UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE DERECHO

SEMINARIO DE DERECHO MERCANTIL

"CARDING ONLINE FRAUDE EN COMPRAS POR INTERNET MEDIANTE LA CLONACION DE TARJETA DE CREDITO BASADO EN EL INDICE DE QUEJAS LEVANTADAS POR USUARIOS DE SERVICIOS FINANCIEROS EN CONDUSEF DURANTE EL AÑO 2013 Y 2014"

TESIS

PARA OBTENER EL TÍTULO

LICENCIADO EN DERECHO

PRESENTA

JOSÉ SALVADOR SÁNCHEZ MARTÍNEZ

ASESOR DE TESIS

DR. ALBERTO FABIAN MONDRAGON PEDRERO

DIRECTOR DEL SEMINARIO DE DERECHO

DR. ALBERTO FABIÁN MONDRAGÓN PEDRERO

CIUDAD UNIVERSITARIA, CD.MX OCTUBRE 2019

Agradecimientos

A mi madre

Porque sin ti esto no habría sido posible, por ser mí ejemplo de superación, mi amiga y aliada en cada uno de los retos que he decidido afrontar, por acompañarme en cada momento y ser mi fortaleza en cada adversidad, gracias infinitas por todo el apoyo en la elaboración de esta tesis y la obtención de este título.

A mi hermano

Por recordarme en cada instante que el compromiso y la constancia son la llave maestra del éxito, que no importa llegar primero sino ser constante y mantenerte hasta el final, y por apoyarme siempre.

Alejandra

Por creer en mí cuando ni siquiera yo mismo creí, por acompañarme en el inicio de este proceso y hasta el final del mismo, por jamás permitirme claudicar, por tu inagotable paciencia y apoyo, por tu estas tonto como vas a dejar la escuela y hacerme recapacitar una y mil veces, solo tú sabes lo que esto costo y sin ti esto jamás habría sido posible, gracias infinitas china.

Rogelio

Por apoyarme y darme las facilidades para poder elaborar este proyecto y consolidar este objetivo, porque por encima de ser un jefe en ti he tenido el placer de encontrar un amigo y un gran ser humano, infinitas gracias.

Fernanda

Por ser una compañera y apoyo en esta etapa, brindándome un apoyo incuestionable e inquebrantable, pero sobre todo por estar ahí aun cuando todo se mostró en contra, infinitas gracias, ya que sin ti esto no habría sido posible.

Alanís

Por ser un amigo, un segundo sinodal y un consejero en este proceso apoyándome en cada paso del mismo, por creer en mí y por hacer que esto fuera posible.

Noemi

Por recordarme que todo aquello que se inicia se concluye, que la mitad de algo es nada y que la determinación, la pasión y la constancia son la llave del éxito, ya que el talento no es suficiente, pero sobre todo por ser en esta etapa mi amiga, mi compañera y mi apoyo en cada momento y decisión que he tomado, por esto y todo aquello que vendrá gracias infinitas.

A la UNAM

Por aceptarme y arroparme en mi etapa estudiantil, y ayudarme a forjar y consolidar este gran sueño hoy convertido en logro, por darme todas las herramientas necesarias y ser mi segundo hogar todo este tiempo.

A todos mis amigos, compañeros y maestros de la UNAM que formaron parte de esta odisea, siempre se quedaran en mis recuerdos.

A mis amigos y familiares gracias por estar conmigo a su confianza y cariño.

Mi agradecimiento total Salvador

Índice

Capitulo uno: Internet

Capítulo dos: Delitos Cibernéticos

Capítulo tres: Carding online

Capítulo cuatro: Medios de defensa de los usuarios de servicios financieros contra delitos cibernéticos

Introducción

Durante la elaboración y conjunción de la información recabada en el siguiente trabajo, se busca iniciar un proceso de concientización de toda persona usuaria de servicios financieros vía internet, dándole las herramientas necesarias para poder entender el trasfondo de las operaciones financieras realizadas mediante la misma.

El uso de la internet para la realización de operaciones financieras es un evento que sucederá de manera gradual y casi obligatoria, esto derivado de la necesaria reducción de tiempos solicitada por los nuevos usuarios de servicios financieros que visualizan como una pérdida de tiempo el hecho de acudir a una sucursal para realizar una operación financiera, así como la necesaria reducción de costos operativos para las diversas instituciones financieras en la oferta de sus servicios.

Por tanto, es tarea mayor darle el grado y nivel de importancia necesario a este tema puesto que nos encontramos ya en este proceso de conversión.

Y en este trabajo busco aportar parte de mi experiencia laboral mezclada con un trabajo de investigación que permitirá conocer parte de este proceso, pero sobre todo brindare mi visión acerca de los puntos rojos a atenderse de manera inmediata para que dicha transición sea lo más amena posible.

Capítulo uno: Internet

1.1 Antecedentes

Internet surge derivado de dos necesidades tecnológicas primordiales, por un lado generar una comunicación expedita y segura por parte del ser humano en sus diversos ámbitos de desenvolvimiento, y la segunda, por la necesidad de almacenamiento, disposición y factibilidad de tener información de manera libre y segura.

Antes de la era del internet y que este lograra posicionarse y exponenciarse a nivel mundial existían otras formas de comunicación y de acceso, resguardo y manejo de información, como el correo postal, el telegrama, el fax y el teléfono, por ejemplificar algunos.

La explosión mediática, funcional y global por parte de internet se dio a principio de la década de 2000´s, pero antes existían diversos medios de comunicación utilizados por el ser humano para atender estas necesidades como son las cartas, el telegrama, la radio, televisión y el teléfono.

Así, para el caso de la comunicación la tendencia masificada utilizada por el ser humano fueron los medios escritos y los medios electrónicos, los cuales se pueden enlistar de la siguiente manera:

"La carta: es un medio de comunicación escrito entre dos personas, que consiste en una hoja de papel en la cual una persona escribía todo aquello que quisiera decir a otra y se envía vía correo postal, la ventaja que tiene este medio era su bajo costo y disponibilidad para comunicarse mediante él envió a casi cualquier rincón del mundo; su gran desventaja es que en el traslado de la misma sufría de manera constante el extravió de estas cartas y el tiempo que se tardaba en llegar las mismas era demasiado."[1]

[1] Rojas Amandi, V. M. (2001). *El uso de internet en el derecho*. México: Oxford University. Press.248 paginas

El telegrama: es un medio de comunicación entre dos personas, que consiste en él envió de información a través de hilos que trasmiten el mensaje en clave a Morse de una estación a otra, es decirla la persona que genera el mensaje (trasmisor) se dirige a una estación de radiotelegrafía solicitando a un operador enviar el mensaje (telegrama) y este se manda a otra estación distante para que lo reciban, el operador descifra y escribe la transmisión para dárselo a la persona (receptor) de dicho mensaje; la ventaja que tiene este medio es que la información viaja de manera rápida; la gran desventaja es que el costo del envió es por palabra y por ende es muy costoso.

La radio: Es un medio de comunicación que mediante la transmisión de ondas electromagnéticas permite el envío de información sonora y fue creado para comunicarse de manera masiva, este es un medio electrónico de comunicación en tiempo real que permite a cualquier persona recibir un mensaje contando siempre y cuando con un aparato de radio recepción; las ventajas es que el mensaje es transmitido en tiempo real, la desventaja es que si la comunidad no cuenta con antenas de trasmisión de radio, difícilmente podrán recibir su señal.

La televisión: Es un aparato que funciona con la fotoelectricidad, enviando audio e imagen a un aparato receptor denominado televisor, la ventaja de este medio electrónico de comunicación masiva es su transmisión en tiempo real, la desventaja es que el costo para difundir mensajes por este medio es sumamente alto.

El teléfono: Es un medio de comunicación que utiliza un aparato trasmisor y un receptor, que envía audio mediante una red de cableado o mediante el envío de paquetes de información vía satelital y esta señal permite enlazar y comunicar a dos o más personas situadas en diferentes lugares del mundo, la ventaja que brinda es una comunicación rápida a un costo relativamente bajo, la desventaja que presenta es que solo permite la comunicación con un número limitado de personas.

Para el caso de la entrega, distribución, expansión y acopio de la información el hombre creo diversas formas de comunicación escrita y electrónica, antes de la masificación del internet; destacando entre las escritas:

Periódico: Es un medio de información y comunicación escrita que se utilizó de manera constante antes de la aparición del internet; este consiste en la impresión en hojas de papel de las noticias e información relevante a nivel nacional e internacional y se distribuye de manera masiva; la ventaja que oferta este medio es el bajo costo de adquisición y distribución; la desventaja que presenta es la tardía actualización de noticias que maneja, esto debido a que solo se realiza su impresión al final del día.

Una vez que indicado la diversidad de medios para la trasmisión de información y conocimiento, debe señalarse la existencia de recintos de recopilación y consulta de documentos como la biblioteca. Que resguarda información en sus diversas formas de comunicación: hemeroteca; videoteca, fonoteca, y Fototeca, poniendo los documentos disponibles para su consulta al público en general; la ventaja de esta es el acceso abierto para poder consultar información, y la desventaja es la dificultad para poder localizar el material de consulta.

1.2 Origen

La idea de una red entre computadoras para permitir la comunicación y envió de información entre usuarios, se fue convirtiendo con el paso y desarrollo del mismo como una necesidad prioritaria. Esto se llevó a cabo mediante varios desarrollos, los cuales tuvieron como resultado la red de redes que conocemos como Internet.

“Internet es un conjunto de archivos interconectados mediante un sistema maestro de redes de cómputo. Teniendo como base dos funciones básicas: medio de comunicación y medio de información.”[2]

El proyecto inicial por el cual se dio origen a “Internet no se concibió como una red de sistemas de cómputo; más bien, debía satisfacer necesidades del Ministerio de Defensa de Estados

[2] Op.cit

Unidos de América. Para lograrlo, se necesitaba una red que no fuera dependiente de una sola computadora central. Esto es importante, pues el concepto original de red de computadoras exige una computadora central (servidor) que administre la información y esté al servicio de los usuarios, esté es el sistema de red de computadoras que los juristas veían habitualmente en los centros de trabajo antes de la aparición del internet."[3]

El proyecto inicial sentó las bases sobre el inicio de pruebas y diversos experimentos y mecanismos, que dieron origen al internet, sin embargo, durante el mismo proceso hubo errores y fallas.

"La primera persona que visualizó la futura existencia de la internet fue Nikola Tesla (1856-1943), quien predijo la existencia de un sistema energético de distribución mundial que permitiría conectar todas las estaciones telefónicas del mundo, la difusión mundial de información y noticias, correo y otros escritos, la reproducción y envío de fotografías e imágenes, la implantación de un sistema de difusión musical, la impresión a distancia y la implantación de un registro horario universal".[4]

Como se puede observar, los medios de comunicación se concentrarían en una forma única de mandar y recibir información a través de un solo medio y que a su vez podría tener la posibilidad de almacenar y consultar documentos de forma inmediata.

"Una de las influencias decisivas para el inicio del proyecto que a la postre tendría como fruto la creación de la internet fue Vannevar Bush, no sólo por sus ideas sobre el hipertexto, sino también por su labor política y científica, ya que promovió las relaciones entre el gobierno federal de los Estados Unidos, la comunidad científica norteamericana y los empresarios. Así, se crearon la Fundación nacional de la ciencia (NSF, National Science Foundation) y la Agencia de Proyectos avanzados de Investigación (ARPA, Advanced Research Projects Agency).

[3] Op.cit
[4] Casafranca, N. (Diciembre 3, 2016). *Historia del internet*. Marzo 2018, de LinkedIn Corporation Sitio web: https://www.slideshare.net/nicolecasafranca/historia-del-internet-69790623

En 1957, el gobierno de los Estados Unidos formó la agencia Advanced Research Projects Agency (ARPA), un segmento del Departamento de Defensa encargado de asegurar el liderazgo de los Estados Unidos en la ciencia y la tecnología con aplicaciones militares. El motivo fue el lanzamiento por parte de los soviéticos del satélite Sputnik que originó una crisis en la confianza americana. En 1969, ARPA estableció ARPANET, la red predecesora de Internet." [5]

"En enero de 1960 J.C.R. Licklider, comprendió la necesidad de una red mundial, según consta en su documento Man-Computer Symbiosis (Simbiosis Hombre-Computadora) en el cual indicó:

Una red de muchos [ordenadores], conectados mediante líneas de comunicación de banda ancha" las cuales proporcionan las funciones hoy existentes de las bibliotecas junto con anticipados avances en el guardado y adquisición de información y [otras] funciones simbióticas.

En octubre de 1962, Licklider fue nombrado jefe de la oficina de procesado de información DARPA, y empezó a formar un grupo informal dentro del DARPA del Departamento de Defensa de los Estados Unidos para investigaciones sobre ordenadores más avanzadas. Como parte del papel de la oficina de procesado de información, se instalaron tres terminales de redes: una para la System Development Corporation en Santa Monica, otra para el Proyecto Genie en la Universidad de California (Berkeley) y otra para el proyecto Multics en el Instituto Tecnológico de Massachusetts. La necesidad de Licklider de redes se haría evidente por los problemas que esto causó".[6]

Robert Taylor intentó hacer reales las ideas de Licklider sobre un sistema de redes interconectadas. Junto con Larry Roberts del MIT, inició un proyecto para empezar con una red similar. La primera conexión de ARPANET se estableció el 21 de noviembre de 1969, entre la Universidad de California, Los Ángeles y el Instituto de Investigaciones de Stanford. Antes del 5 de diciembre de 1969, se había formado una red de 4 nodos, añadiendo la Universidad de Utah

[5] Torres Saavedra, N. (Diciembre 13, 2015). *Historia del Internet*. Diciembre 2018, de blogspot.com Sitio web: http://comunicacioniccs.blogspot.com/2015/12/maria-jesus-lamarca-lapuente_90.html

[6] Duarte Galvis, D. (Junio 1, 2011). *Historia del Internet*. Diciembre 2019, de Blog de Duarte Galvis D Sitio web: https://sites.google.com/site/historiadelinternetbycarolina/j-c-r-licklider

y la Universidad de California, Santa Barbara. Usando ideas desarrolladas en la ALOHAnet, la ARPANET se inauguró en 1972 y creció rápidamente hasta el 1981. El número de hosts creció a 213, con uno nuevo añadiéndose aproximadamente cada 20 días.

ARPANET se convirtió en el núcleo de lo que posteriormente sería Internet, y también en una herramienta primaria en el desarrollo de la tecnología del momento. ARPANET evolucionó usando estándares del proceso RFC, aún usado actualmente para proponer y distribuir protocolos y sistemas de Internet. El RFC1, titulado "Host Software", fue escrito por Steve Crocker desde la Universidad de California, Los Ángeles, y publicado el 7 de abril de 1969." [7]

ARPANET es el nombre del proyecto de índole militar con el que se nombró a la primera red de computadoras construida, este proyecto fue la base sobre la cual se construyó un par de décadas después la internet.

"Los científicos del Ministerio de Defensa de Estados Unidos de América desarrollaron una red con las características mencionadas, la cual se puso en funcionamiento con el nombre de ARPANET."[8]

ARPANET es la primera base sólida sobre la que se inició el desarrollo del internet, este es la primera conexión entre computadoras que se tiene documentada y que resulto funcional arrojando con el pasar del tiempo como resultado que el ser humano visualizara y proyectara el impacto funcional y tecnológico que a la postre tendría este proyecto.

Sin embargo, el proyecto ARPANET tuvo un gran inconveniente, su desarrollo se llevó a cabo únicamente con fines militares situación que restringió su acceso y no permitió que este avanzara de la manera y con la velocidad necesaria, aun a pesar de esto el proyecto continuo durante las siguientes décadas con la firme ideología de ir enlazando cada vez más computadoras y mejorando la capacidad de almacenamiento y distribución de información en las mismas.

---

[7] Vega Cruz, A. (Noviembre 2007). *Introducción a las ciencias de la computación*. Diciembre 2018, de Blog de Vega Cruz Alejandra Sitio web:https://www.blogger.com/profile/08225975711776843269

[8] Op.cit

“Para el funcionamiento del sistema ARPANET fue necesario construir procesadores de mensaje de interfaz (IMP, Interface Message Processors), que debían funcionar como nodos en la red. El primer procesador de este tipo fue puesto en funcionamiento el 1 de agosto de 1969 en la Universidad de California en los Ángeles (UCLA), con una microcomputadora Honeywell 516 que tenía 12 KB de memoria, Pocas semanas después se instalaron IMP en el Stanford Research Institute en Menlo Park, California, en la Universidad de California en Santa Bárbara y en la Universidad de Utah en Salt Lake City. Cuando estos procesadores comenzaron a intercambiar paquetes de datos a larga distancia, ya había nacido ARPANET. En 1972 se habían instalado 37 IMP. El 1 de junio de 1990 se desinstaló ARPANET, lo que pasó inadvertido porque ya había en las grandes ciudades un número suficiente de proveedores de servicios de Internet.

ARPANET funcionó con un programa de computación especial denominado Network Control Protocol (NPC), que hizo posible el uso descentralizado de la red. Una gran ventaja que ofreció el NPC fue que trabajaba con diferentes tipos de computadoras y programas, lo que condujo a una expansión considerable de ARPANET. En la década de 1970, esta red creció más allá de sus objetivos originales de sistema de información del Ministerio de Defensa, debido a que varias redes científicas se enlazaron al sistema. Científicos y profesores de Estados Unidos de América comenzaron a considerar la posibilidad de transmitir mensajes electrónicos mediante la red para participar en el desarrollo de proyectos científicos.

En la década de 1980 el NPC fue sustituido por un programa nuevo llamado TCP/IP convierte los datos en pequeños paquetes, los envía a su lugar de destino con base en sus direcciones a través de diferentes puntos de enlace de Internet y la computadora de destino los recompone.

A principios de la década de 1980 Internet se separó de ARPANET, de tal forma se desligó de los objetivos militares y se expandió de una manera más rápida. Esto permitió que instituciones científicas tanto estadounidenses como extranjeras se enlazaran a Internet.

En 1986 se fundó la NSFNET. Financiada por el gobierno federal estadounidense, la NSFNET creó diferentes líneas de enlace para Internet, a las que se denominó backbones (espina dorsal), con

las que facilitaba la transferencia de datos. A partir de entonces, Internet inicio su expansión hacia el exterior de Estados Unidos de América, sobre todo hacia Europa." [9]

En 1993, la National Science Foundation crea INTERNIC (Internet Network Information Center), una especie de centro administrativo para Internet a fin de proveer acceso vía ftp, gopher, wais, e-mail y www, servicios de registro de dominios y un directorio de recursos de Internet.

Durante 1993 el número de servidores INTERNET sobrepasa los 2.000.000. También NSF patrocina la formación de una nueva organización, ínterNIC, creada para proporcionar servicios de registro en Internet y bases de datos de direcciones. En este año en el National Center for Supercomputing Aplications (NCSA), en la Universidad de Illinois, Mac Andreessen junto con un grupo de estudiantes crean un programa llamado Mosaic (Web Browser), el cual ganó fama rápidamente. Mac Andreessen, al poco tiempo, se alejó del NCSA y junto con Jim Clark (fundador y renunciante de Sylicon Graphics) fundan Netscape. Aparece la aplicación WinSock 1.1 estandarizando las posibilidades de aplicaciones Windows basadas en aplicaciones TCP/IP.

En 1994 David Filo y Jerry Yang crean el directorio-buscador de Internet YAHOO! (Yet Another Hierarchical Officious Oracle), sus tempranos esfuerzos por ofrecer una guía de navegación para acceder a los miles de sitios existentes en la red se verán coronados por éxito.

También en 1994 el número de servidores de Internet alcanza los 3.800.000. Las primeras tiendas Internet empiezan a aparecer junto con "emisores" de radio on-line. El conflicto potencial entre los internautas tradicionales y los nuevos usuarios se manifestó con fuertes protestas ante la aparición de publicidad en Internet, como avisos ostensibles en algunas páginas y el comienzo de lo que se conocerá como spam.

En 1995 hay más de 5 millones de servidores conectados a Internet. La espina dorsal de NSFNET (red académica de la National Science Foundation) empieza a ser sustituida por proveedores comerciales interconectados. La política de privatización de la NSF culmina con la eliminación de la financiación del backbone NSFNET. Los fondos así recuperados fueron redistribuidos

[9] Vega Cruz, A. (Noviembre 2007). *Introducción a las ciencias de la computación*. Diciembre 2018, de Blog de Vega Cruz Alejandra Sitio web:https://www.blogger.com/profile/08225975711776843269

competitivamente entre redes regionales para comprar conectividad de ámbito nacional a Internet a las ahora numerosas redes privadas de larga distancia.

Microsoft saca al mercado conjuntamente con su sistema operativo Windows 95 la primera versión del browser Internet Explorer 1.0, el cual da como pauta a la apertura total comercial del internet y se puede indicar que en este punto es donde inicia la era actual del internet.[10]

Hasta 1995, la NSFNET intentó imponer una política de uso aceptable (acceptable use politicy), con el fin de que Internet se tuviera solo con propósitos científicos, no comerciales. Sin embargo, dicha política fue puesta fuera de vigor a principio de 1995, cuando el gobierno estadounidense decidió privatizar y no otorgar más subsidios a Internet. Desde ese año es posible utilizar este sistema para objetivos de índole muy diversa, incluidos los de carácter comercial." [11]

El fin inicial del internet fue un tema militar que permitiría la integración, conjunción e intercambio de información entre diversas áreas gubernamentales para el mejor funcionamiento de las mismas, el experimento inicial visualizaba únicamente esta integración la cual fue modificada con el pasar del desarrollo del mismo y el análisis de los resultados.

Así se empezaron a realizar pruebas sobre el internet, los empresarios es decir el sector privado empezaron a visualizar los diversos beneficios y usos de esta red y se determinaron iniciar la apertura hacia su uso de manera en primera instancia en el sector privado y a la postre liberado de manera gradual al público en general.

Internet se convirtió en el proyecto militar más importante del siglo pasado, trayendo como resultado la consagración y realización de uno de los mayores sueños que hasta antes de la liberación de este parecía utópico, el cual fue interconectar a todo el mundo, a partir de la liberación del uso de internet de manera general se consagro este logro; ya que al día de hoy prácticamente todo el mundo está conectado y en uso constante e inclusivo adictivo a esta red.

---

[10] Para libros medios. (1998-2008). *Internet y la World Wide Web*. Agosto 2018, de Para libros medios Sitio web: http://www.paralibros.com/passim/p20-tec/pg2052ci.htm

[11] Op.cit

Internet se ha consolidado como el medio para concentrar y distribuir información de todas las partes del mundo, y ha logrado interconectar a prácticamente toda la población, es la vía idónea para realizar diversos procesos desde un mismo punto físico, facilitando procesos y minimizando los costos de estos.

1.3 Actualidad

En la actualidad internet es una herramienta que va creciendo y desarrollándose día a día a pasos agigantados, en retrospectiva si se observa en una forma comparativa con el ser humano, Internet hoy en día se asimila a un adolescente, esto debido a que aún está conociendo sus propios límites y con el porvenir de los siguientes años se estará encontrando poco a poco su madurez.

Internet actualmente se utiliza como medio de comunicación, de almacenamiento y distribución de información, pero esto es solo una parte mínima de lo que exponencialmente se podrá lograr en unos años obteniendo su máximo esplendor de sincronía o simbiosis ser humano- internet.

La actualidad del internet es promisoria, pero para poder validarlo a la fecha se debe segmentar en diversos ámbitos de la vida diaria, a saber:

En el ámbito financiero, tiene un impacto en el tema de los costos tanto para personas físicas como para personas morales, ya que conforme hay una mayor penetración en el uso del mismo, existen mayor cantidad de procesos que se deben ejecutar de manera virtual sin necesidad de la presencia física de una persona, por ejemplo, pago de servicios, o pago de impuestos.

En ámbito laboral, destaca un impacto en el tema de costos y tiempos de ejecución, operaciones que se hacían de manera física mediante el uso de internet ya se pueden realizar de manera remota, disminuyendo tiempos y costos, lo cual es fundamental para cualquier empresa.

Respecto al ámbito bancario, tiene un impacto de reducción de tiempos, ya que actualmente mediante el uso de internet se pueden realizar operaciones financieras desde cualquier punto que tenga acceso a internet y con el uso de un teléfono inteligente.

Destaca en el ámbito académico, el uso de internet, el cual ha creado un nuevo campo de oportunidades en cuanto a educación se refiere, ya que antes del uso del mismo únicamente se podían tener cursos de manera física y presencial en un aula determinada, y con el uso de este medio electrónica se pueden tomar y acreditar diversos cursos y grados escolares de manera remota con el simple uso de una computadora con conexión a internet.

Aun en el ámbito Social, el uso de internet ha creado nuevas formas de relaciones sociales que sirven para interconectar a la gente de una manera rápida y sencilla, rompiendo las barreras de la distancia, las cuales se pueden identificar de manera clara con la creación de las denominadas redes sociales.

"La Asociación Mexicana de Internet (AMIPCI) dio a conocer su estudio de Hábitos de los Usuarios de Internet en México 2014 que indica que el número de usuarios de internet en México creció a 51.2 millones de internautas, es decir, un 13% más, desde los 45.1 que existían el año anterior.

Este número de usuarios se encuentra distribuido por género en proporciones idénticas de 50%. Por rangos de edades, se observa una alta participación de población juvenil, con un 57% compuesto por población entre los 6 y 24 años; mientras el 52% fluctúa entre los 19 y 55 años.

Respecto al promedio de antigüedad de empleo de internet, el reporte indicó que entre el universo de usuarios es de 6.1 años. 10% tiene menos de dos años que se conectó por primera vez; un 28% lo hace desde entre dos a cinco años, y la mayoría (62%) tiene más de cinco años usando la red de redes.

La actividad que dio lugar al primer uso de internet entre la población analizada, es el correo electrónico con un 71%, seguido de la búsqueda de información (64%), el uso de redes sociales (40%) y el uso de videojuegos (25%). El tiempo promedio de conexión de los usuarios de internet es de cinco horas y 36 minutos al día, 26 minutos más que en 2013, detalló la asociación.

Llama la atención la proporción de los usuarios que se conecta en cualquier sitio, mediante dispositivos móviles, que se redujo de 48.7% del año pasado, a un 31% en 2014. Por el contrario, la escuela creció de 20.6% en 2013 a 34% este año.

Al medir el tipo de dispositivos empleados para la conexión, PC y Laptop siguen siendo el medio más común (59 y 57%, respectivamente), aunque el uso de teléfonos inteligentes alcanza ya casi a la mitad de los usuarios (49%), seguido de teléfonos celulares (27%), tabletas electrónicas (20%) y dispositivos móviles como el iPod o consolas de juego portátiles (18%).

Al medir el uso exclusivamente laboral, domina el correo electrónico con un 53%, seguido de las búsquedas de información con el 51, y el envío y recepción de documentos (44%).

La situación es diferente en el uso de internet en actividades recreativas, o de ocio, donde las redes sociales predominan entre las actividades de los usuarios (81%), relegando a las descargas de música a un lejano segundo lugar, con el 45%. La visita de portales noticiosos se queda en 43% y los juegos en línea en cuarto sitio con 26%."[12]

Las cifras citadas otorgadas por la AMIPCI (Asociación Mexicana de Internet) indican de manera fehaciente el constante crecimiento del uso de Internet y nos van conllevando a una notoria realidad en la cual ya estamos inmersos que se resume de manera simple en el sentido de que el ser humano tiene una tendencia hacia la necesidad de vivir en línea, es decir de vivir conectado de manera constante y casi total a la denominada red de redes. Por consiguiente, nosotros como estudiosos y profesionistas del Derecho, y necesitamos comenzar a entender este proceso y avance tecnológico como una constante que nos orilla a una la necesidad de estar actualizados día a día para poder ser los profesionistas que nuestra sociedad actual requiere.

Internet es y será durante los siguientes años, la manzana de la discordia del desarrollo humano porque, así como trae consigo progreso, avance tecnológico, y un sinfín de cosas positivas; también traerá en sentido negativo la creación de nuevos y más complejos Delitos Cibernéticos,

[12] Calderón, E. (Mayo 21, 2014). *Crece número de usuarios en internet*. Diciembre 2018, de E Logística, Revista Énfasis Sitio web: http://www.logisticamx.enfasis.com/notas/69665-crece-numero-usuarios-internet-mexico#

que serán el reto para todos aquellos profesionistas y estudiosos del Derecho deberán de enfrentar.

1.4 Beneficios Sociales del uso del internet

En la actualidad, el uso del internet conlleva un sinfín de beneficios sociales los cuales se pueden clasificar en dos grandes grupos, el primero de ellos será beneficios hacia los adolescentes los cuales sólo por citar algunos son los siguientes:

- "Facilita su proceso de socialización a través del uso de servicios como son los chats, juegos en red, participación en ciertas redes sociales, etcétera. De esta forma el menor se siente integrado en un grupo con el que se comunica y comparte inquietudes y aficiones.

- Facilita su acceso a la ciencia, y cultura favoreciendo y completando así su educación fuera del ámbito de la escuela.

- Facilita la realización de tareas escolares y trabajos personales potenciando su capacidad de búsqueda, análisis y toma de decisiones de forma individual.

- Facilita la realización de tareas escolares en grupo poniendo a su disposición herramientas colaborativas en línea.

- Facilita el proceso de aprendizaje a alumnos que padecen enfermedades de larga duración y que tiene que permanecer lejos de las aulas durante largos períodos de tiempo.

- Facilita el seguimiento por parte de los padres del proceso de enseñanza-aprendizaje de sus hijos. La labor tutorial se beneficia ya que la comunicación padres-tutor es más rápida y eficaz.

- Mejora los resultados académicos, según muestran estadísticas realizadas sobre estos temas."[13]

[13] Comic69. (Mayo 17, 2015). *El uso del internet*. Septiembre 2018, de Blog Comic69 Sitio web: https://elusodelinternet1.wordpress.com/2015/05/17/hola-mundo/

En el segundo grupo serán aquellos beneficios sociales que tienen para el individuo ya en edad adulta, los cuales por citar algunos son los siguientes:

- “Inmediatez de la información: Con los buscadores se puede tener acceso a la información en cuestión de segundos. No solamente para estar al día en las noticias, sino para consultar un tema específico.

- Masificación de contenido: Se consigue que un mayor número de personas lean un artículo y lo difundan. A su vez, permite generar campañas de solidaridad en masa y ayudar para una causa o fin benéfico.

- Se eliminan las barreras de tiempo y espacio, pues una persona que está en un lugar alejado, puede asistir a una clase en tiempo real que se dicta en otra parte del mundo.

- Ayudas didácticas: Se puede navegar por un sin número de páginas para practicar actividades educativas. Hoy en día se tiene acceso a millones de páginas web gratuitas para buscar recursos educativos. Esto aplica a varias profesiones en los campos de educación, medicina, arquitectura, ingeniería, etc. Incluso se realizan visitas virtuales a museos, monumentos, iglesias y hacer verdaderos tours a través de la tecnología.

- Con una buena guía del maestro, se apoya en la tecnología para estimular una nueva forma de aprendizaje.

- Interdisciplinariedad y personalización: Con el uso de la tecnología podemos elaborar proyectos colaborativos en línea donde se diseña material didáctico y trabajos en varias disciplinas a la vez.

- Interacción con una comunidad: A través de redes sociales, videoconferencias, chats o portales especializados se accede a debates, comentarios, opiniones, fotos, videos de otras personas y tener una comunicación sincrónica o asincrónica.

- Mayor contacto con personas afines ya sea en fines profesionales o personales, el internet permite tener una mejor comunicación con personas de todo el mundo. "[14]

Todos estos beneficios son parte del desarrollo contemporáneo del internet, ya que el mismo tiene una interferencia medular en el desarrollo y accionar del ser humano en el día a día. Sin embargo, son innumerables la cantidad de beneficios a mediano y largo plazo, debido a que un sinfín de personas están trabajando día a día en encontrar nuevas formas de uso del internet.

Por tanto, como seres humanos disfrutaremos de todos los beneficios de aprender y actualizarnos día a día en el mismo progreso y uso del internet, en el entendido que, de no aprovechar estos avances, estaríamos quedando obsoletos para el desarrollo de nuestras actividades diarias, ya sea como empleado de una oficina o prestador de servicios que requiera el uso de internet o manejo de aplicaciones en función de su desempeño laboral.

Sin embargo, se debe de estar en constante capacitación y actualización en el uso de internet, para poder aprovechar al máximo este fin de oportunidades.

1.5 Riesgos del uso del internet

Como se ha mencionado, el internet conlleva de manera real a un sinfín de beneficios sociales, sin embargo, a la par de estos también tiene diversos tipos de riesgos, los cuales se pueden clasificar de la siguiente manera:

Relativos al tipo y acceso a la información

El usuario tiene disponible grandes volúmenes de información de diversos temas, sin ningún tipo de clasificación y control de acceso la mayor parte de las veces. Esto favorece el camino a la información con contenidos violentos, xenófobos, prácticas religiosas, delincuenciales, pornográficas, o relacionados con el ciberbullying, esto solo por mencionar algunos ejemplos, lo cual ha tenido como consecuencia la desviación social del usuario, es decir, empezar a tener

[14] Rodríguez, S. (Agosto 2014). *Internet ventajas vs desventajas*. Diciembre 2018, de blog de Rodríguez Stefani Sitio web: http://523634635.blogspot.com/2014/08/la-evolucion-y-el-acceso-hacen-que.html#comment-form

conductas asociales, para sociales o en el peor de los casos antisociales. Situación que debe ser tomada con la seriedad debida por la sociedad

Un individuo que accede al internet, puede si así lo desea encontrar información e indicaciones precisas de cómo construir una bomba, realizar un fraude o ingresar a una secta, imagínense toda esta información en manos de una persona menor de edad o un adolescente que enganchado por la mentira y la atracción de contenidos, genere peligro para él o su familia o de un sujeto que atraviesa por una crisis emocional o una depresión.

Relativos a relaciones personales

El Internet favorece las relaciones interpersonales ya que acerca a los individuos, aunque de forma telemática (datos a través del teléfono). Pero esto, en sí mismo entraña un riesgo ya que el usuario puede falsear la realidad y mostrarse a los demás de una forma diferente a como es en realidad, e incluso simular su identidad.

Por otra parte, Internet puede favorecer el aislamiento. El menor con problemas de socialización puede encerrarse en sí mismo, ya que al disponer de una herramienta que le abre las puertas al mundo no necesita la comunicación directa con los demás.

"Así mismo, Internet también puede producir peligrosas adicciones, como son los juegos de red, las redes sociales, los chats, participación en subastas, juegos de azar, etcétera".[15]

Este tipo de riesgos pueden detonar y tener como resultado la comisión de diversos delitos, como crear un perfil falso para contactar con un grupo social en el cual el usuario no puede ingresar, ya sea por edad, género o estereotipo físico, imaginen ustedes un hombre de edad avanzada mediante un perfil falso en una red social contactando mujeres que sean menores de edad.

Relativos al propio funcionamiento de Internet

[15] Comic69. (Mayo 17, 2015). *El uso del internet*. Septiembre 2018, de Blog Comic69 Sitio web: https://elusodelinternet1.wordpress.com/2015/05/17/hola-mundo/

“Existen también riesgos derivados de la propia red. En Internet continuamente se producen situaciones de riesgo derivadas de la tecnología utilizada. Los temibles virus, gusanos, puertas traseras, que pueden producir grandes daños a nuestros ordenadores domésticos."[16]

Este tipo de riesgos se dan mediante la creación de páginas apócrifas, o por mensajes de correo electrónico, o ventanas emergentes en el cual comunican que el usuario en ese momento, fue acreedor a algún tipo de premio, en ese momento nosotros aceptamos o damos click y termina por descargar en nuestro equipo un virus que en el menor de los casos solo alentará nuestro equipo y en el peor de los casos accederán de manera remota a toda la información que tengamos guardada dentro del mismo.

