UNIVERSIDAD LA SALLE

DERECHO

TEMA:

MECANISMOS NORMATIVOS PARA LA INTRODUCCIÓN DEL PHISHING COMO DELITO INFORMÁTICO EN BOLIVIA.

LUÍS BERNARDO PARAVICINI BILBAO

TUTOR:

DR.GONZALO CONTRERAS GUTIÉRREZ

LA PAZ- BOLIVIA

2013

Dedicatoria

A Dios.-

Por haberme dado las fuerzas suficientes y la fe para creer que con sacrificio y perseverancia las cosas se pueden lograr, que nunca hay que dejar de luchar, y que ante las adversidades no hay que rendirse.

A mis padres.-

Por haberme apoyado en todo momento, por sus consejos, por los valores inculcados, por haberme enseñado a ser una persona de bien, por haber creído en mí, motivándome a luchar por mis sueños y conseguir mis metas.

A mis hermanos.-

Por ser un ejemplo de superación, por ser las personas más maravillosas que he conocido, por toda la ayuda incondicional que me han dado durante toda mi vida, no tengo palabras de agradecimiento ni forma de mostrar mi inmensa gratitud.

A mis amigos y catedráticos.-

Por ser una persona inmensamente bendecida con la calidad de amigos que tengo, que siempre han mostrado su apoyo, respeto y cariño incondicional hacia mí, siendo un pilar fundamental para salir adelante, y para no rendirme en las dificultades que se presentan en la vida. A mi universidad y sus catedráticos, que además de ser excelentes profesionales, son personas increíbles, siendo un motivo de orgullo poder considerarlos amigos y estar enormemente agradecido por las enseñanzas que me dejan.

A mi abuelita Elena Cortez Arce (QEPD).-

Por haberme criado, defenderme en todo momento, por todo el cariño y comprensión. Es para mí un motivo de felicidad cumplir con la promesa que un día le hice, y aunque ella no se encuentra a mi lado, sé que desde el cielo se siente muy orgullosa.

ÍNDICE

Contenido

promueven a un amplio debate para definirlos pues no existe una definición en la cual los juristas y estudiosos del derecho estén de acuerdo, es decir no existe una uniformidad en el concepto adecuado para así nombrar a los delitos informáticos.

Por su parte, el tratadista de Derecho Penal italiano Carlos Sarzana, sostiene que los delitos informáticos son:

> "Cualquier comportamiento criminal en que la computadora está involucrada como material, objeto o mero símbolo". (Sarzana, 2000, pág. 37)

Rafael Fernández Calvo, define al delito informático como

> "La realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando un elemento informático o telemático contra los derechos y libertades de los ciudadanos definidos en el título I de la Constitución Española". (Delitos Informáticos, 2012)
>
> "Los delitos informáticos se realizan necesariamente con la ayuda de los sistemas informáticos, pero tienen como objeto del injusto la información en sí misma." (Carrion, 2001)

En la actualidad se encuentran una serie de delitos cometidos a través de la informática, como es el caso del *phishing*. Este término es usado para denominar a una especie de delito informático que se caracteriza por ser una estafa cibernética mediante el cual se intenta adquirir información confidencial de forma fraudulenta, en casos como el robo de información bancaria.

John LaCour, director de Soluciones *Antiphising* de *MarkMonitor* menciona que el *phishing*

> "Es una estafa online que consiste en remitir engañosamente a los usuarios a páginas web fraudulentas, principalmente mediante e-mails que parecen auténticos, y en pedirles que proporcionen información personal como nombres de usuario, contraseñas, números de cuenta, direcciones, números de identificación personal (PIN), etc. Después, el estafador utiliza esa información para usurpar la identidad de la víctima y sacar dinero de su cuenta bancaria, organizar subastas online, solicitar tarjetas de crédito, pedir préstamos, blanquear dinero y llevar a cabo diferentes actividades ilegales online. Aunque el blanco de estas estratagemas son los consumidores individuales, las entidades por las que se hacen pasar los estafadores también son víctimas: se está atentando contra su marca y la buena reputación que tanto les ha costado conseguir. Los bancos son el objetivo más común de los ataques de tipo *phishing*, aunque cada vez se producen más ataques contra todo tipo de empresas". (La amenaza *phishing*, 2012)

De acuerdo con el informe realizado por el la organización *"Antiphishing"*, que se dedica a la lucha y concientización del *phishing* y así como otros estudios realizados por otras empresas como Panda se estima que son millones de personas en todo el mundo que son víctimas de este tipo de delito. De estos informes también se puede destacar a que el 35% de los usuarios de Facebook, una red social que consta de más de cien millones de usuarios en el mundo, han sido víctimas de esta estafa cibernética.

Como conclusión de todo lo investigado y desarrollado se fundamentará la razón por la que existe la necesidad de regular el *phishing* como delito informático en Bolivia, buscando su regulación y aplicación jurídica.

I.1. FORMULACIÓN DEL PROBLEMA.-

La falta de normativa que regule la informática, los nuevos delitos informáticos que se cometen, así como la inseguridad en la transmisión de datos a través de la internet, herramienta indispensable para la comunicación y realización de negocios, hace que Bolivia, se encuentre rezagada respecto a la regulación de estos delitos, en comparación con otras legislaciones, y que además exista la necesidad de contar con normas para sancionar a quienes cometan este tipo de ilícitos.

Por lo tanto, para determinar la necesidad de la regulación del *phishing* como delito informático se deberá responder a las siguientes interrogantes: ¿Qué se entiende por delitos informáticos? ¿Cuál es la relevancia de la comisión de estos delitos en la sociedad? ¿Es el *Phishing* un delito informático?

En conclusión la normativa boliviana respecto a los delitos informáticos necesita ser actualizada y complementada para imposibilitar que ante la comisión de estos hechos ilícitos queden impunes y no sean castigados como corresponde, con el fin de proporcionar seguridad jurídica a la colectividad boliviana que hace uso de estos mecanismos informáticos.

I.2. DELIMITACIÓN DEL PROBLEMA.-

El presente trabajo de investigación tiene como finalidad establecer la necesidad que tiene el país para complementar y actualizar sus normas que regulan los delitos informáticos, siendo el *Phishing* el delito al que se le prestará el objeto de la presente investigación.

I.3. PREGUNTA DE INVESTIGACIÓN.-

¿Se deben generar mecanismos normativos para la introducción del *Phishing* como delito informático en Bolivia?

I.4. OBJETIVOS.-

I.4.1. OBJETIVO GENERAL.-

Proponer mecanismos normativos para la introducción del *Phishing* como delito informático en Bolivia.

I.4.2. OBJETIVOS ESPECÍFICOS.-

- Conocer que se entiende por *Phishing,* como delito informático y su relevancia jurídica.
- Determinar las diferencias entre *Phishing,* Estafa y Manipulación Informática.
- Analizar las soluciones normativas que las legislaciones de distintos países, así como los convenios internacionales ofrecen para prevenir los daños que provoca el *Phishing* como delito informático.

I.5. JUSTIFICACIÓN

I.5.1. JUSTIFICACIÓN JURÍDICA

¿Por qué es importante regular al *Phishing* como delito informático dentro del Código Penal? Para imposibilitar que estos hechos delictivos queden impunes a una sanción.

Los actos que realiza una persona no pueden ser considerados delictivos, a menos que se encuentren regulados por una norma que así lo establezca.

Esto se basa en el Principio de Legalidad *"Nullum crimen nullum poena sine previa lege"* (No ha crimen, no hay sanción sin ley previa).

En ese sentido el Tribunal Constitucional Plurinacional de Bolivia estableció en la Sentencia Constitucional 0034/2006 un criterio respecto al principio de Legalidad y la prohibición en materia penal de sancionar por analogía, estableciendo lo siguiente:

> *"Nullum crimen, nulla poena, sine lege stricta*: los delitos y las penas deben estar determinadas exclusivamente por la Ley; lo que significa que no se puede recurrir a la analogía para extraer de su aplicación consecuencias desfavorables, aun cuando el comportamiento que se trata de incriminar sea similar al previsto en la ley penal.
>
> El fundamento de la prohibición de analogía radica en que, debido a la gravedad de la sanción contenida en la norma penal, ésta sólo debe responder a los supuestos que los representantes de la soberanía popular (legisladores) han establecido a través de la ley, vedándose de esta manera la extensión de la arbitrariedad del juzgador, exigiéndose, en cambio, la sujeción de éste a la Ley."(Tribunal Constitucional Plurinacional,2006)

El *Phishing* consiste en una estafa cibernética, que viola la seguridad jurídica de las personas, y se adecua a una conducta propiamente ilícita. Nuestro Código Penal respecto a la regulación de delitos informáticos solo cuenta con dos artículos (363 bis y 363 ter) dentro del Capítulo XI "Delitos Informáticos" por lo que se puede evidenciar la falta de normativa que tipifique conductas delictivas de los delitos informáticos.

Es así y según lo establecido por la doctrina y las distintas teorías que el Estado es quién debe hacer uso de sus facultades para regular normas que establezcan que hechos se van a considerar delitos y cual va ser la responsabilidad y sanción de quién cometa estos actos.

