equifax. [En línea]. (16 de septiembre de 2017), [Consultado: 22 de marzo de 2019]. Disponible en Internet:

Marriot	En noviembre de 2018 la cadena hotelera Marriot emitió una comunicación la cual dejaba en evidencia la vulneración a una de sus bases de datos lo cual puso en riesgo la información de una cantidad notable de clientes de la cadena hotelera. Marriott recibió una alerta de una herramienta de seguridad interna con respecto a un intento de acceder a la base de datos de reservas en Starwood en Estados Unidos, así se logró comprobar que había habido acceso no autorizado a la red de Starwood desde 2014. La compañía descubrió recientemente que una parte no autorizada había sido copiada y la información había sido codificada y tomó medidas para eliminarla. El 19 de noviembre de 2018, Marriott pudo descifrar la información y determinó que el contenido era de la base de datos de reservas de Starwood.[35]
RAPPI	En octubre de 2018 se presentaron a través de redes sociales múltiples denuncias relacionadas con la aparición de pagos por concepto de compras no realizadas por parte de usuarios de la aplicación, frente a tal eventualidad se generó una investigación que determino que Rappi no uso los métodos estándar de seguridad ni se tomaron las precauciones necesarias. Específicamente, la compañía recolectó los datos de tarjetas desde su página web usando un protocolo de seguridad inadecuado y obsoleto para ese fin: operaban desde su página web. Desde que se reportó el incidente, Rappi tardó

https://www.economiadigital.es/tecnologia-y-tendencias/asi-se-gesto-el-hackeo-financiero-a-la-multinacional-estadounidense-equifax_508497_102.html.

[35] SUNSENTINEL. Valdez, Y. Alerta: Marriott anuncia robo masivo de datos de clientes...qué hacer para protegerte. [En línea]. (30 de noviembre de 2018), [Consultado: 23 de marzo de 2019]. Disponible en Internet: http://touch.sun-sentinel.com/#section/-1/article/p2p-109807162/.

	61 días en resolverlo. Ahora, los datos de las tarjetas no van directamente al procesador de pagos, sino que pasan por los servidores de la nube (o lo que es igual, AWS) administrados por Rappi desde donde, se estima, agregan las tarjetas al compartimento seguro. [36]
Uber	La plataforma de servicio Uber ha venido creciendo significativamente en los últimos años a nivel global, su esencia radica en el uso de vehículos particulares como forma de transporte público, inicialmente su uso dependía de brindar la información de una tarjeta de crédito para garantizar el pago del servicio, pero dicha condición produjo que en el año 2016 se generara una violación a dichos protocolos, lo grave del asunto fue que tal vulneración fue ocultada por la compañía por casi un año, como resultado de la falla se despidieron dos empleados quienes fueron los culpables del hecho, entre la información sustraída se destaca correos electrónicos, números de teléfono, identificaciones e información sensible de más de 500000 conductores de la empresa.[37]

FUENTE: DURAN, Jonathan. Recopilación de información bibliográfica plasmadas en las referencias 34, 35, 36 y 37. [Tabla]. Bogotá D.C. 2018. Presentación casos referencia empresarial.

Casos como los anteriormente mencionados, dan a conocer que sin importar la magnitud o connotación de la organización las amenazas siempre estarán latentes

[36] INFOTECHNOLOGY. Infotechnology. Falla de seguridad en Rappi deja expuestas las tarjetas de crédito. [En línea]. (23 de octubre de 2018), [Consultado: 26 de marzo de 2019]. Disponible en Internet: https://www.infotechnology.com/online/Falla-de-seguridad-en-Rappi-deja-expuestas-las-tarjetas-de-credito-20181023-0001.html.