Este riesgo se puede ejemplificar con la recepción de un correo que llega de un remitente desconocido y que en el momento de abrirlo contenga un mensaje que indica que se ganó un viaje, dinero o su banco le condono su deuda y se debe de dar click en el enlace, y al darle click, este inicia la instalación de un virus dentro de nuestra computadora, lo cual le permite acceso a nuestra información a la persona que envió dicho correo.

Relativos a temas económicos

“Muchos usuarios no son conscientes de la conexión a determinadas páginas web requiere facilitar datos que pueden constituir un gasto importante. Además, están las compras de naturaleza oscura, engaños, negocios ilegales, solo por mencionar algunos ejemplos. Existe un abanico muy amplio de opciones en la red que puede suponer un engaño y éste nos afecte económicamente.” [17]

Este tipo de riesgos se magnifica si se considera que actualmente existen diversos hackers (personas expertas en el conocimiento de informática o la que descubre debilidades de una red informática) que utilizan páginas apócrifas para obtener información financiera de los usuarios,

[16] Comic69. (Mayo 17, 2015). *El uso del internet*. Septiembre 2018, de Blog Comic69 Sitio web: https://elusodelinternet1.wordpress.com/2015/05/17/hola-mundo/

[17] Comic69. (Mayo 17, 2015). *El uso del internet*. Septiembre 2018, de Blog Comic69 Sitio web: https://elusodelinternet1.wordpress.com/2015/05/17/hola-mundo/
https://elusodelinternet1.wordpress.com/

por citar un ejemplo: Digamos que en el buscador web, se pone el nombre de una empresa de venta de productos, una vez que busca la información el buscador despliega en la parte inferior, más de cinco páginas con el mismo nombre de aquella que se buscaba, y se ingresa a una de ellas para realizar una compra, sin percatarse que esta no es la página oficial de la tienda o producto, sino una réplica de la misma, subida a la red por un hacker y al realizar la compra se llenan todo los campos con los datos de la tarjeta de crédito, situación que tendrá como consecuencia que un tercero sin autorización tendrá todos los datos de la tarjeta y podrá en un futuro realizar cargos sin que se reconozcan los mismos.

Este tipo de riesgos es latente en los usuarios de servicios en línea que utilizan páginas de internet para realizar servicios financieros o para la prestación de un servicio de entretenimiento o comunicación.

Relativos a comisión de delitos en línea

Por otra parte, muchos usuarios tampoco son conscientes del tema de las descargas ilegales ya sea de películas, libros, juegos o música, sin darse cuenta de que están cometiendo un delito el cual tiene consecuencias jurídicas, debido a que esto es solo la punta del iceberg.

Las descargas ilegales es una situación que atañe sobre todo a los jóvenes, ya que están acostumbrados a pasar mucho tiempo en la red y la gran mayoría de ellos no cuentan con los recursos para poder comprar material en línea, por tanto, si ellos desean ver una película estando en la red, ellos buscan la forma de descargar en una página de manera ilegal, sin que puedan comprender el alcance y consecuencias jurídicas que implica este tipo de decisiones.

En este primer capítulo, se realizó un análisis general de aquello que es el internet, no sin mediar que este análisis es superficial derivado de que internet es el sistema de información más complejo creado por el hombre, por consiguiente para desmenuzar cada uno de los detalles de este tema sería necesario realizar una investigación enfocado únicamente en este tema, en este sentido se indicó de manera global los lineamientos generales sobre los cuales se constituyó el mismo y las primeras reacciones derivados durante la creación del mismo.

En una segunda parte sobre este mismo primer capítulo enuncio lo que a mi parecer son los puntos importantes a tener en cuenta derivado del uso de internet tanto en el aspecto positivo como en el aspecto negativo, buscando dar una guía general que permita al lector de este trabajo entender que internet es la herramienta de comunicación y almacenamiento de información más importante creada por el hombre, y por tanto para poder hacer uso del mismo se deberá de tener un conocimiento previo sobre lo positivo y negativo para evitar tener consecuencias mediante su uso, es de importancia leerlo de manera analítica para poder entender y permearse de cada uno de los puntos que conlleva el uso del mismo. Así mismo cabe resaltar que internet es una herramienta que sufre de una evolución constante, en palabras simples lo que hoy se conoce del mismo en un par de meses comienza un proceso de obsoletismo.

Sin embargo, estos aspectos que se tratan en este primer capítulo son únicamente definiciones y temas de carácter general, que servirán para tener una base de evaluación y entendimiento sobre los alcances que el uso de internet da a la vida cotidiana, permitiendo entender que esta figura paso de ser un proyecto en desarrollo de nivel gubernamental a una herramienta global, la cual hoy día rige la manera de comunicarnos, informarnos, aprender, interactuar y un sinfín de cosas más.

Todas estas aristas que plantea el uso de internet serán analizadas de manera individual enfocándome de manera especial en cada uno de los delitos que se presentan con el uso del internet, es decir, los denominados delitos cibernéticos.

Capítulo dos: Delitos cibernéticos

2.1 Antecedentes

"La noción de digital, data de alrededor del año 1860. Los primeros cables que transmitían los mensajes en clave Morse utilizando puntos y rayas, presentaba la dificultad de que la señal llegaba a destino debilitada y distorsionada, por lo que él que debía codificar el mensaje se enfrentaba, a menudo, a un grave problema en la comunicación. Como consecuencia de este inconveniente, en las líneas submarinas empezó a usarse un código denominado *cable code.* Este consistía en que el operador del cable debía manipular un interruptor funcionaba como puente para posibilitar que el cable se conectara al polo negativo o al positivo de una batería, obteniendo así un punto o una raya respectivamente" [18]

Este sistema utilizó un principio similar al que actualmente utilizan las computadoras y las telecomunicaciones, es decir, *una convención binaria.*

Justo en este punto de la historia el ser humano empezó a entender que existía más de una forma de comunicación escrita y oral, que eran las que se conocían hasta esa época. Sin embargo, el uso de la clave Morse, y los diferentes códigos desarrollados a raíz del descubrimiento de la misma, fueron la base para iniciar con la era digital, teniendo como resultado nuevos usos de comunicación iniciando con él envió de información a través de diversos códigos, terminando con las nuevas vías de comunicación como las computadoras, los correos electrónicos, y el uso de teléfonos inteligentes.

Pero este tipo de avances son enunciativos más no limitativos, es decir el nivel exponencial de cambios que se avecinan con el desarrollo de la tecnología es inimaginable, se está en un punto de avance constante, que tendrá como consecuencia el desarrollo de nuevas formas de comunicación.

[18] Reggini Horacio, C. (1996). *Los caminos de la palabra: Las telecomunicaciones de morse a Internet*. Buenos Aires: Galápagos.248 páginas.

"Históricamente, el ser humano ha adoptado una actitud egocéntrica frente al mundo, con una permanente y sistemática resistencia al cambio. Así, por ejemplo, Galileo Galilei llego a sufrir tortura para que modificara su visión de que la Tierra no era el centro del universo. También Darwin fue objeto de persecuciones por sostener que el hombre descendía del mono. En el siglo XX se ha evidenciado la resistencia a máquinas y artefactos creados por el hombre, por la creencia de que puedan superarlo en algunos aspectos".[19]

Se puede observar que en los años sesentas los contenidos escritos, audiovisuales y cinematográficos tenían relatos de ficción, en donde el ser humano era virtualmente oprimido por su propia creación. Notando en la sociedad un claro cambio en el uso y aplicación de la tecnología, pero también en el remplazo del hombre por la máquina.

El ser humano de manera sistemática e inconsciente, desarrolla un complejo para manejar los cambios, esto debido a diversos miedos pero existe uno en específico que se trata de los derivados por avances tecnológicos, este miedo nace de la idea de perder terreno y valor contra la tecnología, esto es, un maquilador tiene miedo de ser sustituido por los avances tecnológico, y se crea que una máquina puede despojarle de su empleo o en su defecto que el ingreso de esta maquinaria en la fábrica, generará la necesidad de capacitarse.

"El surgimiento de la era digital ha suscitado la necesidad de repensar importantes aspectos relativos a la organización social, la democracia, la tecnología, la privacidad, la libertad, y se observa que muchos enfoques no presentan la complejidad teórica que semejantes problemas requieren; se esterilizan obnubilados por la retórica, la ideología y la ingenuidad."[20]

La era digital ha venido a romper los paradigmas culturales y tecnológicos que se creyeron imposibles de romper. Así hace apenas cien años era absolutamente irrisorio de visualizar en

[19] Sarra, A. (2001). *Comercio Electrónico y derecho*. Buenos Aires: Astrea.pp.120

[20] Rodotá, S. (Mayo 8, 1998). *Libertà, opportunità, democrazia, informazione*. Internete privacy:qualiregole?, Supplemento n. 1al Bollettino n. 5.Presidenza del Consiglio dei Ministridipartimento per l'informazione e l'editor. pp.202.

ese contexto, sin embargo, actualmente se puede y debe entender que todo aquello que se deba por correcto puede ser cambiado con la evolución tecnológica.

"Cada vez que apareció una nueva tecnología, se presentó la necesidad de agrupar su problemática en derredor de un corpus cognoscitivo especifico"[21]. De manera ineludible la sociedad humana va evolucionando en cada uno de los ámbitos en que se desenvuelven, y el internet es sin duda es el mayor ejemplo de avance vertiginoso que ha tenido el ser humano en el último siglo.

Esto ha tenido como consecuencia la necesidad de la actualización de la norma jurídica al contexto actual e inclusive en algunos casos específicos la generación de nuevas ramas del derecho. Internet es una red internacional de computadoras interconectadas, que permite comunicarse entre sí a decenas de millones de personas, así como acceder a una inmensa cantidad de información de todo el mundo.

Pueden observarse algunas características jurídicamente relevantes:

- Es una red abierta, puesto que cualquiera puede acceder a ella;

- Es interactiva, ya que el usuario genera datos, navega y establece relaciones;

- Es internacional, en el sentido que permite trascender las barreras internacionales

- Hay una multiplicidad de operadores;

- Tiene una configuración de sistema autorreferente, y por ello carece de un centro que pueda ser denominado "autoridad"; opera descentralizada mente y construye el orden a partir de las reglas del caos;

- Tiene aptitud para generar sus propias reglas sobre la base de la costumbre;

- Muestra una aceleración del tiempo histórico;

[21] Lorenzetti, R. (2001). *Comercio Electrónico*. Buenos Aires: Abeledo-Perrot. pp. 9-10.

- Permite una comunicación en "tiempo real" y una "desterritorialización" en las relaciones jurídicas;

- Disminuye drásticamente los costos de transacción."[22]

"La vida digitalizada nos hará cada vez más independientes del hecho de tener que estar en un lugar específico, en un momento determinado. Incluso, la misma transmisión de lugares geográficos pronto comenzara a ser posible."[23]

El paradigma de lo digital

"A menudo se escucha hablar de "digital" o "digitalizar" e incluso mencionamos estos términos con frecuencia; es probable que en esas ocasiones no se sepa exactamente a que se están refiriendo. El vocablo "digital" hace referencia a "dígito" o "número" y es la manera de representar información (de cualquier especie) numéricamente, en anotación binaria, es decir, mediante ceros y unos, El *bit* es la partícula mínima de la información. Digitalizar significa traducir señales de texto, imágenes, sonido o video a lenguaje binario o *bits,* que cuando se reproducen a gran velocidad, se obtiene una réplica, en apariencia, exacta al original. La digitalización permite la comprensión y transmisión de gran cantidad de información a bajo costo, con alta fidelidad (debido a la posibilidad de corrección de errores que esta permite) y a una gran velocidad."[24]

El ser humano se encuentra en una etapa de evolución que está teniendo como resultado la necesidad de migrar a una era digital, la cual está comenzando a eliminar procesos, métodos y conceptos ligados a épocas anteriores a esta era digital teniendo como resultado la eliminación de tabúes; esto es necesario debido a que en el contexto actual en el que vivimos es necesario

[22] Op.cit.
[23] Op.cit.
[24] Codina, L. (Abril 1996). *Negroponte, medios de comunicación y cuñadas digitales*. Septiembre 2018, de El profesional de la Información. Revista científica y profesional Sitio web: http://www.elprofesionaldelainformacion.com/contenidos/1996/abril/negroponte_medios_de_comunicacin_y_cuadas_digitales.html

una mayor velocidad en la elaboración de operaciones, procesos, transportación de información, manejo de datos solo por citar algunos ejemplos.

"La tecnología es la llave de la culminación exitosa de la infraestructura de la información y también es la tecnología que reinventará la manera en que la gente vivirá, trabajará y se divertirá…La digitalización consumará el casamiento de la televisión, las computadoras y el teléfono, haciendo posible la comunicación con cualquiera, en cualquier lugar y en cualquier momento"[25]

El fin primordial del uso de la tecnología para el ser humano es el mejoramiento de su calidad de vida, situación que ha sido exitosa con el avance que la misma ha presentado al día de hoy, por ejemplo, el ser humano puede estar conectado casi de manera permanente si así lo desea desde cualquier lugar, es decir una persona hoy puede ir de vacaciones a acampar y tener un teléfono móvil, una laptop o quizá una Tablet y estar conectado desde donde este acampando, hacer llamadas, ver la tv, escuchar noticias e inclusive si así lo desea trabajar.

"Las multinacionales están creando redes que escapan del marco de la nación – Estado… Hacia la mitad del próximo siglo, naciones- Estado como Alemania, Italia, Estados Unidos o Japón ya no serán las entidades socioeconómicas más relevantes y la configuración política definitiva. En su lugar áreas como el condado californiano de Orange, Osaka en Japón, la región de Lyon en Francia o la Ruhrgebiete alemana adquirirán un rango socioeconómico predominante."[26]

Esta revolución digital y de tecnología, tendrá como parte de los cambios una reestructuración social, económica, política y territorial, solo por mencionar algunas, es decir a mayor avance y desarrollo tecnológico, mayor será el reordenamiento de las estructuras sociales que conocemos hoy día.

"El efecto amortizador de la digitalización ya se está haciendo sentir. Disciplinas y empresas que antes estaban en todo separadas, comienzan a elaborar entre si un lugar de competir. Está

[25] Naisbitt, J. (1995*). Global Paradox*. E.U.A.: Avon Books.p.61.
[26] Toffler, T. (1994). *Las guerras del futuro: La supervivencia en el alba del siglo XXI*. España. p.338.

apareciendo un lenguaje común, antes inexistente, que permite a la gente más allá de toda frontera interactuar. Pero, ante todo, mi optimismo nace de la naturaleza motivadora de estar digitalizado. El acceso la movilidad y la habilidad para efectuar cambios son lo que hará que el futuro sea tan diferente al presente"[27]

El ser humano está entrando en un proceso de globalización que está cambiando los paradigmas con que se desenvolvía hasta hoy, esta globalización es el primer paso hacia un proceso de eliminación de las barreras de territorio, jurisdicción, lenguaje, comerciales y esto solo por citar algunos ejemplos; lo cual permite visualizar un futuro diferente en donde el ser humano como individuo y como parte activa de la sociedad, podrá interactuar de una manera libre.

"En este presente que parece futuro en el que la hiperconexión, la hipercomunicación y el conocimiento aparecen como fundamentos, pareciera que uno de los mayores beneficios que ofrece la tecnología es la libertad relativa que pueden tener las personas, porque en un mundo telecomunicado digitalmente los individuos serán libres de trabajar en cualquier lugar del planeta, dado que sus computadoras y sus recursos de interconexión personal les permitirán estar en contacto con su estudio, oficina fábrica o negocio, cualquiera sea el lugar en donde estén."[28]

Estas características mencionadas anteriormente indican de manera enunciativa, más no limitativa, algunos de los puntos importantes a considerar en cuanto al uso e intervención del internet en el ámbito jurídico.

Visualizar de manera general la inmensidad del internet y la inmensidad de ilícitos que se pueden cometer con el uso de estas nuevas tecnologías; es sumamente abierto debido a que,

---

[27] Codina, L. (Abril 1996). *Negroponte, medios de comunicación y cuñadas digitales*. Septiembre 2018, de El profesional de la Información. Revista científica y profesional Sitio web: http://www.elprofesionaldelainformacion.com/contenidos/1996/abril/negroponte_medios_de_comunicacin_y_cuadas_digitales.html

[28] Op.cit.

ante cada actualización tecnológica, cada tecnología, cada software, y cada avance derivado de estos supondrá nuevas formas y oportunidades de delinquir.

Dando como resultado un sinfín de variables y resultados diversos; generando la necesidad de renovar, actualizar y definir conceptos ya establecidos o generando conceptos nuevos, imaginemos que una persona realiza un ilícito desde un país Europeo y la persona afectada por dicho ilícito podría estar en un país de América, situación que genera diversos temas a tratar tanto para el juzgador como para la defensa del juzgado como lo es la jurisdicción, la territorialidad, tiempo, modo o lugar solo por citar un ejemplo.

Los delitos cibernéticos son una nueva forma de delinquir y son el futuro inmediato hacia las formas en que el ser humano atentará contra sí mismo, esto debido a que mientras mayor sea la migración de la información hacia la red, mayor será la cantidad de riesgo y tentación que generara el cometer estos ilícitos, es como el tema de las operaciones bancarias. Hoy en día se está en un proceso de migración donde la mayoría de las operaciones bancarias se busca ser realice mediante el uso de la red denominada internet, esto debido al ahorro de tiempo y al ahorro de costos que este tipo de cambios conlleva.

2.2 Elementos Jurídicos del Delito Cibernético

"El carácter abierto, interactivo, global del Internet, sumado a los bajos costos de transacción que presenta como tecnología, produce un gran impacto en la dogmática: las nociones de tiempo, espacio, frontera estatal, lugar, privacidad, bienes públicos y otras."[29]

"El impacto de la tecnología digital se estudia solo cuando se logra la separación de los siguientes puntos.

Desterritorialización y espacio virtual: Existe un nuevo espacio: el cibernético ("ciberespacio"[30]), distinto del espacio físico, con una arquitectura especializada en la maleabilidad, puesto que cualquiera puede redefinir códigos e interactuar en él (The Harvard Law Review Association. Mayo

[29] Op.cit.
[30] El término proviene del inglés; ha sido tomado de una novela, *Neuromancer*, de William Gibson, de 1984, y se ha difundido ampliamente.

1999), lo que lo convierte en un objeto inasible y renuente a las reglas legales que toman en cuenta este elemento para decidir numerosos aspectos jurídicos.

Este ciberespacio es *autónomo*, en el sentido que funciona según las reglas de un sistema autorreferente[31]. Es *pos orgánico*, ya que no está formado por átomos ni sigue las reglas de funcionamiento y localización del mundo orgánico: se trata de bits. Tiene una naturaleza no territorial y comunicativa, un *espacio-movimiento*, en el cual todo cambia respecto de todo, es decir que el "espacio virtual" no es siquiera asimilable al espacio real, porque no está fijo; no es localizable mediante pruebas empíricas." [32]

El ciberespacio abre debates acerca de cómo manejar jurídicamente toda aquella acción realizada mediante el uso del internet, al no existir un espacio físico determinado en la realización de cualquier acción mediante el uso del mismo, esto tiene como consecuencia que en la comisión de un delito se difiera donde se originó el mismo, cuál sería la norma jurídica aplicable y como poder fijar la jurisdicción dela comisión del mismo.

Esta adversidad trae como consecuencia la necesidad imperiosa por parte de los juristas de la actualización de los diversos sistemas jurídicos aplicables, ya que el derecho es una ciencia que necesita desarrollarse día a día de manera urgente debido a que la norma aplicable en un contexto de tiempo y espacio diferente al actual queda de manera ineludible obsoleta al avanzar la tecnología, al desarrollarse nuevas formas de gobierno, y a la avanzada manera de la sociedad en la que el jurista se desenvuelve.

"Tiempo Virtual: una de las características actuales es la aceleración del tiempo histórico. Se ha comparado el tiempo transcurrido desde el descubrimiento de distintas tecnologías hasta su difusión masiva, con los siguientes resultados aproximados: 112 años para la fotografía, 56 para el teléfono, 35 para la radio, 15 para el radar, 12 para la televisión, 5 para el transistor, 3 para el circuito integrado. También se ha analizado la velocidad que imprime cada tecnología en el

[31] Lo que define un sistema es una organización autorreferente de elementos interrelacionados de un modo autónomo; la autorreferencia, la autoorganización y la homeostasis son características del sistema, en el sentido de que su orden es interno es generado a partir de la interacción de sus propios elementos; que se reproducen así mismos, son funcionalmente diferenciados y buscan una estabilidad dinámica.
[32] Op.cit

transporte de personas y de información, de la siguiente manera: en 6000 a.C., el vehículo más rápido era el camello, que se movía a una velocidad media de 12 km por hora; en 1600 a.C. con el carro, esta aumento a 30 km por hora, casi 3500 años más tarde, en 1784, la primera diligencia postal entro en operación en Inglaterra a razón de 15 km por hora; la locomotora en 1825, tuvo una velocidad de 18 km, y en 1880, la locomotora de vapor alcanzó 180 km por hora, en 1938, los aviones comenzaron a desarrollar velocidades cada vez mayores, que se fueron duplicaron cada década, hasta llegar al cohete y la nave espacial.

Este fenómeno hace que el presente se torne "omnipresente" y que la dimensión del futuro o pasado se adelgacen.

El tiempo virtual, al igual que el espacio, se divorció de las categorías comunitarias y naturales que configuraron el tiempo real. El día y la noche definieron el tiempo para el trabajo y el descanso, pero ahora se trabaja en lugares cerrados, frente a computadoras, sin que importe si es de día o de noche".[33]

El tiempo virtual es una nueva tendencia surgida por la evolución de la tecnología, refiere al tiempo que se dedica mediante el uso de nuevas tecnologías para tener contacto con amigos, familiares y diversas personas, es el tiempo que no se trasmite a una persona mediante el contacto físico y el estar ambos en el mismo lugar, sino estando ambos en dos puntos físicos diferentes, esto se detona por la falta de tiempo real por cuestiones de trabajo, de tráfico, y/o de las diversidades actividades que realizamos en el día, un ejemplo claro de este es el tiempo que brindamos mediante aplicaciones o redes sociales y esto se realiza mediante celular, computadora o videojuegos para poder hablar con alguien.

"El domicilio privado: Las relaciones jurídicas efectuadas por medios electrónicos pueden plantear serios problemas para determinar donde se realizan; por ejemplo un ingeniero que está en Argentina desarrolla un proyecto, supervisado por una empresa germana de ingeniería, situada en Alemania, conectados ambos con una computadora en los Estados Unidos, donde se

[33] Op.cit.

están diseñando una máquina para ser enviada a la India."[34] En el campo del consumo, el usuario del Internet puede emitir declaraciones de voluntad desde una computadora, la que puede estar ubicada en un sitio diferente a su lugar de residencia o de trabajo, o bien estar en movimiento, cuando, por ejemplo, se envía un e-mail desde un aeropuerto o desde un tren." [35]

Actualmente se genera una desterritorialización para el sujeto activo que ejercita una acción en dos o más países dando como resultado una dificultad para definir de manera objetiva para el juzgador ¿En qué territorio se realizó el acontecimiento?, ¿Dónde inicio la misma?, ¿Dónde terminó la acción?, ¿En cuántos países se realizaron los hechos o actos jurídicos?, ¿Cuántos países intervienen en el resultado de la acción?, esto solo por mencionar algunas de las interrogantes que surgen. Esta situación genera la necesidad de una mayor especialización por parte de la comunidad que interviene dentro de la elaboración de las leyes de una nación, los cuales deben de estar en constante actualización entendiendo como una prioridad imperante que conforme se va realizando una mayor evolución tecnológica, la ley tiene que evolucionar de la mano de la misma.

"Barreras nacionales frente a la tecnología global: La evolución de las tecnologías de la comunicación muestra un ascenso hacia un status global, que fue incipiente con el surgimiento del correo, aumento con el teléfono y la televisión y alcanza un estado superior con Internet, que permite a los sujetos comunicarse entre sí, sin que se sienta una presencia del Estado nacional y su sistema regulatorio."[36]

El avance constante y vertiginoso de la tecnología durante los últimos cincuenta años ha tenido como resultado que en algunos puntos se ha sobrepasado la capacidad del estado como ente regulador, por citar solo un ejemplo hoy se pueden realizar una compra de una computadora en línea en México de origen Chino mediante una compañía Estadounidense, en este caso las barreras nacionales han sido traspasadas por el avance de la tecnología global, ya que para todo este proceso el Estado ha sido un sujeto inactivo que no tuvo participación.

---

[34] Greco, M. (2000). *Internet e Direito*. Sao Paulo: Dialéctica.2nda.ed.
[35] Op.cit
[36] Op.cit.

“Privatización del tiempo y el espacio comunitarios: Se ha señalado que una de las características de la tecnología es su potencialidad para afectar la noción jurídica de espacio y tiempo. Así frente a una tecnología típicamente posmoderna, en el sentido de que puesta en mano de un sujeto cada vez más individualista, es usada de modo heterogéneo y fractura algunos aspectos importantes de la regulación que se basa en presupuestos comunitarios.

En este contexto reina el pluralismo y la diferencia.

La categoría de espacio-tiempo se configuraba a partir de la imposición del mundo natural, el hombre acomodaba su tiempo a fronteras que él no había creado: el día y la noche. Actualmente puede crearlas y con ello, afectar categorías comunitarias sobre las cuales se basa el derecho.

Lo que permite la tecnología ahora es la violación privada, silenciosa, de las categorías generales.”[37]

La tecnología genera una ola de cambios constantes y necesarios, derivados de la misma, esto hace que el ser humano en ocasiones casi de manera imperceptible realice cambios en su forma de contextualizar sus acciones, esto se debe a que el uso del internet permite romper diversas barreras como el tiempo y el espacio comunitario.

Esto por ejemplo sucede cuando un contribuyente puede realizar la presentación de su declaración de impuestos desde su casa mediante una computadora utilizando el internet, siendo un cambio radical que realiza de manera casi imperceptible y que varía la forma en que se maneja el concepto del tiempo ya que aun a pesar de que el horario de la oficina de la Secretaria de Administración Tributaria (SAT) haya concluido, el sujeto podrá presentar fuera de este horario su declaración.

“Segmentación de conceptos generales: El legislador y el juez utilizan conceptos generales que se adaptan al caso concreto, tomando en cuenta las costumbres de cada región geográfica y de cada tiempo histórico. Esta práctica puede enfrentar problemas serios en Internet: declarar la

[37] Op.cit

ilicitud de la pornografía es una tarea ardua, puesto que el estándar es diferente en una dimensión trasnacional; de tal modo, lo que sería pornográfico en países de cultura Islámica no lo seria en la Argentina o en Holanda.

La cláusula general es una norma de sentido genérico, no específico, cuyo contenido debe ser precisado por el juez según la evolución de la conciencia social; es una medida, una directiva para la decisión, un modelo decisional preconstituido por una *fattispecie (figura)* normativa abstracta (Mengoni.1986). Son clausulas generales la buena fe, la equivalencia de las prestaciones, los motivos justos, el uso regular, la emergencia económica y muchas otras que el legislador de todas las latitudes utiliza frecuentemente."[38]

Con la explosión masiva en el uso del internet se necesita realizar constantes actualizaciones a los conceptos que sirven de base para la norma jurídica porque para adaptar los mismos a un caso concreto se requiere un análisis profundo debido a que aquello que es permitido en un país puede ser prohibido en otro y en el caso concreto de México recae en la interpretación del Juez para dictar sentencia.

Por lo tanto, mientras menor sea la actualización y especialización de conceptos que sirven de base para la norma, mayor será el margen de interpretación del juez, teniendo como consecuencia un mayor grado de ambigüedad en la determinación de sentencias, debido a que dos casos iguales sentenciados por diferente juez pueden tener sentencias encontradas.

"Lo anterior, permite vincular el espacio e imputabilidad: hacia la abstracción de las tecnologías jurídicas. En tal virtud, es posible que algunas reglas de derecho de las opciones reales de espacio y tiempo, aceptando otras de carácter ficticio, siendo así factible la abstracción

La posibilidad existe, ya que hubo una época en la que el derecho creo los "títulos valores", a las cuales les otorgo características especiales: abstracción e independencia de la causa que les dio origen, autosuficiencia en el sentido de que se bastan así mismos, crenado una ficción jurídica.

[38] Op.cit.

En numerosos aspectos, puede llegar un momento en que se prescinda del espacio y tiempo reales y se les sustituya por otras categorías. Así en los contratos, lo que interesa verdaderamente es que haya una manera segura de imputar efectos jurídicos al acuerdo de voluntades y no determinar si alguien vive en ese lugar, o si estuvo en el para la celebración o el cumplimiento; en la web hay y habrá muchas maneras de cumplir con ese requisito.

El lugar "jurídico" puede ser un nombre de dominio, que no coincida con el "lugar real" donde esté efectivamente situado el sujeto. La circunstancia de que el legislador determine una noción de establecimiento económico, diferente del lugar donde está el centro tecnológico, muestra la diferencia entre un concepto normativo y uno empírico. Puede adoptarse una regla general de imputación que sea enunciada de la siguiente manera: quien utiliza el medio electrónico y crea una apariencia de que este pertenece a su esfera de intereses, soporta los riesgos y la carga de demostrar lo contrario. También se puede sustituir el requisito del conocimiento de la declaración por la presunción de responsabilidad diciendo: la declaración se considera conocida cuando entra en la esfera de control del receptor, y existe una carga de autoinformación y de custodia a cargo del sujeto identificado como titular.[39]

La concepción de espacio e imputabilidad son conceptos que se deben adecuar conforme al avance tecnológico, entendiéndose que el espacio contextual en que cada uno de los conceptos jurídicos han sido plasmados e influye directamente en la definición que el legislador dio a cada uno de ellos, pero ¿qué pasa con el uso de nuevas tecnologías? .Estas de manera natural vienen y rompen los paradigmas ya instituidos, debido a que no es posible encuadrar hechos o actos jurídicos que suceden basados en el uso de nuevas tecnologías con la conceptualización que se le dio en un espacio y tiempo diferente, por ejemplo al realizar una compra venta en internet es completamente diferente a una compra venta realizado de manera física y esta a su vez es diferente si el método de pago es en efectivo o mediante tarjeta electrónica ya sea de débito o crédito, o mediante una transferencia electrónica, cualquiera de estos supuestos necesita un análisis y definición de manera independiente y un encuadre en algunos, inclusive encontrado porque en cada uno de ellos el espacio y tiempo son diferentes, es decir el lugar jurídico de una

[39] Op.cit.

compraventa en línea es el sitio o página web donde se realizó y en cambio el lugar jurídico para una compraventa física es el lugar donde se realizó dicha compra, por ejemplo un centro comercial.

"El incremento del comercio electrónico, como ya se ha manifestado, ha conducido a reconfigurar el comercio mundial en virtud de su globalización. Lo mismo ocurre con las transacciones y las comunicaciones privadas y con la organización de los servicios públicos y de la justicia. Las empresas utilizan métodos de colaboración laboral mediante redes que enlazan todo el planeta, rediseñan sus organizaciones y generan configuraciones virtuales, buscan nuevos canales de distribución de productos y servicios o analizan las posibilidades del entorno de redes abiertas para crear nuevos procedimientos de *marketing.* Los particulares, por su parte, se comunican cada vez con mayor habitualidad por correo electrónico y los Estados comienzan a utilizar estas redes para facilitar las declaraciones de impuestos, el intercambio de formularios o *workflow,* las consultas remotas de expedientes administrativos o judiciales, etcétera"[40]

En la actualidad el ser humano comienza a migrar instrumentos que sean viables hacia la Internet, es decir todo aquello que se pueda usar, hacer, investigar, informar, comunicar, etc. mediante el uso de una computadora, un software y la red denominada Internet, esto para poder elevar su calidad de vida disminuyendo los costos y tiempos que se utilizan para realizar una acción que se puede realizar mediante el uso de la internet, actualmente el ser humano puede disminuir costos y tiempos en tramites diversos como presentar un declaración de impuestos en la cual se puede realizar mediante el uso de un software y el envió de datos mediante el internet, esto evita costos de transporte para ir a una oficina de hacienda, evita el costo de la papelería que se entrega acompañando la declaración, y evita los tiempos de traslado y espera para presentar la misma.

"En la problemática de la instrumentación de los actos jurídicos mediante la utilización de las nuevas tecnologías digitales, surgen dos cuestiones que deben de ser analizadas con carácter

[40] Op.cit.

preliminar y que tienen que ver con la difundida denominación de documentos electrónicos. Con relación a ello se destacan dos aspectos fundamentales:

a) Por una parte, se denomina como documento a la entidad jurídica que constituye un instrumento. Esta última noción conlleva una entidad jurídica implícita, mientras que un documento la lleva si se le adosa el término jurídico.

b) Por otra parte, el término "electrónico" no avala la noción que se intenta transmitir del modo en que lo hace el término digital. Generalmente, ambas expresiones suelen mencionarse indistintamente. En realidad, según interpretación estrictamente tecnológica, el término electrónico hace referencia al dispositivo en el que está almacenado el instrumento o por medio del cual fue confeccionado.

El vocablo digital, en cambio, además de su definición estrictamente tecnológica, tiene una connotación diferente a la que aquí apelamos, puesto que implica ausencia de tangibilidad. En suma, si al termino documento se le adita la palabra electrónico se sigue manteniendo la dependencia del instrumento con su soporte, impidiendo de este modo el desprendimiento conceptual de ambos." [41]

Estas definiciones apoyan la determinación del concepto de delito cibernético, ya que parte medular para entender dicho concepto surge de saber y entender, que actualmente no solo existen los documentos escritos sino también existen documentos electrónicos los cuales tienen la misma validez jurídica, es decir un contrato que se realiza mediante un documento escrito, tiene la misma validez que un contrato que se realiza mediante un documento electrónico.

"Desde una óptica netamente económica, la figura que cobra especial importancia en las transacciones es el contrato. De hecho, esta figura jurídica ha sido el instrumento básico en las relaciones de las sociedades humanas. El contrato es el centro de la vida de negocios y el instrumento práctico que realiza las más variadas finalidades de la vida económica, de manera

[41] Op.cit.

tal que toda persona, aun quien carece de bienes, está comprendida dentro de la red de sus negociaciones."[42]

"La contratación electrónica es aquella que se realiza mediante la utilización de algún elemento electrónico cuando este tiene, o puede tener, una incidencia real y directa sobre la formación de la voluntad o el desarrollo o interpretación futura del acuerdo."[43]

"Por lo tanto, la contratación por medios digitales es la que se lleva a cabo, desde la formación del consentimiento hasta la ejecución del contrato, mediante dispositivos de enlace electrónico que se comunican interactivamente por canales de red basados en el procesamiento y transmisión de datos digitalizados, con el fin de crear, modificar, transferir, conservar o aniquilar derechos."[44]

En los contratos realizados mediante comercio electrónico, generalmente la oferta y su aceptación se realizan por medios electrónicos y no existe la posibilidad de realizar contraofertas. El usuario selecciona el producto que desea y abona el precio indicado, es decir, acepta en forma lisa y llana los términos y condiciones del contrato. Por esta razón puede decirse que, en la gran mayoría de los casos, en el comercio electrónico se utiliza la modalidad de contrato de adhesión. Este puede ser definido como aquel en el cual el contenido contractual ha sido determinado con prelación, por uno solo de los contratantes, al que se deberá adherir el contratante que desee formalizar una relación jurídica obligatoria.

Por otra parte, debe destacarse que es fundamental pactar el *momento* exacto en que la oferta se considerará realizada o retractada y aceptada. Para el caso específico de las contrataciones efectuadas por redes abiertas, si las partes no acuerdan el momento en que se considerará realizada la oferta, debería entenderse que ha sido hecha cuando el contrato instrumentado digitalmente ingresa a un sistema de información ajeno al control de quien genero el mensaje (o contrato) o de la persona que lo envía por cuenta de aquel.

