UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ACATLÁN

El *phishing* como medio para realizar operaciones con recursos de procedencia ilícita en México.

S E M I N A R I O C U R R I C U L A R

QUE PARA OBTENER EL TÍTULO DE

L I C E N C I A D A E N D E R E C H O

Presenta:

GABRIELA FLORENCIO SÁNCHEZ

Asesora:

Mtra. María Iracema Cristal González Martínez

Santa Cruz Acatlán, Naucalpan Edo. de Méx., Noviembre 2020.

AGRADECIMIENTOS

"En algún momento, siempre llega una razón para comenzar de nuevo."

Para mi mamá, por ser esa luz que ilumina mi vida, por cuidarme en este camino de constantes altas y bajas, por ser mi paño de lágrimas y mi mejor consejera, por enseñarme día con día a ser fuerte y salir adelante, tal y como ella lo ha hecho. Por ser ese apoyo cuando llego a caer, por todo el amor que me ha dado. Gracias a ella, hoy estoy aquí y aunque el camino no fue fácil, hoy puedo decir, ¡Lo logramos, ma!

Para mi papá, donde quiera que se encuentre, este logro también va para él.

Para mi hermana Alma y mi cuñado César, por su apoyo incondicional, por hacerme reír en mis peores momentos y por demostrarme que no estoy ni estaré sola, es bonito saber que hay personas que te quieren sin esperar algo a cambio.

Para mi mejor amigo, Luis Jair Flores Ávila, por enseñarme a amar el Derecho tanto como él, por estar en mis mejores y peores momentos. Sin duda alguna, su llegada fue magia para mi vida, de esa magia que no creía encontrar, pero tuve la fortuna de hacerlo, ¡Gracias por llegar, pero sobre todo, por permanecer, Flores Ávila!

Para mi amiga y futura colega, Itzel Consuelo García Yáñez, por ser una de las personas que más admiro y que estuvo a mi lado desde el inicio hasta el final de esta aventura, porque con ella, la palabra amistad tiene varios significados.

Para la familia Hernández Sánchez, Martínez Sánchez y mis abuelitos maternos, Antonino y Honorina, por darme ánimos de seguir adelante y demostrarme el significado de la palabra familia.

Para mi mejor amiga, Diana Gómez Bautista, por enseñarme que ni el tiempo ni la distancia son más fuerte que una amistad. Doy gracias a la vida y a las clases de latín por regalarme amistades como ella.

Para mis amigas de nivel medio superior, Ruth, Caris y Liz, porqué como bien dijo alguna vez una maestra, “las amistades que haces en CCH son para toda la vida” y no llevamos una vida, pero espero así sea.

Para mis amigos de esta aventura, Edson, Paniagua, Tony, Camarguito, Andrea, Sofi, Susu, Itz, Anita, Mido, Paquito y Daniel; así como todos aquellos que fueron parte de esta etapa, por su apoyo en el ámbito personal y académico, por hacer la carrera menos pesada, por compartir sus conocimientos conmigo, pero sobre todo, por estar en las buenas, malas y peores a mi lado.

Para Gustavo Domínguez, por llegar de manera inesperada a mi vida pero en el momento indicado, demostrándome que siempre se puede comenzar de nuevo y como dice aquella canción, “cuando se perdió la fe y dejaba de creer, me di vuelta y te encontré”.

A mi asesora, la Mtra. María Iracema Cristal González Martínez, por todo su apoyo tanto profesional como personal, siendo parte fundamental para poder culminar este trabajo de investigación satisfactoriamente.

A mi amada Universidad Nacional Autónoma de México, quien me abrió sus puertas desde hace 8 años, convirtiéndose en mi segunda casa, quien a lo largo de todos esos años, se encargó de prepararme tanto profesional como personalmente para enfrentar aquellos retos que la vida te pone.

Por último, a todas aquellas personas que se han cruzado en mi camino y han sido parte de esto.

TABLA DE CONTENIDOS.

Introducción……..……..I-II

CAPÍTULO I: ANTECEDENTES DE LA CONDUCTA DE *PHISHING* Y EL DELITO DE OPERACIONES CON RECURSOS DE PROCEDENCIA ILÍCITA.

1.1.- Definición de delito informático……..……..…..…….1

1.1.1.- Clasificación de los delitos informáticos……..…….....2

1.1.2.- Características de los sujetos activos en los delitos informáticos……..….....4

1.2.- La conducta de *phishing*……..…….5

1.2.1.- Técnicas para llevar a cabo la conducta de *phishing*…….....7

1.2.2.- El robo de identidad…….....9

1.3.- El delito de operaciones con recursos de procedencia ilícita……..11

1.3.1.- Etapas del lavado de dinero…….....14

1.3.2.- Características del lavado de dinero……19

CAPÍTULO II.- ORDENAMIENTOS NORMATIVOS QUE REGULAN LA CONDUCTA DE *PHISHING* Y EL DELITO DE OPERACIONES CON RECURSOS DE PROCEDENCIA ILÍCITA.

2.1.- Regulación de la conducta de *phishing* en el ordenamiento normativo mexicano…….....21

2.2.- Regulación del *phishing* en el ordenamiento normativo internacional…….....29

2.3.- Regulación del delito de operaciones con recursos de procedencia ilícita en el ordenamiento normativo mexicano…….....33

2.4.- Regulación del delito de operaciones con recursos de procedencia ilícita en el ordenamiento normativo internacional…….....37

CAPÍTULO III.- LA COMISIÓN DE LA CONDUCTA DE *PHISHING* Y EL DELITO DE OPERACIONES CON RECURSOS DE PROCEDENCIA ILÍCITA.

3.1.- Relación entre el *phishing* y el delito de operaciones con recursos de procedencia ilícita…….....43

3.1.1.- Formas de comisión conjunta del *phishing* y el delito de operaciones con recursos de procedencia ilícita…….....44

3.1.2.- Los intermediarios o muleros en la conducta de *phishing* y el delito de operaciones con recursos de procedencia ilícita……..……48

3.1.3.- Comisión de la conducta de *phishing* y el delito de operaciones con recursos de procedencia ilícita en México…….....51
Conclusiones……....61
Propuestas…….....63
Índice de cuadros…….....64
Bibliografía……..65

INTRODUCCIÓN

El delito de operaciones con recursos de procedencia ilícita ha tenido un aumento considerable desde el año 2016 a la fecha. Este delito puede llevarse a cabo de diferentes maneras, una de ellas es a través de la conducta de *phishing*[1], por medio de la cual, se utilizan los datos de cuentahabientes para abrir nuevas cuentas bancarias a su nombre, concretándose el robo de identidad del cuentahabiente y con ello introducir de manera legal, el dinero que fue obtenido de la comisión de otro delito, sin que los sujetos que llevan a cabo el delito de lavado de dinero puedan ser descubiertos.

En tal virtud, el *phishing* no tiene una regulación específica en el Código Penal Federal, por lo que, al no estarlo, la sanción impuesta por esta conducta ilícita no es considerada, sino que la sanción exclusivamente se enfatiza en el delito de lavado de dinero.

Derivado del problema mencionado con antelación, en la presente investigación, se planteó como hipótesis descriptiva que, la conducta de *phishing,* al no estar tipificada de manera específica dentro del Código Penal Federal, trae como consecuencia que al cometerse esta conducta para llevar a cabo el lavado de dinero, no se tenga una sanción proporcional para el *phishing* y el lavado de dinero, ya que solo se sanciona el delito de operaciones con recursos de procedencia ilícita, entonces, se debe regular la conducta de *phishing* y el delito de operaciones con recursos de procedencia ilícita en un mismo ordenamiento jurídico, máxime que uno es el medio para llegar a la comisión del otro.

Para poder resolver el planteamiento del problema, así como comprobar la hipótesis descriptiva, se planteó como objetivo el demostrar que la conducta de

[1] El *phishing* como lo menciona Palomá: “Es una técnica de engaño utilizada para obtener información confidencial de un usuario y se trata de duplicar algo haciendo creer al usuario que está usando el producto original (…)”. Tomado de: Palomá Parra, Luis Orlando, *Delitos informáticos (en el espacio) doctrina y análisis de casos reales,* Colombia, Ediciones Jurídicas Andrés Morales, 2012, p. 39.

phishing al no estar tipificada de manera específica dentro del Código Penal Federal, sino solo estar mencionada dentro del capítulo correspondiente a los delitos informáticos, entonces causa que solo se sancione el delito de operaciones con recursos de procedencia ilícita.

Precisado lo anterior, el presente trabajo de investigación se compone de tres capítulos. Respecto del capítulo primero, en este se podrá percibir todo el marco conceptual de la conducta de *phishing* y el delito de operaciones con recursos de procedencia ilícita, sus características y su forma de comisión, con la finalidad de describir los aspectos generales de los mismos.

En tanto, por lo que hace al capítulo segundo, en este se podrá apreciar los ordenamientos normativos a nivel nacional como internacional, en los cuales se encuentra regulado el delito de lavado de dinero y la conducta de *phishing*, con la finalidad de identificar que ordenamientos normativos los regulan y el contenido de manera general de cada uno de ellos.

Por último, en el tercer capítulo se podrá apreciar la relación que existe entre el delito de operaciones con recursos de procedencia ilícita y la conducta de *phishing,* así como el impacto que ambos han tenido en México, teniendo como finalidad explicar en qué momento el *phishing* funge como medio para llevar a cabo la comisión de lavado de dinero.

CAPÍTULO I: ANTECEDENTES DE LA CONDUCTA DE *PHISHING* Y EL DELITO DE OPERACIONES CON RECURSOS DE PROCEDENCIA ILÍCITA.

1.1.- DEFINICIÓN DE DELITO INFORMÁTICO.

Antes de profundizar en el estudio del *phishing*, cabe mencionar que este se desprende de los delitos informáticos, ya que para su comisión se utilizan aparatos tecnológicos como son las computadoras y un vasto conocimiento en temas relacionados con la informática, en tal virtud, tal como lo define Téllez: "los delitos informáticos son actitudes contrarias a los intereses de las personas en que se tiene a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin (concepto típico)".[1]

Por otra parte, el autor Loredo refiere lo siguiente: "Delito informático es el uso de cualquier sistema informático como medio o fin de un delito. De esta manera se abarcan todas las modalidades delictivas de acuerdo al marco legal de cada país; (…)".[2]

De las definiciones propuestas se puede constatar que, dichos delitos tal y como lo define el autor Loredo, pueden ser también un medio para cometer otros delitos, como es el caso del *phishing.* Del mismo modo, otra definición de derecho informático es la que refiere Estrada:

> (…) implica actividades criminales que en un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos o hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etc. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de las computadoras, lo que ha propiciado a su vez la necesidad de regulación por parte del Derecho. [3]

[1] Téllez Váldes, Julio, *Derecho informático*, 3a. ed., México, McGraw-Hill Interamericana, 2004, p. 163.
[2] Loredo González, Jesús Alberto, "Delitos informáticos: su clasificación y una visión general de las medidas de acción para combatirlo", *Celerinet, 2013,* enero-junio, p. 45, fecha de consulta: 04 de marzo de 2019, *http://eprints.uanl.mx/3536/1/Delitos_informaticos.pdf.*
[3] Estrada Garavilla, Miguel, "Delitos informáticos", p. 4, fecha de consulta: 04 de marzo de 2019, *https://www.unifr.ch/ddp1/derechopenal/articulos/a_20080526_32.pdf.*

Por último, pero no menos importante, en su libro el autor Díaz menciona que Libano define al delito informático como:

> (…) todas aquellas acciones u omisiones típicas, antijurídicas y dolosas, trátese de hechos aislados o de una serie de ellos, cometidos contra personas naturales o jurídicas, realizadas en uso de un sistema de tratamiento de la información y destinadas a producir un perjuicio en la victima a través de atentados a la sana técnica informática, lo cual, generalmente, producirá de manera colateral lesiones a distintos valores jurídicos, reportándose, muchas veces, un beneficio ilícito en el agente, sea o no carácter patrimonial, actúe con o sin ánimo de lucro.[4]

Las definiciones anteriormente descritas mantienen un común denominador que son los sistemas informáticos y los equipos de cómputo, los cuales se utilizan como medios o fines para cometer dichos delitos. Visto lo anterior, desde mi perspectiva defino a los delitos informáticos como aquellas conductas ilícitas realizadas por personas que tienen un extenso conocimiento en temas relacionado con la informática, utilizando equipos tecnológicos para su comisión y las cuales están en constante cambio, derivado de la evolución tecnológica que se da día con día.

Los delitos informáticos se han intentado encuadrar en aquellos delitos tipificados en el Código Penal Federal, entre ellos el robo y el fraude, dando a entender que como tal, no tienen el carácter de delitos informáticos, ya que derivan de delitos generales.

1.1.1.- CLASIFICACIÓN DE LOS DELITOS INFORMÁTICOS.

El autor Téllez hace una clasificación de los delitos informáticos en su obra Derecho Informático conforme a los elementos siguientes:

[4] Libano Manzur, Claudio: *loc. cit*., Díaz García, Alexander, *Derecho informático, elementos de la informática jurídica,* Colombia, Leyer, 2012, p. 155.

CUADRO 1.- CLASIFICACIÓN DE LOS DELITOS INFORMÁTICOS.

COMO INSTRUMENTO O MEDIO	COMO FIN U OBJETIVO
En esta categoría tenemos a aquellas conductas que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito.	En esta categoría encuadramos a las conductas que van dirigidas en contra de la computadora, accesorios o programas como entidad física.
EJEMPLOS:	**EJEMPLOS:**
1.- Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etcétera).	1.- Programación de instrucciones que producen un bloqueo total al sistema.
2.- Variación de los activos y pasivos en la situación contable de las empresas.	2.- Destrucción de programas por cualquier método.
3.- Planeación o simulación de delitos convencionales (robo, homicidio, fraude, etcétera).	3.- Daño a la memoria.
4.- Robo de tiempo de computadora.	4.- Atentado físico contra la máquina o sus accesorios (discos, cintas, terminales, etcétera).
5.- Lectura, sustracción o copiado de información confidencial. (…)	5.- Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados. (…)[5]
Fuente: Cuadro elaboración propia con datos obtenidos de Téllez Valdés, Julio, *op. cit.*, pp. 165, 166.	

De la clasificación anterior, se desprende dos modalidades, como instrumento o medio y como fin u objeto, en tal virtud y sin adentrarse aún al estudio de la conducta de *phishing,* esta se clasificaría como “instrumento o medio”, toda vez que el medio para la comisión de dicha conducta son las computadoras, ya que a través del uso de éstas es como se puede realizar el *phishing*, tal y como lo refiere la clasificación mencionada con antelación.

[5] Téllez Valdés, Julio, *op. cit.*, pp. 165-166.

Asimismo, Díaz en su obra cita la clasificación del autor Claudio Libano Manzur y en esta hace referencia a la manipulación indebida de datos, delito de espionaje informático, delito de sabotaje informático, delito de piratería de programas, delitos de *hacking*, delito de homicidio, delito de hurto calificado, delito de acceso electrónico doloso y culposo y delito de falsificación informática. [6] En ese sentido, este autor hace una clasificación enfocada más a los delitos informáticos que existen y de los cuales, pueden derivar otros delitos.

1.1.2.- CARACTERÍSTICAS DE LOS SUJETOS ACTIVOS EN LOS DELITOS INFORMÁTICOS.

Las personas que llevan a cabo los delitos informáticos, se caracterizan por tener ciertos aspectos que son esenciales para poder cometerlos, tal y como lo menciona Téllez:

> Las personas que cometen este tipo de delitos son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aun cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.[7]

Como lo menciona este autor, el sujeto activo en los delitos informáticos, debe tener un conocimiento basto respecto a los sistemas informáticos, sin embargo, este conocimiento va a variar dependiendo del delito que se quiera realizar. Otras características de los sujetos activos, son las que establece el autor Díaz:

> (…)
>
> 2. Poseen importantes conocimientos de informática.
>
> 3. Ocupan lugares estratégicos en su trabajo, en los cuales se maneja información de carácter sensible (se los ha denominado delitos

[6] Libano Manzur, Claudio: *loc. cit*., Díaz García, Alexander, *op. cit.*, pp. 155-159.
[7] Téllez Valdés, Julio, *op. cit.*, pp. 163-164.

ocupacionales ya que se cometen por ocupación que se tiene y el acceso al sistema).

4. Se tiene que considerar que son personas diferentes, porque no es lo mismo el joven que entra a un sistema informático por curiosidad, por investigar o con la motivación de violar el sistema de seguridad como desafío personal, que el empleado de una institución financiera que desvía fondos de las cuentas de sus clientes.

5. Son personas inteligentes, motivadas y dispuestas a aceptar el desafío tecnológico.

6. Estos delitos se han calificado de cuello blanco, porque el sujeto que comete el punible es una persona de cierto status socioeconómico.

(…)[8]

De las características antes mencionadas, se hace evidente que para cometer este tipo de delitos se necesita de lugares estratégicos, es decir, que los sujetos activos puedan realizar los delitos en sus zonas de trabajo, las cuales deben estar relacionadas con sus conocimientos en informática.

1.2.- LA CONDUCTA DE *PHISHING.*

Etimológicamente *phishing,* es una palabra en inglés, que como lo menciona el autor Palomá en su obra:

> El término *phishing* proviene de la palabra inglesa *Phishing* (pesca), haciendo alusión al intento de hacer que los usuarios caigan en la trampa o engaño. (…) También se dice que el término *phishing* es la contracción de "*password harvesting phishing"* que significa cosecha y pesca de contraseñas, aunque esto posiblemente es un acrónimo, dado que la escritura "ph" es comúnmente utilizada por *hackers* para sustituir la f, como raíz de la antigua forma de *hacking* telefónico conocida como *phreaking. [9]*

En ese sentido, el primer contacto que se puede tener con el significado de esta conducta ilícita es el que se tiene con la traducción de esta palabra, sin embargo, su simple traducción no puede englobar lo que es la propia conducta de

[8] Díaz García, Alexander, *op. cit*., pp. 159-160.
[9] Palomá Parra, Luis Orlando*, Delitos informáticos (en el ciberespacio). Doctrina y análisis de casos reales,* Colombia, Ediciones jurídicas Andrés Morales, 2012, p.113.

phishing y todo lo que conlleva, toda vez que dicha traducción refiere a una pesca de información, pero hasta esa momento, aún no se concreta dicha conducta como tal, ya que no refiere con qué fin utilizan la información sustraída.

