BENEMÉRITA UNIVERSIDAD AUTÓNOMA DE PUEBLA

FACULTAD DE DERECHO Y CIENCIAS SOCIALES

ESTUDIO TELEOLÓGICO DEL CARDING Y BINS. SU IMPUNIDAD E IMPACTO EN EL SISTEMA BANCARIO MEXICANO

Tesis para obtener el título de
LICENCIADO EN DERECHO

PRESENTA
DANIEL SANCHEZ TORRES

DIRECTOR:
DR. JOSÉ ALFREDO MUÑOZ CARRETO

FEBRERO 2020

AGRADECIMIENTOS

***A mi familia**, por haberme dado la oportunidad de perseguir mis sueños, y haber sido mi apoyo durante todo este tiempo.*

***Al Dr. José Alfredo Muñoz Carreto**, quien me ha acompañado en estos años de investigación cómo director de tesis, debatiendo, estructurando, y sistematizando el conocimiento nuevo que se expone en esta tesis. Gracias por haberme dejado un legado en la investigación, motivándome a escribir un libro y a seguir investigando.*

***Al Mtro. Luis Alberto González Rosas** por haberme orientado y motivado, no solo en la elaboración de este trabajo de titulación, sino a lo largo de mi carrera universitaria y haberme brindado el apoyo para desarrollarme profesionalmente y seguir especializándome en temas legales de ciberseguridad.*

***A la Benemérita Universidad Autónoma de Puebla**, por haberme acogido en sus aulas, dándome la oportunidad de desarrollar mi potencial intelectual, y a desarrollarme como abogado e investigador.*

Tabla de Contenido

Índice de Tablas

INTRODUCCIÓN

Esta investigación se desarrolla como respuesta intelectual ante un fenómeno delictivo que provoca millones de pérdidas económicas, un atraso en el sistema de pagos con tarjetas bancarias y una deficiente inclusión financiera tecnológica: los ciberdelitos financieros del Carding y BINS.

El principal objetivo de la presente investigación es exponer, analizar y estudiar en que consiste el Carding como fenómeno que engloba otras conductas delictivas como los BINS, sus elementos, características, análisis legal, proyecciones e impunidad. Al ser delitos que surgen de la evolución de las nuevas tecnologías de la información y comunicación, combinado con la inclusión del sistema de pagos con tarjetas bancarias, provoca que sean delitos "nuevos" muy poco estudiados. La investigación explicará de manera sistemática como están compuesto estos ciberdelitos del Carding y BINS para su futura investigación, prevención y combate

Desde un primer instante es importante destacar que existe una diferencia entre un ciberdelito, un delito informático, un delito telemático y un delito cibernético. Para este fin el tesista, clasifica a estos cuatro conceptos en dos teorías, la primera de ellas denominada *teoría clásica,* en el que se engloba a los conceptos de delito informático, y cibernético, caracterizada porque la mayoría de definiciones respecto al tema se escribieron con la idea primigenia de la operatividad básica de los delitos conforme al tiempo tecnológico que se vivía en el momento, sin embargo, en la *teoría moderna,* se caracteriza por que se adapta a las nuevas operatividades respecto a las conductas delictivas que se hacen en, por, o con las nuevas herramientas de las tecnologías de la información y comunicación. Para este propósito, en el capítulo uno de la presente investigación se expone que delito telemático es aplicable a la mayoría de las conductas del carding, sin embargo, los delitos informáticos también participan en una pequeña parte del carding, y que *delito cibernético* es técnicamente incorrecto, por lo que, para englobar a los delitos informáticos y telemáticos, se ocupará el término de *ciberdelitos.*

La investigación parte desde un método inductivo, ocupando la técnica de la observación directa no participante, es decir, que el tesista se puso en contacto

directo con el fenómeno del Carding, sin que participará en el, recogiendo información para su estudio y análisis. La investigación fue de tipo longitudinal, es decir, que se estudió el fenómeno del Carding entre el 2015 y 2019 para sistematizar los elementos que se exponen, y sus características.

La presente tesis cuenta con tres capítulos, el primero de ellos denominado “Carding”, con siete subtemas, el primero de ellos conceptúa al Carding, que, a forma de introducción es la generación, obtención, administración, comercialización y uso de información o números de tarjetas bancarias; se explica que el carding no solamente afecta a las tarjetas bancarias, sino también a tarjetas departamentales, y la información que contenida en ellas. Se explica la enorme diferencia entre una conducta tradicional ya que esta afecta directamente al plástico *per se* y el carding, que afecta a la información o números de la tarjeta, sin que el plástico esté presente.

Posteriormente en primer capítulo punto dos, se explican las conductas del fenómeno del Carding, ya que no es independiente, y cuenta con muchas modalidades. Estas conductas son la generación, obtención, administración, comercialización y uso de información o números de tarjetas bancarias. En la conducta de obtención se explican las técnicas más utilizadas por los ciberdelincuentes para obtener la información o números de tarjetas bancarias, en las que encontramos las técnicas del *SQL injector-dumper, data leakage* o fuga de datos, ingeniería social*,* fuerza bruta*, spam-phishing pharming, keyloggers, robo de credenciales, sniffing, skimmer* remoto, y sabanas de información.

En el tema uno punto tres se explican las diferencias entre, conductas tradicionales y conductas del carding, ya que el objeto material, sujetos pasivos, técnicas, métodos y tipo penal son diferentes. Para este fin, se detallan que en las conductas del carding se distinguen del resto por que no son conductas presenciales, porque debe existir el uso de las nuevas tecnológicas como comisión del delito, y porque el objeto material de la acción son la información o números de la tarjeta bancaria.

En el siguiente tema, uno punto cuatro, se explican la clasificación de ciberdelincuentes, bineros y carders, que son ocho categorías y sus características de cada uno de estos. Esta información permitirá realizan un estudio especializado para la asociación delictuosa del Carding.

En el punto siguiente, se estudia el cuadro normativo del Carding, para ver si se encuentra tipificado en la legislación mexicana, analizando la Ley General de Títulos y Operaciones de Crédito, la Ley de Instituciones de Crédito, el Código Penal Federal, Código Nacional de Procedimientos Penales, y nivel Estado, el Código Penal del Estado de Puebla. Así mismo, se estudia que el Carding es un delito pluriofensivo, que afecta al patrimonio y a la información, a diferencia de las conductas tradicionales. También se distingue que en el Carding es importante distinguir quienes son los ofendidos y las victimas conforme a cada una de las técnicas que se exponen en el punto dos de la presente investigación, para valorar las implicaciones jurídicas del mismo. En el mismo punto, se explica, porque es un delito especial federal, y no un delito estatal, debido al principio de especialidad y competencia de los jueces federales penales.

Finalmente, en el punto siete del primer capítulo se estudia porque el carding debe clasificarse como un delito nuevo, y no como uno más del catálogo de delitos existentes.

En el capítulo dos se estudia a los BINS. Estos parten de conducta del carding, denominada generación, pero por su extensa explicación e importancia se estudia en un capitulado diferente. Se inicia explicando cuales son los elementos para que los números de una tarjeta bancaria sean procesados correctamente, datos objetivos como el nombre, edad, dirección del titular y datos subjetivos básicos técnicos como el *PAN (Primary Account Number),* fecha de vencimiento y código de seguridad.

En consecuencia, se explica las subconductas que conforman a los BINS y su operatividad, ocupándose como ejemplo el algoritmo de *luhn,* como referente tecnológico de los ciberdelincuentes en la evolución de optimizar sus conductas delictivas.

En el tercer y último capítulo, se explican las medidas para prevenir y combatir el Carding y los BINS. Se analiza primeramente desde un carácter internacional, desde normas de seguridad de datos en la industria de tarjetas de pago (*PCI DSS),* así como estándares internacionales, como normas *ISO*, que aportarían criterios para permitir la interoperabilidad de los números de identificación bancaria.

En un segundo nivel se estudia las medidas nacionales, como es la circular de Banco de México, 34/2020; medidas legislativas, la ley para regular las Instituciones de Tecnología Financiera, que de manera indirecta previenen ciertas conductas del Carding. Así mismo se estudian las atribuciones que tiene la Comisión Nacional Bancaria y de Valores y la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros frente al Carding.

Se estudia en el punto tres del último capítulo cuales han sido las medidas que han optado las entidades emisoras para prevenir el carding, como es la creación de *wallets,* sistemas de alertas, *tokens*.

Por último, se analizan los datos del Carding a nivel Federal y en el Estado de Puebla. La notoria diferencia de reportes recibidos en la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros y las denuncias ante el Ministerio Público Federal.

Es importante destacar que en el dos mil diecisiete las ciberconductas del Carding superaron a las tradicionales, denotando que el Carding está evolucionando y desarrollándose. Para este momento, existen tres épocas del fenómeno, la tradicional que engloba a las conductas con el plástico *per se*, el carding como el fenómeno que se conoce y se describe en esta investigación, y el *neocarding*, que es la evolución de las conductas delictivas de las nuevas formas de pago, como es el CODI y haciendo uso de inteligencia artificial.

Esta investigación es la antesala de futuras investigaciones del *neocarding,* ya que respeta los elementos esenciales y primarios del fenómeno, por lo que es importante continuar con su investigación para su prevención y combate.

CAPÍTULO 1. CARDING

1.1. Concepto de Carding

El Carding es un anglicismo[1] compuesto por la unión de dos palabras inglesas que aluden a sus elementos principales: por un lado, *card* que significa tarjeta, y por otro lado *using* gerundio cuya traducción al español es usar, en el que intervienen dos factores elementales, uno es la información o números contenidos en las tarjetas bancarias exclusivamente –sin ser necesario el plástico- y el otro es el uso de las nuevas tecnologías como la informática y telemática.

En un principio, las conductas delictivas con tarjetas, ya sean bancarias, no bancarias o departamentales, de crédito, débito o de servicios eran muy elementales, empero, por diferentes factores sociales, tecnológicos, y financieros se desarrollaron cinco grandes conductas, tipos o modalidades del Carding que son la generación, obtención, administración, comercialización y uso de números o información contenida en las tarjetas bancarias.

Carding es un fenómeno criminógeno desarrollado paralelamente al uso de las nuevas tecnologías con las que se produce, obtiene, administra, comercializa o se usa información o números de tarjetas bancarias o no departamentales con el objetivo de alcanzar un lucro indebido.

Al referirse al Carding, se escribe específicamente sobre la información o números contenidos en la tarjeta, y no del plástico *per se*, aunque *a priori* pareciera ser lo mismo, no lo es. Es menester diferenciar los elementos, características y *modus de operandi* de este nuevo fenómeno para comprender y entender su forma en la que se desarrolla, para tener herramientas y los medios necesarios para combatirlo, logrando la reducción de riesgos del sistema de tarjetas bancarias en el sistema financiero mexicano, alcanzando un

[1] Los anglicismos son palabras originarias de la lengua inglesa pero que son empleadas en el idioma español. Fuente: Cáceres Ramírez, Orlando, *Anglicismos*, consultable en: https://www.aboutespanol.com/anglicismos-2879601, consultado el 16 de junio de 2019.

sistema sólido, seguro y adecuado.

Diversos autores e instituciones conceptualizan al Carding solo desde algunas de sus modalidades, a saber, la Procuraduría General de la Republica[2] describe al Carding como el *uso fraudulento de números de tarjetas*, en la que se clasifica dentro del tipo o modalidad de uso. La CONDUSEF[3] menciona que Carding es una forma de estafa *online*[4] que consiste en *acceder ilegalmente al número de una tarjeta bancaria y a través de un software*[5] *generan de manera aleatoria la fecha de expiración y el código de seguridad*. Por su parte Ojeda Pérez, Jorge *et, al.*[6] establecen que Carding *es el delito de clonación de tarjetas*. Por su parte PROFECO[7] se refiere que el Carding es la *utilización ilegal de tarjetas de crédito*. Acosta Patroni[8] expone que el Carding, o tarjeteo, es el uso ilegal de tarjetas de crédito.

---

[2] Procuraduría General de la República, *Cibercriminalidad, delitos en la red,* D.F., Instituto Nacional de Ciencias Penales, 2006, p, 31.

[3] Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros*, Checa tu estado de cuenta y cuídate del Carding,* consultable en: https://www.gob.mx/condusef/articulos/checa-tu-estado-de-cuenta-y-cuidate-del-carding?idiom=es consultado el 23 de junio de 2019.

[4] *Online*, en español "en línea" significa que está disponible o se realiza a través de internet. Fuente: Léxico, *on line,* consultable en: https://www.lexico.com/es/definicion/on_line, consultado el 16 de noviembre de 2019.

[5] El *software* es la parte lógica que dota al equipo físico de capacidad para realizar cualquier tipo de trabajo. Fuente: Tejeda Anaya, María Antonieta, *Software*, consultable en: https://www.uaeh.edu.mx/docencia/P_Presentaciones/prepa4/informatica/Software_1.pdf, consultado el 17 de junio de 2019.

[6] Ojeda Pérez, Jorge Eliécer et al., *Delitos Informáticos y entorno jurídico vigente en Colombia,* 2010, p. 51*,* consultable en: https://dialnet.unirioja.es/descarga/articulo/3643404.pdf, consultado el 11 de diciembre de 2018.

[7] PROFECO, *El lado oscuro de Internet*, 2006, consultable en: https://www.profeco.gob.mx/encuesta/brujula/bruj_2006/pdf06/2006-11-13%20El%20lado%20oscuro%20de%20Internet.pdf consultado el 11 de diciembre de 2018.

[8] Acosta Patroni, Alejandro, *Hacking, Cracking y Otras Conductas Ilícitas Cometidas a Través de Internet*, 2003, p. 108, consultable en: http://repositorio.uchile.cl/bitstream/handle/2250/114475/de-acosta_a.pdf consultado el 15 de diciembre de 2018.

En sentido amplio, Beltramone[9] menciona que *se llama Carding a la actividad de cometer un fraude o una estafa con un número de tarjeta de crédito*, así mismo señala que el Carding consiste entonces *en usar un número de tarjeta de crédito -ya sea real o creado de la nada mediante procedimientos digitales- para realizar compras a distancia por Internet y efectuar pagos.*

Por su parte Amador[10] expone que Carding es un término usado para describir un uso no autorizado de la tarjeta de crédito, cuenta bancaria u otra información financiera de una víctima. Avilés Gómez[11] menciona que *es la utilización de tarjetas de crédito ajenas o su número, otra variante de esta técnica es la creación fraudulenta de números de tarjetas de crédito*, y también aunando al concepto mencionan que se trata de conseguir los números y claves de tarjetas de crédito a través de la Red para hacer cargos a las mismas.

Existen diferentes tipos de tarjetas, en el capítulo dos de la presente investigación se describe con más detalle el uso, clasificación, elementos y características que debe tener una tarjeta, no obstante, *a priori* se expone que hay tarjetas bancarias que pueden ser de crédito o débito que pertenecen al sistema financiero mexicano y que expiden las sociedades mercantiles o bancarias. En una tarjeta de crédito, el emisor se compromete a pagar las obligaciones que el titular contraiga con los establecimientos comerciales afiliados, y el titular se obliga a reembolsar las cantidades adelantadas por el emisor; por su parte en la tarjeta de débito, el titular dispone de su dinero en una cuenta bancaria.

Las tarjetas no bancarias son aquellas que tienen origen en un contrato en el que un establecimiento comercial otorga a su cliente para que pueda utilizarlas

---

[9] Beltramone, Guillermo, et al, *Nociones básicas sobre los Delitos Informáticos, Santiago,* 1998, p.10, consultable en: http://rodolfoherrera.galeon.com/delitos.pdf consultado el 17 de octubre de 2019.

[10] Hackett Bergmann, Caesars, *Carding Delito Informático,* 2018, consultable en: https://medium.com/@caesarshackettbergmann/carding-v-bfa5f94a750e, consultado el 15 de abril de 2019.

[11] Avilés Gómez, Manuel, *Delitos y delincuentes. Cómo son, cómo actúan*, Alicante, Editorial Club Universitario, 2010, p. 30.

para la adquisición de bienes y servicios en su misma empresa o en establecimientos afiliados. Las tarjetas departamentales o no bancarias están reguladas en la Ley General de Títulos y Operaciones de Crédito.

Para fines de esta investigación al referirse a tarjetas se entenderán a las tarjetas bancarias, y no bancarias ya sean de crédito, débito o de servicios.

1.2. Conductas que integran al Carding y su *modus operandi*

El Carding es un fenómeno que está formado por cinco tipos, conductas o modalidades, que son la generación, obtención, administración, comercialización y uso de información o números de tarjetas. Estas amplias modalidades del carding son debido a la evolución de las nuevas tecnologías y al *modus operandi* de los criminales. Seria equivoco conceptualizar al Carding desde sólo algunas de sus modalidades, como pueden ser uso de números de tarjetas o la generación de información ya que no se incluirían a las nuevas conductas que son indispensables para comprender el fenómeno en su conjunto.

1.2.1. Generación.

Esta modalidad del Carding es sumamente amplia, ya que cuenta con otros subtipos, además de que tiene un gran impacto en el fenómeno, en el subsistema financiero mexicano y sistema bancario de pagos, por lo que se describirá con detalle en el capítulo segundo de la presente investigación, en la que se conceptualiza que es un BIN, los subtipos, que son la producción, alteración, verificación, y obtención de números de tarjetas bancarias, su *modus operandi*, y la importancia del algoritmo de *luhn*[12] como referente tecnológico de las conductas de los criminales.

1.2.2. Obtención de números de tarjas bancarias.

Las nuevas tecnologías como la informática y la telemática traen consigo una evolución en los sistemas de pago del sistema financiero, y de los sistemas de seguridad, asimismo, brinda nuevas herramientas y medios informáticos a los criminales para que puedan perfeccionar sus conductas delictivas. Las ventajas

[12] En el capítulo 2.4 de la presente investigación se explica en que consiste el algoritmo de *luhn.*

de estás nueva tecnologías son dos, la primera son las herramientas tecnológicas para conseguir información o números de tarjetas bancarias y la segunda es el anonimato, provocando que sean factores primordiales para que el Carding se desarrolle.

A continuación, se describen las técnicas más comunes que emplean estas personas para la obtención de información o números de tarjetas bancarias.

I. ***SQL injector-dumper[13]***.

Es un ataque por medio de una herramienta denominada *SQL DUMPER,* por su significado en Inglés *Structured Query Language,* que en español significa *lenguaje de consulta estructurada;* la función que utilizan los criminales es que ingresan de manera remota a los servidores con deficiencias en su seguridad informática, descargando, modificando o copiando las tablas que se encuentren en su servidor; las tablas pueden tener todo tipo de información desde datos objetivos: nombres, domicilios, fechas de nacimiento, etc., hasta datos subjetivos, como son el *PAN[14]*, en otras palabras, los criminales ingresan por medios informáticos a páginas o servidores de internet. Este ataque es masivo y no se limita a un sólo país, ya que el servidor de Internet es mundial, sin embargo, se puede seleccionar el parámetro de búsqueda únicamente de páginas que se presuman como mexicanas o de cualquier otra nacionalidad. Una vez dentro del servidor se descarga toda la información o números de tarjetas con el objetivo de usarlas para sí o para comercializarlas.

[13] Alessandro Elia, Ivano, et al, *Comparing SQL Injection Detection Tools Using Attack Injection: An experimental Study,* consultable en: https://ieeexplore.ieee.org/abstract/document/5635053, consultado el 17 de enero de 2019.

[14] PAN, por sus siglas en *Primary Account Number,* significa Número de Cuenta Principal, sirven para distinguir una tarjeta de otra. Fuente: Acosta, David, *¿Cómo funcionan las tarjetas de pago? Parte I: PAN (Primary Account Number), consultable en* https://www.pcihispano.com/como-funcionan-las-tarjetas-de-pago-parte-i-pan-primary-account-number/, consultado el 11 de junio de 2019.

Al respecto de este método, no se necesitaba ser un gran conocedor de redes, puesto que existen *softwares*[15] libres que, por medio de unos pocos pasos, realizan automáticamente los procesos para extraer información de números de tarjetas.

Por ejemplo, en una página *web*[16] de un establecimiento comercial, donde de manera previa ya se han realizado compras de bienes o servicios por parte de los titulares de las tarjetas quedado guardado en el mismo servidor, el *PAN*[17] consistente en los números de identificación de una tarjeta, la fecha de vencimiento y el código de seguridad, datos subjetivos necesarios para la compra por internet.

La información se encuentra encriptada debido a los estándares internacionales del *PCI DSS*[18] sin embargo, esto no es un obstáculo para las personas que se dedican a obtener información o números de tarjetas, ya que existen programas gratuitos o de paga en internet que sirve para desencriptar la información de una manera sencilla, por ejemplo, *Reverse Hash Tools v3.3*[19].

---

[15] Op. cit., 5.

[16] *Web*, literalmente telaraña de alcance mundial, es un término usado en informática cuya traducción podría ser Red Global Mundial o "Red de Amplitud Mundial"; es un sistema de documentos de hipertexto o hipermedios enlazados y accesibles a través de Internet. Fuente: EcuRed, *web*, consultable en: https://www.ecured.cu/Web, consultado el 17 de noviembre de 2019.

[17] Op. cit., 14.

[18] *PCI DSS* por sus siglas en inglés *Payment Card Industry Security Standars* que significa Estándar de Seguridad de Datos de la Industria de tarjetas de Pago. Es un estándar de seguridad orientado a la definición de controles para la protección de los datos del titular de la tarjeta y/o datos confidenciales de autentificación durante su procesamiento, almacenamiento y/o transmisión. Fuente: Acosta, David, *¿Qué es PCI DSS?,* consultable en: https://www.pcihispano.com/que-es-pci-dss/, consultado el 27 de noviembre de 2019.

[19] *Reverse Hash Tools* significa “herramientas de hash inverso”. Es un *software* que escanea multiprocesos MD5, MD4, SHA-1/256/384/512, RIPEMD-128/160 y otros hashes para la presencia de sus bases de datos en línea, con la capacidad de agregar nuevos y editar servicios existentes. Fuente: *Online Reverse Hash Tool. V.3.3,* consultable en

A finales del 2017, está técnica fue casi obsoleta, porque los sistemas de seguridad de las páginas invirtieron muchos millones de dólares en desarrollar nuevos mecanismos sofisticados de seguridad, limitando el área del actuar de estos criminales. Como *Mozila Firefox*[20] que a través de su programa denominado *Web Bug Bounty*[21] recompensaba a todo aquel que encontrara errores en esta técnica de obtención de números de tarjetas bancarias, apoyando a plataformas y páginas *web*[22] debido a que muchos de estos utilizan su sitio *web*[23] para comunicarse y coordinar su actividad.

Los criminales han buscado nuevos métodos telemáticos e informáticos para seguir usando está técnica, sin embargo, ya quedan pocas personas que explotan el *SQL*[24]. A estos sujetos se les conoce como criminales de cuello blanco, debido a su habilidad en conocimiento de redes e informática, siento un sujeto activo con características especiales.

II. D*ata leakage*[25] o fuga de datos*.*

https://appo.pro/11-online-reverse-hash-tool-v33-orht-v33.html, consultado el 27 de noviembre de 2019.

[20] Mozilla Firefox es un navegador web de código abierto y software libre, desarrollado por la Fundación Mozilla, Fuente: EcuRed, *Mozilla Firefox,* consultable en: https://www.ecured.cu/Mozilla_Firefox, consultado el 27 de noviembre de 2019.

[21] Su traducción al español es web generosa, sin embargo es recomendable respetar el nombre del programa en su idioma original, Fuente: Mozilla, *Preguntas Frecuentes,* consultable en: https://www.mozilla.org/en-US/security/bug-bounty/faq-webapp/, consultado el 17 de junio de 2019.

[22] Op. cit., 16.

[23] Op. cit., 16.

[24] Op. cit., 13.

[25] La fuga de datos o *Date Leakage* es la trasmisión no autorizada de datos desde una organización a un destino o destinatario externo. Fuente: Ciber Edu, *What is Data Leakage,* consultable en: https://www.forcepoint.com/cyber-edu/data-leakage, consultado el 17 de junio de 2019.

Acurio del Pino[26] señala que esta técnica también es conocida como divulgación no autorizada de datos reservados, además escribe que es una variedad del espionaje industrial, por la cual se sustrae información confidencial de una empresa, por parte del personal que tengan carácter de consejero, funcionario o empleados, a estas personas son llamados *insiders*[27].

Algunas de los empleados son corrompidas por asociaciones delictivas que buscan personal dentro de las entidades emisoras para controlar la información desde adentro, ofreciéndoles una comisión por las actividades que se generen del Carding.

La razón por la que está considerada dentro de las técnicas del Carding, es porque el principal medio de contacto de los *insiders*[28] y las personas que compran la información o números de tarjetas es por la red mundial, internet, y en especial por las redes sociales.

III. **Ingeniería Social:**

Es la práctica de manipular psicológicamente a las personas para que compartan información confidencial o hagan acciones inseguras para vulnerar su seguridad. La diversidad en las herramientas tecnológicas es la base de esta técnica y el engaño, ya que utilizan todas las herramientas disponibles para lograr su propósito, puede ir desde correos electrónicos, mensajes en redes sociales hasta mensajes codificados en la *Deep web*[29].

---

[26] Acurio del pino, Santiago, *delitos informáticos*: *generalidades*, consultable en: https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf consultado el 13 de octubre de 2018, p.27.

[27] Proviene del inglés y quiere decir “el que está dentro”. Fuente: Quintero, Antonio, *Definición de Insider*, 2018, consultable en: https://www.economiasimple.net/glosario/insider, consultado el 17 de noviembre de 2019.

[28] Op. cit., 27.

[29] La *Deep web* es aquella parte de la red que contiene material, información, y páginas web que no están indexadas en ningún de los buscadores existentes. Fuente: Carles, Joan, *Acceder a la*

Está técnica puede estar vinculada a otras técnicas más, y es la más factible dentro de una sociedad con una mala educación en temas tecnológicos.

IV. **Fuerza Bruta;**

Consiste en la utilización de *scripts*[30] o de *softwares*[31] para la automatización de procesos. Es parecido al método de los BINS para la obtención de información o números de tarjetas bancarias, la única diferencia es que los BINS es un proceso sistematizado, y este como su nombre lo indica es rudimentario.

Los pasos son los siguientes:

1. Identificación de página e-commerce[32] que acepte el pago de bienes o servicios que ofrece mediante tarjeta y que no cuente con un alto sistema de seguridad o con los medios de seguridad descritos en el capítulo tres punto cinco de la presente investigación.
2. Creación de los procesos automatizados o *scripts*[33], con la finalidad de generar decenas o centenas de *PAN*[34], por medio de una tarjeta base, además de que se generan sus códigos de seguridad, y fecha de vencimiento (véase capítulo 2 de la investigación).
3. Se verifica la información de manera individual, hasta que se procese con éxito la orden de compra.

Deep web de forma segura, 2013, consultable en: https://geekland.eu/acceder-a-la-deep-web/, consultado el 28 de junio de 2019.

[30] El *script* es un proceso informático que contiene instrucciones escritas en códigos de programación. Fuente: *Script,* consultable en: https://www.significados.com/script/, consultado el 10 de noviembre de 2019.

[31] Op. cit., 5.

[32] El *E-commerce* consiste en la distribución, venta, compra, marketing y suministro de información de productos o servicios a través de Internet. Fuente: Rodríguez, Cristina, *¿Qué es E-commerce o comercio electrónico*?, 2015, consultable en: https://marketingdigital.bsm.upf.edu/e-commerce-comercio-electronico/, consultado el 13 de enero de 2019.

[33] Op. cit., 30.

[34] Op. cit., 14.

4. Si no se tiene éxito, se borra historial, se elimina el *cache*[35], y se repite el paso tres.

Está técnica puede ocuparse de manera eventual, teniendo pocas probabilidades de éxito, o bien, de manera profesional, en donde se desarrollan programas informáticos especializados en este tema, teniendo grandes resultados. Actualmente es poco usada.

V. ***Spam – phishing[36]***

El *spam* es definido como correo basura no deseado, no solicitado o de algún contacto desconocido que son enviados de manera masiva. Por su parte en el *phishing*[37] los criminales se hacen pasar por alguna institución financiera o por algún establecimiento mercantil en internet, en la que piden a la víctima que actualice la información de su cuenta personal, para copiar su información confidencial de sus tarjetas; el *modus operandi* es el siguiente:

- **Etapa preparatoria**: Se envían correos masivos a las personas, simulando ser una institución financiera o algún establecimiento mercantil.

[35] El *cache* es aquella cantidad de información que permanece de manera temporal en la computadora. Fuente Bembibre, Victoria, *Definición de Memoria Cache,* consultable en: https://www.definicionabc.com/tecnologia/memoria-cache.php, consultado el 17 de junio de 2019.

[36] El *phishing* es el acto de intentar engañar al destinatario de un correo electrónico malicioso para que lo abra y siga sus instrucciones. Fuente: Akamai, *¿Qué es el phishing?,* consultable en: https://www.akamai.com/es/es/resources/what-is-phishing.jsp, consultado el 17 de noviembre de 2019.

[37] Op. cit., 36.

- **Etapa Media**: Hacen creer a la persona que el correo, el *link*[38] o la página *web*[39] es de toda confianza, sin darse cuenta de que es una imitación de la página que es controlada por el criminal.
- **Etapa de Espera:** El criminal espera que la víctima ingrese a la página e inserte su información, pensando que es un sitio seguro, escribiendo, entre otros datos, su nombre, su domicilio, *el PAN*[40] fecha de vencimiento, y código de seguridad, inclusive en algunas veces su *NIP*[41].
- **Etapa conclusiva:** La información es obtenida por el criminal, para ser usada para sí o para ser comercializada.

La CONDUSEF[42] expresa que el *phishing*[43] también es conocido como suplantación de identidad.

La misma Comisión[44] señala que existe una técnica similar denominada *smishing*[45] que consiste en enviar mensajes *SMS*[46] al teléfono móvil con la misma finalidad que el *phishing*[47].

---

[38] Un *link*, también llamado hipervínculo o enlace, es un elemento conector que facilita la navegación en sitios web y la base del trabajo. Fuente *¿Qué es un link? Definición y tipos de enlaces*, consultable en: https://powertoyourseo.com/blog/es/que-es-un-link/, consultado el 17 de noviembre de 2019.

[39] Op. cit., 16.

[40] Op. cit., 14.

[41] Número de Identificación Personal.

[42] Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, *Fraudes Financieros ¡No te dejes engañar!,* consultable en https://www.gob.mx/cms/uploads/attachment/file/240481/FRAUDES_FINANCIEROS_web.pdf consultado el 22 de junio de 2019 p. 16.

[43] Op. cit., 36.

[44] Ídem.

[45] Su nombre viene de la combinación de las siglas SMS, que significan Short Messaje Service y de la técnica *phishing*. Fuente: Rouse, Margaret, *Short Message Service*, consultable en: https://searchmobilecomputing.techtarget.com/definition/Short-Message-Service, consultado el 18 de junio de 2019.

[46] Ídem.

[47] Op. cit., 36.

VI. ***Pharming[48]*:**

Es un tipo de fraude que cumple el mismo objetivo que el *phishing*[49]: robo de información financiera del usuario de servicios financieros. Este tipo de técnica[50] se realiza cuando una aplicación o programa se instala en el ordenador de la víctima, y al ingresar a un determinado sitio *web*[51], se redirecciona a otra página *web*[52] predeterminada por el atacante con el mismo diseño y apariencia que la original con el fin de obtener claves, contraseñas y números de cuenta.

Se diferencia del *phishing*[53] porque este se envía mediante *spam*[54] o mensajes, sin embargo, el *pharming*[55] está integrado en el *software*[56], aplicación o programa.

VII. ***Keyloggers*[57].**

Un *keylogger*[58] es un programa informático o telemático[59] que registra cada tecla que se pulsa en una computadora, sin el consentimiento o conocimiento del usuario. Este método ha estado

---

[48] *Pharming* proviene de la palabra *Farm*, que significa granja y al igual que el *smishing* es una variante de la técnica *phising,* Fuente: Kaspersky, *¿Qué es el pharming y cómo evitarlo?,* consultable en: https://latam.kaspersky.com/resource-center/definitions/pharming, consultado el 18 de noviembre de 2019.

[49] Op. Cit., 36.

[50] PROFECO, "*El lado oscuro...", Op. Cit.*

[51] Op. cit..,16.

[52] Ídem.

[53] Op. Cit., 36.

[54] Ídem.

[55] OP. cit., 48.

[56] Op. Cit., 5.

[57] *Keylogger* proviene del inglés y significa "registrador de teclas". Fuente: *Que significa keylogger en español,* consultable en: https://es.bab.la/diccionario/ingles-espanol/keylogger, consultado el 18 de noviembre de 2019.

[58] Ídem.

[59] Si bien es cierto que por su naturaleza técnica entra dentro de la informática, también es cierto que con las nuevas modalidades de los keyloggers modernos, permiten la operatividad de la telemática.

presente desde hace años, en los cuales es común encontrar en lugares públicos tales como cibercafés, universidades, centros de trabajo, etc.