---

[42] Mosset Iturraspe, J. (2016). *Contratos*. Argentina: Rubinzal-Culzoni.p.34-52.
[43] Davara Rodríguez, M. (1997). *Manual de derecho informático*. Pamplona: Aranzandi.p.166.
[44] Op.cit.

Es indudable que el comercio electrónico no se detiene ante la ausencia de regulaciones específicas y las transacciones fluyen sin solución de continuidad, porque este tipo de comercio tiene su propia lógica. Ello trae aparejada la celebración de contratos que, en la mayoría de los casos, terminarán ante los estrados judiciales por falta de estipulaciones precisas.

Para el caso de los contratos, mientras no existan normas vigentes que dispongan al respecto, las partes deberán pactar incluso el reconocimiento mutuo del mundo digital y acordar la validez del contrato que celebraran de ese modo, lo cual se estudiará previamente a las reflexiones jurídicas sobre delitos cibernéticos.

Los componentes necesarios para la celebración de un contrato digital son:

1) Validez de la instrumentación para las partes. - Es necesario que durante la realización de una transacción vía Internet se realice la validación de cada una de las partes, es decir el nombre, la dirección, los datos generales, los montos de la operación, todo esto deberá realizarse de manera segura mediante el llenado de diversos formularios por las partes y validando dicha información para concretar la operación.

2) Validez de la escritura digital. - Es necesario que durante la realización de una transacción vía Internet se realice la validación de la escritura digital, esto mediante el uso de un software que proveerá la parte vendedora y que permitirá mediante este validar la escritura digital de cada una de las partes para proseguir con la operación.

3) Validez de la firma digital. - Es necesario que durante la realización de una transacción vía Internet se realice la validación de la firma digital, esto deberá de realizarse mediante el uso de un software que proveerá la parte vendedora y que permitirá mediante este validar la firma digital de la parte compradora para proseguir con la operación.

4) Determinación de que los contratos celebrados electrónicamente tendrán los mismos efectos que un contrato escrito o verbal.- Durante la realización de una transacción vía Internet se debe validar que el contrato celebrado de manera electrónica cumpla con los

elementos esenciales del mismo, es decir que cumpla y tenga la misma validez y efectos jurídicos de un contrato escrito o verbal."[45]

En la definición y análisis de estos puntos para la realización del comercio electrónico, el punto en el que se realiza mayor énfasis es la firma digital esto debido a lo siguiente:

"El concepto histórico de la firma y, a la vez, el más amplio y genérico, ha sido de cualquier rasgo hecho, con la intención de exteriorizar a la manifestación de voluntad vertida en el instrumento.

La firma sirve a los siguientes propósitos:

a) *Consentimiento.* La firma expresa la aceptación sobre lo escrito o la intención de asignarle efectos jurídicos. La declaración escrita se hace poniendo el nombre propio debajo de un acto escrito, y la firma establece que el acto expresa el pensamiento y la voluntad del que lo firma.

b) Formalidad. El hecho de firmar un documento llama a la reflexión al firmante respecto del significado jurídico del acto que realiza y, en consecuencia, esta formalidad tiende a evitar la asunción de compromisos de manera inconsciente.

c) Prueba. Una firma autentica el cuerpo de escritura que le precede al identificar a su signatario. Cuando el signatario coloca al pie de un documento un rasgo distintivo que lo caracteriza, la escritura se vuelve *prima facie* atribuible a él.

d) Forma. En ocasiones, la firma hace a la validez de los actos jurídicos que se celebran. Tal es el caso de los actos formales *ad solemnitatem,* en los que la forma es un requisito inexcusable de su validez."[46]

[45] Op.cit.
[46] Op.cit.

“La firma es la manera habitual con que una persona escribe su nombre y apellido con el objeto de asumir las responsabilidades inherentes al documento que suscribe”[47]

La firma electrónica da certidumbre de la voluntad de las partes dentro de la realización de una transacción realizada mediante el uso de Internet, es el medio por el cual las partes confirman su deseo de realizar dicha operación y comprometerse en la misma, en el momento del uso de la misma esta surte efectos jurídicos. Es decir, en cuanto se realiza la validación de la firma electrónica, esta operación tiene validez.

Sin embargo, se debe tener en cuenta que en la utilización de esta firma electrónica se carece de la presencia física de las partes, situación que deja un hueco en la realización de la transacción, ya que al no existir presencia física de las partes, puede existir la manipulación o intervención de un tercero dentro del proceso, esto puede presentarse mediante el hackeo o la usurpación de identidad por un tercero, esto por consiguiente da como resultado el surgimiento de nuevos delitos, los cuales necesariamente requieren del uso de internet para su ejecución y que requieren que los usuarios de dicha firma electrónica, lleven un proceso de seguridad en el uso de la misma, como lo es el uso de antivirus dentro de la máquina que se utiliza, no utilizar maquinas o dispositivos de terceros para hacer uso de la misma, que la clave tenga la mayor complejidad posible como lo es el no uso de números o letras consecutivas en ella como 1, 2, 3, 4 o a, b, c, d; aunado a que en el momento del uso de la misma se verifique que la pagina donde se realiza la firma electrónica sea la página oficial donde deseamos utilizarla.

Esto da como resultado evitar el surgimiento de nuevos delitos que a la postre se clasificaran como Delitos Cibernéticos.

Sin embargo, conforme al avance tecnológico se va dando a nivel mundial y este empieza a permear a los distintos sectores de la población, empiezan a surgir nuevas formas de delinquir, situación que genera la necesidad de realizar un nuevo análisis que detonara con el surgimiento de una nueva clasificación denominada delitos bancarios.

[47] Borda,G. (1999). *Tratado de derecho civil argentino: Parte general*. Tomo I. Argentina: La Ley.p.168.

Pero antes de hondar en el tema se debe de entender que los delitos bancarios son aquellos que atañen dentro de la rama del derecho bancario, pero ¿Qué es derecho Bancario?, aquí citaré algunas definiciones:

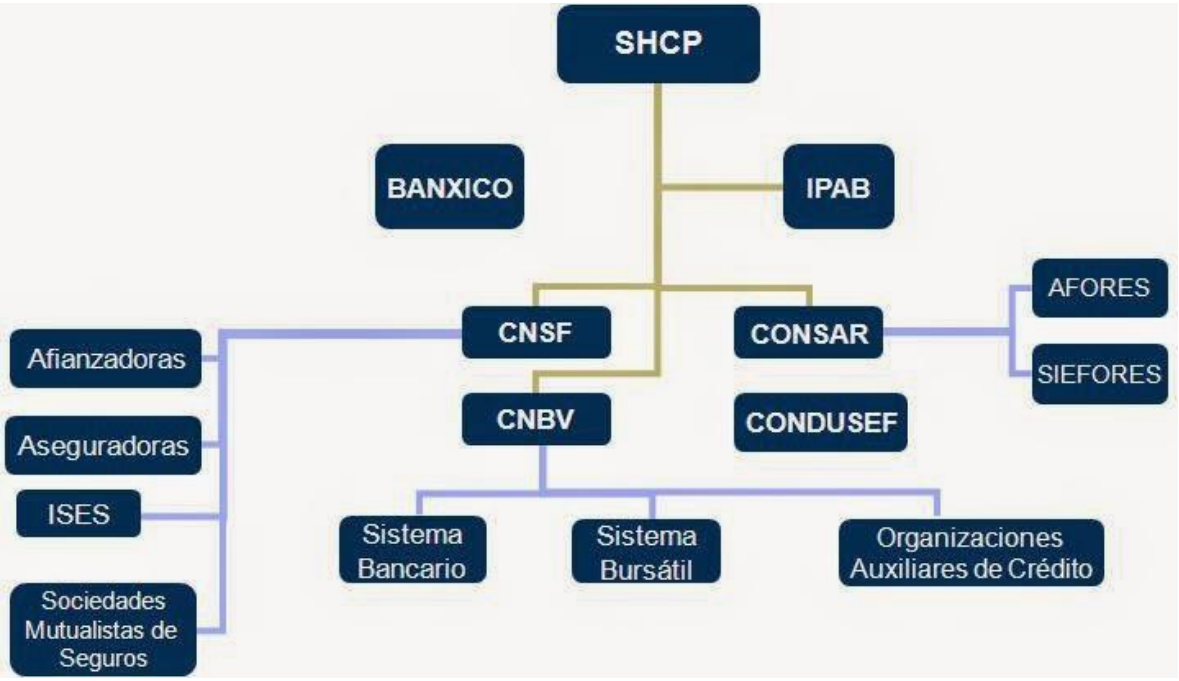
Para a "Paolo Greco derecho bancario "es el conjunto de principios y normas que se refieren a la empresa y las operaciones bancarias, se trata de una rama del derecho comercial y no una rama autónoma del derecho"[48]

Derecho Bancario es el conjunto de normas, jurisprudencias y doctrina que regula el organigrama, funciones, estructura y alcance de las Entidades de Crédito bancarias o entidades de depósito dentro del Sistema Financiero Mexicano.

El Derecho Bancario tiene como objeto la regulación de operaciones realizadas dentro del Sistema Financiero Mexicano, tanto de personas físicas como de personas morales ya sean estas de nacionalidad mexicana o extranjera.

Y dentro de este ámbito de validez que tiene el Derecho Bancario este tiene como delimitante su interacción y validez dentro del Sistema Financiero Mexicano, el cual se encuentra delimitado de la siguiente manera:

[48] Flores, C. (Abril 23, 2017). *Fundamentos de Administración V2 Características del Administrador*. Diciembre 2018, de clubensayos.com Sitio web: https://www.clubensayos.com/Temas-Variados/Fundamentos-de-Administraci%C3%B3n-V2-Caracter%C3%ADsticas-del/3935662.html



Dentro del Derecho Bancario existe normatividad específica emitida para delimitar sus funciones, la cual se puede enunciar de la siguiente forma de manera enunciativa y no limitativa:

Código de Comercio (CCo)

Ley de Instituciones de Crédito (LIC)

Ley General de Organizaciones y Actividades Auxiliares de Crédito (LGOAAC)

Ley General de Sociedades Mercantiles (LGSM)

Ley General de Títulos y Operaciones de Crédito (LGTOC)

Ley y Reglamentos del Banco de México (LBM)

Ley de Protección al Ahorro Bancario (LPAB)

Ley de Protección y Defensa al Usuario de Servicios Financieros (LPDUSF)

Ley Federal de Instituciones de Fianza (LFIF)

Ley para Regular las Instituciones Financieras (LRAF)

Ley General de Instituciones y Sociedades Mutualistas de Seguros (LGlySMS)

Ley sobre Contratos de Seguros (LSCS)

Ley de Sociedades de Inversión (LSI)

Ley sobre el Mercado Valores (LMV)

Ley Orgánica de la Comisión Nacional Bancaria y de Valores (LOCNBV)

Ley de los Sistemas de Ahorro para el Retiro (LSAR)

Ley de Concursos Mercantiles. (LCM)

Así, dentro de "esta normatividad existen Circulares emitidas por la Comisión Nacional Bancaria de Valores que tienen como delimitación un campo de acción especifico, ya que solo son aplicables a las Instituciones pertenecientes al Sistema Financiero Mexicano, es decir estas Circulares no tienen validez en personas físicas o morales no pertenecientes a dicho sistema.

A continuación, se buscará definir que es un delito:

Pero que es un delito, siguiendo al penalista Cesare Beccaria proponía en su clásico indiscutible de la doctrina jurídica del derecho penal, una división para esas conductas antijurídicas denominadas *delitos*. Delitos de lesa majestad, delitos contra la seguridad de los particulares, injurias, duelos, contrabandos, hurtos eran efectivamente, algunas de las categorías tipificantes que se articulaban en el sumario de su inmortal *De los delitos y de las penas.*

Acorde a Cuello Calón delito es la acción prohibida de una ley bajo la amenaza de una pena"[49]

[49] Márquez Piñero, R. (1997). *Delitos Bancarios*. México: Porrúa.3era Ed.p. VII y VIII.

“Un delito es aquella acción, o en su defecto omisión deliberada a la normativa vigente y acreedora a un castigo, porque en efecto está tipificada y penada en el derecho. También es posible que el delito sea la consecuencia de una imprudencia, es decir, no existió una intención de antemano de contrariar la ley pero se hizo y deberá ser sancionado como si lo hubiese sido.”[50]

Regresando al punto central de este trabajo se debe entender que los delitos cibernéticos son el resultado del avance tecnológico global que estamos viviendo en esta época; siendo una nueva forma de delinquir por parte de individuos que tiene una capacidad sobresaliente enfocada al uso de las actuales tecnologías; y que aprovechándose del vertiginoso cambio que nos brindan y del lento avance de la regulación en esta materia están teniendo como resultado un creciente y preocupante escenario en esta materia.

“El delito informático implica actividades criminales que los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos, hurtos, fraudes, falsificaciones, perjuicios, estafas, sabotajes. Sin embargo, debe destacarse que los usos de las técnicas informáticas han creado nuevas posibilidades del uso indebido de las computadoras, lo que genera la necesidad de regulación por parte del derecho.

No es labor fácil dar un concepto sobre delitos informáticos o cibernéticos, en razón de que su misma denominación alude a una situación especial, ya que para hablar de "delitos" en el sentido de acciones típicas, es decir, tipificadas o contempladas en textos jurídicos penales, se requiere que la expresión "delitos informáticos" esté consignada en los códigos penales, lo cual en nuestro país, al igual que en otros muchos no han sido objeto de tipificación aún."[51]

La mayor complejidad dentro del surgimiento de los delitos cibernéticos se debe a la severa dificultad que tiene el legislador al realizar la tipificación de estos en el momento de la comisión de los mismos, ya que existen lagunas dentro del marco conceptual actual que orillan al

[50] Ucha, F. (Marzo 12 2014). *Definición del delito*. Octubre 2018, de Definición ABC Sitio web: https://www.definicionabc.com/?s=Delito

[51] Télles Valdez, J. (1996). *Derecho Informático*. México: Mc Graw Hill.pp.103-104.

juzgador a tener que encuadrar estos delitos en diversas tipificaciones como los son el fraude, robo o estafa esto por citar algunos teniendo como consecuencia que en el momento de encuadrar el tipo penal, se carezca de elementos para poder procesar al indiciado.

“En 1983, la Organización de Cooperación y Desarrollo Económico (OCDE) inicio un estudio de las posibilidades de aplicar y armonizar en el plano internacional las leyes penales a fin de luchar contra el problema del uso indebido de los programas computacionales.

En 1992 la Asociación Internacional de Derecho Penal, durante el coloquio celebrado en Wurzburgo (Alemania), adoptó diversas recomendaciones respecto a los delitos informáticos, entre ellas que, en la medida que el Derecho Penal no sea suficiente, deberá promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos, si no basta con la adopción de otras medidas como por ejemplo el "principio de subsidiariedad.[52]

“Finalmente la OCDE publicó un estudio sobre delitos informáticos y el análisis de la normativa jurídica en donde se reseñan las normas legislativas vigentes y define Delito Informático como cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos.[53]

El Grupo de Lyón utilizó el término para describir, de forma imprecisa, los tipos de delitos perpetrados en la red o en las nuevas redes de telecomunicaciones que tuvieran un rápido descenso en los costos.

Al mismo tiempo, y guiado por los participantes del grupo de Lyón, el Consejo Europeo comenzó a diseñar el Tratado sobre Delito Informático. Este tratado, fue presentado a la opinión pública por primera vez en el año 2000. Incorporando una gama de técnicas de vigilancia que las agencias encargadas de la aplicación de la ley consideraban necesarias para combatir el “delito informático”. Así la versión final de ese tratado, aprobada en noviembre de 2001 después de los acontecimientos del 11 de septiembre, no definió el concepto. Es un término amplio referido a

[52] Colorado, P. (Noviembre 18, 2008). *Delitos informáticos*. Abril 2018, de Blogspot Sitio web: http://gonzo-stelgon.blogspot.com/2008/11/historia-de-delitos-informticos.html

[53] Definición elaborada por un Grupo de Expertos, invitados por la OCDE a París en Mayo de 1993.

los problemas que aumentaron el poder informático, abaratando las comunicaciones y provocando que haya surgido el fenómeno de Internet para las agencias policiales y de inteligencia. El tratado describe de la siguiente manera las diferentes disposiciones y áreas temáticas en las que se requiere una nueva legislación:

- Delitos contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos.

- Delitos relacionados con las computadoras [falsificación y fraude].

- Delitos relacionados con el contenido [pornografía].

- Delitos relacionados con la violación del derecho de autor y los derechos asociados.

-Responsabilidades secundarias y sanciones [cooperación delictiva, responsabilidad empresarial].”[54]

Acorde a lo mencionado se debe de analizar que parte de las áreas y temáticas requieren una legislación actualizada al identificarse delitos contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos; situación que apegada al enfoque de este trabajo se debe matizar puesto que se está en un proceso que va contra reloj y que con el simple transcurrir del tiempo se está perdiendo seguridad jurídica.

Considero que el delito informático tiene diversas connotaciones y diversos aristas, pero de todo esto el más grande tema es el factor de variabilidad acelerada que conllevan los delitos informáticos, esto debido a que este tipo de ilícitos evolucionan de manera paralela a la evolución tecnológica, por consiguiente la detección y análisis de los mismos es insuficiente ya que para poder encuadrar estos delitos es necesario que de manera paralela a la identificación de los mismos, el legislador haga los ajustes necesarios a las diversas leyes para que en el momento de la detección de las nuevas modalidades vinculadas con los delitos informáticos,

[54] Colorado, P. (Noviembre 18, 2008). *Delitos informáticos*. Abril 2018, de Blogspot Sitio web: http://gonzo-stelgon.blogspot.com/2008/11/historia-de-delitos-informticos.html

exista una norma para que exista una sanción y el infractor pueda ser juzgado. Evitando que la comisión de dichos delitos quede impune por lagunas de la legislación.

En consecuencia, es necesario homologar en la mayor medida posible el derecho positivo y el derecho natural, porque cabe recordar que en el caso de que no exista una norma tipificada dentro de la legislación vigente, no existirá la comisión de un delito, por consiguiente acorde a la corriente iusnaturalista puede existir un delito a pesar de no estar tipificado dentro de la ley, (el deber ser y el ser) , siendo el dilema en la comisión de delitos apegados al uso de la tecnología que al existir un avance tan acelerado, es difícil para el legislador encuadrar esto delitos dentro la norma vigente, de los cuales varios de los mismos no pueden ser encuadrados dentro de los delitos tipificados en la legislación, situación que hace necesario que la legislación sea actualizada conforme a la evolución misma de los ilícitos, para encontrar el punto medio donde se pueda mediar el derecho positivo y el derecho natural.

La utilización de nuevas tecnologías ha traído el uso indebido de la información que se procesa a través del uso de las mismas; de ahí la necesidad de establecer tipos penales que sancionen esa ilícita conducta.

Sin embargo, para poder generar una nueva norma dentro del Estado de Derecho Mexicano se debe de realizar mediante el siguiente procedimiento legislativo:

“El Poder Legislativo mexicano, encarnado en la figura del Congreso de la Unión, es el órgano responsable, de producir normas legales que expresan la voluntad del pueblo mexicano y que se constituyen, en razón de su origen y procedimiento de elaboración, en las normas primordiales del ordenamiento jurídico mexicano, únicamente sometidas a la Constitución.

“Previo al estudio de los delitos tecnológicos es interesante dar a conocer la forma de elaboración de normas siendo trascendente el señalamiento que realiza el autor Eduardo García Máynez, quien distingue seis etapas típicas de elaboración de la ley, a saber:

a) Iniciativa,

b) Discusión,

c) Aprobación,

d) Sanción,

e) Publicación,

f) Iniciación de la vigencia."[55]

Otros autores, suelen reducirlas a cinco etapas, excluyendo del procedimiento a la sanción e iniciación de la vigencia y agregando la de promulgación.

Se acepte una u otra clasificación, con la mirada puesta en la Constitución, se proponen tres fases delimitadas que conforman el llamado procedimiento legislativo, a saber:

1) Fase de iniciativa;

2) Fase de discusión y aprobación por las Cámaras; y

3) Fase integradora de la eficacia.

1) Fase de iniciativa. Este primer momento del procedimiento legislativo se encuentra regulado por los artículos 71 y 122, base primera, fracción V, inciso ñ), constitucionales, así como por el 55 del Reglamento para el Gobierno Interior del Congreso General de los Estados Unidos Mexicanos (en adelante RICG). De esta manera, el derecho de hacer propuestas o presentar proyectos de ley está reconocido por la propia Constitución mexicana, la cual indica de manera clara quiénes son los titulares en exclusiva de esta potestad. Señalando tales artículos lo siguiente:

El Presidente de la República como facultado para ejercer el derecho de iniciativa. De esta manera, el Ejecutivo Federal puede presentar cualquier tipo de iniciativa de ley o decreto; pero de manera exclusiva le corresponderá presentar las iniciativas de:

[55] Cámara de Diputados. (Mayo 2015). *Procedimiento legislativo*. Diciembre 2018, de Dirección General del Centro de Documentación, información y análisis Sitio web: http://www.diputados.gob.mx/bibliot/publica/prosparl/iproce.htm

La Ley de Ingresos,

El Presupuesto de Egresos de la Federación, y

La Cuenta Pública.

Con base en la normativa citada, los miembros de una y otra Cámara, es decir, los diputados y los senadores, son titulares de la iniciativa legislativa. Los legisladores pueden presentar proyectos de ley o decreto sin más restricciones que respetar las materias reservadas al Presidente de la República. No se exige, incluso, que el proyecto de ley o decreto sea suscrito por un número determinado de legisladores. En este sentido es válido pensar en que la iniciativa legislativa pueda ejercitarse individualmente por cada uno de los parlamentarios y también presentarse proyectos de manera conjunta.

Finalmente, los citados artículos 71 constitucional y 55 de la Red Interamericana de Compras Gubernamentales (RICG) en su fracción tercera, otorgan, este derecho a las legislaturas de los estados por la vía del artículo 122, base primera, fracción V, inciso ñ), para presentar iniciativas en materias relativas al Distrito Federal ante el Congreso de la Unión.

Todos los proyectos de ley o decretó pueden presentarse indistintamente en cualquiera de las Cámaras, a elección de él o de los proponentes, los cuales pasarán de inmediato a comisión. Pero esta regla general encuentra dos excepciones, a saber:

Los proyectos que versaren sobre empréstitos, contribuciones e impuestos; o bien sobre reclutamiento de tropas, los cuales, por mandato constitucional (artículo 72 inciso h), deberán discutirse primero en la Cámara de Diputados.

Para conocer de las incitativas de ley o decreto es necesario, con fundamento en el artículo 63 constitucional, que se integre el quórum necesario, es decir, deben estar presentes la mitad más uno de los miembros de las Cámaras. Finalmente hay que señalar que nuestra Norma Fundamental establece que, si el proyecto de ley ha sido rechazado por la Cámara de Origen, el mismo no podrá presentarse en las sesiones de ese año (artículo 72, inciso g).

2) Fase de discusión y aprobación. Una vez presentado el proyecto de ley o decreto por alguno de los titulares de la iniciativa legislativa, se da inicio a la etapa de discusión y aprobación del proyecto de ley o decreto; en este periodo del procedimiento legislativo ordinario se pretende fijar el contenido de la ley. Esta fase está regulada por los artículos 72 de la Constitución y del 95 al 134 de RICG.

Recibido el proyecto por una de las Cámaras, el presidente de la misma lo turnará a la comisión a la que corresponda el estudio en razón de la materia que entrañe la iniciativa legislativa, misma que será publicada en la Gaceta Parlamentaria. De esta manera, la Cámara que ha recibido la iniciativa se constituye en la Cámara de Origen, quedando a su colegisladora la función de Cámara Revisora.

Este es el momento en el que las comisiones legislativas desplegarán sus trabajos y harán uso de sus facultades para solicitar documentos y mantener conferencias con Secretarios de Despacho, Jefes de Departamento, etcétera, a fin de presentar un dictamen de los negocios de su competencia.

Todo dictamen de comisión deberá contener una parte expositiva de las razones en que se funde y concluir con proposiciones claras y sencillas que puedan sujetarse a votación. Para que haya dictamen, éste deberá presentarse firmado por la mayoría de los individuos que componen la Comisión. Si alguno o algunos no están de acuerdo con la mayoría, podrán presentar su voto particular por escrito.

Una vez que los dictámenes estén firmados por la mayoría de los miembros de la Comisión encargada del asunto, se publicarán junto con los votos particulares, si los hubiera, a más tardar cuarenta y ocho horas antes del inicio de la sesión en que serán puestos a discusión y votación. Los dictámenes publicados de esta manera, podrá dispensarse su lectura, previa consulta al Pleno en votación económica.

Los dictámenes en su totalidad estarán sujetos a discusión en lo general, pero en lo particular sólo se discutirán los artículos reservados.

En relación con las discusiones en general de un dictamen de ley, cada grupo parlamentario contará con quince minutos para su intervención; después de ésta se abrirán hasta dos turnos de cuatro oradores en pro y cuatro en contra, los que dispondrán de diez minutos cada uno. La participación de los grupos parlamentarios se realizará en orden creciente en razón del número de diputados que lo conforman.

Agotada la discusión en lo general y consultado el Pleno sobre artículos reservados para discusión en lo particular, en un solo acto se votará el dictamen en lo general y los artículos no reservados.

Si el dictamen fuere rechazado al término de la discusión en lo general, en la sesión siguiente se pondrá a discusión el voto particular. Si fuesen más de uno los votos se discutirá el del grupo parlamentario de mayor número de diputados y si éste se rechaza también, se procederá a discutir en la siguiente sesión el del Grupo Parlamentario que siga en importancia numérica, y así sucesivamente hasta agotarlos todos.

La discusión en lo particular es de la siguiente manera: se discutirá cada artículo reservado; cuando el proyecto conste de más de treinta artículos se consultará al Pleno si procede su discusión por capítulos. Una vez que se haya llegado a un acuerdo al respecto se procederá a abrir un turno de hasta cuatro oradores en contra y cuatro a favor, por cada artículo o grupo de éstos; de tal manera que cada orador dispondrá de cinco minutos si se discute por artículos y de diez minutos cuando se discuta por grupo de artículos.

Si un artículo o grupo de artículos fuese rechazado por la Cámara, esa parte del dictamen regresará a comisión para que ésta lo reelabore, tomando en consideración todo lo dicho durante la discusión, y lo presente nuevamente en sesión posterior. Entretanto, el resto del proyecto de ley aprobado quedará a disposición de la Presidencia de la Mesa Directiva y no podrá turnarse a la colegisladora hasta que no se presente la nueva propuesta de la Comisión Dictaminadora y la Cámara resuelva al respecto. Concluidas las discusiones en lo general y en lo particular, se procede a la votación, misma que se realiza a través del sistema electrónico de asistencia y votación.

Aprobado un proyecto en la Cámara de Origen, pasará a la Cámara Revisora, que de igual manera procederá a la discusión y aprobación de la iniciativa de ley. En este momento pueden presentarse tres situaciones distintas, a saber:

1) Que la Cámara Revisora la apruebe sin modificaciones; en cuyo caso se continuará con el procedimiento legislativo iniciándose así la fase que he denominado integradora de la eficacia (artículo 72, inciso a, constitucional).

2) Que algún proyecto de ley o decreto fuese desechado en su totalidad por la Cámara Revisora, en cuyo caso volverá a la Cámara de Origen con las observaciones que aquélla le hubiese hecho. Si una vez examinado fuese aprobado por la mayoría absoluta de los miembros presentes de la Cámara de Origen, pasará a la Cámara Revisora, que lo desechó, la cual deberá volverlo a tomar en consideración y si lo aprobare por la misma mayoría se pasará a la siguiente etapa del procedimiento legislativo. Pero, en caso contrario, si la Cámara Revisora lo volviera a rechazar, dicha iniciativa de ley no podrá presentarse nuevamente en el mismo periodo de sesiones (artículo 72, inciso d, de la Constitución).

3) Si no se presentará ninguno de los dos supuestos anteriores y un proyecto de ley o decreto fuese desechado en parte, modificado, o adicionado por la Cámara Revisora; la discusión de la Cámara de Origen versará únicamente sobre lo desechado o sobre las reformas o adiciones, sin poder alterarse en manera alguna los artículos aprobados. Si las adiciones o reformas hechas por la Cámara Revisora fuesen aprobadas por la mayoría absoluta de los votos presentes en la Cámara de Origen se pasará a la siguiente fase del procedimiento legislativo.

Si por el contrario, las reformas o adiciones, elaboradas por la Cámara Revisora, fuesen rechazadas por la mayoría de los votos en la Cámara de Origen, la iniciativa volverá a aquélla para que considere las razones expuestas por ésta, y si por mayoría absoluta de los votos presentes, en la Cámara Revisora se desecharen en esta segunda revisión dichas adiciones o reformas, el proyecto en lo que haya sido aprobado por ambas cámaras se someterá a la siguiente fase (artículo 72, inciso e, constitucional).

Si la Cámara Revisora insistiere, por la mayoría absoluta de los votos presentes, en dichas adiciones o reformas, todo el proyecto no volverá a presentarse sino hasta el siguiente periodo de sesiones, a no ser que ambas cámaras acuerden, por mayoría absoluta de sus miembros presentes, que se expida la ley o decreto sólo con los artículos aprobados y que se reserven los adicionados o reformados para su examen y votación en las sesiones siguientes (artículo 72, inciso e, constitucional).

3) Fase integradora de la eficacia. Una vez aprobado el proyecto de ley o decreto por la Cámara de Diputados y la de Senadores, se comunicará al Ejecutivo, firmado por los presidentes de cada una de las cámaras. Corresponde en este momento al Presidente de la República manifestar su acuerdo sancionando la ley y ordenando su promulgación o expresar su disconformidad formulando objeciones al proyecto.

En caso de que el Presidente esté de acuerdo con la totalidad del proyecto procederá a sancionarlo y a disponer que se promulgue como ley. La sanción es el acto de aceptación de una iniciativa de ley o decreto por parte del Poder Ejecutivo y en tal sentido la Constitución Mexicana en su artículo 72 b) señala que: "Se reputará aprobado todo proyecto no devuelto con observaciones a la Cámara de su origen, dentro de diez días útiles; a no ser que, corriendo este término, hubiere el Congreso cerrado o suspendido sus sesiones, en cuyo caso la devolución deberá hacerse el primer día útil en que el Congreso esté reunido".

Como puede inferirse de lo enunciado, este es el momento en el que el Presidente de la República puede ejercer su derecho de veto sobre cualquier ley. De tal manera que, si el proyecto de ley es desechado en todo o en parte por el Ejecutivo, será devuelto, con sus observaciones, a la Cámara de origen, misma que deberá discutirlo nuevamente y si fuese confirmado por las dos terceras partes del número total de votos, pasará otra vez a la Cámara revisora y si fuese sancionada por ésta por la misma mayoría, el proyecto de ley o decreto será devuelto al Ejecutivo para su promulgación.

La promulgación consiste en una declaración solemne de acuerdo con una fórmula especial mediante la cual se formaliza la incorporación de la ley de manera definitiva al ordenamiento

jurídico. Dicha fórmula, conforme al artículo 70 de la Constitución, es la siguiente: "El Congreso de los Estados Unidos Mexicanos decreta (texto de la ley o decreto)". La sanción y la promulgación no se diferencian espacial y temporalmente, sino que se efectúan en el mismo acto.

Junto con la sanción y la promulgación, el Presidente de la República debe proceder a la publicación de la ley. La promulgación en el derecho mexicano incluye la obligación de publicar la ley, como medio de que se vale el poder público para dar a conocer la nueva ley a todos los ciudadanos. La publicación de las leyes se realiza en el Diario Oficial de la Federación, órgano de difusión del Estado.

REGLAS PARA EL DEBATE DEL DICTAMEN EN EL PLENO DE LA

CÁMARA DE DIPUTADOS

PUBLICACIÓN

Los dictámenes, sin excepción deberán publicarse en la Gaceta Parlamentaria a más tardar 48 horas antes del inicio de la sesión en que serán puestos a disposición en la sesión.

Podrá dispensarse la segunda lectura del dictamen, previa consulta del pleno en votación económica, cuando ya ha sido publicado. Dicha publicación surtirá los efectos del artículo 108 del RICG que establece que al principio de la discusión cuando lo pida algún legislador, la Comisión Dictaminadora deberá explicar los fundamentos de su dictamen y aun leer las constancias del expediente, si fuera necesario; acto continuo, seguirá el debate. Artículo 12 y 14 del Acuerdo Parlamentario relativo a las sesiones, integración del orden del día, los debates y las votaciones de la Cámara de Diputados (en adelante Acuerdo Parlamentario 11/97).

DISCUSIÓN EN LO GENERAL

Cada grupo parlamentario dispondrá de 15 min. Para una intervención.

De manera excepcional cuando se discuten reformas constitucionales las intervenciones serán de 20 min.

Las intervenciones de los grupos parlamentarios se realizarán en orden creciente en razón de los diputados que los conforman.

Los diputados sin grupo parlamentario acordarán con uno de éstos su participación en la discusión. Art. 97 del RICG y arts. 15 y 16 del Acuerdo Parlamentario 11/97.

Se integrarán listas de los diputados que soliciten la palabra en contra y otra lista en favor, las cuales se leerán antes de comenzar la discusión.

Si algún diputado que haya pedido la palabra no estuviere presente en el salón cuando le toque hablar, se le colocará al final de la lista. Arts. 96 y 99 del RICG.

PRIMER TURNO: cuatro oradores a favor y cuatro en contra, de 10 min. Cada intervención.

De manera excepcional cuando se discuten reformas constitucionales las intervenciones serán de 15 min.

Los diputados sin grupo parlamentario podrán inscribirse directamente.

Los oradores hablarán alternativamente en contra o en pro de acuerdo al orden de las listas comenzando por el inscrito en contra.

El Presidente consultará al Pleno si el asunto se encuentra suficientemente discutido. Arts. 115, 148, 149 y 150 del RICG. Art. 16 del Acuerdo Parlamentario 11/97.

SEGUNDO TURNO cuatro oradores en pro y cuatro en contra de 10 min., cada intervención.

De manera excepcional cuando se discuten reformas constitucionales las intervenciones serán de 15 min. Art. 16 del Acuerdo Parlamentario 11/97.

Los Diputados, aun cuando no estén inscritos en las listas de oradores, podrán pedir la palabra para rectificar hechos o contestar alusiones personales, cada intervención será de 5 min., pero pasarán a tribuna después de concluido el turno correspondiente. Sólo podrán realizarse hasta 5 intervenciones de este tipo, una vez agotadas éstas, la Presidencia consultará al Pleno si se

procede a dar curso al turno de oradores siguiente o a la votación, según sea el caso. Art. 102 del RICG y art. 20 del Acuerdo Parlamentario 11/97.

Se consulta al Pleno sobre los artículos reservados para su discusión en lo particular. Art. 17 del Acuerdo Parlamentario 11/97.

Votación nominal del dictamen en lo general y en los artículos no reservados. Arts. 117, 134, 147 148 del RICG. Art. 17 del Acuerdo Parlamentario 11/97.

En caso de ser aprobado se procederá a su discusión en lo particular. Por el contrario, si fuese rechazado, se preguntará en votación económica, si vuelve o no el dictamen a comisión.

Si la resolución fuese afirmativa, volverá en efecto, para que lo reforme; pero si fuera negativa se tendrá por desechado.

En caso de ser rechazado un dictamen y si existiere voto particular se pondrá a discusión en la siguiente sesión.

Si hubiese más de un voto particular se discutirá primero el que presente el diputado perteneciente al grupo parlamentario de mayor número de integrantes, si fuere rechazado se discutirá en la siguiente sesión, el voto particular presentado por el diputado perteneciente al grupo parlamentario que siga en importancia numérica, y así sucesivamente hasta que fuese necesario. Art. 117 del RICG. Art. 17 del Acuerdo Parlamentario 11/97.

DISCUSIÓN EN LO PARTICULAR

Se discutirá cada artículo reservado.