La Constitución Política del Estado en su artículo 9, señala como fines y atribuciones del Estado

> "Constituir una sociedad justa y armoniosa, cimentada en la descolonización, sin discriminación ni explotación, con plena justicia social, para consolidar las identidades plurinacionales.(Inciso 1)"
>
> "Y Garantizar el bienestar, el desarrollo, la seguridad y la protección e igual dignidad de las personas, las naciones, los pueblos y las comunidades, y fomentar el respeto mutuo y el diálogo intercultural, y plurilingüe". (Inciso 2) (Constitución Política del Estado, 2009, Gaceta Oficial de Bolivia)

Además el artículo 115 de la citada norma determina que:

> "Toda persona será protegida oportuna y efectivamente por los jueces y tribunales en el ejercicio de sus derechos e intereses legítimos."
>
> "II. El Estado garantiza el derecho al debido proceso, a la defensa y a una justicia plural, pronta, oportuna, gratuita, transparente y sin dilaciones." Constitución Política del Estado, 2009, Gaceta Oficial de Bolivia)

Es en ese sentido que para que el Estado pueda cumplir con sus fines de garantizar el bienestar, la paz social, la protección de las personas, además de protegerla oportuna y efectivamente por los jueces y tribunales cumpliendo con

preceptos y principios como una justicia pronta y oportuna que se ve en la obligación de regular normas que busquen mantener la seguridad jurídica de las personas.

El presente trabajo pretende ayudar al mejor funcionamiento jurisdiccional en los casos de delitos informáticos, específicamente en el caso del *Phishing*, evitando así que siga existiendo la poca relevancia jurídica y el vacío normativo que tiene nuestro Código Penal por la falta de actualización y complementación de nuevas normas que regulen estos hechos.

I.5.2 JUSTIFICACIÓN SOCIAL

El avance tecnológico, los alcances de la globalización, el internet como herramienta fundamental para el desarrollo han generado que se presenten situaciones negativas por el mal uso, y mal aprovechamiento de personas que buscan beneficiarse haciendo uso de sus conocimientos informáticos a costa de las demás personas.

El alto índice de situaciones que ocurren en internet y que se convierten en delito al causarse daño o violar derechos de las personas a través de engaños se ha vuelto muy común hoy en día en todas partes.

Es necesario que los Estados tomen la iniciativa en el ámbito informático y generen normas que protejan los derechos de las personas y castiguen a aquellos que hagan mal uso de esta herramienta para aprovecharse de otras personas de forma dolosa y que generen daños a la sociedad, al provocar inseguridad jurídica en el uso del internet y la informática.

Con el análisis que se hará en el presente trabajo sobre *Phishing* se podrá establecer el impacto que tiene en la sociedad los delitos informáticos, teniendo como ejemplo este hecho delictivo en particular. Tratando de demostrar la vulneración de derechos que pueden generar, la inseguridad jurídica que provocan y finalmente a través de la investigación concientizar a las personas de los distintos peligros que se pueden generar por la comisión de hechos delictivos como es el *Phishing*.

I.5.3. JUSTIFICACIÓN ECONÓMICA

Los casos de delitos informáticos como clonación de tarjetas o *Phishing* generan pérdidas importantes tanto como para personas naturales como personas jurídicas. El impacto económico por la comisión de hechos delictivos como el *Phishing* según lo establecido por empresas como Microsoft u organizaciones como *ANTIPHISHING* es de una magnitud sumamente relevante, y dentro de las numerosas víctimas que se reportaron, Bolivia no fue la excepción.

El Banco Nacional de Bolivia reportó según lo establecido por el Instituto Boliviano de Comercio Exterior (IBCE) que el 15 de junio de 2011 se detectaron 600 débitos dudosos y por lo tanto recibieron quejas de sus clientes. Según lo reportado los montos extraídos iban desde los 1.730 bolivianos hasta 2.250 bolivianos.

Por el robo a más de 600 clientes del Banco Nacional de Bolivia, tanto sus clientes que fueron víctimas de la sustracción del dinero de sus cuentas, como la institución bancaria y aseguradores que tuvieron que hacer el rembolso, sufrieron considerables pérdidas económicas.

El banco informó que los días 10 y 11 de junio la mayoría de estas personas hicieron transacciones y consultas de saldo por internet y

posteriormente se estableció que los clientes fueron víctimas de estafas cibernéticas. (IBCE, 2012)

A través del *Phishing* a éstas personas les fueron sustraída información personal como su pin y que posteriormente derivó en la sustracción de dinero de sus cuentas bancarias.

El presenta trabajo plantea la regulación del Phishing como delito informático con el fin de proteger de daños que puedan impactar en la economía

de la sociedad, y además al regular el *Phishing* como delito informático, no solo se plantea la sanción y el castigo a quienes cometan estos hechos, sino se plantea que como elemento adicional exista la reparación de daños y perjuicios que pueda ocasionar.

I.6. LIMITACIONES DE LA INVESTIGACIÓN

El presente trabajo se limitará a debatir sobre la necesidad de la regulación del Phishing como delito informático en la legislación del país. Para ello será necesario determinar que son los delitos informáticos, su relevancia en la sociedad y específicamente como afecta el Phishing a la sociedad. Esto se realizará a través de la utilización de métodos científicos - metodológicos de investigación que nos permitan encuadrar el objetivo de este trabajo.

I.7. RELEVANCIA, NOVEDAD, PERTINENCIA

RELEVANCIA.- En Bolivia es necesario establecer nuevas conductas delictivas que se presentan por los cambios y los avances en la sociedad. La globalización, el desarrollo tecnológico, la importancia de la informática en nuestras actividades cotidiana han hecho que se presenten nuevas situaciones que pueden poner en peligro la paz social y la seguridad jurídica de las personas. Este es el caso de los delitos informáticos, específicamente este trabajo se centra en el *Phishing* como un peligro inminente para las personas, por lo que se considera imprescindible su regulación dentro de la normativa boliviana.

NOVEDAD.- En Bolivia no se ha realizado aún un estudio profundo sobre la necesidad de regular el *Phishing* como un delito informático dentro de la legislación nacional. Es evidente que existe un vacío normativo respecto a la regulación de los delitos informáticos, y aunque han existido debates para ver la necesidad de regular este tipo de delitos, no se ha entrado específicamente a ver cada tipo de hecho que se puede dar, como es el caso del *Phishing*, un tipo de delito informático dentro de la extensa variedad que existen.

UTILIDAD.- En la gran parte de las universidades bolivianas no se han profundizado el estudio del Derecho Informático, así como los delitos informáticos tampoco han sido analizados y estudiados. Respecto a los delitos informáticos no existe grande estudios debido a que no existe normativa jurídica

vigente en extenso, es decir nuestro Código Penal solo consta de dos artículos que regulan delitos informáticos, por lo que se necesita hacer un estudio de este tipo de hechos delictivos en la informática, para plantear su regulación. En el caso del *Phishing* al ser un delito relativamente nuevo en el mundo en general, es aún más complejo su estudio, por lo que el presente trabajo a través de su estudio y conceptualización planteará la necesidad de su regulación en la normativa boliviana.

I.8. HIPÓTESIS

La introducción del *phishing,* como delito informático en Bolivia, proporcionará seguridad jurídica a la población usuaria de internet.

II.MARCO METODOLÓGICO.-

II.1 MÉTODO DOGMÁTICO JURÍDICO.-Según Jorge Wikter y Larios "El derecho se constituye por sus fuentes formales; la ley, la costumbre, los principios generales, el negocio jurídico y la jurisprudencia". (Witker & Larios, 1997, pág. 193)

En el presente trabajo de investigación se realizará una revisión de la normativa nacional vigente respecto a los delitos informáticos para determinar si existe la necesidad de complementar y actualizar la normativa, además se revisará la doctrina y las teorías para determinar que se entiende por *Phishing* y por delitos informáticos desde diferentes ópticas conceptuales.

Finalmente se revisará la normativa internacional y la legislación comparada contrastando con nuestra legislación nacional vigente y haciendo un análisis (objeto método dogmático jurídico).

III. MARCO TEÓRICO.-

CAPÍTULO 1.- EL PHISHING COMO DELITO INFORMÁTICO Y SU RELEVANCIA JURÍDICA.-

1.1 Delitos Informáticos.-

Orígenes.-

Indudablemente así como la computadora se presenta como una herramienta muy favorable para la sociedad, también se puede constituir en un medio o instrumento que facilite la comisión de actos ilícitos. Este tipo de actos encuentran sus orígenes en el surgimiento de la tecnología informática, ya que sin la existencia de las computadoras, estas acciones no existirían. Por otra parte, las facilidades que se presentan para la realización de las labores que se consiguen con la utilización de dichos aparatos genera que, en un momento dado, el usuario tenga las herramientas necesarias para poder realizar se una serie de actos ilícitos.

> "Por el mismo egoísmo humano se establece una especie de "duelo" entre el hombre y la máquina, lo cual en última instancia provoca el surgimiento de ilícitos en su mayoría no intencionados, por ese "deseo" del hombre de demostrar su superioridad frente a las máquinas, y en este caso específico las computadoras.