Cuando la víctima compra bienes o servicios en las páginas de internet, escribe en el teclado los datos subjetivos necesarios para el procesamiento exitoso de la compra (véase capítulo 2) que se quedan registrados en un archivo oculto para que el criminal lo pueda ver posteriormente.

Los *keyloggers*[60] cada día son más sofisticados, más herramientas son incluidas, en las que no únicamente registra las teclas que son pulsadas, si no también capturas de pantalla de lo que sucede cada momento, y son enviadas de manera remota al criminal.

VIII. **Robo de credenciales**

Sandra[61] menciona que el Carding se realiza robando las credenciales de acceso de algunas páginas *web*[62], sobre todo de comercio electrónico de víctimas que han utilizado estas plataformas para hacer alguna compra, aportando sus datos bancarios.

Esta técnica es parecida al *phishing*[63], y al *Pharming*[64].

IX. ***Sniffing***[65]

Víctor Gómez[66] *menciona que es una técnica que consiste en "escuchar" o capturar toda la información que circula por una red*. Es una técnica con cierto grado de preparación técnica puesto que el criminal interfiere en la comunicación de una red inalámbrica, copiando

---

[60] Ídem.

[61] Sandra López, *Carding: la nueva modalidad de fraude a tarjeta bancaria, consultable en* https://www.oinkoink.com.mx/noticias/carding-nueva-modalidad-fraude-tarjeta-bancaria/, consultado el 14 de octubre de 2018.

[62] Op. cit., 16.

[63] Op. cit., 36.

[64] Op. cit., 48.

[65] *Sniffing* proviene de la palabra *sniff* que significa "olfatear o husmear". Fuente: Cambridge Dictionary, *Sniff*, consultable en: https://dictionary.cambridge.org/es/diccionario/ingles-espanol/sniff, consultado el 18 de noviembre de 2019.

[66] Gómez, Víctor, *Sniffing,* consultable en: https://instintobinario.com/sniffing/, consultado el 18 de noviembre de 2019.

información confidencial como los datos de la tarjeta, fecha de vencimiento y código de seguridad.

X. ***Skimmer***[67] **Remoto**.

Los *skimmers*[68] son pequeños aparatos, que cuenta con una ranura que sirve para copiar la banda magnética de las tarjetas bancarias, además de que en la mayoría de estos dispositivos cuenta con una diminuta cámara fotografía que permite además de copiar la banda magnética de las tarjetas de crédito, que graba el *NIP*[69] ingresado por el tarjetahabiente. Toda la información que se obtiene se envía de manera remota a los servidores de los criminales.

XI. **Otros métodos poco estudiados**

Una técnica que desde hace tiempo está presente es conocida como “sabanas de información” que además de obtener más información como del cliente, como nombre, fecha de nacimiento, domicilio, sirve como técnica para obtener datos de tarjetas bancarias.

Está técnica sigue en proceso de investigación.

1.2.3. Administración.

Cuando se obtiene la información o los números de la tarjeta, los criminales la utilizan para dos cosas, la primera es usar dicha información para la compra de bienes o productos para sí y la segunda es para enajenarla a otros miembros que estén interesados en la compra de números de tarjetas bancarias, para esto la información la organizan, la administran y clasifican para después enajenarla en los grupos de Carding de redes sociales o páginas de internet.

---

[67] Skimmer significa espumadera, o utensilio para recoger hojas de la superficie de una piscina. Fuente: bab.la dictionary, *skimmer*, consultable en: https://es.bab.la/diccionario/ingles-espanol/skimmer, consultado el 18 de noviembre de 2019.

[68] Security Standards Council, *Skimming Prevention: Overview of Best Practices for Merchants*, consultable en: https://www.pcisecuritystandards.org/documents/skimming_prevention_overview_one_sheet.pdf consultado el 10 de noviembre de 2019.

[69] Op. cit., 41.

Las asociaciones delictivas del Carding están clasificadas en tres grupos, y cada una de ellas tiene sus propias características.

a) **Juniors o nivel 1:** Están conformado de tres a cinco miembros, se caracterizan por ser revendedores de números de tarjetas bancarias. Ninguno de los miembros sabe obtener tarjetas bancarias, por lo que tienen que comprar a otros grupos de mayo grado. Se caracterizan porque son revendedores; ocupan generalmente los números para compra de bienes y servicios para sí, y participan en el cibermercado azul[70] de manera discreta.
b) **Halfboys o nivel 2:** Están conformados de 6 a 10 miembros. Están organizados estratégicamente en el cibermercado azul[71]; sólo un miembro es el que obtiene números de tarjetas bancarias, y los demás se encargan de vender esa información a usuarios individuales o a los grupos de nivel 1.

   Cuentan con miembros especializados en falsificar documentos para poder confirmar la compra cuando alguna página de establecimiento comercial solicita más información, por ejemplo, una imagen sobre su identificación personal.

   Las compras de bienes y servicios para terceros tienen mayor peso, y este es su principal fuente de ilícitos, ya que publican diferentes ofertas en diferentes grupos en redes sociales en donde ofertan bienes o servicios a un costo mucho menor.
c) **Seniors o nivel 3:** Más de 11 miembros, esta es la categoría más peligrosa, porque son varios los que saben obtener números de tarjetas bancarias, y ejercen control en los grupos de menor nivel.

   Además de las características de los otros grupos. Tienen miembros que obtienen números de tarjetas bancarias, otros se dedican a encontrar nuevos clientes, ya sea para revenderles los números de tarjetas bancarias o para la venta de bienes y servicios a un costo menor, dichos

[70] Véase capítulo 1.2.4 de la presente investigación.

[71] Ídem.

productos que son vendidos se obtienen de manera ilícita por medio de las técnicas descritas con anterioridad.

Cuentan con miembros especializados en el proceso de BINS, además de cuentan con verificadores, otros miembros buscan vulnerabilidades en páginas de establecimientos comerciales.

1.2.4. Comercialización:

La enajenación de la información o de los números de las tarjetas bancarias tuvo su auge en el año 2015. Antes de que las redes sociales fueran de los principales espacios virtuales para la enajenación de información o números de tarjetas existían diferentes páginas en internet para el mismo fin, y más en la *Deep web*[72] en plataformas como *4chan*[73], sin embargo, la red social *Facebook* se convirtió en el principal cibermercado para la enajenación de tarjetas bancarias.

Las autoras Davara Fernández de Marcos[74] señalan que existen delitos informáticos haciendo uso de o gracias a las Redes Sociales, precisan que hay tres grandes conductas que pueden utilizar a las redes sociales para la comisión de un delito: el primero es ser víctimas de acoso, el segundo libertad de expresión llevada al extremo, y la tercera injurias y calumnias. Sin embargo, en el Carding, existe una cuarta división: la enajenación de información o números de tarjetas bancarias en el cibermercado azul.

[72] Op. cit., 29.

[73] *4chan* viene del japonés y significa literalmente “cuatro hojas”; fue creada en 2003 por Christopher Poole con la intención de que fuese un sitio donde discutir sobre mangas y animes japoneses, sin embargo, evolucionó a una plataforma en la que se albergaba contenido ilegal como pornografía infantil. Fuente: Morales, Miguel, *Qué es 4chan, el peculiar foro donde se colgó el Fappening*, 2014, consultable en: https://computerhoy.com/noticias/internet/que-es-4chan-peculiar-foro-donde-colgo-fappening-18819, consultado el 18 de noviembre de 2019.

[74] Davara Fernandez Elena, et al., *delitos informáticos*, Pamplona, Aranzadi, 2017, p. 57.

Se llama Cibermercado azul por sus principales elementos, el primero de ellos *ciber*, el diccionario de la Real Academia Española vigesimotercera edición[75] expresa que *ciber indica relación con redes informáticas.* Clasifica a este término como elemento compositivo[76], es decir, el componente, no independiente, por lo general de origen griego o latino, que interviene en la formación de palabras compuestas, anteponiéndose o posponiéndose a otras. El segundo de ellos *mercado*, porque se manejan elementos similares a lo de un mercado real, existiendo la oferta y la demanda de números de tarjetas bancarias; y el último elemento, el adjetivo azul es por analogía al mercado negro[77], con la única diferencia que es azul porque la red social más utilizable para esta conducta es Facebook, y esta se identifica por su color azul en su logo y página de internet.

El *modus operandi* de esta conducta por parte de los usuarios es el siguiente:

I. **Búsqueda**: Los compradores interesados se unen a grupos de *Facebook* para comprar números de tarjetas bancarias. Los grupos son públicos, cerrados o secretos, y muchos de ellos tienen nombres discretos tales como "panes baratos, pollos económicos, galletas para vender", sin embargo, esto no siempre fue así, anteriormente se ocupaban nombres que hacían referencia al fenómeno, como "*Carding, compra y venta* de cc, *venta de bins,* etc.".

II. **Contacto**: los vendedores de información bancaria publican anuncios en los que incluye la venta de la información bancaria, el costo, y algunas veces una especie de garantía, por ejemplo "*ccs de 500 pesos, te aseguramos 2k[78]" o "pollos a 650, garantía de 1.5".* El primer término hacen referencia a la información bancaria, en donde *ccs* significa tarjeta de crédito, por la contracción en inglés, *crédito card,* el segundo elemento

[75] Diccionario de la Real Academia Española, vigesimotercera edición, *Ciber-*., Consultable en: https://dle.rae.es/srv/search?m=30&w=ciber-, consultado el 28 de junio de 2019.

[76] Centro de Investigación y Desarrollo de Recursos Científicos BioScripts, *elemento compositivo*, consultable en: https://www.biodic.net/palabra/elemento-compositivo/#.XcIgQdJKgdU, consultado el 28 de julio de 2019.

[77] Compra venta o intercambio clandestinos de bienes y productos, que viola diferentes ordenamientos legales.

[78] La letra "K" se refiere a múltiplos de mil en pesos mexicanos.

es el precio por la información y el tercero es una especie de garantía que ofrecen por la cantidad que señalan, en donde la letra *k* significa mil pesos, en otras palabras, si la información que te venden no procesa como exitosa para la compra de bienes y servicios entonces reponen esa información por otra hasta que el pedido se procese correctamente.

III. **Acuerdo:** El comprador se pone de acuerdo con el comprador por medio de los mensajes en *Facebook*, a lo cual el comprador le pasa su número de tarjeta para una transferencia o depósito bancario, posterior a esto, el comprador realiza el pago o depósito, y envía un comprobante de pago por medio de fotografías.

IV. **Entrega de información:** El comprador envía por mensaje al comprador los datos subjetivos necesarios para la compra a distancia, envía el *PAN*[79] consistente en los números de identificación bancaria, generalmente los dieciséis o quince números de la tarjeta, la fecha de vencimiento, y código de seguridad, aunque en algunas ocasiones también envía datos objetivos del titular de la tarjeta, como el nombre, domicilio, etc.

1.2.5. Uso.

Consiste en hacer uso de la información o números de las tarjetas bancarias en compras por internet o vía telefónica de manera ilegítima, con el fin de obtener un lucro indebido.

El criminal ocupa los datos subjetivos de la tarjeta, es decir el *PAN*[80], la fecha de vencimiento y el código de seguridad, datos elementales para la confirmación de la compra, sin embargo, hay más datos que son necesarios en el momento de transacción, como son el nombre, domicilio, en algunas ocasiones el Registro Federal de Contribuyente, no obstante, esta información se puede inventar en este punto, y aunque *a priori* pareciera que la información del titular de la tarjeta registrada en el sistema de los negocios adheridos o de las instituciones bancarias tuviera que coincidir con la información que se ingresa en la compra a distancia, no es siempre así.

---

[79] Op. cit., 14.

[80] Ídem.

La compra consiste en dos pasos, el primero de ellos es la confirmación de pedido, en el cual se autoriza que la tarjeta tiene el saldo suficiente y que cumple con los requisitos de la entidad emisora para la compra en internet, el segundo es la verificación de compra, en el que el negocio adherido o la entidad emisora pueden solicitar más información al comprador para acreditar que la compra sea legítima, por lo que solicita, por ejemplo, escaneo de identificación personal, de su tarjeta, de estado de cuenta, comprobante de domicilio, etc. No obstante, esta información se puede falsificar por medio de los integrantes de los grupos delictivos del Carding, en donde tienen miembros especializaos en hacer identificaciones, estados de cuenta, comprobantes de domicilio falsos.

Andrés Mariño[81] se refiere a esta conducta como *uso fraudulento en la contratación a distancia*, y escribe que es realizada por medios electrónicos, y que la tarjeta no se presenta al establecimiento adherido en forma directa por quien disfruta de su tenencia, sino que éste transmite el número de tarjeta de crédito y sus datos identificatorios, además de que un tercero realice pagos, por medio de aquélla y nombre de éste.

El referido autor[82] escribe que el negocio adherido no puede controlar los datos subjetivos ni objetivos de la tarjeta, y que, con esta operativa, se multiplican los riesgos de utilización indebida con la tarjeta por medio de un tercero no autorizado, pues surge la imposibilidad de verificación y control por parte del establecimiento adherido de la operación de pago,

1.3. Diferencias entre conductas delictivas tradicionales y Conductas del Carding

Las conductas de conductas delictivas tradicionales respecto de tarjetas bancarias y no bancarias son diferentes a las conductas o modalidades del Carding, ya que el objeto material, los sujetos pasivos, técnicas, métodos y tipo penal son diferentes.

---

[81] Mariño López, Andrés, *Uso fraudulento de tarjetas de crédito por terceros no autorizados,* Madrid, Ediciones Jurídicas y Sociales, S.A. 2006, p.25.

[82] Ídem.

1.3.1. Conductas delictivas tradicionales

Las conductas delictivas tradicionales se distinguen por los siguientes puntos:

1.- El plástico es esencial. Es decir, que tiene que estar presente la tarjeta de manera física en las conductas que se realicen con esta. Por ejemplo, cuando un tarjetahabiente extravía su tarjeta bancaria, y una persona tercera a esta retira dinero en el cajero automático sin estar legitimado para ello, o en la falsificación física de la tarjeta, a lo que se le conoce como *clonación de tarjetas*, donde es indispensable la presencia física del plástico.

2.- La conducta delictiva tiene que ser directa y presencial. En un primer instante pareciera irracional este requisito, sin embargo, por los avances de la tecnología, actualmente se pueden cometer conductas delictivas en diferentes lugares del planeta, y en diferente temporalidad. Es importante precisar, que, aunque sea directo y presencial pueden ocuparse la tecnología o medios electrónicos, v.g.: las terminales de punto de venta usan tecnología, empero, al ser de manera directa y presencial encuadra dentro de las conductas tradicionales.

El objeto material de las conductas delictivas tradicionales es principalmente el plástico en sí mismo, aunque en algunas conductas se involucre de manera indirecta la información contenida en estas.

1.3.2. Tipos de Conductas delictivas tradicionales.

Las conductas tradicionales se dividen en obtención, falsificación, administración, comercialización y uso tarjetas plásticas *per se.*

1.3.2.1. Obtención

Para comprender mejor las técnicas tradicionales para la obtención de tarjetas bancarias de manera tradicional, y como un medio para comparar a las conductas del Carding se describen algunas de las técnicas más usuales.

a. ***Skimmer***[83]**:** Es un aparato[84] de un diminuto tamaño, cuenta con una ranura que copia la banda magnética de las tarjetas de crédito y débito, cuando son deslizadas para alguna operación. Tiene dos variantes, portátil y fijo, la portátil es frecuentemente utilizadas en lugares que acepten pago con tarjeta, y en la que el titular de la tarjeta, por factores no preste la debida atención; los lugares más frecuentes son gasolineras, cadenas comerciales, bares, pequeños y medianos negocios que tengan la modalidad de pago con tarjeta.

   Esta técnica entra dentro de la categoría de las conductas tradicionales, ya que aún al utilizar medios tecnológicos, se realiza de manera directa y presencial, teniendo acceso a la tarjeta plástica y es una relación directa entre el que realiza la conducta delictiva y el tarjetahabiente.

b. **Fotografías y videograbaciones en establecimientos comerciales:** Se toman fotografías o videos en los lugares comerciales donde acepten tarjetas bancarias. El trabajador del lugar coloca previamente diminutas cámaras fotográficas en lugares estratégicos para que pueda video grabar el plástico de las tarjetas que usen las titulares de las mismas, en el momento exacto cuando se realiza la compra mediante la terminal punto de venta.

c. **Robo.** Generalmente esta es una conducta accesoria, puesto que el objetivo general del delincuente es apoderarse de otros bienes ajenos a la tarjeta.

d. **Introducción desde el extranjero.** El Carding es un fenómeno internacional, y tiene como consecuencia que grupos delictivos extranjeros, introduzcan de manera ilegítima -además de otras cosas- tarjetas bancarias falsificadas. Sin embargo, no es tan común encontrar esta conducta desde el auge del Carding

[83] Op. cit., 67.

[84] Ba.la *dictionary*, "*skimmer*", Op. cit.,

1.3.2.2. Falsificación

Esta técnica era muy popular y poco conocida a principios del año 2002, y es que solo pocas personas tenían acceso a falsificar una tarjeta bancaria. Esto es a lo que la sociedad le ha denominado *Clonación de Tarjetas*, que no es otra cosa que duplicar la tarjeta real.

Se necesitan tres factores para lograr esta conducta:

- **A.** Acceso a la tarjeta plástica, y a los datos subjetivos contenidos en ella.
- **B.** Contar con las herramientas materiales especializadas para lograr esta conducta. Son difíciles de conseguir, y solo se presume que se encuentran en el mercado negro.
- **C.** Contar con conocimientos avanzados sobre el *modus operandi* de esta conducta, por lo que entraría a la categoría doctrinal de delincuente de cuello blanco. Se piensa que muchos de los que comenten estás conductas son auxiliados por personal dentro de instituciones financieras, o comerciales., a los que se les conoce como *insiders*[85].

Andrés Mariño[86] describe que la falsificación de la tarjeta puede darse, básicamente de dos formas, *la primera de ellas es simulando completamente la tarjeta o en una segunda, adulterando la tarjeta, modificando su texto, sustituyendo el nombre, aumentando el límite de crédito, extendiendo la fecha de caducidad, etc.*

1.3.2.3. Administración

El tipo de Administración se da cuando el criminal detenta, posee, distribuye o administra las tarjetas.

En líneas anteriores se explicaron que existen grupos delictivos de Carding en el cual están organizados y poseen un sistema de organización. Para las conductas tradicionales también hay asociaciones delictivas que cuentan con un *modus*

[85] Op. cit., 27.

[86] Mariño, Andrés, “Uso fraudulento de tarjetas… “, Op. cit., p. 24.

operandi muy similar, aunque en esta conducta y tratándose de delitos tradicionales es poco común encontrarlos.

1.3.2.4. Comercialización

La comercialización es la enajenación de tarjetas bancarias, entre grupos delictivos. Aunque esta práctica ya no es tan usada, por las nuevas conductas del Carding

1.3.2.5. Uso

Consiste en el uso indebido de la tarjeta, realizado por terceros no autorizados, en perjuicio de su titular, de los establecimientos adheridos o entidades emisoras.

Andrés Mariño[87] menciona que, frente a los establecimientos adheridos, la tenencia de la tarjeta, permite a su titular efectuar operaciones de pago, y que, en ocasiones, un tercero que se la ha apropiado, la utiliza ilegítimamente en provecho propio, produciendo daños a uno o más de los integrantes del sistema.

La responsabilidad de la tarjeta es absoluta del titular de la misma, debe tener la diligencia necesaria para conservar y custodiar de la forma más adecuada el plástico y, en su caso, el *NIP*[88] de seguridad.

1.3.3. Conductas del Carding

En las conductas del Carding es obligatorio el uso de las nuevas tecnologías, como la informática y la telemática, y se distingue por los siguientes puntos:

1.- No es presencial. Es decir, que ocupa la informática, telemática o medios electrónicos para cometer las conductas delictivas del Carding a distancia. Por ejemplo, en la obtención de números de tarjetas cometidos por internet, o en el

[87] Ibídem p.24.

[88] Op. cit., 41.

uso indebido de los números de tarjetas bancarias en pago de bienes y servicios por internet.

2. Debe existir la presencia de las nuevas tecnologías como medio de comisión del delito. La informática es definida[89] como un conjunto de técnicas destinadas al tratamiento lógico y automático de la información para una mejor toma de decisiones. Por su parte, telemática[90] es la disciplina que trata la comunicación entre equipos de computación distantes. El concepto de telemática[91] refiera a la combinación de la informática y de la tecnología de la comunicación para el envió y la recepción de datos.

3. El objeto material de la acción son la información o los números contenidos en la tarjeta, por ejemplo, en cargos desconocidos por compras en internet, en donde no se ocupó el plástico, si no los números subjetivos de esta, es decir, el *PAN*[92] la fecha de vencimiento y el código de seguridad, o en la producción de números de tarjetas, BINS, donde no existe un plástico, y únicamente se basa en las cadenas de información que procesa los sistemas de seguridad como válidos.

1.4. Clasificación de ciberdelincuentes: Bineros y Carders

Se empezará desde el nivel más inferior al superior, teniendo como factores la preparación intelectual del criminal, el impacto económico, social, y las tendencias a otros miembros que se puede generar.

1. **Curioso.** Es la persona que, en redes sociales, especialmente en grupos de *Facebook* vio alguna publicación de *compras a mitad de precio* o publicaciones similares, o bien porque escuchó esporádicamente -ya sea en el colegio, con sus amigos o familia- el término BIN y decidió saber que

[89] Téllez, Julio, *Derecho Informático*, 2a ed. México, Graw Hill, 2001, p. 15.

[90] *¿Qué es telemática?*, consultable en: http://www.cavsi.com/preguntasrespuestas/que-es-telemática/ consultado el 27 de junio de 2019.

[91] Definición de telemática, consultable en: https://definicion.de/telematica/, consultado el 27 de julio de 2019.

[92] Op. cit., 14.

era, buscando en internet, llegando a grupos de *Facebook* o tutoriales de YouTube teniendo una primera noción de que es este fenómeno.

Lo único que hacen son copiar BINS, o números de tarjetas bancarias que se han utilizado previamente, con la intención de tratar de ocuparlas una vez más, sin embargo, su éxito es casi nulo.

2. **Aprendiz.** Busca ayuda para aprender a utilizar los BINS a través de un miembro de las redes sociales o por video tutoriales en plataformas como YouTube; su objetivo es aprender y su rango es la compra de servicios básicos como de entretenimiento, *streaming*[93], plataformas de música, etc. Él que no sabe generar BINS, tampoco va más allá de copiar los dieciséis dígitos, la fecha de caducidad y el código de seguridad.

3. **Binero Pasivo.** Se encuentra presente dentro del cibermercado azul, no interviene directamente, no publica ni comenta nada, sólo se encuentra a la espera de algún miembro que comparta un BIN o compra los mismos en el cibermercado con los de nivel superior. Es capaz de hacer cuentas *premium*[94] en diferentes plataformas de manera ilícita, además de que genera tarjetas bancarias falsas de un BIN; aún no sabe realizar compras, ni busca comprar BINS o tarjetas bancarias.

4. **Binero Activo:** Sabe extrapolar una tarjeta, esto es, generar sus propios BINS (véase capítulo 2 de la presente investigación), además de que ya participa en el cibermercado azul, vendiendo BINS, y cuentas de servicios que generó por los procedimientos del Carding.

---

[93] El streaming simplemente es la tecnología que nos permite ver un archivo de audio o video directamente desde internet en una página o aplicación móvil sin descargarlo completamente a nuestro dispositivo para reproducirlo. Fuente: Ávila, Fabián, *¿Qué es y para qué sirve el streaming?,* consultable en: https://eventovirtual.co/que-es-y-para-que-sirve-el-streaming/, consultado el 27 de noviembre de 2019.

[94] *Premium* es un adjetivo que se utiliza para calificar a un servicio o un producto de características especiales, de calidad superior a la media. Y se tiene que pagar un monto adicional. Fuente: Pérez Porto, Julián, et al., *Definición de Premium,* consultable en: https://definicion.de/premium/, consultable en 19 de noviembre de 2019.

5. **Aprendiz Carder:** Este puede saber o no saber sobre BINS, pero por su impacto en el cibermercado azul tiene mayor jerarquía. Ha escuchado o visto publicaciones sobre la importancia que tienen las tarjetas bancarias alteradas en la compras y pagos de servicios por un costo menor. La ventaja que tiene una tarjeta bancaria sobre un BIN es que hay más probabilidades de que sea procesada como exitosa la solicitud de compra. Una característica es que el aprendiz carder tiene cierta precaución por lo que realiza compras pequeñas que van desde un peso hasta los novecientos noventa y nueve, y la mayoría de los productos que le llegan son para su uso personal. En este nivel no paga servicios avanzados como son pago de luz, pago de agua, de electricidad, etcétera.

6. **Carder Nivel Medio:** Cuenta con experiencia dentro del campo, la compras que realiza son mayores, que van desde mil pesos hasta los cuatro mil novecientos noventa y nueve pesos. Participa en el cibermercado azul; no sólo los productos que consigue son para sí mismo, sino que también ya vende para terceros ajenos interesados; sus limitaciones son conseguir tarjetas bancarias de manera directa, y recurre a la compra de las mismas en el cibermercado.

7. **Carder Nivel Avanzado:** Es un participante activo en el cibermercado azul, distribuye y maneja grandes cantidades de información de tarjetas bancarias. Las compras indebidas de bienes y servicios que realizan alcanzan hasta los cien mil pesos. Estas personas están posicionadas en el cibermercado azul de manera estratégica. Realizan muchas compras de bienes y servicios por internet con los números de tarjetas que obtienen; además de que cuentan con “comisionistas” que son miembros de la asociación delictiva que le ayudan a buscar nuevos clientes interesados con el Carding. Cuentan con una experiencia mínima de cuatro años.

8. **Proveedor de CCS.** Es aquel que tiene forma de conseguir información o números de tarjetas bancarias, ya sea porque tiene contactos en establecimientos comerciales, ocupando las técnicas que se expusieron en el presente capítulo de la investigación, o bien porque tiene una

preparación tecnológica que permite obtener información subjetiva de manera única.

9. **Carder con "*Cash Out*".** La palabra *Cash Out*[95] hace referencia a que consigue dinero en efectivo de manera directa y rápida con ayuda de las tarjetas bancarias que consigue. Se encuentra en la más alta categoría puesto que obtiene dinero en efectivo de manera directa, y esto le permite financiar más proyectos delictivos, pudiendo ser dentro de este campo o conexos.

1.5. Cuadro normativo del Carding a nivel federal.

En las primeras líneas del capítulo presente se describieron los cinco tipos, conductas o modalidades del Carding, y se expusieron sus elementos, características, *modus operandi.* No obstante, el tipo penal para cada tipo es diferente, por lo que se analizará cada una de ellas.

En el siguiente análisis, los artículos 432, 433, 433 y 435 de la Ley General de Títulos y Operaciones de Crédito[96], y los artículos 112 bis,112 ter, 112 Quáter, y 112 Quintus de la Ley De Instituciones de Crédito[97] tienen una semejanza en los

---

[95] *Cash Out* significa literalmente retirar dinero. Fuente: Linguee, *cash out*, consultable en: https://www.linguee.es/ingles-espanol/traduccion/cash+out.html, consultado el 19 de noviembre de 2019.

[96] Los artículos 432 al 435 de la Ley General de Títulos y Operaciones de Crédito forman parte del título tercero denominado "De los delitos en materia de Títulos y Operaciones de Crédito"; en páginas siguientes del presente trabajo se analizarán cada uno de estos. Fuente: Estados Unidos Mexicanos, *Ley General de Títulos y Operaciones de Crédito*, Diario Oficial de la Federación, 27 de agosto de 1932, última reforma publicada en el Diario Oficial de la Federación el 22 de junio de 2018, consultable en: http://www.diputados.gob.mx/LeyesBiblio/pdf/145_220618.pdf, consultado el 12 de octubre de 2019.

[97] Los artículos 112 bis,112 ter, 112 Quáter, y 112 Quintus forman parte del capítulo IV de la Ley de Instituciones de Crédito, denominado "de los delitos", en páginas siguientes del presente trabajo se analizarán cada uno de estos. Fuente: Estados Unidos Mexicanos, *Ley de Instituciones de Crédito,* Diario Oficial de la Federación, 18 de julio de 1990, última reforma publicada en el Diario Oficial de la Federación el 4 de junio de 2019. Consultable en: http://www.diputados.gob.mx/LeyesBiblio/pdf/43_040619.pdf, consultado el 12 de octubre de 2018.

supuestos de hecho, pareciendo quizás ser iguales, sin embargo, existe una gran diferencia, y se analizan de manera paralela porque son las mismas conductas que se pueden emplear en el Carding.

Los artículos 432, 433, 434 y 435 de la Ley General de Títulos y Operaciones de Crédito describen el tipo penal creado específicamente para sancionar las conductas ilícitas que se cometan respecto de tarjetas de crédito o de servicios para la adquisición de bienes y servicios, expedidas en el país o en el extranjero por entidades comerciales no bancarias, es decir, aquellas tarjetas[98] que tienen origen en un contrato en el que una empresa comercial otorga a un cliente un crédito por una cantidad determinada para que pueda obtener, en los establecimientos comerciales de dicha empresa, bienes y servicios cuyo precio pagará en la forma en que se haya convenido, a este objeto se le ha nombrado para fines de esta investigación como tarjetas no bancarias, ya que no participan instituciones de crédito o bancarias en la operación puesto que sólo es una relación entre la empresa comercial y el cliente.

En los artículos 112 bis, 112 ter, 112 quáter, y 112 quintus de la ley de Instituciones de Crédito se describen a las tarjetas bancarias emitidas por instituciones de crédito, instituciones bancarias, estás pueden ser tarjetas de crédito o débito. Algunos autores en la doctrina como Andrés Mariño[99], se refieren solo a las tarjetas de crédito, pero sería incorrecto no incluir a las tarjetas de débito ya que pueden ser también objetos de conductas delictivas. En los apartados siguientes se analizará con precisión cada uno de estos

[98] Tesis I.6o.P.137 P, visible a página seiscientos quince, libro ll, tomo l del Semanario Judicial de la Federación y su Gaceta, con número de registro 160702, noviembre de 2011, novena época, bajo el rubro: COMPETENCIA PARA CONOCER DE LOS DELITOS EN LOS QUE SE UTILICE UNA TARJETA EMITIDA POR UNA ENTIDAD COMERCIAL NO BANCARIA PARA LA ADQUISICIÓN DE BIENES Y SERVICIOS. SE SURTE A FAVOR DE LOS JUECES FEDERALES EN MATERIA PENAL, consultable en: http://sjf.scjn.gob.mx/sjfsist/Documentos/Tesis/160/160702.pdf, consultado el 2 de agosto de 2019.

[99] Mariño, Andrés, “Uso fraudulento de tarjetas… “, Op. cit., p.29.

1.5.1. Consideraciones Previas al análisis

A) En Cuanto al Bien jurídico Protegido

El bien jurídico protegido es el patrimonio, pero, además, el bien jurídico de la protección es la información. Con los avances tecnológicos han permitido que las conductas delictivas evolucionen, y obligan al legislador a encuadrar los supuestos de hecho con las nuevas conductas y su *modus operandi*.

Santiago Acurio del Pino[100] expresa *que la emergente Sociedad de la Información hace totalmente necesaria la incorporación de valores inmateriales y de la información misma como bienes jurídicos de protección, esto tomando en cuenta las diferencias existentes por ejemplo entre la propiedad tangible y la intangible.*

Para los autores Claudio Magliona y Macarena López[101], los delitos informáticos tienen el carácter de pluriofensivos o complejos, *es decir que se caracterizan porque simultáneamente protegen varios intereses jurídicos, sin perjuicio de que uno de tales bienes está independientemente tutelado por otro tipo.*

En el Carding, los datos y la información son el objeto material de la acción, Alexander Díaz[102] escribe que *el bien jurídico protegido solo cambia en cuanto al ámbito de protección que lo sujeta*, y es precisa esta afirmación, ya que a diferencia de las conductas tradicionales con tarjetas donde se protege el plástico *per se*, en el Carding, solo se centra en los números, en los datos, en la información, sin ser necesario el plástico.

---

[100] Acurio del Pino, Santiago, "*Delitos Informáticos*…", Op. Cit., p.20.

[101] MAGLIONA MARKOVICTH, Claudio Paúl, LÓPEZ MEDEL Macarena, *Delincuencia y Fraude Informático,* Editorial Jurídica de Chile, 1999.

[102] Díaz, Alexander, El bien jurídico tutelado del dato y los nuevos verbos rectores de los delitos electrónicos, p. 4. consultable en: http://www.redipd.es/noticias_todas/2011/tribuna/common/1/EL_BIEN_JURIDICO_TUTELADO_DEL_DATO_Y_LOS_NUEVOS_VERBOS_RECTORES_DE_LOS_DELITOS_ELECTRONICOS_USC.pdf, consultado el 13 de enero de 2019.