Cuando el dictamen contenga más de 30 artículos se consultará al pleno si procede su discusión por grupo de artículos.

Se podrán apartar las fracciones o incisos que se quieran impugnar, y lo demás del proyecto que no amerite discusión se podrá reservar para votarlo después en un sólo acto.

Cuando se discuten reformas constitucionales solo se podrán discutir artículo por artículo. Arts. 132 y 133 del RICG. Artículo 18 del Acuerdo Parlamentario 11/97.

Se integrarán listas de los diputados que soliciten la palabra en contra y en pro, las cuales se leerán antes de comenzar la discusión de cada artículo.

Si algún diputado que haya pedido la palabra no estuviere presente en el salón cuando le toque hablar, se le colocará al final de la lista. Arts. 96 y 99 del RICG.

Un turno de cuatro oradores en pro y cuatro en contra, de 5 min. Cada intervención cuando se discuta por artículo y de 10 min. Cuando se discute por grupo de artículos.

De manera excepcional cuando se discutan reformas constitucionales las intervenciones serán de 15 min. Art. 18 del Acuerdo Parlamentario 11/97.

El Presidente consultará al Pleno, mediante votación económica, si el artículo se encuentra lo suficientemente discutido. Art. 115, 148 a 150 del RICG.

Los diputados, aun cuando no estén inscritos en las listas de oradores, podrán pedir la palabra para rectificar hechos o contestar alusiones personales, cada intervención será de 5 min. Pero pasarán a tribunal después de concluido el turno correspondiente.

Sólo podrán realizarse hasta 3 intervenciones de este tipo, una vez agotadas éstas, la presidencia consultará al Pleno, mediante votación económica si se procede a dar curso al turno siguiente de oradores o a la votación, según sea el caso. Arts. 20 del Acuerdo Parlamentario 11/97 y 102 del RICG.

Se llevará a cabo la votación nominal del artículo o del grupo de artículos reservados.

Si un artículo o grupo de artículos sometidos a discusión en lo particular fueren rechazados, esa misma parte del dictamen regresará a comisión para que ésta lo reelabore. El resto del dictamen aprobado quedará a disposición de la presidencia y no podrán turnarse a la colegisladora hasta que no se presente nueva propuesta de la comisión dictaminadora y la cámara resuelva lo pertinente. Arts. 147 y 148 del RICG y 19 del Acuerdo Parlamentario 11/97.

MOCIONES

En la fase de discusión y aprobación pueden presentarse diversos tipos de mociones, éstas son interrupciones que, al discurso de un orador, al trámite por acordar o a la decisión de la Mesa, presenta un legislador para diferentes fines y efectos.

Dentro del procedimiento legislativo y concretamente en la fase de discusión de las iniciativas, los legisladores tienen derecho para que, sin observar el turno reglamentario, dirijan a la presidencia (en cualquier estado que se encuentre el debate), alguna moción. El Presidente les dará o negará trámite.

Las mociones pueden ser de diversos tipos según se solicite la interrupción de un discurso y podemos clasificarlas de la siguiente manera:

MOCIÓN DE ORDEN: Procede en los siguientes casos: a) para ilustrar la discusión con la lectura de un documento; b) cuando se infrinjan artículos del reglamento para el gobierno interior del congreso general de los Estados Unidos Mexicano, en cuyo caso deberá ser citado el articulo respectivo; c) cuando se viertan injurias contra alguna persona o corporación, pero no podrá llamarse al orden al orador que critique o censure a funcionarios públicos por faltas o errores cometidos en el desempeño de sus atribuciones; d) cuando el orador se aparte del asunto sometido a discusión. Artículos 104, 105 y 107 del RICG.

MOCIÓN SUSPENSIVA: Se leerá la proposición y, sin otro requisito que oír a su autor, si la quiere fundar, y a algún impugnador, si lo hubiere, se preguntará a la cámara si se toma en consideración inmediatamente. En caso afirmativo se discutirá y votará en el acto, pudiendo hablar al efecto, 3 individuos en pro y 3 en contra; pero si la resolución de la cámara fuese negativa, la proposición se tendrá por desechada. No podrá presentarse más de una moción suspensiva en la discusión de un negocio. Arts. 110 y 111 de RICG.

MOCIÓN ACLARATIVA: Cuando alguien de los presentes solicite el uso de la palabra para que se lea algún documento en relación con el debate para ilustrar la discusión, pedirá la palabra para el solo el efecto de hacer la moción correspondiente, si es aceptada por la cámara la lectura de

dicho documento deberá hacerse por uno de los secretarios, continuando después en el uso de la palabra el orador. Art. 113 del RICG.

SUSPENSIÓN DE LAS DISCUSIONES

Finalmente, hay que señalar bajo qué circunstancias pueden suspenderse las discusiones, el art. 109 del RICG señala que ninguna discusión podrá suspenderse, sino por las causas siguientes:

PRIMERA, por ser la hora en que el Reglamento fija para hacerlo, a no ser que se prorrogue por acuerdo de la cámara.

SEGUNDA, porque la cámara acuerde dar preferencia a otro negocio de mayor urgencia o gravedad.

TERCERA, por graves desórdenes en la misma cámara.

CUARTA, por falta de quórum. Si el número de asistentes es dudoso, se comprobará pasando lista y si es verdaderamente notoria la falta de éste, bastará la simple declaración del presidente.

QUINTA, por proposición suspensiva que presente alguno o algunos de los miembros de la cámara y que ésta apruebe"[56]

Este procedimiento legislativo que se realiza dentro del Estado de Derecho Mexicano tiene la grave problemática de la dilatación del mismo, por ejemplo en el supuesto que hoy día se detectase una actividad ilícita que se debiera de encuadrar como un nuevo delito identificado de manera oportuna por el legislador, este deberá de iniciar el citado procedimiento legislativo para crear una norma que encuadre el nuevo tipo de delito detectado y esto podría inclusive tardar meses en su aprobación e inicio de vigencia y esto en el sentido que no existiera oposición por parte de alguna de las cámaras o se aplicara el derecho de veto que tiene el ejecutivo, e inclusive ya aprobada la norma y entrada en vigencia alguna de las personas físicas

[56] Cámara de Diputados. (Mayo 2015). *Procedimiento legislativo*. Diciembre 2018, de Dirección General del Centro de Documentación, información y análisis Sitio
web: http://www.diputados.gob.mx/bibliot/publica/prosparl/iproce.htm

o morales que recaigan en los supuestos de esta y sean afectadas podrán interponer un procedimiento como por ejemplo el juicio de amparo ante esta; dando como resultado en caso de así considerarlo el juzgador la detención de la aplicación de la norma para una persona en concreto o en su defecto inclusive emitiendo una jurisprudencia que podría dejar sin efecto la norma emitida y esto es un común denominador para la diferente legislación emitida por parte del poder ejecutivo y legislativo derivado de que antes de la aprobación de la norma esta no es revisada por el Poder Judicial de la Federación, situación que genera lagunas técnico jurídicas en la norma emitida que en el menor de los casos hacen necesaria su revisión de nueva cuenta para subsanar dichas lagunas y en el peor de los casos inclusive podría el Poder Judicial solicitar la no aplicación de la norma y esto cabe aclarar que para llegar a este punto la cantidad de tiempo transcurrido puede resultar inclusive irrisoria, y estos temas únicamente validando una cuestión meramente de espacio-tiempo, ahora si esto agregamos el tema del costo que genera la realización de dicho proceso, estamos hablando de una dificultad severa a la hora de la necesidad de actualización de la norma jurídica a un ilícito recientemente identificado.

Ahora imaginemos que estamos ante un nuevo ilícito “cualquiera” cometido dentro del área informática, supongamos que una clonación de tarjeta de crédito mediante el uso de un software y el cual después de un arduo proceso el legislador lograr encuadrar este delito en un nuevo tipo penal después de un proceso de varios meses, justo en este punto derivado del avance tecnológico acelerado puede suscitarse que el uso de este software y esta forma de clonación de tarjetas ya no sea utilizado, quizá porque las entidades financieras, un particular, una empresa de seguridad privada o cualquier tercero contratado por las personas físicas o morales para subsanar este tipo de ilícitos(todo esto derivado de los largos periodos de tiempo utilizado en el proceso legislativo por parte del Estado).

Ya lograron identificar el delito de manera anticipada a la aprobación de la norma y los particulares afectados por la comisión de este ilícito ya buscaron y encontraron formas de evitar este tipo de fraudes, por consiguiente pudieron haber actualizado su software y poner diversas medidas de seguridad, situación que generaría que el infractor de este tipo de ilícitos cambie su forma de operar realizando la clonación de la tarjeta de crédito por otro medio, situación que

traería como consecuencia que en el momento de la aprobación de la norma y entrada en vigencia esta quedaría obsoleta o como a lo que comúnmente se le denomina letra muerta, es decir normas tipificadas dentro de una ley que ya no se utilizaran por estar enfocadas a hechos o supuestos jurídicos que ya no se realizan o en este tipo de delitos informáticos en específico la forma de delinquir fue perfeccionada.

Se debe realizar un cambio de este proceso legislativo, reduciendo la burocratización del mismo, recortando y disminuyendo los tiempos dentro del mismo, el legislador debe de adaptar los procesos a la actualidad en que se desenvuelve la sociedad, entendiendo que la forma, medios y velocidad en que hoy se realizan las diversas actividades sociales no es la misma de hace veinte, treinta o cuarenta años.

Todos estos tópicos son parte de los antecedentes sociales que influyen de manera trascendental en entender y comprender la dificultad que los delitos informáticos conllevan de manera natural, esto debido a que hay que recordar que a diferencia de las otras ramas del Derecho el área informática es sumamente cambiante.

Situaciones que nos dejan con la idea de que estamos en un proceso de evolución tecnológica donde desafortunadamente la parte infractora está superando de manera importante al Estado, debemos entender la dificultad y todas las variantes que debe de enfrentar el Estado para poder realizar cambios, situación que sin duda es un tema sumamente complejo y por consiguiente si logramos entender esta parte, debemos como personas físicas o morales poner de nuestra parte para disminuir este tipo de ilícitos, siguiendo todas y cada una de las recomendaciones emitidas por las diversas instituciones financieras, empresas de ciberseguridad o el mismo Estado, esto con la finalidad de disminuir el riesgo de ser afectadas por este tipo de ilícitos.

Porque si bien es cierto la finalidad del Estado es la de proveer una seguridad jurídica a los individuos que se desenvuelven dentro de los límites territoriales dentro de los cuales este tiene injerencia, al igual que el mismo Estado nosotros los particulares debemos de entender que al ser rebasado este por un sinfín de temas como pueden ser la falta de recursos económicos, el avance tecnológico acelerado, la dificultad que se enfrenta el Estado para la actualización de

procesos solo por citar algunos recae en nosotros como particulares tomar las medidas mínimo necesarias para salvaguardarnos de ser víctimas de estos nuevos ciberdelincuentes.

2.3 Definición de delito cibernético

La Organización para la Cooperación y el Desarrollo Económico (OCDE) publicó un estudio sobre delitos informáticos y el análisis de la normativa jurídica en donde se reseñan las normas legislativas vigentes y se define Delito Cibernético como cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos.[57]

Para que una acción u omisión realizada por una persona física o moral sea considerada como delito, esta debe estar tipificada dentro una ley, en caso de realizarse una acción u omisión por parte de una persona física o moral y esta no se encuentra tipificada dentro de una ley esta no podrá ser calificada como delito.

"Los delitos cibernéticos se realizan necesariamente con la ayuda de los sistemas informáticos, pero tienen como objeto del injusto la información en sí misma[58].

Los delitos cibernéticos o informáticos son aquellos que una persona física o moral realiza mediante el uso de la tecnología, estos tienen la peculiaridad de ser de difícil rastreo para el común de las personas, debido a que se necesita tener un conocimiento amplio en el uso de los sistemas informáticos tanto para su realización, como para su detección y análisis.

“Julio Téllez Valdez clasifica a los delitos informáticos en base a dos criterios:

Como instrumento o medio: se tienen a las conductas criminales que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito.“[59]

---

[57] Guzmán, B. (2011). *La Información y el Delito*. Octubre 2018, de Blog Guzmán Bruno Sitio web: https://sites.google.com/site/legisydelitosinfoform/creditos

[58] Checks. (Noviembre 14, 2011). *Delitos informáticos*. Noviembre 2018, de Blog de Checks Sitio web: https://www.blogger.com/profile/07575685817478971568

[59] Op.cit.

“María Luz Lima, por su parte, presenta la siguiente clasificación de Delitos Informáticos

Como Método: conductas criminales en donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito.

Como Fin: conductas criminales dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla.” (Lima Malvido, M .1984)

El Delito Cibernético es la acción antijurídica realizada por una persona física o moral que se encuentra tipificada dentro de una ley, en el cual para la comisión de los mismos interviene de manera obligatoria el uso de las nuevas tecnologías.

La realización de delito cibernético por parte de un infractor o delincuente es el resultado de la evolución misma de los delitos, los cuales trascienden y evolucionan de manera histórica, esto sucede de manera simultánea a la evolución de la sociedad donde se realiza, esto quiere decir que, a mayor avance y modernización dentro de una sociedad, la forma de delinquir dentro de esta sociedad evolucionar de la mano a este desarrollo.

Sin embargo, el gran tema a tatar con respecto a este tipo de Delitos es que la gran mayoría de los mismos aún no se encuentran clasificados en un delito específico y se tiende a ser homologados dentro de delitos que se asemejen, situación que hace complejo poder clasificarlos, esto debido a que conforme avanza y evoluciona la tecnología, los delitos cibernéticos también lo hacen.

2.4 Actualidad

La vertiginosa inclusión del uso del internet dentro de la sociedad contemporánea ha tenido como consecuencia dos vertientes como en todo aquello que se busca implementar con tintes de modernidad, por un lado el sentido positivo de aquello que se está modernizando en este caso específico el internet, el cual en este sentido nos ha traído un sinfín de beneficios entre los cuales se pueden identificar los siguientes:

-Información al momento

-Comunicación instantánea entre dos o más personas

-Realización de trámites en línea

-Disminución de tiempos en la realización de diversas actividades

Y la segunda vertiente que es el sentido positivo de aquello que se está modernizando en este caso específico el internet, el cual nos ha traído entre los diversos temas a preocuparse entre varios los siguientes puntos:

-Comercio de cualquier artículo en línea tanto aquellos de uso benéfico como aquellos de uso perjudicial como pueden ser armas, drogas, pornografía infantil, etcétera.

-Usurpación de identidad en línea esto sucede sobretodo en el uso de las redes sociales, en las cuales al no estar de manera física con la persona con quien se interactúa, existe el riesgo de que esta persona no sea quien dice ser.

-Apropiación de manera unilateral de información confidencial de un tercero.

-Clonación de bines de tarjetas de crédito.

-Compra, venta y distribución de material protegido por el autor sin su autorización (piratería)

Todo este desenvolvimiento y vertiginoso desarrollo, comercialización y expansión dela red denominada internet como lo indicamos anteriormente tiene cosas sumamente positivas y otras sumamente negativas, pero en este tema habrá que mencionar, que su desenvolvimiento y desarrollo, al ser tan rápido es sumamente complejo identificar todos y cada uno de los puntos positivos y negativos, situación que deja puntos muertos en las medida de precaución que deben de tener los diversos usuarios de esta red.

En cifras de Instituto Nacional de Estadística y Geografía (INEGI) se encuentra de la siguiente manera:

-“Al segundo trimestre de 2015, el 57.4 por ciento de la población de seis años o más en México se declaró usuaria de Internet.

-El 70.5 por ciento de los cibernautas mexicanos tiene menos de 35 años.

-El 39.2 por ciento de los hogares del país tienen conexión a internet.

-El uso de internet está asociado al nivel de estudios; entre más estudios, mayor uso de la red.

-La obtención de información y la comunicación son las principales actividades realizadas en internet.

-77.7 millones de personas usan celular y dos de cada tres usuarios cuenta con un teléfono inteligente."[60]

En palabras simples que en promedio arriba del 60 por ciento de la población en México tiene acceso al uso de internet.

2.5 Clasificación y penalidad de delitos cibernéticos

Los delitos cibernéticos tienen un tinte y forma de análisis especial, como lo he indicado anteriormente se debe específicamente a la celeridad con que estos surgen y evolucionan, esto se debe a que tenemos que contextualizarnos espacial y temporalmente para comprender esta situación, entendiendo y anteponiendo que la sociedad y evolución tecnológica contemporánea avanza de manera diferente a sociedades anteriores, por citar un ejemplo entre el descubrimiento de la tinta y el papel pasaron siglos para poder desarrollar la imprenta, desarrollo tecnológico que comparado con la temporalidad de avance tecnológico en nuestra sociedad contemporánea resulta irrisoria actualmente tenemos avances tecnológicos en sistemas informáticos casi de manera diaria.

Así, el realizar la clasificación de este tipo de delitos es compleja y por decirlo lo menos variada, esto debido a que el tipo de delitos tipificados en un territorio determinado puede ser diferente a los tipificados en otro punto, así mismo este tipo de delitos no son identificados de manera

[60] Thirión J & Valle Zárate, J. (2018). *La brecha digital y la importancia de las tecnologías de la información y la comunicación en las economías regionales de México*. Diciembre 2018, de Revista Internacional de Estadística y Geografía "INEGI". Vol. 9, Núm. 2, mayo-agosto 2018. Sitio web: https://www.inegi.org.mx/rde/2018/11/07/la-brecha-digital-la-importancia-las-tecnologias-la-informacion-la-comunicacion-en-las-economias-regionales-mexico/

sencilla como por ejemplo homicidio, el cual se encuentra tipificado y es de fácil identificación en prácticamente todo el mundo, en cambio un delito cibernético puede diferir en su forma de realización, clasificación y puede diferir su identificación en diversos territorios.

Sin embargo, para clasificar los delitos cibernéticos, en primera instancia se debe identificar las definiciones de los actores y términos que intervienen dentro de los delitos cibernéticos, la cual es la siguiente:

Cracking

“Acceso ilícito a sistemas y equipos de informática. Es quien sin autorización acceda, modifique, destruya o provoque perdida de información contenida en sistemas o equipos de informática".

Hacker

Es un término en inglés con el que se define a las personas dedicadas, por afición u otro interés, a violar programas y sistemas supuestamente impenetrables y constituyen una muestra de la nueva faceta de la criminalidad, el delincuente silencioso o tecnológico.

Es aquel que simplemente le gusta husmear por todas partes.

Un hacker es una persona interesada en el funcionamiento de los distintos sistemas operativos; por lo general suele tener mucho conocimiento en lenguaje de programación.

Hacker es el neologismo utilizado para referirse a un experto en varias o alguna rama técnica relacionada con las tecnologías de la información y las telecomunicaciones: programación, redes de computadoras, sistemas operativos, hardware de red/voz, etc.

Crackers

Son personas que se introducen en sistemas remotos con la intención de destruir datos, denegar el servicio a usuarios legítimos, y en general a causar problemas a los sistemas, procesadores o redes informáticas. A los crackers también se les conoce con el nombre de piratas informáticos.

Cyberpunk

El termino cyberpunk o vándalos cibernéticos se refiere a las conductas tendientes a causar daños en toda el área vinculada a la informática, esto es, afectando, los datos programas o soportes informáticos, fundamentalmente atreves de internet.

Phreaker

Constituyen equipos electrónicos que pueden interceptar y hasta ejecutar llamadas de aparatos telefónicos celulares sin que el titular se percate de ello. Estas personas poseen conocimientos de tarjetas de prepago ya que la telefonía celular las emplea habitualmente.

Buscan burlar la protección de las redes públicas y cooperativas de telefonía, con el fin de poner a prueba conocimientos y habilidades.

Cyberbullying

(Amenazas e intimidación a través de sistemas digitales): Uso de imágenes de otros como forma de chantaje, al que "amenace a otro ", haciendo uso o empleo de comunicados o mensajes enviados a través de medios o sistemas informáticos o le amenace con divulgar la información, datos o imágenes obtenidas a través del acceso ilícito a dichos medios o sistemas informáticos.

Spam

Son mensajes no solicitados y enviados comúnmente en cantidades masivas. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es por correo electrónico. Otras tecnologías de internet que han sido objeto de spam incluyen grupos de noticias, motores de búsqueda y blogs. El spam también puede tener como objetivo los celulares a través de mensajes de texto y los sistemas de mensajería instantánea.

Fraude

El fraude informático es inducir a otro a hacer o a restringirse en hacer alguna cosa de lo cual el criminal obtendrá un beneficio por lo siguiente: Alterar el ingreso de datos de manera ilegal. Esto requiere que el criminal posea un alto nivel de técnica y por lo mismo es común en

empleados de una empresa que conocen bien las redes de información de la misma y pueden ingresar a ella para alterar datos como generar información falsa que los beneficie, crear instrucciones y procesos no autorizados o dañar los sistemas. Alterar, destruir, suprimir o robar datos, un evento que puede ser difícil de detectar.

Alterar o borrar archivos.

Alterar o dar un mal uso a sistemas o software, alterar o reescribir códigos con propósitos fraudulentos. Estos eventos requieren de un alto nivel de conocimiento."[61]

Estos términos son los más comunes utilizados dentro de los delitos cibernéticos, por tanto para poder entender de una mejor manera la definición de los delitos cibernéticos es necesario conocer estos.

Después de conocer y poder identificar estos términos podemos mencionar la clasificación de los delitos cibernéticos, entendiendo que su comprensión e interpretación será con mayor facilidad:

DELITOS CONTRA EL HARDWARE.

"Existen diversos delitos perpetrados contra la parte única del sistema de computación, contra la parte denominada ``hardware´´ que comprende redes e instalaciones, así como también, en un sentido algo más amplio, las redes de comunicación del sistema."[62]

Este tipo de delitos atentan directamente contra el hardware de los sistemas informáticos, estos se caracterizan porque el ilícito depende de un cambio en los componentes externos de los sistemas informáticos, estos son por ejemplo cuando por medio de una modificación del

[61] Sánchez López, K. (Noviembre 29, 2012). *Delitos Informáticos (México)*. Octubre 2018, de Estudiante Sánchez López Karla para monografias.com Sitio web:https://www.monografias.com/trabajos94/delitosinformaticos/delitosinformaticos.shtml

[62] Sánchez López, K. (Noviembre 29, 2012). *Delitos Informáticos (México)*. Octubre 2018, de Estudiante Sánchez López Karla para monografias.com Sitio web:https://www.monografias.com/trabajos94/delitosinformaticos/delitosinformaticos.shtml

hardware se logra bloquear o inutilizar un sistema informático, una de sus características principales es que en este tipo de ilícitos solo es un medio para cometer otros.

DELITOS CONTRA EL SOFTWARE.

"Existen delitos perpetrados contra los programas, contra el llamado software del sistema computacional. Los programas representan un área valiosa desde el punto de vista financiero y fundamental operativamente hablando, ya que dichos programas representan las directrices, las instrucciones con las cuales el sistema procesara los diversos datos. De ahí de su destrucción total o parcial implique pérdidas financieras y operativas considerables."[63]

Este tipo de ilícitos se realizan directamente contra el software de un sistema informático, y la gran diferencia que tiene con los delitos contra hardware es que estos se pueden cometer de manera personal donde se encuentra el equipo informático o se pude realizar de manera remota mediante una computadora.

DELITOS CONTRA LA MEMORIA DE LA COMPUTADORA.

"Existen, finalmente, delitos perpetrados contra los datos que reposan en la memoria del ordenador. Estos actos contra las bases de datos atentan contra la fiabilidad, la memoria y la integridad del sistema informático, son además, en muchos casos, el instrumento o mecanismo para la comisión de delitos patrimoniales."[64]

Este tipo de ilícitos se realizan a los computadores de los sistemas informáticos, estos se realizan de manera personal donde se encuentra el servidor o se puede realizar de manera remota mediante una computadora, este tipo de ilícitos atentan directamente contra bases de datos, un ejemplo reciente de ellos son los ilícitos cometidos contra las bases de datos de la

[63] Sánchez López, K. (Noviembre 29, 2012). *Delitos Informáticos (México)*. Octubre 2018, de Estudiante Sánchez López Karla para monografias.com Sitio web:https://www.monografias.com/trabajos94/delitosinformaticos/delitosinformaticos.shtml

[64] Sánchez López, K. (Noviembre 29, 2012). *Delitos Informáticos (México)*. Octubre 2018, de Estudiante Sánchez López Karla para monografias.com Sitio web:https://www.monografias.com/trabajos94/delitosinformaticos/delitosinformaticos.shtml

empresa japonesa Play Station, en el cual robaron la base de datos de sus clientes con cuenta en sus servidores.

Esta clasificación identifica delitos informáticos y los actores que participan en la misma y en esta se puede identificar el fraude el cual para el tema centrar de nuestra investigación, funge como parte de los delitos que el "carding online" realiza.

Así mismo cabe resaltar que esta clasificación de los tipos de delitos cibernéticos es enunciativa y no limitativa debido a la singularidad que tienen este tipo de ilícitos, como lo he mencionado con anterioridad este tipo de delitos pueden tener diferente forma de ser catalogados acorde al territorio donde suceden.

Por otro lado, se tiene una clasificación de este tipo de delitos acorde hacia donde se dirigen o la parte que afectaran de los sistemas informáticos, la cual es la siguiente:

Existe una clasificación realizada por la Unión Europea para este tipo de ilícitos realizada en 2001 la cual es la siguiente:

Clasificación según el "Convenio sobre la Ciberdelincuencia de 1 de Noviembre de 2001

Con el fin de definir un marco de referencia en el campo de las tecnologías y los delitos para la Unión Europea, en Noviembre de 2001 se firmó en Budapest el "Convenio de Ciberdelincuencia del Consejo de Europa". En este convenio se propone una clasificación de los delitos informáticos en cuatro grupos:

Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos:

Acceso ilícito a sistemas informáticos.

Interceptación ilícita de datos informáticos.

Interferencia en el funcionamiento de un sistema informático.

Abuso de dispositivos que faciliten la comisión de delitos.

Algunos ejemplos de este grupo de delitos son: el robo de identidades, la conexión a redes no autorizadas y la utilización de spyware y de keylogger.

Delitos informáticos:

Falsificación informática mediante la introducción, borrado o supresión de datos informáticos.

Fraude informático mediante la introducción, alteración o borrado de datos informáticos, o la interferencia en sistemas informáticos.

El borrado fraudulento de datos o la corrupción de ficheros algunos ejemplos de delitos de este tipo.

Delitos relacionados con el contenido:

Producción, oferta, difusión, adquisición de contenidos de pornografía infantil, por medio de un sistema informático o posesión de dichos contenidos en un sistema informático o medio de almacenamiento de datos.

Delitos relacionados con infracciones de la propiedad intelectual y derechos afines:

Un ejemplo de este grupo de delitos es la copia y distribución de programas informáticos, o piratería informática.

Con el fin de criminalizar los actos de racismo y xenofobia cometidos mediante sistemas informáticos, en enero de 2008 se promulgó el "Protocolo Adicional al Convenio de Ciberdelincuencia del Consejo de Europa" que incluye, entre otros aspectos, las medidas que se deben tomar en casos de:

Difusión de material xenófobo o racista.

Insultos o amenazas con motivación racista o xenófoba.

Negociación, minimización burda, aprobación o justificación del genocidio o de crímenes contra la humanidad.

Ejemplos:

Instrucciones que producen un bloqueo parcial o total del sistema.

Destrucción de programas por cualquier método.

Atentado físico contra la computadora, sus accesorios o sus medios de comunicación.

Secuestro de soportes magnéticos con información valiosa, para ser utilizada con fines delictivos.

Adicionalmente, la OCDE elaboró un conjunto de normas para la seguridad de los sistemas de información, con la intención de ofrecer las bases para que los distintos países pudieran erguir un marco de seguridad para los sistemas informáticos.

1. En esta delincuencia se trata con especialistas capaces de efectuar el crimen y borrar toda huella de los hechos, resultando, muchas veces, imposible de deducir como es como se realizó dicho delito.

2. Convierten en un medio idóneo para la comisión de nuevos tipos de delitos que en gran parte del mundo ni siquiera han podido ser catalogados.

3. La legislación sobre sistemas informáticos debería perseguir acercarse lo más posible a los distintos medios de protección ya existentes, pero creando una nueva regulación basada en los aspectos del objeto a proteger: la información.

En este punto debe hacerse un punto y notar lo siguiente:

- No es la computadora la que atenta contra el hombre, es el hombre el que encontró una nueva herramienta, quizás la más poderosa hasta el momento, para delinquir.

- No es la computadora la que afecta nuestra vida privada, sino el aprovechamiento que hacen ciertos individuos de los datos que ellas contienen.

- La humanidad no está frente al peligro de la informática sino frente a individuos sin escrúpulos con aspiraciones de obtener el poder que significa el conocimiento.

- Por eso la amenaza futura será directamente proporcional a los adelantos de las tecnologías informáticas.

- La protección de los sistemas informáticos puede abordarse desde distintos perspectivas: civil, comercial o administrativa.

Lo que se deberá intentar es que ninguna de ellas sea excluyente con las demás y, todo lo contrario, lograr una protección global desde los distintos sectores para alcanzar cierta eficiencia en la defensa de estos sistemas informáticos."[65]

En este tipo de delitos el interés jurídico a tutelar varía debido a que puede ser desde la información, que se procesa y almacena en un sistema informático, la propiedad, de una persona que realiza transacciones dentro de un sistema informático, o inclusive la vida, la cual aunque pueda parecer ambiguo o difícil de entender, puede suceder por ejemplo en el caso del bullyng este delito después de un tiempo puede desencadenar en la muerte del afectado, situación que hace indispensable contar con normas que prevean las penas aplicables para quienes desplieguen conductas que atenten contra la privacidad e integridad de esa información.

En México se produjo un cambio sustancial para el análisis, clasificación y penalidad de los delitos informáticos a partir de la reforma de 1999.

"El Estado mexicano, obligado a proteger los bienes jurídicos de los sectores que utilizan la informática como instrumento de desarrollo, requería un marco jurídico acorde al avance tecnológico, que permitiera prevenir y sancionar conductas que lesionaran o pusieran en peligro tales bienes.

Con anterioridad a la reforma al Código Penal Federal de 1999, sólo algunos estados de la República, como Sinaloa, Morelos y Tabasco, conscientes de la necesidad de legislar en esta materia, habían incorporado en sus ordenamientos penales normas tendentes a la protección

[65] Segu. Info. Seguridad de la información. (2000-2009). *Legislación y Delitos Informáticos - La Información y el Delito*. Octubre 2018, de Seguridad de la información Sitio web: https://www.segu-info.com.ar/legislacion/

de la información mediante la tipificación del delito informático y del de violación a la intimidad personal.

“La inexistencia, hasta antes de 1999, de tipos penales exactamente aplicables a esas conductas ilícitas daba lugar a la impunidad, de manera que resultaba imperativo prever en la ley estas nuevas formas de delincuencia. La magnitud de los daños que esas conductas pueden ocasionar depende de la información que se vulnere, la cual puede tener un fuerte impacto en el desarrollo de la economía y la seguridad nacionales, o en las relaciones comerciales, tanto el sector público como privado.

Por tal motivo, resultaba necesario proteger la privacidad e integridad de la información contenida en sistemas y equipos de cómputo, así como su almacenamiento o procesamiento. Tal situación impulsaba a establecer normas que sancionaran a quienes, sin tener derecho a ello, accedieran a los equipos y sistemas de terceras personas para vulnerar la privacidad de la información, dañarla, alterarla o provocar su pérdida.

La iniciativa que presentó el Congreso mexicano y que dio origen a las reformas publicadas en el Diario Oficial de la Federación el 17 de mayo de 1999, propuso adicionar un capítulo al Código Penal Federal para sancionar al que sin autorización acceda a sistemas y equipos informáticos protegidos por algún mecanismo de seguridad, con el propósito de conocer, copiar, modificar o provocar la pérdida de información que contengan. Esta iniciativa dio origen al capítulo denominado “Acceso ilícito a sistemas y equipos de informática”, que comprende los artículos 211 bis 1 al 211 bis 7, tutelándose así, a partir de dicha reforma, el bien jurídico consistente en la privacidad y la integridad de la información.

A su vez, se propuso establecer una pena mayor cuando las conductas son cometidas en agravio del Estado, pues la utilización de sistemas de cómputo, computadoras, bases de datos y programas informáticos es cada vez mayor, como lo es la regulación por las leyes federales; tal es el caso de la Ley de Información, Estadística y Geográfica, la Ley del Mercado de Valores, la Ley que Establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública y la Ley

Federal para el Control de Precursores Químicos, Productos Químicos Esenciales y Máquinas para Elaborar Cápsulas, Tabletas o Comprimidos, entre otras.

Además, en virtud de que las instituciones que integran el sistema financiero han sido con mayor frecuencia las víctimas por la comisión de estas conductas, se creó un artículo específico para proteger la información propiedad de aquéllas, el cual permite aumentar la pena hasta en una mitad cuando las conductas previstas sean cometidas por miembros de las propias instituciones.

Las referidas disposiciones, que fueron adicionadas al Código Penal Federal en el año de 1999, esencialmente tipifican comportamientos de quienes son conocidos en el ámbito de la informática como hackers o crackers, personas que atentan contra sistemas de cómputo.

“Jesús Antonio Molina Salgado “La legislación mexicana en materia de delitos informáticos dista mucho de ser perfecta, es sólo el primer paso para lograr un ambiente sano y seguro para los negocios y comunicaciones electrónicas en nuestro país.

Algunas críticas a estas disposiciones, se pueden resumir en los siguientes términos:

• Se constituye el delito sólo si se accede a un sistema informático protegido por un mecanismo de seguridad. Esto es tan absurdo como si dijéramos que para que se actualice el delito de allanamiento de morada es necesario que la casa habitación cuente con un candado, llave, portón o cadena protectora. La justicia no puede limitarse a quienes tienen los medios económicos para proteger su computadora con un mecanismo de seguridad.

• El ordenamiento penal no define lo que debe entenderse por “mecanismo de seguridad” de un sistema informático. ¿Debemos entender por ello una clave de acceso (password)?, ¿un candado contra robo (físico)?, ¿un sistema criptográfico de llave pública?, o simplemente ¿tener la computadora encerrada en un cuarto bajo llave? Esta falta de precisión originará innumerables problemas de interpretación.

• El código no contempla todos los tipos más comunes de ataques informáticos.

• El capítulo adicionado mediante la reforma del 17 de mayo de 1999 denomina incorrectamente: "Acceso ilícito a sistemas y equipos de informática", ya que su articulado no se refiere exclusivamente a esa conducta.

• Además, ataques informáticos se perpetran sin necesidad de acceder directamente a un sistema informático. El mejor ejemplo es la "denegación de servicios" (denial of services o distributed denial of services), cuyo objetivo no es "modificar, destruir o provocar pérdida de la información", como reiteradamente lo establece el Código Penal Federal, sino simplemente imposibilitar o inhabilitar temporalmente un servidor para que sus páginas o contenidos no puedan ser consultados mientras el servidor esté fuera de servicio o caído."[66]

"Por su parte, el jurista mexicano Raúl Carrancá y Rivas escribe sobre esta reforma en la nota referente al artículo 211 bis 7: "En la especie, y en cuanto hace a la acción delictiva, no hay a mi juicio sino tres posibilidades: que se actúe terroristamente, en provecho propio o en provecho ajeno. Si se trata de lo primero, habría que remitirse al artículo 139 del Código Penal, siendo innecesaria, en consecuencia, la inclusión en el Código de este nuevo tipo. Por lo que atañe a la información obtenida y utilizada en provecho propio o ajeno, excepción hecha del terrorismo como ya queda dicho, a mi juicio es evidente que se da en todos los casos, o sea, es parte substancial de la acción delictiva. No es un añadido, un agregado de la acción. En consecuencia para qué agravar las penas"[67]

"Otros autores disienten de la posición del doctor Carrancá y Rivas, aduciendo que, si bien en su mayoría son organizaciones delictivas las que realizan este tipo de conductas, también es cierto que existen particulares que no obtienen provecho alguno con el acceso a ciertos bancos de información, como es el caso de quien ingresa de manera ilícita al correo electrónico de otra persona para conocer el contenido de sus comunicaciones, transgrediendo así el ámbito de su

[66] Landa Durán, G. (Julio 2007). *Los delitos informáticos en el Derecho penal de México y España*. Diciembre 2018, de Revista del Instituto de la Judicatura Federal. Núm., 24 Sitio web: https://app.vlex.com/#sources/4800/issues/173617

[67] Carrancá y Trujillo, R. & Carrancá y Rivas R. (2000). *Código Penal anotado*. México: Porrúa.

intimidad, por lo que la conducta ilícita puede ocurrir fuera del contexto precisado por el doctor Carrancá." [68]

México fue uno de los primeros países a nivel Latinoamérica en implementar una reforma al sistema de justicia penal para iniciar la inclusión de los delitos informáticos o cibernéticos dentro de la legislación, esta inclusión tuvo como infortunio el hecho de ser realizada de manera muy temprana y con un tinte de realizarse al vapor, esto debido a que durante la inclusión de la misma los medios informáticos estaban en un desarrollo prematuro.