> De esta forma se ha establecido que estas acciones, más que resultado de una situación socioeconómica, se derivan de una actitud antropológica y psíquica, aunque en el terreno de los hechos son una realidad sociológica bien determinada y que requiere, por ende, de un tratamiento jurídico especifico". (Téllez Valdez, 1996, pág. 103)

María Luz Lima, por su parte, presenta la siguiente clasificación de "delitos electrónicos":

> "1. Como Método: conductas criminales en donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito.
>
> 2. Como Medio: conductas criminales en donde para realizar un delito utilizan una computadora como medio o símbolo.
>
> 3. Como Fin: conductas criminales dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla." (Lima de la Luz, 1984, pág. 33)

1.1.2. Concepto típico y atípico.-

> *"Dar un concepto sobre delitos informáticos no es labor fácil y esto en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de "delitos" en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídico-penales, se requiere que la expresión "delitos informáticos esté consignada en los códigos penales." (Téllez Valdez, 1996, pág. 103)*

1.1.3. Informática, objeto del Derecho.-

> "Al igual que en otros muchos, no ha sido objeto de tipificación aún; sin embargo, y habida cuenta de la urgente necesidad de esto, se empleará dicha alusión, aunque para efectos de una conceptuación, haciendo el distingo pertinente entre lo típico y lo atípico.
>
> De esta manera tenemos que, dependiendo del caso, los delitos informáticos son actitudes ilícitas en que se tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin (concepto típico).
>
> Por otra parte, de entre los contados tratadistas penales que han incursionado en el tema tenemos al italiano Carlos Sarzana, quien menciona que los delitos informáticos son "cualquier comportamiento criminogeno en que la computadora está involucrada como material, objeto o mero símbolo". (Téllez Valdez, 1996, pág. 104)

1.1.4. Principales características.-

Algunas de las características fundamentales que revisten este tipo de acciones:

> "a) Son conductas criminogenas, en tanto que sólo determinado número depersonas con ciertos conocimientos (en este caso técnicos) pueden llegar a cometerlas.
>
> b) Son acciones ocupacionales, en cuanto que muchas veces se realizan cuando el sujeto se halla trabajando.
>
> c) Son acciones de oportunidad, en cuanto que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.

e) Provocan serias pérdidas economicas, ya que casi siempre producen "beneficios" de más de cinco cifras a aquellos que los realizan.

d) Ofrecen facilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.

e) Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.

f) Son muy sofisticados y relativamente frecuentes en el ámbito militar.

g) Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.

h) Ofrecen facilidades para su comisión a los menores de edad.

i) Tienden a proliferar cada vez más, por lo que requieren una urgente regulación.

j) Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley". (Téllez Valdez, 1996, pág. 104)

1.1.5. La clasificación.-

Existen tratadistas como Carlos Sarzana que mencionan que estos actos ilícitos pueden clasificarse en atención a que producen un provecho para el autor y provocan un daño contra la computadora como entidad física y que procuren un daño a un individuo o grupos, en su integridad física, honor o patrimonio, el tratadista Julio Téllez Valdez los clasifica en atención a dos criterios: como instrumentos o medio, o como fin u objetivo

1.1.6. Como instrumento o medio.-

Dentro de esta categoría se encuentran las conductas criminológicas que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito, por ejemplo:

> "a) Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etcétera).
>
> b) Variación de los activos y pasivos en la situación contable de las empresas.
>
> c) Planeación, simulación de delitos convencionales (robo, homicidio, fraude, etcétera). "Robo" de tiempo de computadora.
>
> d) Lectura, sustracción o copiado de información confidencial.
>
> e) Modificación de datos tanto en la entrada como en la salida.

f) Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas (esto es lo que se conoce en el medio como el método del "Caballo de Troya").

g) Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa, método conocido como la "técnica de salami",

h) Uso no autorizado de programas de cómputo.

i) Introducción de instrucciones que provocan "interrupciones" en la lógica interna de los programas, a fin de obtener beneficios, tales como "consulta a su distribuidor".

j) Alteración en el funcionamiento de los sistemas, a través de los cada vez más temibles "virus informáticos".

k) Obtención de información residual impresa en papel o cinta magnética luego de la ejecución de trabajos.

l) Acceso a áreas informatizadas en forma no autorizada.

m) Intervención en las líneas de comunicación de datos o teleproceso". (Téllez Valdez, 1996, pág. 106)

1.1.7. Como fin u objeto.-

Dentro de esta categoría se enmarcan las conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física. Algunos ejemplos son los siguientes:

"a) Programación de instrucciones que producen un bloqueo total al sistema.

b) Destrucción de programas por cualquier método.

c) Daño a la memoria.

d) Atentado físico contra la máquina o sus accesorios (discos, cintas, etcétera).

e) Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.

g) Secuestro de soportes magnéticos en los que figure información valiosa con fines de chantaje (pago de rescate, etcétera). (Téllez Valdez, 1996, pág. 107)

"Cabe hacer mención que una adecuada legislación al respecto traería consigo efectos no sólo correctivos sino eventualmente preventivos, de tal forma que se reducirían en buen número este tipo de acciones que tanto daño causan a los intereses individuales y sociales". (Téllez Valdez, 1996, pág. 108)

1.1.8. Delitos basados en técnicas de ingeniería social.-

"Los delitos basados en técnicas de ingeniería social son relativamente similares a los tradicionales "timos", en los que se engaña a la víctima para que haga algo (revelar información sensible de carácter personal e incluso cometer él mismo- de manera inconsciente- la actividad delictiva) que normalmente no haría y que va a ocasionar un perjuicio económico, ya sea a él o a terceros. Entre ellos destaca cuantitativamente el fraude denominado phishing, junto a otros como las llamadas "cartas nigerianas", el scam y otras modalidades." (Téllez Valdez, 1996, pág. 108)

1.1.9. Delitos que se aprovechan de vulnerabilidades en el sistema.-

"Los delitos que se aprovechan de vulnerabilidades en el sistema requieren normalmente una habilidad mayor por parte del delincuente, ya que parten de la utilización (y en ocasiones creación) de programas que aprovechen los fallos de sistema de información para causar daños. Además, no requieren de la "colaboración" de la víctima, ya que ésta, sin haber omitido ninguna norma de seguridad, puede verse perjudicada a través de un tercero. En este grupo

podríamos situar al pharming y al más tradicional hacking. "(Téllez Valdez, 1996, pág. 108)

1.2 Principales delitos informáticos.-

Delitos informáticos: Son todos aquellos que son cometidos contra un sistema y los cometidos por medio de sistemas informáticos, o a los bienes jurídicos que se han relacionado con la información: datos, documentos electrónicos, cuentas bancarias, etc. Predominan:

> **Acceso no autorizado:** "El uso legítimo de contraseñas *(passwords)* y el ingreso a un sistema informático sin la autorización del propietario está tipificado como un delito, puesto que el bien jurídico que acostumbra a protegerse con la contraseña es lo suficientemente importante para que el daño producido sea grave." (Derecho Informático, 2012)
>
> **Destrucción de datos:** "Los daños causados en la red mediante la introducción de virus, bombas lógicas y demás actos de sabotaje informático no disponen en algunos países de preceptos que permitan su persecución." (Derecho Informático, 2012)
>
> **Infracción de los derechos de autor:** "La interpretación de los conceptos de copia, distribución, cesión y comunicación pública de los programas de ordenador utilizando la red provoca diferencias de criterio a nivel jurisprudencial. No existe una opinión uniforme sobre la responsabilidad del propietario de un servicio on-line o de un *sysop* respecto a las copias ilegales introducidas en el sistema. Mientras un tribunal condenó a un *sysop* porque en su BBS había imágenes *scaneadas* de la revista Playboy, en el caso *LaMacchia,* el administrador del sistema fue hallado no responsable de las copias de programas que albergaba su BBS. El recurso de los propietarios de sistemas on-line y BBS ha sido incluir una advertencia o una cláusula contractual que los exonera de responsabilidad frente a un *upload* de un programa o fichero que infrinja los derechos de autor de terceros." (Derecho Informático, 2012)

Intercepción de E-mail: "La violación de correspondencia, y la Intercepción de telecomunicaciones, de forma que la lectura de un mensaje electrónico ajeno reviste la misma gravedad." (Derecho Informático, 2012)

Estafas electrónicas: "Las compras electrónicas son un atractivo más para que aumente los casos de estafa, existiría un engaño a la persona que compra al distribuidor, al banco y/o al equipo principal encargado de la operación La proliferación de las compras telemáticas permite que aumenten también los casos de estafa.

Una de las cosas que proporciona la informática es poder realizar muchas tareas sin moverse de casa o la oficina. Esto supone que ya no existe un contacto directo entre las personas para acometer determinadas faenas. Como consecuencia de ello se ha producido un gran cambio en el mundo empresarial y de negocios, y, entre otras cosas, se han abierto nuevas perspectivas de consumo mediante el uso de Internet. Todos los que navegamos por Internet, conocemos que se venden cientos de productos, de diferentes marcas y modelos a través de la red, el ciberespacio se ha convertido en un nuevo sector a tener en cuenta para las empresas; lo cual es muy lógico, pues se ahorran muchos costos y amplían su potencial de mercado, Lógicamente todo depende del tipo de empresa de que se trate y del producto o servicio que venda, nos podemos encontrar con que la supuesta empresa nos manda productos que no son, no podemos reclamar directamente porque no sabemos dónde se ubica la empresa, o simplemente hemos hecho un pago con la tarjeta de crédito y no nos han dado el servicio o producto; todo esto afecta al consumidor, pero las empresas también pueden ser objeto en este comercio de una estafa, piénsese en dar número de tarjetas de crédito falsas pero que el robot acepta como válidas (conocido en el mundo de Internet como *"carding"*), etc. Con todo esto vemos que tanto empresas como consumidores pueden ser estafados usando medios informáticos. (Derecho Informático, 2012)

Se trataría en este caso de una dinámica comisiva que cumpliría todos los requisitos del delito de estafa, ya que además del engaño y el "*animus defraudandi*" existiría un engaño a la persona que compra. No obstante seguiría existiendo una laguna legal en países como el nuestro en el que nuestra legislación no prevea los casos en los que la operación se hace engañando al ordenador. (Derecho Informático, 2012)

Con todo lo anterior podemos definir la estafa informática como la "manipulación o alteración del proceso de elaboración electrónica de

cualquier clase y en cualquier momento de éste, realizada con ánimo de lucro y causando un perjuicio económico a un tercero" (Derecho Informático, 2012)