Por consiguiente, al tener el conocimiento general de lo que implica un delito informático, se puede comenzar el estudio en particular sobre el *phishing.* El autor Palomá cita la definición de la autora Márquez González en su obra, la cual define a esta conducta como:

> (…) una técnica de engaño utilizada para obtener información confidencial de un usuario y se trata de duplicar algo haciendo creer al usuario que está usando el producto original. Por ejemplo, duplican la página *web* de un banco, que es casi exactamente la misma y el usuario creyendo que está en la página original ingresa todos sus datos. Entonces…Adiós dinero. [10]

Principalmente la comisión de esta conducta se basa primordialmente en el engaño del que son víctimas los sujetos pasivos, es decir, las personas a las cuales se les ha robado su información confidencial. De acuerdo con esto, Montoya, lo menciona como: "Conducta fraudulenta que mediante la utilización de páginas de dominio falsas se apodera de los datos de los usuarios que accedan a ellas. En ocasiones se puede fraguar el engaño con una combinación de *phisihing* (sic) y de SPAM". [11]

Algo que menciona el autor Velasco en su obra, es que el *phishing* en ciertas legislaciones de algunos países lo utilizan como sinónimo de robo de identidad, por ello, la definición que este autor cita del *Anti-Phishing Working Group* tiene que ver con lo que él menciona, toda vez que: "lo define como un mecanismo que emplea tanto técnicas de ingeniería social y técnicas evasivas para robar la identidad, los datos personales y la información financiera de los consumidores". [12]

En conclusión, el *phishing* se basa principalmente en el engaño y el robo de información de las personas que son víctimas de esta conducta, trayendo consigo

---

[10] *Ibídem.,* p. 39.
[11] Montoya Piña, Javier Omar, *Delitos federales cometidos a través de medios informáticos,* México, Flores Editor y Distribuidores, S.A. de C.V., 2015, p. 118.
[12] Velasco San Martín, Cristos, *La jurisdicción y competencia sobre delitos cometidos a través de sistemas de cómputo e internet,* España, Tirant lo Blanch, 2012, p. 71.

que se pueda dar un robo de identidad, como lo destaca el autor Velasco, siempre y cuando una vez que ha sido sustraída dicha información confidencial, sea utilizada para llevar a cabo un hecho ilícito. Cabe destacar que al tener una estrecha relación la conducta de *phishing* con el robo de identidad, también se debe adentrar al estudio del segundo, sin embargo, para no perder la secuencia del estudio de esta conducta ilícita, se estudiará el delito de robo de identidad con posterioridad.

1.2.1.- TÉCNICAS PARA LLEVAR A CABO LA CONDUCTA DE *PHISHING.*

Todo delito se caracteriza por tener técnicas o modos de concretarse que los distinguen de otros delitos, es decir, dependiendo del delito que se cometa, es la técnica que los sujetos activos llevarán a cabo. Respecto a la conducta ilícita de *phishing,* puede llevarse a cabo de diferentes maneras, entre ellas las siguientes:

> (…) (i) *«Pharming»* que además de utilizar las técnicas comunes de falsificación de sitios, redirige a los usuarios de un sitio autentico hacia un sitio fraudulento similar al original mediante la modificación de las direcciones IP; (ii) *«smishing»* mediante el cual los usuarios de telefonía móvil reciben mensajes SMS en donde se falsifican los sitios y vínculos de portales para robar la información personal de los usuarios; (iii) *«vishing»* que es una técnica relativamente reciente que utiliza la telefonía basada sobre protocolo IP (VoIP) en donde se envían mensajes de correo falsificando el nombre y marca de alguna institución bancaria o sistemas de pago e invitando a los usuarios a marcar un número de teléfono en donde sistemas automatizados contestan solicitando información personal, bancaria y contraseña con el propósito de verificar la seguridad; (…).[13]

De estas técnicas se puede apreciar que los instrumentos para llevarlos a cabo, recaen principalmente en sitios de internet, mensajes de texto y llamadas telefónicas, aunque la última de ellas solo al principio utiliza correos electrónicos y finaliza con una llamada telefónica, máxime que todas ellas tienen como fin el robo de información de las personas.

[13] *Idem.*

Para ejemplificar lo anterior, en uno de los artículos de la revista Proceso, se informa que la Fiscalía General de la República emitió una alerta por ciertos códigos que tiene como fin robar la información crediticia de las personas, toda vez que "este código se propaga por medio de correo electrónico, a través de un mensaje que solicita la identificación de un depósito por un monto económico y que incluye un enlace a una página de internet externa"[14] por lo que, una vez que la persona ingresa sus datos crediticios en la página externa que supuestamente pertenece a la institución financiera, esta capta sus datos, concretándose así el *phishing.*

Otra clasificación de técnicas para llevar a cabo la conducta de *phishing* son las que menciona el autor Palomá:

CUADRO 2.- TÉCNICAS PARA REALIZAR LA CONDUCTA DE *PHISHING.*

1.- Diseño para mostrar que un enlace es un correo electrónico (sic) parezca una copia de la organización por la cual se hace pasar el impostor.
2.- *URLs* mal escritas o el uso de subdominios.
3.- El atacante utiliza contra la víctima el propio código de programa del banco o servicio por el cual se hace pasar, (…) dirige al usuario a iniciar sesión en la propia página del banco o servicio, donde la *URL* y los certificados de seguridad parecen correctos. En este método de ataque (conocido como *Cross site scripting)* los usuarios reciben un mensaje diciendo que tienen que "verificar" su cuentas, seguido por un enlace que parece la página *web* auténtica; en realidad el enlace está modificado para realizar este ataque; (…)[15]
*Fuente: Cuadro elaboración propia con datos obtenidos de Palomá Parra, Luis Orlando,*op. cit.,* p. 115.

[14] "La redacción, FGR alerta sobre código malicioso que roba información crediticia", *Proceso. com.mx,* 18 de marzo de 2019, fecha de consulta: 19 de marzo de 2019, *https://www.proceso.com.mx/575799/fgr-alerta-sobre-codigo-malicioso-que-roba-informacion-crediticia?fbclid=IwAR3HuDesMHcOUNH5nAKkGlIHj-4H9ZDqG-NDLbEUKuZzlMt-jdXwlAv8Jzw.*

[15] Palomá Parra, Luis Orlando*, op. cit.,* p. 115.
Respecto a la técnica marcada con el número 1, se refiere a que los correos que reciben las victimas a pesar de que son idénticos a aquellos correos que la propia organización puede mandar, estos no provienen de dicha organización, toda vez que son copia exacta creada por los sujetos activos para hacer creer a la víctima que es un correo original cuando en realidad sólo es una simulación para el robo de información.
Ahora bien, respecto a la técnica marcada con el número 2, una *URL* es aquella dirección que, al escribirla en el ordenador, nos lleva a una página de internet, sin embargo, como lo menciona dicha técnica, al estar mal escrita la *URL,* puede ser la clave para que se dirija a una página diferente a la que se quiere entrar y así llevarse a cabo el *phishing.*

De lo anterior, se puede percibir que dichas técnicas tienen en común el robo de información confidencial para concretar la conducta tipificada en los delitos informáticos.

1.2.2.- EL ROBO DE IDENTIDAD.

Como se mencionó en el apartado correspondiente al *phishing,* respecto al robo de identidad, algunos autores lo manejan como sinónimo de la conducta de *phishing*, por lo que resulta importante conocer sobre el mismo. Para comenzar, primero se debe tener una aproximación conceptual sobre la palabra identidad, como bien lo refiere Romero, la identidad "hace referencia a un conjunto de características, datos o información que permiten individualizar a una persona"[16] por ejemplo, el nombre, la huella digital, la Clave Única de Registro de Población, entre otros.

Ahora bien, respecto del delito de robo de identidad, no hay una definición concreta para tal delito, sin embargo, Romero se refiere a este como "(…) la apropiación indebida de la identidad o de cualesquiera otros datos personales (…)"[17] y como bien lo define este autor, el robo de identidad se refiere a aquel apoderamiento que una persona hace de los datos propios de otra persona sin su consentimiento, pero no sólo el delito se concreta en la simple apropiación de esos datos, sino, también el fin para los cuales van a ser utilizado, ya que una de las funciones de este delito es poder cometer otra actividad ilícita, con la finalidad de que los sujetos activos no sean descubiertos.

Asimismo, el autor Velasco refiere que el delito de robo de identidad "(…) es comúnmente utilizado para describir que la información personal de un individuo, tal y como información identificable, financiera o médica, ha sido obtenida y utilizada sin su consentimiento y con el propósito de cometer una actividad ilícita

[16] Romero Flores, Rodolfo, "El robo o usurpación de identidad por medios informáticos o telemáticos: su tratamiento jurídico", fecha de consulta: 12 de marzo de 2019, *https://archivos.juridicas.unam.mx/www/bjv/libros/6/2958/20.pdf.*
[17] *Ibídem*, p. 305.

fraudulenta”[18], donde dicha actividad ilícita es poco probable que sea descubierta a tiempo por las víctimas, pero sobre todo poder descubrir de manera fácil quién realizó dichas actividades, ya que derivado del robo de identidad, las personas a las cuales pertenece esa información, pueden considerarse como aquellas que cometieron los delitos posteriores a dicho robo de información, sin ser ellas los verdaderos sujetos activos.

El delito de robo de identidad como la conducta de *phishing,* se puede constatar que, no es del todo correcto utilizar el primero como sinónimo del segundo, como lo utilizan ciertos autores, toda vez que, el *phishing,* al estar dentro del apartado de los delitos informáticos, necesita de sistemas informáticos para su comisión y con ello poder obtener la información de las víctimas, en tanto, el robo de identidad, puede darse de muchas maneras, como lo menciona Amigón:

> Si no tomas las debidas precauciones al realizar compras, pagos de servicios, de impuestos, o transacciones bancarias vía internet, robo de teléfonos celulares, si proporcionas demasiada información a través de redes sociales, en estado de cuenta o documentos personales que tiras sin precaución a la basura, robo de correspondencia, robo de carteras o bolsos con tarjetas de crédito o identificaciones.[19]

Ya que se puede o no hacer uso de los sistemas informáticos como lo hace el *phishing,* sin embargo, lo que ambos tienen en común es la obtención de información de las personas para realizar actividades ilícitas, por ello, se puede apreciar que el delito de robo de identidad va de la mano con la conducta de *phishing,* por lo tanto, no son sinónimo uno del otro.

[18] Velasco San Martín, Cristos, *op, cit.,* p. 72.
[19] Amigón, Edgar, “Robo de identidad, un delito en aumento”, *Primer Plano,* p. 23, fecha de consulta: 19 de marzo de 2019, *https://www.condusef.gob.mx/Revista/PDF-s/2015/186/robo.pdf.*

1.3.- EL DELITO DE OPERACIONES CON RECURSOS DE PROCEDENCIA ILÍCITA.

Como introducción se darán los antecedentes que dieron origen al delito de operaciones con recursos de procedencia ilícita o también llamado lavado de dinero, desde qué momento se empezó a realizar la comisión de dicho delito y quienes fungieron como autores originales del mismo, principalmente como lo refiere Figueroa:

> (…) los primeros capitales lavados lo habrían sido en Estados Unidos de Norteamérica, en la época de los *gángsters* y de la Ley Seca, principalmente con Al Capone, Lucky Luciano, Bugsy Moran y Meyer Lansky quienes literalmente crearon compañías (lavanderías) para ocultar el dinero sucio en Chicago. Otros precisan que se habría originado durante la segunda guerra mundial. Tanto Alemania como Italia remitían oro a Suiza para proveerse de las divisas necesarias para importar oro obtenido del saqueo efectuado por las tropas en diversos países avasallados por la fuerza de las armas, aunque también algunas remesas eran propiedad del Estado y de particulares. Nunca fue posible probar fehacientemente estos hechos, pues el oro era fundido y vendido en lingotes a destinatarios desconocidos por los bancos suizos.
>
> Con Italia, debido a la frontera en común, se hicieron asiduos negocios al terminar la guerra, a tal punto que la zona suiza se pobló de bancos dispuestos a no preguntar de dónde provenía el dinero, (…) .Sin embargo, es preciso destacar que este problema cobró cada vez más relevancia a partir no sólo de la globalización de los mercados financieros, sino también del incremento en el tráfico internacional de drogas o los llamados narcodólares (…)[20]

En ese sentido, el origen de lavado de dinero data aproximadamente desde el año de "1900, la época dorada de los *gangsters*"[21], por lo que hace a Estado Unidos. En tanto, en Alemania, este delito tuvo sus primeros orígenes en los inicios de la segunda guerra mundial, en el año de 1939, aunque ambas fechas son distantes, lo cierto es que su origen se da en la época de los noventa, teniendo

[20] Figueroa Velázquez, Rogelio M., *El delito de lavado de dinero en el derecho penal mexicano,* México, Porrúa, 2001, pp. 1-2.

[21] "De Al Capone a Lucky Luciano: 'gangsters' que marcaron época y estilo", *Gentleman. El Confidencial,* 2017, fecha de consulta: 19 de marzo de 2019, *https://www.gentleman.elconfidencial.com/multimedia/album/reportajes/2017-10-24/gansters-estilo-al-capone-lucky-luciano-bugsy-siegel_1329527#0.*

como objetivo ocultar los activos obtenidos de forma ilícita. Otro de los orígenes es el que hace referencia a las lavanderías utilizadas en aquella época, como se precisa a continuación:

> El término "lavado de dinero" surgió en los Estados Unidos en la década de 1920. Aparentemente, era utilizado por los oficiales de policía estadounidenses para referirse a la propiedad y al uso de lavanderías de ropa y de carros por parte de grupos de la mafia. Estos grupos mostraban gran interés en comprar estas lavanderías, muchas de las cuales ya pertenecían a otros grupos delictivos, porque esos negocios les permitían dar una apariencia legítima al dinero que provenía de sus actividades delictivas. El dinero obtenido de los actos ilícitos era declarado como si hubiera sido una ganancia obtenida a través de las lavanderías. El hecho de que las lavanderías operaban con mucho dinero en efectivo y con billetes de baja denominación, ayudaba a que fuera más difícil determinar el origen del dinero.[22]

De la transcripción anterior, se advierte con mayor precisión el origen del término utilizado para el delito de operaciones con recurso de procedencia ilícita, esto es el lavado de dinero, toda vez que, la manera en que ocultaban los recursos obtenidos indebidamente era a través del uso de lavanderías, por ello, al ser una actividad normal que generaban ingresos, era la manera perfecta para ocultar los recursos obtenidos de actividades ilícitas.

Ahora bien, una vez conocido el origen de dicho delito, se debe tener una concepción del mismo, puesto que su interpretación literal, cambia el verdadero sentido del delito, esto es que, al utilizarse el término lavado de dinero, los lectores pueden pensar que dicha actividad no es ilícita, cuando la realidad es que sí lo es, por lo que, una definición de este delito es la que refiere Figueroa:

> Por nuestra parte, entendemos que el lavado de dinero es una forma típica y antijurídica de delinquir organizadamente, dando como consecuencia que las ganancias producidas del ilícito se transformen en ingresos aparentemente lícitos, que son manipulados por instituciones financieras así como por otros tipos de empresas como si fueran ganancias lícitas.[23]

[22] Guillermo, Jorge *et al.,* (coord.), *Lavado de activos: un nuevo modelo de investigación,* 2da. ed., República Dominicana, Ministerio, 2010, p. 19.
[23] Figueroa Velázquez, Rogelio M., *op. cit.,* p. 65.

De dicha concepción sobre el delito de lavado de dinero, se puede apreciar que su finalidad es que las ganancias obtenidas de la actividad ilícita, puedan ser ingresadas en el sistema financiero y así volverse ganancias lícitas, para así ocultar el verdadero origen de éstas y por lo tanto, los sujetos activos puedan seguir cometiendo más delitos de los cuales resulten más ganancias que puedan seguir siendo consideradas de origen lícito.

En aras de ampliar el concepto del delito de lavado de dinero, otra definición es la que refiere Ferrusquía del Dr. Zamora:

> Es un proceso mediante el cual se realiza cualquier acto u operación con divisas o activos que provengan de una actividad tipificada como delito por la legislación del país en el que se efectúen dichos actos u operaciones, con el propósito fundamental de ocultar el origen ilícito de tales divisas y activos, utilizando una serie de actos permitidos por la ley, para llegar a un fin prohibido por la misma.[24]

Dicha definición precisa que los activos son obtenidos a través de actividades ilícitas, "entre las que pueden mencionarse el tráfico de estupefacientes, la evasión de impuestos y la corrupción"[25]. Asimismo, dichas actividades ilícitas son realizadas no sólo por una persona, como se pueden llevar a cabo otros delitos, sino por un grupo de personas, conocido como delincuencia organizada.

La Ley Federal Contra la Delincuencia Organizada, prevé que existe este tipo de organización "cuando tres o más personas se organicen de hecho para realizar, en forma permanente o reiterada, conductas que por sí o unidas a otras personas, tiene como fin o resultado cometer alguno o algunos de los delitos siguientes"[26] entre ellos dicha ley menciona el terrorismo, acopio y tráfico de armas, tráfico de personas, de órganos, entre otros.

En tal virtud, Callegari refiere que:

---

[24] Zamora Sánchez, Pedro: *loc. cit.,* Ferrusquía Canchola, Manuel, *El sistema jurídico en lavado de dinero,* México, Flores Editor y Distribución, 2013, p. 6.
[25] Zamora Sánchez, Pedro, *Marco jurídico del lavado de dinero,* México, Oxford, 2000, p. 2.
[26] Artículo 2, de la Ley Federal Contra la Delincuencia Organizada, fecha de consulta: 02 de abril de 2019 de *http://www.diputados.gob.mx/LeyesBiblio/pdf/101_070417.pdf*.

> Aunque no haya un concepto definido de criminalidad organizada su vinculación con el delito de blanqueo de capitales es estrecha, pues las características de este delito requieren algunos requisitos que son identificables con la estructura de las organizaciones criminosas. Algunos de los delitos previos en los cuales provienen los bienes objeto de blanqueo ya requieren, por su estructura, una organización para su comisión.[27]

Y si bien ya se mencionó, aquellos recursos ilícitos, son obtenidos de actividades ilícitas, la delincuencia organizada es quien las lleva a cabo, por ello, reiterando lo que refiere el autor, la delincuencia organizada y el lavado de dinero guardan una estrecha relación, ya que es necesaria la existencia del primero para poder iniciar el segundo delito.

1.3.1.- ETAPAS DEL LAVADO DE DINERO.

Para que se pueda dar la comisión de algún delito, los sujetos activos necesitan seguir una serie de etapas para realizar su cometido, aunque en algunos delitos pueden ser las etapas más visibles que en otros, en la especie, "el lavado de dinero se realiza en tres etapas: colocación del dinero, distribución del dinero e integración del dinero"[28], a través de estas tres etapas, el sujeto infractor puede cometer el delito de lavado de dinero.

Sin embargo, dichas etapas pueden ir variando al paso de los años, como resultado de "la avanzada tecnología en lo que se refiere a sistemas de información en una economía globalizada como la que vivimos ha facilitado el acceso a nuevos y más complejos mecanismos o modalidades de lavado de dinero, lo que ha hecho más difícil la identificación estructural de la operación de lavado o de sus etapas"[29], pese a ello, las evoluciones que puedan tener las etapas correspondientes al lavado

---

[27] Callegari, André Luis, *Lavado de dinero, blanqueo de capitales. Una perspectiva entre los Derechos Mexicano, Español y Brasileño,* México, Flores Editor y Distribuidor, S.A. de C.V., 2010, p. 18.
[28] Zamora Sánchez, Pedro, *op. cit.,* p. 3.
[29] Orozco-Felgueres Loya, Carlos, *Efectos fiscales en materia de lavado de dinero,* 3a. ed., México, Thomson Reuters, 2015, p. 84.

de dinero, los fines de éstas seguirán siendo los mismos, aun cuando cambien un poco la forma de llevarse a cabo o se agreguen otras etapas.