Situémonos contextualmente en esa época y contexto histórico, la época durante la cual se realizó esta reforma fue cuando los medios informáticos empezaban su distribución masiva, es decir para 1999 los hogares que contaban con una computadora era muy bajo, aun se vivía una época donde la realización de trámites, trabajos, búsqueda y envió de información se realizaba de la manera tradicional, es decir mediante bibliotecas, uso de correo postal, uso de cuadernos y libretas y esto solo por ejemplificar; todo esto hablando de población en general ahora si esto lo vemos a nivel Estado es sumamente menor el alcance y penetración de los medios informáticos dentro de él; todo esto tiene como consecuencia que esta primera reforma penal quedara sumamente corta y realizada al vapor porque si el proceso legislativo es sumamente complejo identificando plenamente e delito, ahora imaginemos que tan complejo es realizar una reforma penal sin identificar plenamente el delito, esto es similar a realizar una reforma a ciegas.

Por consiguiente, esta quedo en una buena intención del legislador, que sirvió como precedente y allano el camino hacia las reformas que deberán de realizarse en un futuro cercano.

2.6 Instituciones facultadas para atender delitos cibernéticos

Durante la realización de un delito se puede saber de manera relativamente rápida y acertada quien es la institución encargada para darle seguimiento a la investigación de este hecho, así mismo se podría determinar el lugar donde ocurrió el mismo con un rango mínimo de error, citando un ejemplo en el momento de la realización de un robo se puede tener certeza de con

[68] Op.cit.

qué autoridad asistir y se puede determinar el lugar donde se realizó dicho ilícito rango mínimo de error, esto le da una certeza relativa en su actuar a una persona víctima de un delito.

Sin embargo, en el supuesto de la comisión de un delito cibernético, durante la ejecución de estos se presentan diversas dificultades para determinar estas hipótesis como, por ejemplo:

-Lugar de los hechos

-Autoridad competente0

-Objeto del delito

-Clasificación de delito

Y esto solo por citar algunas, situación que dificulta la forma que la víctima debe de actuar después ser víctima del ilícito.

Ya que surgen diversas dudas de forma común como son:

¿Dónde acudir?

¿Qué tipo de delito es?

¿Qué autoridad es competente?

Este tipo de delitos cibernéticos o informáticos son sumamente complejos, en primera instancia de identificar y en segunda instancia cometido el mismo en el actuar de la víctima después de haber sufrido el mismo.

Por ejemplo en México repasemos el mismo delito de robo, en el sentido de un robo tradicional, la victima sabe que debe de asistir a una agencia del ministerio público y tiene la certeza de cómo actuar y como indicarle los hechos al agente del ministerio público; la victima podrá indicar el horario en que se realizó el delito, la forma en que le despojaron de sus bienes, si el infractor tenía un arma, podrá indicar el lugar donde sucedieron los hechos, podrá dar cuantía de los robado, y demás comentarios que puedan ayudar en el esclarecimiento del ilícito; sin embargo en un delito informático, por ejemplo el robo del saldo de una cuenta de ahorro a un

cuentahabiente, de inicio la víctima del delito puede tardar tiempo indeterminado en identificar el delito, aunado a ello la victima de manera individual no podrá saber en qué momento determinado se realizó el delito, probablemente con la involucración y el apoyo de un tercero que sería la Institución Financiera donde tenía su cuenta podrá determinar este horario, la persona que realizó el delito podría estar en otro estado o inclusive país, pero sobretodo de manera inicial la victima de este ilícito de manera común no sabe con qué autoridad dirigirse para dar seguimiento al ilícito, existen victimas que acuden a la Procuraduría General de la República (P.G.R.) algunas otras asisten a la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUCEF)..

Por tanto, se debe conocer y entender la forma en que el Estado Mexicano atiende, actúa y da seguimiento a este tipo de delitos para poder actuar de la manera correcta y mejorar tiempos y procesos para este tipo de ilícitos.

2.6.1 Procuraduría General de la Republica

La procuraduría General de la Republica surge como respuesta a la separación necesaria de las funciones de impartir justicia por parte del Estado Mexicano, esto debido a que hasta antes del surgimiento de dicha institución el Estado mexicano tenía una función de juez y parte en la impartición de justicia dentro del territorio mexicano. Su fundamento radica en el artículo 102 de la Constitución Política de los Estados Unidos Mexicanos el cual indica:

Articulo 102.-

A. “El Ministerio Público de la Federación se organizará en una Fiscalía General de la República como órgano publico autónomo, dotado de personalidad jurídica y patrimonio propio

En este sentido la Constitución Política de los Estados Unidos Mexicanos indica la forma en que se organizará al Ministerio Público de la Federación y crear un órgano público autónomo dotado de personalidad jurídica propia como es en este caso la Procuraduría General de la Republica.

"La Procuraduría General de la República es el órgano del poder Ejecutivo Federal, que se encarga principalmente de investigar y perseguir los delitos del orden federal y cuyo titular es el Procurador General de la República, quien preside al Ministerio Público de la Federación y a sus órganos auxiliares que son la policía investigadora y los peritos.

Es la encargada del despacho de los asuntos que la Constitución Política de los Estados Unidos Mexicanos, la Ley Orgánica de la Procuraduría General de la República, su Reglamento y otros ordenamientos, le encomiendan al Procurador General de la República y al Ministerio Público de la Federación.

Misión

Contribuir a garantizar el Estado democrático de Derecho y preservar el cumplimiento irrestricto de la Constitución Política de los Estados Unidos Mexicanos, mediante una procuración de justicia federal eficaz y eficiente, apegada a los principios de legalidad, certeza jurídica y respeto a los derechos humanos, en colaboración con instituciones de los tres órdenes de gobierno y al servicio de la sociedad.

Visión

Institución de Procuración de Justicia eficiente, eficaz y confiable, integrada por servidores públicos éticos, profesionales y comprometidos; sólidamente organizada bajo un enfoque integral y operativamente ágil; con contundencia legal y cercana a la sociedad, que coadyuve al desarrollo del país y al disfrute de las libertades y derechos en la Nación."[69]

Este de manera global es el alcance y lineamiento sobre los cuales se rige la Procuraduría General de la Republica, es decir se identifica claramente que la misma es un órgano creado para investigar y perseguir delitos federales, así mismo podemos ver que esta depende del Gobierno Federal, desglosando que de igual manera su presupuesto es de índole federal y podemos saber que la preside el Procurador General de la Republica.

[69] Procuraduría General de la Republica. (2018). *¿Qué Hacemos?*. Diciembre 2018, de Fiscalía General de la Republica Sitio web: https://www.gob.mx/pgr/que-hacemosquobit.mx.(abril 21,2018).

Retomando que la PGR es un órgano mediante el cual se atiende y da seguimiento a los diversos delitos federales cometidos dentro del territorio nacional, por tanto debemos determinar ¿qué tipo de delito son los delitos informáticos? y esto lo podemos encontrar en el Código Penal Federal en el siguiente apartado:

"Capitulo II

Acceso ilícito a sistemas y equipos de informática

Artículo 211 bis 1.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

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.

Artículo 211 bis 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, 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.

Las sanciones anteriores se duplicarán cuando la conducta obstruya, entorpezca, obstaculice, limite o imposibilite la procuración o impartición de justicia, o recaiga sobre los registros relacionados con un procedimiento penal resguardados por las autoridades competentes.

Artículo 211 bis 3.- Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.

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 cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, 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, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública.

Artículo 211 bis 4.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Artículo 211 bis 5.- Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, 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.

Artículo 211 bis 6.- Para los efectos de los artículos 211 Bis 4 y 211 Bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 Bis de este Código.

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.

Por tanto, al ser delitos que se encuentran tipificados en el Código Penal Federal podemos clasificarlos como delitos federales y por ende estos serán investigados y se les dará seguimiento por parte de la Procuraduría General de la Republica.

Sin embargo en el momento de revisar de manera analítica cada uno de los tipos identificados y descritos dentro del Código Penal Federal estos no conllevan todos los tipos de delitos informáticos o cibernéticos que se realizan de manera actual; situación que deja al afectado o víctima de este tipo de delitos, en un estado de indefensión y delimita las funciones del Ministerio Publico.

Es del conocimiento común aquel tipo de delito que no se encuentre normado aun a pesar del daño que este le ocasione al afectado, el órgano judicial no podrá intervenir; a este tipo de situaciones debemos de sumarizar el hecho de que en variadas ocasiones la laguna en la legislación, la falta de conocimiento en el tema del órgano judicial competente y/u otra infinidad de etcéteras tienen como resultado que el delito se encuadre en un tipo penal diferente situación que tiene como consecuencia que al no cumplir con las diversos requerimientos necesarios del tipo penal en el que se encuadro el delito informático o cibernético este sea desechado.

Retomando lo indicado con anterioridad este tipo de delitos son de tipo federal y deben de ser absorbidos y atendidos por la Procuraduría General de la Republica, teniendo como una máxima constante que la cantidad de los mismos rebase la capacidad de dicho órgano y derivado de esto se tomó la determinación de crear la División Científica de la Policía Federal y facultar una división de Policía Cibernética estatal.

Ambas divisiones trabajan en el día a día en el seguimiento de los diversos delitos cibernéticos y también de manera muy puntual en buscar acuerdos de colaboración con diversas empresas o particulares para poder apoyarse en el seguimiento de este tipo de delitos, porque como lo indicamos con anterioridad México se encuentra en vía de desarrollo y especialización de sus diversos sistemas y divisiones de las diversas policías dentro de su territorio conforme a este tipo de ilícitos, por tanto requiere de gente especializada en este tema que pueda apoyar y dar soporte para de una u otra manera nivelar la balanza, situación que se puede validar con el acuerdo firmado por aparte de la División Científica de la Policía Federal en mayo de 2014:

“Con el objetivo de impulsar la prevención de conductas ilícitas, así como de promover la seguridad en internet, la oficina del Comisionado Nacional de Seguridad por conducto de la Policía Federal y Microsoft México, establecieron un acuerdo de cooperación para llevar a cabo acciones enfocadas al combate de los delitos cibernéticos.

La División Científica de la Policía Federal, suscribió un convenio que le permite compartir experiencias y casos de éxito en materia de detección, captación, análisis, clasificación y registro de la información, que resulte de la vigilancia y monitoreo de conductas que pudieran ser constitutivas de delitos en medios electrónicos.

En este marco, el Ex-Comisionado General de la Policía Federal Enrique Galindo Ceballos, destacó que la coordinación con Microsoft México permitirá disminuir la brecha digital para alcanzar una Policía Federal a la vanguardia, que cuente con mayor capacidad de respuesta tecnológica a favor de la ciudadanía. “Debemos aprovechar, conocer, comprender y explotar cada una de estas herramientas valiosas para que juntos las usemos y que permita colocar en una mejor posición a la Policía Federal, para perfeccionar su trabajo en beneficio de los usuarios”. Destacó Galindo Ceballos.

En el encuentro desarrollado en la Ciudad de México, el Dr. Ciro Humberto Ortiz Estrada, titular de la División Científica de la Policía Federal, resaltó que la ciberseguridad es un tema que la corporación atiende para prevenir la comisión de ilícitos, expresando_

"Las supercarreteras de la información hay que cuidarlas, protegerlas, procurarlas, ya que estas vías de comunicación generan una riqueza invaluable al país, por lo que deben ser más seguras y confiables para los usuarios". Resaltó Ortiz Estrada.

Por su parte, el Ingeniero Juan Alberto González Esparza, director de Microsoft México, aseguró que la empresa desarrolla y pone a disposición una nueva generación de servicios y de tecnologías de la información a favor de la ciberseguridad, con una amplia experiencia en el combate al crimen cibernético y en programas para prevenir conductas delictivas.

Indicando:

"Con esta iniciativa trabajaremos de la mano con la Policía Federal para poner todas nuestras experiencias, activos y acervos de conocimientos, para colaborar como pieza estratégica, para hacer más eficiente la prevención, el control y el combate a los delitos cibernéticos.

La dinámica de trabajo de la Policía Federal y Microsoft México va enfocada a establecer un marco de cooperación que le permitirá a la Policía Federal acceder a la experiencia y los activos desarrollados por esta empresa para la prevención y combate de delitos cibernéticos, entre ellos, un centro de datos contra la Delincuencia Cibernética ubicado en Redmond, Washington, en los Estados Unidos.

De esta forma, la Policía Federal refrenda su compromiso por hacer de la tecnología un aliado clave en materia de promoción y fomento a la seguridad, por lo que el acuerdo contempla también el intercambio de material informativo para concientizar a la población sobre las afectaciones y formas de prevenir los delitos cibernéticos.

Este encuentro forma parte de los trabajos que la Oficina del Comisionado Nacional de Seguridad lleva a cabo con el objetivo de aprovechar y explotar el intercambio de información, lo que permitirá combatir cualquier acto ilícito en la red pública de internet. "[70]

Este tipo de acuerdos son parte de la necesidad que tiene el sistema de justicia en México para estar a la vanguardia con el avance tecnológico, también mediante el mismo podemos discernir dos grandes vertientes encontradas en este mismo acuerdo por un lado está el sentido positivo del convenio, en el cual el órgano encargado de la procuración de justicia en materia

[70]Comisión Nacional de Seguridad. (Mayo 8, 2014). *Impulsan policía federal y microsoft México seguridad informática y prevención de delitos cibernéticos*. Octubre 2018, de Comisión Nacional de Seguridad Sitio web: http://www.cns.gob.mx/portalWebApp/appmanager/portal/desk?_nfpb=true&_pageLabel=portals_portal_page_m3p2_boletin&id=1344173

informática en México consolida sinergias positivas con una empresa particular que tiene toda la infraestructura necesaria como para poder dar soporte y apoyo en este tipo de delitos.

La otra vertiente en sentido negativo, se puede dilucidar que los delitos informáticos son un problema grande y creciente que necesitan una solución rápida y efectiva, la cual debe de ir acompañada del soporte y de una infraestructura que por ello cada estado dentro del territorio mexicano ha creado uno a uno una policía cibernética a nivel estatal para auxiliar en el seguimiento y atención de este tipo de delitos.

Surgiendo de esta determinación, por ejemplo en el caso de la Ciudad de México la Policía Cibernética de la Secretaria de Seguridad Publica de la Ciudad de México, dan seguimiento y atención a este tipo de ilícitos, tal como lo indica su página de internet:

Policía de Ciberdelincuencia Preventiva

"Como principales líneas de acción la Policía de Ciberdelincuencia Preventiva realiza:

Monitoreo de redes sociales y sitios web en general.

Pláticas informativas en centros escolares e instituciones del Distrito Federal, con el objetivo de advertir los delitos y peligros que se cometen a través de internet, así como la forma de prevenirlos, creando una cultura de autocuidado y civismo digital.

Ciberalertas preventivas las cuales se realizan a través del análisis de los reportes recibidos en las cuentas de la Policía de Ciberdelincuencia Preventiva.

Para ello ponemos a sus órdenes nuestros medios de contacto para atender reportes derivados de internet, recibir información o solicitar pláticas informativas, con atención a la ciudadanía las 24 horas y 365 días del año."[71]

[71] Gobierno de la Ciudad de México. (2018). *Policía de Ciberdelincuencia Preventiva*. Abril 2018, de Gobierno de la Ciudad de México. Secretaria de Seguridad Ciudadana Sitio web: http://data.ssp.cdmx.gob.mx/ciberdelincuencia.html

Estas instituciones son las que ha creado el Estado para poder atender las demandas de las personas físicas y morales, que se encuentran dentro de la delimitación territorial donde ellos ejercen sus funciones.

Sin embargo, estas instituciones se encuentran en un proceso de maduración y consolidación, por tanto en reiteradas ocasiones tienden a ser superadas por los infractores de este tipo de delitos.

2.6.2 Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF)

Como lo indiqué, con los delitos informáticos o cibernéticos ya se encuentran en un proceso de tipificación por parte del legislador e inclusive el mismo de manera reactiva ha comenzado con la creación de órganos e instituciones facultadas para la atención y seguimiento de los mismos. Sin embargo, estas mismas instituciones se encuentran en proceso de maduración; situación que no les permite aun dar soporte integral en tiempo y forma a toda la demanda de la población general derivada de estos ilícitos.

Así la seguridad informática, en el caso de que una persona física o moral tenga la necesidad de una protección más allá de la que el estado otorga, esta persona podrá proceder a realizar la contratación de un tercero que pueda apoyarle a subsanar esta carencia, y ahí tendremos a personas morales y personas físicas ofertando servicios desde seguridad, rastreo, resguardo y protección de la información, software y un sinfín de opciones que podrá adquirir quien así lo desee.

Por consiguiente existen diversas personas físicas y morales destinados y enfocados al seguimiento, investigación, análisis y planteamiento de mejoras y seguimiento de todo este tipo de delitos, a grandes rasgos podemos hablar de todas las compañías que fabrican software para identificar y evitar los diferentes virus que pueden ingresar a los equipos de cómputo o medios informáticos, aquellas dedicadas a crear antivirus, podemos hablar de personas físicas expertas en análisis de los patrones e identificación de los distintos tipos de delitos informáticos.

Retomando el tema central de nuestra investigación, es decir el carding online, debo de reemitir al punto inicial donde se parte hacia la ejecución de este delito es decir el Sistema Bancario Mexicano, ya que mediante la emisión de las diversas tarjetas de crédito este brinda a sus usuarios de servicios financieros la posibilidad de realizar transacciones y diversas operaciones vía online es decir internet.

Pero porque debemos de partir de este punto es sencillo ya que sin los sistemas que utiliza cada banco para realizar transacciones en línea no existiera siquiera la posibilidad de realizar este delito en específico.

Sin embargo, con el crecimiento e inmersión de la tecnología dentro del uso cotidiano de los diversos servicios financieros; las instituciones financieras se han quedado cortas en cuanto a recursos, manejo y celeridad del manejo de las diversas incidencias que se presentan en las mismas.

Motivo por el cual para poder apoyar en este tipo de incidencias se creó la Comisión Nacional para la Protección de los Usuarios de Servicios Financieros la cual se creó el 19 de abril de 1999.

Como respuesta del Estado mexicano a la necesidad de garantizar la adecuada defensa de los derechos de los usuarios de servicios financieros, hace 17 años se creó la CONDUSEF.

El 19 de Abril de 1999 entró en funciones, con el firme propósito de asesorar, proteger y defender a los usuarios ante cualquier conflicto e irregularidad que se presente entre éstos y las Instituciones que conforman el Sistema Financiero Mexicano. Así como la creación y fomento de una cultura adecuada respecto de las operaciones y uso de los servicios financieros.

“En dicho año la Comisión Nacional era un organismo conciliador, es decir, únicamente daba asesorías, atendía quejas y emitía recomendaciones a las instituciones financieras. Sin embargo, con las reformas a la Ley para la Transparencia y Ordenamiento de los Servicios Financieros de 2009, se le dan nuevas facultades para supervisar y regular temas asociados a la transparencia financiera, sanas prácticas y publicidad para la banca y otras entidades financieras que otorgan crédito.

No obstante, su cambio más amplio y trascendental se deriva de la Reforma Financiera del 2014, a través de la cual nace el Buró de Entidades Financieras, se emiten las disposiciones en materia de sanas prácticas para los despachos de cobranza de las instituciones financieras, la prohibición de cláusulas abusivas en los contratos de adhesión, el nuevo Sistema Arbitral y la emisión de dictamen como título ejecutivo.

Si bien es cierto que en su primer año de operación (1999), la CONDUSEF apenas realizó en total 93 mil 160 acciones de defensa, en el año 2015 se registraron casi 1 millón 500 mil, logrando acumular a lo largo de sus 17 años poco más de 12.1 millones de acciones de defensa a través de sus 36 delegaciones."[72]

Por consiguiente, se debe entender que la CONDUSEF pasó de ser un conciliador sin mayor injerencia que el de dar una recomendación a las instituciones en el Sistema Financiero Mexicano durante la década de 2000 a 2010, a convertirse en la siguiente década, es decir 2011 a la fecha en una entidad con un contrapeso entre usuarios e instituciones específico y con facultadas para sancionar e imponer multas.

CONDUSEF se enfoca en dar orientación y atender quejas de los usuarios de servicios financieros, y en el debido proceso el usuario en primera instancia deberá de ingresar seguir para levantar una queja por cualquier anomalía en los servicios contratados con una entidad del Sistema Financiero Mexicano por parte de un usuario de servicio financiero en México.

[72] Gobierno de México. (2013). Página Oficial. Abril 2018, de Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros Sitio web: https://www.gob.mx/condusef

Por consiguiente para el caso concreto de esta investigación es necesario entender el proceso a seguir para atender los delitos informáticos que van en contra del sistema financiero mexicano, en concreto los bancos, el cual como he de aclarar inicia con el levantamiento de la queja ante la entidad financiera con la que el usuario sufrió el delito informático; después de realizar esto el usuario afectado por dicho ilícito deberá de dar seguimiento con la entidad financiera a la queja realizada, en caso de que la institución financiera resuelva la queja el usuario se dará por satisfecho, en caso de que no el usuario podrá acudir a la siguiente instancia que será CONDUCEF e iniciar el proceso de su queja ante dicha dependencia y esta institución resolverá dicha queja, la cual puede o no satisfacer al usuario y este en caso de quedar satisfecho, dará por cerrada la queja, en caso de no ser así, podrá recurrir con la policía cibernética del estado donde sucedió el ilícito para poder dar seguimiento al mismo y en este caso la misma policía

cibernética deberá de dar una resolución al asunto dando el cierre al ilícito cometido en contra del usuario del servicio financiero.

2.7 Tópicos que dificultan seguimiento a delitos cibernéticos:

Existen diversos tópicos que dificultan el seguimiento de los diversos delitos cibernéticos o informáticos como que pueden ser cometidos desde un territorio específico y afectar a una persona ubicada en otro territorio, situación que también afecta la jurisdicción de la autoridad competente y la competencia de la misma autoridad.

Creando diversas interrogantes que de no ser planteadas de manera correcta generarán dudas que tendrán como consecuencia la intervención de manera equívoca de la autoridad o en su defecto la nula intervención de la misma, derivado de la mala interpretación del delito.

2.7.1 Jurisdicción

"La palabra jurisdicción proviene del latin iurisdictio, onis, que significa poder o autoridad que tiene uno para gobernar o poner en ejecución las leyes para aplicarlas en juicio" (Real Academia Española.1984)

"La jurisdicción es la parte del derecho procesal que como función del Estado tiene por objeto regular y organizar la administración de justicia y seguridad jurídica mediante los órganos especializados y competentes para resolver en forma imparcial las controversias y planteamientos jurídicos, con base en reglas de procedimiento establecidas para la sustanciación de procesos."[73]

En relación con el lugar que la jurisdicción ocupa dentro del derecho, el maestro Niceto Alcalá-Zamora y Castillo señala que sabe con precisión su encuadramiento, ya sea en la ciencia del derecho procesal o en la del derecho constitucional, lo que deriva de su situación de confluencia, en virtud de que esta institución debe ser analizada desde dos ángulos y perspectivas, tomando en cuenta que para el constitucionalismo, es una de las tres funciones

[73] Ponce de León Armenta, L. (1992). *La Jurisdicción*. Abril 2018, de Instituto de Investigaciones Juridicas (UNAM) Sitio web: https://revistas.juridicas.unam.mx/index.php/derecho-comparado/article/view/2919/3175

del Estado y que para el procesalista es la actividad del propio Estado, que imparte la función jurisdiccional a través del proceso"[74]

"Solo puede hablarse de plenitud de la norma jurídica cuando existe la posibilidad real procesal o instrumental de su aplicación mediante la jurisdicción, la acción y el proceso; de lo contrario, consideramos que la expresión legislativa se convierte en principio de derecho o simple aspiración."[75]

La jurisdicción es la facultad que tiene una persona para poder imponer o aplicar la ley sobre una persona determinada, esta es derivada de la soberanía del Estado, esta es irrevocable y definitiva, es decir que la autoridad que tiene jurisdicción sobre un asunto determinado, tiene la facultad de imponer y aplicar la norma jurídica de una manera coercitiva y unilateral apegada a derecho.

Sin embargo, la jurisdicción en el sentido de los delitos informáticos tiene un tinte complejo, derivado de que este tipo de delitos tienen la dificultad de poder ser encuadrados de manera correcta, es decir en primera instancia identificar el tipo de delito por ejemplo el fraude de tarjeta de crédito, puede ser encuadrado como un simple fraude o que tal un robo de identidad, el cual en primera instancia es difícil de detectar al parecer que los hechos fueron realmente realizados por el afectado; por consiguiente al no poder ser encuadrados y ubicados este tipo de delitos; será complicado determinar la jurisdicción al decir el derecho conociendo, resolviendo y ejecutando, teniendo como medida o contenido a la competencia.

2.7.2 Competencia

"La competencia es la medida de la jurisdicción por limites en cuanto la materia, cuantía, grado, turno, territorio imponiéndose por tanto una competencia, por necesidades de orden práctico.

[74] Medina, I. (enero-junio de 1977). *Problemática de la jurisdicción voluntaria*. Revista de la facultad de Derecho, números. 105-106. p.229.

[75] Ponce de León Armenta, L. (1992). *La Jurisdicción*. Abril 2018, de Instituto de Investigaciones Juridicas (UNAM) Sitio web: https://revistas.juridicas.unam.mx/index.php/derecho-comparado/article/view/2919/3175

Se considera, entonces, tanto como facultad del juez para conocer en un asunto determinado, como también el conflicto que puede existir por razón de competencia.

La jurisdicción es el género, mientras que la competencia viene a ser la especie, todos los jueces tienen jurisdicción, pues tienen el poder de administrar justicia, pero cada juez tiene competencia para determinados asuntos.

División de clases de competencia.

Se consideraba antiguamente dividida la competencia por razón de la materia, de calidad de las personas, y su capacidad y finalmente por el territorio. Sin embargo, la clasificación más aceptada es la considerada como la competencia objetiva en cuanto al valor y la naturaleza de la causa; competencia territorial. Otras clasificaciones aunque tienen valor doctrinario, no se ajustan a la realidad, a una sistemática clasificación como la anteriormente mencionada.

Competencia objetiva, funcional y territorial.

La competencia objetiva es la que se encuentra determinada por la materia o el asunto, como la cuantía, elementos determinantes. Así, que para los asuntos civiles y comerciales en el país, son competentes los jueces especializados en lo civil así como para los asuntos penales lo serán los especializados en lo penal y para los asuntos laborales los que conocen de esta especialidad, ahora incorporadas por tal razón dentro del Poder Judicial totalmente unificado.

El criterio de cuantía es determinante para la competencia de un juzgado, pues mientras esta cuantía sea mínima, puede presentarse la competencia el juez de paz o de cuantía menor, mientras que si pasa el límite señalado establecido por la ley, será competencia del juez de Primera Instancia. En nuestro ordenamiento procesal, se dan las reglas para determinar el valor del juicio, en ese caso de dificultad, contenidas en los nuevos reglamentos procésales.

La competencia funcional, corresponde a los organismos judiciales de diverso grado, basada en la distribución de las instancias entre varios tribunales, a cada uno de los cuales le corresponde una función; cada instancia o grado se halla legalmente facultado para conocer determinada

clase de recursos (Primera Instancia, Corte superior, Corte Suprema), también conocida como límite de competencia en razón de grado.

Las disposiciones sobre competencia, son imperativas con lo que se quiere explicar que deben ser acatadas necesariamente; si un tribunal carece de competencia, debe inhibirse y los interesados en su caso están asistidos del perfecto derecho de ejercer la impugnación que creyeran conveniente.

Las normas contenidas en la Ley Orgánica del Poder Judicial, fijan en nuestro país, los grados o instancias de los Juzgados de Primera Instancia, Cortes Superiores y 2nda. Instancia y en materia de Amparo los Tribunales Colegiados de Circuito y excepcionalmente la Suprema Corte de Justicia de la Nación.

Competencia Territorial. Se justifica por razones geográficas o de territorio en la que se encuentra distribuidos los juzgados y tribunales superiores de cualquier país; se refiere a esta clase de competencia únicamente a los organismos de primera instancia puesto que los tribunales superiores intervienen solo en razón de su función.

Antiguamente esta competencia se conocía con el nombre de fuero; había el fuero general y el especial; el fuero general ha sido el domicilio del demandado en que podía ser emplazado para cualquier clase de procesos; el fuero especial constituía la excepción; a estos fueros se agregaban los fueros en razón de la persona o de sus bienes.

Para los casos del fuero instrumental, o sea para la prestación de la obligación contractual o cuasi contractual, se sigue la misma norma de ser competente el juez del domicilio de la persona a la cual se demanda (domicilio del demandado), pero en nuestro país puede a elección demandar ante el juez del lugar señalado para el cumplimiento de la obligación; o ante el juez donde desempeña la administración, en las demandas sobre rendición y aprobación de cuentas."[76]

[76] Rodríguez, J. (2009). *La Competencia*. Diciembre 2018, de Monografia.com Sitio web: https://www.monografias.com/trabajos7/compro/compro.shtml

La competencia es la que determina si un juez tiene facultades para conocer de un asunto, por tanto esta podrá ser una causa de exclusión para conocer del mismo, así mismo en caso de no cumplir de manera completa con cada uno de los filtros que la misma requiere para que el juez conozca del asunto; el mismo no deberá de participar en este, por ejemplo aun a pesar de que el juez sea competente por territorio si el mismo no es competente por cuantía no deberá de intervenir y en el supuesto de que un juez conozca del asunto sin haber cumplido con todos los requisitos de competencias las parte afectada podrá hacer valer incompetencia.

Así en el caso de la jurisdicción, en el supuesto de la comisión de un delito cibernético es complejo determinar diferentes elementos para clasificar el mismo; ahora en el caso de la competencia es aún ambiguo y difícil la intervención de la autoridad competente de manera plena, esto debido a que en este tipo de delitos es complejo determinar todas las variables que indaguen de manera plena quien es la autoridad competente, ya que habrá que identificar el territorio en la comisión del delito sin embargo, en estos delitos puede el infractor cometerlo en un territorio determinado y la persona afectada puede estar en un territorio diferente, creando una dificultad para definir a la autoridad competente y así en cada uno de los elementos que deben de cumplirse a cabalidad para que la autoridad sea competente de manera plena.

Capítulo tres: Carding online

3.1 Definición de carding online

Identificando que es un delito informático y/o cibernético, se tomara en cuenta que cualquier tipo de movimiento, uso, búsqueda y/o cualquier tipo de actividad que se realice en internet deja un rastro y el mismo es imposible de borrar, situación que hace necesario tener cuidado y ser consiente en el uso de la información que se sube, envía y se hace del conocimiento público por internet.

En el contexto social en el que nos desenvolvemos actualmente el uso de internet es el medio por el cual se pueden realizar diversas tareas, situación que lo empieza a volver indispensable.

Y en el caso de los servicios financieros que se brindan en México se está volviendo la herramienta base sobre la cual, dichas instituciones están montando sus diversos servicios ofertados, esto derivado a que reduce costos de manera exponencial y la gente de manera general no tiene el tiempo necesario para estar acudiendo a una sucursal a realizar sus diversos trámites, por lo cual se están empezando a otorgar

Carding online es un delito informático en el cual una persona X realiza transacciones u operaciones financieras en internet mediante el ingreso de los dieciséis dígitos de una tarjeta de crédito o debido de una persona Y, sin el consentimiento de la misma.

3.2 Antecedentes y surgimiento de carding online

Para entender el origen de la tarjeta de crédito se debe de remontar al origen de los primeros sistemas de intercambio es decir el trueque, el cual es el origen del comercio situación que con el devenir de los años y el avance del mismo desencadeno en el uso de diversos medios pago que a su vez originaron el uso del crédito y con este la generación de diversos medios de pago y de uso del mismo, que tendría como resultado el desarrollo del método de pago mediante de la tarjeta de crédito.

“El sistema de intercambio o trueque de mercancías impulsó al hombre a solicitar crédito para sus actividades agrícolas a otras personas, quienes por lo general eran representantes de la iglesia. El hecho descrito constituye un caso clásico de intermediación financiera que ilustra claramente el proceso de captación de recursos monetarios. Más importante aún es observar que hace 4000 años quedaban definidas las principales funciones de una intermediaria financiera las cuales fueron: Custodia de fondos, Transferencia de fondos y Concesión de crédito.

La intermediación financiera apareció y floreció en diferentes regiones a medida que las actividades agrícolas o comerciales se fueron arraigando y generalizando en diferentes partes del mundo. A través del tiempo surge la banca moderna con instituciones que ejercían la intermediación monetaria atendiendo a todo cliente que se acercara en su mayoría, a título individual

Otras industrias aparte de la netamente financiera, daba origen a nuevos sistemas de concesión de crédito de transferencia de fondos y de uso de medios de pago. Durante la época colonial, en los Estados Unidos surgió el crédito para compras al detalle como resultado de la escasez de circulante, pero no fue sino 200 años después que se introdujo el concepto de crédito. “[77]

Este tipo de operaciones comerciales con montos mayores cada vez, tuvieron como consecuencia la necesidad de financiamiento por parte de terceros, situación que abrió la escena para la incorporación de las instituciones financieras en esta intermediación, sin embargo para poder llevar el control de estos créditos se necesitaba de un medio en el cual poder tener la información del deudor y poder trasladar la información de un lado a otro de manera oportuna, expedita y sin correr mayor riesgo situación que dio pie a la pionera inclusión de la tarjeta de crédito.

[77]Rodríguez, B. (Marzo 1, 2007). Origen y evolución histórica de las tarjetas de crédito. Dicoembre 2018, de gestiopolis.com Sitio web: https://www.gestiopolis.com/origen-y-evolucion-historica-de-las-tarjetas-de-credito/

“1920

En Estados Unidos, la empresa pionera Western Union, comienza a entregar a un grupo selecto de sus clientes una placa de metal que les permitía identificarse y diferir sus pagos. Hoteles, tiendas departamentales, empresas de ferrocarriles copiaron la idea

1924

Entre las grandes compañías de petróleo, la General Petroleum Corporation fue la primera en emitir una tarjeta de crédito para gasolina.

1929

La depresión económica obstaculizó su crecimiento y las cuentas en mora se incrementaron de manera alarmante.

1932

Algunas empresas inician la tarea de revivir las tarjetas de crédito con el argumento de incrementar las ventas. La American Telephone & Telegraph emite la tarjeta de crédito Bell.

1942

La Segunda Guerra Mundial, retrasó el despegue definitivo de las tarjetas de crédito. El Federal Reserve Board expide el Reglamento W, que restringe el uso del plástico hasta que terminara la contienda.

1946

Flatbush Bank, de New York, introduce el plan charge-it, emitiendo vales para que sus clientes pudieran comprar en comercios afiliados al sistema.