Transferencias de fondos: "Este es el típico caso en el que no se produce engaño a una persona determinada sino a un sistema informático ya sea por el mal uso de *passwords*, tarjetas electrónicas falsificadas, llaves falsas o adulterando el contenido de la información externamente calificando dicha conducta como robo; debería calificarse dicha conducta como robo, existe todavía una falta de uniformidad en la materia. Delitos Convencionales Todos los delitos que se dan sin el empleo de medios informáticos y que con la aparición de las rutas virtuales se están reproduciendo también en el ciberespacio. También los actos que no son propiamente delitos sino infracciones administrativas o ilícitos civiles: Predominan": (Derecho Informático, 2012)

Espionaje: "Se están presentando casos de acceso no autorizado a sistemas informáticos e intercepción de correo electrónico de entidades gubernamentales, entre otros actos que podrían ser calificados de espionaje si el destinatario final de esa información fuese un gobierno u organización extranjera, evidenciándose una vez más la vulnerabilidad de los sistemas de seguridad gubernamentales pro personas especializadas. Entre los casos más famosos podemos citar el acceso al sistema informático del Pentágono y la divulgación a través de Internet de los mensajes remitidos por el servicio secreto norteamericano durante la crisis nuclear en Corea del Norte en 1994, respecto a campos de pruebas de misiles. Aunque no parece que en este caso haya existido en realidad un acto de espionaje, se ha evidenciado una vez más la vulnerabilidad de los sistemas de seguridad gubernamentales". (Derecho Informático, 2012)

Terrorismo: "La presencia de equipos que encubren la identidad del remitente, convirtiendo el mensaje en anónimo, los servidores que ofrecen servicio de correos gratis permitiendo ingresar datos personales y direcciones ficticias para crear cuentas de correo que posteriormente aprovecharon personas o grupos terroristas para enviar amenazas, remitir consignas y planes de actuación ilícitos." (Derecho Informático, 2012)

Otros delitos: "Al igual que los narcotraficantes, se presentan los traficantes de armas, las sectas satánicas, entre otros, obteniendo las mismas ventajas que encuentran en Internet aprovechadas para la

planificación de los respectivos ilícitos que se están trasladando de lo convencional al ciberespacio o viceversa." (Derecho Informático, 2012)

Difusión de pornografía." En la mayoría de países así como en nuestro país es ilegal la comercialización de pornografía infantil o cualquier acto de pederastia. Un ejemplo de conducta activa sería remitir una recopilación de imágenes pornográficas *scaneadas a los mailbox* de un país en donde estuvieran también prohibidos los actos de difusión o comercialización de las mismas." (Derecho Informático, 2012)

Manipulación de los datos. "Este fraude conocido también como sustracción de datos, representa el delito informático más representativo ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos. De acuerdo a la información entregada por entidades de seguridad a nivel mundial, el 75% de los casos de sustracción de datos lo realiza personal interno de la organización o que pertenecieron." (Derecho Informático, 2012)

Manipulación de programas. "Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o rutinas. Uno de los métodos utilizados por las personas que tienen conocimientos especializados en programacion informática es el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal". (Derecho Informático, 2012)

Manipulación informática: "Es una alteración o modificación de datos, ya sea suprimiéndolos, introduciendo datos nuevos y falsos, colocar datos en distinto momento o lugar, variar las instrucciones de elaboración, etc.

Se diferencia en las estafas informáticas de las cometidas dentro del sistema y las cometidas fuera del sistema. Las primeras son las manipulaciones realizadas directamente sobre el sistema operativo, y no existe ningún engaño ni error sobre un ser humano. Las estafas cometidas fuera del sistema, son las manipulaciones de datos hechas antes, durante o después de la elaboración de los programas, siendo éstas las causantes del

engaño que determina de disposición patrimonial." (Derecho Informático, 2012)

1.2.1. Falsificaciones informáticas

Considerada como objeto cuando se trata de alterar datos de documentos almacenados en una computadora, en algunos casos se da al compartir directorios y con esto se permite que varios usuarios tengan acceso abriendo un riesgo en el sentido de que personas ajenas ingresen en forma fraudulenta a esta información. Para contrarrestar este acceso es necesario que los usuarios tengan conocimiento tanto de las ventajas como son el acceso siempre con claves, y las desventajas de esta herramienta, además de la adquisición inmediata de programas que ayuden a autentificar usuarios y ubicar las vulnerabilidades de la red.

Considerada como instrumento cuando las computadoras son utilizadas para efectuar falsificaciones de documentos. Esto puede darse con la ayuda de un escáner y de impresoras de alta calidad y no solo para modificarlos, sino incluso se pueden crear documentos falsos sin tener que utilizar uno original donde se necesita un experto para poder diferenciarlos de los documentos auténticos.

1.2.2. Sabotaje informático.-

Realizado por medio de cualquiera de estos métodos:

"**Virus.** Los virus son un grave problema, ya que a pesar de ser programas muy pequeños pueden hacer mucho, y más si se utiliza Internet como vía de infección. Un virus informático es un programa diseñado para que vaya de sistema en sistema, haciendo una copia de sí mismo en un fichero. Los virus se adhieren a cierta clase de archivos, normalmente *EXE y COM*, cuando estos ficheros infectados se transmiten a otro sistema éste también queda infectado, y así sucesivamente. Los virus entran en acción cuando se realiza una determinada actividad, como puede ser el que se ejecute un determinado fichero. Como hemos dicho los virus son programas, y para crearlos los programadores de virus utilizan kits de desarrollo de virus que se distribuyen por Internet, entre las que podemos destacar las siguientes: *Virus Creation Laboratories, Virus Factory, Virus Creation 2000, Virus C destruction Est, o The Windows virus Entine*. Por ello cualquiera que se haga con alguno de estos kits y sepa programación pueda crear sus propios virus, en este contexto no es raro que la estimación de los virus que existen en la actualidad sea de más de 7.000. Pueden ingresar en un sistema por la copia de un archivo infectado o por Internet que infectan algunos archivos de su sistema y lo pueden transmitir a otros equipos; En 1983 ya hablamos de las primeras referencias del virus. (Derecho Informático, 2012)

Gusanos. "Se fabrican de forma similar al virus con el objetivo de infiltrarlo en programas originales o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. Podría decirse que es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus, es decir, un programa gusano que posteriormente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita y luego destruirse." (Derecho Informático, 2012)

Bomba ilícita o cronológica." Exige conocimientos especializados ya que requiere programar la destrucción o modificación de datos en el futuro. Lo contrario de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso entre todos los dispositivos informáticos criminales, la bombas lógicas son las que poseen el máximo

potencial de daño. Su activación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. Puede utilizarse como material de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba."

Acceso no autorizado La corriente reguladora sostiene que el uso ilegítimo de *passwords* y la entrada en un sistema informático sin la autorización del propietario debe quedar tipificado como un delito, puesto que el bien jurídico que acostumbra a protegerse con la contraseña es lo suficientemente importante para que el daño producido sea grave. (Derecho Informático, 2012)

Piratas informáticos o *hackers*. "El acceso se efectúa a menudo desde un lugar exterior, recurriendo a uno de los diversos medios como son:

Aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema.

Los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.

En todos estos casos se producen pérdidas dinerarias provocadas por las conductas involucradas." (Derecho Informático, 2012)

1.3 Qué es el *Phishing*.-

El término *phishing* proviene de la palabra inglesa "*fishing"* (pesca), haciendo referencia al intento de hacer que los usuarios "piquen en el anzuelo" y se conviertan en víctimas.

A la persona que pone en práctica este delito se le conoce como *phisher*.

"El origen de este delito data de la década de los noventa, y su operativa se centraba en el envío de correos electrónicos fraudulentos a los clientes de entidades financieras. En un principio estos mensajes estaban mal redactados, con una burda traducción al español y con errores ortográficos, sin embargo, en la actualidad, su redacción es mucho más perfeccionada, por lo que consiguen conferir mayor credibilidad al mensaje." (Delitos Informáticos, 2012)

"La primera cita a la palabra *"phishing"* se puede encontrar en el popular grupo de noticias de hacking alt.2600 en enero de 1996, cuando varios delincuentes obtuvieron datos y contraseñas de usuarios de AOL (*America On Line)*. Este vocablo "*phishing"* fue acuñado por ser la contracción de *"Password Harvesting Fishing"*, literalmente "cosecha y pesca de contraseñas", donde se destaca que en su propio nombre no se menciona el método ni el objetivo para el cual esos datos son recolectados". (Derecho Informático, 2012)

"En 1997, esta técnica ya era ampliamente conocida y utilizada para obtener datos y comercializarlos en el mercado negro. En todos los casos analizados, se hace referencia al uso de técnicas de ingeniería social, donde se engaña y manipula psicológicamente a la víctima para que revele datos que no brindaría en circunstancias normales *(lure*). En estos casos, el engaño se efectúa a través del uso de cualquier medio de comunicación tecnológico como el teléfono, fax, correo electrónico, chat, SMS, etc. Más allá de lo expuesto, cabe aclarar que la dificultad en la conceptualización de esta técnica, viene relacionado a que su práctica y caracterización ha ido mutando constantemente." (Derecho Informático, 2012)

1.3.1 Funcionamiento del *Phishing*.-

Esta estafa consta de varias fases:

"En la primera, los estafadores, normalmente de países del este, y con grandes conocimientos técnicos, recaban de manera fraudulenta las claves de acceso online a cuentas bancarias, a través de múltiples

> métodos que a continuación analizaremos. Una vez disponen de las claves de acceso, retiran, de manera fraudulenta y sin consentimiento dinero de la cuenta bancaria de dicho usuario". (Delitos Informáticos, 2012)

Esta primera fase se trata de la obtención de información confidencial o sensible del usuario a través de las distintas técnicas. En este caso el delincuente hace contacto con la víctima a través de un medio de comunicación y, con un componente de ingeniería social, engaña al usuario para conseguir que este entregue voluntariamente información personal, como son, nombres de usuario, contraseña, número de cuenta bancaria, PIN de tarjetas de crédito y de débito.