Dichas etapas también pueden variar de forma doctrinaria, un claro ejemplo es el que maneja el autor Orozco-Felgueres en su obra, toda vez que este incluye una cuarta etapa, como se aprecia a continuación:

> Las etapas básicas del lavado de dinero y activos son las siguientes:
>
> **a)** Producto de los actos ilícitos: Obtención de dinero en efectivo o medios de pago en desarrollo y sus consecuentes actividades ilícitas (venta de productos o prestación de servicios ilícitos).
>
> **b)** Destino del producto: Colocación o incorporación del producto ilícito en el sistema financiero o no financiero de la economía local o internacional.
>
> **c)** Dispersión del producto: Mediante la estratificación, diversificación o transformación, el dinero o los bienes introducidos en una entidad financiera o no financiera se estructuran en sucesivas operaciones para ocultar, invertir, transformar, asegurar o dar en custodia bienes provenientes del delito, o bien se mezclan con dinero de origen legal, con el propósito de disimular su origen ilícito y alejarlo de su verdadera fuente.
>
> **d)** Reintegración del producto en propiedad o en derechos: Mediante la inversión o goce de los capitales ilícitos, éstos regresan al sistema financiero o no financiero, disfrazados como dinero legítimo.[30]

De las etapas anteriores se puede apreciar que dicho autor también toma en cuenta, independientemente de las etapas posteriores, la que da origen al lavado de dinero, es decir, los delitos previos de los cuales derivaron los recursos ilícitos, y no sólo comienza con la primera que corresponde a la colocación del dinero; estando de acuerdo con dicho autor, ya que, si bien es cierto, el lavado de dinero puede comenzar al colocarse los recursos ilícitos, también es cierto que los delitos previos también forman parte de este delito, ya que sin ellos, simplemente no existiría el delito de operaciones con recursos de procedencia ilícita.

Visto lo anterior, se describirán las etapas que componen el delito de operaciones con recursos de procedencia ilícita.

---

[30] *Ídem.*

1.- Colocación de los recursos ilícitos.

Una vez que se llevó a cabo la comisión del delito del que derivaron los recursos de procedencia ilícita, lo que procede es colocar estos recursos en el Sistema Financiero Mexicano, "según la doctrina ésta es la fase en que los delincuentes procuran desembarazarse materialmente de las importantes sumas en efectivo que generan sus actividades ilícitas"[31], es decir, no quedarse con esos recursos, ya que esto traería como consecuencia ser descubiertos, al no poder acreditar el origen real de la cantidad de dinero que tienen a su disposición, pues el verdadero origen deriva de la comisión de un delito.

Sin embargo, al ser grandes cantidades de dinero, los delincuentes corren más peligro de ser descubiertos en la colocación del dinero en el Sistema Financiero, tal y cómo refiere Zamora:

> El problema para los delincuentes radica en que el ingreso al sistema financiero de montos significativos de efectivo en billetes de baja denominación, es fácilmente detectable por las autoridades.
>
> Por tal motivo, la colocación del dinero se realiza frecuentemente por medio de la creación de empresas de papel, sociedades pantalla o entidades fantasma. Este método no crea otra etapa en el proceso de lavado de dinero; sólo pretende encubrir y disimular el origen de los activos, ligándolos con empresas legítimas para desvincularlos de las actividades ilícitas.[32]

Como bien lo refiere este autor, la creación de dichas sociedades, sirven como medio de ocultamiento, es decir, hacen creer que el dinero es resultado de las actividades realizadas en estas empresas constituidas de manera legítima, y así dicha colocación es más difícil de ser detectada por las autoridades.

2.- Distribución de los recursos ilícitos.

La siguiente etapa es la distribución del dinero, la cual consiste en llevar a cabo "la transferencia de éste a distintas cuentas o instituciones para apartar el dinero de su fuente original"[33], con ello lograr romper el vínculo que existe entre los

[31] Vidales Rodríguez: *loc. cit.,* Callegari, André Luis, *op. cit.,* pp. 30-31.
[32] Zamora Sánchez, Pedro, *op. cit.*, p. 12.
[33] *Ibídem,* p. 3.

sujetos activos y el dinero que es fruto de una actividad ilícita, sin embargo, estas transferencias deben tener un alto grado de complejidad ya que "la forma compleja en que las transacciones son encadenadas, entremezcladas y superpuestas tienen como finalidad hacer extremadamente difícil su detección para las autoridades".[34]. Dichas transferencias como ya bien se mencionó, pueden ser desde diferentes cuentas abiertas en diferentes países, donde dichas transferencias deben hacerse de manera sigilosa y rápida, para no dejar huella de las operaciones realizadas por los delincuentes.

Otra de las maneras en las que se puede conocer a esta etapa es por el nombre de "estratificación", como bien lo refiere García en el artículo de la revista Forbes:

> **Estratificación:** Es la separación de fondos ilícitos de su fuente mediante una serie de transacciones financieras sofisticadas, cuyo fin es desdibujar la transacción original. Esta etapa supone la conversión de los fondos procedentes de actividades ilícitas a otra forma y crear esquemas complejos de transacciones financieras para disimular el rastro documentado, la fuente y la propiedad de los fondos.[35]

Como bien se ha visto y a pesar de que el nombre de esta etapa puede cambiar dependiendo del autor que se consulte, su sentido es el mismo, toda vez que la finalidad de la misma es llevar a cabo la transacción o transferencia de los recursos ilícitos en diversas cuentas bancarias, tanto nacionales como extranjeras, dando un paso más para concluir el delito de operaciones con recursos de procedencia ilícita.

3.- Integración de los recursos ilícitos.

Esta es la última etapa para concluir el delito de lavado de dinero la cual "consiste en la introducción del dinero en el mercado formal –bancario, de bienes raíces, financiero, bursátil, etc – como si fuera total y absolutamente legítimo."[36].

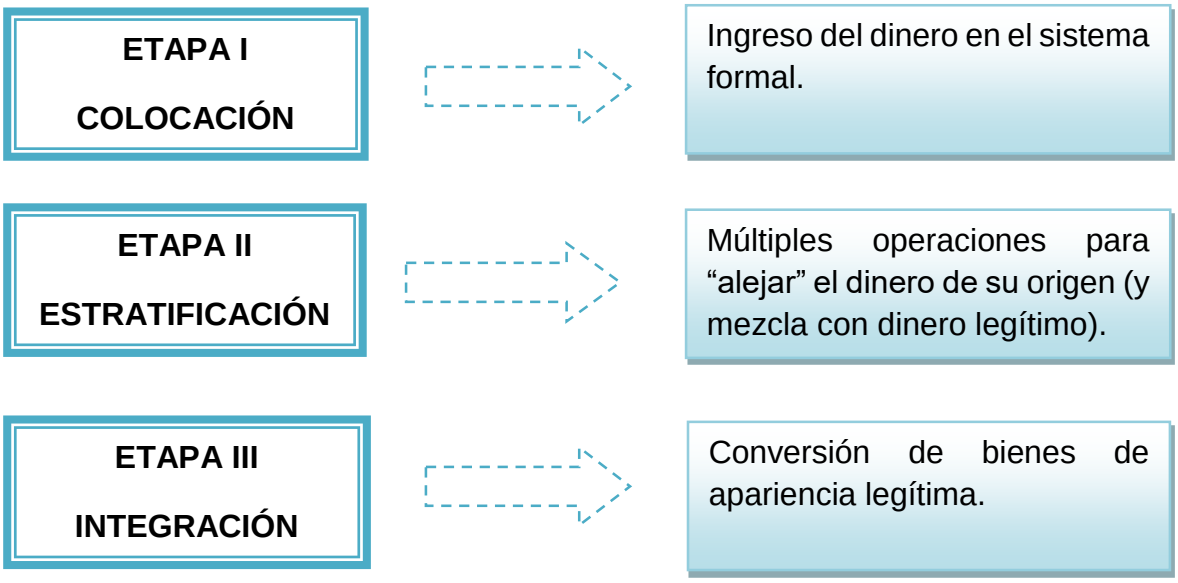
---

[34] Callegari, André Luis, *op. cit.,* p. 39.
[35] García Gibson, Ramón, "Las 3 etapas del lavado de dinero", *Forbes México,* fecha de consulta: 02 de abril de 2019, *https://www.forbes.com.mx/las-3-etapas-del-lavado-de-dinero/.*
[36] Guillermo, Jorge *et al.,* (coord.), *op. cit.,* p. 21.

Con ello, se logra que dichos recursos sean oficialmente lícitos y así los sujetos activos queden deslindados de su verdadero origen, toda vez que al ser ya recursos lícitos, dichos delincuentes pueden demostrar que el origen del dinero que se encuentra en su poder, proviene de actividades igualmente lícitas. Asimismo, "cuando se llega a este estadio (sic), es muy difícil la detección del origen ilícito de los fondos. A menos que se haya podido seguir su rastro a través de las etapas anteriores, resultará muy difícil distinguir los capitales de origen ilegal de los de origen legal"[37], cumpliéndose así el delito de lavado de dinero y con ello, llevar nuevamente a cabo las etapas de este delito.

Después de haber visto cada etapa de manera amplia, sirve de apoyo el diagrama siguiente:

DIAGRAMA 1: EL PROCESO DE LAVADO DE ACTIVOS EN NEGOCIOS ILÍCITOS QUE GENERAN GRANDES CANTIDADES DE DINERO EN EFECTIVO.



*Fuente: Diagrama tomado de Guillermo, Jorge *et al.,* (coord.), *op. cit.,* p. 21.

[37] Callegari, André Luis, *op. cit.,* p. 42.

Con el diagrama anterior, los lectores pueden tener una mejor apreciación del desarrollo del delito de lavado de dinero, toda vez que manera concisa y concreta se da una explicación de dicho desarrollo.

1.3.2.- CARACTERÍSTICAS DEL LAVADO DE DINERO.

Este tipo de delitos tiene ciertas características como son las que se muestran en el cuadro siguiente:

CUADRO 3.- CARACTERÍSTICAS DEL DELITO DE OPERACIONES CON RECURSOS DE PROCEDENCIA ILÍCITA.

1.- INTERNACIONALIZACIÓN DE LAS ACTIVIDADES DE BLANQUEO.	La doctrina señala que una de las características del fenómeno del blanqueo de capitales es su internacionalidad, pues sobrepasa las fronteras nacionales de los Estados e implica su desarrollo en otros.
2.- PROFESIONALIZACIÓN DEL TRABAJO.	La doctrina señala que la organización criminal es una entidad colectiva ordenada en función de estrictos criterios de racionalidad. Sería como piezas que se integran en una sólida estructura en que cada uno de sus miembros desempeña un determinado cometido para el que se encuentra especialmente capacitado en función de sus aptitudes.
3.- VOCACIÓN DE PERMANENCIA.	En la comisión del blanqueo generalmente actúan organizaciones criminales y, a diferencia de la concepción tradicional del delito, la infracción criminal cometida por las organizaciones criminales no se agota en sí misma, pues es despojada de esa autonomía para pasar a ser un elemento más de un programa preestablecido que se prolonga indefinidamente en el tiempo.
4.- COMPLEXIDAD O VARIEDAD DE LOS MÉTODOS EMPLEADOS.	De acuerdo con la doctrina, una de las características principales es de los blanqueadores en su facilidad de adaptación a las nuevas situaciones y la rapidez en el desarrollo de nuevos métodos, lo que permite alcanzar en ocasiones un

	grado muy alto de sofisticación en las operaciones realizadas.
5.- VOLUMEN DEL FENÓMENO.	Para un sector de la doctrina el volumen de capitales de origen delictivo que es objeto de blanqueo es una de las características de este delito.
6.- CONEXIÓN ENTRE REDES CRIMINALES.	Las organizaciones criminales se estructuran a través de una coordinación y subordinación, o entre familiar y carteles empeñados en ámbitos delictivos de la más diversa índole que se extiende por todo el mundo, lo que favorece el establecimiento de las denominadas "redes corporativas de asociaciones criminales", entre cuyos objetivos se encuentra el de prestar apoyo logístico mutuo.
*Fuente: Cuadro elaboración propia con datos obtenidos de Callegari, André Luis, *op. cit*, pp. 23-29.	

Es de esta manera, que el delito de lavado de dinero, cuenta con características especiales que lo particularizan y con las cuales puede llevarse a cabo dicho delito de manera rápida y fácil, pero sobre todo, lograr la finalidad del lavado de dinero, sin embargo, dichas características no son estáticas, siempre se encuentran en constante cambio, por lo que también provoca que el delito de lavado de dinero mejore y sea más difícil descubrirlo por las autoridades comisionadas para ello.

Como se aprecia en este capítulo, la conducta de *phishing* y el delito de lavado de dinero, tienen características y formas de comisión diferentes, que sin ellas no se podrían concretar. En tal virtud, una vez que se ha tenido un panorama teórico de éstos, se puede dar paso a identificar los ordenamientos normativos en los que se encuentran regulados tanto la conducta de *phishing* como el delito de lavado de dinero y conocer en el ámbito tanto internacional como nacional el manejo de éstos.

CAPÍTULO II.- ORDENAMIENTOS NORMATIVOS QUE REGULAN LA CONDUCTA DE *PHISHING* Y EL DELITO DE OPERACIONES CON RECURSOS DE PROCEDENCIA ILÍCITA.

2.1.- REGULACIÓN DE LA CONDUCTA DE *PHISHING* EN EL ORDENAMIENTO NORMATIVO MEXICANO.

Es indispensable que se tenga en cuenta que la conducta de *phishing* no se encuentra regulada de manera particular en el Código Penal Federal, en específico, dentro del capítulo de los delitos informáticos en su título noveno, capítulo segundo, acceso ilícito a sistemas y equipos de informática, que abarca del artículo 211 Bis 1 al 211 Bis 7, sin embargo, dentro de los artículos 211 Bis 4 y 211 Bis 5, de dicho ordenamiento, se encuentran reguladas ciertas conductas que pueden tener una semejanza con la conducta de *phishing,* donde dichos artículos refieren lo siguiente:

> **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.

En el segundo párrafo de este precepto, en específico, en la parte resaltada del mismo, se puede apreciar una semejanza a la conducta de *phishing*, toda vez que, el robo de información de una persona puede ser respecto al ámbito financiero, es decir, cuentas bancarias o claves bancarias, sin embargo, el sentido de la conducta del *phishing*, se pierde al llevarse a cabo directamente de los sistemas o equipos de los sistemas financieros, ya que, la finalidad de dicha conducta, es que la persona sea quien proporcione de manera directa su información a través de páginas simuladas a las originales y no así como se estipula en dicho precepto.

> **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.[38]

Ahora bien, por lo que hace a este artículo, al igual que el artículo anterior, podría considerarse tener una semejanza con la conducta de *phishing*, sin embargo, cabe precisar que, la única diferencia que existe con el precepto anterior, es la autorización que tienen aquellas personas que acceden a los sistemas o equipos de informática, ya que aquí dichas personas sí deben contar con una autorización para llevar a cabo la conducta tipificada en el artículo citado con antelación.

De los artículos transcritos con antelación se puede apreciar que estas conductas hacen referencia a aquellas personas que conozcan o copien información de los sistemas o equipos informáticos de las instituciones del servicio financiero o que estando autorizadas para acceder a dichos sistemas o equipos, copien la información contenida en éstos. Pero, si bien es cierto, se da una obtención de información contenida en los sistemas o equipos por personas que están o no autorizadas por las instituciones que integran el sistema financiero, no se especifica qué tipo de información se obtiene, ya que puede ser información relacionada con la propia institución o con las personas conocidas como cuentahabientes, provocando una gran laguna en dichos preceptos, también, dichas conductas se llevan a cabo directamente por los sujetos activos, sin tener alguna interacción con las víctimas, por lo que tampoco se concreta el engaño al que hace referencia la conducta de *phishing.*

En tal virtud, a pesar de que las conductas a las que hacen referencia dichos preceptos en un primer momento pueden aparentar tener una semejanza con el *phishing,* no es así, ya que no cubren los requisitos que la conducta de *phishing* necesita para que se concrete.

[38] Artículo 211 Bis 4 y 211 Bis 5, del Código Penal Federal. Lo resaltado es por la autora, toda vez que, se puede apreciar la parte de los artículos donde se puede considerar tener una semejanza con el *phishing.*

Del mismo modo, tampoco se tiene una regulación especial en alguna ley sobre esta conducta ilícita, por lo que de cierta manera, esto provoca cierta incertidumbre respecto a las sanciones que deban tener las personas que lleven a cabo la conducta de *phishing* y en sí, a todo lo que engloba esta conducta.

Aunado a ello, se han propuesto a lo largo de los años, en específico, a partir del año 2011 a la fecha, ciertas iniciativas para la regulación de esta conducta y de otras tantas que se encuentran dentro del catálogo de delitos informáticos, una de ellas se llevó a cabo en el año de 2011, por los diputados Juan José Guerra Abud y Rodrigo Pérez Alonso González, del Grupo Parlamentario del Partido Verde Ecologista de México, a la cual le denominaron "Iniciativa con proyecto de decreto por el que se reforman y adicionan diversas disposiciones al Código Penal Federal, en Materia de Delitos en contra de medios o sistemas Informáticos o cometidos mediante el uso o empleo de los mismos", en dicha iniciativa se propuso lo siguiente:

> (…) tipificar conductas para tutelar bienes jurídicos que actualmente no gozan de la protección del derecho, por lo que se encuentran expuestos a los ataques de individuos que aprovechando los vacíos legales y por ende, los espacios de impunidad que éstos generan, atentan y lesionan con métodos y mecanismos hasta hace poco desconocidos ya que derivan de los avances tecnológicos en que se han visto envueltas las sociedades y comunidades de todo el orbe, según puede apreciarse en la siguiente (…)[39]

En el apartado correspondiente a la argumentación de esta iniciativa se establece que al haber un constante avance respecto al tema de las tecnologías, esto:

> (…) obliga a definir nuevos esquemas y revisar la legislación en materia penal con el fin de reflejar los cambios derivados de este nuevo mecanismo de interacción y comunicación, promoviendo esquemas adecuados y acordes con el uso de las TIC y el acceso digital. Si bien ya existen en la legislación actual disposiciones en materia de delitos informáticos, los vertiginosos avances tecnológicos obligan a actualizar el catálogo de delitos en materia del uso de las tecnologías de la información y comunicaciones.[40]

[39] *Gaceta Parlamentaria,* año XV, número 3401-V, martes 29 de noviembre de 2011, consultada el 05 de abril de 2019, *http://gaceta.diputados.gob.mx/Gaceta/61/2011/nov/20111129-V.html*.
[40] *Ídem.*

Con esta iniciativa se demuestra que no solo basta con que las conductas ilícitas referentes al catálogo de los delitos informáticos estén previstas en un ordenamiento normativo, sino que también se deben modificar conforme el paso del tiempo, y así evitar los vacíos legales que hoy en día existen en muchos de los ordenamientos, respecto de los delitos informáticos.