[37] CICESE. Seguridad de la información. UBER ESCONDIÓ UN GRAVE HACKEO DURANTE UN AÑO. [En línea]. (23 de noviembre de 2017), [Consultado: 28 de marzo de 2019]. Disponible en Internet: https://seguridad.cicese.mx/alerta/296/Uber-escondi%C3%B3-un-grave-hackeo-durante-un-a%C3%B1o.

y representaran un porcentaje amplio de atención para el liderazgo de la misma, el año 2019 plantea grandes retos en el ámbito operacional, a pesar de las lecciones que ha dejado el mundo corporativo en los últimos años en cuanto a las vulnerabilidades que implica estar conectados, un reporte de la consultora EY que consultó a 1.400 líderes de riesgo y seguridad cibernética de algunas de las organizaciones más grandes del planeta, reflejó que el 80% de las juntas directivas no hacen de la ciberseguridad un tema estratégico para sus compañías. El 87% de las organizaciones todavía operan con niveles limitados de ciberseguridad y resiliencia, mientras que el 77% trabaja con medidas de protección básicas en materia de ciberseguridad y buscan avanzar hacia capacidades más alineadas con la realidad.

Entre tanto, la mayoría de las organizaciones (el 77%) están dispuestas a buscar este año más allá de las técnicas básicas de seguridad cibernética para perfecciones sus capacidades, haciendo uso de tecnologías avanzadas como inteligencia artificial, automatización robótica de procesos y analítica de datos, entre otras.[38]

7.2 CARDING EN EL ÁMBITO PERSONAL

Al desarrollar tal postulado es importante mencionar que todas las acciones anteriormente descritas plantean las diferentes formas de afectación que puede sufrir un tarjetahabiente por el solo de hecho de ser acreedor de tal producto. Lo que realmente debe conocerse son las diferentes modalidades ya planteadas para evitar estos medios de perpetración, aunque la responsabilidad principal de promover la seguridad de la información recae en la entidades prestadoras de servicio, nos damos cuenta que no siempre la perpetración del carding depende

[38] DINERO. Ciberseguridad. Guía de ciberseguridad para el 2019. [En línea]. (06 de enero de 2019), [Consultado: 01 de abril de 2019]. Disponible en Internet: https://www.dinero.com/tecnologia/articulo/ciberseguridad-en-el-2019-en-colombia/265858.

exclusivamente de brechas o fallos de seguridad en la red o bases de datos, sino en la pericia del delincuente quien con distintas estrategias puede llegar a inducir a la víctima a coadyuvar con el cumplimiento de su objetivo o simplemente caer en su juego. Es importante para el ciudadano del común que tanto las empresas privadas como el gobierno nacional a diario promueven estrategias en pro de minimizar dichos riesgos y que su conocimiento puede ser fundamental para la prevención de los mismos.

Una de estas herramientas está en cabeza de la Policía Nacional de Colombia, quien mediante la implementación del CAI virtual o centro cibernético policial que busca la focalización en la denuncia de los diferentes delitos que aquejan nuestro país diariamente. En dicha plataforma es posible hallar información de interés en aspectos de ciberseguridad, servicios, ciber incidentes, entre otros. Además, allí es posible realizar denuncias sobre situaciones que el usuario considere relevantes a fin de prevenir y actuar en cuanto a estas conductas. Para más información la página está disponible en el URL https://caivirtual.policia.gov.co.

Figura 10 Presentación Centro Cibernético Policial

FUENTE: POLICÍA NACIONAL, Dirección de Investigación criminal e interpol. Centro Cibernético Policial. [Fotografía]. [Consultado: 15 de abril de 2019]. Disponible en internet: https://caivirtual.policia.gov.co/

8 CONCLUSIONES

Aunque el Carding es considerado por algunos como una modalidad delictiva emergente, tienen sus inicios de bastante tiempo atrás, su conocimiento se ha extendido debido al potenciamiento del internet y las redes sociales

Existen métodos de perpetración de la conducta tanto físicos como digitales, es importante generar una diferenciación entre ambos tipos, sin desorientar la finalidad de la misma.

La ingeniería social, aunque puede parecer una técnica ingenua, cobra cantidad de víctimas diariamente, es importante crear conciencia situacional para evitar caer en dicha modalidad.