Generalmente la forma más común de llevar adelante esta primera fase es a través del envío masivo de correo electrónico no deseado conocido como *spam,* a miles o millones de direcciones previamente recolectadas para que posteriormente el usuario ingrese a un sitio web de características similares al de una entidad de confianza del usuario y pueda colocar allí la información necesaria para que se concrete la segunda etapa. Es en este sentido que una importante cantidad de casos busca obtener los datos vinculados a aspectos financieros de la víctima y así concretar futuras estafas. Hay que destacar que esta primera fase no solo se la considera asociada exclusivamente al fraude informático.

> "Esta etapa inicial de captación ilegítima de datos, puede ser utilizada para obtener cualquier tipo de información de utilidad para

> el delincuente, tales como datos de autenticación *(login*), datos de una cuenta de red social, blog, cuenta bancaria o casilla de correo, incluso hasta información más puntual, como los secretos industriales de una empresa, que son obtenidos por el delincuente mediante trampas (engaños/*lure*) especialmente diseñadas para esos fines." (Derecho Informático, 2012)
>
> "En esta fase también es común la utilización de técnicas específicamente tecnológicas como los programas dañinos (malware) y la explotación de debilidades en el sistema operativo y aplicaciones instaladas por el usuario (vulnerabilidades o bugs) pero, al margen de la metodología aplicada, el objetivo sigue siendo la obtención de información de la víctima.
>
> En un análisis realizado durante 2011 por Segu-Info, se consultó sobre las entidades de las cuales es más común recibir correos electrónicos falsos. En este caso los sitios bancarios/financieros alcanzaron el primer puesto, seguidos muy de cerca por el *phishing* de redes sociales, los *webmail* y los sitios de compra/venta/subasta de productos". (Derecho Informático, 2012)
>
> "En una segunda fase, buscan a una persona que pueda poner a su disposición una cuenta bancaria (prefieren los Bancos antes que las Cajas de ahorro) para transferir a la misma el dinero que han sustraído. Esta persona tiene el papel de mulero (mulero bancario), que si bien es una víctima del engaño, coopera sin saberlo ni consentirlo en la estafa". (Delitos Informáticos, 2012)

Al concluir la primera fase que consiste en la captación de los datos del usuario, se procede a una segunda etapa, donde el delincuente se encuentra con un marco de posibilidades. Según datos estadísticos, se puede evidenciar que por lo general estos datos obtenidos son utilizados por el delincuente para obtener beneficios económicos perjudicando el patrimonio de la víctima, con el transcurso del tiempo esta actividad se ha ido desprendiendo de esta finalidad casi exclusiva, existiendo una serie de

otras opciones que se pueden realizar con los datos captados. Entre las opciones se encuentran: La venta de la información obtenida a otros delincuentes en el mercado negro.

> "En este caso la información cotiza de acuerdo al grado de plenitud y exactitud (no es lo mismo una base de datos con el nombre de usuario y contraseña que aquella que además contiene el número de tarjeta de crédito y su PIN)". (Derecho Informático, 2012)

- "Realización de transferencias de manera directa por el delincuente a cuentas propias (poco frecuente por su posibilidad de rastreo).
- Utilización de "mulas", aquellas personas que, de forma inocente y generalmente sin conocimiento, facilitan su cuenta bancaria para realizar movimientos de dinero obtenido de transacciones fraudulentas. Este tipo de acción, calificado como "lavado de dinero", generalmente se realiza a través de la captación de víctimas con ofertas de trabajos sencillos y demasiado bien remunerados ("trabaje 2 hs desde su casa y gane $5.800").
- Adquisición de bienes o servicios a través de canales virtuales que no soliciten la presencia del titular o de su documentación. En este tipo de fraude es común la compra de crédito para líneas de teléfono móvil. Esta actividad si se encuentra tipificada en Argentina (art. 173 inc. 16 CP).
- Ejecución de una "broma" a la víctima, donde se establecen comunicaciones o se generan perfiles falsos en su nombre. Esta actividad es muy común en los jóvenes y es generalmente llevada a cabo en las redes sociales y chats. No se encuentra tipificada en Argentina (aunque podría existir el delito de injurias para casos graves).
- Suplantación de identidad de la víctima, provocando un daño patrimonial - estafas- o personal -injuria, daños a la reputación, lesión al honor- en nombre de la víctima. Esta actividad no se encuentra tipificada en Argentina, excepto para casos de estafa, que opera como delito autónomo.
- Publicación de la información obtenida en Internet. En ocasiones, el delincuente se limita a captar ilegítimamente los datos para posteriormente "colgarlos" en la red, a sabiendas que su difusión

generará consecuencias en los medios y en la opinión pública sobre la empresa u organismo encargado de la seguridad de esos datos.

- Colección personal. Pueden existir casos donde el sujeto que capto la información, decida no utilizarla en ninguna de las alternativas descriptas, limitándose a recolectarlas de manera privada sin posterior uso." (Derecho Informático, 2012)

1.3.2 Partes.-

El delincuente, como sujeto activo, que con la utilización de un programa o *software* especializado planea y ejecuta la acción. Pueden existir otros sujetos intermediarios que colaboren en la ejecución que pueden ser incluidos en el mismo grupo delictivo."

Como sujeto pasivo se encuentra la entidad bancaria u organización gubernamental cuya imagen es tomada por el delincuente para llevar adelante la acción fraudulenta donde se produce un caso de suplantación de identidad para engañar al usuario.

También como sujeto pasivo el cliente o usuario afectado por la acción fraudulenta.

> "En cuanto al primer ítem, desde hace tiempo los delincuentes se han comenzado a agrupar en organizaciones delictivas (crimen organizado) y jerárquicas que les permite aprovechar la experiencia y técnica de cada una de las partes involucradas. En este sentido, el *FBI* ha tipificado al menos diez "profesiones o especializaciones" relacionadas con el cibercrimen: programadores, distribuidores, expertos, investigadores, defraudadores, proveedores de *hosting,* vendedores, muleros, blanqueadores y líderes. Una vez comprendida

> la acción criminal del agente activo, cabe preguntarse ¿existe responsabilidad por parte del cliente, por creer en el ardid o engaño? ¿Cuál es la responsabilidad de la entidad que presta un servicio, por no actuar parar prevenir la posible acción delictiva? Acción que es conocida, previsible y practicada en forma masiva en todo el mundo. (Derecho Informático, 2012)
>
> "La respuesta a estas preguntas no es sencilla y para contestarla INTECO entrevistó a distintos expertos que, si bien no coincidían en algunos detalles, acuerdan que existe responsabilidad compartida: "Tratándose de un fenómeno basado en la ingeniería social, el usuario ha de asumir cierta responsabilidad en este tema, manteniendo un comportamiento prudente y seguro a la hora de usar dichos servicios". (Derecho Informático, 2012)

1.3.3 Procedimiento.-

La víctima ingresa a ver su cuenta bancaria y descubre que alguien ha transferido dinero, sin su consentimiento, ni conocimiento, por lo que acude a su banco a pedir explicaciones o a la policía donde interpone una denuncia.

Es en ese momento en que se debería poner en marcha una investigación policial encaminada a determinar la relación de los hechos delictivos e identificar al autor o autores de la acción delictiva.

En algunos casos la transferencia sm consentimiento puede tener como destinatario al mulero, víctima ocasional que ha sido parte de la acción delictiva sin saberlo al utilizar sus datos personales o bancarios para realizar la acción, y estos mismo quedan identificados en el sistema informático de control de operaciones que utiliza el banco, por lo que al ser considerado como sospechoso

de haber participado en la acción fraudulenta lo llaman a declarar, estando en la obligación de demostrar su inocencia constituyéndose en una víctima más, y así evitar que cualquier futura sanción caiga contra él.

1.3.4 Modalidades de Phishing.-

Dentro de las modalidades de *phishing*, la más común que se utiliza para la recopilación fraudulenta de claves bancarias es el *Pharming* (simulación de entidad bancaria)

> "Los estafadores simulan o copian una pagina web de un banco *(pharming)* y realizan un *mailing* para que los posibles clientes del mismo accedan a dichas *url's* y faciliten sus datos de usuario mediante alguna excusa (actualización del sistema, verificación de datos, etc...)." (Derecho Informático, 2012)

El *mailing* es enviado a millones de usuarios al azar que pueden o no ser clientes del banco, ampliando las posibilidades de que algún cliente del banco pique el anzuelo, y proporcione sus datos en la web falsa.

El usuario, por tanto, recibe el mensaje de correo electrónico que parece proceder de una entidad bancaria de la que en muchos casos es cliente, y es víctima del engaño. Normalmente, en este correo electrónico se afirma que como medida de protección de los datos confidenciales o como consecuencia de algún cambio de los sistemas informáticos del banco, es necesario que el usuario

vuelva a introducir datos tales como números de cuentas bancarias y de taljetas de crédito, logins, contraseñas, números PIN, etc.

Dentro del texto del correo electrónico recibido figura una dirección de Internet, o más frecuentemente un *link* en el cual el usuario tiene que hacer *click* para acceder a un formulario donde debe introducir los datos solicitados.

El problema es que el servidor donde se encuentra este formulario no tiene nada tiene que ver el con la entidad bancaria, siendo estas páginas web creadas por hackers donde reciben directamente los datos confidenciales que la víctima ha introducido.

Con las claves bancarias, pueden transferirse el dinero sin ningún obstáculo.