La entidad emisora de las tarjetas es el propietario de las tarjetas y de los datos subjetivos de ella, ya que la institución produce la tarjeta de una manera sistemática y bajo ciertos protocolos por medio del *MII*[103], *IIN*[104]/BIN, *IAI*[105] y del *Check*[106] (véase capítulo 2 de la presente investigación). Además de que, en los contratos de apertura de crédito[107] y accesoriamente en el contrato de tarjeta de crédito, se dispone expresamente dentro de las cláusulas del mismo.

El usuario solo es titular del contrato de apertura de crédito o de depósito (tarjeta de débito) en donde se emite una tarjeta como contrato accesorio para que sea utilizada como instrumento de pago y de los datos objetivos que se guardan en el sistema de las tarjetas: Nombre, domicilio, edad, y datos de la misma índole.

B) En cuanto al Sujeto Pasivo

Es importante destacar que existe una diferencia entre víctima y ofendido, a saber, el Código Nacional de Procedimientos Penales[108] en el numeral 108 expresa que *se considera víctima del delito al sujeto pasivo que resiente directamente sobre su persona la afectación producida por la conducta delictiva. Asimismo, se considerará ofendido a la persona física o moral titular del bien*

[103] Major Industry Identified significa Identificador principal de la industria.

[104] Issuer Identified que significa Identificación del emisor.

[105] *Individual Account Identification* que significa identificación de cuenta individual.

[106] *Check* que significa comprobar, verificar.

[107] Véase contrato de apertura de crédito, BBVA BANCOMER: "Las "TARJETAS" son propiedad de "BANCOMER" y éste se reserva el derecho de sustituirlas, subsistiendo respecto de la nueva "TARJETA" que se entregue a "EL CLIENTE", todos los derechos y obligaciones derivados del presente contrato, traspasando el saldo de la "TARJETA" sustituida, al número asignado a la nueva "TARJETA". Consultable en: https://www.bbva.mx/content/dam/public-web/mexico/documents/personas/tarjetas/do-6-contrato-de-adehsion-feb.pdf, consultado el 1 de junio de 2019. Lo mismos sucede con el contrato de apertura de crédito de Santander: "... La tarjeta será propiedad de SANTANDER CONSUMO" consultable en https://www.santander.com.mx/PDF/cntrts/contrato_unico_de_tarjeta_de_credito_dic_2012.pdf, consultado el 1 de junio de 2019.

[108] Estados Unidos Mexicanos, *Código Nacional de Procedimientos Penales,* Diario Oficial de la Federación, 5 de marzo de 2014, última reforma publicada 9 de agosto de 2019, consultable en: http://www.diputados.gob.mx/LeyesBiblio/pdf/CMPP_210618.pdf, consultado el 1 de junio de 2019.

jurídico lesionado o puesto en peligro por la acción u omisión prevista en la ley penal como delito.

Dependiendo de la modalidad del Carding que se realice (generación, obtención, administración, comercialización y uso) se determinará quién es víctima, ofendido o ambas.

I. **En tarjetas de crédito:** La institución emisora de las tarjetas tiene el papel de víctima directa y de ofendido. De victima directa porque resiente la afectación producida por la conducta delictiva, ya que en primer instante la entidad emisora es quien asume el pago de una suma de dinero por el titular de la tarjeta al negocio adherido. Y ofendido por ser el titular de los bienes jurídicos protegidos, es decir, la información y el Patrimonio.

   El usuario o tarjetahabiente es víctima solo en unas técnicas de obtención, y en ofendido en cuanto al bien jurídico tutelado de patrimonio y en casos muy especiales el patrimonio.

II. **En tarjetas de débito:** La institución emisora tiene el carácter de ofendido, ya que es el titular del bien jurídico protegido de la información subjetiva, y víctima en las modalidades específicas del carding, sin embargo, el usuario puede ser víctima dependiendo de la modalidad y ofendido por el ser el titular de los datos objetivos y del patrimonio.

1.5.2. Generación o BINS

Dentro de la generación encontramos cuatro conductas que siguen un proceso lógico: producción, alteración, verificación y obtención de números de tarjetas bancarias o departamentales. Se analizará cada uno de estas para identificar si están encuadrados como un delito o son atípicos.

1.5.2.1. Producción de números de tarjetas bancarias:

No existe un tipo penal para la única producción de números de tarjetas bancarias o no bancarias.

A razón de análisis, la ley de instituciones de crédito en el artículo 112 bis de la Ley de Instituciones de crédito[109] para tarjetas bancarias y el artículo 432 de la Ley General de Títulos y Operaciones de Crédito[110] para tarjetas no bancarias o departamentales describen a las conductas de producción y fabricación de tarjetas bancarias, sin incluir la información o números contenidos en ellas, por lo que encuadraría dentro de la descripción de conductas tradicionales, pero no dentro del Carding.

Existe un debate doctrinario respecto de esta conducta, ya que se considera un subtipo de ciberfraude, sin embargo, se analizará con más detalle en investigaciones posteriores.

1.5.2.2. Alteración:

No existe un tipo penal para la alteración de números de tarjetas bancarias.

La ley de instituciones de crédito en el artículo 112 bis de la Ley de Instituciones de Crédito para tarjetas bancarias y el artículo 432 de le Ley General de Títulos y Operaciones de Crédito para tarjetas no bancarias, describen la conducta de alteración, pero únicamente de tarjetas bancarias, del plástico *per se* y no de la información o de los números contenidos en estas, por lo que sería una conducta tradicional y no del fenómeno de los BINS.

1.5.2.3. Verificación

El hecho de comprobar información no está encuadrado como un delito tradicional, ni menos en el fenómeno del Carding. Esto se debe a que cuando se describieron los supuestos de hecho el legislador no contemplo esta conducta, ya que es una técnica informática y telemática que se desarrolló con posterioridad.

---

[109] Estados Unidos Mexicanos, "*Ley de Instituciones de crédito",* Op. cit.,

[110] Estados Unidos Mexicanos, "*Ley General de Títulos y* …", Op. cit.,

1.5.2.4. Obtención

Finalmente, cuando la verificación es exitosa, en realidad se presume que se obtuvo información de una tarjeta bancaria o departamental, lo cual sería un tipo penal distinto, sería una técnica más de obtención de números de tarjetas, encuadrándose en los artículos 112 bis de la Ley de Instituciones de Crédito y en el 432 de la Ley General de Títulos y Operaciones de Crédito.

Sin embargo, bajo la exposición del capítulo 2, sobre el fenómeno de los BINS, existe una corriente de que muchas de las tarjetas que son obtenidas son válidas, sin embargo, no son reales, o más bien, que no están asociadas a ningún cliente, y que por una anomalía informática o telemática funcionan para compras de bienes de bajo valor económico, en pago de servicios o para las pruebas gratuitas que ofrecen diferentes páginas de entretenimiento, por ejemplo, en servicios de *streaming*[111], en el que ofertan días o meses de prueba con tarjetas bancarias.

No existen estudios o análisis públicos por las instituciones emisoras bancarias sobre este peculiar caso de los BINS; por lo que se concluye *a priori* que son objetos ficticios, por lo que no cumple con los elementos del tipo.

Enrique Nava[112], *et.al.* encuadran a este subtipo como un tipo de delito informático, denominado *Manipulación de los datos de salida*, expresando que es un fraude efectuado por manipulación informática que aprovecha las repeticiones automáticas de los procesos de computo.

[111] Op. cit., 93.

[112] Nava Garcés, Alberto Enrique, *Análisis de los Delitos Informáticos*, México, Porrúa, 2005. P.30

1.5.3. Obtención

1.5.3.1. Ley de Instituciones de Crédito. - Tarjetas bancarias.

La conducta de obtención de información o números de tarjetas bancarias está tipificada por el capítulo lV de la Ley de Instituciones de Crédito[113], denominado *De los Delitos.*

> *Artículo 112 Bis. - Se sancionará con prisión de tres a nueve años y de treinta mil a trescientos mil días multa, al que sin causa legítima o sin consentimiento de quien esté facultado para ello, respecto de tarjetas de crédito, de débito, cheques, formatos o esqueletos de cheques o en general cualquier otro instrumento de pago, de los utilizados o emitidos por instituciones de crédito del país o del extranjero:*
>
> *(…)*
>
> *III. Obtenga, comercialice o use la información sobre clientes, cuentas u operaciones de las instituciones de crédito emisoras de cualquiera de los objetos a que se refiere el párrafo primero de este artículo;*
>
> *V. Sustraiga, copie o reproduzca información contenida en alguno de los objetos a que se refiere el párrafo primero de este artículo, o*
>
> *(…)*

Sujetos y objetos

Activo: Puede ser cualquier persona, sin embargo, el artículo 112 Quintus de la propia ley, estipula que la pena podrá aumentarse si tienen el carácter de consejero, funcionario, empleado o prestador de servicios de cualquier institución de crédito, o las realice dentro de los dos años siguientes de haberse separado de alguno de dichos cargos, o sea propietario o empleado de cualquier entidad mercantil

[113] Estados Unidos Mexicanos, "*Ley de Instituciones de crédito",* Op. cit.,

Pasivo: Depende del tipo de técnica que se haya utilizado para obtener información de los números de las tarjetas bancarias, ya que puede ser el titular de la tarjeta bancaria, la institución que emitió la tarjeta bancaria, o el negocio mercantil adherido, en todos los casos siguientes el ofendido es la Institución de crédito en cuanto a la información y el titular de la tarjeta en cuanto al patrimonio.

- *SQL injector-dumper*[114]. Víctima: negocios mercantiles adheridos que tengan página en internet.
- Fuga de datos de datos o *data leakage*[115]. Víctima: Institución de Crédito
- Ingeniería social. Víctima: Tarjetahabiente.
- Fuerza Bruta. Víctima: Páginas *web*[116] de negocios mercantiles
- *Spam- Phishing*[117]. Víctima: Tarjetahabiente
- *Pharming*[118] Víctima: Tarjetahabiente
- *Keyloggers.*[119] Víctima: Tarjetahabiente
- Robo de credenciales: Tarjetahabiente
- *Sniffing*[120]: Tarjetahabiente, instituciones de crédito.
- *Skimmer*[121] remoto: Tarjetahabiente
- Sabanas de información: Instituciones de crédito

Objetos

Bien jurídico protegido: Es un delito pluriofensivo, afecta a la información y al patrimonio.

[114] Op. cit., 13.

[115] Op. cit., 25.

[116] Op. cit., 16.

[117] Op. cit., 36.

[118] Op. cit., 48.

[119] Op. cit., 57.

[120] Op. cit., 65.

[121] Op. cit., 67.

Material. Por si mismos la información está contenida en datos electrónicos, sin embargo, estos no están en un mundo físico, más bien en un ciberespacio.

Conducta típica

Pueden presentarse las siguientes maneras de realizarlo:

A. Al que sin causa legítima o sin consentimiento de quien esté facultado para ello.
B. Cuatro verbos rectores: obtenga, sustraiga, copie o reproduzca.

Formas y medios de ejecución

El tipo no exige ningún medio comisivo, lo que se desprende de la expresión legal *por cualquier medio*. A esto solo en la conducta del Carding se podría añadir que el medio comisivo sea a través de medios informáticos o telemáticos.

Consumación y tentativa

Consumación

Ocurre cuando se obtiene la información de las tarjetas o números de tarjetas bancarias.

Tentativa

Si es posible su configuración.

Culpabilidad

Dolosa en la mayoría de situaciones, sin embargo, se puede presentar el error esencial de hecho invencible, por ejemplo, al auditar el sistema de seguridad de alguna institución por cuestiones de protocolos de seguridad, arrojando datos vulnerables entre ellos información confidencial de números de tarjetas bancarias.

Punibilidad

La ley de Instituciones de crédito[122] señala que se sancionará con prisión de tres a nueve años y multa de treinta mil a trescientos mil días de multa.

Sin embargo, las penas se reducirán a un tercio cuando se acredite haber reparado el daño o haber resarcido el perjuicio ocasionado.

1.5.3.2. Ley General de Títulos y Operaciones de Crédito. - Tarjetas no Bancarias.

El delito de obtención de información o números de tarjetas no bancarias, está tipificado como delito especial, artículo 432 de Ley General de Títulos y Operaciones de crédito[123]:

> *Artículo 432.- Se sancionará con prisión de tres a nueve años y multa de treinta mil a trescientos mil días multa, al que sin causa legítima o sin consentimiento de quien esté facultado para ello, respecto de tarjetas de servicio, de crédito o en general, instrumentos utilizados en el sistema de pagos, para la adquisición de bienes y servicios, emitidos en el país o en el extranjero, por entidades comerciales no bancarias:*
>
> *(…)*
>
> *lll. Obtenga, comercialice o use la información sobre clientes, cuentas u operaciones de las entidades emisoras de cualquiera de los objetos a que se refiere el párrafo primero de este artículo;*
>
> *(…)*
>
> *V. Sustraiga, copie o reproduzca información contenida en alguno de los objetos a que se refiere el párrafo primero de este artículo, o*
>
> *(…)*

[122] Estados Unidos Mexicanos, "*Ley de Instituciones de crédito*", Op. cit.,

[123] Estados Unidos Mexicanos, "*Ley General de Títulos y* …", Op. cit.,

Sujetos y objetos

Activo: Puede ser cualquier persona, sin embargo, en el artículo 435 de la propia ley, estipula que la pena podrá aumentarse en caso de que el activo tenga el carácter de consejero, funcionario, empleado o prestador de servicios de cualquier entidad emisora, o que sea propietario o empleado de cualquier entidad mercantil.

Pasivo: Depende del tipo de técnica que se haya utilizado para obtener información de los números de las tarjetas no bancarias, seguirán los mismos tipos del sujeto pasivo de la conducta de obtención de tarjetas bancarias.

Objetos

Material. Por si mismos la información está contenida en datos electrónicos, sin embargo, estos no están en un mundo físico, más bien en un ciberespacio.

Jurídico. La información y el patrimonio

Conducta típica

Pueden presentarse las siguientes maneras de realizarlo:

A. Al que sin causa legítima o sin consentimiento de quien esté facultado para ello.
B. Obtenga, sustraiga, copie o reproduzca. El verbo rector del tipo penal es “obtenga” ya que las otras conductas de sustraiga, copie o reproduzca son verbos que refieren a la obtención de información o números de tarjetas bancarias.

Formas y medios de ejecución

El tipo no exige ningún medio comisivo, lo que se desprende de la expresión legal *por cualquier medio*. A esto solo en la conducta del Carding se podría añadir que el medio comisivo sea a través de medios informáticos o telemáticos.

Consumación y tentativa

Consumación

Ocurre cuando se obtiene la información de las tarjetas o números de tarjetas bancarias.

Tentativa

Si es posible su configuración.

Culpabilidad

Dolosa en la mayoría de situaciones, sin embargo, se puede presentar el error esencial de hecho invencible, por ejemplo, al auditar el sistema de seguridad de alguna institución por cuestiones de protocolos de seguridad, arrojando datos vulnerables entre ellos información confidencial de números de tarjetas bancarias.

Punibilidad

La Ley General de Títulos y Operaciones de Crédito[124] señala que se sancionará con prisión de tres a nueve años y multa de treinta mil a trescientos mil días de multa.

1.5.3.3. Código Penal Federal

La mayoría de las técnicas para la obtención de información o números de tarjetas bancarias están tipificadas en capítulo ll denominado *Acceso ilícito a sistemas y equipos de informática* del Código Penal Federal. Las técnicas que encuadra son: *SQL injector-dumper*[125], fuga de datos o *data leakage*[126].

[124] Estados Unidos Mexicanos, “Ley General de Títulos y …”, Op. cit.,

[125] Op. cit., 13.

[126] Op. cit., 25.

ingeniería social, fuerza bruta, *spam*[127] – *phishing*[128], *pharming*[129], *keyloggers*[130], robo de credenciales, *sniffing*[131].

> *Artículo 211 bis 1*[132]*. (..)*
>
> *Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.*

Sujetos y objetos

Activo: Puede ser cualquier persona, no obstante, el artículo 211 bis 3, señala que al activo tiene que ser aquel que esté autorizado para para acceder a sistemas y equipos de informática del estado, asimismo el artículo 211 bis señala que el que esté autorizado para acceder a sistemas y equipos de informática y copie la información que contenga.

Pasivo: Se dividen en dos tipos, el que recibe directamente la conducta delictiva y el indirecto, este último es el titular de la tarjeta bancaria.

El directo son los sistemas o equipos de informática protegidos por algún mecanismo de seguridad, y el indirecto, los titulares de las tarjetas bancarias.

Objetos

---

[127] Op. cit. 36

[128] Ídem.

[129] Op. cit., 48.

[130] Op. cit., 57.

[131] Op. cit., 65.

[132] Estados Unidos Mexicanos, *Código Penal Federal, Diario Oficial de la Federación*, 14 de agosto de 1931, última reforma publicada en el Diario Oficial de la Federación el 14 de agosto de 2019, consultable en: http://www.diputados.gob.mx/LeyesBiblio/pdf/9_081119.pdf, consultado el 2 de junio de 2019.

Material. Por si mismos la información está contenida en datos electrónicos, sin embargo, estos no están en un mundo físico, más bien en un ciberespacio.

Jurídico. La información y el patrimonio

Conducta típica

Pueden presentarse las siguientes maneras de realizarlo:

- **A.** Al que sin autorización
- **B.** Conozca o copie
- **C.** Información contenida en sistemas o equipos de informática
- **D.** Protegidos por algún mecanismo de seguridad.

Formas y medios de ejecución

El tipo no exige ningún medio comisivo. A esto solo en la conducta del Carding se podría añadir que el medio comisivo sea a través de medios informáticos o telemáticos.

Consumación y tentativa

Consumación

Ocurre cuando se obtiene la información de las tarjetas o números de tarjetas bancarias.

Tentativa

Si es posible su configuración.

Culpabilidad

Dolosa.

Punibilidad

Las penas están señaladas por el Código Penal Federal[133]:

Artículo 211 bis de tres meses a un año de presión y de cincuenta a ciento cincuenta días multa.

Artículo 211 bis 2 se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá, además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.

211 bis 3. se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa

211 bis 4. se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

211 bis 5. se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa. Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

Artículo 211 bis 7.- Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.

[133] Estados Unidos Mexicanos, "*Código Penal Federal*" Op. cit.,

1.5.4. Administración

Sin tipo penal

1.5.5. Comercialización

1.5.5.1. Ley de Instituciones de Crédito. Tarjetas Bancarias

La conducta de comercialización de información o números de tarjetas bancarias está tipificada por el capítulo lV de la Ley de Instituciones de Crédito, denominado *De los Delitos.*

> *Artículo 112 Bis[134].- Se sancionará con prisión de tres a nueve años y de treinta mil a trescientos mil días multa, al que sin causa legítima o sin consentimiento de quien esté facultado para ello, respecto de tarjetas de crédito, de débito, cheques, formatos o esqueletos de cheques o en general cualquier otro instrumento de pago, de los utilizados o emitidos por instituciones de crédito del país o del extranjero:*
>
> *(…)*
>
> *III. Obtenga, comercialice o use la información sobre clientes, cuentas u operaciones de las instituciones de crédito emisoras de cualquiera de los objetos a que se refiere el párrafo primero de este artículo;*
>
> *(…)*

Sujetos y objetos

Activo: Puede ser cualquier persona, sin embargo, el artículo 112 Quintus de la propia ley, estipula que la pena podrá aumentarse hasta en una mitad más si quien realice cualquiera de las conductas señaladas en los artículos 112 Bis, 112 Ter y 112 Quáter tiene el carácter de consejero, funcionario, empleado o prestador de servicios de cualquier institución de

[134] Estados Unidos Mexicanos, "*Ley de Instituciones de crédito*", Op. cit.,

crédito, o las realice dentro de los dos años siguientes de haberse separado de alguno de dichos cargos, o sea propietario o empleado de cualquier entidad mercantil

Pasivo: El titular de la tarjeta bancaria y la institución que emitió la tarjeta bancaria.

Objetos

Material. Por si mismos la información está contenida en datos electrónicos, sin embargo, estos no están en un mundo físico, más bien en un ciberespacio.

Jurídico. La información y el patrimonio

Conducta típica

Pueden presentarse las siguientes maneras de realizarlo:

A. Al que sin causa legítima o sin consentimiento de quien esté facultado para ello.
B. Comercialice la información sobre clientes, cuentas u operaciones de las instituciones de crédito

Formas y medios de ejecución

El tipo no exige ningún medio comisivo. A esto solo en la conducta del Carding se podría añadir que el medio comisivo sea a través de medios informáticos o telemáticos.

Consumación y tentativa

Consumación

Ocurre cuando se enajena la información de las tarjetas o números de tarjetas bancarias.

Tentativa

Si es posible su configuración.

Culpabilidad

Dolosa

Punibilidad

La referida ley[135] expresa que se sancionará con prisión de tres a nueve años y multa de treinta mil a trescientos mil días de multa.

Sin embargo, las penas se reducirán a un tercio cuando se acredite haber reparado el daño o haber resarcido el perjuicio ocasionado. Artículo114 bis.

1.5.5.2. Ley General de Títulos y Operaciones de Crédito. - Tarjetas No Bancarias

La conducta de comercialización de información o números de tarjetas no bancarias, está tipificado como delito especial, artículo 432 de Ley General de Títulos y Operaciones de crédito:

> *Artículo 432[136].- Se sancionará con prisión de tres a nueve años y multa de treinta mil a trescientos mil días multa, al que sin causa legítima o sin consentimiento de quien esté facultado para ello, respecto de tarjetas de servicio, de crédito o en general, instrumentos utilizados en el sistema de pagos, para la adquisición de bienes y servicios, emitidos en el país o en el extranjero, por entidades comerciales no bancarias:*
>
> *(…)*
>
> *lll. Obtenga, comercialice o use la información sobre clientes, cuentas u operaciones de las entidades emisoras de cualquiera de los objetos a que se refiere el párrafo primero de este artículo;*
>
> *(…)*

[135] Estados Unidos Mexicanos, "*Ley de Instituciones de crédito*", Op. cit.,

[136] Estados Unidos Mexicanos, "*Ley General de Títulos y* …", Op. cit.

Sujetos y objetos

Activo: Puede ser cualquier persona, sin embargo, en el artículo 435 de la propia ley, estipula que la pena podrá aumentarse en caso de que el activo tenga el carácter de consejero, funcionario, empleado o prestador de servicios de cualquier entidad emisora, o que sea propietario o empleado de cualquier entidad mercantil.

Pasivo: La entidad comercial emisora de tarjetas y el cliente.

Objetos

Material. Por si mismos la información está contenida en datos electrónicos, sin embargo, estos no están en un mundo físico, más bien en un ciberespacio.

Jurídico. La información y el patrimonio

Conducta típica

Pueden presentarse las siguientes maneras de realizarlo:

A. Al que sin causa legítima o sin consentimiento de quien esté facultado para ello.
B. Comercialice la información sobre clientes, cuentas u operaciones de las entidades emisoras respecto de tarjetas de servicio, de crédito o en general, instrumentos utilizados en el sistema de pagos, para la adquisición de bienes y servicios

Formas y medios de ejecución

El tipo no exige ningún medio comisivo. A esto solo en la conducta del Carding se podría añadir que el medio comisivo sea a través de medios informáticos o telemáticos.

Consumación y tentativa

Consumación.

Ocurre cuando se enajena la información de las tarjetas o números de tarjetas bancarias.

Tentativa.

Si es posible su configuración.

Culpabilidad

Dolosa

Punibilidad

Se sancionará con prisión de tres a nueve años y multa de treinta mil a trescientos mil días de multa.

1.5.6. Uso

1.5.6.1. Ley de Instituciones de Crédito. Tarjetas Bancarias

La conducta de uso de información o números de tarjetas bancarias está tipificada por el capítulo lV de la Ley de Instituciones de Crédito, denominado *De los Delitos.*

> *Artículo 112 Bis[137]. - Se sancionará con prisión de tres a nueve años y de treinta mil a trescientos mil días multa, al que sin causa legítima o sin consentimiento de quien esté facultado para ello, respecto de tarjetas de crédito, de débito, cheques, formatos o esqueletos de cheques o en general cualquier otro instrumento de pago, de los utilizados o emitidos por instituciones de crédito del país o del extranjero:*
>
> *(…)*

[137] Estados Unidos Mexicanos, "*Ley de Instituciones de crédito*", Op. cit.,

III. Obtenga, comercialice o use la información sobre clientes, cuentas u operaciones de las instituciones de crédito emisoras de cualquiera de los objetos a que se refiere el párrafo primero de este artículo;

(…)

Sujetos y objetos

Activo: Puede ser cualquier persona, sin embargo, el artículo 112 Quintus de la propia ley, estipula que la pena podrá aumentarse hasta en una mitad más si quien realice cualquiera de las conductas señaladas en los artículos 112 Bis, 112 Ter y 112 Quáter tiene el carácter de consejero, funcionario, empleado o prestador de servicios de cualquier institución de crédito, o las realice dentro de los dos años siguientes de haberse separado de alguno de dichos cargos, o sea propietario o empleado de cualquier entidad mercantil que a cambio de bienes o servicios reciba como contraprestación el pago a través de cualquiera de los instrumentos mencionados en el artículo 112 Bis

Pasivo: El titular de la tarjeta bancaria o la institución que emitió la tarjeta bancaria, dependiendo de cuál haya sido la técnica para la obtención de la información o de los números de la tarjeta bancaria.

Objetos

Material. Por si mismos la información está contenida en datos electrónicos, sin embargo, estos no están en un mundo físico, más bien en un ciberespacio.

Jurídico. La información y el patrimonio.

Conducta típica

Pueden presentarse las siguientes maneras de realizarlo:

A. Al que sin causa legítima o sin consentimiento de quien esté facultado para ello.

B. Use la información sobre clientes, cuentas u operaciones de las instituciones de crédito.

Formas y medios de ejecución.

El tipo no exige ningún medio comisivo. A esto solo en la conducta del Carding se podría añadir que el medio comisivo sea a través de medios informáticos o telemáticos.

Consumación y tentativa

Consumación

Ocurre cuando se usa la información de las tarjetas o números de tarjetas bancarias.

Tentativa

Si es posible su configuración.

Culpabilidad

Dolosa

Punibilidad

Se sancionará con prisión de tres a nueve años y multa de treinta mil a trescientos mil días de multa.

1.5.6.2. Ley General de Títulos y Operaciones de Crédito. Tarjetas No Bancarias

La conducta de uso de información o números de tarjetas no bancarias, está tipificado como delito especial, artículo 432 de Ley General de Títulos y Operaciones de crédito:

Artículo 432[138].- Se sancionará con prisión de tres a nueve años y multa de treinta mil a trescientos mil días multa, al que sin causa legítima o sin consentimiento de quien esté facultado para ello, respecto de tarjetas de servicio, de crédito o en general, instrumentos utilizados en el sistema de pagos, para la adquisición de bienes y servicios, emitidos en el país o en el extranjero, por entidades comerciales no bancarias:

(…)

lll. Obtenga, comercialice o use la información sobre clientes, cuentas u operaciones de las entidades emisoras de cualquiera de los objetos a que se refiere el párrafo primero de este artículo;

(…)

Sujetos y objetos

Activo: Puede ser cualquier persona, sin embargo, en el artículo 435 de la propia ley, estipula que la pena podrá aumentarse en caso de que el activo tenga el carácter de consejero, funcionario, empleado o prestador de servicios de cualquier entidad emisora, o que sea propietario o empleado de cualquier entidad mercantil.

Pasivo: El titular de la tarjeta bancaria y la Institución que la emitió

Objetos

Material. Por si mismos la información está contenida en datos electrónicos, sin embargo, estos no están en un mundo físico, más bien en un ciberespacio.

Jurídico. La información y el patrimonio

Conducta típica

[138] Estados Unidos Mexicanos, "*Ley General de Títulos y* …", Op. cit.,

Pueden presentarse las siguientes maneras de realizarlo:

A. Al que sin causa legítima o sin consentimiento de quien esté facultado para ello.

B. Use la información sobre clientes, cuentas u operaciones de las entidades emisoras respecto de tarjetas de servicio, de crédito o en general, instrumentos utilizados en el sistema de pagos, para la adquisición de bienes y servicios.

Formas y medios de ejecución

El tipo no exige ningún medio comisivo. A esto solo en la conducta del Carding se podría añadir que el medio comisivo sea a través de medios informáticos o telemáticos.

Consumación y tentativa

Consumación

Ocurre cuando se usa la información de las tarjetas o números de tarjetas bancarias.

Tentativa

Si es posible su configuración.

Culpabilidad

Dolosa

Punibilidad

Se sancionará con prisión de tres a nueve años y multa de treinta mil a trescientos mil días de multa.

1.5.6.3. Código Penal Federal, Delito de Fraude

Además, la conducta de uso de información o números de tarjetas bancarias está tipificada como fraude en el código penal federal*: Artículo 386*[139]*.- Comete el delito de fraude el que engañando a uno o aprovechándose del error en que éste se halla se hace ilícitamente de alguna cosa o alcanza un lucro indebido. (…)*

Sujetos y objetos

Activo: Puede ser cualquier persona.

Pasivo: El negocio adherido, la institución bancaria y el titular de la tarjeta.

Objetos

Material. Por si mismos la información está contenida en datos electrónicos, sin embargo, estos no están en un mundo físico, más bien en un ciberespacio.

Jurídico. La información y el patrimonio

Conducta típica

Pueden presentarse las siguientes maneras de realizarlo:

A. Engañando a uno o
B. Aprovechándose del error en que éste se halla
C. Se hace ilícitamente de alguno cosa o
D. Alcanza un lucro indebido

Formas y medios de ejecución

[139] Estados Unidos Mexicanos, "*Código Penal Federal*" Op. cit.,

El tipo no exige ningún medio comisivo. A esto solo en la conducta del Carding se podría añadir que el medio comisivo sea a través de medios informáticos o telemáticos.

Consumación y tentativa

Consumación

Ocurre cuando se usa la información de manera fraudulenta las tarjetas o números de tarjetas bancarias.

Tentativa

Si es posible su configuración.

Culpabilidad

Dolosa

Punibilidad

El Código Penal Federal señala las penas siguientes[140]:

I.- Con prisión de 3 días a 6 meses o de 30 a 180 días multa, cuando el valor de lo defraudado no exceda de diez veces el salario;

II.- Con prisión de 6 meses a 3 años y multa de 10 a 100 veces el salario, cuando el valor de lo defraudado excediera de 10, pero no de 500 veces el salario;

III.- Con prisión de tres a doce años y multa hasta de ciento veinte veces el salario, si el valor de lo defraudado fuere mayor de quinientas veces el salario.

[140] Estados Unidos Mexicanos, "*Código Penal Federal*" Op. cit.,

1.6. Cuadro normativo a nivel local: Estado de Puebla

En el Código Penal del Estado de Puebla solo describe algunas de las conductas del Carding.

1.6.1. Producción

Sin tipo penal.

1.6.2. Obtención

La conducta de obtención de información bancaria en algunas de sus técnicas como ingeniería social o *spam-phishing*[141] podrían encuadrarse dentro del delito de fraude y está tipificado en el artículo 402 del Código Penal para el Estado de Puebla*: Artículo 402*[142]*.- Comete el delito de fraude el que engañando a uno o aprovechándose del error en que éste se halla se hace ilícitamente de alguna cosa o alcanza un lucro indebido*. *(…)*

Sujetos y objetos

Activo: Puede ser cualquier persona.

Pasivo: El negocio adherido, la institución bancaria o el tarjetahabiente, dependiendo de la técnica usada.

Objetos

Material. Por si mismos la información está contenida en datos electrónicos, sin embargo, estos no están en un mundo físico, más bien en un mundo virtual.

Jurídico. La información y el patrimonio

Conducta típica

[141] Op. cit., 36.

[142] Estados Unidos Mexicanos, *Código Penal del Estado Libre y Soberano de Puebla*, Periódico Oficial del Estado, 23 de diciembre de 1986, última reforma 04 de abril de 2019.

Pueden presentarse las siguientes maneras de realizarlo:

A. Engañando a uno o
B. Aprovechándose del error en que éste se halla
C. Se hace ilícitamente de alguno cosa o
D. Alcanza un lucro indebido.

Formas y medios de ejecución

El tipo no exige ningún medio comisivo. A esto solo en la conducta del Carding se podría añadir que el medio comisivo sea a través de medios informáticos o telemáticos.

Consumación y tentativa

Consumación

Ocurre cuando se usa la información de manera fraudulenta las tarjetas o números de tarjetas bancarios.

Tentativa

Es posible su configuración.

Culpabilidad

Dolosa

Punibilidad

El Código Penal de Puebla señala las siguientes penas en el relativo 403[143]:

> *I.- Con multa de cinco a cincuenta días de salario y prisión de seis meses a tres años, si no se puede determinar el valor de lo defraudado o este valor no es superior a cien días de salario.*

[143] Ídem.