1950

Dos jóvenes abogados llamados Frank McNamara y Ralph Schneider cenaban en un elegante restaurante de Nueva York; llegando el momento de pagar, ambos se dieron cuenta de que habían olvidado sus billeteras. De ahí surgió la idea de crear un club que reuniera a personas que frecuentaban ciertos restaurantes y que permitiera mediante la presentación de una credencial, efectuar los pagos a través de una factura bancaria. Era el embrión de las tarjetas de crédito actuales.

1951

El Franklin National Bank, de Long Island, expide la primera tarjeta bancaria y era aceptada por los comerciantes adheridos al sistema. Si alguien se excedía en los límites establecidos, el comerciante llamaba al banco para que éste aprobara la transacción.

1959

American Express presentó la primera tarjeta de plástico (tarjetas anteriores estaban hechas de cartón o de celuloide).

1960

Fue inventada la banda magnética por IBM. Las primeras tarjetas con este dispositivo fueron usadas en el transporte público de Londres.

1960

En Estados Unidos son emisores de tarjetas de crédito las principales cadenas de almacenes de venta al por menor (entre ellas Sears), la Asociación de Líneas Aéreas, la AT&T (principal compañía de teléfonos), la cadena de hoteles Hilton, etc.

1962

Dos de los bancos más importantes, el Chase Manhattan Bank y el Morgan Guarantee Bank, tuvieron grandes pérdidas y resolvieron transferir sus carteras en este año. Un banco inglés de primera línea, el Barclays Bank, emite una tarjeta, dando origen a la utilización masiva en Europa.

1966

El Bank of America (luego Visa) estableció una organización nacional para otorgar franquicias de operación de tarjetas BankAmericard.

1967

Un grupo de bancos de California desarrolló un programa de tarjetas de crédito llamado Master Charge, que eventualmente cambio su nombre a MasterCard.

1968

En México se introduce la primera tarjeta de crédito. Se trataba de Bancomático y la lanzó Banamex en afiliación con Interbank, hoy MasterCard.

1969

Otro de los grandes bancos de México, el Banco de Comercio, afiliado al entonces Sistema BankAmericard, hoy Visa, organiza su propio sistema con la tarjeta de crédito Bancomer. Otros bancos estudian la posibilidad de introducir su propia tarjeta; deciden unirse debido a los costos operativos. Banco Serfin, Multibanco Comermex, Banco Internacional, Banco Confía, Banco del Atlántico y Banco Mexicano Somex crean Prosa, conformándola como una empresa encargada de desarrollar e introducir la tarjeta de crédito en estos bancos (marca Carnet). La posterior afiliación de MasterCard y Visa, le permitió a Carnet emitir tarjetas con validez internacional.

1987

Otra entrada en el negocio de tarjetas fue la tarjeta Discover, originalmente parte de la Corporación Sears. Su primera tarjeta se dio a conocer en el Tazón de 1986.

2002

El auge del comercio electrónico demando un medio de pago adecuado y seguro; se visualizó a las tarjetas de crédito como el medio idóneo para dicho comercio.

2003

Con más de 50 años con la misma forma y medidas (8.5 x 5.5 cms.) las marcas empiezan a buscar elementos diferenciadores: con diferentes imágenes, dimensiones e incluso recortes en sus bordes.

2013

Actualmente, las tarjetas de crédito siguen renovándose. Las instituciones financieras mexicanas tienen hasta diciembre de 2013 para migrar todos sus plásticos de banda magnética a chip (mecanismo que resulta más seguro). En ese lapso, también los lectores de tarjetas en puntos de venta, los cajeros automáticos y las cajas registradoras deberán haberse adaptado a esa tecnología.

Además se está trabajando en tarjetas de crédito con tecnología RFID, de forma que sólo habrá que acercarlas a la terminal punto de venta, sin necesidad de introducirlas."[78]

La tarjeta de crédito paso de ser un proyecto y medio para llevar la información de un cliente para el uso de un crédito, a un medio por el cual un usuario realiza casi la totalidad de sus operaciones financieras, esto derivado a que es un medio de menor riesgo en su transportación y de mayor seguridad para el usuario que el uso y transportación de efectivo.

Aunado a que las instituciones financieras y el comercio en general están migrando la gran mayoría de sus operaciones al uso de la misma, generando la necesidad apremiante de estar en los procesos y medios necesarios para salvaguardar nuestra información.

Por consiguiente se debe identificar quienes son las instituciones más importantes que dan soporte y viabilidad a estas operaciones, las cuales actualmente son la empresa VISA y la empresa MASTERCARD.

[78] Pastrana, R. (s.f.). *El origen del plástico*. Diciembre 2018, de Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros Sitio web: https://www.condusef.gob.mx/Revista/index.php/credito/tarjeta/200-el-origen-del-plastico

Para fines didácticos y de entendimiento de este trabajo de investigación analizaremos la a MASTERCARD, esto debido a que tanto MASTERCARD como VISA son empresas espejo especializadas en el mismo ramo:

"1966 Un grupo de bancos crea la Asociación Interbancaria de Tarjetas (ICA).

1969 ICA adquiere el nombre Master Charge y la marca comercial de los círculos entrelazados.

1979 Master Charge se convierte en Mastercard.

1980s Mastercard es la primera tarjeta de pago emitida en la República Popular de China, la primera en introducir un holograma láser en las tarjetas. Se lanza la primera tarjeta Mastercard comercial.

1990s Mastercard es la primera tarjeta de pago emitida en la República Popular de China, la primera en introducir un holograma láser en las tarjetas. Se lanza la primera tarjeta Mastercard comercial.

2001 Mastercard lanza Mastercard Advisors, una organización global de servicios profesionales centrada exclusivamente en la realización de pagos.

2002 Mastercard se integra con Europay International y se convierte en una sociedad limitada privada.

2006 Mastercard pasa a una nueva forma de gobierno corporativo y estructura de propiedad y comienza a cotizar en la Bolsa de Valores de Nueva York con el código de cotización MA.

2008 Mastercard Europe y Europay France integran sus operaciones.

2009-2012Mastercard adquiere Orbiscom, DataCash, la compañía de gestión de programas prepagados de Travelex (Access Prepaid), Trevica y Truaxis."[79]

[79] Mastercard Latinoamérica. (Mayo 25, 2006). *Hemos hecho historia durante casi cincuenta años*. Junio 15,2018, de Mastercard Sitio web: https://latinamerica.mastercard.com/es-region-lac/acerca-de-mastercard/quienes-somos/historia.html

Mastercard es un banco que creció a partir de la mitad del siglo XX y que tuvo su boom con la explotación del crédito, mientras mayor otorgamiento y cobertura de crédito se otorgó a nivel global mayor fue su crecimiento, esto derivado a que fue la institución pionera en brindar cobertura, respaldo y protección a las diversas operaciones realizadas por las demás instituciones.

Mastercard es un banco que respalda las operaciones financieras de bancos o instituciones financieras de menor envergadura durante la realización de transacciones, por citar un ejemplo tú tienes una tarjeta de crédito de un banco X el cual te otorga un crédito a ti, sin embargo tu sales de viaje a otro país y para realizar operaciones en este país tu banco X no tiene la cobertura e infraestructura necesaria para que puedas hacer uso de tu tarjeta, por tanto este se asocia con este MASTERCARD que digamos en términos simple respalda al banco de menor envergadura cubriendo la deuda de tu operación en este otro país y el voltea con tu banco X y le realiza el cobro de la operación que tu realizaste y este a su vez te realiza el cobro de esta operación a ti.

Servicio por el cual MASTERCARD cobra comisiones a los diversos bancos que respalda por cada una de las transacciones que protege; por consiguiente la mayoría de los comercios electrónicos, servicios y o pagos que se realizan mediante el uso de una tarjeta de crédito piden que la tarjeta mediante la cual se va a realizar una transacción tenga el respaldo de cualquiera de estos dos monstruos de empresas, ya que cada uno de ellos tiene el poderío económico y la infraestructura necesaria para dar soporte y respaldo a cada una de las operaciones que se realizan respaldadas por ellos.

Por tanto estas dos empresas son las pioneras en los diversos candados mínimo necesarios para realizar transacciones en línea, y por tanto son la punta de lanza a nivel global para el seguimiento y corrección de los problemas suscitados por los ciberdelincuentes, pero este tema lo retomaremos más delante.

Ahora debemos de retomar el antecedente del tipo panal antecesor al carding online el cual es el fraude; sin embargo ¿Qué es el fraude?

Fraude: “En el ámbito del derecho penal, que es donde tiene mayor cabida este vocablo, se estima que la esencia del delito de fraude, es el engaño de que se vale el. agente, para hacerse en perjuicio de otro de un objeto de ajena procedencia. Al observar que es el patrimonio el principal interés que se protege dentro de la sociedad, advertimos que las relaciones de sus integrantes deben desarrollarse libres de engaños o maquinaciones que induzcan a error; pero de igual forma se reconoce, que la astucia del hombre lo ha llevado a través del tiempo a obtener mucho de lo que se propone, lo que también ha proyectado en el renglón de lo ilícito, cuando ansioso de riqueza refina su mente y empuja la voluntad del semejante a un camino equivocado para causarle un perjuicio patrimonial, con el que se beneficia el creador del engaño o artificio.”[80]

El Código Penal Federal señala:

Artículo 386.- 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.

El delito de fraude se castigará con las penas siguientes:

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.

Este es el tipo penal que antecede al carding online debido a que el medio que dio origen a este delito fue con un fraude electrónico en el cual mediante diversos engaños perpetrados por el infractor obtiene el número de la tarjeta de crédito mediante la cual obtendrá un beneficio económico, situación que se verá posteriormente ha evolucionado.

[80] Enciclopedia Jurídica Online. (s.f.). *Derecho de Internet en el Derecho Mercantil Mexicano*. dicmebre 2018, de Enciclopedia Jurídica Online Sitio web: https://mexico.leyderecho.org/mercantil/derecho-de-internet/ https://mexico.leyderecho.org/fraude/

3.3 Forma de obtención de datos de usuarios de servicios financieros

Existen diversos medios de actuar para que los denominados bineros, quienes son las personas encargadas de obtener la información de bins de tarjetas de créditos de los usuarios de servicios financieros, para lucrar con ellas ya sea de manera directa esto realizando la compra directa ellos mismos o mediante un tercero que será a quien ellos vendan el bin para que este tercero realice la compra en línea; cabe resaltar que uno de los mayores riesgos del carding online es que la persona que obtenga un bin funcional para compras sea el mismo que realiza las compras, esto lo explicaré posteriormente, de momento enlistaré y desarrollaré las formas de obtención de estos bines actualmente utilizadas y que son:

3.3.1 Robo de correspondencia

El robo de correspondencia es un medio utilizado de manera tradicional para la obtención de toda clase de información, y el carding online no es la excepción, esto debido a que mediante correspondencia las diversas instituciones financieras envían la información de los diversos servicios que tiene contratados una persona con la institución.

Este tipo de robo se realiza de diversas formas siendo una forma común cuando:

Una persona que labora dentro del servicio de correspondencia vende esta información al denominado binero.

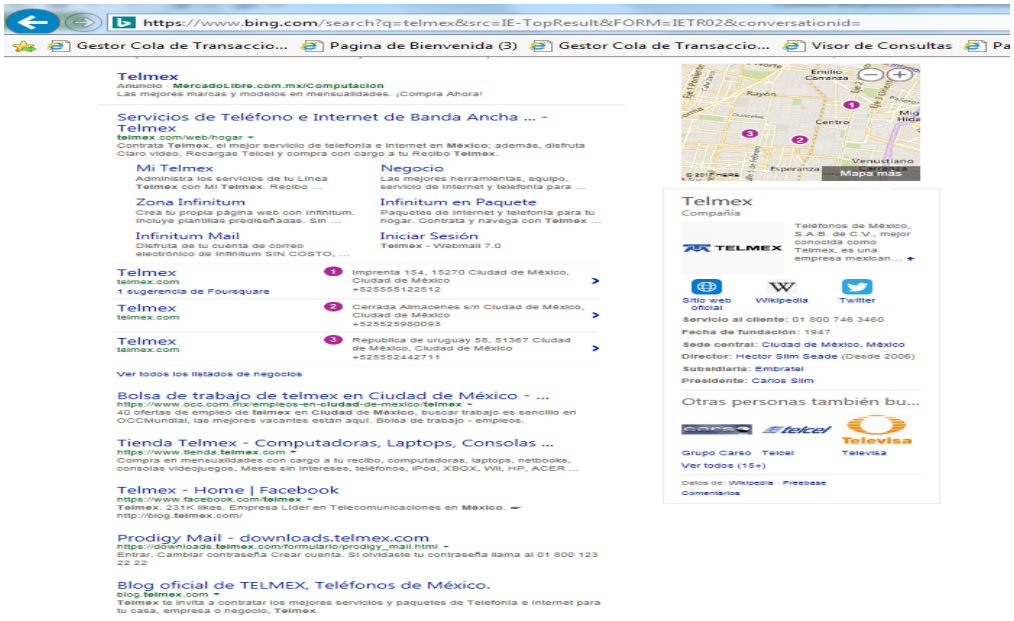
La persona a quien se le robará su correspondencia vive en zonas con áreas comunes donde se entrega la información de correspondencia como condóminos, departamentos, unidades habitacionales, etc., y por tanto el denominado binero ingresa a estas áreas comunes donde se deja la correspondencia a sustraerla.

Por tanto, es recomendable que toda persona usuaria de servicios financieros que recibe información de los mismos vía correspondencia, de un seguimiento puntual a la recepción de esta y en caso de no recibirla comunicarse con la institución para evitar que pueda existir el riesgo de robo, ya que el mayor problema de este tipo de robos es que en la mayoría de las

ocasiones la persona afectada no se percata del robo, sino que tiende a creer que la correspondencia se perdió en el camino o por alguna situación rara la entidad no le envió su estado de cuenta.

3.3.2 Llenado de datos de tarjeta en un portal falso

El llenado de datos de tarjeta en un portal falso, es una forma de obtención de bines, de una manera más sofisticada ya que el binero para poder ejecutarla necesita de manera inequívoca un conocimiento específico en medios informáticos, en este caso deberá saber cómo hacer una página de internet y cómo hacer que la misma tienda a ser una réplica parecida a la página oficial. Esta forma de actuar es compleja y eficaz ya que pongámonos en el lugar de una persona que no tiende a usar en demasía el internet y desea realizar un pago en línea porque una persona X le dijo que era sencillo, esta persona que lo realizara a su vez no sabrá cuál es la página oficial y en el momento de indicar en el navegador el nombre del pago que desea realizar, dicho navegador les disparara diez o veinte opciones con títulos similares, tal como lo podemos notar en la imagen siguiente:



Al disparar todos estos títulos e indicar el nombre de la empresa, la persona podrá cliquear cualquiera de ellos y podrá cometer el error de ingresar a una página equivocada o fantasma y

en esta a su vez proceder a realizar lo que para ella es un pago seguro, así que el dinero servirá para guardar todos los datos de pago mediante la página falsa que había creado y mediante la cual indujo al error a un indeterminado número de personas.

También existe la posibilidad de obtener estos datos mediante la recepción de un correo falso que llegará a nuestra bandeja de entrada en el cual indicará que hemos ganado un premio ya sea en efectivo, un vehículo o inclusive una casa y en el cual solicitara que para acceder a este necesitamos llenar unos formularios con nuestros datos e indicar un número de cuenta en la cual se nos depositará el premio; situación que induce al error en personas que no manejan y/o conocen de manera plena el actuar y finalidad de estas estafas.

En tal virtud es necesario que al detectar páginas y/o mensajes que generan desconfianza evitar dar datos personales de cualquier índole; ya que en el caso de haber dado información es complejo para la persona que la otorgo darse cuenta del error que cometió, por tanto es recomendable no abrir correos de origen desconocido y activar en los equipo de cómputo los diversos bloqueos en la navegación que ofertan para evitar abrir páginas de origen desconocido y en caso de ser viable se recomienda que durante la primera transacción que se haga en línea acercarse con una persona que ya lo haya hecho para que nos ayude en identificar los sitios correctos y evitar estos errores.

3.3.3 Hackeo de bases de datos

El hackeo de bases de datos es una forma de obtener información de los bineros que requiere conocimientos previos en programación de sistemas informáticos, y un dominio de software diverso para ir desbloqueando cada uno de los candados de seguridad que las empresas aplican para proteger la información confidencial otorgada por sus usuarios.

Este método de obtención de datos de usuarios es el más redituable, porque en el supuesto de que el hacker logre pasar todos los candados y medidas de seguridad de la empresa, este no tendrá acceso a la información de una sola persona sino que será de cientos o quizá miles, por tanto, esta es la forma de obtención de información más peligrosa, este tipo de obtención de

información puede inclusive llevar a la empresa afectada a la quiebra, porque cabe señalar que el activo más importante para una empresa son sus clientes, y al ser este el punto afectado, la empresa podría tener afectaciones de las cuales no se podría recuperar.

Este tipo de obtención de información por más complejo que parezca de realizarse, ha tenido lugar como fue en la siguiente noticia que impacto a nivel mundial:

"Sony explica cómo hackearon PlayStation Network

Encubrieron el ataque como una compra en el servicio.

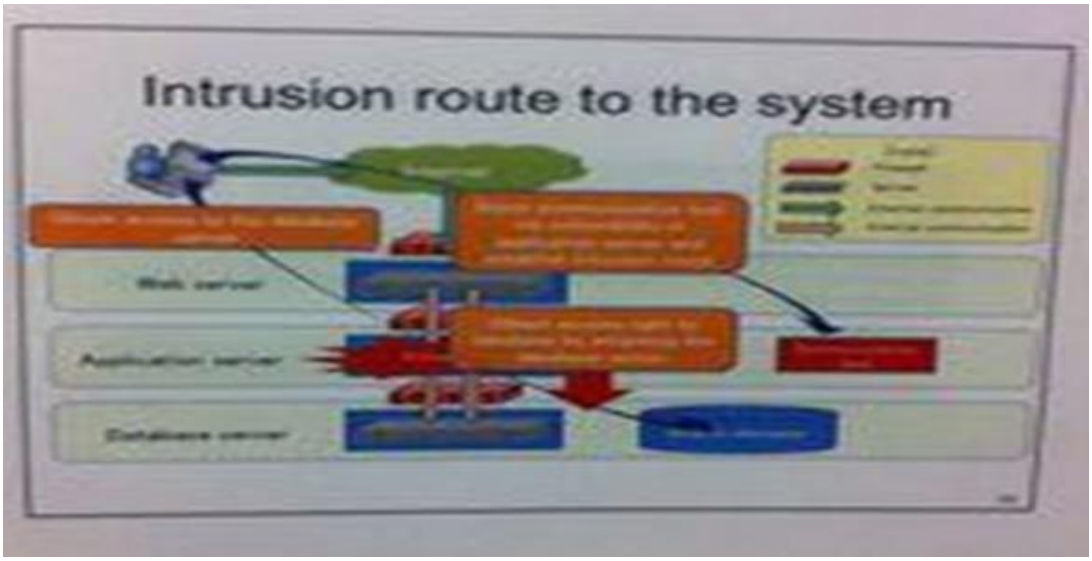
Se conoció nueva información sobre el ataque a PlayStation Network, después de que Sony llevase a cabo una rueda de prensa pidiendo disculpas por lo sucedido y anunciando que en los próximos días volverán los servicios online de la plataforma.

Sony explico cómo se llevó a cabo el ataque contra su plataforma. El ataque a la base de datos de clientes se realizó desde un servidor de aplicaciones conectado con ella, y que está tras un servidor web y dos cortafuegos o firewalls. Según los responsables de la compañía, el modo en que se realizó el hackeo "es un técnica sofisticada".

Los autores del ataque lo encubrieron como una compra en la plataforma online de Sony, por lo que los sistemas de seguridad no detectaron nada raro, y tras pasar del servidor web, lograron explotar una vulnerabilidad del servidor de aplicaciones para instalar un software que más tarde fue usado para acceder al servidor de la base de datos, protegido por un tercer firewall.

La vulnerabilidad del servidor de aplicaciones donde se instaló el software para acceder a la base de datos era desconocida por Sony, que ya se ha apresurado a crear un puesto de jefe de seguridad de la información para supervisar la seguridad de los datos de ahora en adelante, además, de haber rehecho la seguridad de la plataforma PlayStation Network para evitar que esto vuelva a pasar.

La compañía ha mostrado un diagrama esquematizando cómo ha sido el ataque."[81]



Analizando esta noticia se tiene que entender que ninguna persona física o moral por mayor infraestructura que posea medidas de seguridad que el mismo emplee, se encontrara exento de que un hacker informático sustraiga información de sus sistemas.

Por consiguiente, las personas físicas o morales deberán de mantener una adecuación constante en sus sistemas de seguridad, esto para poder hacer frente a cada una de las amenazas latentes que pudieran surgir.

3.3.4 Compra de bases de datos

Para la compra de base de datos existen dos métodos, en el primero es el complemento de las acciones realizadas por una persona especializada en el hackeo de bases de datos, en está transacción de manera recurrente es realizada por bineros carentes del conocimiento técnico teórico para poder realizar ambas operaciones de manera correcta; es decir aquí el binero no

[81] Vandal/Noticias. (Febrero 5,2011*). Sony explica cómo hackearon PlayStation Network. Encubrieron el ataque como una compra en el servicio*. Junio 14,2018, de Vandal Sitio web: https://vandal.elespanol.com/noticia/55869/sony-explica-como-hackearon-playstation-network/

puede ingresar a las bases de datos y obtener la información de manera individual sino que necesita de un tercero y el únicamente se dedicará a comprar las bases de datos ya sea para revenderlas a terceros o para utilizarlas de manera directa realizando compras o pagos de servicios.

Este método es peligroso debido a que estas bases de datos son amplias y en la compra de una de ellas se puede tener datos de cientos e inclusive miles de personas.

En el segundo método existe una persona dentro de una empresa y esta persona tiene acceso a información privilegiada de la base de clientes de la empresa, en este ejemplo la persona que labora en la empresa roba dicha información y la vende al binero o en su defecto la utiliza de manera personal.

En este caso, es riesgoso porque la cantidad de información que se roba no tiene un límite, ni una forma de detección oportuna, debido a que se empiezan a identificar las transacciones ilegales hasta que se realizan, es decir cuando existe un robo por hackeo la empresa en automático puede empezar a trabajar en detener estos fraudes y compras ilegales realizadas, sin embargo cuando la persona que sustrajo la información labora en la empresa, esta no se dará cuenta hasta que empiece a realizar un número constante de transacciones y se encuentre un patrón que conduzca a entender que no es un hecho aislado sino una fuga y/o robo de información de manera interna, por tanto esto se puede convertir en un robo hormiga constante de información que podría únicamente terminar en algunas ocasiones por la detección de la persona por parte de la empresa o por la renuncia de la misma persona; pero entre el tiempo en que la persona que labora empieza a realizar el robo de la información y la detección o el desistimiento de la misma persona en realizar el ilícito pueden ser meses e inclusive años.

Por tanto, la única recomendación que se puede realizar en este sentido es el constante monitoreo de las diversas cuentas que pueda tener una persona en el sistema financiero mexicano.

3.3.5 Obtención de un número de tarjeta partiendo de otro

La obtención de un número de tarjeta partiendo de otro es otra de las maneras de obtención de bines, ya que para ejecutarse se requiere de personas hábiles en la utilización y/o creación de diversos softwares casero que se utilizara para empezar a descifrar los números de la tarjeta de crédito partiendo de otro.

Me refiero a que la persona encargada de obtener este número de tarjeta nuevo parte de otro, primero deberá de obtener una tarjeta de crédito, la cual puede ser inclusive de el mismo o de un familiar, se la puede comprar a alguien más, se la puede encontrar o inclusive la puede robar, por tanto, una de las principales medidas que siempre se recomienda para un usuario de tarjeta de crédito es que no preste su tarjeta a nadie más, y que en caso de ya no utilizar la misma destruirla.

En este sentido esta persona ya obtuvo por el medio que considero factible la tarjeta de crédito y enseguida se dispondrá a sacar la información necesaria para obtener otro número de tarjeta de crédito; para esto se debe conocer lo que significa cada uno de los dígitos plasmados en una tarjeta de crédito, los cuales son:

“Primer número de la tarjeta, el tipo de tarjeta

De la numeración de la tarjeta, el primer número representa el **tipo de tarjeta por el rango de emisor**. Por ejemplo, una tarjeta emitida por una compañía petrolera comenzará por 7 y una tarjeta emitida por una aerolínea comenzará por 1.

Identificación de país y emisor, posiciones 1 a 7 de la tarjeta

Los primeros siete dígitos de todas las tarjetas corresponden con el **número de emisor de la empresa o entidad financiera y el país**. Se incluye el primer número como parte del emisor para el tipo de tarjeta estudiado anteriormente. Por motivos de seguridad, los rangos completos de emisores y países son privados, aunque si se conocen los principales rangos de comienzo de cada una de las tarjetas.

Por ejemplo, las tarjetas VISA comienzan todas por 4, si son del tipo VISA Electron tienen rangos comprendidos entre 4026, 417500, 4508, 4844, 4913, 4917; Mastercard tiene asignados los rangos entre 51 y 55 y las tarjetas Maestro numeraciones de comienzo que sean alguno de estas series 5018, 5020, 5038, 6304, 6759, 6761, 6763.

Estos rangos complementados hasta los 7 primeros dígitos ubican el tipo de tarjeta, el tipo de emisor y la zona geográfica en la que se ha emitido la tarjeta.

Resto de números de la tarjeta

Los demás números corresponden al **código interno de la entidad para asociar la tarjeta al cliente** y responden a sus propios criterios de numeración. El número total de dígitos de una tarjeta es variable, pudiendo oscilar entre 13 y 18, aunque las tarjetas más habituales tienen 16 dígitos.

Las excepciones típicas son American Express que tiene 15 dígitos, Dinners Club que tiene entre 14 y 15 dígitos y a partir de 16 dígitos para el resto, con un máximo de 19.

La mayoría de las tarjetas, **destinan uno de esos dígitos al dígito de control**. Este dígito es un número que cumple el algoritmo de Luhn, que relaciona algebraicamente el resto de números para devolver el valor del dígito de control y se encuentra en una posición determinada. Para las tarjetas, VISA, Maestro y Mastercard, el dígito de control se encuentra en la posición 16.

No obstante, no todas las tarjetas tienen un dígito de control asociado. Por ejemplo, algunos tipos de tarjetas Dinners Club no tienen este elemento de seguridad. Por otro lado, las tarjetas emitidas por China mobipay no responden al algoritmo de Luhn descrito."[82]

En este tenor es de fácil comprensión saber que de manera común la tarjeta de crédito consta de 16 dígitos, de los cuales los primeros 7 indican el tipo de tarjeta, el tipo de emisor y la zona

[82]Banco Bilbao Vizcaya Argentaria, S.A. . (2019). *¿Qué significan los números de las tarjetas de crédito o débito?*. Abril 26, 2018, de BBVA Sitio web:https://www.bbva.com/es/como-afecta-la-subida-del-salario-minimo-a-la-economia/

geográfica en la que se ha emitido la tarjeta, los restantes 11 dígitos son variables y corresponden al número de identificación del cliente que da de manera interna a la institución emisora; por consiguiente los primeros 7 dígitos son los que el binero utilizará de la tarjeta de crédito base para obtener números de otras tarjetas de crédito.

Los siguientes 11 dígitos son designados mediante el algoritmo de Luhn, el cuales es el siguiente:

"El algoritmo de **Luhn** es un método creado para la verificación de números de identificación, como los números de las tarjetas de crédito (Visa, MasterCard) o el **IMEI** de los teléfonos móviles.

Su creador fue **Hans Peter Luhn, un científico de IBM** y su uso ha sido tan extendido que desde que fuera creado hoy controla la creación y validación de la mayoría de los plásticos que se otorgan a los tarjetahabientes de todo el mundo.

Este algoritmo es simple, en el mismo sabes que un número que contenga solamente dígitos [0-9], una tarjeta de crédito es válida si y solo si, obteniendo la reversa de este número, y la suma sus dígitos debe ser un múltiplo de 10, es decir que la suma módulo 10 debe ser igual a cero.

La forma en sumar es la siguiente, una vez hayamos invertido el número, si es posición impar, sumamos el dígito, si es posición impar, multiplicamos ese dígito por dos y sumamos los dígitos de ese número, para hacerlo más práctico, si el doble de ese dígito es mayor o igual a 10, le restamos 9 a ese doble, y finalmente se debe verificar que la suma que se realizó sea un múltiplo de 10.

Así funciona el algoritmo de Luhn

Explicare el algoritmo de validación con un ejemplo.

Tenemos el número 49927398716.

1. Multiplicamos por 2 los dígitos que ocupan las posiciones pares empezando por el final:
   (1×2) = 2, (8×2) = 16, (3×2) = 6, (2×2) = 4, (9×2) = 18
2. Sumamos los dígitos que ocupaban las posiciones impares con los dígitos de los productos obtenidos:
   6 + (2) + 7 + (1+6) + 9 + (6) + 7 + (4) + 9 + (1+8) + 4 = 70
3. Si el resto de dividir el total entre 10 es igual a cero, el número es correcto:
   70 mod 10 = 0

4	9	9	2	7	3	9	8	7	1	6
4	18	9	4	7	6	9	16	7	2	6

"[83]

Este algoritmo es el que designa y permite validar si el número de una tarjeta de crédito es correcto o no, por tanto la persona que se dedica a obtener números de tarjeta de crédito a partir de otro lo utiliza.

Retomando el tema la persona que obtuvo la tarjeta de crédito ya tiene en primera instancia los 7 dígitos constantes de la tarjeta y los 11 dígitos restantes los obtendrán mediante el uso de un software casero que tendrá como llave el algoritmo de Lunh y por tanto dará estos 11 dígitos sin error.

Por tanto dicha persona con la obtención de una tarjeta de crédito, podrá obtener cientos de combinaciones de tarjetas de crédito mediante el uso de un software que realice la validación del algoritmo de Luhn.

3.3.6 Llamada telefónica para obtener datos

La llamada telefónica para obtener datos es el medio más sencillo para obtener información de tarjetas de crédito, esta operación se realiza mediante una llamada telefónica de dos maneras diferentes, en la primera se realiza de cero es decir la persona que contacta con el usuario de

[83] *Así funciona el Algoritmo de Luhn para generar números de tarjetas de crédito*. Abril 6, 2018, de quobit.mx Sitio web:https://www.quobit.mx/asi-funciona-el-algoritmo-de-luhn-para-generar-numeros-de-tarjetas-de-credito.html

servicios financieros indagará toda la información necesaria para obtener sus datos de tarjetas de crédito, esto se realiza de manera común mediante diversos engaños como indicar que se han hecho acreedores a un premio motivo por el cual deberán de indicar un número de cuenta y datos financieros para depositar dicho premio, en este caso el afectado dará los datos necesarios de la tarjeta de crédito.

En el método dos se partirá la llamada ya con información específica del titular de la tarjeta de crédito esto será para obtener la información faltante para realizar las diversas operaciones en línea, en este caso se podría decir que la llamada telefónica es el complemento idóneo cuando ya se obtuvo por otro medio la información , es decir ya se tiene el bin y este es correcto pero le hace falta al binero para realizar la transacción la fecha de vencimiento o el ccv o cv de la misma, y por consiguiente mediante diversos engaños vía telefónica contacta a la persona usuaria de esta tarjeta para que se lo dé, esto puede ser indicándole de igual manera que ganó un premio, que se le ofrece un seguro gratuito o simplemente que se le habla de su banco para renovar su tarjeta o incrementar su línea de crédito y por tanto el titular de la tarjeta de crédito dará dicha información.

Este es uno de los métodos sencillos y de menor riesgo para el binero debido a que no tendrán que realizar un robo de manera directo o ingresar a un sistema de base de datos de una empresa, y/o tener que contactar con alguien que labore dentro de una empresa para conseguir las bases de datos y por tanto en este método es mucho más complejo detectarlo a tiempo y rastrearlo ya que estas llamadas se tienden a realizar de teléfonos móviles y en caso de realizarse mediante el uso de una línea fija para rastrear esta llamada se requiere forzosamente del ordenamiento expreso de un juez.

3.4 Forma de ejecución del carding online

El carding online lo ejecuta dos tipos de personas por un lado puede ser el binero quien como lo he indicado es quien se dedica a obtener bines de tarjetas de crédito o por otro lado una persona que realizará transacciones en línea con los bines de las diversas tarjetas obtenidos; para ejecutarlo en primera instancia se hace una labor de recopilación de una base de tarjetas

de crédito o en algunos casos de débito estas siempre y cuando se haya podido confirmar que cuenten con saldo y normalmente; enseguida se confirman dichos datos con la institución financiera; después de esto se realiza una compra en línea de prueba y por último se confirma la misma recibiendo el producto.

Sin embargo, considero necesario desentrañar este proceso en los siguientes puntos de este trabajo de investigación para que cualquier lector del mismo pueda comprender este ilícito.

3.4.1 Obtención de datos de usuarios de servicios financieros

La obtención de datos de usuarios de servicios financieros es lo complejo de todo este ilícito; me refiero este es el trabajo arduo repetitivo y constante que realiza una o varias personas para cumplir con un objetivo específico, siendo este en gran medida el menos remunerado pero el más difícil de ejecutar; en este punto quien realiza este trabajo deberá de apoyarse y /o ejecutarlo por cualquiera de los puntos mencionados anteriormente como son:

-Robo de correspondencia

-Llenado de datos de tarjeta en un portal falso

- Hackeo de bases de datos

- Compra de bases de datos

- Obtención de un número de tarjeta partiendo de otro

- Llamada telefónica para obtener datos

Cabe resaltar que en este punto el ilícito, es casi imposible de identificar debido a que en el proceso de obtención de datos el usuario de servicios financieros transgredido tiende a no identificar o darse cuenta de que sus datos, números de cuenta y/o información financiera han sido comprometidos.

3.4.2 Confirmación de datos con la institución financiera

La confirmación de datos con la institución financiera es el paso que sigue después de obtener los datos financieros de las diversas tarjetas o cuentas de crédito, para esta parte del proceso del ilícito existen tres formas identificadas para realizarse:

-Acudir de manera personal el ejecutor del ilícito a una sucursal bancaria a la cual pertenece la tarjeta de crédito a utilizar para cometer el ilícito; esto para corroborar datos de la citada tarjeta; esto puede realizarse por dos vertientes en la primera el ejecutor del ilícito se presenta con identificaciones falsas y con el conocimiento previo de los datos del titular de la tarjeta de crédito obtenidos y verificados con anterioridad normalmente mediante una llamada telefónica al titular de dicha tarjeta; y la segunda vertiente se presenta en la sucursal el ejecutor de dicho delito pero en contubernio con una persona que labora dentro de la institución bancaria obtiene el resto de la información necesaria de la tarjeta de crédito a defraudar.

-Mandar a un tercero a recopilar el resto de la información de la tarjeta de crédito a una sucursal bancaria a la cual pertenece dicha tarjeta; en este tipo la persona que ejecuta el carding online oferta dinero a un tercero para que obtenga los datos faltantes de la tarjeta de crédito como lo son que la misma este activa, así como el saldo de la misma para poder realizar compras, se manda dicha persona ya sea con identificaciones falsas o un su defecto en colusión con un ejecutivo de banco que labora de igual manera con el ejecutor del carding online; esto se hace para disminuir riesgos de ser detenido e identificado el ejecutor del carding online, así como para evitar levantar sospechas en las diversas sucursales del banco del que este va a obtener información ya que al ser necesario obtener información de “n” numero de cuentas sería absurdo y sospechoso presentarse todos los días para solicitar información de diversos clientes.

-Solicitud de información mediante una llamada telefónica a la institución financiera emisora de la tarjeta de crédito a defraudar, esta forma de operar es la menos riesgosa y simple de realizar ya que con la información obtenida previamente con el titular de dicha cuenta en la cual el ejecutor del ilícito se hizo pasar con el titular como la institución financiera ahora hará

exactamente lo mismo pero al revés, es decir se hará pasar ante la institución financiera como el titular de la tarjeta de crédito.