Respecto a la conducta ilícita que nos ocupa, en dicha iniciativa se propuso reformar el artículo 211 Bis 1, el resultado quedaría de la manera siguiente:

> **Capítulo 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.
>
> **Se aplicará una pena de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa al que sin autorización acceda, modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática que no estén protegidos por algún mecanismo de seguridad o también sin autorización acceda a dichos sistemas o equipos de informática o mediante cualquier mecanismo que de manera próxima o remota les cause un daño.**
>
> **En los casos en que el daño provocado por el acceso o la modificación no autorizados obstaculice o disminuya la capacidad de funcionamiento del sistema o equipo informático las penas previstas en los párrafos anteriores se incrementarán hasta en dos terceras partes.**
>
> 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 **seis** meses a **dos años** de prisión y **de cien a trescientos** días multa.
>
> **La pena aplicable será de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa al que sin autorización conozca o copie información contenida en sistemas o equipos de informática no protegidos por algún mecanismo de seguridad.**[41]

En la especie, a pesar de que en dicha iniciativa, no se agregó un apartado específico respecto a la conducta *phishing,* para que dejara de ser considerada

[41] *Ídem.*

como una conducta ilícita y fuera considera como delito, sí se agregó un apartado a dicho precepto normativo referente a esta conducta, ubicado en su último párrafo, donde establece una pena a aquellas personas que copien información contenida en sistemas o equipos de informática, los cuales no deben estar protegidos por algún tipo de mecanismos de seguridad, sin embargo, aunado a ello, aún con dicha iniciativa no queda del todo concretada la regulación que el *phishing* requiere.

A partir de dicha iniciativa a la fecha, se han planteado otras más, como la propuesta en el año 2013, por el diputado Felipe Arturo Camarena García, integrante del Grupo Parlamentario del Partido Verde Ecologista de México de la LXII Legislatura del H. Congreso de la Unión, la cual retomó el mismo sentido que la iniciativa anterior, es decir, enfocarse en regular los delitos informáticos en el Código Penal Federal; así como en el año 2015, la propuesta emitida por los Senadores del Grupo Parlamentario del Partido Revolucionario Institucional, a través de la cual, se solicita a la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros y a la División Científica de la Comisión Nacional de Seguridad a implementar una campaña preventiva en contra del *phishing.*

Asimismo, otras iniciativas que van de la mano con la conducta de *phishing,* son las correspondientes al robo de identidad, ya que, de cierta manera, al llevar a cabo el *phishing,* se está dando un robo de identidad.

Principalmente fueron tres iniciativas referentes al robo de identidad, la primera de ellas y una de las más apegadas a la conducta de *phishing,* se dio en el año 2011, por la diputada Adriana Sarur Torre, del Grupo Parlamentario del Partido Verde Ecologista de México, a través de la cual se proponía adicionar diversos artículos que regularían el robo de identidad, más en específico, “busca reformar la denominación del capítulo IV del título vigésimo segundo, para crear el tipo penal de “usurpación de identidad”, con ello se busca sancionar **a quienes lleven a cabo a través de medios electrónicos o tecnológicos o personales el apoderamiento, o se haga pasar, o utilice, o usurpe o sustituya la identidad de**

otra persona."[42], por ello, es una de las iniciativas que más se relaciona a la conducta de *phishing,* toda vez que, se da un robo de identidad a través de medios tecnológicos.

La segunda iniciativa se llevó a cabo en el año 2015, por el diputado César Flores Sosa, del Grupo Parlamentario del Partido Acción Nacional, en la cual se pretendía adicionar un capítulo correspondiente al robo de identidad, quedando la iniciativa de la siguiente manera:

> **Decreto que adiciona el capítulo VII al título vigésimo segundo del libro segundo y el artículo 399 Ter al Código Penal Federal**
>
> **Único.** Se adicionan el capítulo VII al título vigésimo segundo del libro segundo y el artículo 399 Ter al Código Penal Federal, en los términos siguientes:
>
> **Capítulo VII**
> **De la Usurpación de Identidad**
>
> **Artículo 399 Ter. Comete el delito de usurpación de identidad al que por sí o por interpósita persona, usando cualquier medio lícito o ilícito, se apodere, apropie, transfiera, utilice, suplante o disponga de datos personales sin autorización de su titular, con fines ilícitos en perjuicio de este.**
>
> **Se impondrá una pena de cinco a diez años de prisión y multa de 900 a 1,200 días de salario mínimo y, en su caso, la reparación del daño que se hubiera causado, a quien cometa el delito de usurpación de personalidad.**
>
> **Las penas previstas en el párrafo anterior se aumentarán hasta en una mitad además de inhabilitación o suspensión para ejercer la profesión o cargo por un tiempo igual a la pena de prisión, cuando el ilícito sea cometido por un servidor público aprovechándose de sus funciones, por un trabajador del sistema bancario o por quién se valga de su profesión y/o estudios para ello.[43]**

[42] *Gaceta Parlamentaria*, año XIV, número 3223-II, jueves 17 de marzo de 2011, consultada el día 13 de mayo de 2019, *http://gaceta.diputados.gob.mx/Gaceta/61/2011/mar/20110317-II.html#Iniciativa6.* Lo resaltado es de origen.
[43] Gaceta Parlamentaria, año XIX, número 4407-IV, miércoles 18 de noviembre de 2015, consultado el día 13 de mayo de 2019, *http://gaceta.diputados.gob.mx/Gaceta/63/2015/nov/20151118-IV.html.* Lo resaltado es de origen.

Si bien, a pesar de que no se menciona de manera específica que los medios para llevar a cabo el robo de identidad pueden ser los medios informáticos, como en la iniciativa anterior, implícitamente va inmerso en el mismo.

La tercera iniciativa, se propuso en el año 2016, por la senadora Martha Angélica Tagle Martínez, integrante de la LXIII Legislatura del Congreso de la Unión, a través de la cual se pretendía adicionar un artículo al Código Penal Federal, para tipificar el robo de identidad, quedando de la siguiente manera:

> **Decreto que reforma el Código Penal Federal**
>
> **Artículo Único.** Se adiciona un Capítulo III, intitulado (sic) "Suplantación de Identidad", al Título Décimo Octavo y el artículo 287 al Código Penal Federal, para quedar como sigue:
>
> **Capítulo III**
> **Suplantación de Identidad**
>
> **Artículo 287 Bis. Comete el delito de suplantación de identidad el que utilizando cualquier medio, se apropie y utilice de manera ilícita datos e información personal que legítimamente pertenezcan a otra persona, ya sea con consentimiento o sin consentimiento de ella, obteniendo un lucro o beneficio indebido de otra naturaleza para sí o para otro, ocasionando daño moral o patrimonial, se le impondrá una pena de dos a seis años de prisión y de quinientos a setecientos días del Valor diario de la Unidad de Medida y Actualización.**
>
> **Se aumentará en una mitad las penas previstas en el párrafo anterior, a quien se valga de la homonimia, parecido físico o cuando el ilícito sea cometido por un servidor público provechándose de sus funciones, o por quien sin serlo, se valga de su profesión, confianza o empleo para ello.**
>
> **Las penas previstas en el presente artículo se impondrán sin perjuicio de las que correspondan por los delitos que resulten, aplicándose las reglas del concurso real.**[44]

En dicha iniciativa, tampoco se especifica cuáles serán los medio por los cuales se obtendría la información de las personas, para llevar a cabo la usurpación de identidad, sin embargo, como en la primera iniciativa, va implícitamente que pueden ser utilizados medios tecnológicos para ello, otra de las propuestas que las

[44] *Gaceta Parlamentaria*, año XIX, número 4441-II, jueves 7 de enero de 2016, consultada el día 13 de mayo de 2019, *http://gaceta.diputados.gob.mx/Gaceta/63/2016/ene/20160107-II.html*. Lo resaltado es de origen.

iniciativas anteriores no tienen es la referente al consentimiento de dichas personas afectadas, ya que puede haber o no consentimiento, creando una semejanza con el *phishing,* ya que no se necesita del consentimiento de las personas para obtener dicha información personal.

Pese a todo, como se puede apreciar en los preceptos correspondientes en el Código Penal Federal vigente, ninguna de ellas prosperó, por lo que, aún los legisladores no logran apreciar la gran laguna que existe respecto de los delitos informáticos hoy en día.

Por otra parte, el 19 de marzo del presente año, la senadora Jesús Lucia Trasviña Waldenrath, Senadora de la República en la LXIV Legislatura e integrante del Grupo Parlamentario del Movimiento Regeneración Nacional (MORENA), propuso una iniciativa con Proyecto de Decreto por el que se reforman y derogan diversas disposiciones del Título Noveno, Libro Segundo del Código Penal Federal y se expide la Ley de Seguridad Informática, en tal virtud, lo que resalta la atención es la expedición de dicha Ley.

En efecto, una de las muchas preguntas que surgen a partir de esta iniciativa es la correspondiente a, ¿qué es la Ley de Seguridad Informática?, para ello, el periodista Riquelme, en el artículo del periódico *El Economista,* refiere que, con esta Ley se pretende que "se agrupe a estos delitos informáticos y en la que se contempla la creación de una Agencia Nacional de Seguridad Informática (ANSI), adscrita a la Secretaría de Seguridad y Protección Ciudadana"[45]; con dicha propuesta a grandes rasgos se puede apreciar la creación de una Ley especial para dichos delitos informáticos y con ello, revertir las lagunas que se encuentran en el Código Penal Federal, si bien, al ser una iniciativa, basta de sobra decir que se debe llevar todo el proceso legislativo correspondiente para poder saber si dicha propuesta de Ley, llegará a regular todas las inconsistencias correspondientes a los

[45] Riquelme, Rodrigo, "¿Qué es la Ley de Seguridad Informática propuesta por Morena?, *El Economista,* fecha de consulta: 07 de mayo de 2019, *https://www.eleconomista.com.mx/tecnologia/Que-es-la-Ley-de-Seguridad-Informatica-propuesta-por-Morena-20190402-0053.html.*

delitos informáticos que existen hoy en día, por lo que, sólo queda esperar el resultado al que lleguen los legisladores.

2.2.- REGULACIÓN DEL *PHISHING* EN EL ORDENAMIENTO NORMATIVO INTERNACIONAL.

Al existir una evolución inminente de la tecnología, es claro que simultáneamente los delitos informáticos tendrán la misma evolución, en la especie, la conducta de *phishing*, tendrá una regulación normativa a nivel internacional, sin embargo, como es en el caso de México, hay algunos países que tampoco cuentan con dicha regulación, por ello, son muy pocos los países a nivel mundial que tipifican esta conducta como delito en sus diferentes marcos normativos.

En tal virtud, y como se ha mencionado con antelación, la regulación de la conducta de *phishing* es muy escasa y muchas veces, no viene como tal en los ordenamientos normativos, es decir, no viene con el nombre de dicha conducta, sin embargo, los legisladores de esos países la consideran como *phishing* por las características que tiene en el marco normativo.

Un primer ejemplo de ello, es el Código Penal Español, tal y como lo refiere Estévez, "los delitos informáticos no están contemplados como un tipo especial de delito en la legislación española"[46], en tanto, en el caso del *phishing*, este se encuentra contemplado como una estafa informática, tal y como se establece en el artículo 248, punto dos, incisos a) y b), del Código Penal Español, que a la letra refieren:

> **Artículo 248.**
>
> (…)
>
> 2. También se consideran reos de estafa:

[46] Estévez Martín, Sonia, "Delitos informáticos", 2010, p. 40, fecha de consulta: 05 de mayo de 2019, *http://gpd.sip.ucm.es/sonia/docencia/master1011/delito.pdf.*

> a) Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.
>
> b) Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo.

Como se menciona en dicho precepto, el *phishing* es equiparado con una estafa, y si nos vamos al significado de la palabra, se pude encontrar que una estafa es el "delito consistente en provocar un perjuicio patrimonial a alguien mediante engaño y con ánimo de lucro"[47], con dicho concepto, se puede apreciar que, sí se puede considerar una estafa respecto a la comisión de la conducta de *phishing,* toda vez que, se causa un daño patrimonial mediante un engaño a la persona estafada, siempre que, y es ahí cuando se concreta dicha conducta, se utilice algún tipo de manipulación o programa informático.

En la misma vertiente se encuentra el Código Penal Argentino, a través del cual a partir del 2008, por medio de la Ley 26.388, en su artículo 9, se estipuló agregar el inciso 16, al artículo 173, de dicho Código, siendo considerando el *phishing* como un tipo de estafa, dándole el sentido de ser un delito informático, al utilizar la informática para dicha comisión, tal y como se establece a continuación:

> ARTICULO 173.- Sin perjuicio de la disposición general del artículo precedente, se considerarán casos especiales de defraudación y sufrirán la pena que él establece:
>
> (…)
>
> 16. El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos. (Inciso incorporado por art. 9° de la Ley N° 26.388, B.O. 25/6/2008).

Como sucede también en la legislación española, se considera un caso especial de estafa, toda vez que, para poder ser considerado como *phishing,* se

[47] Real Academia Española, fecha de consulta: 05 de mayo de 2019, *https://dle.rae.es/?id=Gk0Xp1o|Gk1qslk.*

tuvo que hacer uso de sistemas informáticos, a través de los cuales se pudiera dar el robo de información de las personas defraudadas.

El Código Penal de Colombia es otro de los ordenamientos normativos que incluye el delito de *phishing* en su apartado de delitos informáticos, más en específico, en el capítulo I, "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos", de dicho Código Penal, en el artículo 269 G, que a la letra refiere:

> **Artículo 269 G Suplantación de sitios web para capturar datos personales**. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.
>
> En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.
>
> La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.[48]

En este artículo se establece que se va a dar una sustitución de sitios *web* para que las personas que utilicen dichas páginas, ingresen sus datos personales y a partir de ello, se dé el robo de dicha información, cumpliendo con ello la finalidad del *phishing.*

Cómo se mencionó con antelación, estos son de los pocos países donde se encuentra tipificado el *phishing,* o mejor dicho, de los países donde la tipificación es más parecida a dicha conducta.

[48] Fecha de consulta: 14 de mayo de 2019, *http://perso.unifr.ch/derechopenal/assets/files/legislacion/l_20160208_02.pdf.* Lo resaltado es de origen.

Por último, a nivel internacional se encuentra el Convenio sobre Ciberdelincuencia, mejor conocido como Convenio de Budapest, su creación tiene como objetivo:

> (…) prevenir los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos, garantizando la tipificación como delito de dichos actos, tal y como se define en el presente Convenio, y la asunción de poderes suficientes para luchar eficazmente contra dichos delitos, facilitando su detección, investigación y sanción, tanto a nivel nacional como internacional, y estableciendo disposiciones materiales que permitan una cooperación internacional rápida y fiable; (…)[49]

Dicho convenio fue creado por el Consejo Europeo, sin embargo, aun cuando "(…) fue creado en el seno de una institución europea, está abierto para que otros estados puedan adherirse. Actualmente, hay 56 estados parte que provienen de los cinco continentes (…)[50].

Con este, se pretende que los países parte, en sus respectivas legislaciones, adopten las medidas necesarias para la regulación y sanción de los delitos informáticos; en lo particular, dicho convenio, en el título 2, delitos informáticos, en los artículos 7 y 8, que tratan sobre la falsificación informática y el fraude informático, es donde se encuentran las medidas que los Estados parte deben adoptar en sus legislaciones para poder llevar a cabo la tipificación de los delitos que sean referentes a las conductas que están establecidas en dichos artículos, las cuales, son lo más parecido a la conducta de *phishing.*

[49] "Convenio sobre ciberdelincuencia", Budapest, 2001, fecha de consulta: 14 de mayo de 2019, *https://www.oas.org/juridico/english/cyb_pry_convenio.pdf.*

[50] Asociación por los Derechos Civiles, "La convención de cibercrimen de Budapest y América Latina. Breve guía acerca de su impacto en los derechos y garantías de las personas", 2018, volumen I, pág. 8, fecha de consulta: 14 de mayo de 2019, *https://adcdigital.org.ar/wp-content/uploads/2018/03/Convencion-Budapest-y-America-Latina.pdf.*

2.3.- REGULACIÓN DEL DELITO DE OPERACIONES CON RECURSOS DE PROCEDENCIA ILÍCITA EN EL ORDENAMIENTO NORMATIVO MEXICANO.

El delito de operaciones con recursos de procedencia ilícita ha estado regulado en varios ordenamientos normativos, dicha regulación comenzó desde el año de 1990 en el Código Fiscal de la Federación, en el artículo 115 Bis, siendo catalogado como un delito fiscal, sin embargo, el 13 de mayo de 1996, se emitió un "acuerdo por el que se reforman, adicionan y derogan diversos artículos del Código Penal para el Distrito Federal en Materia de Fuero Común y para toda la República en materia de Fuero Federal, del Código Fiscal de la Federación (…)" y es ahí donde dejó de ser un delito fiscal al ya no encontrarse regulado en el Código Fiscal de la Federación y se empieza a regular en el artículo 400 bis, del actual Código Penal Federal, hasta la fecha; en tanto, en el año 2012, se expidió la Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita, encontrándose ya este delito regulado en lo general y en lo particular, es decir, en el Código Penal Federal y en su Ley especial, mencionada con antelación.

Pero, a pesar de que el lavado de dinero se regula principalmente en estos dos ordenamientos normativos, cabe precisar que también se encuentra en otros, como lo son la Ley General de Organizaciones y Actividades Auxiliares de Crédito, la Ley de Instituciones de Crédito, la Ley del Mercado de Valores, la Ley de Fondos de Inversión (antes Ley de Sociedades de Inversión) y la Ley de Instituciones de Seguros y de Fianzas; en cada una de estas leyes se establece que las instituciones respectivas deben llevar a cabo medidas y procedimientos para prevenir y detectar las actividades que puedan originar el delito de operaciones con recursos de procedencia ilícita.

Respecto de lo anterior, como ya se comentó, el delito de lavado de dinero se encuentra tipificado en el Código Penal Federal, en el artículo 400 bis, que a la letra refiere:

> Artículo 400 Bis. Se impondrá de cinco a quince años de prisión y de mil a cinco mil días multa al que, por sí o por interpósita persona realice cualquiera de las siguientes conductas:

> I. Adquiera, enajene, administre, custodie, posea, cambie, convierta, deposite, retire, dé o reciba por cualquier motivo, invierta, traspase, transporte o transfiera, dentro del territorio nacional, de éste hacia el extranjero o a la inversa, recursos, derechos o bienes de cualquier naturaleza, cuando tenga conocimiento de que proceden o representan el producto de una actividad ilícita, o
>
> II. Oculte, encubra o pretenda ocultar o encubrir la naturaleza, origen, ubicación, destino, movimiento, propiedad o titularidad de recursos, derechos o bienes, cuando tenga conocimiento de que proceden o representan el producto de una actividad ilícita.
>
> (…)

En dicho precepto se establecen las acciones que pueden traer consigo la comisión del delito de lavado de dinero, así como las sanciones correspondientes a la comisión de este delito. Por lo que, el delito de lavado de dinero requería una regulación más específica, toda vez que en el Código Penal Federal, sólo se establecen las acciones por las que se puede dar la comisión del delito de lavado de dinero, así como sus sanciones, por ello, se expidió la Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita, la cual está compuesta por 65 artículos, donde la finalidad de la creación de esta ley es la que se establece en el artículo 2, que a la letra refiere:

> **Artículo 2.** El objeto de esta Ley es proteger el sistema financiero y la economía nacional, estableciendo medidas y procedimientos para prevenir y detectar actos u operaciones que involucren recursos de procedencia ilícita, a través de una coordinación interinstitucional, que tenga como fines recabar elementos útiles para investigar y perseguir los delitos de operaciones con recursos de procedencia ilícita, los relacionados con estos últimos, las estructuras financieras de las organizaciones delictivas y evitar el uso de los recursos para su financiamiento.

Como bien establece este artículo, la finalidad de la creación de dicha ley es la prevención de dicho delito, a través de actividades de investigación, asimismo, la recolección de elementos que puedan comprobar que se está cometiendo el delito de lavado de dinero, para que posteriormente puedan ser sancionadas aquellas personas involucradas en su comisión.