II.- Con multa de cincuenta a doscientos cincuenta días de salario y prisión de tres a cinco años, si el valor de lo defraudado excediere de cien días de salario, pero no de quinientos;

III.- Con multa de doscientos cincuenta a quinientos días de salario y prisión de cinco a siete años, cuando el valor de lo defraudado excediere de quinientos días de salario, pero no de mil, y

IV.- Con multa de quinientos a mil días de salario y prisión de siete a diez años, cuando el valor de lo defraudado excediere de mil días de salario.

1.6.2.1. Carding como delito Informático

Producción

La conducta de obtención de información o de números de tarjetas bancarias se encuadra como un delito informático y está tipificado en el Código Penal para el Estado de Puebla[144]*:*

Artículo 476 (…) Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa. Sujetos y objetos

Artículo 478 (…)

Al que, estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a dos años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

Sujetos y Objetos

[144] Ídem.

Activo: Puede ser cualquier persona, pero el artículo 478 del Código Penal establece como agravante al que esté autorizado para acceder a sistemas y equipos de informática del Estado o de seguridad pública.

Pasivo: El negocio adherido y la institución bancaria. Sin embargo, el artículo 478 menciona que tienen que ser los sistemas y equipos de informática del Estado de Puebla.

Objetos

Material. Por si mismos la información está contenida en datos electrónicos, sin embargo, estos no están en un mundo físico, más bien en un mundo virtual.

Jurídico. La información y el patrimonio

Conducta típica

Pueden presentarse las siguientes maneras de realizarlo:

A. Al que sin autorización
B. Conozca o copie
C. Información contenida en sistemas o equipos de informática
D. Protegidos por algún mecanismo de seguridad

Formas y medios de ejecución

El tipo no exige ningún medio comisivo. A esto solo en la conducta del Carding se podría añadir que el medio comisivo sea a través de medios informáticos o telemáticos.

Consumación y tentativa

Consumación

Ocurre cuando se obtiene la información o números de la tarjeta bancaria, es decir, cuando se conoce o se copia la información contenida en las tarjetas bancarias.

Tentativa

Si es posible su configuración.

Culpabilidad

Dolosa, sin embargo, se puede presentar el error esencial de hecho invencible, por ejemplo, al auditar el sistema de seguridad de alguna institución por cuestiones de protocolos de seguridad, arrojando datos vulnerables entre ellos información confidencial de números de tarjetas bancarias.

Punibilidad

El Código Penal de Puebla[145], señala las penas siguientes:

I. Artículo 476 fracción segunda, se impondrá de tres meses a un año de prisión y de cincuenta a ciento cincuenta días de multa.

II. Artículo 478 fracción segunda, se impondrá de uno a dos años de prisión y de ciento cincuenta a cuatrocientos días de multa.

1.6.3. Administración

Sin tipo

1.6.4. Comercialización

Sin tipo penal

1.6.5. Uso

La conducta de uso de información o números de tarjetas bancarias podría encuadrarse como fraude, y está tipificado en el artículo 402 del Código Penal para el Estado de Puebla*: artículo 402[146].- Comete el delito de fraude el que engañando a uno o aprovechándose del error en que éste se halla se hace ilícitamente de alguna cosa o alcanza un lucro indebido. (…)*

[145] Ídem.

[146] Ídem.

Sujetos y objetos

Activo: Puede ser cualquier persona.

Pasivo: El negocio adherido y la institución bancaria.

Objetos

Material. Por si mismos la información está contenida en datos electrónicos, sin embargo, estos no están en un mundo físico, más bien en un ciberespacio.

Jurídico. La información y el patrimonio

Conducta típica

Pueden presentarse las siguientes maneras de realizarlo:

A. Engañando a uno o
B. Aprovechándose del error en que éste se halla
C. Se hace ilícitamente de alguno cosa o
D. Alcanza un lucro indebido

Formas y medios de ejecución

El tipo no exige ningún medio comisivo. A esto solo en la conducta del Carding se podría añadir que el medio comisivo sea a través de medios informáticos o telemáticos.

Consumación y tentativa

Consumación

Ocurre cuando se usa la información de manera fraudulenta las tarjetas o números de tarjetas bancarios.

Tentativa

Si es posible su configuración.

Culpabilidad

Dolosa

Punibilidad

El Código Penal de Puebla, establece en el artículo 403[147] las penas siguientes:

I.- Con multa de cinco a cincuenta días de salario y prisión de seis meses a tres años, si no se puede determinar el valor de lo defraudado o este valor no es superior a cien días de salario.

II.- Con multa de cincuenta a doscientos cincuenta días de salario y prisión de tres a cinco años, si el valor de lo defraudado excediere de cien días de salario, pero no de quinientos;

III.- Con multa de doscientos cincuenta a quinientos días de salario y prisión de cinco a siete años, cuando el valor de lo defraudado excediere de quinientos días de salario, pero no de mil, y

IV.- Con multa de quinientos a mil días de salario y prisión de siete a diez años, cuando el valor de lo defraudado excediere de mil días de salario.

1.6.6. Análisis de competencia

En el Estado de Puebla no son competentes para conocer de los delitos que conforman el Carding, ni tampoco de las conductas tradicionales, así lo establece la tesis XV.4o.5 P, visible a página mil quinientos diecinueve, tomo XXII del Semanario Judicial de la Federación y su Gaceta, con número de registro 177826, julio de 2005, novena época, bajo el rubro: **Reproducción de tarjetas de crédito o débito. Al estar dicha conducta prevista como delito en la ley de Instituciones de Crédito, el proceso que se instruya al**

[147] Ídem.

inculpado debe seguirse ante un juez del fuero federal[148]**,** en la que se argumenta que si los hechos que dieron inicio a la averiguación previa de los de delitos de reproducción de tarjetas de crédito o débito, resulta ilegal que se instruya proceso por los ilícitos de fraude genérico o falsificación de documento ante un juez del fuero común, aunque estas conductas estén reguladas en la legislación del fuero común, pues este ordenamiento legal tiene la finalidad de regular el servicio de banca y crédito, la organización y funcionamiento de las instituciones crediticias, así como sus actividades y operaciones.

Por tanto, conforme con el diverso 50, fracción I, inciso a), de la Ley Orgánica del Poder Judicial de la Federación que dice:

> *Artículo 50. Los jueces Federales penales conocerán:*
>
> *Son delitos del orden federal*
>
> *a) Los previstos en las leyes federales y en los tratados internacionales. En el caso del Código Penal Federal, tendrán ese carácter los delitos a que se refieren los incisos b) a l) de esta fracción*;

Por lo que corresponde conocer de tales hechos del Carding a un Juez Federal.

A razón de un análisis sistemático, existe un principio de especialidad contenido en la que la Tesis IV.1o.52 P, visible a página tres mil setecientos cuarenta y cinco, libro lll, tomo cinco del Semanario Judicial de la Federación y su Gaceta, con número de registro 160603, diciembre de 2011, novena época[149], bajo el

---

[148] Tesis XV.4o.5 P, visible a página mil quinientos diecinueve, tomo XXII del Semanario Judicial de la Federación y su Gaceta, bajo el rubro: REPRODUCCIÓN DE TARJETAS DE CRÉDITO O DÉBITO. AL ESTAR DICHA CONDUCTA PREVISTA COMO DELITO EN LA LEY DE INSTITUCIONES DE CRÉDITO, EL PROCESO QUE SE INSTRUYA AL INCULPADO DEBE SEGUIRSE ANTE UN JUEZ DEL FUERO FEDERAL, consultable en: http://sjf.scjn.gob.mx/sjfsist/Documentos/Tesis/177/177826.pdf, consultado el 21 de octubre de 2019.

[149] Tesis IV.1o.52 P, visible a página tres mil setecientos cuarenta y cinco, libro lll, tomo cinco del Semanario Judicial de la Federación y su Gaceta, con número de registro 160603, diciembre de

rubro: **Concurso aparente de normas. el auto de formal prisión dictado por el juzgador del fuero común por el delito de robo equiparado previsto en el artículo 365, fracción vi, del Código Penal para el Estado de Nuevo León, cuando el acto atribuido al inculpado consista en el uso de una tarjeta departamental no bancaria para obtener en su beneficio una cosa que estaba a la venta, es violatorio de garantías, al resultar aplicable, en atención al principio de especialidad, el tipo penal específico previsto en el numeral 432, fracción ii, de la ley general de títulos y operaciones de crédito.**

> *En esta tesis, existe un razonamiento en la que se advierte la actualización del fenómeno jurídico del concurso o conflicto aparente de normas penales , al comparar el artículo 365 del Código Penal de Nuevo León, con el numeral 432 de la Ley General de Títulos y Operaciones de Crédito, y en ambas se regula la misma conducta censurable; por tanto, debe resolverse bajo el principio de especialidad, conforme al cual la norma especial desplaza la aplicación de la general, tomando en cuenta que el caso concreto, la última de las normas mencionadas contempla un tipo penal formado con mayores elementos y alternativas, al establecer que se sancionará a aquella persona que, sin causa legítima o sin consentimiento de quien esté facultado para ello, utilice tarjetas de servicio, de crédito o, en general, instrumentos utilizados en sistema de pagos, para la adquisición de bienes y servicios emitidos en el país o en el extranjero por entidades comerciales no bancarias.*

Por las razones expuestas deviene violatorio de garantías el auto de formal prisión que dicte el Juez del fuero común por el delito de equiparable al robo, si se atribuye al inculpado el uso de una tarjeta departamental no bancaria para obtener en su beneficio personal una

---

2011, novena época, consultable en: http://sjf.scjn.gob.mx/SJFSist/Documentos/Tesis/160/160603.pdf, consultado el 12 de octubre de 2019.

cosa que estaba a la venta, pues ante la existencia de un conflicto aparente de leyes, debió recurrirse a la regla de especialidad de la norma y, por tratarse de una ley del orden federal la que debía aplicarse, declinar la competencia por razón del fuero[150].

Por lo expuesto anteriormente, y bajo la hipótesis que, al ser un delito descrito en una ley Federal, y bajo el principio de especialidad, es por lo que es competente un Juez Federal y no el juez del fuero común del Estado de Puebla.

1.7. Diferencias entre tipo penales

1.7.1. Porque la conducta de obtención del Carding no encuadra como robo y sí un delito especial.

El delito de robo está regulado por el Código Penal Federal, en el Título Vigesimosegundo "Delitos en contra de las personas en su patrimonio", capítulo l "robo", del artículo 367 al 381 bis[151], definiéndolo como: *Comete el delito de robo: el que se apodera de una cosa mueble, sin derecho y sin consentimiento de la persona que puede disponer de ella con arreglo de ley*.

Asimismo, el artículo 368 estipula conductas equiparables al robo en las que se encuentra en primer lugar el apoderamiento o destrucción dolosa de una cosa propia mueble, si ésta se halla por cualquier título legítimo en poder de otra persona y no medio consentimiento, y en segundo lugar el uso o aprovechamiento de energía eléctrica, magnética, electromagnética, de cualquier fluido, o de cualquier medio de transmisión, sin derecho y sin consentimiento de la persona que legalmente pueda disponer de los mismos.

El objeto material de la acción es la cosa ajena mueble. De lo expuesto con anterioridad surgen una serie de preguntas ¿La información es un bien mueble? ¿O su naturaleza jurídica es distinta?

---

[150] Ídem.

[151] Estados Unidos Mexicanos, "*Código Penal Federal*" Op. cit.,

La Suprema Corte De Justicia[152] expresa que se debe considerar cosas muebles a los que debido a su naturaleza intrínseca del objeto son susceptibles de ser cambiados de ámbito territorial por aplicación de una fuerza externa sin alterarlo en esencia y finalidad.

A razón de interpretación sistemática, el código civil federal, en el artículo 752 describe que son bienes muebles por su naturaleza los que pueden trasladarse de un lugar a otro, ya se muevan por sí mismo o por efecto de una fuerza exterior y son bienes muebles por determinación de la ley, las obligaciones y los derechos o acciones que tienen por objeto cosas muebles o cantidades exigibles en virtud de acción personal.

En el artículo 759 del código civil federal, y la Suprema Corte de Justicia de la Nación[153] expresan que son bienes muebles, todos los demás no considerados por la ley como inmuebles, por lo que la información entraría dentro de un bien mueble.

Ahora bien, se analizará la conducta típica del apoderamiento. Yuridia Rebollar[154] menciona que consiste en la acción de tomar o capturar una cosa con intención de ejercer poder de hecho sobre ella. González de la Vega[155] estima "apoderar de la cosa significa que el agente tome posesión material de la misma, la ponga bajo su control personal".

---

[152] Tesis visible a página mil doscientos dieciséis, del Semanario Judicial de la Federación, con número de registro: 284044, bajo el rubro BIENES MUEBLES E INMUEBLES, consultable en: http://sjf.scjn.gob.mx/SJFSist/Documentos/Tesis/284/284044.pdf, consultada el 3 de agosto de 2018.

[153] Ídem.

[154] Rebollar, Yuridia, *Delitos en Particular*, p. 121. consultable en: https://www.umla.edu.mx/PlataformaDigital/Antologias/DERECHO%20PENAL%20PARTE%20ESPECIAL%20Y%20DELITOS%20EN%20PARTICULAR.pdf consultado el 10 de agosto de 2019.

[155] Gonzáles de la Vega, Francisco, *Derecho Penal Mexicano*, 10a., Ed. Porrúa, México 1970, p. 170.

Existen diversas teorías sobre el apoderamiento en el delito de robo, la más antigua es "apprenhensio rei"[156], en la que se consideraba el apoderamiento cuando el sujeto tocaba la cosa, pero en la actualidad no tiene relevancia. Otra teoría más es la de "remoción", que es cuando la persona pone la mano sobre el objeto que quiere robar, lo mueve para el fin del delito del sitio donde su propietario lo había dejado.

Otra teoría es conocida como "ablatio"[157] que es cuando el objeto debe salir de la esfera jurídica del dueño y encontrarse en la del ladrón. Y finalmente la última teoría más conocida[11] es cuando el agente del delito transporta el objeto al lugar seguro a donde se propuso desde antes de ejecutar el robo.

La Suprema Corte de Justicia de la Nación[158], en cuanto al apoderamiento en el robo ha indicado que son dos elementos del apoderamiento en el delito de robo: el material o externo, que consiste en la aprehensión de la cosa, y el moral o interno consistente en el propósito del Activo.

La información no puede ser objeto de apoderamiento externo, ya que, para el Carding, la información puede estar almacenada en medios electrónicos o informáticos, en el ciberespacio, en donde es un lugar ficticio donde no hay contacto material o externo. Además, bajo la teoría de "ablatio"[159], el objeto nunca sale de la esfera jurídica del dueño, ya que únicamente es sustraída, copiada, u obtenida.

La materia penal es una ciencia exacta y por lo tanto no se permite la analogía y debe ser aplicada la ley en estricto sentido, por lo tanto, bajo los argumentos anteriores, la información no puede ser robada.

---

[156] Ídem.

[157] López Betancourt, Eduardo. *Delitos en Particular, tomo I, 8a., Ed.* Editorial Porrúa, México, 2002, p. 250

[158] Tesis VI.2o.8 P, visible a página quinientos treinta y cinco, tomo I. junio de 1995, del Semanario Judicial de la Federación y su Gaceta, novena época, bajo el rubro: ROBO, APODERAMIENTO COMO CONSUMACIÓN DEL, consultable en: http://sjf.scjn.gob.mx/SJFSist/Documentos/Tesis/205/205104.pdf, consultado el 14 de septiembre de 2019.

[159] González de la Vega, Francismo, "*Derecho penal*…", Op. cit., 171.

CAPÍTULO 2. BINS

2.1. Datos necesarios de una tarjeta para la compra de bienes y servicios por internet

2.1.1. *PAN* o *Primary Acount Number*[160]

En 1989 la *International Organization for Standardizatión*[161] (ISO) publicó el estándar *ISO/IEC* 7812[162] "*identification cards*[163]"-*Identification of issuers*[164]-, con la que se establecieron una serie de criterios para permitir la interoperabilidad de los *PAN*[165] tanto en comercios como en proveedores de servicios y bancos adquirientes, en otras palabras, el *PAN*[166] son los números de identificación bancaria, o los números de cuenta principal, que distinguen una tarjeta de otra, haciéndola única e irrepetible y se encuentran en la parte frontal del plástico, estos números pueden ir desde los nueve dígitos hasta los diecinueve y depende de la marca de la tarjeta que lo gestiona y del área de emisión. En la mayoría de las tarjetas bancarias son dieciséis o quince dígitos[167]. Por ejemplo:

1234 5678 9876 5432

---

[160] Op. cit., 14.

[161] La Organización Internacional de Normalización o estandarización se dedica a la creación de normas o estándares para asegurar la calidad, seguridad y eficiencia de productos y servicios. Fuente: López, Sonia*, Que es ISO*, consultable en: https://www.certificadoiso9001.com/que-es-iso/, consultado el 21 de noviembre de 2019.

[162] ISO/IEC 7812-1:2017 Identification cards — Identification of issuers — Part 1: Numbering system, consultable en: https://www.iso.org/standard/70484.html, consultado el 5 de agosto de 2019.

[163] *Identificatión cards,* significa identificación de las cartas.

[164] *Identification of issuers* significa identificación de los emisores.

[165] Op. cit., 14.

[166] Acosta, David, *¿Cómo funcionan las …",* Op? cit.,

[167] En el caso de *VISA* y *MASTERCARD* son dieciséis números, a diferencia de *American Express* que cuenta con quince.

La esquematización de los números se divide en cuatro tipos: *MII*[168], *IIN*[169] */BIN*[170], *IAI*[171] y el *Check*[172]. El primer dígito del ejemplo, en este caso el número 1 le corresponde el *Major Industry Identifier*[173]; el 1,2,3,4,5,6 se refiere al *Issuer Identified*[174], 7,8,9,8,7,6,5,4,3 son los *Individual Account Identification*[175], y finalmente el último dos le corresponde al *Check Digit*[176].

I. *Major Industry Identifier*[177]: Es el primer dígito de la tarjeta bancaria, que pueden ir del 0 al 9, correspondiéndole[178]:
    1. *ISO/TC*[179] 68 y otros.
    2. Aerolíneas.
    3. Aerolíneas y otros.

[168] Op. cit., 103.

[169] Op. cit., 104.

[170] *Bank Identificatión Number* significa “identificación de cuenta bancaria”.

[171] Op. cit., 105.

[172] Op. cit., 106.

[173] *Major Industry Identifier* significa “identificador principal de la industria”.

[174] Op. cit., 164.

[175] *Individual Account Identification,* significa “identificación de cuenta individual”-

[176] Op. cit., 105.

[177] Op. cit., 173.

[178] Acosta, David, *¿Cómo funcionan las …”,* Op? cit.,

[179] *Technical Committees*, o comité técnico en español, dedicados a la estandarización en el campo de la banca, valores y otros servicios financieros, consultable en: https://www.iso.org/committee/49650.html, consultado el 21 de noviembre de 209.

4. Viajes, entretenimiento y finanzas, incluye a *American Express*[180], *JCB*[181] y *Diners Club*[182].
5. Banca y finanzas, *VISA*[183].
6. Banca y finanzas, *MasterCard*[184].
7. Mercadeo y banca/finanzas.
8. Empresas petroleras y otros.
9. Salud, telecomunicaciones y otros.
10. Asignaciones futuras.

---

[180] *American Express*, *Company*, S.A. de C.V. y/o *American Express Bank*, S.A., Institución de Banca Múltiple son compañías globales de Servicios Integrados de Viajes y Financieros diversificadas con operaciones en más de 200 países y con presencia en México desde 1852. Fuente: *American Express*, *acerca de la compaña,* consultable en: https://www.americanexpress.com/mx/about-the-company.html, consultado el 21 de noviembre de 2019.

[181] *JCB o "Bamford Excavators Limited",* es una empresa multinacional que se dedica a fabricar equipos para la construcción. Fuente: *JCB, sobre JCB,* consultable en: https://www.jcb.com/es-pa/acerca-de, consultado el 16 de noviembre de 2019.

[182] *Diners Club* es una compañía dedicada a proveer diferentes tipos de tarjetas de crédito, tiene presencia en 185 países alrededor del mundo, Norte América, Latinoamérica, Europa, Oceanía, Medio Oriente, África y Asia, con aceptación en 22 millones de comercios. Fuente: *Diners Club, quienes somos mundo*, consultable en: https://www.mundodinersclub.com/quienes-somos-mundo.html, consultado el 21 de noviembre de 2019.

[183] *VISA* por su sigla en inglés significa "*Visa International Service Association"* que su equivalente al español es asociación de servicios internacionales de visa. Es una red comercial de pagos electrónicos, y es una marca de servicios financieros globales, en la que facilita el comercio global a través de la transferencia de valores e información entre instituciones financieras, comercios, consumidores, compañías y entidades gubernamentales. Fuente: *VISA, acerca de visa,* consultable en: https://www.visa.com.mx/acerca-de-visa.html, consultado el 21 de noviembre de 2019.

[184] *Mastercard* es un proveedor mayoritario de tarjetas, es una compañía estadounidense y un sistema de pago global que ofrece servicios dirigidos a entidades de crédito y débito. Fuente: *Mastercard*, *acerca de mastercard*, consultable en: https://www.mastercard.com.mx/es-mx/acerca-de-mastercard.html#, y https://www.bnamericas.com/es/perfil-empresa/mastercard-inc, consultado el 21 de noviembre de 2019.

II. *Issuer Identifier Number*[185]. Acosta, David[186] escribe que está compuesto por los seis primeros dígitos de la tarjeta (incluyendo el *MII*[187]). En el fenómeno del Carding al *IIN*[188] también se le conoce como BIN. El referido autor[189] señala que el *IIN*[190] permite identificar al banco emisor de la tarjeta para efectos de enrutamiento de transacciones interbancarias. Actualmente es gestionado por la *American National Standards Institute*[191].

III. ***Individual Account Identification*[192]:** Este número lo componen los dígitos a partir del séptimo hasta el penúltimo digito e identifica el número de cuenta asociado al titular de tarjeta; son los números que diferencian una tarjeta de otra, por lo que son irrepetibles.

Para la operatividad de la producción de números de tarjetas bancarias este factor del *IAI*[193] es elemental, dado a que se utiliza como elemento intelectual informático y telemático para la producción en serie de posibles *PAN*[194].

IV. ***Check Digit*[195]:** Es el último dígito de la tarjeta y es calculado usando el algoritmo de *Luhn*[196].

---

185 *Issuer Identifier Number* significa “número de identificación del emisor”.

186 Ídem.

187 Op. cit., 103.

188 Op. cit., 104.

189 Ídem.

190 Op. cit., 104.

191 *American National Standars Institute* significa Instituto Americano de Estándares Nacionales.

192 Op. Cit., 175.

193 Op. cit., 105.

194 Op. cit. 14.

195 Op. cit., 106.

196 En la parte final de este capítulo se describe que es el algoritmo de *Luhn*.

Así mismo, en la circular 34/2010[197] de Banco de México, en el punto 2.3, inciso "a" señala que las tarjetas de crédito deberán contar con *dígitos de identificación única de la Tarjeta de Crédito*.

2.1.2. Código de seguridad.

De manera histórica el código de seguridad se crea con la finalidad de evitar pérdidas económicas mediante fraudes; los bancos decidieron optar por añadir un código especial de seguridad que permitiera validar los cargos que se hicieran con la tarjeta de manera presencial. Este código se le denominaron[198] *CVV* o *Card Verificatión Value*[199], o *CVC Card Validation Code*[200], se encontraba almacenado en el *track*[201] 2 de la banda magnética y era visible por el titular de la tarjeta.

---

[197] Texto compilado de la Circular 34/2010 publicada en el Diario Oficial de la Federación el 12 de noviembre de 2010, incluyendo sus modificaciones dadas a conocer mediante Circulares 43/2010, 10/2011, 13/2014, 9/2018 y 13/2018, publicadas en el referido Diario el 20 de diciembre de 2010, 10 de mayo de 2011, 28 de julio de 2014, 18 de julio de 2018 y 3 de octubre de 2018, respectivamente. Fuente: Banco de México, *Circular 34/2010, Reglas de Tarjetas de Crédito,* p. 3, consultable en: https://www.banxico.org.mx/marco-normativo/normativa-emitida-por-el-banco-de-mexico/circular-34-2010/%7B0C55B906-6DB4-6B88-FED0-67987E9FB3CC%7D.pdf, consultado el 25 de noviembre de 2019.

[198] Acosta, David *¿Cómo funcionan las tarjetas de pago? Parte II: CID/CAV/CVC2/CVV2 consultable en* https://www.pcihispano.com/como-funcionan-las-tarjetas-de-pago-parte-ii-cidcav2cvc2cvv2/, consultado el 11 de junio de 2019.

[199] *Card Verification value, o* valor de la verificación de la tarjeta, o verificación del valor de la tarjeta. Fuente: Número *CVV de la tarjeta de crédito o débito, ubicación e información,* consultable en: https://www.cvvnumber.com/, consultado el 23 de noviembre de 2019.

[200] *Card Validation Code*, o Código de Validación de Tarjeta en español es una serie de tres o cuatro números en el anverso o reverso de una tarjeta de crédito. Este código ayuda a proporcionar una capa adicional de seguridad cuando se utiliza una tarjeta de crédito para realizar una compra en línea o por teléfono. Fuente: Kagan, Julia, *validation code,* consultable en: https://www.investopedia.com/terms/v/validation-code.asp, consultado el 27 de noviembre de 2019.

[201] Los *tracks* en el sistema de bandas magnéticas son también llamados pistas. Fuente: Tec Electrónica, *El ABC de la banda magnética,* consultable en: https://www.tec-mex.com.mx/promos/bit/bit0703-msr.htm, consultado el 25 de noviembre de 2019.

Este código era generado en el momento de la estampación de la tarjeta[202] utilizando el PAN[203], la fecha de expiración de la tarjeta y el código de servicio. Estos datos eran encriptados utilizando dos llaves de cifrado en posesión del banco emisor y usando para esta labor el algoritmo DES[204]. Cuando se realizaba una transacción empleando una tarjeta con banda magnética, estos datos son enviados y procesados por el banco emisor y comparados contra una base de datos de referencia[205]. Si los datos coinciden indica que los datos de la tarjeta no han sido manipulados y que se trata de una transacción realizada con una tarjeta legítima.

A pesar que el concepto es el mismo, cada una de las marcas de tarjetas optó por darle un nombre diferente a este código[206]:

Posteriormente con la llegada del comercio en línea, se necesitaba ingresar el *PAN*[207] pero este único requisito no sería suficiente para evitar los ciberfraudes y ciberconductas delictivas, por lo que la solución fue emplear el mismo concepto del código de seguridad y estamparlo en el plástico para que el titular lo pudiera ver.

---

[202] Ibídem

[203] Op. cit., 14.

[204] *DES* por sus siglas en inglés: *Data Encryptión Standard,* en español estándar de cifrado de datos, es un esquema de encriptación simétrico desarrollado en 1977 por el Departamento de Comercio y la Oficina Nacional de Estándares de Estados Unidos de América en colaboración con la empresa *International Business Machines*, que se creó con objeto de proporcionar al público en general un algoritmo de cifrado normalizado para redes de ordenadores. Estaba basado en la aplicación de todas las teorías criptográficas existentes hasta el momento, y fue sometido a las leyes de Estados Unidos de américa. Fuente: *DES*, consultable en: http://neo.lcc.uma.es/evirtual/cdd/tutorial/presentacion/des.html, consultado el 25 de noviembre de 2019.

[205] Ídem.

[206] Ídem.

[207] Op. cit., 14.

En la circular 34/2010 de Banco de México[208], en el punto 2.3, inciso "d" señala que las tarjetas de crédito deberán contar con *el código de seguridad de la tarjeta, asignado como dato adicional de seguridad en la realización de operaciones no presenciales con la tarjeta.* Señala la misma circular[209] que:

> *La Emisora que emita Tarjetas de Crédito con circuito integrado o chip[210] deberá observar los estándares de seguridad y procesamiento establecidos por la empresa constituida conforme a la legislación de los Estados Unidos de América, denominada EMVCo[211], LVV[212] o, en su caso, aquellos otros que el Banco de México determine como equivalente en relación con el uso y funcionamiento del referido circuito integrado o chip[213], en aquellos supuestos en que la operación con tarjeta implique obtener la información de la tarjeta directamente de dicho circuito integrado o chip[214].*

[208] Banco de México, "*Circular 34/2010",* Op. cit., p. 4.

[209] Ídem.

[210] *Chip*, es un circuito electrónico de material semiconductor, especialmente silicio, en forma de cubo minúsculo, que, combinado con otros componentes, forma un sistema integrado más complejo y realiza una función electrónica específica. Fuente: Lexico, *chip*, consultable en: https://www.lexico.com/es/definicion/chip, consultado el 25 de noviembre de 2019.

[211] EMVCo facilita la interoperabilidad mundial y la aceptación de transacciones de pago seguras, por medio de diferentes tecnologías, por ejemplo: de contacto, sin contacto, móvil *tokenización* de pago, códigos QR, comercio remoto seguro, *3-D secure.* Fuente: *EMVCo*, consultable en: https://www.emvco.com/, consultado el 25 de noviembre de 2019.

[212] *LLC* o *Limited Liability Company* significa Sociedad de Responsabilidad Limitada. Fuente: Company Combo, *¿Cuál es la diferencia entre una empresa LLC y una CORP?,* consultable en: http://companycombo.com/es/faq/cual-es-la-diferencia-entre-una-empresa-llc-y-una-corp/, consultado el 25 de noviembre de 2019.

[213] Op. cit., 210.

[214] Op. cit., 210.

Con el *PAN*[215], la fecha de vencimiento y el código de seguridad formaban tres candados para transacciones en internet, dificultando las actividades delictivas que pudieras suscitarse con ellas.

2.1.3. Fecha de vencimiento

La fecha de vencimiento es también conocida como fecha de expiración, está impresa en el plástico, forma parte de los elementos de datos del titular de la tarjeta. Sirve además de identificar que la tarjeta siga vigente, como un requisito para las compras de bienes y servicios.

En la circular 34/2010[216] en el punto 2.3, número siete, señala que la fecha de vencimiento es un requisito que deberá contener por lo menos, las tarjetas de crédito.

2.1.4. Nombre

El nombre es un elemento de los datos del titular de la tarjeta. En el momento del uso indebido con una tarjeta por un tercero no autorizado en compras a distancia, el nombre no es un requisito indispensable para la confirmación de compra, ya que en un primer instante únicamente se verifican que los datos subjetivos de la tarjeta: el *PAN*[217], la fecha de vencimiento y el código de seguridad sean correctos, y que la cuenta bancaria a la tarjeta disponga de saldo suficiente para procesar la compra, este proceso dura segundos, por lo que no se verifica.

Posteriormente el establecimiento comercial o la entidad emisora se encargan de verificar los datos objetivos y subjetivos del mismo, por lo que piden datos adicionales como son identificación oficial, estados de cuenta, fotografía de la tarjeta bancaria, para confirmar los datos subjetivos y objetivos de la compra con los documentos requeridos y así validar la compra. Como se escribió en el

---

[215] Op. cit., 14.

[216] Banco de México, "*Circular 34/2010",* Op. cit., p.3.

[217] Op. cit., 14.

capítulo primero del presente trabajo, estos documentos pueden ser falsificados por los delincuentes.

En la circular 34/2010[218] de Banco de México, en el punto 2.3, número siete, menciona que deberá contener el nombre del Tarjetahabiente como requisito mínimo que deberá llevar la tarjeta de crédito.

2.2. Concepto de BINS

De manera concreta y práctica se entiende por BIN a la serie de números base de una tarjeta para la generación y producción en serie de la misma, el cual se compone de por lo menos 6 dígitos base y el resto, pueden ser números o letras colocados en lugares estratégicos para la generación masiva de números de tarjetas bancarias, por medio de programas informáticos o telemáticos. Un ejemplo de un BIN es: 543924xx7x8x6xxx

Varios autores tienen un concepto general de lo que son los BINS, Carlos Tovar[219] expone que:

> *Los BINS son derivados del código binario, donde partiencido de los primeros cuatro o seis números de las tarjetas bancarias, se pueden generar el resto mediante programas especiales que se encuentran en internet, además de que con este programa se pueden obtener las fechas de vencimiento y códigos de seguridad, donde los bineros, es decir, las personas que realizan esta práctica se dedican a encontrar y crear números de tarjetas bancarias para hacer comprar falsas, o bien a nombre de usuarios reales de bancos.*

Blaker[220] señala que *un BIN son los seis primeros números de una tarjeta la cual identifica al banco y al tipo de tarjeta que es,* y agrega que *los BINS nos permiten*

---

[218] Banco de México, "*Circular 34/2010",* Op. cit., p.