Dentro de las formas de digitales de perpetración de la conducta hallamos el phishing, vishing y smishing, cada uno, aunque con características similares representan una actuación con diferentes connotaciones.

El skimming ha representado un porcentaje amplio de afectación a empresas y personas, pero con la adaptación de tarjetas con chip se logró una disminución significativa en la comisión de la conducta.

La destreza de los delincuentes no tiene límites, a medida que pasan los años y se adoptan medidas para la mitigación de la conducta, surgen nuevas maneras de perpetración, las cuales seguirán siendo un desafío para la seguridad, de allí la importancia de conocer y actualizar los conceptos frente a las modalidades delictivas.

Aunque la jurisdicción colombiana es drástica con la imposición de sanciones sobre los delitos, esto no es impedimento para su comisión, es importante que las organizaciones y ciudadanía generen las respectivas denuncias para su investigación y judicialización.

9 RECOMENDACIONES

Es importante generar recomendaciones que permitan crear conciencia al público en general tanto en el ámbito personal como organizacional frente a la ocurrencia en las modalidades de la conducta, por tanto, es propicio plantear lo siguiente:

- Plantear programas de prevención dentro de la organización que permitan el conocimiento y cursos de acción para la mitigación de la conducta.
- Potenciar la alerta situacional en acciones que representan comercio electrónico y demás transacciones en las cuales se pueden presentar modalidades de estafa.
- Consultar con las respectivas entidades financieras antes de adquirir cierto producto (tarjeta crédito-debito) las garantías y políticas en cuanto a seguridad de la información que ofrece el ente para evitar ser víctima de algunas de las modalidades de Carding ya antes vistas.
- Aunque se cuente con protección por parte de las entidades financieras para la aprobación de transacciones, es relevante recordar que el ingenio del delincuente puede hacer que en ocasiones la victima apruebe de manera inconsciente movimientos o revele datos sensibles que amenacen la seguridad.
- En cuanto a lo concerniente al skimming, se debe tener presente que es posible la alteración de los distintos cajeros automáticos con dispositivos que permiten la clonación de tarjetas, y que no solo finaliza ahí la modalidad, también delincuentes pueden dar apariencia de benevolencia y amabilidad con el único fin de observar claves.
- En el entorno laboral se debe generar pruebas a los empleados, en donde se permita establecer el grado de vulnerabilidad frente a modalidades de carding, para con los resultados de estas plantear estrategias de acción.

10 REFERENCIAS

1. ARTEAGA, Sahnya. Delito: Crimen Electrónico citado por MORANTES, Ceudiel, Fraude electrónico financiero en Colombia, Bogotá 2010, 20p, Trabajo de grado para optar al título de Especialista en Administración de la Seguridad, UMNG, Facultad de relaciones internacionales, estrategia y seguridad, Cundinamarca.

2. AVAST, Hacker. [En línea]. [Consultado: 14 de febrero de 2018] Disponible en internet: https://www.avast.com/es-es/c-hacker.

3. BBC mundo, “Los secretos del cibercrimen organizado para robar tarjetas de crédito”. [en línea] [Consultado: 05 de noviembre de 2017]. Disponible en internet:(http://www.bbc.com/mundo/noticias/2014/11/141110_tecnologia_crimen

4. BBVA, Seguridad, ¿Qué es el VIshing? [en línea]. BBVA página oficial. (25 de noviembre de 2015), [Consultado: 08 de octubre de 2018]. Disponible en Internet: https://www.bbva.com/es/vishing-la-imaginacion-los-estafadores-no-limites/.

5. CICESE. Seguridad de la información. UBER ESCONDIÓ UN GRAVE HACKEO DURANTE UN AÑO. [En línea]. (23 de noviembre de 2017), [Consultado: 28 de marzo de 2019]. Disponible en Internet: https://seguridad.cicese.mx/alerta/296/Uber-escondi%C3%B3-un-grave-hackeo-durante-un-a%C3%B1o.