Ahora bien, el órgano encargado de vigilar y llevar a cabo lo establecido tanto en la ley como en el reglamento, es la Secretaría de Hacienda y Crédito Público, la

cual goza de ciertas facultades, tal y como lo establece el artículo 5, de la ley en comento, entre ellas está el recibir los avisos correspondientes a las Actividades Vulnerables, realizar las denuncias respectivas ante el Ministerio Público cuando detecte aquellas actividades que puedan generar algún delito, requerir toda aquella información y documentación que puedan servir para el ejercicio de sus facultades.

Asimismo, otra de las autoridades relacionadas con este delito es la Procuraduría General de la República, hoy Fiscalía General de la República, la cual cuenta con la Unidad Especializada en Análisis Financiero, y como lo establece el artículo 7 de dicha ley, “es el órgano especializado en análisis financiero y contable relacionado con operaciones con recursos de procedencia ilícita”.

En otro de los apartados de la ley, se establece un listado correspondiente a aquellas actividades que se consideran como vulnerables, es decir, aquellas a través de las cuales se puede llevar a cabo el delito de operaciones con recursos de procedencia ilícita, por ser actividades donde su seguridad jurídica tiene mayor riesgo, entre ellas se encuentran las que estén relacionadas con los juegos de apuesta, concursos o sorteos, la emisión o comercialización de tarjetas de servicio, de crédito, de todas aquellas que se utilicen como instrumento de almacenamiento de valor monetario, el ofrecimiento de operaciones de mutuo o de garantía, así como de otorgamientos de préstamos o créditos, la prestación de servicios de construcción o desarrollo de bienes inmuebles, por mencionar algunas de ellas.

Derivado de estas actividades ilícitas, las personas que las realicen, deben generar los avisos correspondientes, estos se llevarán a cabo a través de los medios electrónicos y en el formato establecido por la Secretaría de Hacienda y Crédito Público; estos avisos contendrán lo establecido en el artículo 24 de la ley, como son los “datos generales de quien realice la actividad vulnerable, datos generales del cliente, usuarios o del Beneficiario Controlador, y la información sobre su actividad y ocupación, así como la descripción general de la actividad vulnerable sobre la cual se dé aviso”.

Con dichos avisos se pretende evitar que las actividades vulnerables puedan ser un medio para la comisión del lavado de dinero, actuando como una forma de control de la Secretaría de Hacienda y Crédito Público, ante estas actividades. Se debe también tener en cuenta que, al momento de que el Ministerio Público, se encuentre llevando a cabo su investigación y tenga en su resguardo los avisos, este no debe basar la misma solo en los propios avisos, sino que también en todas aquellas pruebas que sustenten las actividades vulnerables.

Otra de las formas por la cual la Secretaría puede controlar las actividades vulnerables es a través de las visitas de verificación, tal y como se encuentra regulado en el capítulo VI de la ley, estas visitas serán de oficio, estando dirigidas a todas aquellas personas que lleven a cabo actividades vulnerables y las cuales no presenten la información requerida, por lo que dichas visitas solo abarcarán lo concerniente a ellas, partiendo desde la fecha en que se esté llevando a cabo a los 5 años anteriores a esa fecha, por lo que las personas se encuentran obligadas a exhibir toda aquella documentación correspondiente a las actividades llevadas a cabo durante ese lapso.

Como bien se establece en la ley en comento, para llevar a cabo el objetivo de la misma, habrá una coordinación institucional, esto es que, la Secretaría de Hacienda y Crédito Público se coordinará con otras instituciones tanto a nivel nacional como internacional, para el intercambio de información que pueda ayudar a corroborar que se ha realizado o no el delito de operaciones con recursos de procedencia ilícita.

Por último, otros de los aspectos que regula la ley es respecto a las sanciones administrativas y los delitos cometidos, por lo que hace a las sanciones, éstas se darán cuando se infrinja dicha ley, por ejemplo, se incumpla con las obligaciones previstas en la misma; en tanto, por lo que hace a los delitos, se van a dar cuando se proporcione de manera dolosa información o documentos que sean falsos, estén alterados o se encuentren ilegibles y que sean anexados a los avisos que se tengan que presentar o que de dicha información sea parte del contenido de los mismos.

La Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita, es uno de los ordenamientos normativos que más importancia tiene respecto al delito de operaciones con recursos de procedencia ilícita, toda vez que en este se encuentran las bases para su investigación en caso que exista la comisión de dicho delito o para prevenir el mismo.

2.4.- REGULACIÓN DEL DELITO EN EL ORDENAMIENTO NORMATIVO INTERNACIONAL.

Como se mencionó en el capítulo anterior, las características del delito de lavado de dinero conllevan a que su marco normativo no sólo se encuentre a nivel nacional, sino que también sea extensivo a nivel internacional, por ello, varios países a lo largo de los años han creado instrumentos necesarios para la prevención y erradicación del delito de lavado de dinero. Para comenzar, uno de los primeros instrumentos fue la Convención de Naciones Unidas contra el Tráfico Ilícito de Estupefacientes y Sustancias Psicotrópicas de 1988, tal y como lo refiere Chavarría:

> Esta convención fue aprobada el 20 de diciembre de 1988, en Viena, Austria, por lo que se le conoce como la "Convención de Viena", ratificada por el gobierno mexicano el 27 de febrero de 1990 y publicada en el Diario Oficial de la Federación el 5 de septiembre de 1990.
>
> Es el primer instrumento internacional que tiene entre sus propósitos combatir el lavado de dinero, aún cuando no utiliza este término, sólo se conceptualiza y lo limita al delito de narcotráfico, en ella se delinearon estrategias novedosas para afectar los recursos económicos de las organizaciones criminales, pretendiendo reducir su capacidad de inversión, operatividad y comercialización.[51]

Como ya se mencionó, en dicha convención no se encuentra regulado el delito de lavado de dinero de manera expresa, pero, sí otros delitos de los cuales pueden generarse recursos obtenidos de manera ilícita, con ello, al estar regulados, se puede lograr la disminución de su comisión.

[51] Silvia Chavarría, Cedillo, "La normatividad internacional en materia de lavado de dinero y su influencia en el sistema jurídico mexicano", p. 58, fecha de consulta: 30 de abril de 2019, *http://revista.ibd.senado.gob.mx/index.php/PluralidadyConsenso/article/download/161/161.*

Otro instrumento relacionado con el delito de lavado de dinero es la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, suscrita en diciembre del 2000, en Palermo, Italia. En esta Convención se encuentra regulada la penalización del blanqueo del producto del delito, dicho de otra manera al delito de lavado de dinero, en el artículo 6, que establece lo siguiente:

> 1. Cada Estado Parte adoptará, de conformidad con los principios fundamentales de su derecho interno, las medidas legislativas y de otra índole que sean necesarias para tipificar como delito, cuando se cometan intencionalmente:
>
> a) i) La conversión o la transferencia de bienes, a sabiendas de que esos bienes son producto del delito, con el propósito de ocultar o disimular el origen ilícito de los bienes o ayudar a cualquier persona involucrada en la comisión del delito determinante a eludir las consecuencias jurídicas de sus actos;
>
> ii) La ocultación o disimulación de la verdadera naturaleza, origen, ubicación, disposición, movimiento o propiedad de bienes o del legítimo derecho a éstos, a sabiendas de que dichos bienes son producto del delito;
>
> b) Con sujeción a los conceptos básicos de su ordenamiento jurídico:
>
> i) La adquisición, posesión o utilización de bienes, a sabiendas, en el momento de su recepción, de que son producto del delito;
>
> ii) La participación en la comisión de cualesquiera de los delitos tipificados con arreglo al presente artículo, así como la asociación y la confabulación para cometerlos, el intento de cometerlos, y la ayuda, la incitación, la facilitación y el asesoramiento en aras de su comisión.

El artículo anterior hace referencia a que todo Estado parte tiene la obligación de utilizar los ordenamientos normativos de dicho país, para sancionar el delito, siempre y cuando se lleven a cabo las actividades descritas en el precepto, las cuales son semejantes a las mencionadas en el artículo 400 Bis, del Código Penal Federal.

También, en dicha Convención en el artículo 7, se establecen las medidas que se deben implementar para combatir el blanqueo de dinero, entre ellas el establecer una reglamentación y supervisión de los bancos e instituciones financieras no bancarias, con la finalidad de prevenir y detectar todo lo concerniente

al lavado de dinero, también la posibilidad que tienen las autoridades relacionadas con el delito, de poder intercambiar información con otras instituciones a nivel tanto nacional como internacional, donde cada una de ellas debe tener una dependencia en la cual se encuentre almacenada esta información, todo ello con el fin de lograr combatir el delito de lavado de dinero.

Otro instrumento normativo internacional es la Declaración de Principios del Comité de Basilea de 1988, con dicha declaración se pretende prevenir la utilización del sistema bancario, como intermediario del delito de lavado de dinero, toda vez que:

> Los bancos y otras instituciones financieras pueden servir involuntariamente de intermediarios para la transferencia o depósito de fondos de origen criminal. Este tipo de operaciones pretenden a menudo ocultar al verdadero propietario de los fondos. Esta utilización del sistema financiero preocupa directamente a la policía y a las autoridades responsables del cumplimiento de la Ley. También es motivo de preocupación para los supervisores bancarios y para los gestores de los bancos dado que la confianza del público en los bancos puede verse minada por la asociación de éstos con delincuentes.
>
> La presente Declaración de Principios pretende señalar un cierto número de reglas y procedimientos cuya puesta en práctica debería ser garantizada por los gestores de los bancos a fin de colaborar en la eliminación de las operaciones de blanqueamiento de dinero por medio del sistema bancario nacional e internacional. La Declaración busca reforzar las mejores prácticas bancarias existentes y, particularmente alentar la vigilancia contra la utilización del sistema de pagos con fines criminales, promover la puesta en marcha de medidas preventivas eficaces y favorecer la cooperación con las autoridades encargadas del cumplimiento de las leyes.[52]

Con dichos principios se crearon medidas de protección para las entidades financieras, derivado de las actividades financieras que realizan, al no tener la suficiente regulación pueden ser objeto de las organizaciones criminales, al depositar los recursos obtenidos de manera ilícita en las cuentas de dichas instituciones y con ello, comenzar la primera etapa del delito de lavado de dinero.

[52] Declaración del comité de autoridades de supervisión bancaria del grupo de los diez y de Luxemburgo, hecha en Basilea en diciembre de 1988, sobre prevención en la utilización del sistema bancario para blanquear fondos de origen criminal, fecha de consulta: 27 de abril de 2019, *http://www.pnsd.mscbs.gob.es/pnsd/legislacion/pdfestatal/i47.pdf.*

Cabe precisar que otro de los instrumentos importantes que existe para combatir el delito de operaciones con recursos de procedencia ilícita, son las Cuarenta Recomendaciones del Grupo de Acción Financiera Internacional, este

> (…) es un organismo intergubernamental cuyo propósito es elaborar y promover medidas para combatir el blanqueo de capitales, proceso consistente en ocultar el origen ilegal de productos de naturaleza criminal. Estas medidas intentan impedir que dichos productos se utilicen en actividades delictivas futuras y que afecten a las actividades económicas lícitas. [53]

Las recomendaciones emitidas se dividen en siete ejes temáticos, los cuales son: Políticas y Coordinación ALA/CFT[54], Lavado de Activos y Decomiso, Financiamiento del Terrorismo y Financiamiento de la Proliferación, Medidas Preventivas, Transparencia y Beneficiario Final de las Personas Jurídicas y Otras Estructuras Jurídicas, Facultades y Responsabilidades de las Autoridades Competentes y Otras Medidas Institucionales y por último, la Cooperación Internacional[55], que a su vez, engloban las 40 recomendaciones, todas ellas dirigidas al delito de lavado de dinero.

Las recomendaciones 3 y 4 hacen referencia al delito de lavado de activos y al decomiso de los recursos, tal y como se transcribe a continuación:

> **3. Delito de lavado de activos**
>
> Los países deben tipificar el lavado de activos en base a la Convención de Viena y la Convención de Palermo. Los países deben aplicar el delito de lavado de activos a todos los delitos graves, con la finalidad de incluir la mayor gama posible de delitos determinantes.
>
> **4. Decomiso y medidas provisionales**
>
> Los países deben adoptar medidas similares a las establecidas en la Convención de Viena, la Convención de Palermo y el Convenio Internacional para la Represión de la Financiación del Terrorismo, incluyendo medidas

[53] Silvia Chavarría, Cedillo, *op. cit.,* pp. 59-60.
[54] Dichas siglas significan “Anti Lavado de Activos y Contra Financiamiento del Terrorismo” en sus siglas en español.”, fecha de consulta: 30 de abril de 2019, *https://www.gafilat.org/index.php/es/gafilat/preguntas-frecuentes.*
[55] “Estándares internacionales sobre la lucha contra el lavado de activos y el financiamiento del terrorismo y la proliferación. las recomendaciones del GAF”, Febrero 2012, fecha de consulta: 30 de abril de 2019, *https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF-40-Rec-2012-Spanish.pdf.*

> legislativas, que permitan a sus autoridades competentes congelar o incautar y decomisar lo siguiente, sin perjuicio de los derechos de terceros de buena fe: (a) bienes lavados, (b) producto de, o instrumentos utilizados en, o destinados al uso en, delitos de lavado de activos o delitos determinantes , (c) bienes que son el producto de, o fueron utilizados en, o que se pretendía utilizar o asignar para ser utilizados en el financiamiento del terrorismo, actos terroristas u organizaciones terroristas, o (d) bienes de valor equivalente.
>
> Estas medidas deben incluir la autoridad para: (a) identificar, rastrear y evaluar bienes que están sujetos a decomiso; (b) ejecutar medidas provisionales, como congelamiento y embargo, para prevenir manejos, transferencias o disposición de dichos bienes; (c) adoptar medidas que impidan o anulen acciones que perjudiquen la capacidad del Estado para congelar o embargar o recuperar los bienes sujetos a decomiso; y (d) tomar las medidas de investigación apropiadas.
>
> Los países deben considerar la adopción de medidas que permitan que tales productos o instrumentos sean decomisados sin que se requiera de una condena penal (decomiso sin condena), o que exijan que el imputado demuestre el origen lícito de los bienes en cuestión que están sujetos a decomiso, en la medida en que este requisito sea compatible con los principios de sus legislaciones nacionales.[56]

En dichos puntos se establece que los países deben tipificar dicho delito siguiendo los lineamientos establecidos en la Convención de Viena y de Palermo, del mismo modo, establece que también estos países deben llevar a cabo las medidas necesarias para el decomiso de todos aquellos recursos o instrumentos que serían utilizados para la comisión del delito, están siendo utilizados o fueron utilizados para los mismos fines. Entre las recomendaciones emitidas por el GAFI, se encuentran aquellas que van dirigidas a la implementación de medidas de protección y regulación de las Instituciones Financieras, retomando temas manejados en la Convención de Palermo, asimismo, también se establece la coordinación internacional entre los países para evitar y combatir el delito de lavado de dinero.

Visto lo anterior, se puede apreciar los diversos ordenamientos normativos a nivel nacional e internacional que regulan el delito de lavado de dinero, y la conducta de *phishing*; en tanto, respecto a la conducta de *phishing*, cabe precisar que a nivel nacional, aún no se cuenta con una regulación de la misma, en tanto, a nivel

[56] *Ídem.*

internacional, hay países en los que el delito de *phishing* lo consideran como un fraude informático. También, por lo que hace al delito de operaciones con recursos de procedencia ilícita, este se encuentra regulado tanto a nivel nacional como internacional, donde dicha regulación contempla las sanciones correspondientes al cometerlo, pero imprescindibles los actos que se deben llevar a cabo para su prevención.

CAPÍTULO III.- LA COMISIÓN DE LA CONDUCTA DE *PHISHING* Y EL DELITO DE OPERACIONES CON RECURSOS DE PROCEDENCIA ILÍCITA.

3.1.- RELACIÓN ENTRE EL *PHISHING* Y EL DELITO DE OPERACIONES CON RECURSOS DE PROCEDENCIA ILÍCITA.

A lo largo de la presente investigación se han descrito aspectos generales de la conducta de *phishing* y el delito de operaciones con recursos de procedencia ilícita, asimismo, se han identificado aquellos ordenamientos normativos a nivel nacional como internacional en los que se encuentran regulados. En tal virtud, es el momento de explicar la relación que existe entre ambos, ya que uno es el medio por el cual se puede llegar a la comisión del otro.

Para comenzar, la conducta de *phishing,* pertenece al catálogo de delitos informáticos, mientras que el delito de lavado de dinero, es parte de los delitos financieros, esto es "cualquier delito no violento que da lugar a una pérdida financiera, constituyen uno de los más grandes retos que encaran las instituciones financieras, los delincuentes financieros profesionales han aumentado su habilidad y sofisticación gracias a los avances en la tecnología disponible"[57], algo que se debe destacar de lo anterior, es lo referente a los avances tecnológicos, toda vez que es ahí donde se da la relación entre el *phishing* y el lavado de dinero.

Como se pudo apreciar en el capítulo primero de esta investigación, tanto el *phishing* como el lavado de dinero, tienen características y formas de comisión distintas, sin embargo, la evolución que ha tenido el delito de lavado de dinero al paso de los años, ha provocado que, independientemente de los delitos cometidos de los que derivan los recursos ilícitos, se utilicen otras conductas ilícitas para la comisión del lavado de dinero, siendo el caso, la conducta de *phishing,* toda vez que esta al ser el medio para llegar a la comisión del delito de operaciones con recursos de procedencia ilícita, provoca que sea más difícil la localización y rastreo de los delincuentes, al ser utilizadas otras personas para llevar a cabo todas las actividades concernientes a ello y que estos, en dado caso de descubrirse las

[57] Acata Águila, Isaías Jorge, "Prevención del delito financiero", p. 1, fecha de consulta: 17 de mayo de 2019, *http://acacia.org.mx/busqueda/pdf/01_PF212_Prevenci__n_del_Delito_Financiero.pdf.*

actividades delictivas por las autoridades, queden como los principales responsables de la comisión de las mismas.

3.1.1.- FORMAS DE COMISIÓN CONJUNTA DEL *PHISHING* Y EL DELITO DE OPERACIONES CON RECURSOS DE PROCEDENCIA ILÍCITA.

Tanto la conducta de *phishing* como el delito de operaciones con recursos de procedencia ilícita tienen una forma diferente y particular de realizarse, no obstante, al haber una relación entre ambos, esto provoca que la comisión de éstos pueda darse de manera conjunta, ya que, como se ha mencionado con anterioridad, uno es el medio para poder llevar a cabo el otro, en la especie, la conducta de *phishing* es uno de los medios para la comisión del delito de lavado de dinero. En tal virtud, a continuación se desarrollarán las diferentes maneras en las que pueden realizarse.

Para comenzar, la conducta de *phishing* es la primera que se tiene que realizar, teniendo por una parte a una persona o un grupo de personas que tienen conocimientos amplios y sólidos en temas relacionados con sistemas informáticos, y por el otro lado, a la persona a la que le va a recaer dicha conducta, en tal virtud, existen diferentes formas de comisión, entre ellas las que se efectúan a través de correos electrónicos, los cuales dirigen a la persona perjudicada a una página de internet falsa y aquellas personas que al intentar ingresar a la página de una institución de banca múltiple, directamente son dirigidas a una página falsa, con dichas formas se tiene la finalidad de robar su información, para posteriormente ser utilizadas, tal y como se apreciará a lo largo de este capítulo.