> "Este método ha evolucionado ya que los estafadores son conscientes de que el usuario, al acceder al enlace establecido en el correo electrónico, queda al descubierto su verdadera *URL*, y el usuario puede entonces percatarse del engaño, de manera que en lugar de encontrarnos un enlace en el correo remitido por la supuesta entidad bancaria, nos encontramos con un archivo adjunto *html*." (Derecho Informático, 2012)
>
> "El usuario abre el archivo y complementa el formulario de recogida de datos, los cuales, viajan directamente al estafador, el cual puede operar en su cuenta libremente y sin que el propietario se percate.
>
> Esta técnica consiste en modificar el sistema de resolución de nombres de dominio *(DNS)* para conducir al usuario a una página web falsa.

Cuando un usuario teclea una dirección en su navegador, esta debe ser convertida a una dirección *I*P numérica. Este proceso es lo que se llama resolución de nombres, y de ello se encargan los servidores DNS." (Derecho Informático, 2012)

"Sin embargo, en la actualidad existen ejemplares de *malware* diseñados con la intención de modificar el sistema de resolución de nombres local, ubicado en un fichero denominado *HOSTS*.

Este fichero permite almacenar de forma local esa resolución de nombres asociadas a direcciones IP. De esta manera, aunque el usuario introduzca en el navegador el nombre de una página web legítima, el ordenador primero consultará a ese fichero HOSTS si existe una dirección IP asociada a ese nombre. En caso de no encontrarla, lo consultará con el servidor DNS de su proveedor.

Esta técnica conocida como *pharming* es utilizada normalmente para realizar ataques de *phishing*, redirigiendo el nombre de dominio de una entidad de confianza a una página web, en apariencia idéntica, pero que en realidad ha sido creada por el atacante para obtener los datos privados del usuario, generalmente datos bancarios.

A diferencia del *phishing*, el *pharming* no se lleva a cabo en un momento concreto, ya que la modificación del fichero *HOSTS* permanece en un ordenador, a la espera de que el usuario acceda a su servicio bancario." (Modalidades de Phishing - Pharming, 2012)

1.3.4.1 Phishing engañoso – Deceptive Phishing.-

"Esta es la forma primitiva de phishing. Aunque en sus inicios (cuando el objetivo básico era la captura de cuentas de AOL) la herramienta de comunicación utilizada eran las aplicaciones de mensajería instantánea, en la actualidad la forma más habitual de desarrollar este tipo de delito (o al menos de iniciarlo) es mediante el coneo electrónico. Precisamente, un típico ataque de esta variedad de phishing conlienza cuando el phisher envía un correo electrónico falso". (Modalidades de Phishing -Pharming, 2012)

1.3.4.2. Vishing

> "El *vishing* utiliza el teléfono como herramienta. Se basa en el uso de un tipo de software denominado *"war dialers"* cuya función es realizar la marcación de teléfonos desde un ordenador, utilizando la tecnología de telefonía sobre IP. Una vez que el usuario atacado descuelga se activa una grabación que trata de convencerle o bien de que visite un sitio web para dar sus datos personales o bien de que directamente "confirme" sus datos en la misma llamada. El verdadero problema de este tipo de ataques es la confianza que la población tiene en el teléfono y en el uso que tradicionalmente han hecho de él las empresas legítimas". (Modalidades de Phishing - Pharming, 2012)

CAPÍTULO 2.- -ANÁLISIS SOBRE LAS DIFERENCIAS ENTRE PHISHING, ESTAFA Y MANIPULACIÓN INFORMÁTICA

2. Phishing.-

> "Proviene de la palabra inglesa "fishing" (pesca), haciendo alusión al intento de hacer que los usuarios "piquen en el anzuelo" y se conviertan en víctimas". (Delitos Informáticos, 2012)

De acuerdo con el documento publicado por el *Financial Services Technology Consortium* -FSTC- lo que diferencia al *phishing* de otros tipos de fraude es que combina cuatro elementos fundamentales:

i) "Ingeniería social: El *phishing* explota las debilidades de los individuos para engañarles y hacer que actúen contra sus propios intereses.
ii) Automatización: Las tecnologías de la información son utilizadas para desarrollar los ataques de *phishing* de forma masiva.

iii) Comunicación electrónica: Usan redes de comunicación, especialmente Internet.

iv) Suplantación: Un ataque de *phishing* requiere que los delincuentes suplanten a una empresa legítima o a una agencia gubernamental." (Evolución del *Phishing,* 2012)

- A la persona que pone en práctica este delito se le conoce como *phisher.*
- El origen de este delito data de la década de los noventa, y su operativa se centraba en el envío de correos electrónicos fraudulentos a los clientes de entidades financieras.
- consta de varias fases:

2.1 Primera Fase.-

- Los ciberdelincuentes de manera fraudulenta recaban las claves de acceso online a cuentas bancarias, a través de múltiples métodos.
- Una vez disponen de las claves de acceso, retiran, de manera fraudulenta y sin consentimiento consentida dinero de la cuenta bancaria de dicho usuario.
- La forma más tradicional de llevar adelante esta etapa es realizar el envío masivo de correo electrónico no deseado -*spam*-
- Esta etapa inicial de captación ilegítima de datos, puede ser utilizada para obtener todo tipo de información de utilidad para el delincuente, como son: Datos de autenticación *(login),* datos de una cuenta de red social, blog, cuenta bancaria o casilla de correo, llegando hasta información más puntual, como los secretos industriales de una empresa

2.1.1 Segunda Fase.-

- Se concentran en buscar a una persona que pueda poner a su disposición una cuenta bancaria.
- Esta persona tiene el papel de mulero (mulero bancario), que si bien es una víctima del engaño, coopera sin saberlo ni consentirlo en la estafa.

2.1.2 Partes.-

- **Sujeto Activo:** El ciberdelicuente que realiza la estafa electrónica o programa algún software para la captación y *pesca (phishing)* que son necesarios para culminar la estafa.
- **Sujeto Pasivo:** La entidad bancaria u organización gubernamental cuya imagen es tomada por el delincuente para llevar adelante la acción fraudulenta.
- El mulero como elemento esencial que coopera sin saberlo y se convierte en víctima.
- El cliente o usuario afectado que ha sido engañado.

2.1.3 Conducta.-

La persona que mediante engaños y a través de medios informáticos como son emails, *spam,* y todo tipo de software que parecen auténticos remita a los usuarios a páginas web fraudulentas, para conseguir que proporcionen información personal como nombres de usuario, contraseñas, números de cuenta, direcciones, números de identificación personal (PIN), con el fin de usurpar la identidad de la víctima y sacar dinero de su cuenta bancaria, organizar subastas online, solicitar tarjetas de crédito, pedir préstamos, blanquear dinero y llevar a cabo diferentes actividades ilegales online.

2.2. Estafa.-

> "Delito genérico de defraudación que se configura por el hecho de causar a otro un perjuicio patrimonial, valiéndose de un engaño, tales como el uso de nombre supuesto, de calidad simulada, falsos títulos, influencia mentida, abuso de confianza o ficción de bienes, crédito, comisión, empresa o negociación" (Delitos Informáticos, 2012)

Nuestro Código Penal define a la estafa dentro del artículo 335 bajo los siguientes parámetros.

> Artículo 335°.- (Estafa). "El que con la intención de obtener para sí o un tercero un beneficio económico indebido, mediante engaños o artificios provoque o fortalezca error en otro que motive la realización de un acto de disposición patrimonial en perjuicio del sujeto en error o de un tercero, será sancionado con reclusión de uno

(1) a cinco (5) años y con 1973, multa de sesenta (60) a doscientos (200) días,. (Codigo. Penal, Gaceta oficial de Bolivia)

- La prueba del engaño debe basarse en documentos, testimonios y pericias
- Es necesario conocer bien el engaño y sus medios de prueba para ser admitidos por el fiscal y el juez.
- Generalmente la víctima puede establecer quién es el estafador al haber tenido algún tipo de relación o contacto que llevó posteriormente al engaño.
- A diferencia del *phishing* no existe la figura del mulero.

2.2.1 Código Penal Boliviano.-

Artículo 335°.- (Estafa). "El que con la intención de obtener para sí o un tercero un beneficio económico indebido, mediante engaños o artificios provoque o fortalezca error en otro que motive la realización de un acto de disposición patrimonial en perjuicio del sujeto en error o de un tercero, será sancionado con reclusión de uno (1) a cinco (5) años y con multa de sesenta (60) a doscientos (200) días". (Código Penal, 1973, Gaceta oficial de Bolivia)

Artículo 363 bis.- (Manipulación Informática). "El que con la intención de obtener un beneficio indebido para sí o un tercero, manipule un procesamiento o transferencia de datos informáticos que conduzca a un resultado incorrecto o evite un proceso tal cuyo resultado habría sido correcto, ocasionando de esta manera una transferencia patrimonial en perjuicio de tercero, será sancionado

con reclusión de uno (1) a cinco (5) años y con multa de sesenta (60) a doscientos (200) días". (Código Penal, 1973, Gaceta oficial de Bolivia)

- Define al sujeto que manipula un procedimiento para sacar un beneficio.
- El *Phishing* no manipula el procedimiento ya que es un software especializado creado específicamente para generar la estafa.
- El artículo sanciona la manipulación de datos informáticos o económicos.
- El *Phishing* consta de varias fases que son conductas delictivas:

  a) La captación y pesca de víctimas a través de un software especializado que genera el engaño a los usuarios.

  b) El robo de la información, ya sea para su uso o para ser vendido en el mercado negro online, para la comisión de otros delitos (robo de identidad, pornografía, suplantación, terrorismo, muleros)

  c) En el *phishing* siempre existen víctimas múltiples (El usuario que ha sido engañado, la entidad a la cual se ha tomado su imagen para engañar, el mulero que actúa sin saberlo ayudando a traspasar los datos el dinero a través de su cuenta bancaria o bases de datos personales
- El *phishing* tiene como particularidad que la acción realizada por el delincuente puede consumarse en estafa o simplemente quedarse en robo de datos, dependiendo el uso que le dé a los mismos, puede ser en

beneficio del ciberdelincuente o de un tercero, así como de varias personas u organizaciones.