3.4.3 Validación de datos mediante una compra de prueba

El siguiente paso en la ejecución del ilícito denominado carding online es realizar una compra prueba en una página de internet para confirmar que el bin de la tarjeta de crédito se encuentra activa y con saldo disponible para realizar compras, así como para medir el nivel de respuesta y reacción por parte del titular de la misma.

Esta acción se realiza mediante compras de bajo perfil, es decir por montos bajos y de artículos de uso común para evitar que la institución financiera pueda bloquear el plástico o el titular de la misma se percate y la cancele.

3.4.4 Búsqueda de portales para realizar pagos o compras

El siguiente paso por parte del ejecutor del ilícito es buscar en la denominada red mundial "internet" diversas páginas de compra y venta y pago de servicios diversos, que le permitan el uso de los bines de tarjeta de crédito que ha conseguido y validado.

Este paso se realiza mediante la fórmula de acierto error, es decir el ejecutor del ilícito empieza a realizar comprar con todos los bines que tiene en diferentes portales probando los niveles de reacción de la institución financiera, del cliente y de la empresa con quien realizó las diversas compras vía su página de internet.

Después de realizar este análisis de acierto error el ejecutor del ilícito podrá saber que bin le sirve y que bin no le sirve ya sea por algún error en la recopilación de los datos, porque el usuario dueño de la tarjeta de crédito ya no cuenta con saldo o porque el usuario dueño de dicho bin ya cancelo la tarjeta de crédito, o solicito su reemplazo dejando inservible dicho bin.

3.4.5 Validación de portales mediante compras varias

Esta validación de portales mediante compras varias es para revisar los niveles de seguridad de la empresa con quien se realizará la compra o el pago de servicios, así como los diversos candados que la misma tendrá para la entrega de los productos diversos comprados.

Se debe de considerar que dependiendo del giro y tamaño de operaciones de las diversas empresas que otorgan sus servicios de compra venta y/o pago de servicios en sus páginas de internet en línea variará ineludiblemente por el prestigio y /o tamaño de la misma, es decir no será el mismo nivel de seguridad y candados para realizar una compra en línea por ejemplo realizarla en la página de palacio de hierro que realizarlo en una página de internet de venta de ropa diversa que va iniciando sus operaciones; esto debido a que es diferente el nivel de infraestructura de seguridad que tiene el cual es determinado por sus ingresos y por ende mientras más grande e importante sea la empresa mayor será su seguridad.

Por tanto cualquier binero que realiza este tipo de compras lo realizara en páginas que no tengan este tipo de candados.

Así uno de los usos comunes para dichos bines es el pago de servicios ya que el mismo es complejo para identificar por las diversas empresas que ofrecen este tipo de servicios en su página en línea, debido a que parte de sus políticas de mercadeo es que al realizar tu pago en línea de los diferentes servicios este será aplicado a tu cuenta de manera inmediata, por consiguiente no existe una etapa de validación como si existe en la compra de un producto ni el tiempo como para poder cuestionarle al titular de la tarjeta de crédito que está siendo defraudado si el autorizo la transacción, situación que en el caso de la compraventa si se puede dar, aunado a ello en este tipo de transacciones se tiene la dificultad que son pagos por montos inferiores y por ende de difícil rastreo; por citar un ejemplo un pago de línea Telmex, el costo de su servicio de telefonía e internet básico se encuentra ofertado por la cantidad de trescientos ochenta y nueve pesos mexicanos mensuales con impuestos incluidos, y si este se paga con un bin con un saldo de crédito de doscientos mil pesos mexicanos, es muy probable que se concrete transacción sin ningún tipo de sospecha por el bajo perfil de la operación.

3.4.6 Oferta de pago de servicios o compra de materiales en redes sociales

Blogs y páginas de internet.

En la oferta de pago de servicios o compra de materiales en redes sociales, blogs y páginas de internet varias se debe de concebir entendiendo la regla básica y eje primordial del comercio, es decir “oferta y demanda”, si el carding online es un delito en apogeo y realización, se debe de manera al creciente número de personas que entienden la forma de hacer dicho ilícito ya que cabe resaltar que para la ejecución del mismo basta con poner el mismo en el buscador de google o buscar tutoriales que en algunos casos se pueden ver inclusive en youtube, así mismo el desenvolvimiento prematuro y acelerado de las redes sociales sin el control de lo que en las mismas se puede ofertar y publicar, por tanto existen demasiadas personas con el conocimiento necesario y por tanto existe una amplia gama de oferta del mismo como se puede observar en la siguiente imagen donde una persona “X” oferta el pago de servicios mediante la red social Facebook.

En este sentido se debe entender que la exposición masiva del uso de la gente hacia el internet causa grandes beneficios pero también traer con ellos un sinfín de problemáticas difíciles de contrarestar, debido a que una persona por ejemplo en la red social Facebook puede crear un perfil falso y ofertar cualquier tipo de artículos ya sean legales o ilegales y el tiempo de detección de este tipo de ilícitos varia derivado a que no se cuenta con todas las herramientas informáticas para identificar esto de manera automática, y en sentido positivo aun identificando el perfil mediante el cual se oferta dichos servicios se podrá realizar la baja de este perfil pero el mismo ejecutor del delito podrá dar de alta otro nuevo para seguir realizando este tipo de ofertas.

Por otro lado, se tiene la parte de la demanda y en este sentido ante esta oferta existe "N" cantidad de personas que al ver que la transacción se realiza de manera correcta y su servicio o producto es entregado y no termina por ser rechazado; el número de personas que buscan estos servicios crece de manera considerable.

3.4.7 Cancelación de cuentas en redes sociales, blogs y páginas de internet

La cancelación de cuentas en redes sociales, blogs y páginas de internet es la forma más rápida en que se intenta combatir este ilícito, debido a que al ser todo de manera virtual tanto la ejecución del ilícito, como la oferta y la demanda; la vía rápida y fácil que se puede encontrar para combatirlo es dar de baja perfiles en redes sociales que ofertan estos servicios, así como páginas y blogs donde se oferta estos servicios.

Sin embargo, en el caso de redes sociales la ejecución del ilícito en México, no es legal por parte de la policía cibernética cerrar estos perfiles de manera directa por tanto primero necesita investigar, confirmar el ilícito, recabar pruebas y después solicitar la baja del perfil, y en este sentido existe la complejidad de que muchos de estos perfiles se desenvuelven en grupos cerrados de compraventa dentro de las redes sociales donde los integrantes si han hecho uso de los servicios del carding no indicarán el suceso y tampoco solicitaran la baja del perfil, a no ser

que este ofertante del carding online transgreda su patrimonio o no realice las operaciones que indicó realizaría.

Por tanto, en este delito en específico se puede caer en un contubernio difícil de enfrentar y quebrantar entre el ofertante y el demandante, ya que mientras el demandante reciba servicios por parte del ofertante en tiempo y forma y con menor costo, es casi imposible que estos señalen como y donde contactar con los ofertantes.

3.5 Impacto financiero en México del carding online

El impacto financiero de los delitos cibernéticos en México es un tema complejo de cuantificar debido a que los números arrojados por las diversas instituciones financieras solamente consideraran los delitos reportados por los usuarios de los servicios financieros dejando de lado todos aquellos delitos que no son reportados o ni siquiera son identificados; a esto debemos enfatizar que varios de los delitos considerados en el conteo de las diversas autoridades pueden estar siendo realizados con un desfase de tiempo debido a que un delito cibernético o informático se podría realizar en una fecha inicial determinada y detectado en una fecha posterior, es decir un persona puede ser defraudada con compras no autorizadas cargadas a su tarjeta de crédito en enero y el delito detectado en marzo y a esto habría que sumar la variante del tiempo que pudiera tardar en determinarse si el fraude es clasificado como procedente o no en la revisión de la Institución Financiera emisora de la tarjeta de crédito en la que se realizó el fraude, es decir retomando el ejemplo la compra se realiza en enero y el usuario de servicios financieros titular de la tarjeta de crédito lo detecta en marzo y en ese momento ingresa su aclaración con la Institución Financiera, está tardara un periodo aproximado de noventa días en aclarar dicho requerimiento del cliente, por tanto entre el momento de la ejecución del fraude, es decir enero y el momento en que se determina en promedio el tiempo es de más de un ciento ochenta días; por tanto esto no permite arrojar cifras reales de estos delitos ya que delitos cometidos en un mes se reportan en otro, o delitos que no son detectados por parte de los usuarios no son contabilizados en dicho impacto, o inclusive los delitos que el usuario de servicios financieros reporta a su Institución Financiera y este usuario desiste durante el

proceso o la Institución indica que la aclaración no es procedente; por tanto estos datos son meramente informativos y sirven de parámetro para visualizar la magnitud del impacto de estos delitos.

En relación a este tema los datos del impacto económico son generales e involucran todas las operaciones reportadas como fraudulentas sin poder distinguir el medio o la forma en que se realizó dicho fraude; acotado este tema los números reportados por delitos cibernéticos son los indicados en la siguiente nota:

"40% de las tarjetas de crédito son víctimas de fraude

En México, 4 de cada 10 tarjetas bancarias son víctimas de fraude. Además es el país con el mayor porcentaje de incidentes (44%), según un artículo de la compañía especializada en asesoría empresarial, KPMG Group.

Dicha cifra supera a la de Estados Unidos (42%), el mercado de pagos bancarios más grande del mundo. Los países con menores índices de fraude son Holanda y Suecia (uno de cada 10).

Esta estadística se atribuye al fácil acceso a ciudades fronterizas en Estados Unidos, donde tarjetas falsificadas y cuentas fraudulentas pueden ser utilizadas, además del refinamiento tecnológico del crimen organizado.

El impacto mayor lo padecen los comerciantes, que cubren costos por fraude en pagos electrónicos hasta 10 veces más que las instituciones bancarias, y 20 veces más que los consumidores. Los comerciantes regularmente cubren el reembolso del monto defraudado, y, en ocasiones, el costo del bien o servicio perdido.

Si se suma los costos de administración relacionados, los comercios llegan a pagar hasta tres veces el monto original defraudado.

El daño reputacional es también un efecto considerable: uno de cada tres consumidores que ha sufrido cargos indebidos en un establecimiento, decide llevar consumos futuros a otro lugar.

KPMG consideró que la mejor respuesta de los comercios ante situaciones complejas de fuga de datos de pago y crimen cibernético consiste en:

• Revisar de punta a punta los procesos para identificar mejoras de seguridad y robustecer los métodos de prevención de fraude

• Ofrecer servicios de detección a los clientes y otorgar el reemplazo inmediato de tarjetas

• Realizar un manejo mediático dinámico y ágil para mantener puntualmente informados a clientes y público en general, sobre la situación y las medidas que se están tomando para corregirla.

En México todavía no se consolida el comercio electrónico como en Estados Unidos, según el estudio "Brújula Digital" del Banco Nacional de México (Banamex) de octubre de 2013, por primera vez, hay más usuarios de la banca con acceso a Internet que personas sin acceso a bancos y a la red, un hito en temas de bancarización y brecha digital

Los clientes de la banca pasan un promedio de 8.2 horas al día conectados de alguna forma a Internet.

El teléfono móvil se ha convertido para este grupo en el principal medio de conexión, pasando de 15% en 2011 a 38% en 2013."[84]

Acorde a este informe reportado por la página de la revista Forbes se puede identificar que una de cada cuatro tarjetas de crédito es víctima de un fraude situación que maximiza el impacto real de dicho delito cibernético y su proceso de ejecución; por tanto es sumamente necesario concientizarnos en cada una de las formas en que utilizamos una tarjeta de crédito y tener una mayor y mejor cultura en lo que a refiere a comercio electrónico.

[84] Forbes Staff. (julio 21,2014). *40% de las tarjetas de crédito son víctimas de fraude*. marzo 5,2018, de Forbes México Sitio web:https://www.forbes.com.mx/40-de-las-tarjetas-de-credito-son-victimas-de-fraude/

En este tercer capítulo se llegó el tema central de esta investigación después de desmenuzar los diversos delitos cibernéticos que afectan a los diversos usuarios de servicios financieros.

Se debe de entender en primera instancia que las Instituciones Financieras en México y el resto del mundo se encuentran en proceso de migración de sus servicios hacia internet, todo esto derivado de los altos costos que conlleva el mantenimiento, servicios, arrendamiento y demás costos asociados en tener una sucursal física abierta; por tanto la ideología que marca la actualidad en el mercado es la de disminución de gasto centralizando la mayor cantidad de operaciones posibles en el uso de internet.

Así con el simple transcurso del tiempo la cantidad de operaciones a realizarse en línea estarán aumentando y el uso y realización de operaciones de manera física en una sucursal disminuirán.

Esto tendrá como consecuencia que la cantidad de delitos cibernéticos realizados incremente, por ejemplo, si hoy existe el riesgo de al acudir a una sucursal y retirar dinero en efectivo surgiendo un asalto durante tu trayecto al salir de la misma; sin embargo, con este cambio tecnológico este delito será sustituido de manera exponencial por el fraude a una cuenta vía internet.

Este delito se ha dispersado de manera simple mediante el uso de las redes sociales donde una persona puede ofertarlo por un indeterminado tiempo, hasta que alguien lo reporta en la misma red social y teniendo como consecuencia única dar de baja su perfil dentro de la red social o en el mejor de los casos una investigación por parte de autoridad competente, la cual difícilmente rendirá frutos sin tener un querellante, es decir ellos sabrán que se oferta un delito pero no tienen o conocen a la persona afectada del mismo.

Por tanto, como usuarios de dichos servicios financieros debemos de tener una cultura amplia en este tipo de delitos y adentrarnos en los medios de ejecución, para poder prevenirlos, y sobre todo seguir todo tipo de indicaciones que se ofertan por parte de las instituciones financieras para atacar estos temas.

Capítulo cuatro: Medios de defensa de los usuarios de servicios financieros contra delitos cibernéticos.

4.1 CONDUSEF

"A partir del 19 de Abril de 1999 entra en funciones la Comisión Nacional para la Protección y Defensa de los Usuarios del Servicio Financiero (CONDUSEF), tiene las mismas facultades y sirve para atender las quejas de los usuarios del Sistema Financiero. Esto es, que la CONDUSEF fue creada con el firme propósito de ayudar a resolver cualquier conflicto e irregularidad que se presente entre los usuarios de los servicios financieros, con todos y cada una de las organizaciones que conforman el Sistema Financiero Mexicano, incluyendo además el propio Sistema Bursátil Mexicano.

Creada por decreto presidencial y publicada en el D.O.F. el 18 de enero de 1999. Se constituye como un Organismo Público Descentralizado, cuya finalidad es: la promoción, asesoría, protección y defensa de los derechos e intereses de los usuarios que utilizan o contratan un producto o servicio financiero ofrecido por las Instituciones que conforman el Sistema Financiero y que además operen dentro del territorio nacional, así como también la creación y fomento entre los usuarios, de una cultura adecuada respecto de las operaciones y servicios financieros" [85]

"¿Qué hacemos?

Orientación, atención y quejas

En este apartado te orientamos para resolver las dudas, reclamaciones y quejas más comunes que atiende la CONDUSEF.

Información de Productos y Servicios Financieros

[85] Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros. (2018). *¿Qué hacemos?*. Febrero 10, 2018, de Gobierno de México Sitio web: https://www.gob.mx/condusef/que-hacemos

Misión:

Promover y difundir la educación y la transparencia financiera para que los usuarios tomen decisiones informadas sobre los beneficios, costos y riesgos de los productos y servicios ofertados en el sistema financiero mexicano; así como proteger sus intereses mediante la supervisión y regulación a las instituciones financieras y proporcionarles servicios que los asesoren y apoyen en la defensa de sus derechos.

Visión:

Ser una institución pública especializada en materia financiera, que promueve entre la sociedad conocimientos y habilidades que le permiten tomar decisiones adecuadas para el ahorro constante y el pago responsable; y un organismo efectivo para la protección y defensa de los intereses y derechos de los usuarios ante las instituciones financieras, contribuyendo, de esta manera, al sano desarrollo del sistema financiero mexicano.

Tener arraigada una cultura institucional basada en la transparencia, el combate a la corrupción y la igualdad entre mujeres y hombres."[86]

CONDUCEF es la Comisión Nacional para la Protección de los Usuarios de Servicios Financieros, y tiene como finalidad el atender, y dar seguimiento a toda queja y anomalía que surja en una operación financiera realizada entre un usuario de servicios financieros y una entidad financiera; la finalidad de la misma es servir como mediador entre las partes y lograr un acuerdo.

Para poder aplicar dichas medidas la CONDUCEF tiene las facultades necesarias para que su resolución a una queja específica, sea de obligatorio cumplimiento hacia las instituciones financieras, ya que esta tiene la facultad de interponer multas a las instituciones financieras en caso de incumplimiento a una resolución de su parte.

[86] Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros. (2018). *¿Qué hacemos?*. Febrero 10, 2018, de Gobierno de México Sitio web: https://www.gob.mx/condusef/que-hacemos

4.1.1 Jurisdicción

La jurisdicción de la CONDUSEF está delimitada dentro de los siguientes artículos de la Ley de Protección y Defensa al Usuario de Servicios Financieros:

Artículo 3°.- Esta Ley es de orden público, interés social y de observancia en toda la República, de conformidad con los términos y condiciones que la misma establece. Los derechos que otorga la presente Ley son irrenunciables.

Artículo 4°.- La protección y defensa de los derechos e intereses de los Usuarios, estará a cargo de un organismo público descentralizado con personalidad jurídica y patrimonio propios, denominado Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, con domicilio en el Distrito Federal.

La protección y defensa que esta Ley encomienda a la Comisión Nacional, tiene como objetivo prioritario procurar la equidad en las relaciones entre los Usuarios y las Instituciones Financieras, otorgando a los primeros elementos para fortalecer la seguridad jurídica en las operaciones que realicen y en las relaciones que establezcan con las segundas.

Por consiguiente la competencia de la CONDUSEF es aplicable a todo el territorio de la República Mexicana para intervenir en las relaciones entre los usuarios de servicios financieros y las entidades otorgantes de los mismos, todo esto derivado de las facultades otorgadas por el Honorable Congreso de la Unión.

4.1.2 Conciliación

La función principal de la CONDUSEF durante la intervención de la misma en una queja específica es para servir de balanza entre las dos partes, es decir dar seguridad jurídica a ambas partes de que durante su actuar en la celebración de la operación financiera lo hicieron cumpliendo de manera cabal con lo pactado, por ejemplo validar que no existen vicios ocultos.

Situación que sirve para entender de manera objetiva el actuar de las dos partes y por tanto brindarle las herramientas e información necesaria a la CONDUCEF validando estos hechos y en este tenor la misma intervenir buscando la conciliación entre las partes.

Esta conciliación siempre se buscará lograr mediando los puntos expuestos entre cada una de las partes y de manera objetiva esclarecer los hechos para dar su resolución a las partes, indicando los motivos y/o violaciones que encuentre en cada una de las mismas, así como las acciones y/o sanciones a realizar para poder enmendar el daño ocasionado por cada una de ellas.

Todo esto mediante la conciliación de las partes, logrando la CONDUSEF que este tipo de asuntos se ventilen únicamente en sus instancias sin tener que recurrir a otras.

4.1.3 Consulta

El proceso de conciliación que realiza la CONDUSEF es el resultado último de llevar a cabo este tipo de revisiones, sin pero para llegar a él se necesita obligatoriamente pasar por varios pasos previos y el primero de estos es la consulta:

"En CONDUSEF, una Consulta se refiere a recibir tus dudas acerca de:

1. Cualquier producto y/o servicio financiero disponible en el país:

- Características del producto.
- Forma de operación
- Derechos y obligaciones asumidos por las partes.

2. Cuál es la forma de operar en CONDUSEF:

- Horarios de atención.
- Alcance de la Comisión en los casos que presentan los usuarios, dependiendo de la naturaleza de sus asuntos."[87]

[87] Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros. (s.f.). *Formatos para presentar una Reclamación*. Diciembre 2018, de CONDUCEF Sitio web: https://phpapps.condusef.gob.mx/condusefenlinea/TATJ.php

El tipo de consultas indicadas son las que se encuentran permitidas para dar seguimiento y atención por parte de CONDUSEF. Sin embargo existen otro tipo de consultas y/o reclamaciones que no son permitidas como las siguientes:

Soporte Jurídico

- Por tratarse de una Reclamación o Consulta en contra de una Institución no Financiera.
- Por asuntos en los que el usuario reclama por un monto mayor a 3 millones de Unidades de Inversión y sólo para asuntos relacionados con el Sector Seguros, por un monto mayor a 6 millones de Unidades de Inversión.
- Cuando la Reclamación o Consulta, no se refiera a la contratación de un producto o servicio financiero.
- Cuando las inconformidades derivadas de las variaciones en las tasas de interés pactadas entre el usuario y la Institución Financiera, sean consecuencia directa de condiciones generales observadas en los mercados.
- Cuando tu asunto tiene más de 2 años de antigüedad, a partir de la fecha de ocurridos los hechos.
- Cuando solicitas una reestructura de tu deuda."[88]

Por tanto, se debe de tener conocimiento de aquello que podrá ser posible revisar por parte de la CONDUSEF y aquello que no podrá ser revisado por la misma para proseguir con el proceso.

4.1.4. Desahogo de informe y audiencia de conciliación

El desahogo del informe es el proceso mediante el cual las partes tienen la posibilidad de dar la información concerniente al asunto específico, es decir la consulta o reclamación realizada por parte de un usuario de servicios financieros y la respuesta de la Institución Financiera.

[88] Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros. (s.f.). *Formatos para presentar una Reclamación*. Diciembre 2018, de CONDUCEF Sitio web: https://phpapps.condusef.gob.mx/condusefenlinea/TATJ.php

Después de desahogar este informe las partes tendrán una audiencia de conciliación en la cual la CONDUSEF actuará como mediador buscando una resolución entre las partes, y esta parte del proceso está definida en los siguientes artículos de la Ley de Protección y Defensa de los Usuarios de Servicios Financieros:

Artículo 68 I Bis La Comisión Nacional citará a las partes a una audiencia de conciliación que se realizará dentro de los veinte días hábiles siguientes contados a partir de la fecha en que se reciba la reclamación. La conciliación podrá celebrarse vía telefónica o por otro medio idóneo, en cuyo caso la Comisión Nacional o las partes podrán solicitar que se confirmen por escrito los compromisos adquiridos.

La conciliación podrá celebrarse vía telefónica o por otro medio idóneo, en cuyo caso la Comisión Nacional o las partes podrán solicitar que se confirmen por escrito los compromisos adquiridos.

II. La Institución Financiera deberá, por conducto de un representante, rendir un informe por escrito que se presentará con anterioridad o hasta el momento de la celebración de la audiencia de conciliación a que se refiere la fracción anterior;

III. En el informe señalado en la fracción anterior, la Institución Financiera, deberá responder de manera razonada a todos y cada uno de los hechos a que se refiere la reclamación, en caso contrario, dicho informe se tendrá por no presentado para todos los efectos legales a que haya lugar; La institución financiera deberá acompañar al informe, la documentación, información y todos los elementos que considere pertinentes para sustentarlo, no obstante, la Comisión Nacional podrá en todo momento, requerir a la institución financiera la entrega de cualquier información, documentación o medios electromagnéticos que requiera con motivo de la reclamación y del informe;

IV. La Comisión Nacional podrá suspender justificadamente y por una sola ocasión, la audiencia de conciliación. En este caso, la Comisión Nacional señalará día y hora para su reanudación, la cual deberá llevarse a cabo dentro de los diez días hábiles siguientes.

La falta de presentación del informe no podrá ser causa para suspender la audiencia referida.

V. La falta de presentación del informe dará lugar a que la Comisión Nacional valore la procedencia de las pretensiones del Usuario con base en los elementos con que cuente o se allegue conforme a la fracción VI, y para los efectos de la emisión del dictamen, en su caso, a que se refiere el artículo 68 Bis

VI. La Comisión Nacional cuando así lo considere o a petición del Usuario, en la audiencia de conciliación correspondiente o dentro de los diez días hábiles anteriores a la celebración de la misma, podrá requerir información adicional a la Institución Financiera, y en su caso, diferirá la audiencia requiriendo a la Institución Financiera para que en la nueva fecha presente el informe adicional; Asimismo, podrá acordar la práctica de diligencias que permitan acreditar los hechos constitutivos de la reclamación.

VII. En la audiencia respectiva se exhortará a las partes a conciliar sus intereses, para tal efecto, el conciliador deberá formular propuestas de solución y procurar que la audiencia se desarrolle en forma ordenada y congruente. Si las partes no llegan a un arreglo, el conciliador deberá consultar el Registro de Ofertas Públicas del Sistema Arbitral en Materia Financiera, previsto en esta misma Ley, a efecto de informar a las mismas que la controversia se podrá resolver mediante el arbitraje de esa Comisión Nacional, para lo cual las invitará a que, de común acuerdo y voluntariamente, designen como árbitro para resolver sus intereses a la propia Comisión Nacional, quedando a elección de las mismas, que sea en amigable composición o de estricto derecho.

Para el caso de la celebración del convenio arbitral correspondiente, a elección del Usuario la audiencia respectiva podrá diferirse para el solo efecto de que el Usuario desee asesorarse de un representante legal. El convenio arbitral correspondiente se hará constar en el acta que al efecto firmen las partes ante la CONDUSEF.

En caso que las partes no se sometan al arbitraje de la Comisión Nacional se dejarán a salvo sus derechos para que los hagan valer ante los tribunales competentes o en la vía que proceda.

Estos dos rubros del proceso de conciliación brindan a las partes la posibilidad de presentar las pruebas necesarias para poder corroborar la verdad que cada uno considera correcta, y dará certeza de igualdad durante esta parte del proceso.

Así mismo, aunado a la presentación de informes por las partes se tendrá la posibilidad de tener un careo por parte de los involucrados mediante una audiencia en la cual se buscara que la intervención por parte de la CONDUSEF sirva de guía para encontrar una solución a la controversia suscitada.

4.1.5 Convenio

El siguiente punto del proceso de intervención de la CONDUSEF es en el supuesto de todo haber transcurrido de manera positiva durante la conciliación, es decir que las partes llegaran a un acuerdo de sus voluntades para poder poner punto final al origen de la misma consulta o reclamación final; se procederá a la formalización de un convenio, esta parte del proceso se encuentra fundamentada en el la Ley de Protección y Defensa al Usuario de Servicios Financieros en los siguientes artículos:

Artículo 68 VIII. En caso de que las partes lleguen a un acuerdo para la resolución de la reclamación, el mismo se hará constar en el acta circunstanciada que al efecto se levante. En todo momento, la Comisión Nacional deberá explicar al Usuario los efectos y alcances de dicho acuerdo; si después de escuchar explicación el Usuario decide aceptar el acuerdo, éste se firmará por ambas partes y por la Comisión Nacional, fijándose un término para acreditar su cumplimiento. El convenio firmado por las partes tiene fuerza de cosa juzgada y trae aparejada ejecución;

IX. La carga de la prueba respecto del cumplimiento del convenio corresponde a la Institución Financiera y, en caso de omisión, se hará acreedora de la sanción que proceda conforme a la presente Ley, y

En este punto con la elaboración del convenio se dará por terminada la intervención de la CONDUSEF dentro de esta consulta o reclamación realizada por parte del usuario de servicios

financieros. Así mismo en este mismo sentido en el momento de la firma del convenio por las partes tendrá la eficacia de cosa juzgada y traerá aparejada ejecución.

Motivo por el cual en el momento de la firma del convenio se da por terminado el asunto.

4.1.6 Registro de pasivo contingente y reserva técnica

La CONDUCEF después de la firma de la celebración del convenio solicitara a la Institución Financiera el registro de pasivo contingente y reserva técnica, es decir que reserve el importe del gasto en el que incurrirá para subsanar la reclamación del importe solicitado por parte del usuario de servicios financieros, este proceso se encuentra definido en la Ley de Protección y Defensa de los Usuarios de Servicios Financieros en los siguientes artículos:

Articulo 68 X. Concluidas las audiencias de conciliación y en caso de que las partes no lleguen a un acuerdo se levantará el acta respectiva. En el caso de que la Institución Financiera no firme el acta, ello no afectará su validez, debiéndose hacer constar la negativa. Adicionalmente, la Comisión Nacional ordenará a la Institución Financiera correspondiente que registre el pasivo contingente totalmente reservado que derive de la reclamación, y dará aviso de ello a las Comisiones Nacionales a las que corresponda su supervisión. En el caso de instituciones y sociedades mutualistas de seguros, la orden mencionada en el segundo párrafo de esta fracción se referirá a la constitución e inversión conforme a la Ley en materia de seguros, de una reserva técnica específica para obligaciones pendientes de cumplir, cuyo monto no deberá exceder la suma asegurada. Dicha reserva se registrará en una partida contable determinada. En los supuestos previstos en los dos párrafos anteriores, el registro contable podrá ser cancelado por la Institución Financiera bajo su estricta responsabilidad, si transcurridos ciento ochenta días naturales después de su anotación, el reclamante no ha hecho valer sus derechos ante la autoridad judicial competente o no ha dado inicio el procedimiento arbitral conforme a esta Ley. El registro del pasivo contingente o la constitución de la reserva técnica, según corresponda, será obligatoria para el caso de que la Comisión Nacional emita el dictamen a que hace referencia el artículo 68 Bis de la presente Ley. Si de las constancias que obren en el expediente respectivo se desprende, a juicio de la Comisión Nacional, la improcedencia de las

pretensiones del Usuario, ésta se abstendrá de ordenar el registro del pasivo contingente o la constitución de la reserva técnica, según corresponda.

XI. Los acuerdos de trámite que emita la Comisión Nacional no admitirán recurso alguno.

La creación de pasivo contingente y reserva técnica refiere directamente a una prevención que debe de realizar la Institución Financiera para amortizar la perdida que tendrá que afrontar por el convenio ante la CONDUSEF. Así la Institución Financiera deberá de reconocer un pasivo, es decir una deuda hacia dicho cliente por tanto deberá de reconocer un pasivo contingente para no afectar sus resultados financieros e identificar hacia sus inversionistas y socios de manera clara y oportuna de donde se originó esa deuda.

4.1.7 El arbitraje

De manera común la CONDUSEF buscará que se firmen entre las partes convenios con efectos de sentencia ejecutoriada y con una fecha cierta de cumplimiento y con condiciones específicas, sin embargo existirán asuntos donde a petición o determinación de las partes, se llevé a cabo mediante un arbitraje, es decir, al no llegar el usuario y la institución financiera a un convenio de manera conjunta, la CONDUSEF fungirá como árbitro determinando de manera individual el resultado de dicha controversias, todo esto basado en los principios de legalidad, objetividad, buena fe, estableciendo etapas, métodos y plazos, esto se encuentra fundamentado en la Ley de Protección y Defensa al Usuario de Servicios Financieros en los siguientes artículos:

Artículo 73.- En el convenio que fundamente el juicio arbitral en amigable composición, las partes facultarán a la Comisión Nacional para resolver en conciencia, a verdad sabida y buena fe guardada, la controversia planteada, y fijarán de común acuerdo y de manera específica las cuestiones que deberán ser objeto del arbitraje, estableciendo las etapas, formalidades, términos y plazos a que deberá sujetarse el arbitraje.

Para todo lo no previsto en el procedimiento arbitral se aplicará supletoriamente el Código de Comercio.

Artículo 74.- En el convenio que fundamente el juicio arbitral de estricto derecho, las partes facultarán a la Comisión Nacional, a resolver la controversia planteada con estricto apego a las disposiciones legales aplicables, y determinarán las etapas, formalidades, términos y plazos a que se sujetará el arbitraje, con arreglo a lo dispuesto en el artículo 75 de esta Ley.

Artículo 75.- El procedimiento arbitral de estricto derecho se sujetará como mínimo a los plazos y bases siguientes:

I. La demanda deberá presentarse dentro del plazo que voluntariamente hayan acordado las partes, el cual no podrá exceder de nueve días hábiles; a falta de acuerdo entre ellas, dentro de los seis días hábiles siguientes a la celebración del convenio, debiendo el actor acompañar al escrito la documentación en que se funde la acción y las pruebas que puedan servir a su favor en el juicio o en su caso ofrecerlas;

II. La contestación a la demanda deberá presentarse dentro del plazo que voluntariamente hayan acordado las partes, el cual no podrá exceder de nueve días hábiles; a falta de acuerdo entre ellas, dentro de los seis días hábiles siguientes a la notificación de la misma, debiendo el demandado acompañar a dicho escrito la documentación en que se funden las excepciones y defensas correspondientes, así como las pruebas que puedan servir a su favor en el juicio o en su caso ofrecerlas;

III. Salvo convenio expreso de las partes, contestada la demanda o transcurrido el plazo para hacerlo, se dictará auto abriendo el juicio a un período de prueba de quince días hábiles, de los cuales los cinco primeros serán para ofrecer aquellas pruebas que tiendan a desvirtuar las ofrecidas por el demandado y los diez restantes para el desahogo de todas las pruebas. Cuando a juicio del árbitro y atendiendo a la naturaleza de las pruebas resulte insuficiente el mencionado plazo, éste podrá ser ampliado por una sola vez. Concluido el plazo o la prórroga otorgada por el árbitro, sólo les serán admitidas las pruebas supervenientes, conforme a lo previsto en el Código de Comercio; Se tendrán además como pruebas todas las constancias que integren el expediente, aunque no hayan sido ofrecidas por las partes;

IV. Los exhortos y oficios se entregarán a la parte que haya ofrecido la prueba correspondiente, para que los haga llegar a su destino, para lo cual tendrá la carga de gestionar su diligenciación con la debida prontitud. En este caso cuando a juicio del árbitro no se desahoguen las pruebas por causas imputables al oferente, se le tendrá por desistido del derecho que se pretende ejercer;

V. Ocho días comunes a las partes para formular alegatos;

VI. Una vez concluidos los términos fijados, sin necesidad de que se acuse rebeldía, el procedimiento seguirá su curso y se tendrá por perdido el derecho que debió ejercitarse, salvo en caso de que no se presente la demanda, supuesto en el que se dejarán a salvo los derechos del reclamante;

VII. Los términos serán improrrogables, se computarán en días hábiles y, en todo caso, empezarán a contarse a partir del día siguiente a aquél en que surtan efectos las notificaciones respectivas;

VIII. Se aplicará supletoriamente el Código de Comercio, a excepción del artículo 1235 y a falta de disposición en dicho Código, se aplicarán las disposiciones del Código de Procedimientos Civiles para el Distrito Federal, a excepción del artículo 617, y IX. En caso de que no exista promoción de las partes por un lapso de más de sesenta días, contado a partir de la notificación de la última actuación, operará la caducidad de la instancia.

4.1.8 Tipos de arbitraje

La CONDUSEF es un órgano que buscar la conciliación entre el usuario de servicios financieros y la entidad miembro del sistema financiero mexicano, y en su caso sirviendo como árbitro entre las partes acorde al siguiente proceso

4.1.9 Requisitos para el juicio arbitral de estricto derecho

Los requisitos para el juicio arbitral de estricto derecho los contiene la Ley de Protección y Defensa de los Usuarios de Servicios Financieros en los siguientes artículos:

Artículo 73.- En el convenio que fundamente el juicio arbitral en amigable composición, las partes facultarán a la Comisión Nacional para resolver en conciencia, a verdad sabida y buena fe guardada, la controversia planteada, y fijarán de común acuerdo y de manera específica las cuestiones que deberán ser objeto del arbitraje, estableciendo las etapas, formalidades, términos y plazos a que deberá sujetarse el arbitraje.

Para todo lo no previsto en el procedimiento arbitral se aplicará supletoriamente el Código de Comercio.