[219] Tovar, Carlos, *Los niños ratas del ciberespacio,* 2014, consultable en: https://www.elmanana.com/los-ninos-ratas-del-ciberespacio/2604450 consultado el 15 de abril de 2019.

[220] Blaker, Cristian, *Bins y Carding*| *Todo lo que debes aprender,* 2018, consultable en: https://rincondelgeek.com/Bins+y+carding+, consultado el 15 de abril de 2019.

generar tarjetas de crédito o débito, así mismo genera la fecha, es decir, el mes y año en que caduca la tarjeta, y el "CVV[221]".

La Comisión Nacional para la Protección y Defensa de los Usuarios de los Servicios Financieros[222] combina el concepto de Carding con el de BINS, al expresar que *carding es una forma de estafa online[223] que consiste en acceder ilegalmente al número de una tarjeta bancaria y a través de un software[224] generan de manera aleatoria la fecha de expiración y el código de seguridad.* La primera parte describe una modalidad del carding, y la última se refiere a un subtipo de los BINS que es la generación de información o números de tarjetas.

Los BINS, son un subtipo del Carding, que incluyen varias subconductas, y su modo de operación es complejo. En primer lugar, consiste en la producción de posibles *PAN*[225], fechas de vencimiento y códigos de seguridad; se dice que son posibles porque la producción se genera de manera masiva, -decenas o centenas de grupos de información- sin embargo, dentro de toda la información generada puede que solamente una cadena de información se procese como exitosa en el pago de bienes o productos, y que toda la demás sean únicamente un conjunto de datos sin orden.

Un segundo elemento es la alteración de los números de tarjetas bancarias o departamentales, y estos son aprovechados por los fallos de los sistemas de seguridad de los procesadores de compras de bienes y servicios en internet, puesto que un BIN no es única y exclusivamente tomar los primeros seis dígitos de la tarjeta bancaria, por ejemplo 543924 y rellenarlo con la letra «X» para que el programa informático pueda cambiar el resto de las *X* por números aleatorios y que coincidan con el número de alguna tarjeta real de algún tarjetahabiente, -

---

[221] Op. cit., 199.

[222] Comisión Nacional para la Protección y Defensa de los Usuarios de los Servicios Financieros, *Checa tu estado de cuenta y cuídate del Carding,* consultable en: https://www.gob.mx/condusef/articulos/checa-tu-estado-de-cuenta-y-cuidate-del-carding?idiom=es consultado el 23 de junio de 2019.

[223] Op. cit., 4.

[224] Op. cit., 5.

[225] Op. cit., 14.

más bien eso sería la técnica vista en el capítulo 1 de la presente investigación llamada fuerza bruta- si no que, además, requiere un cuidadoso estudio de las vulnerabilidades tecnológicas, y la colocación estratégica de las letras *X* en los BINS, pudiendo quedar de la siguiente manera 543924xx7x8x6xxx. Siendo estos números el mínimo denominador de las tarjetas bancarias que está procesando como válida o exitosa la página, a este paso se le conoce como alteración, porque modifican los números de una tarjeta bancaria real, para encontrar vulnerabilidades.

Un tercer punto, es comprobar si la información generada corresponde a una tarjeta que puede ser procesada con éxito para la compra de bienes y servicios, y esto se realiza de dos formas, la primera es comprobar manualmente en páginas de internet donde su seguridad sea escasa o mínima, por ejemplo, en servicios básicos como de entretenimiento, *streaming*[226], plataformas de música, etc., o bien, por medio de verificadores *checkers*[227], o comprobadores de pago.

Estos verificadores son programas informáticos, ya sea públicos o privados que procesan toda la información que se creó de manera masiva por medio de los BINS, colocándola en su procesador de datos, y por medio de complejos procedimientos informáticos y telemáticos, comprueban en diferentes páginas de internet en donde se puedan realizar compras por internet -ya sean nacionales o extranjeras- que la información generada sea procesada con éxito y al final del proceso muestran en la ventana principal todos los números de tarjetas que son válidos para la compra de bienes y servicios en internet.

Existe un debate entre si la información generada y procesada con éxito en las compras por internet son de una tarjeta real o no, algunos escritores manifiestan que los números generados por medio estos programas informáticos, que se

[226] Op. cit., 93.

[227] *Checkers* o verificadores son *softwares* públicos u onerosos que sirven para comprobar si una tarjeta es procesada con éxito en una compra no presencial.

verifican y se usan son falsos, al respecto García[228] menciona que los *números generados de un BIN no son de gente real ya que únicamente son algoritmos.* Anónimo[229] expone que son tarjetas de crédito falsas generados por medio de *softwares*[230] virtuales con derechos de autor; los cuales son desarrollados usando un avanzado lenguaje de programación. Además, argumentan de que las compras son procesadas con números de tarjetas bancarias que no existen, y esto es gracias a un error en el sistema de pagos.

La corriente de pensamiento afirma que las tarjetas que son obtenidas son válidas, no obstante, eso no quiere decir que sean reales o que estén asociadas a un cliente de alguna institución o negocio mercantil, y que posiblemente son procesadas dado a algún fallo en la administración por parte del emisor de la tarjeta o por fallos en el sistema de pagos.

Las instituciones emisoras de las tarjetas bancarias, departamentales, y los sistemas de seguridad de procesadores de compras no han manifestado nada al respecto, por lo que se presume que los números generados a través de estos programas pueden tener el carácter de reales o ficticios inexistentes.

2.3. Conductas y *Modus Operandi* de los BINS

Generalmente después de usar una tarjeta bancaria de manera indebida, el criminal simplemente borra o ignora los números de la tarjeta bancarias, o bien, puede extrapolar los datos de la tarjeta bancaria, es decir, hace el proceso de creación de un BIN de manera estratégica para la compra de bienes y servicios, generalmente para encontrar un fallo en el sistema de pagos de la página.

El criminal no forzosamente tiene que ser un experto en informática o telemática para encontrar fallos en el sistema de alguna página, ya que generalmente es

---

[228] García, Yesenia, *BINS primeros pasos,* 2016, p. 3, consultable en: https://www.academia.edu/28287735/BINS_PRIMEROS_PASOS_Conceptos_b%C3%A1sicos consultado el 15 de abril de 2019.

[229] *Tarjetas de crédito falsas*, consultable en*:* https://www.tarjetasdecreditofalsas.com/, consultado el 15 de enero de 2019.

[230] Op. cit., 5.

por medio de comprobación manual y directa, y este proceso puede tardar hasta días para ser exitoso.

Un ejemplo de un formato de un BIN puede ser 435687xxxxxxxxx, posterior a este paso, se ingresa toda la cadena de información a programas informáticos o telemáticos, por ejemplo, páginas como discard[231], namso[232], bincodes[233], *fake card*[234], en los que todas las *X* que están en el BIN serán sustituidas por números aleatorios, y además está la opción de generar la fecha de vencimiento y el código de seguridad.

Una vez creada toda la información, el criminal debe de comprobar que los números de las tarjetas bancarios son válidos, por los que cuenta con dos opciones, la primera es verificar manualmente en alguna página de internet con poca seguridad los procesa como válidos, generalmente los verifican en servicios de entretenimiento, *streaming*[235], plataformas de música; el segundo método es por medio de los *checkers*[236]*,* verificadores o comprobadores de pago, sin embargo, la mayoría de estos son onerosos y pocos tienen acceso a ellos.

Teniendo los números de las tarjetas bancarias que son procesados como válidos, pueden ser usados para generar más BINS, con los números comunes a todos ellos, por ejemplo, si diez de los números tarjetas bancarios que son procesados con éxito son los siguientes:

4356873756556801

4356874783625262

---

[231] Consultable en: https://www.elfqrin.com/discard_credit_card_generator.php, consultado el 1 de agosto de 2018.

[232] Consultable en: https://namso-gen.com/ https://www.fakepersongenerator.com/credit-card-generator, 1 de agosto de 2018.

[233] Consultable en: https://www.bincodes.com/ https://www.fakepersongenerator.com/credit-card-generator, 1 de agosto de 2018.

[234] Consultable en: https://www.fakepersongenerator.com/credit-card-generator, 1 de agosto de 2018.

[235] Op. cit., 93.

[236] Op. cit., 227.

4356876283706633

4356875517333057

4356876014441385

4356872782464170

4356876006306547

4356878465816040

4356877486704672

4356878316705707

Los primeros seis números son el BIN, y se busca los demás números comunes en el total de tarjetas procesadas con éxito, por ejemplo:

4356873**7**5**6**556801

4356874**7**8**6**625262

4356876283706633

4356875517333057

435687601**6**441385

4356872**7**82464170

435687600**6**306547

4356878**7**65816040

435687748**6**704672

4356878**7**1**6**705707

Obteniendo como fin el BIN: **434687x7x6xxxxxx**, en el que se hará el mismo procedimiento mencionado con anterioridad.

Posteriormente, el criminal ocupa toda la información que se generó para ocuparla para sí mismo, o bien, para vender el BIN generado en internet, especialmente en la red social *Facebook*, en donde dicha información ronda desde los cien pesos hasta los cien mil pesos dependiendo de la página en la que se haya encontrado la vulnerabilidad.

2.4. La importancia del algoritmo de *Luhn* en los BINS

El algoritmo de *Luhn* fue creado por el científico de *International Business Machines*[237] Hans Peter *Luhn* (razón por la cual se denomina así) con la finalidad de validar que los números de una tarjeta bancaria sean correctos. Sin embargo, este algoritmo se tomó como un referente real y material en el fenómeno del Carding para el uso de herramientas tecnologías para perfeccionar sus conductas delictivas.

A manera de antecedente histórico, cuando las personas que se dedicaban a realizar la producción de manera masiva de posibles *PAN*[238] lo hacían sin ningún conocimiento sobre si eran correctas o no, por lo que su grado de preparación intelectual era mínimo, sin embargo, cuando se divulgó sobre este conocimiento, cambio el paradigma del Carding, de delitos de fuerza bruta a delitos de cibercuello blanco, evolucionando las conductas delictivas del propio fenómeno y de las que se puedan generar del mismo.

La operatividad del algoritmo[239] de *Luhn* es tomar la serie de números del *PAN*[240], contándose desde el penúltimo dígito tomado desde la derecha y se multiplica por dos alternadamente entre cada digito, (si el resultado son dos dígitos, se suman los dos valores), posteriormente se suman todos los dígitos obtenidos. Véase

---

[237] International Business Machines o IBM (conocida coloquialmente como el Gigante Azul): Es una empresa transaccional que fabrica y comercializa herramientas, programas y servicios relacionados con la informática. Fuete: ecured, *IBM*, consultable en: https://www.ecured.cu/IBM, consultado el 25 de noviembre de 2019.

[238] Op. cit., 14.

[239] Paenza, Adrián, *La matemática del futuro*, Editorial Sudamericana, 2017, p. 33.

[240] Op. cit., 14.

4	3	5	6	8	7	6	0	0	6	3	0	6	5	4	7
x2		x2		x2		x2		x2		x2		x2		x2	
8		1+0=1		1++7=8		1+2=3		2		6		1+2=3		8	
8	3	1	6	7	7	3	0	0	6	6	0	3	5	8	7

Tabla 1. *Operatividad del algoritmo de luhn.*

Al sumar todos los dígitos se obtiene un total de 70, por lo que este se debe dividir entre 10, y si es múltiplo de 10 es un *PAN*[241] válido.

Ahora veremos el ejemplo de un *PAN*[242] invalido[243]

4356874786625262

4	3	5	6	8	7	4	7	8	6	6	2	5	2	6	2
x2		x2		x2		x2		x2		x2		x2		x2	
8		1+0=1		1++7=8		8		1+6=7		1+2=3		1+0=1		1+2=3	
8	3	1	6	7	7	8	7	7	6	3	2	1	2	3	7

Tabla 2. *Ejemplo de un Primary Account Number Inválido verificado por el algoritmo de luhn.*

El resultado de la suma es 78, y al no ser múltiplo de 10, se percata que es un número de tarjeta invalido, y es inventado.

[241] Op. cit., 14.

[242] Op. cit., 14.

[243] Ídem.

CAPÍTULO 3. MEDIDAS PARA COMBATIR EL CARDING Y LOS BINS

3.1. Medidas y protocolos internacionales

a) *Payment Card Industry Data Security Standard* [244].

Las Normas de seguridad de datos de la industria de tarjetas de pago (*PCI DSS*)[245] se desarrollaron para fomentar y mejorar la seguridad de los datos del titular de la tarjeta y facilitar la adopción de medidas de seguridad uniformes a nivel mundial como una guía para evitar las conductas delictivas que involucran tarjetas de pago de débito y crédito.

Antes de que publicara por primera vez la versión del estándar *PCI DSS*[246], cada marca de tarjetas de pago contaban con su propio programa para la protección de la información de los datos del tarjetahabiente. Véase:

- *American Express*[247] *–Data Security Operating Policy*[248]*.*

[244] *Payment Card Industry Data Security Standard* significa Estándar de seguridad de datos de la industria de tarjetas de pago en español. Fuente: *PCI Security,* consultable en: https://www.pcisecuritystandards.org/pci_security/, consultado el 27 de noviembre de 2019.

[245] Op. cit. 18.

[246] Ídem.

[247] Op cit., 180.

[248] *DSOP* por sus siglas en inglés *Data Security Operating Policy,* significa en español política operativa de seguridad de datos. Fuente: *American Express*, *Política operativa de seguridad de datos de American Express para proveedores de servicios,* consultable en: https://www.google.com/search?q=que+es+data+security+operating+policy&oq=que+es+data+security+operating+po&aqs=chrome.1.69i57j33l5.7911j1j7&sourceid=chrome&ie=UTF-8, consultado el 26 de noviembre de 2019.

- *Discover[249] – Discover Information Security Compliance[250]*.
- *JCB[251] International – Data Security Program.[252]*
- *MasterCard[253] – Site Data Protection[254].*
- *Visa[255], Estados Unidos de America – Cardholder Information Security Program[256].*
- *Visa[257] Internacional – Account Information Security Program[258].*

---

[249] Discover Financial Service, empresa de los Estados Unidos de América, operadora y poseedora del sistema de pagos de las transacciones que se llevan a cabo con las tarjetas Discover y otros productos de la marca. Fuente: Fernández Díaz, Macarena, *Cómo solicitar una tarjeta Discover,* 2018, consultable en: https://www.cuidatudinero.com/13170246/como-solicitar-una-tarjeta-discover, consultado el 26 de noviembre de 2019.

[250] DISC por sus siglas en inglés, *Discover Information Security Compliance,* que en español significa Discover, seguridad de la información y cumplimiento. Fuente: *Discover Global Network*, *Discover Informatión Security & Compliance (DISC)*, consultable en: https://www.discoverglobalnetwork.com/en-us/business-resources/fraud-security/pci-rules-regulations/discover-information-security-compliance, consultado el 26 de noviembre de 2019.

[251] Op. cit., 181.

[252] *DSP* por sus siglas en inglés *Data Security Program*, significa Programa de Seguridad de Datos, este ayuda a proteger los datos del titular de la tarjeta y los datos de las transacciones. Fuente: Global JCB, *PCI DSS, Payment Card Industry Data Security Standard*, consultable en: https://www.global.jcb/en/products/security/pci-dss/index.html, consultado el 26 de noviembre de 2019.

[253] Op. cit., 184.

[254] SDP por sus siglas en inglés *Site Data Protection,* que en español significa Protección de datos del sitio. Fuente: *MasterCard, Protecting the payments ecosystem,* consultable en: https://www.mastercard.us/en-us/merchants/safety-security/security-recommendations/site-data-protection-PCI.html, consultado el 26 de junio de 2019.

[255] Op. cit., 183.

[256] *CISP* por sus siglas en inglés *Cardholder Information Security Program* que significa programa de seguridad de la información del titular de la tarjeta visa. Fuente: Dwyer, Ben, *Visa Cardholder Information Security Program,* consultable en: https://www.cardfellow.com/blog/visa-cardholder-information-security-program-cisp/, consultado el 26 de noviembre de 2019.

[257] Op. cit., 183.

[258] *AIS* por sus siglas en inglés *Account Information Security*, significa Seguridad de la Información de la Cuenta mediante el cual proporciona estándares de seguridad de la

Las *PCI DSS*[259] proporcionan una referencia de requisitos técnicos y operativos desarrollados para proteger los datos de los titulares de tarjetas[260]. Las *PCI DSS*[261] se aplican a todas las entidades que participan en el procesamiento de tarjetas de pago[262], entre las que se incluyen comerciantes, procesadores, adquirientes, entidades emisoras y proveedores de servicios, así como en las demás entidades que almacenan, procesan o transmiten datos del titular de la tarjeta o datos de autenticación confidenciales.

La versión 3.2 señala doce requisitos para el cumplimiento, clasificándolos en 6 apartados[263]:

- *Desarrolle y mantenga redes y sistemas seguros*
    1. *Instalar y mantener una configuración de firewall[264] para proteger los datos del titular de la tarjeta.*
    2. *No utilizar contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores.*
- *Proteger los datos del titular de la tarjeta.*
    1. *Proteja los datos del titular de la tarjeta que fueron almacenados.*
    2. *Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas.*

---

información, criterios para validad el cumplimiento, guías y herramientas de ayuda. Fuente: *VISA*, *Information Security,* consultable en: https://aw.visa.com/run-your-business/small-business/information-security/ais-program.html, consultado el 26 de noviembre de 2019.

[259] Op. cit., 18.

[260] Ídem.

[261] Op. cit., 18.

[262] Ídem.

[263] Ídem.

[264] Un firewall es un dispositivo de seguridad de la red que monitorea el tráfico de red -entrante y saliente- y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad. Fuente: CISCO, *¿Qué es un firewall?,* consultable en: https://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html, consultado el 26 de noviembre de 2019.

- *Mantener un programa de administración de vulnerabilidad*
    1. *Utilizar y actualizar con regularidad los programas o softwares[265] antivirus[266].*
    2. *Desarrolle y mantenga sistemas y aplicaciones seguras.*
- *Implementar medidas sólidas de control de acceso.*
    1. *Restinga el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa.*
    2. *Identifique y autentique el acceso a los componentes del sistema.*
    3. *Restringir el acceso físico a los datos del titular de la tarjeta*
- *Supervisar y evaluar las redes con regularidad*
    1. *Rastree y supervise todos los accesos a los recursos de red y a los datos de los titulares de las tarjetas*
    2. *Pruebe con regularidad los sistemas y procesos de seguridad.*
- *Mantener una política de seguridad de información*
    1. *Mantenga una política que aborde la seguridad de la información para todo el personal.*

B) *ISO/IEC[267]* 7812-1:2006 *Identification cards[268], Identification of issuers[269], Part 1: Numbering system*

[265] Op. cit., 5.

[266] El antivirus es una aplicación independiente o un conjunto de programas que detectan y eliminan virus de ordenadores y redes. Fuente: *SoftwareLab*, *¿Qué es un antivirus? La definición y los 5 ejemplos principales,* consultable en: https://softwarelab.org/es/que-es-un-antivirus/, consultado el 26 de noviembre de 2019.

[267] Op. cit., 162.

[268] Op. cit., 163.

[269] Op. cit., 164.

Para permitir operatividad entre los diferentes tipos y marcas de tarjetas, en 1989 la *ISO*[270] publicó el estándar *ISO/IEC* 7812[271] "*Identification cards*[272] — *Identification of issuers*[273]". En este estándar se establecían una serie de criterios para permitir la interoperabilidad de los *PAN*[274] tanto en comercios como en proveedores de servicio y bancos adquirientes.

3.2. Medidas y disposiciones nacionales

3.2.1. Banco de México

Circular 34/2010.

Esta circular ha tenido modificaciones[275] mediante las circulares 43/2010, 10/2011, 13/2014, 9/2018 y 13/2018, publicadas en el Diario Oficial de la Federación el 20 de diciembre de 2010, 10 de mayo de 2011, 28 de julio de 2014, 18 de julio de 2018 y 3 de octubre de 2018, respectivamente.

La circular está compuesta por cinco apartados

1. Definiciones
2. Disposiciones generales
3. Protección al tarjetahabiente
4. Pago mínimo
5. Cargos Recurrentes

Al respecto, en el punto 3.3 denominado "Aviso de robo o extravió de Tarjetas de Crédito y reclamación de cargos", en donde[276]:

[270] Ídem.

[271] ISO/IEC 7812-1:2017 "*Identification cards*…", Op. cit.,

[272] Op. cit., 163.

[273] Op. cit., 164.

[274] Op. cit., 14.

[275] Banco de México, "*Circular 34/2010",* Op. cit., p.10.

[276] Ibídem, p.10.

la emisora deberá permitir presentar avisos de (i) robo o extravío de la Tarjeta de Crédito correspondiente, o (ii) reclamaciones por cargos a la Cuenta que no reconozcan como propio, de manera personal, o a través de los canales electrónicos o cualquier otro medio de comunicación, en la cual esta deberá entregar un número de referencia del aviso, así como la fecha y hora en que esta se recibió.

En el punto 3.4[277] denominado "responsabilidad por cargos no reconocidos realizados con la Tarjeta de Crédito", expone que *la entidad emisora que reciba algunos de los avisos a que se refiere el primer párrafo del numeral 3.3 estará obligada a abonar, en la respectiva cuenta, a más tardar el segundo día hábil siguiente a la recepción del aviso cuando* (i) los referidos cargos correspondan a operaciones realizadas durante las cuarenta y ocho horas previas a la presentación del aviso antes señalado, y (ii) cuando se haya presentado dentro de un plazo de noventa días naturales posteriores a la fecha en que se realizó el cargo no reconocido.

En el punto 3.6[278] menciona que la emisora únicamente podrá obtener la devolución del monto correspondiente al abono que haya realizado en términos del numeral 3.4, cuando acredite al Tarjetahabiente que el cargo respecto del cual haya realizado dicho abono derivó de una operación ejecutada de conformidad con lo dispuesto en términos del inciso a) del numeral 2.6.

3.2.2. Ley Para Regular Las Instituciones de Tecnología Financiera

El 9 de marzo de 2018 se publicó en el Diario Oficial de la Federación la Ley para Regular Las Instituciones de Tecnología Financiera[279], con el objetivo de regular los servicios financieros que prestan las instituciones de tecnología financiera, bajo los principios de inclusión e innovación financiera, promoción de

[277] Ibídem, p. 11.

[278] Ibídem, p.13.

[279] Estados Unidos Mexicanos, *Ley para regular las Instituciones de Tecnología Financiera*, nueva ley publicada en el Diario Oficial de la Federación el 9 de marzo de 2018, consultable en http://www.diputados.gob.mx/LeyesBiblio/pdf/LRITF_090318.pdf, consultado el 06 de junio de 2019.

la competencia, protección al consumidor, preservación de la estabilidad financiera, prevención de operaciones ilícitas y neutralidad tecnológica.

La ley contiene 145 artículos dividido en siete títulos. El titulo segundo denominado “De las ITF y sus Operaciones”, capítulo segundo “De las Instituciones de fondo de Pago Electrónico”, establece una manera indirecta para prevenir el Carding.

La ley regula los fondos de pago electrónico, o conocidas como *pallets* o monederos electrónicos en los que se permiten hacer pagos, compras y envíos de dinero de manera digital a través de teléfonos móviles. De esta forma, aunque no sea directamente un servicio bancario tradicional, vela por la seguridad de las transacciones, para preservar la información y patrimonio de los usuarios,

Asimismo, con la regulación de la *criptomoneda*[280] como uso de activos serán utilizadas como medio de pago electrónico, ofreciendo más medios de pago, que únicamente pagos por tarjetas.

El artículo veintidós[281] de la Ley para Regular las Instituciones de Tecnología Financiera, menciona que solo las personales morales autorizadas por la Comisión Nacional Bancaria y de Valores, podrán actuar como instituciones de fondos de pago electrónico. El artículo veintitrés[282] de la ley en comento establece que los fondos de pago electrónico son aquellos fondos que estén contabilizados en un registro electrónico de cuentas transaccionales que al efecto lleve una institución de fondos de pago electrónico. Las Instituciones de pago electrónico, además de las operaciones y actividades a que se refiere la mencionada ley, pueden realizar alguna de las funciones siguientes[283]: *Prestar*

---

[280] Cointelegraph, *que son y cómo funciona el dinero digital,* consultable en: https://es.cointelegraph.com/bitcoin-for-beginners/what-are-cryptocurrencies, consultado el 26 de noviembre de 2019.

[281] Op. cit., 279.

[282] Ídem.

[283] Ibídem, artículo 25.

el servicio de transmisión de dinero, realizar operaciones con activos virtuales[284]*, constituir depósitos a la vista o a plazo en entidades financieras autorizadas para recibirlos, entre más. Además, las instituciones de fondos de pago electrónico*[285] *podrán otorgar créditos y préstamos por sobregiros*.

3.2.3. Comisión Nacional Bancaria y de Valores

El artículo cuarto de la Ley de la Comisión Nacional Bancaria y de Valores[286], expresa que corresponde a la Comisión, *fracción XIX, (…) coadyuvar con el ministerio público respecto de los delitos previstos en las leyes al sistema financiero.*

El Reglamento de la Comisión Nacional Bancaria y de Valores[287]

> *Artículo 37, A La Dirección General de Delitos y Sanciones, a través de su titular, le corresponderán las atribuciones siguientes:*
>
> *(…) VII. Dar opinión a la Secretaría de Hacienda y Crédito Público para efectos de la denuncia o querella que corresponda formular a esa Dependencia, para que se proceda por los delitos a que se*

[284] Un activo virtual es una unidad de información que no representa la tenencia de algún activo subyacente a la par, y que es unívocamente identificable, incluso de manera fraccional, almacenada electrónicamente. Fuente. Banco de México, ¿Qué es un activo virtual?, consultable en: https://www.banxico.org.mx/sistemas-de-pago/1---que-es-un-activo-virtua.html, consultado el 26 de noviembre de 2019.

[285] Ibídem, artículo 27.

[286] Estados Unidos Mexicanos, *Ley de la Comisión Nacional Bancaria y de Valores*, Diario Oficial de la Federación, 28 de abril de 1995, última reforma publicada en el Diario Oficial de la Federación el 09 de marzo de 2018, consultable en: http://www.diputados.gob.mx/LeyesBiblio/pdf/46_090318.pdf, consultado el 13 de agosto de 2019.

[287] Estados Unidos Mexicanos, *Reglamento interior de la Comisión Nacional Bancaria y de Valores*, Diario Oficial de la Federación, 12 de noviembre de 2014, México, consultable en. http://www.diputados.gob.mx/LeyesBiblio/regla/n228.pdf, consultado el 13 de agosto de 2019.

refieren la LRAF[288], la LIC[289], la LRSIC[290], la LGOAAC[291], la LMV[292], la LFI[293], la LACP[294], la LUC[295], la LRASCAP[296] y otras leyes que atribuyan a la Comisión dicha competencia.

---

[288] Estados Unidos Mexicanos, *Ley para Regular las Agrupaciones Financieras*, Diario Oficial de la Federación, 10 de enero de 2014, última reforma publicada en el Diario Oficial de la Federación el 03 de marzo de 2018, consultable en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LRAF_090318.pdf, consultado el 14 de agosto de 2019.

[289] Estados Unidos Mexicanos, "*Ley de Instituciones de crédito",* Op. cit.,

[290] Estados Unidos Mexicanos, *Ley para Regular las Sociedades de Información Crediticia*, Diario Oficial de la Federación, 15 de enero de 2002, última reforma publicada en el Diario Oficial de la Federación el 3 de marzo de 2018, consultable en: http://www.diputados.gob.mx/LeyesBiblio/pdf/237_090318.pdf, consultado el 14 de agosto de 2019.

[291] Estados Unidos Mexicanos, *Ley General de Organizaciones y Actividades Auxiliares del Crédito*, Diario Oficial de la Federación, 14 de enero de 1985, última reforma publicada en el Diario Oficial de la Federación el 9 de marzo de 2018, consultable en: http://www.diputados.gob.mx/LeyesBiblio/pdf/139_090318.pdf, consultado el 14 de agosto de 2019.

[292] Estados Unidos Mexicanos, *Ley del Mercado de Valores,* Diario Oficial de la Federación, 30 de diciembre 2005, última reforma publicada en el Diario Oficial de la Federación el 9 de enero de 2019, consultable en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LMV_090119.pdf, consultado el 14 de agosto de 2019.

[293] Estados Unidos Mexicanos, *Ley de fondos de inversión,* Diario Oficial de la Federación, 4 de junio de 2001, última reforma publicada en el Diario Oficial de la Federación el 13 de junio de 2014, consultable en: http://www.diputados.gob.mx/LeyesBiblio/pdf/69_130614.pdf, consultado el 14 de agosto de 2019.

[294] Estados Unidos Mexicanos, *Ley de Ahorro y Crédito Popular ,* Diario Oficial de la Federación, 4 de junio de 2001, última reforma publicada en el Diario Oficial de la Federación el 10 de enero de 2014, consultable en: http://www.diputados.gob.mx/LeyesBiblio/pdf/17.pdf, consultado el 14 de agosto de 2019.

[295] Estados Unidos Mexicanos, *Ley de Uniones de Crédito,* Diario Oficial de la Federación, 20 de agosto de 2008, última reforma publicada en el Diario Oficial de la Federación el 10 de agosto de 2008, consultable en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LUC.pdf, consultado el 14 de agosto de 2019.

[296] Estados Unidos Mexicanos, *Ley para Regular las Actividades de las Sociedades Cooperativas de Ahorro y Préstamo*, Diario Oficial de la Federación, 13 de agosto de 2009, última reforma

Asimismo, la Comisión Nacional Bancaria y de Valores y la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, podrán investigar hechos, actos u omisiones de los cuales pueda presumirse la violación de las leyes mencionadas *ut supra* en el ámbito de su competencia.

3.2.4 Comisión Nacional para la Protección y defensa de los usuarios de servicios financieros. CONDUSEF

En la ley de protección y defensa a los usuarios de servicios financieros, expresa en el artículo once[297], las facultades que tiene la comisión frente al Carding

> *La Comisión Nacional está facultada para: (…)*
>
> *XXVI. Denunciar ante el Ministerio Público cuando se tenga conocimiento de hechos que puedan ser constitutivos de delitos en general y ante la Secretaría cuando se trate de delitos tipificados en leyes que establezcan que el delito se persiga a petición de dicha Secretaría.*

La CONDUSEF creo el Portal de Fraudes Financieros[298] con el objetivo de mitigar los ciberfraudes, en los que se encuadra el Carding en su modalidad de obtención. El Portal cuenta con[299]:

---

publicada en el Diario Oficial de la Federación el 13 de agosto de 2009, consultable en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LRASCAP_280414.pdf, consultado el 14 de agosto de 2019.

[297] Estados Unidos Mexicanos, *Ley de Protección y Defensa al Usuario de Servicios Financieros*, Diario Oficial de la Federación, 18 de enero de 1999, última reforma publicada en el Diario Oficial de la Federación el 18 de enero de 1999, consultable en http://www.diputados.gob.mx/LeyesBiblio/pdf/64_090318.pdf, consultado el 06 de noviembre de 2019.

[298] El portal está disponible en: https://phpapps.condusef.gob.mx/fraudes_financieros/, consultado el 1 de agosto de 2019.

[299] Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, *Conoce el nuevo Portal de Fraudes Financieros*, consultable en:: https://www.gob.mx/condusef/articulos/conoce-el-nuevo-portal-de-fraudes-financieros?idiom=es consultado el 22 de junio de 2019.

- *Monitor de reportes: En la que los usuarios podrán conocer datos fraudulentos reportados, como: números de teléfono, páginas de Internet, correos electrónicos, instituciones falsas, entre otros. Asimismo, la forma en cómo se realizó el fraude con la descripción detallada del modus operandi.*
- *Comparte tu experiencia: los usuarios podrán reportar los casos en los que fueron víctimas o bien, aquellos en los que identificaron un posible fraude al recibir un correo, llamada o mensaje de texto.*

Además, la comisión publica recomendaciones en su página de internet en la que brinda consejos para prevenir el Carding.

El artículo llamado *Checa tu estado de cuenta y cuídate del carding*[300]*,* publicado el 21 de junio de 2019 en la que recomiendan:

I. *Cuando se utilice tu tarjeta no la pierdas de vista o dejes que la persona que te vaya a obrar digite tu código de seguridad o CVV*[301]*, siempre hazlo tú mismo.*
II. *Nunca utilices redes o computadores públicas si vas a hacer compras en línea, también verifica que la página sea segura y cuenta con el protocolo de seguridad "https*[302]*" y un candado cerrado en la barra de dirección.*
III. *Monitorea tus estados de cuenta para identificar compras que tú no hayas realizado, en caso de exista alguna, repórtala inmediatamente con tu banco para realizar el proceso de devolución y cancelación.*

---

[300] Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, *"Checa tu estado de cuenta…",* Op. cit.,

[301] Op. cit., 199.