6. COLOMBIA. CONGRESO DE LA REPÚBLICA. SENADO DE LA REPÚBLICA. Diario Oficial No. 47.223 ley 1273 del 5 de enero 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.

7. COLOMBIA. CONSTITUCION POLITICA DE COLOMBIA. Congreso de la república. Gaceta Constitucional No. 116 de 20 de julio de 1991.

8. COLOMBIA LEGAL CORPORATION, Edición, ¿Qué se considera un delito? [en línea]. Asesores legales especialistas, [Consultado: 15 de enero de 2019]. Disponible en Internet: https://colombialegalcorp.com/se-considera-delito/.

9. COLOMBIA, MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES, Impacto de los Incidentes de seguridad Digital, Colombia, 2017. 130pag.

10. COLOMBIA. Instituto Colombiano de Normas Técnicas y Certificación, NTC 5613, Referencias bibliográficas. Contenido, forma [en línea]. Bogotá: 2008 33 p. [Consultado: agosto 12 de 2017]. Disponible en Internet: ¿https://www.politecnicojic.edu.co/images/downloads/biblioteca/guias/NTC5613.pdf

11. COSTAS, Jesús. Seguridad y alta disponibilidad. Madrid: RA-MA Editorial, 2014. 227 p.

12. CULTURACION, “Carding: El fraude con tarjetas de crédito”. [en línea]. [Consultado 05 noviembre de 2017]. Disponible en internet: (http://culturacion.com/carding-el-fraude-con-tarjetas-de-credito/)

13. DEPARTAMENTO NACIONAL DE PLANEACIÓN, Consejo Nacional de Política Económica y Social, Bogotá, Política Nacional de seguridad Digital, 2016.

14. DINERO. Ciberseguridad. Guía de ciberseguridad para el 2019. [En línea]. (06 de enero de 2019), [Consultado: 01 de abril de 2019]. Disponible en Internet: https://www.dinero.com/tecnologia/articulo/ciberseguridad-en-el-2019-en-colombia/265858.

15. DOEVAN, Jake, “QUÉ ES UN CARDING Y CÓMO ELIMINARLO”, Los Virus. [En línea]. [Consultado 06 noviembre de 2017] Disponible en https://losvirus.es/carding/.

16. ECONOMÍA, Digital, La silicona y el 'skimming': los fraudes más comunes en cajeros automáticos. [En línea]. (15 de marzo de 2018), [Consultado 23 de octubre de 2018]. Disponible en Internet: https://www.economiadigital.es/finanzas-y-macro/silicona-skimming-fraudes-cajeros-automaticos_543278_102.html.

17. ECONOMIA, “Fraude online más común sigue siendo a tarjetas de crédito”, El Espectador. [En línea]. [Consultado 06 noviembre de 2017]. Disponible en internet: https://www.elespectador.com/noticias/economia/fraude-online-mas-comun-sigue-siendo-tarjetas-de-credit-articulo-628856).

18. EDECONOMIADIGITAL, Redacción. Así se gestó el hackeo financiero a la multinacional estadounidense Equifax. [En línea]. (16 de septiembre de 2017), [Consultado: 22 de marzo de 2019]. Disponible en Internet: https://www.economiadigital.es/tecnologia-y-tendencias/asi-se-gesto-el-hackeo-financiero-a-la-multinacional-estadounidense-equifax_508497_102.html.

19. EL ESPECTADOR, Bogotá. Así suplantaban a dueños de tarjetas de crédito en Bogotá. [En línea]. (05 de enero de 2018), [Consultado: 10 de marzo de 2019]. Disponible en Internet: https://www.elespectador.com/noticias/bogota/asi-suplantaban-duenos-de-tarjetas-de-credito-en-bogota-articulo-693714.