Artículo 74.- En el convenio que fundamente el juicio arbitral de estricto derecho, las partes facultarán a la Comisión Nacional, a resolver la controversia planteada con estricto apego a las disposiciones legales aplicables, y determinarán las etapas, formalidades, términos y plazos a que se sujetará el arbitraje, con arreglo a lo dispuesto en el artículo 75 de esta Ley.

Artículo 75.- El procedimiento arbitral de estricto derecho se sujetará como mínimo a los plazos y bases siguientes:

I. La demanda deberá presentarse dentro del plazo que voluntariamente hayan acordado las partes, el cual no podrá exceder de nueve días hábiles; a falta de acuerdo entre ellas, dentro de los seis días hábiles siguientes a la celebración del convenio, debiendo el actor acompañar al escrito la documentación en que se funde la acción y las pruebas que puedan servir a su favor en el juicio o en su caso ofrecerlas;

II. La contestación a la demanda deberá presentarse dentro del plazo que voluntariamente hayan acordado las partes, el cual no podrá exceder de nueve días hábiles; a falta de acuerdo entre ellas, dentro de los seis días hábiles siguientes a la notificación de la misma, debiendo el demandado acompañar a dicho escrito la documentación en que se funden las excepciones y

defensas correspondientes, así como las pruebas que puedan servir a su favor en el juicio o en su caso ofrecerlas;

III. Salvo convenio expreso de las partes, contestada la demanda o transcurrido el plazo para hacerlo, se dictará auto abriendo el juicio a un período de prueba de quince días hábiles, de los cuales los cinco primeros serán para ofrecer aquellas pruebas que tiendan a desvirtuar las ofrecidas por el demandado y los diez restantes para el desahogo de todas las pruebas. Cuando a juicio del árbitro y atendiendo a la naturaleza de las pruebas resulte insuficiente el mencionado plazo, éste podrá ser ampliado por una sola vez. Concluido el plazo o la prórroga otorgada por el árbitro, sólo les serán admitidas las pruebas supervenientes, conforme a lo previsto en el Código de Comercio; Se tendrán además como pruebas todas las constancias que integren el expediente, aunque no hayan sido ofrecidas por las partes;

IV. Los exhortos y oficios se entregarán a la parte que haya ofrecido la prueba correspondiente, para que los haga llegar a su destino, para lo cual tendrá la carga de gestionar su diligenciación con la debida prontitud. En este caso cuando a juicio del árbitro no se desahoguen las pruebas por causas imputables al oferente, se le tendrá por desistido del derecho que se pretende ejercer;

V. Ocho días comunes a las partes para formular alegatos; VI. Una vez concluidos los términos fijados, sin necesidad de que se acuse rebeldía, el procedimiento seguirá su curso y se tendrá por perdido el derecho que debió ejercitarse, salvo en caso de que no se presente la demanda, supuesto en el que se dejarán a salvo los derechos del reclamante; VII. Los términos serán improrrogables, se computarán en días hábiles y, en todo caso, empezarán a contarse a partir del día siguiente a aquél en que surtan efectos las notificaciones respectivas;

VIII. Se aplicará supletoriamente el Código de Comercio, a excepción del artículo 1235 y a falta de disposición en dicho Código, se aplicarán las disposiciones del Código de Procedimientos Civiles para el Distrito Federal, a excepción del artículo 617, y IX. En caso de que no exista promoción de las partes por un lapso de más de sesenta días, contado a partir de la notificación de la última actuación, operará la caducidad de la instancia.

Como todo juicio iniciado por cualquier de las partes que participan en él, es de importancia que se cumplan con todas las fases del procedimiento apegándose a la norma aplicable]; ya que en el caso contrario se podrá quedar en un estado de indefensión alguna de las partes y podría generar nulidad del laudo.

Este juicio arbitral de estricto derecho en el que interviene la CONDUSEF, es una de las medidas que otorga como intermediario y que debe ser aceptada por el usuario de servicios financieros y la Institución Financiera.

4.1.10 Intervención de la CONDUSEF en el cumplimiento de laudos

La CONDUSEF, tiene la obligación de dar seguimiento al cumplimiento del convenio o laudo que se alcanzó entre las partes.

Artículo 80.- Corresponde a la Comisión Nacional adoptar todas aquellas medidas necesarias para el cumplimiento de los laudos dictados por la misma, para lo cual mandará, en su caso, que se pague a la persona en cuyo favor se hubiere emitido el laudo, o se le restituya el servicio financiero que demande.

Artículo 81.- En caso de que el laudo emitido condene a la Institución Financiera y una vez que quede firme, ésta tendrá un plazo de quince días hábiles contado a partir de la notificación para su cumplimiento o ejecución.

Si la Institución Financiera no cumple en el tiempo señalado, la Comisión Nacional enviará el expediente al juez competente para su ejecución.

Las autoridades administrativas y los tribunales estarán obligados a auxiliar a la Comisión Nacional, en la esfera de su respectiva competencia. Cuando la Comisión Nacional, solicite el auxilio de la fuerza pública, las autoridades competentes estarán obligadas, bajo su más estricta responsabilidad, a prestar el auxilio necesario con la amplitud y por todo el tiempo que se requiera.

Artículo 82.- La Comisión Nacional, para el desempeño de las facultades establecidas en este Capítulo, podrá emplear las siguientes medidas de apremio:

I. Multas, en los términos señalados en esta Ley, y

II. El auxilio de la fuerza pública.

Artículo 83.- Tratándose de Instituciones y Sociedades Mutualistas de Seguros, así como de Instituciones de Fianzas, en caso de no ejecución del laudo, se ordenará el remate de valores invertidos conforme a las Leyes respectivas.

Artículo 84.- Para verificar el cumplimiento de los laudos, la Comisión Nacional requerirá al director general o al funcionario que realice las actividades de éste, para que compruebe dentro de las setenta y dos horas siguientes, haber pagado o restituido el servicio financiero demandado, en los términos del artículo 81, las prestaciones a que hubiere sido condenada la Institución Financiera; en caso de omitir tal comprobación, la Comisión Nacional impondrá a la propia Institución Financiera una multa que podrá ser hasta por el importe de lo condenado o bien la establecida en el artículo 94, fracción VII y requerirá nuevamente a dicho funcionario para que compruebe el cumplimiento puntual dentro de los quince días hábiles siguientes. Si no lo hiciere, se procederá en términos del artículo 81 y, en su caso, resultarán aplicables las disposiciones relativas a desacato de una orden judicial.

Sin perjuicio de lo anterior, la parte afectada podrá solicitar a la Comisión Nacional el envío del expediente al juez competente para su ejecución, la cual realizará conforme a lo previsto en su propia ley.

En este sentido se puede concluir que la las facultades de CONDUSEF con respecto a su intervención como ente conciliador entre el usuario de servicios financieros y la Institución Financiera, van más allá de una simple apalabra miento y recomendación entre las partes sino que esta tiene la encomienda de supervisar en su caso la ejecución del laudo, basándose para ello en sus capacidades como institución para vigilar dicho cumplimiento o en su defecto basándose en la intervención de terceros para dar cabal seguimiento este laudo; por tanto se

debe de entender que la CONDUSEF tiene un peso específico dentro de este tipo de conciliaciones, o arbitrajes.

4.1.11 Defensoría Legal

La defensoría legal es una opción que oferta CONDUSEF en el supuesto de que el usuario de servicios financieros opte por no realizar ninguna de las opciones de conciliación que oferta la misma y por tanto decida valorar otras opciones.

Artículo 85.- La Comisión Nacional podrá, atendiendo a las bases y criterios que apruebe la Junta, brindar defensoría legal gratuita a los Usuarios.

La Comisión Nacional se abstendrá de prestar estos servicios en aquellos casos en que las partes se sujeten a un procedimiento arbitral en que la Comisión Nacional actúe como árbitro.

Artículo 86.- Para los efectos del artículo anterior, la Comisión Nacional contará con un cuerpo de Defensores que prestarán los servicios de orientación jurídica y defensoría legal, únicamente a solicitud del Usuario.

Artículo 87.- Los Usuarios que deseen obtener los servicios de orientación jurídica y defensoría legal, están obligados a comprobar ante la Comisión Nacional que no cuentan con los recursos suficientes para contratar un defensor especializado en la materia que atienda sus intereses.

Artículo 88.- En caso de estimarlo necesario, la Comisión Nacional podrá mandar practicar los estudios socioeconómicos que comprueben que efectivamente, el Usuario no dispone de los recursos necesarios para contratar un defensor particular. En el supuesto de que, derivado de los estudios, el Usuario no sea sujeto de la orientación jurídica y defensoría legal, la Comisión Nacional podrá orientar y asesorar, por única vez, al Usuario para la defensa de sus intereses. Contra esta resolución no se podrá interponer recurso alguno.

Artículo 89.- Para el efecto de que la Comisión Nacional esté en posibilidad de entablar la asistencia jurídica y defensa legal del Usuario, es obligación de este último presentar todos los documentos e información que el Defensor designado por la Comisión Nacional le señale. En

caso de que alguna información no pueda ser proporcionada, el Usuario estará obligado a justificar su falta.

Cuando el Usuario no proporcione al Defensor la información solicitada y no justifique su falta, la Comisión Nacional no prestará la orientación jurídica y defensoría legal correspondiente.

En este sentido la defensoría legal se dará por parte de la CONDUSEF solamente a quien compruebe necesitarlo y cumpla cabalmente con lo estipulado en la norma, de esta manera la CONDUFSEF abre la baraja de opciones a considerar por parte del usuario para hacer valer sus derechos.

4.1.12 Recurso de revisión

El recurso de revisión es un medio de impugnación, por parte del afectado por considerar que alguno de sus derechos está siendo violentado u omitido.

El recurso de revisión se deberá de interponer después quince días hábiles siguientes a la fecha en que surta efectos la notificación del acto respectivo con fundamento en el artículo que a la letra regula:

Artículo 99. Los afectados con motivo de los actos de la Comisión Nacional en resoluciones dictadas fuera del procedimiento arbitral que pongan fin a un procedimiento o de la imposición de sanciones administrativas, podrán acudir en defensa de sus intereses interponiendo recurso de revisión, cuya interposición será optativa.

El recurso de revisión deberá interponerse por escrito dentro de los quince días hábiles siguientes a la fecha en que surta efectos la notificación del acto respectivo y deberá presentarse ante la Junta, cuando el acto haya sido emitido por dicha Junta o por el Presidente, o ante este último cuando se trate de actos realizados por otros servidores públicos.

El escrito mediante el cual se interponga el recurso de revisión deberá contener:

I. El nombre, denominación o razón social del recurrente;

II. Domicilio para oír y recibir toda clase de citas y notificaciones;

III. Los documentos con los que se acredita la personalidad de quien promueve;

IV. El acto que se recurre y la fecha de su notificación;

V. Los agravios que se le causen con motivo del acto señalado en la fracción IV anterior, y

VI. Las pruebas que se ofrezcan, las cuales deberán tener relación inmediata y directa con el acto impugnado.

Cuando el recurrente no cumpla con alguno de los requisitos a que se refieren las fracciones I a VI de este artículo, la Comisión Nacional lo prevendrá, por escrito y por única ocasión, para que subsane la omisión prevenida dentro de los tres días hábiles siguientes al en que surta efectos la notificación de dicha prevención y, en caso que la omisión no sea subsanada en el plazo indicado en este párrafo, la Comisión Nacional lo tendrá por no interpuesto. Si se omitieran las pruebas se tendrán por no ofrecidas.

Artículo 100. La interposición del recurso de revisión suspenderá los efectos del acto impugnado cuando se trate de multas.

Artículo 101. El órgano encargado de resolver el recurso de revisión podrá:

I. Desecharlo por improcedente;

II. Sobreseerlo en los casos siguientes:

a) Por desistimiento expreso del recurrente.

b) Por sobrevenir una causal de improcedencia.

c) Por haber cesado los efectos del acto impugnado.

d) Las demás que conforme a la ley procedan.

III. Confirmar el acto impugnado;

IV. Revocar total o parcialmente el acto impugnado, y

V. Modificar o mandar reponer el acto impugnado o dictar u ordenar expedir uno nuevo que lo sustituya.

No se podrán revocar o modificar los actos administrativos en la parte no impugnada por el recurrente.

El órgano encargado de resolver el recurso de revisión deberá atenderlo sin la intervención del servidor público de la Comisión Nacional que haya dictaminado la sanción administrativa que haya dado origen a la imposición del recurso correspondiente.

La resolución de los recursos de revisión deberá ser emitida en un plazo que no exceda de los noventa días hábiles posteriores a la fecha en que se interpuso el recurso, cuando deba ser resuelto por el Presidente, ni a los ciento veinte días hábiles cuando se trate de recursos que sean competencia de la Junta.

La Comisión Nacional deberá prever los mecanismos que eviten conflictos de interés entre el área que emite la resolución objeto del recurso y aquella que lo resuelve.

Artículo 105.- En el caso de que se confirme la resolución recurrida, la multa impuesta se actualizará de conformidad con lo previsto por el Código citado en el artículo 97. Las multas impuestas no se actualizarán por fracciones de mes.

Artículo 106.- Contra la resolución emitida para resolver el recurso de revisión no procederá otro."

El recurso de revisión es una actuación realizada por la parte afectada que sirve para solicitar la subsanación de una parte especifica del proceso que pudo haber sido violada u omitida durante el mismo, por tanto en caso de tener una resolución desfavorable siempre debe de ser la primera opción para revisar el proceso ya que aun a pesar de no ser favorable ´puede sirve para asentar las bases de que es correcto e incorrecto durante dicho proceso y por tanto recurrir a al siguiente instancia.

4.2 Procuraduría General de la Republica (PGR)

"La **Procuraduría General de la República** (PGR) es el órgano del Poder Ejecutivo Federal que se encarga de investigar y perseguir los delitos del orden federal. Ejerce sus atribuciones respondiendo a la satisfacción del interés social y del bien común.

Su titular es el Procurador General de la República, quien preside al Ministerio Público de la Federación.

El Procurador General de la República intervendrá por sí o por conducto de agentes del Ministerio Público de la Federación en el ejercicio de las atribuciones conferidas por la Constitución Política de los Estados Unidos Mexicanos, la Ley Orgánica de la PGR y las demás disposiciones aplicables."[89]

La intervención de la misma dentro de este tipo de delitos es el dar seguimiento a los mismos cuando por cuestiones de cuantía o delimitantes dentro de la normatividad vigente de la CONDUSEF esta no los puede atender o en su defecto cuando el usuario de servicios financieros opta por acudir directamente a la misma para presentar su denuncia o el laudo emitido por la CONDUSEF no satisface sus intereses y por tanto opta por acudir a dicha instancia para poder dar seguimiento a los mismos.

4.2.1 Competencia de la PGR

"Jurisdicción: Potestad y autoridad de una persona para gobernar y para poner en ejecución las leyes."[90]

La PGR al igual que la CONDUSEF tienen facultad para intervenir en asuntos relativos a delitos cibernéticos contra el sistema financiero teniendo como diferencial que la CONDUSEF es únicamente un ente conciliador y la PGR es un ente de Investigación, es decir, mientras la

[89] Procuraduría General de la Republica. (2018). *¿Qué Hacemos?*. Diciembre 2018, de Fiscalía General de la Republica Sitio web: https://www.gob.mx/pgr/que-hacemosquobit.mx. (abril 21,2018).

[90] The free dictionary Bay farlex. (2003). *the free dictionary Bay farlex*. Marzo 21,2018, de the free dictionary Bay farlex Sitio web:http://es.thefreedictionary.com/jurisdicci%C3%B3n

CONDUSEF únicamente emitirá un laudo y buscará el cumplimiento del mismo, la PGR buscará una sentencia y considerarla comisión de un delito.

La sentencia es una resolución judicial dictada por un juez o tribunal que pone fin a la litis (civil, de familia, mercantil, laboral, contencioso-administrativo, etc.) o causa penal.

Por tanto, tiene competencia tanto la CONDUSEF como la PGR pueden intervenir en dichos asuntos pero las consecuencias de las resoluciones de las mismas son sumamente diferentes, mientras el laudo atañe como sanción penas administrativas y multas económicas; la sentencia puede tener consigo sanciones de penas administrativas y multas económicas, así como penas de privación de la libertad para quien resulta responsable de dicho delito.

4.2.2 Presentación de denuncia

En este sentido se debe de indicar que la PGR para poder atender dichos delitos creo la DIVISIÓN CIENTÍFICA DE POLICÍA FEDERAL para poder conocer de los mismos y dar seguimiento, por tanto la presentación de la denuncia se realiza ante esta división, y se realiza de la siguiente manera:

"La Oficina del Comisionado Nacional de Seguridad exhorta a los usuarios a reportar cualquier sospecha de fraude o ataque cibernético al número telefónico **088**, que opera las 24 horas del día, los 365 días del año, así como a realizar denuncias a través de la cuenta de Twitter **@CEAC_CNS**, el correo **ceac@cns.gob.mx** y la aplicación **PF Móvil**, disponible para todas las plataformas de telefonía celular."[91]

Es decir, la policía federal está abierta los 365 días del año las 24 horas del día para recibir denuncias vía telefónica, mediante la red social twitter, correo electrónico y la aplicación móvil de la PF, por tanto cualquier afectado por un delito cibernético tiene la viabilidad de reportarlo

[91] Comisión Nacional de Seguridad. (Agosto 8, 2014). *División científica de policía federal detecta nuevas amenazas cibernéticas que suplantan identidades*. Diciembre 2018, de CNS. gob. Comunicado de Prensa No. 165 Sitio web: http://cns.gob.mx/portalWebApp/appmanager/portal/desk?_nfpb=true&_windowLabel=portlet_1_1&portlet_1_1_actionOverride=%2Fboletines%2FDetalleBoletin&portlet_1_1id=1348059

de manera inmediata y oportuna por esta vía para que se inicia la averiguación de parte de la autoridad competente.

4.2.3 Procedimiento

El procedimiento que se sigue para dar seguimiento a las denuncias presentadas por delitos cibernéticos ante la Policía Federal, es el mismo que se sigue para cualquier delito. Es decir, la Policía Federal recibirá la denuncia y esta será integrada con las pruebas correspondientes para pasar a un Ministerio Publico quien seguirá el siguiente proceso:

En el caso de delitos cibernéticos es sumamente complejo presentar una denuncia y tener identificado o acusar directamente al infractor, así mismo se debe de considerar que para la presentación de la misma esta deberá de ser acompañada por la mayor cantidad de pruebas que se tengan como son estados de cuentas, movimientos o compras no reconocidos, fechas de llamada a la institución financiera reportando el hecho, correos de la Institución financiera de seguimiento y todo aquel documento, audio, video o testigo que pudiera servir para dar validez al hecho que estamos denunciando.

La parte afectada deberá tener en cuenta que en este tipo de delitos específicamente se tendrán varias partes involucradas en el mismo como son la Institución Financiera en primera instancia y esta a su vez podrá negar o aceptar el hecho denunciado y en su caso un tercero que sería la persona que realizo el fraude, por tanto tendrá que ser muy cuidadoso en la presentación de pruebas y en cada uno de los señalamientos que hace en las diversas etapas del juicio, ya que un error en alguna señalización podría tener como consecuencia una sentencia en contra.

Por ejemplo, si se inicia la denuncia de manera directa mencionando a la Institución Financiera como la parte ejecutora del delito, y esta comprueba que la transacción que se reporta como fraudulenta en la cuenta se realizó utilizando la cuenta del cliente y pasando los filtros de seguridad como si fuera el cliente, el resultado sería desfavorable para el usuario.

Por tanto en este tipo de denuncias hay que ser cuidadoso en su redacción y argumentación, así como en la consecución y conjunción de pruebas que puedan soportar dicha denuncia. En este cuarto capítulo se toca el tema de los medios de defensa y procesos a seguir en caso de ser víctima del delito financiero.

Propuesta

Este trabajo de investigación propone dar inicio a un cambio paulatino pero constante en la forma en que cada usuario de la denominada red mundial internet, haga uso de esta proponiendo y fomentando diversos tipos de precauciones que le puedan dar como resultado la disminución de riesgos y vulnerabilidades en el manejo de su información personal.

La propuesta de este proyecto radica en dos puntos principales:

1) Las Instituciones Financieras en caso de no contar con los mecanismos de seguridad necesarios para salvaguardar la información personal de cada uno de los usuarios de los mismos, y que esta sea utilizada de manera indebida, esta deberá de hacer frente a la reparación del daño de manera íntegra, así como en el caso de que este daño afecte al patrimonio del mismo deberá cubrir dicho daño adicionado con la actualización a valor presente del importe de este.

2) Crear una institución especializada con recursos de particulares y fondos gubernamentales para mantener la imparcialidad, encargada de atender todo tipo de delitos cibernéticos, que esta institución tenga jurisdicción federal, y que tenga total autonomía para la imposición de sanciones hacia las personas físicas o morales responsables de cometer un ilícito cibernético.

Conclusión

El sistema jurídico mexicano está siendo rebasado por el voraz avance que tiene la tecnología día a día, situación que requiere de manera urgente profesionistas capaces y que se encuentren abiertos a la constante actualización y capacitación que apoyen en la actualización y formación de nuevas instituciones dentro del sistema de justicia mexicano, así mismo se requiere que las instituciones financieras cree cursos de capacitación y transmita la información a la sociedad general para que pueda esta tener una cultura financiera que les permita realizar una toma de decisiones asertiva considerando los riesgos y tomando todas las medidas pertinentes para poder disminuir los riesgos al realizar el uso de la red denominada internet.

El carding online es un delito de reciente creación que avanza de manera paralela al avance tecnológico aplicable a los modos, formas y empleo de las diversas herramientas usadas para la realización de operaciones financieras mediante el uso de la red mundial denominada Internet.

Por tanto, a mayor uso de las nuevas tecnologías para la realización de operaciones financieras mayor es la realización de este tipo de ilícitos.

En este tema cabe resaltar que México es un país que se encuentra en proceso de la inmersión de los usuarios de servicios financieros hacia el uso de estas tecnologías por tanto aún se encuentra en una etapa de concientización a los mismos para un uso seguro de estas aplicaciones.

De la misma manera se encuentra el marco legal mediante el cual se regula dichas operaciones puesto que debido al avance acelerado con el que se desarrolla nuevo software o aplicaciones, se están generando lagunas en la legislación vigente.

Por tanto, existen dos puntos a tener en cuenta que son aquellos en que se enfoca este trabajo:

1) Campañas de difusión masiva por parte de las Instituciones Financieras a nivel nacional para concientizar a cada uno de sus usuarios de servicios financieros sobre el riesgo, métodos y forma correcta del uso de las diversas aplicaciones y/o software diverso para la realización de estas operaciones.

2) Creación de nuevos órganos regulatorios especializados en el tema de delitos financieros que cuenten con la autonomía para poder sancionar, auditar y dictar resolución sobre asuntos concernientes a este tipo de delitos.

Concluyo este trabajo haciendo énfasis en la necesaria capacitación e inclusión de los usuarios de servicios financieros en este tipo de nuevas tecnologías bajo la tutela necesaria de las instituciones para que de manera conjunta se dé el paso a la modernización, es un paso necesario para ambas partes y que llegara nos guste o no pero que en la medida de lo posible se debe de trabajar en minimizar los riesgos.

Fuentes de Consulta e indagación

Bibliografía

Borda,G. (1999). *Tratado de derecho civil argentino: Parte general*. Tomo I. Argentina: La Ley.p.168.

Carrancá y Trujillo, R. & Carrancá y Rivas R. (2000). *Código Penal anotado*. México: Porrúa.

Davara Rodríguez, M. (1997). *Manual de derecho informático*. Pamplona: Aranzandi.p.166.

Greco, M. (2000). *Internet e Direito*. Sao Paulo: Dialéctica.2nda.ed.

Lima Malvido, M . (1984). *Delitos Electrónicos*. Criminalia, año 1, núm. 1-6, enero-junio, pp. 155.

Lorenzetti, R. (2001). *Comercio Electrónico*. Buenos Aires: Abeledo-Perrot. pp. 9-10.

Márquez Piñero, R. (1997). *Delitos Bancarios*. México: Porrúa.3era Ed.p. VII y VIII.

Medina, I. (enero-junio de 1977). *Problemática de la jurisdicción voluntaria*. Revista de la facultad de Derecho, números. 105-106. p.229.

Mengoni. (1986). *La seguridad jurídica como dato para la decisión empresario*. Revista del Derecho Comercial y de las Obligaciones, abril-junio de 1998. pp.722.

Mosset Iturraspe, J. (2016). *Contratos*. Argentina: Rubinzal-Culzoni.p.34-52.

Naisbitt, J. (1995*). Global Paradox*. E.U.A.: Avon Books.p.61.

Rafael,M. (1997). *Delitos Bancarios*. México: Porrúa. p VII-VII.

Real Academia Española. (1984). *Diccionario de la Lengua Española*. Madrid España: Espasa Calpe.

Reggini Horacio, C. (1996). *Los caminos de la palabra: Las telecomunicaciones de morse a Internet*. Buenos Aires: Galápagos.248 páginas.

Rodotá, S. (Mayo 8, 1998). *Libertà, opportunità, democrazia, informazione*. Internete privacy:qualiregole?, Supplemento n. 1al Bollettino n. 5.Presidenza del Consiglio dei Ministridipartimento per l'informazione e l'editor. pp.202.

Rojas Amandi, V. M. (2001). *El uso de internet en el derecho*. México: Oxford University. Press.248 páginas

Sarra , A. (2001). *Comercio Electrónico y derecho*. Buenos Aires: Astrea.pp.120

Télles Valdez, J. (1996). *Derecho Informático*. México: Mc Graw Hill.pp.103-104.

Toffler, T. (1994). *Las guerras del futuro: La supervivencia en el alba del siglo XXI*. España. p.338.

Télles Valdez, J. (1996). *Derecho Informático*. México: Mc Graw Hill.pp.103-104.

The Harvard Law Review Association. (Mayo 1999). *Developments in the law of cyberspace*. The Harvard Law Review Association, vol.112, num.7, i-viii.

Mesografía

Así funciona el Algoritmo de Luhn para generar números de tarjetas de crédito. Abril 6, 2018, de quobit.mx Sitio web:https://www.quobit.mx/asi-funciona-el-algoritmo-de-luhn-para-generar-numeros-de-tarjetas-de-credito.html

Banco Bilbao Vizcaya Argentaria, S.A. . (2019). *¿Qué significan los números de las tarjetas de crédito o débito?*. Abril 26, 2018, de BBVA Sitio web:https://www.bbva.com/es/como-afecta-la-subida-del-salario-minimo-a-la-economia/

Calderón, E. (Mayo 21, 2014). *Crece número de usuarios en internet*. Diciembre 2018, de E Logística, Revista Énfasis Sitio web: http://www.logisticamx.enfasis.com/notas/69665-crece-numero-usuarios-internet-mexico#

Cámara de Diputados. (Mayo 2015). *Procedimiento legislativo*. Diciembre 2018, de Dirección General del Centro de Documentación, información y análisis Sitio web: http://www.diputados.gob.mx/bibliot/publica/prosparl/iproce.htm

Casafranca, N. (Diciembre 3, 2016). *Historia del internet*. Marzo 2018, de LinkedIn Corporation Sitio web: https://www.slideshare.net/nicolecasafranca/historia-del-internet-69790623

Checks. (Noviembre 14, 2011). *Delitos informáticos*. Noviembre 2018, de Blog de Checks Sitio web: https://www.blogger.com/profile/07575685817478971568

Codina, L. (Abril 1996). *Negroponte, medios de comunicación y cuñadas digitales*. Septiembre 2018, de El profesional de la Información. Revista científica y profesional Sitio web: http://www.elprofesionaldelainformacion.com/contenidos/1996/abril/negroponte_medios_de_comunicacin_y_cuadas_digitales.html

Colorado, P. (Noviembre 18, 2008). *Delitos informáticos*. Abril 2018, de Blogspot Sitio web: http://gonzo-stelgon.blogspot.com/2008/11/historia-de-delitos-informticos.html

Comic69. (Mayo 17, 2015). *El uso del internet*. Septiembre 2018, de Blog Comic69 Sitio web: https://elusodelinternet1.wordpress.com/2015/05/17/hola-mundo/

Comisión Nacional de Seguridad. (Agosto 8, 2014). *División científica de policía federal detecta nuevas amenazas cibernéticas que suplantan identidades*. Diciembre 2018, de CNS. gob. Comunicado de Prensa No. 165 Sitio web: http://cns.gob.mx/portalWebApp/appmanager/portal/desk?_nfpb=true&_windowLabel=portlet_1_1&portlet_1_1_actionOverride=%2Fboletines%2FDetalleBoletin&portlet_1_1id=1348059

Comisión Nacional de Seguridad. (Mayo 8, 2014). *Impulsan policía federal y microsoft México seguridad informática y prevención de delitos cibernéticos*. Octubre 2018, de Comisión Nacional de Seguridad Sitio

web: http://www.cns.gob.mx/portalWebApp/appmanager/portal/desk?_nfpb=true&_pageLabel=portals_portal_page_m3p2_boletin&id=1344173

Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros. (Abril 19, 2016). *Se han realizado poco más de 12.1 millones de acciones de defensa a los usuarios de servicios financieros*. Abril 2018, de Condusef Sitio web: https://www.gob.mx/condusef/articulos/condusef-cumple-17-anos-29097

Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros. (2018). *¿Qué hacemos?*. Febrero 10, 2018, de Gobierno de México Sitio web: https://www.gob.mx/condusef/que-hacemos

Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros. (s.f.). *Formatos para presentar una Reclamación*. Diciembre 2018, de CONDUCEF Sitio web: https://phpapps.condusef.gob.mx/condusefenlinea/TATJ.php

Duarte Galvis, D. (Junio 1, 2011). *Historia del Internet*. Diciembre 2019, de Blog de Duarte Galvis D Sitio web: https://sites.google.com/site/historiadelinternetbycarolina/j-c-r-licklider

Enciclopedia Jurídica Online. (s.f.). *Derecho de Internet en el Derecho Mercantil Mexicano*. dicmebre 2018, de Enciclopedia Jurídica Online Sitio web: https://mexico.leyderecho.org/mercantil/derecho-de-internet/ https://mexico.leyderecho.org/fraude/

Flores, C. (Abril 23, 2017). *Fundamentos de Administración V2 Características del Administrador*. Diciembre 2018, de clubensayos.com Sitio web: https://www.clubensayos.com/Temas-Variados/Fundamentos-de-Administraci%C3%B3n-V2-Caracter%C3%ADsticas-del/3935662.html

Forbes Staff. (julio 21,2014). *40% de las tarjetas de crédito son víctimas de fraude*. marzo 5,2018, de Forbes México Sitio web:https://www.forbes.com.mx/40-de-las-tarjetas-de-credito-son-victimas-de-fraude/

Gobierno de la Ciudad de México. (2018). *Policía de Ciberdelincuencia Preventiva*. Abril 2018, de Gobierno de la Ciudad de México. Secretaria de Seguridad Ciudadana Sitio web: http://data.ssp.cdmx.gob.mx/ciberdelincuencia.html

Gobierno de México. (2013). Página Oficial. Abril 2018, de Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros Sitio web: https://www.gob.mx/condusef

Guzmán, B. (2011). *La Información y el Delito*. Octubre 2018, de Blog Guzmán Bruno Sitio web: https://sites.google.com/site/legisydelitosinfoform/creditos

Landa Durán, G. (Julio 2007). *Los delitos informáticos en el Derecho penal de México y España*. Diciembre 2018, de Revista del Instituto de la Judicatura Federal. Núm., 24 Sitio web: https://app.vlex.com/#sources/4800/issues/173617

Mastercard Latinoamérica. (Mayo 25, 2006). *Hemos hecho historia durante casi cincuenta años*. Junio 15,2018, de Mastercard Sitio web: https://latinamerica.mastercard.com/es-region-lac/acerca-de-mastercard/quienes-somos/historia.html

Para libros medios. (1998-2008). *Internet y la World Wide Web*. Agosto 2018, de Para libros medios Sitio web: http://www.paralibros.com/passim/p20-tec/pg2052ci.htm

Pastrana, R. (s.f.). *El origen del plástico*. Diciembre 2018, de Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros Sitio web: https://www.condusef.gob.mx/Revista/index.php/credito/tarjeta/200-el-origen-del-plastico

Ponce de León Armenta, L. (1992). *La Jurisdicción*. Abril 2018, de Instituto de Investigaciones Juridicas (UNAM) Sitio web: https://revistas.juridicas.unam.mx/index.php/derecho-comparado/article/view/2919/3175

Procuraduría General de la Republica. (2018). *¿Qué Hacemos?*. Diciembre 2018, de Fiscalía General de la Republica Sitio web: https://www.gob.mx/pgr/que-hacemosquobit.mx. (abril 21,2018).

Riveroll, C. (2015*). Fraude*. 02 2018, de mexico.leyderecho.org Sitio web: https://mexico.leyderecho.org/fraude/

Rodríguez, B. (Marzo 1, 2007). *Origen y evolución histórica de las tarjetas de crédito*. Diciembre 2018, de gestiopolis.com Sitio web: https://www.gestiopolis.com/origen-y-evolucion-historica-de-las-tarjetas-de-credito/

Rodríguez, S. (Agosto 2014). *Internet ventajas vs desventajas*. Diciembre 2018, de blog de Rodríguez Stefani Sitio web: http://523634635.blogspot.com/2014/08/la-evolucion-y-el-acceso-hacen-que.html#comment-form

Rodríguez, J. (2009). *La Competencia*. Diciembre 2018, de Monografia.com Sitio web: https://www.monografias.com/trabajos7/compro/compro.shtml

Sánchez López, K. (Noviembre 29, 2012). *Delitos Informáticos (México)*. Octubre 2018, de Estudiante Sánchez López Karla para monografias.com Sitio web:https://www.monografias.com/trabajos94/delitosinformaticos/delitosinformaticos.shtml

Segu. Info. Seguridad de la información. (2000-2009). *Legislación y Delitos Informáticos - La Información y el Delito*. Octubre 2018, de Seguridad de la información Sitio web: https://www.segu-info.com.ar/legislacion/

Torres Saavedra, N. (Diciembre 13, 2015). *Historia del Internet*. Diciembre 2018, de blogspot.com Sitio web: http://comunicacioniccs.blogspot.com/2015/12/maria-jesus-lamarca-lapuente_90.html

The free dictionary Bay farlex. (2003). *the free dictionary Bay farlex*. Marzo 21,2018, de the free dictionary Bay farlex Sitio web:http://es.thefreedictionary.com/jurisdicci%C3%B3n

Thirión J & Valle Zárate, J. (2018). *La brecha digital y la importancia de las tecnologías de la información y la comunicación en las economías regionales de México*. Diciembre 2018, de Revista Internacional de Estadística y Geografía "INEGI". Vol. 9, Núm. 2, mayo-agosto 2018. Sitio web: https://www.inegi.org.mx/rde/2018/11/07/la-brecha-digital-la-importancia-las-tecnologias-la-informacion-la-comunicacion-en-las-economias-regionales-mexico/

Ucha, F. (Marzo 12 2014). *Definición del delito*. Octubre 2018, de Definición ABC Sitio web: https://www.definicionabc.com/?s=Delito

Vandal/Noticias. (Febrero 5,2011*). Sony explica cómo hackearon PlayStation Network. Encubrieron el ataque como una compra en el servicio*. Junio 14,2018, de Vandal Sitio web: https://vandal.elespanol.com/noticia/55869/sony-explica-como-hackearon-playstation-network/

Vega Cruz, A. (Noviembre 2007). *Introducción a las ciencias de la computación*. Diciembre 2018, de Blog de Vega Cruz Alejandra Sitio web:https://www.blogger.com/profile/08225975711776843269

Legislación

1. Constitución Política de los Estados Unidos Mexicanos, México, septiembre de 2018

2. Ley de Banco de México, México, septiembre de 2018

3. Código Nacional de Procedimientos Penales, México, septiembre de 2018

4. Circular Única de Bancos, México, septiembre de 2018

5. Código Penal de la Ciudad de México, México, septiembre de 2018