[302] *HTTPS* es una versión segura del Protocolo de Transferencia de Hipertexto. La 'S' quiere decir 'Seguro'. Es un método para garantizar una comunicación segura entre el navegador de un usuario y un servidor web. Fuente: Pickaweb. *¿Qué es HTTPS?,* consultable en: https://www.pickaweb.es/ayuda/que-es-https/, consultado el 26 de noviembre de 2019.

IV. *Activa las alertas de movimientos que los bancos ofrecen a cada cliente. Acude al ministerio público a levantar un acta, incluso si el banco ya te devolvió tu dinero.*

V. *Acércate a la CONDUSEF en caso de necesitar ayuda o asesoría.*

En la revista Fraudes Financieros[303], brindan consejos de cómo evitar el Carding, en los que recomienda instalar un buen *antivirus*[304] en las computadoras y en los dispositivos móviles, no dar clic o abrir vínculos sospechosos, y descargas aplicaciones por medio de las tiendas y desarrolladores oficiales. Además, menciona como evitar algunas de las técnicas descritas en el capítulo primero de la presente investigación, algunas de las recomendaciones son[305]:

- *Nunca entregar datos financieros por correo electrónico*
- *No dar clic en páginas sospechosas o responder mensajes engañosos*
- *En las compras por internet asegurarse que la dirección del sitio URL*[306] *comience con "https://"*[307]
- *Cuidarse de las páginas que ofrecen productos demasiado baratos, ya que puede tratarse de algún fraude.*
- *No utilizar computadoras o redes públicas al momento de realizar compras en línea.*
- *Monitorear las cuentas personales frecuentemente para evitar sorpresas y cambiar las contraseñas cada mes.*
- *Preguntar por el servicio de alertas*

---

[303] Ídem.

[304] Op. cit., 266.

[305] Ídem.

[306] URL son las siglas en inglés de *Uniform Resource Locator*, que en español significa Localizador Uniforme de Recursos. El URL es la dirección específica que se asigna a cada uno de los recursos disponibles en la red. Fuente: significados, *Qué es URL,* consultable en: https://www.significados.com/url/, consultado el 26 de noviembre de 2019.

[307] Op. cit., 302.

3.2.4. Procuraduría Federal de Protección al Consumidor

Existen tarjetas bancarias y departamentales o no bancarias, en estas últimas es una relación directa entre la entidad y el usuario. La PROFECO[308] es la encargada de promover y proteger los derechos y cultura del consumidor y procurar la equidad y seguridad en las relaciones entre proveedores y consumidores.

La PROFECO[309] ha brindado consejos de seguridad para evitar los ciberfraudes, los cuales son:

1. *Utiliza wi-fi[310] o conexión a internet segura*
2. *Instala en la computadora o en el dispositivo móvil una solución integral de seguridad y mantenla actualizada.*
3. *Compra en sitios web[311] conocidos y revisa la opinión de otros usuarios respecto a su experiencia de compra.*
4. *La navegación segura inicia con la certeza de que estamos en el sitio deseado. Evita los enlaces de correos y anuncios de publicidad.*
5. *Lee cuidadosamente las políticas de privacidad, devoluciones, reembolsos y cancelaciones.*

---

[308] Estados Unidos Mexicanos, *Ley Federal de Protección al Consumidor,* Diario Oficial de la Federación, 24 de diciembre de 1992, última reforma publicada el 09 abril de 2012, consultable en: https://www.profeco.gob.mx/juridico/pdf/l_lfpc_ultimo_CamDip.pdf, consultado el 22 de junio de 2019

[309] Procuraduría Federal del Consumidor, *Consejos de seguridad para evitar el fraude cibernético*, consultable en: https://www.facebook.com/216423475165030/posts/1368153146658718/?app=fbl, consultado el 22 de julio de 2019.

[310] Wifi o Wi-Fi es originalmente una abreviación de la marca comercial Wireless Fidelity, que en inglés significa “fidelidad sin cables o inalámbrica”. Wifi es una tecnología de comunicación inalámbrica que permite conectar a internet equipos electrónicos. Fuente: significados, *significado de Wifi*, consultable en: https://www.significados.com/wifi/, consultado el 26 de noviembre de 2019.

[311] Op. cit., 16.

Además de que la PROFECO creo una red de monitoreo de tiendas virtuales[312], en la que *permite a los consumidores revisar si los sitios de los proveedores que realizan transacciones a través del comercio digital cumplen con las disposiciones contenidas en la Ley Federal de Protección al Consumidor.*

La PROFECO[313] busca con esta herramienta brindar certeza y seguridad a los consumidores, brindando información antes de realizar una transacción electrónica.

3.3. Disposiciones de las entidades emisoras.

La institución de crédito o la entidad emisora toman un papel fundamental en la prevención de las conductas que forman el Carding.

Algunas de las medidas para combatir las conductas tradicionales referentes a tarjetas son[314], en primer lugar, la entrega de la tarjeta por parte de la entidad emisora de una forma segura, en segundo lugar, la entidad emisora se obliga a poner a disposición de los usuarios canales de comunicación, adecuados y permanentes, que permitan a estos comunicarle el robo, extravió u otras situaciones de riesgo para la tarjeta de crédito. Recibida la notificación indicada, la entidad emisora debe bloquear de manera posible el uso de la tarjeta, comunicándolo dicha situación a los establecimientos adheridos.

Otra medida tradicional[315] es la verificación de la regularidad de los pagos efectuados con esta, posteriormente la entidad emisora debe enviar un extracto de las operaciones efectuadas con la tarjeta del usuario. Por último, la entidad emisora está obligada a conservar los documentos justificantes, de las operaciones de pago realizadas con la tarjeta.

---

312 Procuraduría Federal del Consumidor, *Monitoreo de Tiendas* Virtuales, disponible en: https://www.profeco.gob.mx/tiendasvirtuales/index.html

313 Ídem.

314 Mariño, Andrés, “Uso fraudulento de tarjetas… “, Op. cit., p.29.

315 Ibídem, p.30.

La recomendación 88/4590/CE[316] de 17 de noviembre de 1988, expresa en el punto 5 de su anexo, que el emisor no encuadra ningún instrumento de pago a un cliente a menos de que lo haya solicitado. Además, en el artículo 4.3 el emisor no podrá revelar frente al titular el *NIP*[317]. En el artículo 6.1 del anexo señala la obligación de la entidad emisora de llevar registros internos detallados. En el artículo 6.2 impone la carga probatoria al emisor. En el artículo 8.1 establece la obligación del emisor de facilitar los medios por los cuales sus clientes puedan notificar la pérdida, robo o falsificación de sus instrumentos de pago.

En la recomendación 97/489/CE[318] de 30 de julio de 1997 establece en el artículo 7.2 que el emisor a) no revelará el *NIP*[319] del titular u otro código, excepto al propio titular, b) no enviara un instrumento electrónico de pago no solicitado, excepto cuando se trate de la reposición de un instrumento electrónico ya poseído por el titular y c) garantizará la existencia de medios adecuados para permitir al titular efectuar la notificación necesaria en caso de robo o pérdida de su instrumento.

La posición de todos los Bancos frente al Carding es de una posición cerrada, no se pronuncian al respecto, debido a que impacta negativamente a la institución, ergo, los bancos en general han tomado medidas como.

- Creación de *Wallet*, o monederos electrónicos[320], en los se encuentra el manejo de una tarjeta digital, está se crea a partir de una tarjeta física, que puede ser de débito o crédito, con la peculiar característica que cuenta con un número y un vencimiento diferente al de la tarjeta física, pero con las mismas características de saldos y líneas de crédito, además

[316] European noviembre de *1988.*Commission, *Recomendación de la comisión de 17 de noviembre de 1988 relativa a los sistemas de pago y en particular a las relaciones entre titulares y emisores de tarjeas,* Diario Oficial de las Comunidades Europeas, 17 de

[317] Op. cit., 41.

[318] Unión europea. *Recomendación de la Comisión (97/489/CE) relativa a las transacciones efectuadas mediante instrumentos electrónicos de pago, en particular, las relaciones entre emisores y titulares de y tales instrumentos,* Unión europea, 30 de julio de 1997.

[319] Op. cit., 41.

[320] Reyna, Armando, *¿Qué es una tarjeta digital y cómo se usa?,* 2018, consultable en: https://www.bbva.com/es/tarjeta-digital-usa/, consultado el 13 de agosto de 2019.

de sirve para hacer compras seguras por internet con códigos se seguridad únicos.

- Sistema de alertas y notificaciones al momento se realizarse una compra
- Límite diario de gastos a las tarjetas de débito o crédito.
- Apagar temporalmente las tarjetas para mantenerlas seguras cuando no las utilices, y tener la oportunidad de encenderlas inmediatamente.
- Bloquear las tarjetas por robo o extravió por medio de la aplicación de las referidas instituciones.
- Pagar desde el celular en comercios adheridos sin tener que llevar la tarjeta física por medio.

Para fines de esta investigación el investigador y tesista solicitó una entrevista con los encargados regionales en el Estado de Puebla de las Unidades Especializadas de las Instituciones Emisoras, bajo una metodología específica, en la que se escogerían las primeras diez entidades emisoras conforme al historial de reclamaciones de usuarios financieros desde el 2015 al 2018, presentadas ante las propias instituciones financieras por reclamaciones en materia de comercio por internet, para conocer la posición de las instituciones financieras respecto de la impunidad del Carding en el Estado de Puebla, sin embargo, fue una posición cerrada de su parte, sin compartir nada respecto del tema.

3.4. Medidas por el establecimiento adherido.

El establecimiento adherido en las conductas tradicionales es a quien se le presenta la tarjeta y quien acepta a esta como instrumento de pago. Como medida de prevención del uso fraudulento asume el deber de verificar los datos subjetivos y objetos de la tarjeta de crédito, esto es, como menciona el autor Andrés Mariño[321] verificar los datos subjetivos y objetivos de la tarjeta de crédito, esto es, por una parte, comprobar la identidad del titular y la coincidencia del pago.

[321] Mariño, Andrés, “Uso fraudulento de tarjetas… “, Op. cit., p. 30.

Así mismo han optado por mecanismos internos para corroborar los datos subjetivos de la compra, en la que solicitan al comprador que envíe algunos documentos escaneados como pueden ser una identificación oficial, copia de un estado de cuenta, copia de registro federal del contribuyente, etc. Sin embargo, no ha sido una medida suficiente para frenar el Carding.

En el capítulo primero se escribió que dentro de las asociaciones delictivas del Carding, existen miembros que se dedican a falsificar los documentos que piden los establecimientos para confirmar la compra, por lo que no esta medida no es una opción cien por ciento efectiva.

Los establecimientos adheridos cuentan con analistas de fraudes que se encargan de investigar y prevenir los posibles cargos fraudes que se hagan en relación a tarjetas bancarias. Sin embargo, así como previenen algunos cargos fraudulentos, también cancelan compras auténticas de clientes que realmente deseen comprar con ellos, generando una mala coordinación de cliente-negocio.

3.5. Medidas de los procesadores de pago

3.5.1. *Payment Application Data Security Standard* (PA-DSS).[322]

Define los controles necesarios[323] a ser implementados antes, durante y después del desarrollo de aplicaciones licenciadas por parte de terceros que procesen el *PAN*[324].

Los requisitos de las *PA-DSS*[325] (normas de seguridad de datos para las aplicaciones de pago) y los procedimientos de evaluación de seguridad de la *PCI*[326] (industria de tarjetas de pago) definen los requisitos de seguridad y los

[322] PA-DSS o Payment Application Data Security Standard significa en español Estándar de seguridad de datos de la aplicación de pago.

[323] Security Standars Council, "*Industria de tarjetas de pago (PCI)…", Op. cit.,*

[324] Op. cit., 14.

[325] Op. cit., 322.

[326] Op. cit., 18.

procedimientos de evaluación de los proveedores de *software*[327] de aplicaciones de pago.

La *PCI DSS* [328]se aplica a todas las entidades que participan en el procesamiento de las tarjetas de pago[329], entre las que se incluyen comerciantes, procesadores, adquirentes, entidades emisoras y proveedores de servicios.

Las *PA-DSS*[330] se aplican a proveedores de *software*[331] y a otros que desarrollan aplicaciones de pago y que almacenan, procesan o transmiten datos del titular de la tarjeta o datos de autenticación confidenciales.

El *PA-DSS*[332] minimiza las vulnerabilidades en las aplicaciones de pago. El objetivo es evitar que se comprometan los datos completos de la banda magnética ubicados en el reverso de una tarjeta de pago o datos equivalentes de un *chip*[333]. Comerciantes y proveedores de servicios. deben usar aplicaciones de pago certificadas y deben consultar con su institución financiera adquirente para comprender los requisitos y los plazos asociados para el cumplimiento[334]

Está compuesto por 14 puntos[335]:

[327] Op. cit., 5.

[328] Op. cit., 18.

[329] Ídem.

[330] Security Standars Council, "*Industria de tarjetas de pago (PCI)…", Op. cit.,*

[331] Op. cit., 5.

[332] Security Standars Council, "*Industria de tarjetas de pago (PCI)…", Op. cit.,*

[333] Op. cit., 210.

[334] Security Standars Council, *Industria de tarjetas de pago (PCI) Norma de seguridad de datos para las aplicaciones de pago. Requisitos y procedimientos de evaluación de seguridad*, consultable en: https://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs/PA-DSS_v3-2_es-LA.pdf consultado el 30 de abril de 2019.

[335] *Ídem.*

1. *No retener la banda magnética completa, tarjeta, código de verificación o valor, o datos de bloqueo de PIN[336].*
2. *Proteger los datos almacenados del titular de la tarjeta.*
3. *Proporcionar características de autenticación segura*
4. *Registrar actividad de aplicación de pago*
5. *Desarrollar aplicaciones de pago seguras*
6. *Proteger transmisiones inalámbricas*
7. *Probar las aplicaciones de pago para hacer frente a las vulnerabilidades*
8. *Facilitar la implementación segura de la red.*
9. *Los datos del titular de la tarjeta nunca deben almacenarse en un servidor conectado a Internet*
10. *Facilitar el acceso remoto seguro a la aplicación de pago*
11. *Cifrar el tráfico sensible a través de redes públicas*
12. *Cifrar todos los accesos administrativos que no sean de consola.*
13. *Mantener documentación instructiva y programas de capacitación para clientes, revendedores e integradores.*
14. *Mantener documentación instructiva y programas de capacitación para clientes, revendedores e integradores.*

[336] *PIN* por sus siglas en inglés, *Personal Identification Number* que significa número de identificación personal. Fuente: *¿Qué es PIN?*, consultable en: https://es.ccm.net/faq/10682-que-es-el-pin, consultado el 27 de noviembre de 2019.

3.5.2. 3D Secure[337], Verified by Visa[338]-SecureCode[339].

La CONDUSEF[340] expresa que es un procedimiento de seguridad que permite una mejor identificación del tarjetahabiente en las compras de sitios de comercio electrónico. Además de los datos necesarios para comprar en línea (nombre, *PAN*[341], fecha de vencimiento y código de seguridad) este sistema de pago requiere de la contraseña que se generó a través de aplicaciones provistas por el emisor de la tarjeta. Una vez proporcionada la contraseña el banco emisor valida que corresponda con los registros de generación correspondientes.

El sistema de *VISA[342]* se conoce como "*Verifiel by Visa*"[343] mientas que el de *Mastercard[344]* como "*SecureCode*[345]"; es indispensable que el comercio electrónico donde se realice la compra esté afiliado al servicio (a través de su banco adquirente) para poderlo utilizar durante el proceso de pago con tarjeta.

---

[337] *3D Secure* significa seguridad 3D, Es forma de pago desarrollada por *Visa* y *Mastercard* que posibilita la realización de compras seguras en Internet y autentifica al comprador como legítimo titular de la tarjeta que está utilizando. Fuente: tpvcenter, *¿Qué es 3D Secure?,* consultable en: https://www.tpvcenter.com/3DSecure.htm, consultado el 26 de noviembre de 2019.

[338] Op. cit., 183.

[339] *Verified by Visa-SecureCode* significa verificado por visa, código seguro, y son servicios de seguridad para proteger contra el uso no autorizado de la tarjeta mientras el usuario compra o realiza pagos en línea con los comercios participantes en esta modalidad. Fuente. Multipagos, *¿Que es Verified by Visa y MasterCard SecureCode?,* consultable en*:* https://www.multipagos.com.mx/eEmpresa/utils/3DSecure/3DSecure.html, consultado el 26 de noviembre de 2019.

[340] Comisión Nacional para la Protección y Defensa de los Usuarios de los Servicios Financieros, *medidas de seguridad,* consultable en: https://www.condusef.gob.mx/gbmx/?p=medidas-de-seguridad, consultado el 23 de junio de 2019.

[341] Op. cit., 14.

[342] Op. cit., 183.

[343] Ídem.

[344] Op. cit., 184.

[345] Op. cit., 339.

3.6. Medidas de los Usuarios

Escribe Andrés Mariño[346] que el titular de la tarjeta de crédito debe custodiar y conservar en forma adecuada dicho instrumento y, en caso, el *NIP*[347] que se le ha asignado.

Cuando el titular de la tarjeta adquiera conocimiento del extravió o robo de esta o de otra situación de riesgo de uso fraudulento debe notificar en forma inmediata a la entidad emisora.

La recomendación 87/598/CE[348] diciembre de 1987 establece en el apartado lV art. 2 que el titular de la tarjeta de crédito adoptará las precauciones razonables para garantizar la seguridad de la tarjeta emitida y observará las condiciones específicas del contrato que hubiera firmado.

La recomendación 88/590/CE[349] de 17 de febrero de 1988, relativa a los sistemas de pago, y en particular, a las relaciones entre titulares y funcionamiento y uso fraudulento de tarjetas de crédito.

Otra obligación del titular es verificar, en el extracto enviado por la entidad emisora, la regularidad de las operaciones realizadas con la tarjeta. En el art. 5.b)[350] preceptúa que el titular de la tarjeta notificará a la entidad emisora en forma inmediata a su conocimiento de los registros en su cuenta de cualquier transacción no autorizada y de cualquier error u otra anomalía en la gestión de su cuenta por parte del emisor.

---

[346] Mariño, Andrés, "Uso fraudulento de tarjetas… ", Op. cit., p.24.

[347] Op. cit., 41.

[348] Comisión de las Unidades Europeas, recomendación 87/598/CE, Comunidad Europea, 30 de diciembre de 1997.

[349] Unión Europea, *Recomendación 88/590/CE de la Comisión de 17 de noviembre de 1988, (DOCE de 24 de noviembre L 317), relativa a los sistemas de pago y en particular a las relaciones entre titulares y emisores de tarjetas de pago electrónico,* Unión Europea, 17 de noviembre de 1988.

[350] Ídem.

En la circular 34/2010[351] de Banco de México, menciona en el punto 2.3 bis que el adquiriente de una tarjeta deberá observar los estándares de seguridad y procesamientos establecidos por la empresa *EMVCo[352], LVV[353]*, y en el caso de que pretenda utilizar otro estándar distinto, deberá obtener previamente la autorización del Banco de México, *para lo cual deberá presentar la solicitud respectiva a la Gerencia de Autorizaciones, consultas y control de legalidad.*

Finalmente, el usuario, debido a los altos índices que provoca el Carding, y a la mala coordinación entre cliente-negocio, gran parte de la población ha optado por dejar de comprar en internet, y mejor comprar de manera física. Esto provoca que el sistema de pagos se comprometa, disminuyendo la movilidad económica y que el sistema financiero mexicano no se desarrolle.

3.7. Medidas de Facebook

Facebook como principal medio virtual para la enajenación de información o números de tarjetas bancarias tiene parcialmente la responsabilidad de contar con políticas para prevenir el Carding, por lo que cuenta con[354]:

1. Condiciones de servicio - Condiciones que se aceptan al usar Facebook,
2. Política de Datos. - Información que recibe Facebook, y la manera de cómo se gestiona.
3. Normas Comunitarias. - Qué está prohibido y cómo reportar abusos.

En el apartado “combatimos las conductas perjudiciales y protegemos y respaldamos a nuestra comunidad” Facebook[355] expresa que desarrolla sistemas técnicos avanzadas y que cuenta con equipos dedicados en todo el mundo para detectar si sus productos se usan de manera inapropiadas, añade

---

[351] Banco de México, “*Circular 34/2010”,* Op. cit., p. 4.

[352] Op. cit., 211.

[353] Op. cit., 212.

[354] Facebook, *Condiciones y Políticas de Privacidad*, consultable en https://www.facebook.com/policies, consultado el 21 de junio de 2019.

[355] Facebook., *Condiciones de servicio*, consultable en: https://www.facebook.com/legal/terms consultado el 21 de junio de 2019.

que hay conductas delictivas hacia los demás y que surgen situaciones en las que puede contribuir para respaldar o proteger a la comunidad de la red social.

Al tomar conocimiento Facebook[356] sobre contenido o conductas dañinas, aplicará las medidas correspondientes, por ejemplo, ofrecer ayuda, eliminar contenido, bloquear el acceso a ciertas funciones, inhabilitar una cuenta o comunicarse con las fuerzas del orden.

En las mismas condiciones de servicio, en el apartado 2. "*Que contenido puedes compartir y que actividades puedes realizar en Facebook*" describe que no puedes usar sus productos para realizar actividades o compartir contenido que sean ilegales, engañosos, fraudulentas o subir virus, con lo que regularía al Carding en cuanto a algunas técnicas de obtención, y sobre la comercialización de números de tarjetas. En caso de que se adopte estas conductas delictivas, Facebook puede eliminar el contenido que incumpla con estas disposiciones e inhabilitar la cuenta del que lo haya realizado.

Facebook[357] expresa que se esfuerza por proporcionar los mejores productores posibles y definir pautas claras, no obstante, no garantizan que sus productos siempre sean seguros, y que no son responsables de las acciones que las personas u otros hacen o dicen, por sus acciones, o conductas, ni por el contenido que comparten. Expresa que su responsabilidad se limita al máximo alcance que la ley aplicable permita, y que de ninguna circunstancia serán responsables por daños consecuentes, punitivas o de cualquier otra índole.

En la política de datos, Facebook[358] expresa que recopila información sobre transacciones realizadas en sus productos, por ejemplo, cuando se realiza una compra en un juego o en una donación, recopila la información de pago, como el número de tarjeta de crédito o débito y otra información sobre la tarjeta.

---

[356] Ídem.

[357] Ídem.

[358] Facebook, *Política de datos,* consultable en: https://www.facebook.com/about/privacy consultado el 21 de junio de 2019

3.7.1. Facebook colaborador de investigadores y académicos

Facebook[359] brinda la oportunidad de ofrecer información y contenido a investigadores y académicos para que se puedan realizar investigaciones con el objetico de profundizar los conocimientos y la innovación que respalden a su negocio, o que refuercen el descubrimiento y la innovación sobre temas con el bienestar social general, los avances tecnológicos, el interés, la salud y el bienestar público.

3.7.2. Facebook y solicitudes legales.

Facebook menciona que, en respuesta a un requerimiento legal, como puede ser una orden de registro, una orden judicial o una citación, podrán acceder a la información personal de la cuenta y compartirla con organismos reguladores o autoridades.

Los requerimientos legales pueden ser ajenos a la jurisdicción de estados Unidos si a juicio de Facebook son de buena fe, cuando es necesario para detectar, impedir y abordar casos de fraude, usos no autorizados de los productos, incumplimientos de las condiciones o las políticas aplicables, así como otras actividades perjudiciales o ilegales.

Finalmente, en las normas comunitarias[360] se describen que está permitido o no en Facebook, mismas que se aplican en todo el mundo y a todos los tipos de contenido. Tienen como finalidad fomentar que las personas que integran Facebook se expresen y creen un entorno seguro, rigiéndose bajo los principios de seguridad, voz, y equidad.

Facebook[361] prohíbe entre otras, las actividades delictivas, eliminando el contenido que aporte o elogie a grupos, lideres o personas implicadas en estas

---

[359] Ídem.

[360] Facebook, *Normas Comunitarias*, consultable en: https://www.facebook.com/communitystandards/, consultado el 21 de junio de 2019.

[361] Ídem.

actividades. Además de que prohíbe promocionar o anunciar fraudes, como es el caso de la enajenación de números de tarjetas bancarias.

3.8. Análisis de datos a nivel Federal

El total de las reclamaciones de consumos no reconocidos vía internet presentadas ante la CONDUSEF[362] en 2015 fueron un total de 1,029, y ante la propia Institución Bancaria 678,993. En el 2016 se registraron ante CONDUSEF1,495 reclamaciones y ante la institución bancaria 1,650,777. En el 2017 se presentaron ante CONDUSEF un total de 1,349 ante la institución 3,264,105. En 2018 se registraron un total de 1,601, por su parte las reclamaciones de comercio por internet presentadas ante la propia institución bancaria fueron de 4,154,415.

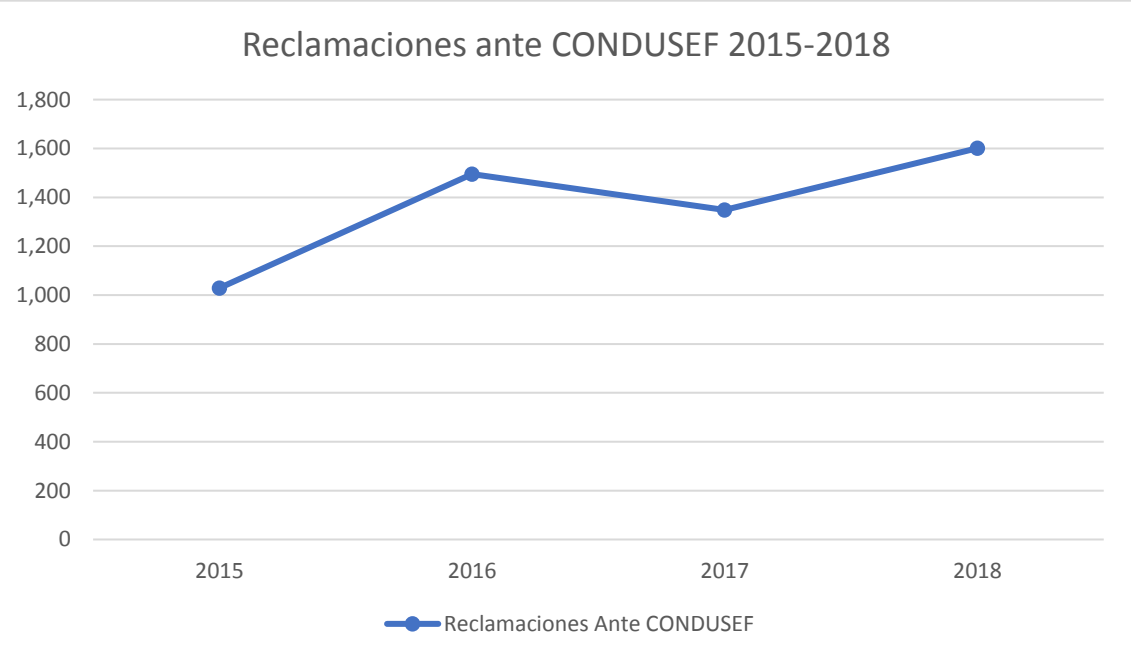

***Tabla 3**. Reclamaciones ante CONDUSEF 2015-2018 de conductas delictivas contra tarjetas bancarias.*

[362] Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, *estadísticas, 2019,* consultable en*:* https://www.condusef.gob.mx/gbmx/?p=estadisticas consultado el 23 de junio de 2019.

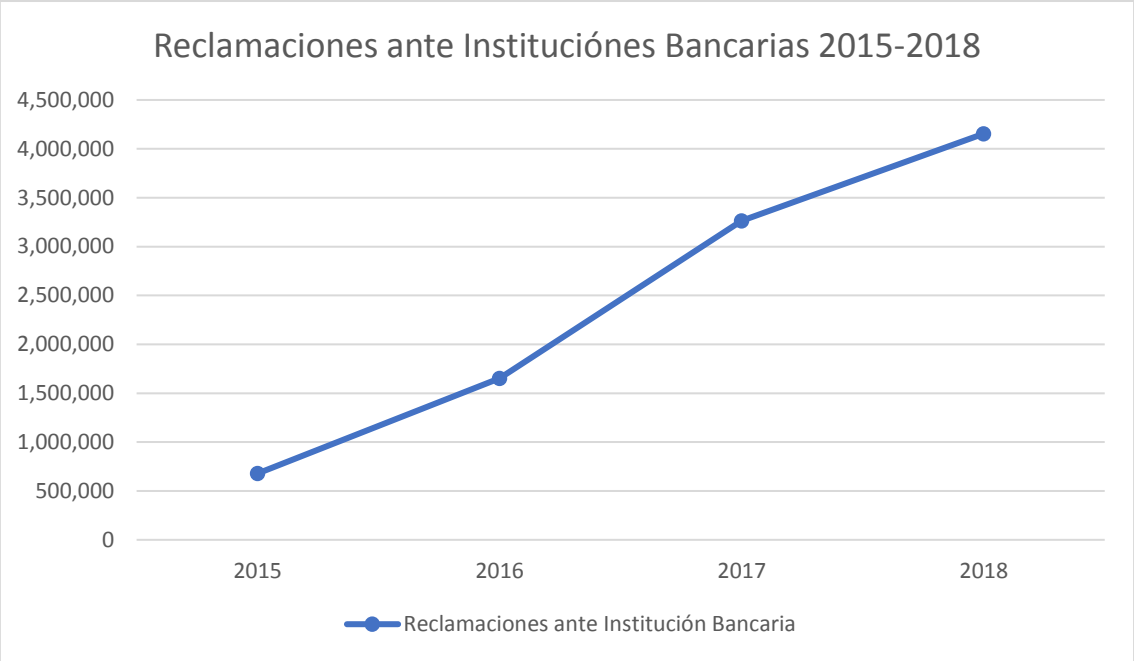

***Tabla 4**. Reclamaciones ante Instituciones Bancarias 2015-2018.*

En 2013 la CONSUSEF[363] reportó un total de 2,949,049 fraudes, de los cuales los cibernéticos[364] suman 359,274 frente a 2,579,769 de fraudes tradicionales. Para el 2014 el total de los fraudes fue de 2,890,693 del que 490,631 eran fraudes cibernéticos, frente a 2,396,672 por fraudes tradicionales. En el 2015 existieron un total de 3,922,913 fraudes, de los cuales 790,936 representan fraudes cibernéticos frente a un total por cargos tradicionales por 3,131,666. Para el 2016 se reportaron un total de 5,297,588 de fraudes, de los cuales 1,765,654 representó los fraudes cibernéticos frente a 3,525,246 de fraudes tradicionales. En el 2017 hubo un total de 6,605,074 de fraudes, con un total de 3,443,605 de fraudes cibernéticos frente a 3,134,353 de fraudes tradicionales. En el 2018, existieron 7,300,575 fraudes, de los cuales 4,313,844 son de fraudes cibernéticos en contra de 2,961,218 de fraudes tradicionales.

[363] Ídem,

[364] En el capítulo 1 del presente trabajo se realizó la aclaración respecto a la terminología adecuada para referirse a estas conductas, sin embargo, para no alterar lo mencionado por la CONDUSEF se dejó el término de “cibernéticos”, ergo lo correcto sería ciberfraudes.

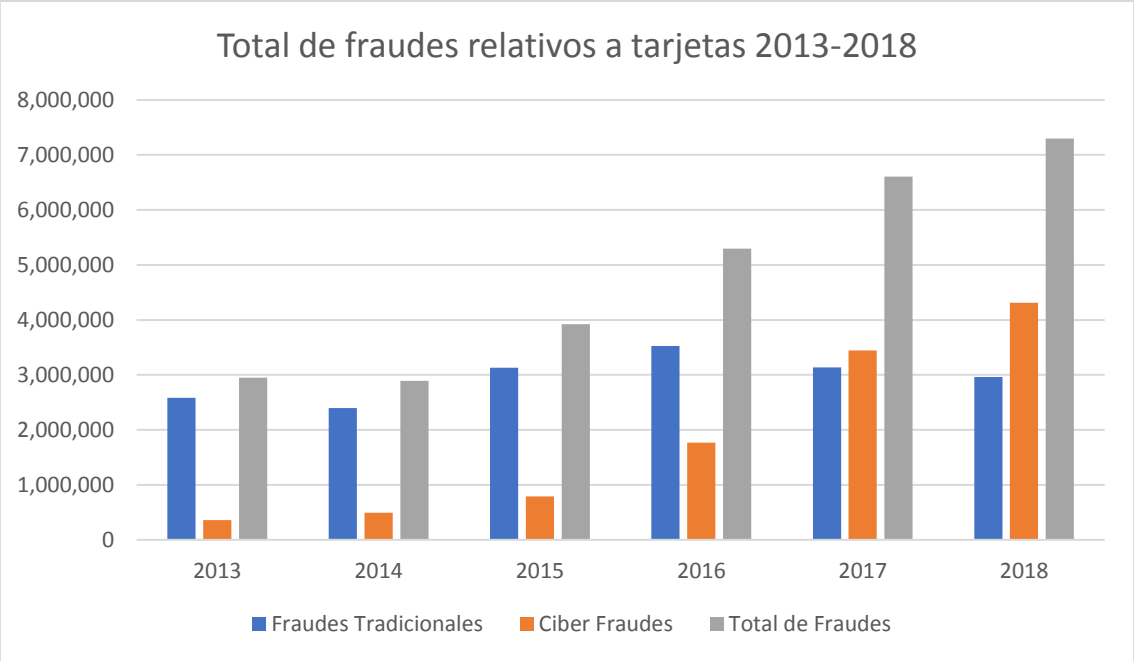

***Tabla 5**. Total de fraudes relativos a tarjetas bancarias 2013-2018.*

En 2017 por primera vez los ciberfraudes superaron en cantidad a los fraudes tradicionales.