20. EL TIEMPO, Tecnología. Ojo con correo falso de Apple que roba sus datos bancarios. [En línea]. (05 de enero de 2018), [Consultado: 10 de marzo de 2019]. Disponible en Internet: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/correo-falso-de-apple-roba-sus-datos-bancarios-171332

21. ESET, Editor, 5 cosas que debes saber sobre la Ingeniería Social [en línea]. Welivesecurity. (6 d enero de 2016), [Consultado: 07 de octubre de 2018]. Disponible en Internet: https://www.welivesecurity.com/la-es/2016/01/06/5-cosas-sobre-ingenieria-social/.

22. FINANZAS PERSONALES, “Los tipos de robos que hacen a través de las tarjetas”. [En línea]. [Consultado 05 noviembre de 2017]. Disponible en: http://www.finanzaspersonales.co/credito/articulo/los-robos-pueden-hacer-tarjetas/53157.

23. INFOTECHNOLOGY. Infotechnology. Falla de seguridad en Rappi deja expuestas las tarjetas de crédito. [En línea]. (23 de octubre de 2018), [Consultado: 26 de marzo de 2019]. Disponible en Internet: https://www.infotechnology.com/online/Falla-de-seguridad-en-Rappi-deja-expuestas-las-tarjetas-de-credito-20181023-0001.html.

24. KASPERSKY, Lab. ¿Qué es el spear phishing? [En línea]. [Consultado: 14 de febrero de 2018] Disponible en internet: https://latam.kaspersky.com/resource-center/definitions/spear-phishing.

25. KASPERSKY, ¿Qué es un botnet? - Definición [En línea]. [Consultado: 14 de febrero de 2018] Disponible en internet: https://latam.kaspersky.com/resource-center/threats/botnet-attacks

26. MARISOL, “Qué es la ingeniería social y cómo protegerse de ello”, Tarjetas de crédito hoy. [En línea]. [Consultado 06 noviembre de 2017]. Disponible en. https://tarjetasdecreditohoy.com/que-es-la-ingenieria-social-y-como-protegerse-de-ello-a-sus-tarjetas/.

27. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES, Impacto de los Incidentes de seguridad Digital, Colombia, 2017.

28. MITNICK, Kevin y SIMON, William. El arte de la intrusión: la a verdadera historia de las hazañas de Hackers, intrusos e impostores. 1 ed. Madrid: RA-MA Editorial, 2007. 349 p.

29. MORANTES, Ceudiel, Fraude electrónico financiero en Colombia, Bogotá, 2010, 20p, Trabajo de grado para optar al título de Especialista en Administración de la Seguridad, UMNG, Facultad de relaciones internacionales, estrategia y seguridad, Cundinamarca.

30. NORTON, Security, ¿Qué es el smishing? Norton by Symantec. [En línea]. [Consultado: 22 de octubre de 2018] Disponible en internet: https://co.norton.com/internetsecurity-emerging-threats-what-is-smishing.html.

31. LISTEK, V. “Tarjetas de crédito: las 5 formas de estafas que más preocupan a todos”, La nación argentina. [En línea]. {06 noviembre de 2017} disponible en internet: http://www.lanacion.com.ar/1862899-tarjetas-de-credito-las-5-formas-de-estafas-que-mas-preocupan-a-todos.

32. LOBOS, Elkjaer, El temido "skimmer" [en línea]. 24 horas. (3 de agosto de 2012), [Consultado: 06 de noviembre de 2018]. Disponible en Internet: https://www.24horas.cl/nacional/conoce-el-skimmer-lo-mas-utilizado-para-clonar-tarjetas-250832.

33. LUNA, Cesar. Perfil criminológico de un delincuente informático. [En línea]. [Consultado: 13 de febrero de 2019]. Disponible en Internet: http://www.derecho.usmp.edu.pe/centro_inv_criminologica/revista/articulos_revista/2013/Articulo_Prof_Cesar_Ramirez_Luna.pdf.