- Finalmente como característica principal que el *phishing* para poder consumarse, se lo hace a través de un software especializado para este tipo de acciones, que puede ser creado por un especialista, pero utilizado por otra persona, o programado en favor de un tercero, que necesariamente debe tomar la imagen de una empresa u organización que sufre de la suplantación de su identidad para la realización de la acción fraudulenta.

CAPITULO 3.- SOLUCIONES NORMATIVAS QUE LA LEGISLACIÓN DE DISTINTOS PAÍSES, ASÍ COMO LOS CONVENIOS INTERNACIONALES OFRECEN PARA LOS DAÑOS QUE PROVOCA EL PHISHING COMO DELITO INFORMÁTICO.

3. Las conductas o acciones que considera las Naciones Unidas como delitos informáticos.-

Las Naciones Unidas considera como delitos informáticos a las siguientes conductas:

> I) "Los Fraudes cometidos mediante manipulación de computadoras: este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más comun.
>
> II) La manipulación de programas; este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas que tienen conocimiento especializados en programación informática.
>
> III) La Manipulación de datos de salida; se efectúa fijando un objetivo al funcionamiento del sistema informático, el ejemplo más común es el fraude que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos.
>
> IV) Fraude efectuado por manipulación informáticas de los procesos de cómputo.
>
> V) Falsificaciones informáticas; cuando se alteran datos de los documentos almacenados en forma computarizada.

VI) Como instrumentos; las computadoras pueden utilizarse también para efectuar falsificación de documentos de uso comercial.

VII) Sabotaje Informático; es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema.

VIII) Los Virus; Es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos.

IX) Los Gusanos; los cuales son análogos al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse.

X) La Bomba lógica o cronológica; la cual exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro.

XI) Acceso no autorizado a servicios u sistemas informáticos; esto es por motivos diversos desde la simple curiosidad, como en el caso de muchos piratas informáticos *(hackers)* hasta el sabotaje o espionaje informático.

XII) Piratas Informáticos o *Hackers*; este acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones.

XIII) Reproducción no autorizada de programas informáticos de protección legal; la cual trae una pérdida económica sustancial para los propietarios legítimos. "(Peritaje Informática, 2012)

3.1. Resolución 55/63 de las Naciones Unidas.-

Las Naciones Unidas emiten en el año 2000 la Resolución 55/63 destinada a combatir el uso delictivo de las tecnologías de la información, planteando a los Estados miembros una serie de necesidades que cubrir, considerando una lista de medidas:

- Los Estados deben asegurarse de que su ordenamiento y práctica jurídicos eliminen los resquicios seguros para los delincuentes informáticos.
- La cooperación entre las Fuerzas de Seguridad de los diferentes países para la investigación y persecución de los delitos informáticos debe ser coordinada entre todos los Estados afectados.
- Los Estados deben intercambiar información acerca de los problemas que afrontan a la hora de combatir los delitos informáticos. Las Fuerzas de Seguridad deben estar preparadas, equipadas y formadas para identificar los delitos informáticos.
- Los ordenamientos jurídicos deben proteger la confidencialidad, integridad y disponibilidad de los datos y los sistemas de información frente a los ataques y asegurarse de que los delitos son perseguidos.
- Los ordenamientos jurídicos deben permitir el mantenimiento y el acceso rápido a los datos relativos a investigaciones criminales en curso.
- Los sistemas de cooperación deben asegurar la información rápida de los delitos informáticos y la recopilación y puesta en común inmediata de las evidencias existentes en estos casos.
- Hay que hacer que la opinión pública tome conciencia de la necesidad de prevenir y combatir los delitos informáticos.
- Hasta donde sea posible, las Tecnologías de la Información y las Comunicaciones deben ser diseñadas de forma que permitan

> prevenir y detectar el uso delictivo, perseguir al criminal y recopilar pruebas. (Peritaje Informática, 2012)

3.2. Derecho Comparado.-

Respecto a la tipificación del phishing en diferentes países, es necesario utilizar como marco comparativo lo establecido por otras legislaciones. En ese sentido, que en general se puede encontrar una buena cantidad de países que ya han emitido normas con el fin de tipificar el fraude informático.

> Entre las legislaciones más modernas se puede citar la Ley sobre "Crímenes y Delitos de Alta Tecnología de República Dominicana", norma especial a destacar por la seriedad en el tratamiento de los delitos informáticos, donde incluso se regula aspectos de derecho procesal penal para combatir el cibercrimen. En el texto de la misma, se encuentran los artículos 14 y 15 donde se regula la obtención ilícita de fondos, así como su transferencia electrónica y la estafa informática. (Seguridad de la Información, 2012)

Dentro de la clasificación, sobre el *Phishing*, se puede evidenciar que algunos países van más allá de la tipificación del fraude informático, si no que incorporan la captación ilegítima de datos.

> "En esta postura se puede citar legislaciones también actuales como Colombia, en cuyo art. 269F sanciona a quien "sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes". En el artículo siguiente (art. 269G), la misma norma sanciona a quien "con objeto ilícito y sin estar facultado para ello,

diseñe, desarrolle, trafique, venda, ejecute, programe envíe páginas electrónicas, enlaces o ventanas emergentes".

Regulaciones más precisas en esta segunda tendencia, las podemos localizar dentro de los EE.UU., como por ejemplo en New York, en cuya Anti-*phishing* se sanciona:

A cualquier persona que, a través de medios electrónicos, solicite, requiera o colecte información personal para representar de manera engañosa, a una empresa u organismo del gobierno, sin contar con su autorización". (Seguridad de la Información, 2012)

Similar redacción posee el Código de Illinois, donde:

"It is unlawful for any person, by means of a Web page, electronic mail message, or otherwise through use of the Internet, to solicit, request, or take any action to induce another person to provide identifying information by representing himself, herself, or itself to be a business without the authority or approval of the business". ("Es ilegal que cualquier persona, a través de una página Web, mensajes de correo electrónico o de otra manera a través del uso de la Internet, realice una solicitud, o r cualquier acción de inducir a otra persona a proporcionar información de identificación mediante la representación de sí mismo, ella misma, o sí es un negocio sin la autorización o aprobación de la empresa ".) (Derecho Informático, 2012)

"Entre sus diferencias se puede observar la inclusión de las personas físicas como sujeto pasivo del delito, así como la ampliación en los verbos, al incluir a "cualquier acción que induzca a una persona a proveer su identificación personal". (Seguridad de la Información, 2012)

3.3. Convenio de Cibercriminalidad de Budapest.-

Este Convenio de Cibercriminalidad de Budapest, fue adoptado por el Comité de Ministros del Consejo de Europa en el año 2001, con la intención de concretar una sola corriente dentro las legislaciones de los estados miembros

para la regulación de los delitos informáticos. Este Convenio consta de 47 miembros y 8 observadores y se encuentra abierta a otros países como Australia, Japón, Canadá, Sudáfrica y los EE.UU. Se pretende mediante este acuerdo regular todas las áreas relevantes de la legislación sobre ciberdelincuencia (derecho penal, derecho procesal y cooperación internacional), tratando con carácter prioritario la construcción de una política penal de cooperación internacional contra la ciberdelincuencia.

> "Actualmente varios países están en vías de adhesión y por lo tanto deben tener en consideración sus lineamientos, dado que desde la fecha de aprobación se computa un plazo donde el nuevo país miembro debe adecuarse a dicho instrumento.
>
> Entre algunos de los aspectos a adecuar en materia de derecho penal material, se encuentra el tema tópico de esta investigación. En relación al mismo se destaca el art. 6 del Convenio, que expresa":
>
> "Artículo 6. Abuso de equipos e instrumentos técnicos
>
> 1. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, las siguientes conductas cuando éstas sean cometidas dolosamente y sin autorización:
>
> a. la producción, venta, obtención para su utilización, importación, difusión u otras formas de puesta a disposición
>
> 1. De un dispositivo, incluido un programa informático, principalmente concebido o adaptado para permitir la comisión de una de las infracciones establecidas en los artículos 2 a 5 arriba citados
>
> 2. De una palabra de paso (contraseña), de un código de acceso o de datos informáticos similares que permitan acceder a todo o parte de un sistema informático, con la intención de utilizarlos como medio para cometer alguna de las infracciones previstas en los artículos 2 a

> 5; y b. la posesion de alguno de los elementos descritos en los parágrafos (a) (1) o (2) con la intención de utilizarlos como medio para cometer alguna de las infracciones previstas en los artículos 2-5.Los Estados podrán exigir en su derecho interno que concurra un determinado número de elementos para que nazca responsabilidad penal". (Seguridad de la Información, 2012)

Los delitos informáticos hoy en día constituyen un gran vacío jurídico en nuestra legislación. Es por eso que a través del derecho comparado que se nos permite evidenciar como otros países han tomado medidas sobre el asunto, demostrándonos la necesidad de un análisis urgente por parte de nuestros legisladores para considerar la regulación urgente y adecuada para enfrentarse con el problema y proporcionar seguridad jurídica a los usuarios de la intemet.