En 2015 la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros reportó contracargos[365] por $129,720,000.00 (ciento veintinueve millones setecientos veinte mil pesos), para el 2016 incremento a la cantidad de $266,640,000.00 (doscientos sesenta y seis millones, seiscientos cuarenta mil pesos), incrementando un 105.55% (ciento cinco punto cincuenta y cinco por ciento) respecto del año pasado; en cuanto al 2017 se registraron $1,084,900,000.00 (un billón ochenta y cuatro millones, novecientos mil pesos) incrementando 306.88% (trescientos seis punto ocho por ciento) respecto del año pasado, denotando una cuantiosa pérdida económica para las entidades financieras. En el 2018 se registraron $1,761,000,000.00 (un billón, setecientos sesenta y uno millones de pesos).

[365] Un contracargo es un mecanismo creado para solucionar aquellos cargos que se realizan a una tarjeta de crédito o débito que no son reconocidos. Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, "*estadísticas" Op. cit.,*

***Tabla 6**. Contracargos 2015-2018.*

No existen estadísticas específicas de cuantos delitos se cometieron específicamente de los artículos que encuadran al Carding, sin embargo, se tomará el máximo de delitos de la misma clasificación hecha por Secretariado Ejecutivo del Sistema de Seguridad Pública, como punto de referencia para el análisis. Se entiende por incidencia delictiva[366]. al número de delitos registrados por el agente del ministerio Público referentes a los presuntos delitos registrados en averiguaciones previas o carpetas de investigación iniciadas.

En delitos de leyes de crédito, inversión, finanzas y seguros, en el 2013 se registraron un total[367] a nivel federal de 4,241, y en Puebla únicamente 32 casos; para el 2014 se registraron 2,563 casos a nivel federal y para puebla sólo 14; en el 2015 se reportaron 3,269 casos, y a nivel local 41; para el 2016 se registraron

[366] Gobierno de México, *incidencia delictiva, 2019,* consultable en. https://www.gob.mx/sesnsp/acciones-y-programas/preguntas-frecuentes-repuve-incidencia-delictiva-rnped-emergencias-066?idiom=es, consultado el 24 de junio de 2019.

[367] Centro Nacional de Información, *reporte de incidencia delictiva del fuero federal por entidad federativa 2012 – 2019, consultable en:* https://drive.google.com/file/d/11jAkigPtlWaq7jtW9bazByachs7fYXAE/view, consultado el 24 de junio de 2019.

4,316, y en Puebla 16; en el 2017 existieron 8,099 casos a nivel federal y 24 a nivel local y para el 2018 10,221 y a nivel local sólo 19.

Al comparar el número total de reportes de fraudes tradicionales y ciberfraudes por la CONDUSEF del 2013 al 2018, con las estadísticas de incidencia delictiva realizadas por el Secretariado Ejecutivo del Sistema de Seguridad Pública se denota una gran diferencia:

Año	ESTADÍSTICAS CONDUSEF	INCIDENCIA DELICTIVA FEDERAL
2013	2,949,049	4,241
2014	2,890,693	2,563
2015	3,922,913	3,269
2016	5,297,588	4,316
2017	6,605,074	8,099
2018	7,300,575	10,221

***Tabla 7**. Comparación incidencia delictiva de CONDUSEF con incidencia delictiva federal*

A pesar de tomar el número máximo de casos dentro de la clásificación de delitos de leyes de crédito, inversión, finanzas y seguros, clasificación hecha por el Secretariado Ejecutivo del Sistema de Seguridad Pública[368], existe una enorme diferencia en ambas columnas. Miles de reportes ante una autoridad administrativa, muy pocos ante la materia Penal.

3.9. Nivel Local

Para fines de esta investigación se solicitó las *estadísticas y datos sobre reclamaciones o quejas en materia de consumos no reconocidos vía internet presentadas ante la propia institución bancaria y ante CONDUSEF, respecto de*

[368] Gobierno de México, "*incidencia delictiva", Op. cit.,*

ciberfraudes a tarjetas bancarias, del periodo de enero de 2015 al 31 de mayo de 2019 en el Estado de Puebla. Además del Monto reclamado concluido, y el monto abonado ante la unidad de transparencia de la Comisión Nacional para la Protección y Defensa de los Usuarios de los Servicios Financieros, mediante número de folio 063700020919.

En el 2015 se reportaron se reportan un total de 6,327 reclamaciones imputables a posible ciberfraudes o al fenómeno del Carding; para el 2016 incrementó a la cantidad de 7,178 reclamaciones; para el 2017 se registraron 20,169 reclamaciones; en el 2018 se reportaron 48,054.

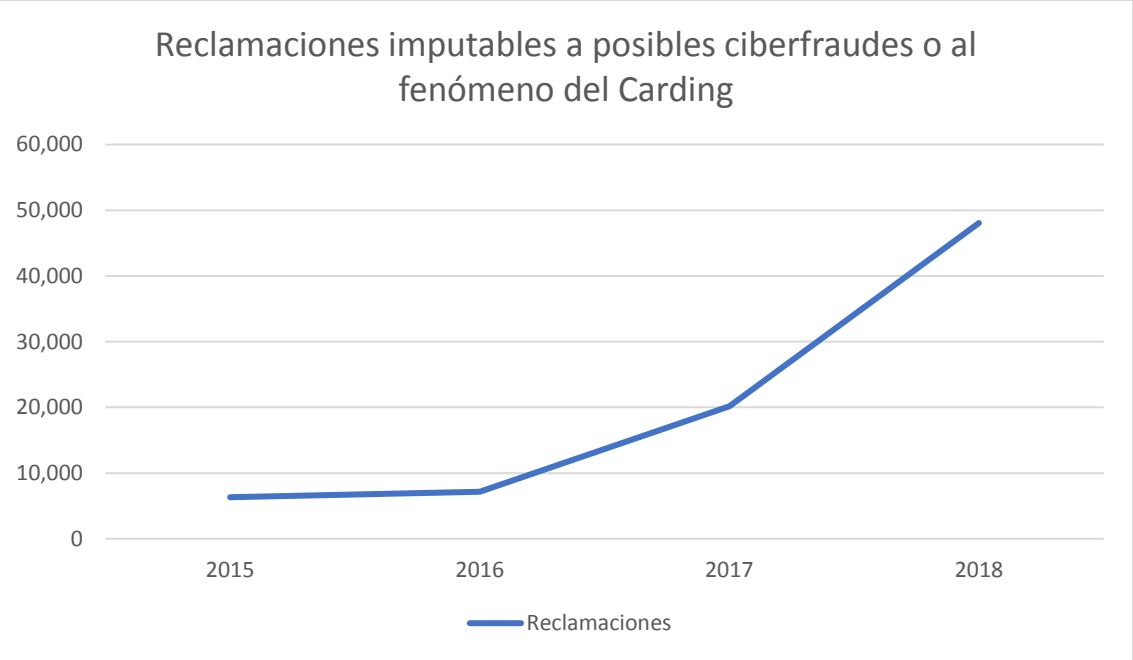

Tabla 8. *Reclamaciones imputables a posibles ciberfraudes o al fenómeno del Carding.*

En el 2015 en el Estado de Puebla, con información de la solicitud 063700020919 ante la Comisión Nacional para la Protección y Defensa de los Usuarios de los Servicios Financieros, el monto reclamado fue $18,179,692.00 de pesos por concepto de reclamaciones imputables a posibles ciberfraudes o al fenómeno del Carding; en el 2016 el monto reclamado fue de $20,385,091.00; para en el 2017 el monto reclamado fue $39,833,663.00, y para el 2018 incrementó a la cantidad de $89,458,315.00

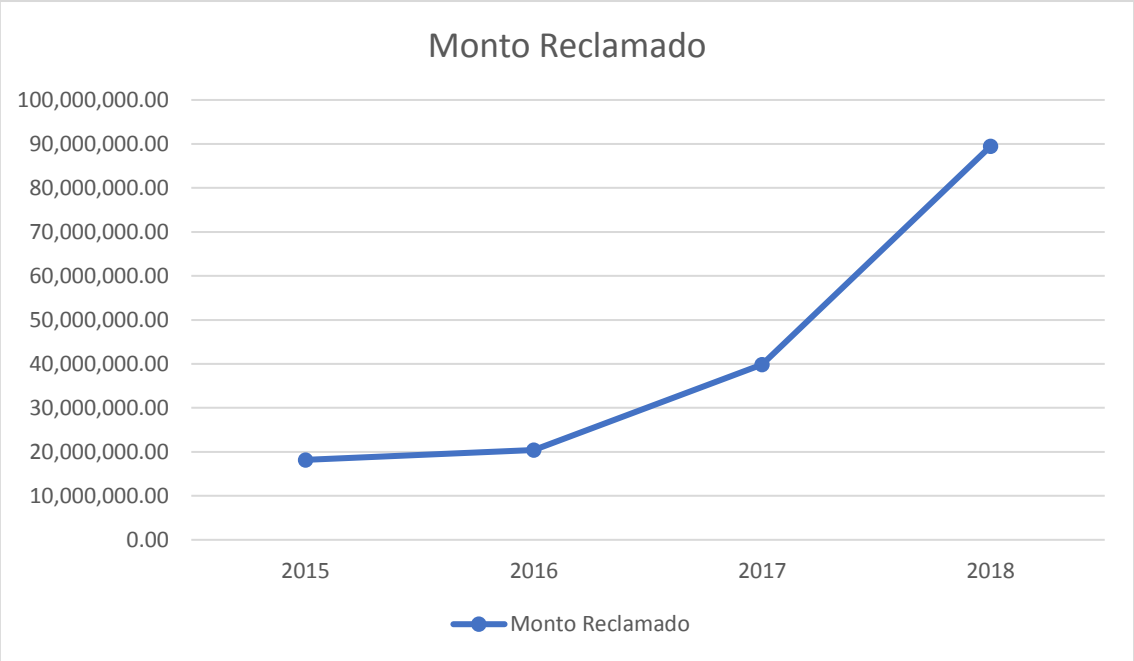

Tabla 9. *Monto Reclamado.*

CONCLUSIONES

La finalidad de esta tesis ha sido investigar y analizar bajo una visión fenomenológica, la relación entre la operatividad de los actuales delitos ciberfinancieros denominados Carding y BINS, la impunidad de los mismos a nivel federal y en el Estado de Puebla, lo que provoca inseguridad jurídica en el sistema bancario mexicano y una enorme pérdida económica.

Por lo que fue indispensable un estudio exploratorio de tipo longitudinal, es decir, un estudio de tipo observacional, en el que se analizó y estudió el fenómeno del Carding y BINS entre el 2015 y 2019 para conocer su operatividad y determinar factores para su investigación, prevención y combate.

En primer lugar, fue importante adentrarse en el fenómeno para observarlo sin alterar ningún factor o elemento del mismo dentro del cibermercado azul mismo que se explicó en el capítulo 1 y 2 de la presente investigación en el que se mencionó que *ciber* no es utilizado como prefijo de la ciencia denominada cibernética, puesto que su área de estudio no tiene relación con la informática o telemática sino más bien que es un elemento compositivo y que este elemento sí indica relación con redes informáticas, con el que se forman palabras compuestas anteponiéndose a otras, por lo que al referirnos a un *ciber*mercado hablamos de un mercado en internet, y el adjetivo de azul hace referencia al principal medio de intercambio que es la red social denominada Facebook.

Los primeras observaciones se hicieron respecto a los BINS; existía mucha confusión en que era, puesto que formalmente significa *número de identificación bancaria,* sin embargo, para el fenómeno estudiado era completamente otra cosa, los BINS es la serie de números base de una tarjeta para la generación y producción en serie de la misma, un ejemplo de un BIN es: 543924xxxxxxxxxx, todo este conjunto de información era procesado por programas informáticos o telemáticos de manera inteligente apoyándose de diferentes algoritmos de comprobación, el más común es el algoritmo de *luhn* que sirve para validad que los números creados sean técnicamente correctos y no sea una generación al azar.

Se observó que las formaciones de los *BINS* eran ocupados por los cuatro primero niveles de la clasificación de *bineros y carders*, es decir, por el nivel 1 que es el “curioso”, aquella persona que busca información del fenómeno ocupando las sobras del conjunto de datos de los demás niveles sin ánimo de encontrar más *BINS*, donde su nivel de éxito es prácticamente nulo; el nivel 2 “aprendiz” al igual que el curioso copia los *BINS* que sobran de los demás niveles con la única diferencia de que estos son más activos y buscan un tutor que les enseñe cual es la operatividad de este subfenómeno; en tercer lugar encontramos al “binero pasivo” que al igual que los anteriores se basa únicamente en copiar los BINS utilizados por los de nivel superior y en este rango ya logran tener éxito en compras de bienes y servicios de muy bajo costo; por último encontramos al “binero activo” que en este rango ya saben extrapolar una tarjeta, es decir, crear sus propios BINS, además de que comercializan en el cibermercado azul con los niveles inferiores y se empiezan a posicionar en el *carding*.

Después de observar el fenómeno de los BINS se estudió a profundidad el fenómeno de donde partía los BINS, es decir, el Carding, que es la producción, obtención, administración, comercialización y uso indebido de números o información de tarjetas bancarias. Se analizó la diferencia entre los delitos tradicionales con tarjetas y el carding determinándose que en el carding existen tres elementos que hacen que se distingan del resto, el primero de ellos es que no es presencial, es decir que hace uso de la telemática, informática o medios electrónicos para cometer las conductas delictivas del carding; el segundo elemento es que debe estar presente las nuevas tecnologías como medio de comisión del delito, es decir la informática, o telemática; y finalmente el tercer elemento es que el objeto material de la acción del carding son la información o los números contenidos en la tarjeta *per se* y no el plástico, aunque pareciera igual se estudió que no son lo mismo y es importante denotar la diferencia para comprender el fenómeno.

La tercer conducta más utilizada es la obtención de números o información de tarjetas bancarias, se expuso, que existen diversas técnicas que se han generado desde principios de la década pasada debido a la evolución de las tecnologías y los sistemas de la información, tal y como se detalló en el cuerpo

de la presente investigación, donde, se explicó que en un principio, la técnica más popular es la denominada *SQL injector-dumper,* mediante la cual, los cibercriminales adentran de manera remota los servidores con deficiencias informáticas y copian las tablas de información en las que se podía estar albergado información de números de tarjetas bancarias.

Posteriormente se estudió la fuga de datos, que es una variedad del espionaje industrial, en el que se sustrae información confidencial de una empresa; la ingeniería social, es engañar a las personas para que compartan información confidencial; la fuerza bruta que es un proceso sistematizado para encontrar posibles números de tarjetas bancarias probando uno por uno; el *spam-phishing*, en el que envían correos masivos basura con la intención de hacerse pasar por alguna empresa o institución pidiendo información confidencialidad; *pharming* que es cuando instalas un programa y este te redirecciona a un sitio *web* fraudulento, con la intención de sustraer información confidencial; los *keyloggers,* registran las pulsaciones de un teclado utilizado en sitios públicos; el robo de credenciales que se utiliza sustrayendo datos confidenciales en páginas *web* de la víctima; *sniffing* que es espiar el tráfico de datos de una red inalámbrica mediante la tecnología *wifi*; los *skimmer* remotos que a diferencia de los tradicionales son colocados en lugares estratégicos y se envía la información de manera remota, y finalmente técnicas poco estudiadas y que conllevan un nuevo eje de estudio que son las sabanas de información.

La segunda conducta más común en el *carding* es la comercialización, se explicó a detalle sobre la figura del cibermercado azul, se explicó la operatividad de la enajenación de tarjetas bancarias que es la búsqueda, contacto, acuerdo y entrega de información.

Finalmente llegamos a la conducta más importante en el carding que es el uso de números o tarjetas bancarias, en el cual, el cibercriminal utiliza los datos subjetivos de la tarjeta, es decir, el *PAN* (*Primary Account Number)* que puede contener desde nueve hasta dieciocho números dependiendo de la compañía o empresa que haya emitido la tarjeta.

En este punto fue importante continuar con la clasificación de Carders y Bineros en el que se encuentran cinco categorías más que son el nivel 5, ”aprendiz carder”, en el que realiza compras de bienes y servicios en internet con números de tarjetas que compró a niveles superiores, sólo que su alcance de compra es el más bajo de los demás niveles, limitándose a compras de hasta novecientos noventa y nueve pesos; posteriormente encontramos al nivel seis, “carder nivel medio”, donde cuenta con experiencia en el cibermercado azul y sus compras van desde los mil pesos hasta los cuatro mil novecientos noventa y nueve pesos; el nivel siete son los “carders nivel avanzado”, son distribuidores más no vendedores directamente de tarjetas bancarias, y sus compras alcanzan hasta los cien mil pesos; en el nivel nueve encontramos a los “proveedores de tarjetas bancarias” quienes obtienen información o números de tarjetas bancarias y la venden a los grupos de nivel inferior; finalmente encontramos a los “carders con *cash out”,* cuentan con técnicas directas para conseguir dinero líquido a partir de los números de las tarjetas; ocupan el último puesto ya que la liquidez inmediata les permite invertir en cualquiera de los demás niveles.

Para terminar todo el estudio sistemático se concluyó en este punto de que el Carding es el fenómeno principal y que dentro de este se encuentra el fenómeno de los BINS; sin embargo, era importante estudiar a profundidad la operatividad de la base particular para comprender el fenómeno general, por lo que se estudiaron los elementos básicos de los números de una tarjeta bancaria.

Se dividen en dos grandes grupos, subjetivos y objetivos; dentro de la primera categoría encontramos al *PAN (Primary Account Number)* que son los números de identificación bancaria o los números de cuenta principal que distinguen una tarjeta de otra, abordándose la esquematización por los tipos *MII, IIN, IAI* y el *Check.* Seguidamente se analizó el segundo elemento que es el código de seguridad y finalmente la fecha de vencimiento.

Dentro de los datos objetivos encontramos información del titular de la tarjeta bancaria como son el nombre y dirección, sin embargo, esta información al momento de realizar una compra *online* no es verificada al momento, debido a que la empresa vendedora no cuenta con estos datos, por lo que solicita más información al cibercriminal para comprobar la compra, sin embargo, se expuso

que esta información puede ser falsificada por los miembros de la asociación delictiva del Carding.

Una vez sistematizado y estudiado a profundidad el fenómeno del Carding fue importante analizarlo legalmente, se concluyó que el término “Carding” no se encuentra explícitamente en ninguna ley mexicana, sin embargo, sí se encuentra materialmente en la Ley General de Títulos y Operaciones de Crédito en los diversos 432, 433, 433 y 434, en la Ley de Instituciones de Crédito artículo 112 bis, 112 ter, 112 Quáter y 112 Quintus, además de que algunas subconductas como es la obtención y sustracción de números de tarjetas bancarias por medio de diferentes técnicas que se explicaron en el contenido de esta tesis están tipificados en el Código Penal Federal.

Además, se concluye que existe una diferencia entre los bienes jurídicos protegidos de una conducta tradicional a una ciberconducta del Carding, puesto que estos son pluriofensivos y que además del patrimonio encontramos la información y la privacidad de la información.

Existe una diferencia entre el ofendido y la víctima en las diversas conductas del carding, puesto que la víctima es quien resiente directamente la conducta y el ofendido es el titular del bien jurídico tutelado y es importante diferenciar para evitar vacíos jurídicos.

Finalmente se analizó la competencia del Carding para ver si era de carácter federal o local (ya que en algunos códigos penales estatales como el de Nuevo León o Puebla encuadran algunas de las subconductas del carding como delito) por lo que la Suprema Corte de Justicia interpretó que al tratarse de delitos especiales que se encuentran en la Ley General de Títulos y Operaciones de Crédito y en la Ley de Instituciones de Crédito, y aunado al principio de especialidad en la materia, además de la asociación delictuosa del carding, es por lo que el Carding es de índole federal y no estatal.

Como tercer y último pilar de la investigación fue conocer las medidas para combatir el Carding, por lo que de manera internacional encontramos a protocolos como el *Payment Card Industry Data Security Standard (PCI DSS)* que son normas de seguridad de datos de tarjetas bancarias, y que brinda

requisitos para el cumplimiento del procesamiento de datos de tarjetas bancarias. Además, se encontraron estándares internacionales como el *ISO/IEC 7812-1:2006 Identification cards, Identification of issuers, Part 1: Numbering system,* en los que se encontraban criterios para permitir la interoperabilidad de los *PAN.*

En medidas nacionales, encontramos múltiples circulares por parte de Banco de México como la 34/2010, en el que se detalla la seguridad y protocolos que debe contener una tarjeta, sus números e información.

Encontramos que la Comisión Nacional Bancaria y de Valores cuenta con facultades para coadyuvar con el ministerio público respecto al Carding, conforme al artículo cuarto de la ley de la propia comisión, así mismo en el artículo 37 del reglamento de la citada ley, menciona que le corresponde dar opinión a la Secretaría de Hacienda y Crédito Público para denunciar el Carding.

Por su parte la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF) también cuenta con atribuciones para denunciar el Carding conforme a la fracción XXVl artículo once de la ley de la propia comisión. Además de que la CONDUSEF creo un portal de Fraudes Financieros con el objetivo de mitigar los ciberfraudes.

Las entidades emisoras de tarjetas bancarias han tomado un papel activo dentro del fenómeno creando diferentes herramientas como la creación de *wallets*, *tokens, sistemas de alertas, sistemas de verificación, banca móvil,* etc., sin embargo, las estadísticas nacionales demuestran que los esfuerzos tecnológicos y logísticos no han sido suficientes para frenar el Carding.

En cuanto al análisis de datos aportados por la CONDUSEF se concluye que antes del 2017 las cifras por conductas tradicionales eran superior que las ciberconductas del Carding, sin embargo, después de este año, el carding se puso a la delantera, advirtiéndose que las cifran sigan en aumento. Esto es debido a la evolución de las tecnologías de la información y comunicación (TIC´S) y a las nuevas técnicas de la operatividad del Carding.

Existe una enorme diferencia entre los reportes recibidos en la CONDUSEF por el fenómeno del Carding y el ministerio público federal; del dos mil trece al dos mil dieciocho hubo un total de 7,300,575 reportes por estas conductas, sin embargo, a nivel federal sólo se registraron 10,221, es decir, sólo se denunciaron el 0.14% de los casos de Carding y de conductas tradicionales.

En el Estado de Puebla para el 2018 el monto reclamado por el carding fue la cantidad de $89,458,315.00, un 224% mayor que en el 2017; un 438% mayor que en el 2016 y un 492% mayor que en el 2015.

El bajo nivel de denuncia se debe a los elementos del carding, es decir, que es no presencial o remotamente y que utiliza las nuevas tecnologías como medio de la comisión del delito; las víctimas saben desde luego que es muy complicado encontrar a los responsables ya que los protege el anonimato.

La falta de conocimiento por parte de las autoridades, instituciones y entidades emisores hace que el carding siga creciendo y que exista impunidad, ya que por una parte existe un papel muy pasivo por parte de la Comisión Nacional Bancaria y de Valores para investigar dentro de sus atribuciones y denunciar el Carding, el mismo papel pasivo lo adopta la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros; por su parte, los hechos denunciados en el ministerio público no tienen seguimiento debido a una falta de capacitación por parte del recurso humano y porque no cuentan con el equipo tecnológico para la debida investigación; así mismo, las víctimas y ofendidos no cuentan con la cultura de denuncia.

PROPUESTAS

Para prevenir y combatir el carding resulta elemental conocer los elementos que lo componen, su operatividad y su evolución. Existen cuatro pilares en las que se debe basar las acciones para prevenir y combatir el carding, el primero de ellos es el que comprende a las entidades emisoras, el segundo a los tarjetahabientes y usuarios de servicios financieros, el tercero a la Secretaría de Hacienda y Crédito Público y finalmente a los Ministerios Públicos, ciberpolicía y Unidades Especializadas de la Fiscalía General de la República.

Primera acción a realizar

Realizar por parte de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF) campañas especializadas y específicas para prevenir el Carding para la población en general.

Las principales técnicas que utilizan los carders para sustraer información o números de tarjetas bancarias de los tarjetahabientes son la ingeniera social*, spam, -phishing, pharming, robo de credenciales* y *keyloggers*; al contar con campañas especializadas para prevenir el Carding le dará a la población las bases técnico jurídicas para que no sean víctimas del Carding y esté será, el primer medio para disminuir este fenómeno.

Una sociedad culta de delitos ciberfinancieros, es la mejor inversión para prevenir el Carding. Las ventajas, es el conocimiento de los tarjetahabientes, una cultura de prevención y acción, además, de una mejor inclusión financiera por parte de las tarjetas bancarias. Retos. Personal especializado, y debidamente capacitado, y la desventaja radica en la falta de interés por parte de la población.

Segunda propuesta

Implementar en conjunto por parte de la Secretaria de Hacienda y Crédito público, entidades emisoras de tarjetas bancarias y Fiscalía General de la República, el sistema de inteligencia artificial ***Machine Learning,*** que permitirá inferir conductas sospechosas del carding, analizando grandes cantidades de

datos con el objetivo de prevenir las conductas directas y futuras de este fenómeno.

Las estadísticas son la parte fundamental de esta propuesta, por lo que se crearía una base de datos especializada en carding por parte de las entidades que se mencionaron al principio de esta propuesta.

Las ventajas es que sería un sistema tecnológico en conjunto especializado que permitiría deducir y prevenir las amenazas reales y futuras del carding. Los retos son la falta de estructura tecnológica y el avance primario de esta tecnología.

Tercera propuesta

Capacitación especializada sobre el carding a Ministerios Públicos y Ciberpolicías.

Las autoridades deben contar con información actualizada respecto de las conductas del carding. Generalmente las conductas del Carding son repetitivas, y con la información actualizada pueden investigar y encontrar a los culpables de estas conductas.

Las ventajas es que se tendrá personal altamente capacitado y actualizado respecto de los nuevos ciberdelitos financieros del Carding y BINS; mayor eficiencia en la investigación de los mismos y será un gran factor para disminuir el Carding.

Cuarta propuesta

A las entidades emisoras incrementar sus protocolos de seguridad con el recurso humano para evitar a los *insiders*, debido a que estos manejan datos objetivos y subjetivos de los tarjetahabientes, mismos que son sustraídos y comercializados en el cibermercado azul.

Las ventajas es que disminuiría un porcentaje considerable del Carding. Los retos son identificar a este personal.

Quinta propuesta

Convención Anual para la prevención y combate del Carding, entre entidades emisoras, representantes de la Secretaría de Hacienda y Crédito Público por conducto de la Comisión Nacional Bancaria y de Valores, la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros y Fiscalía General de la República.

Cada uno de estos cuenta con una perspectiva diferente de cómo afrontar el carding, una mesa de dialogo, intercambio de información, jornadas de actualización, estrategias de prevención, será un medio idóneo para estar a la vanguardia del conocimiento y tener éxito contra el combate y prevención del carding.

Referencias

Libros

Acurio del pino, Santiago, delitos informáticos: generalidades, consultable en: https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf.

Acurio del pino, Santiago, delitos informáticos: generalidades, consultable en: https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf.

Avilés Gómez, Manuel, Delitos y delincuentes. Cómo son, cómo actúan, Alicante, Editorial Club Universitario, 2010.

Beltramone, Guillermo, et al, Nociones básicas sobre los Delitos Informáticos, Santiago, 1998, consultable en: http://rodolfoherrera.galeon.com/delitos.pdf.

Davara Fernandez Elena, et al., delitos informáticos, Pamplona, Aranzadi, 2017.

Gonzáles de la Vega, Francisco, Derecho Penal Mexicano, 10a., Ed. Porrúa, México 1970.

López Betancourt, Eduardo. Delitos en Particular, tomo l, 8a., Ed. Editorial Porrúa, México, 2002.

MAGLIONA MARKOVICTH, Claudio Paúl, LÓPEZ MEDEL Macarena, Delincuencia y Fraude Informático, Editorial Jurídica de Chile, 1999.

Mariño López, Andrés, Uso fraudulento de tarjetas de crédito por terceros no autorizados, Madrid, Ediciones Jurídicas y Sociales, S.A. 2006.

Paenza, Adrián, La matemática del futuro, Editorial Sudamericana, 2017.

Rebollar, Yuridia, Delitos en Particular, consultable en: https://www.umla.edu.mx/PlataformaDigital/Antologias/DERECHO%20PENAL%20PARTE%20 ESPECIAL%20Y%20DELITOS%20EN%20PARTICULAR.pdf.

Téllez, Julio, Derecho Informático, 2a ed. México, Graw Hill, 2001.

Legislación

Estados Unidos Mexicanos, Código Nacional de Procedimientos Penales, Diario Oficial de la Federación, 5 de marzo de 2014, última reforma publicada 9 de agosto de 2019, consultable en: http://www.diputados.gob.mx/LeyesBiblio/pdf/CMPP_210618.pdf.

Estados Unidos Mexicanos, Código Penal del Estado Libre y Soberano de Puebla, Periódico Oficial del Estado, 23 de diciembre de 1986, última reforma 04 de abril de 2019.

Estados Unidos Mexicanos, Código Penal Federal, Diario Oficial de la Federación, 14 de agosto de 1931, última reforma publicada en el Diario Oficial de la Federación el 14 de agosto de 2019, consultable en: http://www.diputados.gob.mx/LeyesBiblio/pdf/9_081119.pdf.

Estados Unidos Mexicanos, Ley de Ahorro y Crédito Popular, Diario Oficial de la Federación, 4 de junio de 2001, última reforma publicada en el Diario Oficial de la Federación el 10 de enero de 2014, consultable en: http://www.diputados.gob.mx/LeyesBiblio/pdf/17.pdf.

Estados Unidos Mexicanos, Ley de fondos de inversión, Diario Oficial de la Federación, 4 de junio de 2001, última reforma publicada en el Diario Oficial de la Federación el 13 de junio de 2014, consultable en: http://www.diputados.gob.mx/LeyesBiblio/pdf/69_130614.pdf.

Estados Unidos Mexicanos, Ley de Instituciones de Crédito, Diario Oficial de la Federación, 18 de julio de 1990, última reforma publicada en el Diario Oficial de la Federación el 4 de junio de 2019. Consultable en: http://www.diputados.gob.mx/LeyesBiblio/pdf/43_040619.pdf.

Estados Unidos Mexicanos, Ley de la Comisión Nacional Bancaria y de Valores, Diario Oficial de la Federación, 28 de abril de 1995, última reforma publicada en el Diario Oficial de la Federación el 09 de marzo de 2018, consultable en: http://www.diputados.gob.mx/LeyesBiblio/pdf/46_090318.pdf.

Estados Unidos Mexicanos, Ley de Protección y Defensa al Usuario de Servicios Financieros, Diario Oficial de la Federación, 18 de enero de 1999, última reforma publicada en el Diario Oficial de la Federación el 18 de enero de 1999, consultable en http://www.diputados.gob.mx/LeyesBiblio/pdf/64_090318.pdf.

Estados Unidos Mexicanos, Ley de Uniones de Crédito, Diario Oficial de la Federación, 20 de agosto de 2008, última reforma publicada en el Diario Oficial de la Federación el 10 de agosto de 2008, consultable en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LUC.pdf.