34. POLICIA NACIONAL DE COLOMBIA, ¿Sabe qué es el “skimming” ?, Policía Nacional página Oficial. [En línea]. (25 de noviembre de 2015), [Consultado 08 de noviembre de 2018]. Disponible en Internet: https://www.policia.gov.co/noticia/%C2%BFsabe-qu%C3%A9-es-el-%E2%80%9Cskimming%E2%80%9D.

35. POLICÍA NACIONAL, Dirección de Investigación criminal e interpol, Caracterización del cibercrimen. [En línea]. Amenazas del cibercrimen en Colombia 2016-2017. Marzo 2017. Colombia. [Consultado: 01 de noviembre de2018]. Disponible en internet: https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-2017.pdf.

36. POLICÍA NACIONAL, Dirección de Investigación criminal e interpol, [En línea]. Boletín de Análisis en Ciberseguridad, El sobrino retenido-estafa VISHING. Colombia. (07 febrero de 2016) [Consultado: 01 de enero de 2019]. Disponible en internet: https://caivirtual.policia.gov.co/sites/default/files/bacib_007.pdf

37. RAMÍREZ, W. Carding: conoce cómo roban las tarjetas de crédito: mdz. [En línea] (2017) [Consultado 05 noviembre de 2017]. Disponible en internet: http://www.mdzol.com/nota/514175-carding-conoce-como-roban-las-tarjetas-de-credito/.

38. RCNRADIO, Blanco. S., Clonador de tarjetas estafó a 500 personas y robó más de $20 millones. [En línea]. (06 de septiembre de 2018), [Consultado: 23 de marzo de 2019]. Disponible en Internet: https://www.rcnradio.com/colombia/santanderes/clonador-de-tarjetas-estafo-500-personas-y-robo-mas-de-20-millones.

39. RIVERO, Mario. GOTTSCHALK, Franz, Los Ataques de Skimming en Cajeros Automáticos y Cómo Prevenirlos. [en línea]. (26 de febrero de 2014), [Consultado 14 de noviembre de 2018]. Disponible en Internet: https://usa.visa.com/dam/VCOM/download/merchants/Webinar-Preventing-ATM-Skimming-Spanish-021914.pdf.

40. TECNOLOGIA, BBC mundo, “Los secretos del cibercrimen organizado para robar tarjetas de crédito”. [En línea]. [Consultado 05 noviembre de 2017]. Disponible en internet: http://www.bbc.com/mundo/noticias/2014/11/141110_tecnologia_crimen_organizado_cibercrimen_tarjetas_credito_ig).

41. URBANO, S. “Fraudes con tarjetas de créditos”, economía finanzas. [En línea]. [Consultado 06 noviembre de 2017] Disponible en internet: https://www.economiafinanzas.com/fraudes-con-tarjetas-de-creditos/).

42. SAVVIDES, Lexy, “Cómo proteger tu tarjeta de crédito cuando compres online'”, cnet. [En línea]. [Consultado 05 noviembre de 2017]. Disponible en internet: https://www.cnet.com/es/como-se-hace/como-proteger-tarjeta-de-credito-cuando-compras-por-internet/).

43. SEGURIDAD DE LA INFORMACION, Amenazas Humanas - Carding – Trashing, segu.info. [En línea]. [Consultado 05 noviembre de 2017] disponible en internet: (http://www.segu-info.com.ar/amenazashumanas/cardingtrashing.htm).

44. SEMANA, “Reglas de oro para evitar fraudes con tarjetas de crédito”. [En línea]. [Consultado 06 noviembre de 2017]. Disponible en internet: http://www.semana.com/economia/articulo/como-evitar-los-fraudes-en-las-tarjetas-de-credito/534427).

45. SUNSENTINEL. Valdez, Y. Alerta: Marriott anuncia robo masivo de datos de clientes...qué hacer para protegerte. [En línea]. (30 de noviembre de 2018), [Consultado: 23 de marzo de 2019]. Disponible en Internet: http://touch.sun-sentinel.com/#section/-1/article/p2p-109807162/.