La primera forma de comisión es a través de correos electrónicos, donde dichos correos provienen de supuestas instituciones financieras y "(…) contienen enlaces a un sitio *web* falso con una apariencia casi idéntica a un sitio legítimo"[58], en lo particular, estos correos no son enviados a una persona en específico, sino

[58] "*Phishing", Seguridad de la información,* fecha de consulta: 20 de mayo de 2019, *https://www.segu-info.com.ar/malware/phishing.htm.*

son enviados a un grupo extenso de personas, siendo un envío al azar, toda vez que no todos los correos van a coincidir con las personas a las cuales fueron enviados, es decir, no todas las personas tienen relación con la institución financiera que les envió ese correo, sin embargo, al coincidir, es cuando se consolida la comisión del *phishing.*

Una vez que la persona abre dicho correo, una de las características que puede ponerla en alerta es que, al ser correos masivos, el correo no va dirigido a la persona en específico, es decir, no aparece la leyenda "Estimado C. (nombre del cuentahabiente)", sino, simplemente se limita a utilizar un nombre en general, esto es, sólo aparece la leyenda "Estimado cuentahabiente" o "Estimado usuario".

En tal virtud, en el contenido del mensaje van inmersas ciertas situaciones, con las cuales se pretende engañar al cuentahabiente, por ejemplo "(…) cambio en la normativa del banco, cierre incorrecto de la sesión del usuario, mejoras en las medidas de seguridad, detectada intrusión en sus sistemas de seguridad, bloqueo de la cuenta por motivos de seguridad, (…)"[59], derivado de ello, se invita al cuentahabiente para ingresar al enlace que se anexa y llevar a cabo la actividad que se indica y con ello, el ingresar su información tanto personal como bancaria en una plataforma falsa.

A pesar de ello, esta invitación tiene consigo una advertencia a la persona, avisándole que, si no lleva a cabo dicha actividad, puede tener ciertas consecuencias que causen una afectación grave e irreversible, por ejemplo, el bloqueo definitivo de su cuenta bancaria y ante el desconocimiento del cuentahabiente sobre tales situaciones, se ve en la obligación de ingresar al enlace que se encuentra en el correo, donde este dirige a la persona a una página de internet idéntica a la del sistema financiero, haciendo creer a la persona que realmente se encuentra en la página de internet del banco y a partir de ello, lograr que la persona ingrese los datos que le solicitan, como por ejemplo, su nombre, los

[59] "Oficina de seguridad del internauta", 11 de abril de 2014, fecha de consulta: 31 de mayo de 2019, *https://www.osi.es/es/actualidad/blog/2014/04/11/aprendiendo-identificar-los-10-phishing-mas-utilizados-por-ciberdelincuentes.*

dígitos de la tarjeta, los tres dígitos que se encuentran al reverso de ésta, fecha de vencimiento de la tarjeta.

Después del ingreso de los datos personales y bancarios de la persona, se concreta el *phishing,* ya que los *phishers*, lograron su objetivo, esto es, obtener los datos de la persona sin que esta tuviera el conocimiento de lo que en realidad estaba haciendo al abrir ese correo electrónico.

La segunda forma de realizar la conducta de *phishing*, es a través de la modificación de las direcciones de internet de las entidades financieras, esto es, "(…) modifica de forma no autorizada la resolución del nombre de dominio enviando al usuario a una dirección IP distinta"[60] o también, "(…) el uso de subdominios (…)"[61]. Sin embargo, para poder explicar esta forma de llevar a cabo la conducta de *phishing,* se debe dar una breve explicación sobre lo que conlleva un dominio y un subdominio en las direcciones de internet.

Respecto al dominio, este "(…) sería el nombre único y exclusivo que se le asigna a tu página *web* en *Internet*. Sería algo así como el equivalente de la matrícula de tu coche, pero aplicado a tu página *web*"[62]. Por lo que hace a un subdominio:

> En Internet se podría decir que el subdominio se utiliza para referirse a una dirección web que trabaja como un anexo de un Dominio de Internet. (…) es un subgrupo o subclasificación del nombre de dominio el cual es definido con fines administrativos u organizativos, que podría considerarse como un dominio de segundo nivel.[63]

---

[60] Padilla Espinosa, Miriam J., "Pescando información *phishing", Seguridad*, Número 2, fecha de consulta: 31 de mayo de 2019, *https://revista.seguridad.unam.mx/print/2169.*

[61] "El *phishing* y sus técnicas", *Internetlab*, fecha de consulta: 31 de mayo de 2019, *https://www.internetlab.es/post/2478/el-phishing/.*

[62] Andrés, Rubén, "¿Qué es y para qué sirve el dominio de tu página web?", *Computer Hoy,* 2014, fecha de consulta: 31 de mayo de 2019, *https://computerhoy.com/noticias/internet/que-es-que-sirve-dominio-tu-pagina-web-22007.*

[63] "¿Qué es un subdominio de internet?", *Digital Awareness,* fecha de consulta: 31 de mayo de 2019, *https://www.tooit.com/es/que-es-un-subdominio-de-internet/.*

Ahora bien, el modo de llevar a cabo la conducta de *phishing,* es a través de la modificación del dominio de la dirección electrónica, por ejemplo, en la dirección de la entidad financiera BBVA Bancomer, https://www.bbva.com/es/mx/, en el subdominio “bbva”, se sustituirá la letra “a”, por la letra “ä”, quedando https://www.bbvä.com/es/mx/, a simple vista puede parecer la misma dirección de *internet*, sin embargo no es así, ya que el segundo enlace, al ser creado por los *phishers,* es el que va a sustituir la página original del banco, para que las personas que quieran ingresar a la página de la entidad a realizar algún trámite, al ingresar sus datos, éstos sean sustraídos por estas personas, sin que dichas personas se den cuenta de lo que está pasando en realidad.

En tanto, por lo que hace al subdominio, se utilizará la misma dirección de *internet* de la entidad financiera BBVA Bancomer, siendo esta https://www.bbva.com/es/mx/, en tanto, al agregarse el subdominio a dicho enlace, quedaría de la siguiente manera: https://tubancoconfiable.bbva.com/es/mx/ y como ya se mencionó con antelación, al intentar ingresar dichas personas a la página de la entidad financiera, éstas se encontrarán con este enlace, por lo que, al ingresar sus datos tanto personales como financieros, es cuando se da la conducta de *phishing,* por lo que, como sucede con los correo electrónicos, las personas que cometen estas conductas delictivas toman los datos ingresados por las personas que ingresan a las páginas de internet de las entidades financieras.

Visto lo anterior, y una vez realizada la conducta de *phishing,* lo siguiente es pasar a la comisión del delito de operaciones con recursos de procedencia ilícita; una vez que este grupo de personas han logrado su primer objetivo, es decir, la sustracción de información tanto personal como bancaria de las personas, llevarán a cabo el siguiente paso, esto es, con esa información pueden actuar de dos formas, la primera de ellas es con la información personal, abrir una o varias cuentas bancarias en las entidades financieras y la segunda manera es desde la propia cuenta bancaria, llevar a cabo todas las transacciones de los recursos ilícitos a otra u otras cuentas, o solo ser depositado en éstas de manera temporal y con ello, se concreta el robo de identidad.

Ya sea actuando de una forma u otra, el objetivo es llevar a cabo la primera etapa del delito de operaciones con recursos de procedencia ilícita, colocando dichos recursos obtenidos de manera ilícita en las cuentas bancarias de las personas a las que les fue robada su información, introduciendo estos recursos al Sistema Financiero Mexicano y con ello, dichos delincuentes se deslindan de responsabilidad, ya que, en un primer momento, las personas propietarias de las cuentas bancarias serían las responsables de explicar la procedencia de dichos recursos.

Respecto a lo anterior, la conducta de *phishing* es un medio para la comisión del delito de operaciones con recursos de procedencia ilícita, al permitirles a los delincuentes introducir los recursos obtenidos de manera ilícita al Sistema Financiero Mexicano, dándose con ello la primera etapa de este delito, sin que estos delincuentes corran el riesgo de ser relacionados con estos recursos, por ello, se debe dar primero la comisión de la conducta de *phishing,* ya que con esta conducta, se utilizan a terceras personas que serán las que tendrán que responder si las autoridades logran localizar estas actividades realizadas.

3.1.2.- LOS INTERMEDIARIOS O MULEROS EN LA CONDUCTA DE *PHISHING* Y EL DELITO DE OPERACIONES CON RECURSOS DE PROCEDENCIA ILÍCITA.

Respecto a lo anterior, de las cuentas bancarias de las personas que fueron víctimas del robo de su información personal y bancaria, se puede llevar de manera directa la colocación de los recursos ilícitos en el Sistema Financiero, sin embargo, existe otra forma en la cual se puede realizar dicha colocación, esto es a través de personas que fungen como intermediarias o también llamadas muleros, es decir:

> (…) el intermediario en los casos de *phishing* suele ser una persona ajena a las intenciones de los estafadores. Para que el intermediario sea útil es necesario que resida en el mismo país que la víctima y la manera de conseguir la colaboración de este intermediario es mediante «técnicas de

> ingeniería social»; es decir, engañando al intermediario haciendo que crea que realiza una actividad lícita.[64]

Cabe precisar varios aspectos de estas personas, la primera de ellas es que dichos muleros también pueden tener noción de que aquellos recursos provienen de operaciones ilícitas, sin embargo, éstos al recibir una gratificante comisión por realizar las actividades, no les importa que se encuentren cometiendo una conducta delictiva; otro de los aspectos que se debe mencionar es correspondiente a la forma en cómo los delincuentes seleccionan a los muleros, principalmente los seleccionan a través de *internet*, utilizando el envío de correos electrónicos con ofertas de trabajo llamativas para estos y grandes ventajas económicas.

Una vez que estas personas se interesan por las ofertas de trabajo, el siguiente paso es:

> Una vez que la víctima contacta con los estafadores tiene que rellenar un formulario donde le solicitan su cuenta bancaria para realizarle un ingreso procedente de una cuenta bancaria de una víctima del *phishing* (sic) (…)
>
> Al tener las claves los estafadores hacen un ingreso bancario a la otra víctima (mulero) (sic), una vez realizada la transferencia bancaria los estafadores avisan al mulero y le dicen que se quede un porcentaje (5% - 10%) que será su comisión de trabajo, el dinero restante tiene que enviarlo por medio *Money Gram* o similares a un destino que los estafadores le indique.[65]

De lo anterior, se debe precisar que, previamente se tuvo que llevar a cabo la conducta de *phishing*, para que, en un primer momento los recursos ilícitos hayan sido depositados en las cuentas de las víctimas de *phishing*, y una vez estando el dinero ahí, es cuando llega la intervención de los muleros, los cuales una vez que son contratados y han aperturado una o varias cuentas bancarias de la misma entidad financiera de la víctima de *phishing,* esto con la finalidad de hacer las transferencias de una manera más rápida, los delincuentes realizan la transferencia

---

[64] "*Phishing.* Mulas y muleros", fecha de consulta: 01 de junio de 2019, *https://tacticalegal.pro/blog/phishing-mulas-y-muleros/.*

[65] "Muleros las otras víctimas del *phishing*", fecha de consulta: 01 de junio de 2019, *https://seguridad.internautas.org/html/511.html.*

en cantidades moderadas para no levantar sospecha de lo que pueda estar pasando.

Una vez que realizan estas transacciones, les avisan a los muleros que el dinero ya está en sus cuentas y les dan la siguiente indicación, siendo esta acción la de retirar todo el dinero de las cuentas y enviarlo por medio de compañías que se dediquen al envío de dinero a diferentes partes del mundo, como *Money Gram,* la cual es "una compañía estadounidense de servicios financieros con presencia en más de 170 países, que ofrece a sus clientes la posibilidad de enviar y recibir dinero en cualquier parte del mundo siempre y cuando el sitio donde estén cuente con una sede *MoneyGram*."[66].

Asimismo, pueden enviar dicho dinero a través de "(…) giros postales al extranjero que no identifiquen al receptor"[67], cabe precisar que, estos envíos por parte de los muleros no se realizan de nuevo por cuentas bancarias, toda vez que los delincuentes estarían propensos a ser identificados, por lo que el objetivo de ello es recibir los recursos sin dejar huella.

Realizado lo anterior, se puede destacar que al ser ingresados los recursos de procedencia ilícita en el Sistema Financiero Mexicano, se está llevando a cabo la primera etapa del delito de lavado de dinero, es decir, la colocación de los recursos, por lo que una vez que dichos recursos pasan a manos de los muleros y posteriormente de nuevo, a disposición de los delincuentes, es cuando se encuentra la comisión de la segunda etapa del lavado de dinero, siendo esta la estratificación de los recursos.

[66] Fecha de consulta: 01 de junio de 2019, *https://www.cuidatudinero.com/13121587/como-funciona-un-moneygram.*
[67] Fernández Teruelo, Javier Gustavo, *Derecho penal e internet. Especial consideración de los delitos que afectan a jóvenes y adolescentes,* España, Lex Nova, 2011, p. 39.

3.1.3.- COMISIÓN DE LA CONDUCTA DE *PHISHING* Y EL DELITO DE OPERACIONES CON RECURSOS DE PROCEDENCIA ILÍCITA EN MÉXICO.

Durante este capítulo se ha explicado la relación que existe entre el *phishing* y el lavado de dinero, las diferentes maneras de poder llevarlos a cabo y las personas involucradas en la comisión de estos. En tal virtud, es momento de explicar cómo estos se realizan en México.

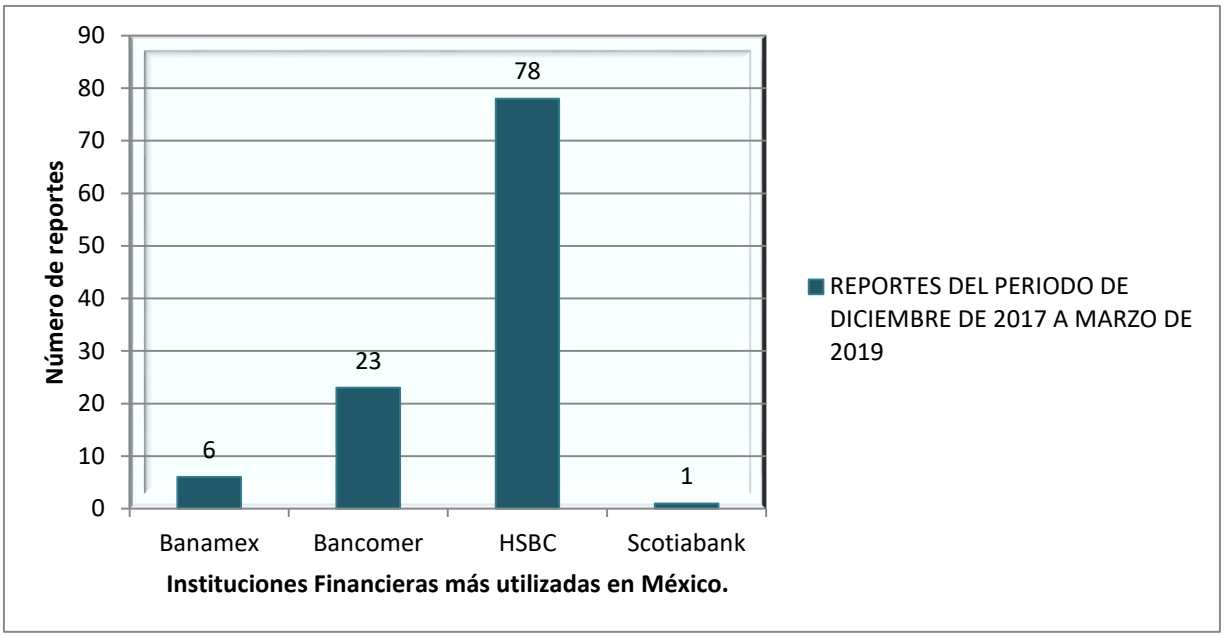
Para comenzar, la conducta de *phishing,* a pesar de que no se encuentra regulada específicamente en un ordenamiento normativo mexicano, esto no exime que se concrete su comisión, por lo que existen instituciones que se encargan de llevar el control y regulación de esta conducta. El primero de ellos es la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF), dicha institución, tiene en su página de *internet* un "Portal de Fraudes Financieros", en este portal, tal y como lo refiere la CONDUSEF en su página oficial:

> (…) todo usuario podrá acceder al "Monitor de Reportes" en donde podrá conocer si cualquier teléfono, página web, perfil de redes sociales o correos electrónicos ha sido reportado como fraudulento. También tendrá la oportunidad de compartir su experiencia en caso de haber sido víctima o haber detectado un posible fraude, para que CONDUSEF analice el caso y se prevenga a otros usuarios del peligro.[68]

En este portal las personas podrán denunciar ya sea los teléfonos, correos electrónicos, páginas de internet, por los cuales intentaron realizar alguna conducta delictiva. En lo particular, en este portal tiene un monitor de reportes dividido en seis apartados, los cuales son: último reporte, teléfonos, correos, suplantación, páginas y ver todo; de dicha página, "Los datos mostrados como fraudulentos, constituyen información de un posible fraude al ser reportados por los usuarios o Instituciones Financieras derivado de una actividad fraudulenta"[69], por lo que se puede observar lo siguiente:

[68] Portal del Gobierno de México, Portal de Fraudes Financieros, fecha de consulta: 01 de junio de 2019, *https://www.gob.mx/condusef/acciones-y-programas/portal-de-fraudes-financieros.*
[69] Portal de Fraudes Financieros, fecha de consulta: 01 de junio de 2019, *https://phpapps.condusef.gob.mx/fraudes_financieros/monitor.php?r=3639&id=5.*

FIGURA 1: REPORTES DEL PERIODO DE DICIEMBRE DE 2017 A MARZO DE 2019.