Estados Unidos Mexicanos, Ley del Mercado de Valores, Diario Oficial de la Federación, 30 de diciembre 2005, última reforma publicada en el Diario Oficial

de la Federación el 9 de enero de 2019, consultable en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LMV_090119.pdf.
Estados Unidos Mexicanos, Ley Federal de Protección al Consumidor, Diario Oficial de la Federación, 24 de diciembre de 1992, última reforma publicada el 09 abril de 2012, consultable en: https://www.profeco.gob.mx/juridico/pdf/l_lfpc_ultimo_CamDip.pdf.
Estados Unidos Mexicanos, Ley General de Organizaciones y Actividades Auxiliares del Crédito, Diario Oficial de la Federación, 14 de enero de 1985, última reforma publicada en el Diario Oficial de la Federación el 9 de marzo de 2018, consultable en: http://www.diputados.gob.mx/LeyesBiblio/pdf/139_090318.pdf.
Estados Unidos Mexicanos, Ley General de Títulos y Operaciones de Crédito, Diario Oficial de la Federación, 27 de agosto de 1932, última reforma publicada en el Diario Oficial de la Federación el 22 de junio de 2018, consultable en: http://www.diputados.gob.mx/LeyesBiblio/pdf/145_220618.pdf.
Estados Unidos Mexicanos, Ley para Regular las Actividades de las Sociedades Cooperativas de Ahorro y Préstamo, Diario Oficial de la Federación, 13 de agosto de 2009, última reforma publicada en el Diario Oficial de la Federación el 13 de agosto de 2009, consultable en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LRASCAP_280414.pdf.
Estados Unidos Mexicanos, Ley para Regular las Agrupaciones Financieras, Diario Oficial de la Federación, 10 de enero de 2014, última reforma publicada en el Diario Oficial de la Federación el 03 de marzo de 2018, consultable en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LRAF_090318.pdf.
Estados Unidos Mexicanos, Ley para regular las Instituciones de Tecnología Financiera, nueva ley publicada en el Diario Oficial de la Federación el 9 de marzo de 2018, consultable en http://www.diputados.gob.mx/LeyesBiblio/pdf/LRITF_090318.pdf.
Estados Unidos Mexicanos, Ley para Regular las Sociedades de Información Crediticia, Diario Oficial de la Federación, 15 de enero de 2002, última reforma publicada en el Diario Oficial de la Federación el 3 de marzo de 2018, consultable en: http://www.diputados.gob.mx/LeyesBiblio/pdf/237_090318.pdf.
Estados Unidos Mexicanos, Reglamento interior de la Comisión Nacional Bancaria y de Valores, Diario Oficial de la Federación, 12 de noviembre de 2014,

México, consultable en. http://www.diputados.gob.mx/LeyesBiblio/regla/n228.pdf.

Web site

¿Qué es PIN?, consultable en: https://es.ccm.net/faq/10682-quees-el-pin.

¿Qué es telemática?, consultable en: http://www.cavsi.com/preguntasrespuestas/que-estelemática/.

¿Qué es telemática?, consultable en: http://www.cavsi.com/preguntasrespuestas/que-estelemática/.

¿Qué es un link? Definición y tipos de enlaces, consultable en: https://powertoyourseo.com/blog/es/que-es-un-link/.

Acosta Patroni, Alejandro, Hacking, Cracking y Otras Conductas Ilícitas Cometidas a Través de Internet, 2003, consultable en: http://repositorio.uchile.cl/bitstream/handle/2250/114475/de-acosta_a.pdf.

Acosta, David ¿Cómo funcionan las tarjetas de pago? Parte ll: CID/CAV/CVC2/CVV2 consultable en https://www.pcihispano.com/como-funcionan-las-tarjetas-de-pago-parte-iicidcav2cvc2cvv2/.

Acosta, David, ¿Cómo funcionan las tarjetas de pago? Parte l: PAN (Primary Account Number), consultable en https://www.pcihispano.com/comofuncionan-las-tarjetas-de-pago-parte-i-pan-primary-account-number/.

Acosta, David, ¿Qué es PCI DSS?, consultable en: https://www.pcihispano.com/que-es-pci-dss/.

Akamai, ¿Qué es el phishing?, consultable en: https://www.akamai.com/es/es/resources/what-is-phishing.jsp.

Alessandro Elia, Ivano, et al, Comparing SQL Injection Detection Tools Using Attack Injection: An experimental Study, consultable en: https://ieeexplore.ieee.org/abstract/document/5635053.

American Express, acerca de la compaña, consultable en: https://www.americanexpress.com/mx/about-the-company.html.

American Express, acerca de la compaña, consultable en: https://www.americanexpress.com/mx/about-the-company.html.

American Express, Política operativa de seguridad de datos de American Express para proveedores de servicios, consultable en: https://www.google.com/search?q=que+es+data+security+operating+policy&oq

=que+es+data+
security+operating+po&aqs=chrome.1.69i57j33l5.7911j1j7&sourceid=chrome&ie=UTF-8.
Ávila, Fabián, ¿Qué es y para qué sirve el streaming?, consultable en: https://eventovirtual.co/que-es-y-para-que-sirve-el-streaming/.
Banco de México, ¿Qué es un activo virtual?, consultable en: https://www.banxico.org.mx/sistemas-de-pago/1---que-es-un-activo-virtua.html.
Banco de México, Circular 34/2010, Reglas de Tarjetas de Crédito, consultable en: https://www.banxico.org.mx/marco-normativo/normativa-emitida-por-el-bancode-mexico/circular-34-2010/%7B0C55B906-6DB4-6B88-FED0-67987E9FB3CC%7D.pdf.
Bembibre, Victoria, Definición de Memoria Cache, consultable en: https://www.definicionabc.com/tecnologia/memoria-cache.php.
Blaker, Cristian, Bins y Carding| Todo lo que debes aprender, 2018, consultable en: https://rincondelgeek.com/Bins+y+carding+.
Cáceres Ramírez, Orlando, Anglicismos, consultable en: https://www.aboutespanol.com/anglicismos-2879601.
Cambridge Dictionary, Sniff, consultable en: https://dictionary.cambridge.org/es/diccionario/inglesespanol/sniff.
Carles, Joan, Acceder a la Deep web de forma segura, 2013, consultable en: https://geekland.eu/acceder-a-la-deep-web/.
Centro de Investigación y Desarrollo de Recursos Científicos BioScripts, elemento compositivo, consultable en: https://www.biodic.net/palabra/elementocompositivo/#.XcIgQdJKgdU.
Centro Nacional de Información, reporte de incidencia delictiva del fuero federal por entidad federativa 2012 – 2019, consultable en: https://drive.google.com/file/d/11jAkigPtlWaq7jtW9bazByachs7fYXAE/view.
Ciber Edu, What is Data Leakage, consultable en: https://www.forcepoint.com/cyber-edu/data-leakage.
CISCO, ¿Qué es un firewall?, consultable en: https://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html.
Cointelegraph, que son y cómo funciona el dinero digital, consultable en: https://es.cointelegraph.com/bitcoin-for-beginners/what-are-cryptocurrencies.

Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, Fraudes Financieros ¡No te dejes engañar!, consultable en https://www.gob.mx/cms/uploads/attachment/file/240481/FRAUDES_FINANCIEROS_web.pdf.

Comisión Nacional para la Protección y Defensa de los Usuarios de los Servicios Financieros, Checa tu estado de cuenta y cuídate del Carding, consultable en: https://www.gob.mx/condusef/articulos/checa-tu-estado-de-cuenta-y-cuidate-delcarding?idiom=es.

Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, Conoce el nuevo Portal de Fraudes Financieros, consultable en: https://www.gob.mx/condusef/articulos/conoce-el-nuevo-portal-de-fraudes-financieros?idiom=es.

Comisión Nacional para la Protección y Defensa de los Usuarios de los Servicios Financieros, medidas de seguridad, consultable en: https://www.condusef.gob.mx/gbmx/?p=medidas-deseguridad.

Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, estadísticas, 2019, consultable en: https://www.condusef.gob.mx/gbmx/?p=estadisticas.

Company Combo, ¿Cuál es la diferencia entre una empresa LLC y una CORP?, consultable en: http://companycombo.com/es/faq/cual-es-la-diferencia-entre-una-empresa-llc-y-una-corp/.

DES, consultable en: http://neo.lcc.uma.es/evirtual/cdd/tutorial/presentacion/des.html.

Díaz, Alexander, El bien jurídico tutelado del dato y los nuevos verbos rectores de los delitos electrónicos, consultable en: http://www.redipd.es/noticias_todas/2011/tribuna/common/1/EL_BIEN_JURIDICO_TUTELADO
_DEL_DATO_Y_LOS_NUEVOS_VERBOS_RECTORES_DE_LOS_DELITOS_ELECTRONICO S_USC.pdf.

Diccionario de la Real Academia Española, vigesimotercera edición, Ciber-., Consultable en: https://dle.rae.es/srv/search?m=30&w=ciber-.

Diners Club, quienes somos mundo, consultable en: https://www.mundodinersclub.com/quienes-somosmundo.html.

Discover Global Network, Discover Informatión Security & Compliance (DISC), consultable en: https://www.discoverglobalnetwork.com/en-us/business-resources/fraud-security/pci-rulesregulations/discover-information-security-compliance.

Dwyer, Ben, Visa Cardholder Information Security Program, consultable en: https://www.cardfellow.com/blog/visa-cardholderinformation-security-program-cisp/.

ecured, IBM, consultable en: https://www.ecured.cu/IBM.

EcuRed, Mozilla Firefox, consultable en: https://www.ecured.cu/Mozilla_Firefox.

EcuRed, web, consultable en: https://www.ecured.cu/Web.

EMVCo, consultable en: https://www.emvco.com/.

Facebook, Condiciones y Políticas de Privacidad, consultable en https://www.facebook.com/policies.

Facebook, Normas Comunitarias, consultable en: https://www.facebook.com/communitystandards/.

Facebook, Política de datos, consultable en: https://www.facebook.com/about/privacy.

Facebook., Condiciones de servicio, consultable en: https://www.facebook.com/legal/terms.

Fernández Díaz, Macarena, Cómo solicitar una tarjeta Discover, 2018, consultable en: https://www.cuidatudinero.com/13170246/como-solicitaruna-tarjeta-discover.

García, Yesenia, BINS primeros pasos, 2016, consultable en: https://www.academia.edu/28287735/BINS_PRIMEROS_PASOS_Conceptos_b%C3%A1sicos.

Global JCB, PCI DSS, Payment Card Industry Data Security Standard, consultable en: https://www.global.jcb/en/products/security/pci-dss/index.html.

Gobierno de México, incidencia delictiva, 2019, consultable en. https://www.gob.mx/sesnsp/acciones-y-programas/preguntas-frecuentes-repuve-incidenciadelictiva-rnped-emergencias-066?idiom=es.

Gómez, Víctor, Sniffing, consultable en: https://instintobinario.com/sniffing/.

Hackett Bergmann, Caesars, Carding Delito Informático, 2018, consultable en: https://medium.com/@caesarshackettbergmann/carding-v-bfa5f94a750e.

https://es.bab.la/diccionario/inglesespanol/skimmer.

https://namso-gen.com/.
https://www.bincodes.com/.
https://www.elfqrin.com/discard_credit_card_generator.php.
https://www.fakepersongenerator.com/creditcard-generator.
https://www.fakepersongenerator.com/credit-cardgenerator.
https://www.fakepersongenerator.com/credit-card-generator.
https://www.santander.com.mx/PDF/cntrts/contrato_unico_de_tarjeta_de_credito_dic_2012.pdf.
ISO/IEC 7812-1:2017 Identification cards — Identification of issuers — Part 1: Numbering system, consultable en: https://www.iso.org/standard/70484.html.
Kagan, Julia, validatión code, consultable en: https://www.investopedia.com/terms/v/validation-code.asp.
Kaspersky, ¿Qué es el pharming y cómo evitarlo?, consultable en: https://latam.kaspersky.com/resource-center/definitions/pharming.
Lexico, chip, consultable en: https://www.lexico.com/es/definicion/chip.
Léxico, on line, consultable en: https://www.lexico.com/es/definicion/on_line.
Linguee, cash out, consultable en: https://www.linguee.es/ingles-espanol/traduccion/cash+out.html.
López, Sonia, Que es ISO, consultable en: https://www.certificadoiso9001.com/que-esiso/.
Mastercard, acerca de mastercard, consultable en: https://www.mastercard.com.mx/esmx/acerca-de-mastercard.html#, y https://www.bnamericas.com/es/perfil-empresa/mastercardinc.
MasterCard, Protecting the payments ecosystem, consultable en: https://www.mastercard.us/en-us/merchants/safety-security/security-recommendations/sitedata-protection-PCI.html.
Morales, Miguel, Qué es 4chan, el peculiar foro donde se colgó el Fappening, 2014, consultable en: https://computerhoy.com/noticias/internet/que-es-4chanpeculiar-foro-donde-colgo-fappening-18819.
Mozilla, Preguntas Frecuentes, consultable en: https://www.mozilla.org/en-US/security/bug-bounty/faq-webapp/.
Multipagos, ¿Que es Verified by Visa y MasterCard SecureCode?, consultable en: https://www.multipagos.com.mx/eEmpresa/utils/3DSecure/3DSecure.html.

Número CVV de la tarjeta de crédito o débito, ubicación e información, consultable en: https://www.cvvnumber.com/.
Ojeda Pérez, Jorge Eliécer et al., Delitos Informáticos y entorno jurídico vigente en Colombia, 2010, consultable en: https://dialnet.unirioja.es/descarga/articulo/3643404.pdf.
Online Reverse Hash Tool. V.3.3, consultable en https://appo.pro/11-online-reverse-hash-tool-v33-orht-v33.html.
PCI Security, consultable en: https://www.pcisecuritystandards.org/pci_security/.
Pérez Porto, Julián, et al., Definición de Premium.
Pickaweb. ¿Qué es HTTPS?, consultable en: https://www.pickaweb.es/ayuda/que-es-https/.
Procuraduría Federal del Consumidor, Consejos de seguridad para evitar el fraude cibernético, consultable en: https://www.facebook.com/216423475165030/posts/1368153146658718/?app=fbl.
Procuraduría Federal del Consumidor, Monitoreo de Tiendas Virtuales, disponible en: https://www.profeco.gob.mx/tiendasvirtuales/index.html
Procuraduría General de la República, Cibercriminalidad, delitos en la red, D.F., Instituto Nacional de Ciencias Penales, 2006, Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, Checa tu estado de cuenta y cuídate del Carding, consultable en: https://www.gob.mx/condusef/articulos/checa-tu-estado-de-cuenta-y-cuidate-delcarding?idiom=es.
PROFECO, El lado oscuro de Internet, 2006, consultable en: https://www.profeco.gob.mx/encuesta/brujula/bruj_2006/pdf06/2006-11-13%20El%20lado%20oscuro%20de%20Internet.pdf.
Que significa keylogger en español, consultable en: https://es.bab.la/diccionario/ingles-espanol/keylogger.
Quintero, Antonio, Definición de Insider, 2018, consultable en: https://www.economiasimple.net/glosario/insider.
Reyna, Armando, ¿Qué es una tarjeta digital y cómo se usa?, 2018, consultable en: https://www.bbva.com/es/tarjeta-digital-usa/.

Rodríguez, Cristina, ¿Qué es E-commerce o comercio electrónico?, 2015, consultable en: https://marketingdigital.bsm.upf.edu/e-commerce-comercio-electronico/.

Rouse, Margaret, Short Message Service, consultable en: https://searchmobilecomputing.techtarget.com/definition/Short-Message-Service.

Sandra López, Carding: la nueva modalidad de fraude a tarjeta bancaria, consultable en https://www.oinkoink.com.mx/noticias/carding-nueva-modalidad-fraude-tarjeta-bancaria/.

Script, consultable en: https://www.significados.com/script/.

Security Standards Council, Skimming Preventión: Overview of Best Practices for Merchants, consultable en: https://www.pcisecuritystandards.org/documents/skimming_prevention_overview_one_sheet.pdf.

Security Standars Council, Industria de tarjetas de pago (PCI) Norma de seguridad de datos para las aplicaciones de pago. Requisitos y procedimientos de evaluación de seguridad, consultable en: https://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs/PA-DSS_v3- 2_es-LA.pdf.

significados, Qué es URL, consultable en: https://www.significados.com/url/.

significados, significado de Wifi, consultable en: https://www.significados.com/wifi/.

SoftwareLab, ¿Qué es un antivirus? La definición y los 5 ejemplos principales, consultable en: https://softwarelab.org/es/que-es-un-antivirus/.

Tarjetas de crédito falsas, consultable en: https://www.tarjetasdecreditofalsas.com/.

Tec Electrónica, El ABC de la banda magnética, consultable en: https://www.tecmex.com.mx/promos/bit/bit0703-msr.htm.

Technical Committees, o comité técnico en español, dedicados a la estandarización en el campo de la banca, valores y otros servicios financieros, consultable en: https://www.iso.org/committee/49650.html.

Tejeda Anaya, María Antonieta, Software, consultable en: https://www.uaeh.edu.mx/docencia/P_Presentaciones/prepa4/informatica/Software_1.pdf.

Tovar, Carlos, Los niños ratas del ciberespacio, 2014, consultable en: https://www.elmanana.com/los-ninos-ratas-del-ciberespacio/2604450.
tpvcenter, ¿Qué es 3D Secure?, consultable en: https://www.tpvcenter.com/3DSecure.html.
VISA, acerca de visa, consultable en: https://www.visa.com.mx/acerca-de-visa.html.
VISA, Information Security, consultable en: https://aw.visa.com/run-your-business/smallbusiness/information-security/ais-program.html.

Tesis Semanario Judicial de la Federación

Tesis visible a página mil doscientos dieciséis, del Semanario Judicial de la Federación, con número de registro: 284044, bajo el rubro BIENES MUEBLES E INMUEBLES, consultable en: http://sjf.scjn.gob.mx/SJFSist/Documentos/Tesis/284/284044.pdf.
Tesis IV.1o.52 P, visible a página tres mil setecientos cuarenta y cinco, libro lll, tomo cinco del Semanario Judicial de la Federación y su Gaceta, con número de registro 160603, diciembre de 2011, novena época, consultable en: http://sjf.scjn.gob.mx/SJFSist/Documentos/Tesis/160/160603.pdf.
Tesis XV.4o.5 P, visible a página mil quinientos diecinueve, tomo XXII del Semanario Judicial de la Federación y su Gaceta, bajo el rubro: REPRODUCCIÓN DE TARJETAS DE CRÉDITO O DÉBITO. AL ESTAR DICHA CONDUCTA PREVISTA COMO DELITO EN LA LEY DE INSTITUCIONES DE CRÉDITO, EL PROCESO QUE SE INSTRUYA AL INCULPADO DEBE SEGUIRSE ANTE UN JUEZ DEL FUERO FEDERAL, consultable en: http://sjf.scjn.gob.mx/sjfsist/Documentos/Tesis/177/177826.pdf.
Tesis VI.2o.8 P, visible a página quinientos treinta y cinco, tomo l. junio de 1995, del Semanario Judicial de la Federación y su Gaceta, novena época, bajo el rubro: ROBO, APODERAMIENTO COMO CONSUMACIÓN DEL, consultable en: http://sjf.scjn.gob.mx/SJFSist/Documentos/Tesis/205/205104.pdf.
Tesis I.6o.P.137 P, visible a página seiscientos quince, libro ll, tomo l del Semanario Judicial de la Federación y su Gaceta, con número de registro 160702, noviembre de 2011, novena época, bajo el rubro: COMPETENCIA PARA CONOCER DE LOS DELITOS EN LOS QUE SE UTILICE UNA TARJETA

EMITIDA POR UNA ENTIDAD COMERCIAL NO BANCARIA PARA LA ADQUISICIÓN DE BIENES Y SERVICIOS. SE SURTE A FAVOR DE LOS JUECES FEDERALES EN MATERIA PENAL, consultable en: http://sjf.scjn.gob.mx/sjfsist/Documentos/Tesis/160/160702.pdf.

Anexos

Solicitud de información a la Comisión Nacional para la Protección y Defensa de los usuarios de Servicios Financieros respecto a estadísticas y datos sobre reclamaciones del carding, del periodo de primero de enero del dos mil quince al treinta y uno de mayo de dos mil diecinueve en el Estado de Puebla. Solicitud con folio número 0637000020919. (Se anexa documento *Ut infra).*

OFICIO:VJ/UT/070/2019

ASUNTO: Se contesta solicitud de información **0637000020919**

Ciudad de México, a 12 de julio de 2019.

ESTIMADO SOLICITANTE
P R E S E N T E.

1

En atención a la solicitud de información con número de folio **0637000020919**, dirigida a la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, que a la letra indica:

Descripción clara de la solicitud de información.

"Estadísticas y datos sobre reclamaciones o quejas en materia de consumos no reconocidos vía internet presentadas ante la propia institución bancaria y ante CONDUSEF respecto de fraudes cibernéticos a tarjetas bancarias, del periodo de 1 de enero del 2015 al 31 de mayo de 2019 en el Estado de Puebla. Además de el monto reclamado, el monto reclamado concluido, el monto abonado." (sic)

Otros datos para facilitar su localización.

"La CONDUSEF emite estadísticas a nivel federal sobre estos datos, sin embargo, para fines de investigación me interesa conocer únicamente lo solicitado en el Estado de Puebla del 2015-31 de mayo del 2019." (sic)

Al respecto, y en términos de las facultades conferidas en la Ley de Protección y Defensa al Usuario de Servicios Financieros y a las atribuciones señaladas en las fracciones XV y XVIII del artículo 14 del Estatuto Orgánico de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, se hace de su conocimiento que mediante memorándum DASPF/SIC/0028/2019 el Titular de la Dirección de Análisis de Servicios y Productos Financieros y Enlace en Materia de Transparencia, Acceso a la Información Pública y Datos Personales en la Vicepresidencia Técnica indicó que la **Dirección de Información y Desarrollo Estadístico de la Dirección General de Desarrollo Financiero, Estadístico y de Tecnologías de Información adscrita a la Vicepresidencia Técnica** de la **Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF)**, declaró ser la unidad administrativa **COMPETENTE** para brindar la atención procedente a la solicitud de información que nos ocupa, por lo que en apego a lo dispuesto por los artículos 131 y 132 de la Ley General de Transparencia y Acceso a la Información Pública, 133 y 135 de la Ley Federal de Transparencia y Acceso a la Información Pública y el lineamiento Octavo de los "Lineamientos que establecen los procedimientos internos de atención a solicitudes de acceso a la información pública", se informó a esta Unidad de Transparencia a través del memorándum DASPF/RSIC/0028/2019, lo siguiente:

En atención a lo solicitado la Dirección de Información y Desarrollo Estadístico de la Dirección General de Desarrollo Financiero, Estadístico y de Tecnologías de Información, indicó que en las bases estadísticas y en los catálogos de productos financieros y causas de reclamación de la CONDUSEF, **no se tiene tipificada una causa específicamente con el rubro fraudes cibernéticos**, sin embargo, privilegiando el principio de máxima publicidad y con base en los términos de su solicitud, se remitió la información del análisis de la clasificación de las causas de reclamación, considerando aquellas que pueden ser imputables a un posible fraude cibernético, con base a los catálogos de esta Comisión Nacional.

Las Causas de reclamación de CONDUSEF utilizadas son las siguientes:

1. **Consumos vía internet no reconocidos**
2. **Inconformidad por el importe de un consumo en comercio por internet**
3. **Transferencia electrónica no reconocida**

En cuanto a las reclamaciones recibidas en la CONDUSEF, se tienen registros de las reclamaciones imputables a un posible fraude cibernético desde enero del 2015 hasta enero - mayo del 2019, sin embargo, con respecto a los montos económicos reclamados y recuperados, le informamos que en las bases estadísticas de la CONDUSEF se registran montos a partir del año 2018 a la fecha.

Por lo anterior, se anexa las siguientes tablas estadísticas en las que encontrará el número de reclamaciones iniciadas imputables a un posible fraude cibernético del Sector Bancario recibidas por la CONDUSEF de la entidad federativa Puebla del periodo 2015 a enero-mayo de 2019, desglosadas por causa y producto financiero (tarjetas bancarias); con respecto al monto reclamado, monto reclamado concluido y monto abonado, se incluye información del periodo 2018 a enero-mayo de 2019.

Reclamaciones iniciadas ante CONDUSEF imputables a un posible fraude cibernético
Banca Múltiple
Tarjetas Bancarias

Estado Puebla
(2015-2017)

Causa de Reclamación (Motivo)	Producto financiero	2015 Reclamaciones	2016 Reclamaciones	2017 Reclamaciones
Consumos vía internet no reconocidos	Tarjeta de crédito	15	16	13
	Tarjeta de débito	7	6	4
Inconformidad por el importe de un consumo en comercio por internet	Tarjeta de crédito	0	0	0
	Tarjeta de débito	0	0	1
Transferencia electrónica no reconocida	Tarjeta de débito	14	38	17
Total		**36**	**60**	**35**

Reclamaciones iniciadas ante CONDUSEF imputables a un posible fraude cibernético incluyendo monto reclamado, monto reclamado concluido y monto abonado
Banca Múltiple
Tarjetas Bancarias

Estado Puebla
(2018- 2019)

Causa de Reclamación (Motivo)	Producto financiero	2018				2019*			
		Reclamaciones	Monto Reclamado	Monto Reclamado Concluido	Monto Abonado	Reclamaciones	Monto Reclamado	Monto Reclamado Concluido	Monto Abonado
Consumos vía internet no reconocidos	Tarjeta de crédito	1	$3,000	$3,000	$13,000	5	$81,394	$98,682	$138,763
	Tarjeta de débito	4	$3,043,106	$3,043,106	$46,344	8	$239,483	$239,483	$78,054
Inconformidad por el importe de un consumo en comercio por internet	Tarjeta de crédito	0	-	-	-	1	$0	$0	$2,230
	Tarjeta de débito	0	-	-	-	1	$0	$0	$0
Transferencia electrónica no reconocida	Tarjeta de débito	24	$2,770,858	$2,655,858	$109,687	12	$861,839	$649,106	$99,003
Total		**29**	**$5,816,964**	**$5,701,964**	**$169,031**	**27**	**$1,182,716**	**$987,271**	**$318,050**

* Cifras enero-mayo 2019

Por otra parte, respecto a la información requerida sobre las reclamaciones presentadas ante las **Instituciones Bancarias**, esta se obtiene del Registro de Información de las Unidades Especializadas (REUNE), el cual reporta la información de forma Trimestral.

Derivado de lo anterior, se anexan las siguientes tablas estadísticas con el número de reclamaciones recibidas en REUNE imputables a un posible fraude cibernético del sector Bancario de la entidad federativa Puebla del periodo 2015 a enero-marzo de 2019 desglosados por causas, producto financiero (tarjetas bancarias), monto reclamado, monto reclamado concluido y monto abonado.

Reclamaciones recibidas en REUNE imputables a un posible fraude cibernético
Banca Múltiple
Tarjetas Bancarias

Estado Puebla

Año 2015

Causa de Reclamación (Motivo)	Producto financiero	2015			
		Reclamaciones	Monto Reclamado	Monto Reclamado Concluido	Monto Abonado
Consumos vía internet no reconocidos	Tarjeta de crédito	5,238	$14,091,053	$14,091,053	$12,121,617
	Tarjeta de Crédito básica	0	-	-	-
	Tarjeta de débito	1,060	$1,684,487	$1,684,487	$1,381,303
	Tarjeta prepagada	0	-	-	-
Inconformidad por el importe de un consumo en comercio por internet	Tarjeta de crédito	0	-	-	-
	Tarjeta de débito	0	-	-	-
Transferencia electrónica no reconocida	Tarjeta de débito	29	$2,404,152	$2,404,152	$27,645
Total		**6,327**	**$18,179,692**	**$18,179,692**	**$13,530,565**

Año 2016

Causa de Reclamación (Motivo)	Producto financiero	2016			
		Reclamaciones	Monto Reclamado	Monto Reclamado Concluido	Monto Abonado
Consumos vía internet no reconocidos	Tarjeta de crédito	4,707	$11,712,529	$11,712,529	$9,419,931
	Tarjeta de Crédito básica	0	-	-	-
	Tarjeta de débito	2,429	$5,731,498	$5,731,498	$4,089,144
	Tarjeta prepagada	0	-	-	-
Inconformidad por el importe de un consumo en comercio por internet	Tarjeta de crédito	1	$2,370	$2,370	$0
	Tarjeta de débito	0	-	-	-
Transferencia electrónica no reconocida	Tarjeta de débito	41	$2,938,694	$2,938,394	$6,082
Total		**7,178**	**$20,385,091**	**$20,384,791**	**$13,515,157**

Año 2017

Causa de Reclamación (Motivo)	Producto financiero	2017			
		Reclamaciones	Monto Reclamado	Monto Reclamado Concluido	Monto Abonado
Consumos vía internet no reconocidos	Tarjeta de crédito	11,586	$25,995,623	$25,962,425	$18,787,045
	Tarjeta de Crédito básica	3	$15,397	$15,397	$15,397
	Tarjeta de débito	8,557	$13,539,035	$13,480,392	$9,529,437
	Tarjeta prepagada	2	$181	$181	$181
Inconformidad por el importe de un consumo en comercio por internet	Tarjeta de crédito	9	$50,497	$50,497	$974
	Tarjeta de débito	6	$454	$454	$304
Transferencia electrónica no reconocida	Tarjeta de débito	6	$232,476	$232,476	$10,500
Total		**20,169**	**$39,833,663**	**$39,741,823**	**$28,343,837**

Año 2018

Causa de Reclamación (Motivo)	Producto financiero	2018			
		Reclamaciones	Monto Reclamado	Monto Reclamado Concluido	Monto Abonado
Consumos vía internet no reconocidos	Tarjeta de crédito	27,801	$58,963,449	$58,950,456	$45,643,832
	Tarjeta de Crédito básica	3	$9,283	$9,283	$356
	Tarjeta de débito	20,187	$29,501,003	$28,907,040	$18,746,766
	Tarjeta prepagada	0	-	-	-
Inconformidad por el importe de un consumo en comercio por internet	Tarjeta de crédito	11	$129,822	$129,822	$11,375
	Tarjeta de débito	34	$131,362	$131,362	$7,894
Transferencia electrónica no reconocida	Tarjeta de débito	18	$723,395	$723,395	$126,114
Total		**48,054**	**$89,458,315**	**$88,851,358**	**$64,536,337**

Año 2019

Causa de Reclamación (Motivo)	Producto financiero	2019*			
		Reclamaciones	Monto Reclamado	Monto Reclamado Concluido	Monto Abonado
Consumos vía internet no reconocidos	Tarjeta de crédito	7,547	$16,542,299	$15,108,110	$12,288,074
	Tarjeta de Crédito básica	0	-	-	-
	Tarjeta de débito	9,044	$10,949,077	$9,335,375	$5,971,123
	Tarjeta prepagada	0	-	-	-
Inconformidad por el importe de un consumo en comercio por internet	Tarjeta de crédito	1	$1,022	$1,022	$0
	Tarjeta de débito	35	$67,042	$67,042	$23,709
Transferencia electrónica no reconocida	Tarjeta de débito	24	$464,012	$444,012	$0
Total		**16,651**	**$28,023,453**	**$24,955,561**	**$18,282,905**

(*) Cifras enero-marzo 2019.

En tal virtud, y bajo los argumentos antes expuestos, esta Comisión Nacional da atención oportuna a la solicitud de información referida, garantizando con ello, el derecho de acceso a la información del peticionario.

No obstante, en caso de no satisfacerle lo antes señalado, y de conformidad con el artículo 142 de la Ley General de Transparencia y Acceso a la Información Pública y 147 de la Ley Federal de Transparencia y Acceso a la Información Pública, así como a lo estipulado en el Trigésimo Tercero de los Lineamientos que establecen los procedimientos internos de atención a solicitudes de acceso a la información Pública, podrá interponer Recurso de Revisión dentro de los quince días siguientes a la fecha de la notificación de la respuesta a su solicitud de información, por sí o a través de su representante legal ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, sita en Avenida Insurgentes Sur No. 3211, Colonia Insurgentes Cuicuilco, Alcaldía Coyoacán, en esta Ciudad de México.

Los requisitos, la manera, el lugar, el medio para presentar el citado medio de impugnación están disponibles para su consulta en la página www.inai.org.mx, al ingresar, localizar y elegir la opción **"Acceso a la Información"**, una vez desplegado su contenido deberá elegir **"Recurso de Revisión"**, apartado que contiene la información relativa a éste.

Debe referirse que el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales ha puesto a disposición de los solicitantes de acceso a la información el Sistema de Gestión de Medios de Impugnación, inserto en la denominada Plataforma Nacional de Transparencia, disponible en la dirección electrónica www.plataformadetransparencia.org.mx, en donde podrá presentar el mencionado Recurso de Revisión.

Finalmente, el presente lo suscribe la Directora General de Dictaminación y Supervisión, de conformidad con el memorándum VJ/045/2019 de fecha 24 de abril de 2019, emitido por la Vicepresidenta Jurídica y Titular de la Unidad de Transparencia, mediante el cual se le designa y habilita para recibir y dar trámite a las solicitudes de acceso a la información, con fundamento en los artículos 45, fracción VII, de la Ley General de Transparencia y Acceso a la Información Pública y 61, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública.

ATENTAMENTE
LA DIRECTORA GENERAL DE DICTAMINACIÓN Y SUPERVISIÓN,
ADSCRITA A LA VICEPRESIDENCIA JURÍDICA, EN LA COMISIÓN NACIONAL
PARA LA PROTECCIÓN Y DEFENSA DE LOS USUARIOS DE SERVICIOS FINANCIEROS

LIC. ELIZABETH ARAIZA OLIVARES.

KVUD