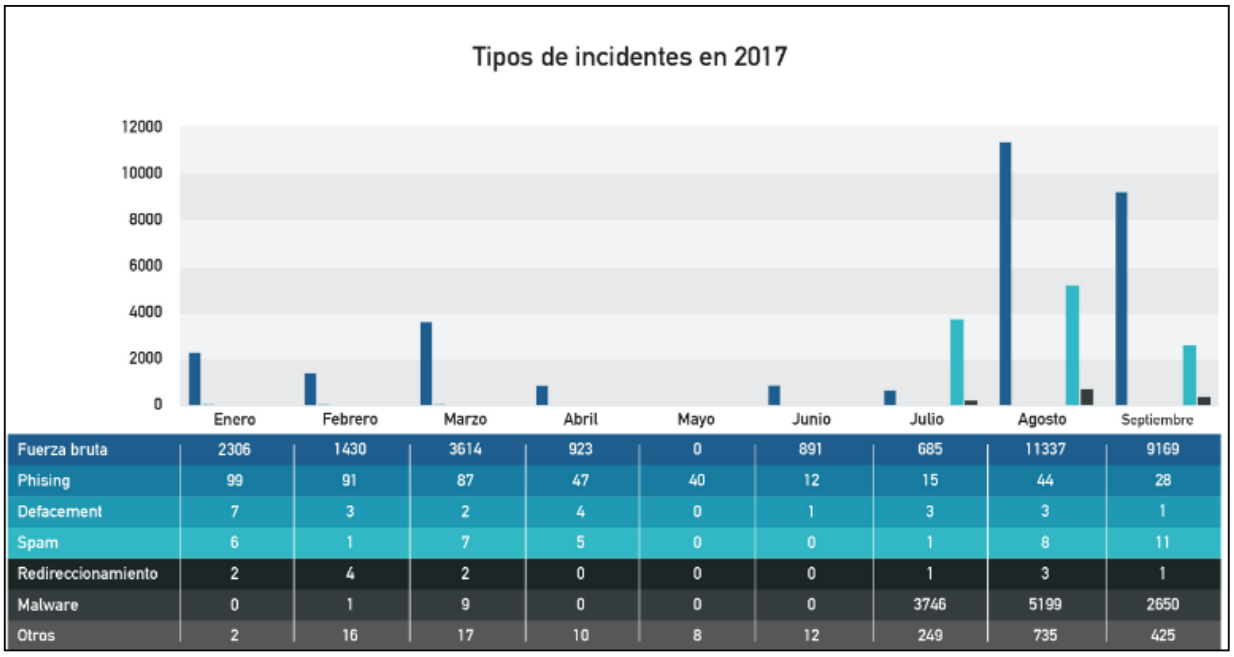
*Fuente: Gráfica creada por la autora con información de: Portal de Fraudes Financieros, fecha de consulta: 01 de junio de 2019, *https://phpapps.condusef.gob.mx/fraudes_financieros/monitor.php?r=3639&id=5.*

De la gráfica anterior se puede apreciar los reportes que las personas realizaron desde el año 2017 al año 2019, de un total de 320 reportes relacionados con la conducta de *phishing,* donde las entidades financieras mencionadas con antelación fueron las involucradas en las conductas llevadas a cabo por los delincuentes.

Asimismo, la Coordinación de Seguridad de la Información (CSI) /UNAM-CERT como parte de la Dirección de Sistemas y Servicios Institucionales dentro de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación, UNAM[70], en las estadísticas que realiza cada año, en las gráficas correspondientes a los años 2016 y 2017, se aprecia la frecuencia con la que se dio la conducta de *phishing*, como se muestra a continuación:

[70] Fecha de consulta: 01 de junio de 2019, *https://www.cert.unam.mx/acerca-de-la-csi.*

FIGURA 2: TIPOS DE INCIDENTES EN 2017.

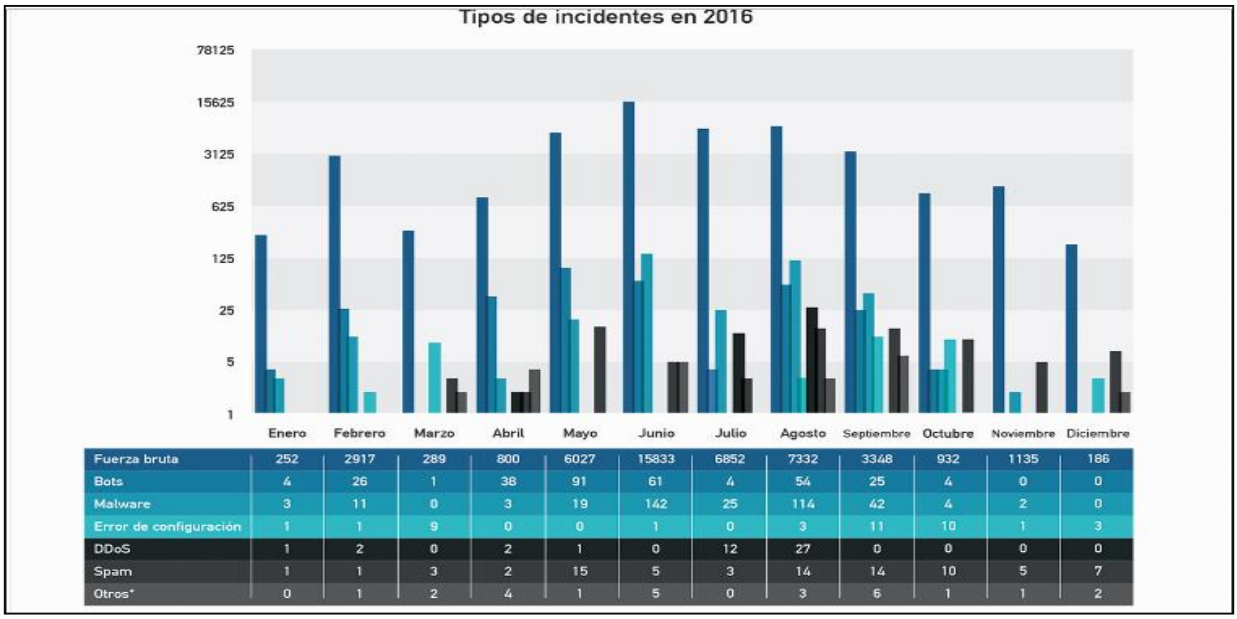


	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre
Fuerza bruta	2306	1430	3614	923	0	891	685	11337	9169
Phising	99	91	87	47	40	12	15	44	28
Defacement	7	3	2	4	0	1	3	3	1
Spam	6	1	7	5	0	0	1	8	11
Redireccionamiento	2	4	2	0	0	0	1	3	1
Malware	0	1	9	0	0	0	3746	5199	2650
Otros	2	16	17	10	8	12	249	735	425

*Fuente: Estadísticas año 2017, fecha de consulta: 02 de junio de 2019, *https://www.cert.unam.mx/estadisticas.*

Como se puede apreciar en la gráfica, el *phishing* fue una de las conductas que más incidencias tuvo, principalmente en los meses de enero, febrero, marzo, abril, mayo y agosto de 2017 en México.

FIGURA 3: TIPOS DE INCIDENTES EN 2016.



*Fuente: Estadísticas año 2016, fecha de consulta: 02 de junio de 2019, *https://www.cert.unam.mx/estadisticas.*

De la gráfica correspondiente al año 2016, se puede apreciar que la conducta de *phishing* no se encuentra entre los supuestos tomados en cuenta como en el año 2017, porque, "en la categoría "Otros" se agrupan los incidentes que por su baja ocurrencia no se desglosan de manera individual. Entre estos incidentes se encuentran *defacement,* redireccionamientos, XSS, *SQLi, phishing y Web Shell*."[71] Por lo que, en este año, la incidencia de la conducta de *phishing* fue menor a la de 2017.

Ahora bien, como se ha estado mencionando, la conducta de *phishing* no se encuentra regulada de manera específica dentro de algún ordenamiento normativo, sin embargo, sí hay una regulación para evitar que se lleve a cabo esta conducta y así como una vigilancia; esta regulación y vigilancia las efectúan a nivel nacional el Centro Nacional de Respuesta a Incidentes Cibernéticos de la Policía Federal, este centro se encarga de realizar:

[71] Estadísticas año 2016, fecha de consulta: 02 de junio de 2019, *https://www.cert.unam.mx/estadisticas*

> **(…) acciones de prevención e investigación de conductas ilícitas a través de medios informáticos, monitorea la red pública de Internet para identificar conductas constitutivas de delito, efectuando actividades de ciber-investigaciones, así como de ciberseguridad en la reducción, mitigación de riesgos de amenazas y ataques cibernéticos.** De igual forma, implementa programas de desarrollo científico y tecnológico en materia cibernética.[72]

Dicha Institución lleva estas acciones para prevenir que se concreten más casos de *phishing*¸ así como orientar a las personas para evitar que sean víctimas de esta conducta.

Respecto de la comisión del delito de operaciones con recursos de procedencia ilícita en México, se tiene que, "entre las medias (sic) puestas en marcha para evitar el blanqueo de dinero en México están la limitación del uso de efectivo para la compra de bienes inmuebles, automóviles, tarjetas prepagadas, apuestas, sorteos, concursos, alhajas, relojes, metales preciosos, obras de arte y donativos, entre otros"[73], toda vez que estas actividades están catalogadas como actividades vulnerables, y al ser realizadas, se puede llevar a cabo el delito de lavado de dinero, por ello, México a nivel internacional se encuentra "en una posición de riesgo intermedio"[74], como se muestra en la gráfica siguiente:

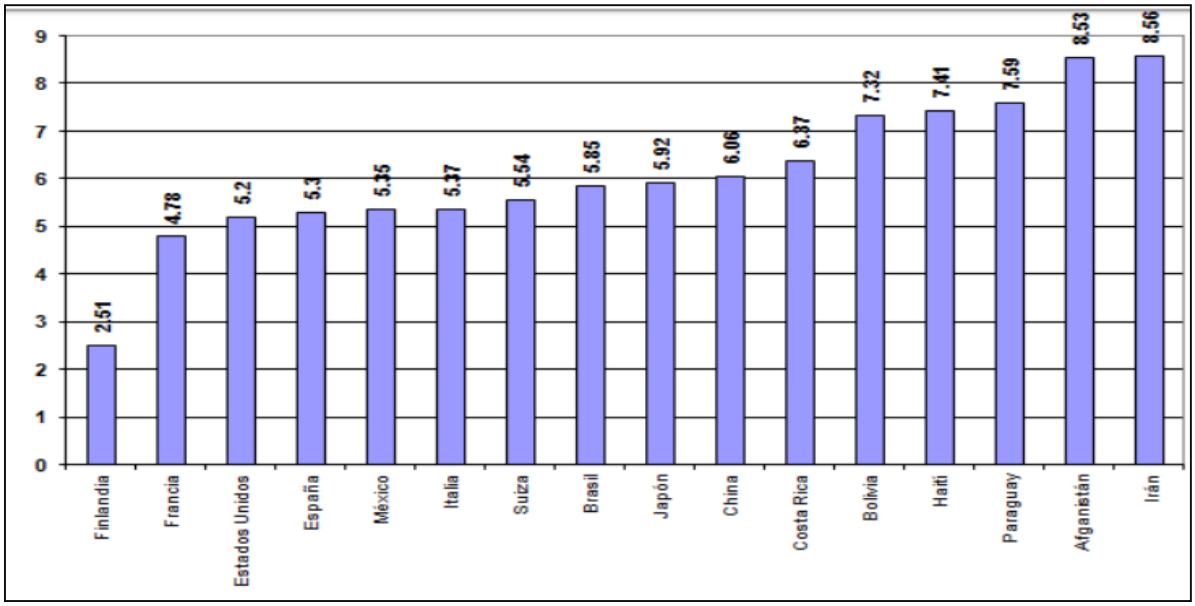
---

[72] Policía Federal, fecha de consulta: 02 de junio de 2019, *https://www.gob.mx/policiafederal/articulos/centro-nacional-de-respuesta-a-incidentes-ciberneticos-de-la-policia-federal?idiom=es,* lo resaltado es de origen.

[73] Aguirre Quezada, Juan Pablo, "Lavado de dinero en México: alcances y retos pendientes", p. 4, fecha de consulta: 02 de junio de 2019, *http://bibliodigitalibd.senado.gob.mx/bitstream/handle/123456789/1940/CI13.pdf?sequence=1&isAllowed=y.*

[74] *Ibídem,* p. 9.

FIGURA 4: CLASIFICACIÓN DE PAÍSES POR RIESGO DE REALIZAR OPERACIONES DE LAVADO DE DINERO (CASOS SELECCIONADOS).



*Fuente: Aguirre Quezada, Juan Pablo, "Lavado de dinero en México: alcances y retos pendientes", p. 9, fecha de consulta: 02 de junio de 2019, *http://bibliodigitalibd.senado.gob.mx/bitstream/handle/123456789/1940/CI13.pdf?sequence=1&isAllowed=y.*

Como se puede apreciar en la gráfica, México se encuentra en el quinto lugar de los países con mayor riesgo de la comisión del delito de lavado de dinero, aun cuando el porcentaje es menor a comparación de los países como Paraguay, Afganistán e Irán, teniendo en cuenta la evolución constante que ha tenido este delito.

Ahora bien, como se mencionó en el segundo capítulo de esta investigación, el delito de operaciones con recursos de procedencia ilícita, se encuentra regulado por diversos ordenamientos normativos, como lo son, la Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita y su reglamento, así como en el Código Penal Federal; dicha ley "tiene por objeto proteger al sistema financiero y la economía nacional, al establecer medidas y procedimientos para prevenir y detectar actos u operaciones que involucren recursos de procedencia ilícita."[75]. Sin embargo, a pesar de las medidas tomadas

[75] Vela, Laura, "¿Qué es y cómo funciona el lavado de dinero?", *Excelsior,* 25 de mayo de 2017, fecha de consulta: 03 de junio de 2019, *https://www.excelsior.com.mx/nacional/2017/05/24/1165451.*

para erradicar la comisión de este delito, no han sido suficientes para erradicarlo por completo, ya que para que inicie la comisión del delito de lavado de dinero, previo a ello debió llevarse a cabo otros delitos, como se muestra a continuación en la tabla siguiente:

FIGURA 5: DELITOS IDENTIFICADOS EN LAS DENUNCIAS FORMULADAS.

Delito previo	2010	2011	2012	2013	2014	2015	2016
Delitos relacionados con drogas	24	11	5	24	29	31	15
Delitos cometidos por funcionarios públicos (malversación de fondos, corrupción, sobornos)	1	-	-	1	1	7	4
Violación de la Ley General de Población	4	-	4	4	3	3	0
Extracción y robo de hidrocarburos	1	-	-	4	1		0
Vehículo sustraído/robado	-	-	1	2	-	1	0
Secuestro	-	1	-	1	2	1	1
Extorsión	-	-	-	-	1	2	0
Fraude	-	-	-	1	3	5	7
Delincuencia organizada	-	-	-	4	3	3	8
Delito fiscal	-	-	-	7	3	22	40
No determinado	22	27	25	36	41	34	32
Otros*							
Total	52	39	35	84	87	109	107

* Delitos relacionados con la Ley de Instituciones de Crédito, terrorismo, tráfico de personas, corrupción de menores y pornografía infantil

*Fuente: “Medidas anti lavado y contra la financiación del terrorismo. México. Informe de evaluación mutua.”, enero de 2018, fecha de consulta: 03 de junio de 2019, *https://www.gafilat.org/index.php/es/biblioteca-virtual/miembros/mexico/evaluaciones-mutuas-10.*

En la presente tabla se pueden percibir todos aquellos delitos cometidos previamente a la comisión del lavado de dinero, teniendo un mayor incremento en los años de 2015 y 2016, y los cuales a la fecha han seguido siendo cometidos.

Por otro lado, en septiembre de 2018, la Procuraduría General de la República, hoy Fiscalía General de la República, emitió su sexto informe de labores, el cual abarca del 2017 al 2018; respecto del delito de lavado de dinero, la Subprocuraduría Especializada en Investigación de Delincuencia Organizada dio a conocer los resultados obtenidos durante ese periodo, los cuales pueden apreciarse en la tabla siguiente:

FIGURA 6: RESULTADOS DEL COMBATE A LAS OPERACIONES CON RECURSOS DE PROCEDENCIA ILÍCITA EN EL PERIODO 2017-2018.

RESULTADO DEL COMBATE A LAS RECURSOS DE PROCEDENCIA Concepto	OPERACIONES CON ILÍCITA [1/] Sep.2017 – jun 2018[p/]
Dinero Asegurado[2/]	
Pesos Mexicanos(millones)	871.4
Dólares americanos (millones)	14.7
Averiguaciones previas iniciadas	5
Averiguaciones previas determinadas	48
Averiguaciones previas consignadas	10
Incompetencias	4
No ejercicio de la acción penal	20
Reservas	9
Acumulaciones	5
Número de personas contra las que no se ejerció acción penal	36
Órdenes de aprehensión libradas (por persona)	8
Procesos penales iniciados (auto de formal prisión por persona)	1
Sentencias condenatorias en sistema tradicional	11
Carpetas de investigación Iniciadas	114
Carpetas de investigación determinadas	12
Carpetas de investigación presentadas ante el órgano jurisdiccional	6
Incompetencias	4
No ejercicio de la acción penal	2
Número de personas presentadas ante el órgano jurisdiccional	11
Procesos penales iniciados (autos de vinculación por personas)	6
TOTAL DE DETENIDOS CARPETAS DE INVESTIGACIÓN	7
SENTENCIAS CONDENATORIAS EN SISTEMA PENAL	6
[1/] Resultados de la Subprocuraduría Especializada en Investigación de Delincuencia Organizada	
[2/] Total de dinero asegurado en efectivo y cuentas bancarias.	
[p/] Cifras preliminares a junio de 2018	

*Fuente: Pérez Macías, Carlos Alberto, "La realidad en números del lavado de dinero en México", *Veritas Online,* 04 de septiembre de 2018, fecha de consulta: 03 de junio de 2019, *https://veritasonline.com.mx/la-realidad-en-numeros-del-lavado-de-dinero-en-mexico/.*

De la tabla anterior, se puede apreciar que el dinero asegurado derivado de este delito fue de 871.4 millones de pesos, cifra que aumentó en comparación al dinero asegurado en el periodo de 2016-2017, ya que "durante 2017 la Procuraduría General de la República (PGR) realizó aseguramientos ministeriales por un total de 866.2 millones de pesos y 19.2 millones de dólares"[76]: del mismo modo, se puede

[76] Cordero, Carlos, "Lavado de dinero dejó 866 mdp y 19.2 mdd asegurados por PGR en 2017", *Quadratín México,* 16 de abril de 2018, fecha de consulta: 03 de junio de 2019,

apreciar que durante ese periodo, sólo se obtuvieron 6 sentencias condenatorias, una cifra baja a comparación de la frecuencia con la que se comete el delito de lavado de dinero.

El delito de operaciones con recursos de procedencia ilícita provoca afectaciones a los sectores sociales, políticos y principalmente al Sistema Financiero Mexicano, causando los efectos siguientes:

> a.) El principal elemento a partir del cual se forja cualquier sistema o institución financiera es la confianza, y es precisamente ésta el elemento más susceptible de ser vulnerado por el blanqueo de dinero.
>
> b.) Se erosiona la confianza de los inversionistas en el mercado y la institución financiera que ha sido penetrada por el delito, vía blanqueo de dinero aumenta la probabilidad de que se incurra en otro delito en prejuicio de los clientes.
>
> c.) Afecta la estabilidad del Sistema Financiero, este delito por parte de las instituciones financieras podría generar un riesgo sistemático en caso de producirse un efecto negativo sobre la reputación del sector a nivel internacional.
>
> d.) Distorsiones en la asignación de recursos de las ganancias derivadas de actividades ilícitas puede dar a quienes blanquean el dinero un poder dominante en los mercados financieros, distorsionando el sistema de precios y, por lo tanto, la asignación de recursos. [77]

Dicha afectación impacta directamente al sistema financiero al ingresarse los recursos de procedencia ilícita a este, al realizar actividades como la adquisición de bienes, inversiones de capital como socio en personas morales, haciendo creer que dichos recursos proviene desde un inicio de formas lícitas, cuando en realidad no fue así, dando como resultado un doble beneficio para dichos delincuentes, por un lado, haber logrado ingresar los recursos ilícitos al sistema financiero y hacerlos

https://mexico.quadratin.com.mx/lavado-de-dinero-dejo-866-mdp-y-19-2-mdd-asegurados-por-pgr-en-2017/.

[77] FERRUSQUÍA: *loc. cit.* Velázquez-Martínez, María de los Ángeles, *El delito de lavado de dinero, instrumentos y efectos económicos,* México, Ecorfan, 2016, p. 140, fecha de consulta: 03 de junio de 2019, *http://www.ecorfan.org/handbooks/Handbook_Matematicas_Aplicadas_a_la_Economia_T1V1/Particiones/11.pdf.*

pasar como recursos lícitos, para posteriormente, invertir éstos en alguna actividad y obtener ganancias con ellos.

Visto lo anterior y conociendo, tanto la conducta de *phishing* como el delito de operaciones con recursos de procedencia ilícita de manera general, se pudo explicar y sobre todo percibir la relación que existe entre ambos, conocer las diferentes formas de comisión del primero para que, después de su comisión, saber el momento exacto de la entrada del delito de lavado de dinero para llevar a cabo su comisión, y así visualizar que el primero es un medio para la comisión del segundo. Asimismo, se pudo apreciar la manera en que ambos se han ido desarrollando y han tenido efectos en México y las afectaciones que en varias esferas han causado, mismas que siguen siendo continuadas.

CONCLUSIONES

De la investigación realizada con antelación y a partir de la hipótesis planteada, se pueden establecer las siguientes conclusiones:

La conducta de *phishing* y el delito de operaciones de recursos de procedencia ilícita, como se ha mencionado a lo largo de la investigación, cuentan con características y formas de comisión diferentes, sin embargo, en el tercer capítulo se demostró la relación que existe entre ambas, la forma de comisión conjunta y como la primera de ellas es el medio para la comisión del segundo.

Aunado a ello, con el desarrollo del capítulo segundo, también se demostró la falta de regulación en los ordenamientos normativos mexicanos de la conducta de *phishing,* así como la falta de concientización del legislador al no dar el proceso legislativo correspondiente a las iniciativas consistentes en la creación de un capítulo especial para la regulación de los delitos informáticos, dando como resultado que el *phishing* aún no sea considerado como un delito y solo forme parte del catálogo de los delitos informáticos que pueden existir y esto a su vez, tenga como resultado que esta conducta no tenga una sanción proporcional a los actos derivados de su comisión, quedando estos impunes.

En tal virtud, el *phishing* al no ser considerado un delito sino solamente una conducta ilícita y ser el medio por el cual se concreta la comisión del delito de operaciones con recursos de procedencia ilícita, al momento de darse la sanción correspondiente, solamente se sanciona el delito de lavado de dinero, dejando impune la conducta de *phishing*, y con ello, todo lo que deriva de dicha conducta, esto es, dejar sin una debida sanción a los delincuentes que engañaron a otras personas, que llevaron a cabo un robo de identidad y que con esto, se dio paso para la comisión de lavado de dinero.

Visto lo anterior, se concluye que la hipótesis descriptiva que se planteó en esta investigación es válida, toda vez que, el delito de operaciones con recursos de procedencia ilícita, al estar regulado en un ordenamientos normativo general, esto es, en el Código Penal Federal, es necesario que la conducta de *phishing* de la

misma manera, sea regulada, pasando de ser una conducta ilícita a ser considerada como un delito, tipificándola en un capítulo especial, con las sanciones equivalente a la conducta y las agravantes que en dado caso amerite.

En tal virtud, al estar ambos tipificados en un mismo ordenamiento normativo general y derivado de su relación, da esto como resultado que el *phishing* sea regulado ahora en una ley especial, esto es la Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita y siguiendo con el propósito de dicha ley, prevenir la comisión del *phishing.*

PROPUESTAS

Una vez concluida la presente investigación y de todo lo concerniente a esta, al ser una hipótesis descriptiva, más no limitativa, nos permite realizar las siguientes propuestas:

1.- Para comenzar se debe reformar el Código Penal Federal, en el que se modifique el capítulo segundo “Acceso ilícito a sistemas y equipos de informática”, del título noveno y se estructure un capítulo exclusivo para los delitos informáticos y, con ello se incluya la conducta de *phishing* para que deje de ser solo una conducta ilícita y sea catalogada como delito, donde se indiquen las sanciones equivalentes para esta conducta.

2.- Una vez siendo considerado el *phishing* como un delito, se debe reformar la Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita, en la especie, el capítulo VIII “De los delitos”, en el cual, se incluiría un apartado respecto al delito de *phishing*¸ en el supuesto de ser utilizado como medio para la comisión del delito de operaciones con recursos de procedencia ilícita. Asimismo, en dicho apartado se incluiría la sanción proporcional al fungir como medio y las formas de prevención e identificación, tal y como se establecen en dicha ley, pero ahora con la conducta de *phishing.*

Con dicha propuesta se espera que el *phishing* al utilizarse como medio para la comisión del delito de lavado de dinero, ambos sean sancionados con la misma proporcionalidad, evitando así que el primero, al no tener una regulación en algún ordenamiento normativo, quede impune, y con ello, todo lo que se llevó a cabo para la comisión de esta conducta ilícita.

ÍNDICE

Cuadro 1: Clasificación de los delitos informáticos……..……..…3
Cuadro 2: Técnicas para realizar la conducta de *phishing*…….……....8
Diagrama 1: El proceso de lavado de activos en negocios ilícitos que generan grandes cantidades de dinero en efectivo……...…..18
Cuadro 3: Características del delito de operaciones con recursos de procedencia ilícita…… 19
Figura 1: Reportes del periodo de diciembre de 2017 a marzo de 2019……..…..52
Figura 2: Tipos de incidentes en 2017……....53
Figura 3: Tipos de incidentes en 2016……54
Figura 4: Clasificación de países por riesgo de realizar operaciones de lavado de dinero (casos seleccionados)…….……..56
Figura 5: Delitos identificados en las denuncias formuladas…….....57
Figura 6: Resultados del combate a las operaciones con recursos de procedencia ilícita en el periodo 2017-2018…….…58

BIBLIOGRAFÍA

CALLEGARI, André Luis, *Lavado de dinero, blanqueo de capitales. Una perspectiva entre los Derechos Mexicano, Español y Brasileño,* México, Flores Editor y Distribuidor, S.A. de C.V., 2010.

DÍAZ GARCÍA, Alexander, *Derecho informático, elementos de la informática jurídica,* Colombia, Leyer, 2012.

FERNÁNDEZ TERUELO, Javier Gustavo, *Derecho Penal e internet. Especial consideración de los delitos que afectan a jóvenes y adolescentes,* España, *Lex* Nova, 2011.

FERRUSQUÍA CANCHOLA, Manuel, *El sistema jurídico en lavado de dinero,* México, Flores Editor y Distribución, 2013.

FIGUEROA VELÁZQUEZ, Rogelio M., *El delito de lavado de dinero en el derecho penal mexicano,* México, Porrúa, 2001.

GUILLERMO, Jorge *et al.,* (coord.), *Lavado de activos: un nuevo modelo de investigación,* 2da. ed., República Dominicana, Ministerio, 2010.

MONTOYA PIÑA, Javier Omar, *Delitos federales cometidos a través de medios informáticos,* México, Flores Editor y Distribuidores, S.A. de C.V., 2015.

OROZCO-FELGUERES LOYA, Carlos, *Efectos fiscales en materia de lavado de dinero,* 3a. ed., México, Thomson Reuters, 2015.

PALOMÁ PARRA, Luis Orlando*, Delitos informáticos (en el ciberespacio). Doctrina y análisis de casos reales,* Colombia, Ediciones Jurídicas Andrés Morales, 2012.

TÉLLEZ VÁLDES, Julio, *Derecho informático,* 3a. ed, México, McGraw-Hill Interamericana, 2004.

VELASCO SAN MARTÍN, Cristos, *La jurisdicción y competencia sobre delitos cometidos a través de sistemas de cómputo e internet,* España, Tirant lo Blanch, 2012.

ZAMORA SÁNCHEZ, Pedro, *Marco jurídico del lavado de dinero,* México, Oxford, 2000.

LEGISGRAFÍA

Código Penal Federal.

Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional.

Convención de Naciones Unidas contra el Tráfico Ilícito de Estupefacientes y Sustancias Psicotrópicas de 1988.

Convenio sobre Ciberdelincuencia Budapest, 2001, fecha de consulta: 14 de mayo de 2019, *https://www.oas.org/juridico/english/cyb_pry_convenio.pdf.*

Cuarenta Recomendaciones del Grupo de Acción Financiera Internacional.

Declaración de Principios del Comité de Basilea de 1988.

Ley Federal Contra la Delincuencia Organizada.

Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita.

CIBERGRAFÍA

ACATA ÁGUILA, Isaías Jorge, “Prevención del delito financiero”, fecha de consulta: 17 de mayo de 2019, *http://acacia.org.mx/busqueda/pdf/01_PF212_Prevenci__n_del_Delito_Financiero.pdf.*

AGUIRRE QUEZADA, Juan Pablo, “Lavado de dinero en México: alcances y retos pendientes”, fecha de consulta: 02 de junio de 2019, *http://bibliodigitalibd.senado.gob.mx/bitstream/handle/123456789/1940/CI-13.pdf?sequence=1&isAllowed=y.*

Asociación por los Derechos Civiles, “La convención de cibercrimen de Budapest y América Latina. Breve guía acerca de su impacto en los derechos y garantías de las personas”, 2018, volumen I, fecha de consulta: 14 de mayo de 2019, *https://adcdigital.org.ar/wp-content/uploads/2018/03/Convencion-Budapest-y-America-Latina.pdf.*

BOTERO BERNAL, José Fernando, *Código Penal Colombiano (Ley 599 de 2000*), fecha de consulta: 14 de mayo de 2019, *http://perso.unifr.ch/derechopenal/assets/files/legislacion/l_20160208_02.pdf.*

Coordinación de Seguridad de la Información, UNAM-CERT, fecha de consulta: 01 de junio de 2019, *https://www.cert.unam.mx/acerca-de-la-csi.*

De Al Capone a Lucky Luciano: 'gangsters' que marcaron época y estilo”, *Gentleman. El Confidencial,* 2017, fecha de consulta: 19 de marzo de 2019, *https://www.gentleman.elconfidencial.com/multimedia/album/reportajes/2017-10-24/gansters-estilo-al-capone-lucky-luciano-bugsy-siegel_1329527#0.*

Declaración del Comité de Autoridades de Supervisión Bancaria del Grupo de los Diez y de Luxemburgo, hecha en Basilea en diciembre de 1988, sobre prevención en la utilización del Sistema Bancario para blanquear fondos de origen criminal, fecha de consulta: 27 de abril de 2019, *http://www.pnsd.mscbs.gob.es/pnsd/legislacion/pdfestatal/i47.pdf.*

Estadísticas año 2017, fecha de consulta: 02 de junio de 2019, *https://www.cert.unam.mx/estadisticas.*

Estándares internacionales sobre la lucha contra el lavado de activos y el financiamiento del terrorismo y la proliferación. Las recomendaciones del

GAF., Febrero 2012, fecha de consulta: 30 de abril de 2019, *https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF-40-Rec-2012-Spanish.pdf.*

ESTRADA GARAVILLA, Miguel, "Delitos informáticos", fecha de consulta: 04 de marzo de 2019, *https://www.unifr.ch/ddp1/derechopenal/articulos/a_20080526_32.pdf.*

Grupo de Acción Financiera de Latinoamérica (GAFILAT), fecha de consulta: 30 de abril de 2019, *https://www.gafilat.org/index.php/es/gafilat/preguntas-frecuentes.*

La redacción, "FGR alerta sobre código malicioso que roba información crediticia", *Proceso.com.mx,* 18 de marzo de 2019, fecha de consulta: 19 de marzo de 2019, *https://www.proceso.com.mx/575799/fgr-alerta-sobre-codigo-malicioso-que-roba-informacion-crediticia?fbclid=IwAR3HuDesMHcOUNH5nAKkGlIHj-4H9ZDqG-NDLbEUKuZzlMt-jdXwIAv8Jzw.*

"Medidas anti lavado y contra la financiación del terrorismo. México. Informe de evaluación mutua.", enero de 2018, fecha de consulta: 03 de junio de 2019, *https://www.gafilat.org/index.php/es/biblioteca-virtual/miembros/mexico/evaluaciones-mutuas-10.*

MEJIAS, Aron, "Cuida tu dinero", fecha de consulta: 01 de junio de 2019, *https://www.cuidatudinero.com/13121587/como-funciona-un-moneygram.*

"Muleros las otras víctimas del *phishing*", fecha de consulta: 01 de junio de 2019, *https://seguridad.internautas.org/html/511.html.*

Oficina de Seguridad del Internauta, 11 de abril de 2014, fecha de consulta: 31 de mayo de 2019, *https://www.osi.es/es/actualidad/blog/2014/04/11/aprendiendo-identificar-los-10-phishing-mas-utilizados-por-ciberdelincuen.*

"*Phishing.* Mulas y muleros", fecha de consulta: 01 de junio de 2019, *https://tacticalegal.pro/blog/phishing-mulas-y-muleros.*

"Phishing", Seguridad de la Información, fecha de consulta: 20 de mayo de 2019, *https://www.segu-info.com.ar/malware/phishing.htm.*

Policía Federal, fecha de consulta: 02 de junio de 2019, *https://www.gob.mx/policiafederal/articulos/centro-nacional-de-respuesta-a-incidentes-ciberneticos-de-la-policia-federal?idiom=es.*

Portal de Fraudes Financieros, fecha de consulta: 01 de junio de 2019, *https://phpapps.condusef.gob.mx/fraudes_financieros/monitor.php?r=3639&id=5.*

Portal del Gobierno de México, Portal de Fraudes Financieros, fecha de consulta: 01 de junio de 2019, *https://www.gob.mx/condusef/acciones-y-programas/portal-de-fraudes-financieros.*

Real Academia Española, fecha de consulta: 05 de mayo de 2019, *https://dle.rae.es/?id=Gk0Xp1o|Gk1qslk.*

SILVIA CHAVARRÍA, Cedillo, "La normatividad internacional en materia de lavado de dinero y su influencia en el sistema jurídico mexicano", fecha de consulta: 30 de abril de 2019, *http://revista.ibd.senado.gob.mx/index.php/PluralidadyConsenso/article/download/161/161.*

VELÁZQUEZ-MARTÍNEZ, María de los Ángeles, *El delito de lavado de dinero, instrumentos y efectos económicos,* México, ECORFAN, 2016, fecha de consulta: 03 de junio de 2019, *http://www.ecorfan.org/handbooks/Handbook_Matematicas_Aplicadas_a_la_Economia_T1V1/Particiones/11.pdf.*

HEMEROGRAFÍA

AMIGÓN, Edgar, “Robo de identidad, un delito en aumento”, *Primer Plano,* p. 23, fecha de consulta: 19 de marzo de 2019, *https://www.condusef.gob.mx/Revista/PDF-s/2015/186/robo.pdf.*

ANDRÉS, Rubén, “¿Qué es y para qué sirve el dominio de tu página web?”, *Computer Hoy,* 2014, fecha de consulta: 31 de mayo de 2019, *https://computerhoy.com/noticias/internet/que-es-que-sirve-dominio-tu-pagina-web-22007.*

CORDERO, Carlos, “Lavado de dinero dejó 866 mdp y 19.2 mdd asegurados por PGR en 2017”, *Quadratín México,* 16 de abril de 2018, fecha de consulta: 03 de junio de 2019, *https://mexico.quadratin.com.mx/lavado-de-dinero-dejo-866-mdp-y-19-2-mdd-asegurados-por-pgr-en-2017/.*

“El phishing y sus técnicas”, *Internetlab,* fecha de consulta: 31 de mayo de 2019, *https://www.internetlab.es/post/2478/el-phishing/.*

ESTÉVEZ MARTÍN, Sonia, “Delitos informáticos”, 2010, fecha de consulta: 05 de mayo de 2019, *http://gpd.sip.ucm.es/sonia/docencia/master1011/delito.pdf.*

Gaceta Parlamentaria, año XIV, número 3223-II, jueves 17 de marzo de 2011, consultada el día 13 de mayo de 2019, *http://gaceta.diputados.gob.mx/Gaceta/61/2011/mar/20110317-II.html#Iniciativa6*

Gaceta Parlamentaria, año XIX, número 4407-IV, miércoles 18 de noviembre de 2015, consultado el día 13 de mayo de 2019, *http://gaceta.diputados.gob.mx/Gaceta/63/2015/nov/20151118-IV.html.* Lo resaltado es de origen

Gaceta Parlamentaria, año XIX, número 4441-II, jueves 7 de enero de 2016, consultada el día 13 de mayo de 2019, *http://gaceta.diputados.gob.mx/Gaceta/63/2016/ene/20160107-II.html*.

Gaceta Parlamentaria, año XV, número 3401-V, martes 29 de noviembre de 2011, consultada el 05 de abril de 2019, *http://gaceta.diputados.gob.mx/Gaceta/61/2011/nov/20111129-V.html*.

GARCÍA GIBSON, Ramón, "Las 3 etapas del lavado de dinero", *Forbes México,* fecha de consulta: 02 de abril de 2019, *https://www.forbes.com.mx/las-3-etapas-del-lavado-de-dinero/.*

LOREDO GONZÁLEZ, Jesús Alberto, "Delitos informáticos: su clasificación y una visión general de las medidas de acción para combatirlo", *Celerinet, 2013,* enero-junio, fecha de consulta: 04 de marzo de 2019, *http://eprints.uanl.mx/3536/1/Delitos_informaticos.pdf.*

PÉREZ MACÍAS, Carlos Alberto, "La realidad en números del lavado de dinero en México", *Veritas online,* 04 de septiembre de 2018, fecha de consulta: 03 de junio de 2019, *https://veritasonline.com.mx/la-realidad-en-numeros-del-lavado-de-dinero-en-mexico/.*

"¿Qué es un subdominio de internet?", *Digital Awareness,* fecha de consulta: 31 de mayo de 2019, *https://www.tooit.com/es/que-es-un-subdominio-de-internet/.*

RIQUELME, Rodrigo, "¿Qué es la Ley de Seguridad Informática propuesta por Morena?, *El Economista,* fecha de consulta: 07 de mayo de 2019, *https://www.eleconomista.com.mx/tecnologia/Que-es-la-Ley-de-Seguridad-Informatica-propuesta-por-Morena-20190402-0053.html.*

ROMERO FLORES, Rodolfo, "El robo o usurpación de identidad por medios informáticos o telemáticos: su tratamiento jurídico", fecha de consulta: 12 de marzo de 2019, *https://archivos.juridicas.unam.mx/www/bjv/libros/6/2958/20.pdf.*

SILVIA CHAVARRÍA, Cedillo, "La normatividad internacional en materia de lavado de dinero y su influencia en el sistema jurídico mexicano", fecha de consulta: 30 de abril de 2019,

http://revista.ibd.senado.gob.mx/index.php/PluralidadyConsenso/article/download/161/161.

VELA, Laura, “¿Qué es y cómo funciona el lavado de dinero?”, *Excelsior,* 25 de mayo de 2017, fecha de consulta: 03 de junio de 2019, *https://www.excelsior.com.mx/nacional/2017/05/24/1165451.*

PADILLA ESPINOSA, Miriam J., “Pescando información *phishing”, Seguridad*, Número 2, fecha de consulta: 31 de mayo de 2019, *https://revista.seguridad.unam.mx/print/2169.*