> "Se ha dicho que algunos casos de abusos relacionados con la informática deben ser combatidos con medidas jurídico-penales. No obstante, para aprehender ciertos comportamientos merecedores de pena con los medios del Derecho penal tradicional, existen, al menos en parte, relevantes dificultades. Estas proceden en buena medida, de la prohibición jurídico-penal de analogía y en ocasiones, son insuperables por la vía jurisprudencial. De ello surge la necesidad de adoptar medidas legislativas.
>
> En los Estados industriales de Occidente existe un amplio consenso sobre estas valoraciones, que se refleja en las reformas legales de los últimos diez años". (Seguridad de la Información, 2012)

3.3.1. Alemania.-

En Alemania, para poder hacer frente a la delincuencia relacionada con los delitos informáticos a partir del 1 de agosto de 1986, se adoptó la Segunda Ley

contra la Criminalidad Económica del 15 de mayo de 1986 en la que se contemplan los siguientes delitos:

Espionaje de datos (202)

Estafa informática (263)

> Falsificación de datos probatorios (269) junto a modificaciones complementarias del resto de falsedades documentales como el engaño en el tráfico jurídico mediante la elaboración de datos, falsedad ideológica, uso de documentos falsos (270, 271, 273) (Seguridad de la Información, 2012)
>
> Alteración de datos (303 a) es ilícito cancelar, inutilizar o alterar datos inclusive la tentativa es punible.
>
> Sabotaje informático (303 b).destrucción de elaboración de datos de especial significado por medio de destrucción, deterioro, inutilización, eliminación o alteración de un sistema de datos. También es punible la tentativa.
>
> Utilización abusiva de cheques o tarjetas de crédito (266b (Seguridad de la Información, 2012)

3.3.2. Argentina.-

En Argentina, el *phishing* fue tipificado en junio de 2008, a través del art. art. 9 de la Ley Nº 26.388.

> "Art. 9º - Incorporase como inciso 16 del artículo 173 del Código Penal, el siguiente:
>
> Inciso 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" (Derecho Informático, 2012)

"De acuerdo a los artículos citados, el *phishing* estaría regulado en Argentina en el inciso 16 del art. 173, por lo tanto, sería un tipo especial de la estafa clásica del art. 172. Siendo así, es menester consultar la doctrina clásica penal del delito de estafa, para así saber cuándo quedará configurado el tipo. Citando la impecable explicación del destacado penalista Edgardo Donna, quien afirma que:

"En la estafa el bien jurídico no es, como podría pensarse, la "buena fe en el tráfico" o la "lealtad en las operaciones" sino el patrimonio. El ardid y engaño previstos en el tipo como formas de comisión constituyen simplemente los medios con los que se produce el daño patrimonial del sujeto pasivo, de modo que el quebrantamiento de la buena fe es el modus operandi que va a determinar la lesión jurídica patrimonial, pero no el objeto de la tutela, ni directa ni indirectamente. Si la buena fe fuese el bien jurídico amparado, la consumación del delito debería producirse con la sola realización del engaño, sin necesidad de que ocasione perjuicio patrimonial alguno, solución que resulta inaceptable desde el punto de vista legal". (Seguridad de la Información, 2012)

"En relación a lo expuesto, se precisa que para la configuración del delito de estafa y por lo tanto, del tipo especial del inc. 16 para "*phishing",* debe existir primero el ardid o engaño y luego un perjuicio patrimonial consecuencia de dicho engaño." (Seguridad de la Información, 2012)

"En la descripción realizada sobre el funcionamiento del *phishing*, se ha señalado la proliferación de personas dedicadas exclusivamente a la captación ilegítima de datos confidenciales *(phishing* propiamente dicho según el concepto defendido en este trabajo), pero que luego optan por otras alternativas diferentes a la estafa tradicional a la víctima. Es decir, la mayoría de los casos de *phishing,* actualmente no son delito en Argentina, puesto que según la estrategia jurídica utilizada por el legislador, se exigen los elementos típicos de la estafa, y por consiguiente, se necesita que exista perjuicio patrimonial para que exista delito" (Seguridad de la Información, 2012)

3.3.3 Austria.-

Ley de reforma del Código Penal de 22 de diciembre de 1987

Esta ley contempla los siguientes delitos:

> "Destrucción de datos (126). En este artículo se regulan no sólo los datos personales sino también los no personales y los programas.
>
> Estafa informática (148). En este artículo se sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el curso del procesamiento de datos. Además contempla sanciones para quienes cometen este hecho utilizando su profesión". (Seguridad de la Información, 2012)

3.3.4. Chile.-

Cuenta con una ley relativa a Delitos Informáticos, promulgada en Santiago de Chile el 28 de mayo de 1993, la cual en sus cuatro numerales menciona:

> "Artículo 1° "El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo".
>
> Artículo 2° " El que con el ánimo de apoderarse, usar o conocer ndebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio".

Artículo 3° " El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado".

Artículo 4° " El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado". (Seguridad de la Información, 2012)

3.4.5. Estados Unidos.-

En 1994 adoptan el Acta Federal de Abuso Computacional (18 U.S.C. Sec 1030), modificando el Acta de 1986.

"Aquí se contempla la regulación de los virus *(computer contaminant*) conceptualizándolos aunque no los limita a los comúnmente llamados virus o gusanos sino que contempla a otras instrucciones designadas a contaminar otros grupos de programas o bases de datos.

Modificar, destruir, copiar, transmitir datos o alterar la operación normal de las computadoras, los sistemas o las redes informáticas es considerado delito. Así, esta ley es un acercamiento real al problema, alejado de argumentos técnicos para dar cabida a una nueva era de ataques tecnológicos. (Seguridad de la Información, 2012)

El FCIC *(Federal Computers Investigation Commitee),* es la organización más importante e influyente en lo referente a delitos computacionales: los investigadores estatales y locales, los agentes federales, abogados, auditores financieros, programadores de seguridad y policías de la calle trabajan allí comunitariamente. El

FCIC es la entrenadora del resto de las fuerzas policiales en cuanto a delitos informáticos, y el primer organismo establecido en el nivel nacional.

Además existe la Asociación Internacional de Especialistas en Investigación Computacional (IACIS), quien investiga nuevas técnicas para dividir un sistema en sus partes sin destruir las evidencias. Sus integrantes son "forenses de las computadoras" y trabajan, además de los Estados Unidos, en el Canadá, Taiwán e Irlanda." (Seguridad de la Información, 2012)

3.4.6. Francia.-

La Ley 88/19 del 5 de enero de 1988 sobre el fraude informático contempla:

"Acceso fraudulento a un sistema de elaboración de datos. Se sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la sanción si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema.

Sabotaje Informático. Falsear el funcionamiento de un sistema de tratamiento automático de datos.

Destrucción de datos. Se sanciona a quien intencionalmente y con menosprecio de los derechos de los demás introduzca datos en un sistema de tratamiento automático de datos, suprima o modifique los datos que este contiene o los modos de tratamiento o de transmisión.

Falsificación de documentos informatizados. Se sanciona a quien de cualquier modo falsifique documentos informatizados con intención de causar un perjuicio a otro. (Seguridad de la Información, 2012)

3.4.7. Inglaterra.-

Luego de varios casos de hacking surgieron nuevas leyes sobre delitos informáticos. En agosto de 1990 comenzó a regir la *Computer Misuse Act* (Ley de Abusos Informáticos).

> "Cualquier intento, exitoso o no de alterar datos informáticos con intención criminal se castiga con hasta cinco años de cárcel o multas sin límite.
>
> El acceso ilegal a una computadora contempla hasta seis meses de prisión o multa de hasta dos mil libras esterlinas.
>
> El acta se puede considerar dividida en tres partes: *hackear* (ingresar sin permiso en una computadora), hacer algo con la computadora *hackeada* y realizar alguna modificación no autorizada.
>
> El último apartado se refiere tanto al *hacking* (por ejemplo, la modificación de un programa para instalar un *backdoor)*, la infección con virus o, yendo al extremo, a la destrucción de datos como la inhabilitación del funcionamiento de la computadora.
>
> Bajo esta ley liberar un virus es delito y en enero de 1993 hubo un raid contra el grupo de creadores de virus. Se produjeron varios arrestos en la que fue considerada la primera prueba de la nueva ley en un entorno real." (Seguridad de la Información, 2012)

3.4.8. Italia.-

Se configura exclusivamente en caso de sistemas informáticos y telemáticos protegidos por dispositivos de seguridad (contraseñas o llaves de hardware) que indiquen claramente la privacidad del sistema y la voluntad del derechohabiente de reservar el acceso a aquél sólo a las personas autorizadas. La comisión de este delito se castiga con reclusión de hasta tres años, previendo agravantes.

> "Abuso de la calidad de operador de sistemas. Este delito es un agravante al delito de acceso abusivo y lo comete quien tiene la posibilidad de acceder y usar un sistema informático o telemático de manera libre por la facilidad de la comisión del delito.
>
> Introducción de virus informáticos. Es penalmente responsable aquel que cree o introduzca a una red programas que tengan la función específica de bloquear un sistema, destruir datos o dañar el disco duro, con un castigo de reclusión de hasta dos años y multas considerables.
>
> Fraude Informático.- Cuando por medio de artificios o engaños, induciendo a otro a error, alguien procura para sí o para otros un injusto beneficio, ocasionando daño a otro. También se entiende como tal la alteración del funcionamiento de sistemas informáticos o telemáticos o la intervención abusiva sobre datos, informaciones o programas en ellos contenidos o pertenecientes a ellos, cuando se procure una ventaja injusta, causando daño a otro. La punibilidad de este tipo de delito es de meses a tres años de prisión, más una multa considerable.
>
> Intercepción abusiva.- Es un delito que se comete junto con el delito de falsificación, alteración o supresión de comunicaciones telefónicas o telegráficas. Asimismo, es la intercepción fraudulenta, el impedimento o intrusión de comunicaciones relativas a sistemas informáticos o telemáticos, además de la revelación al público,

mediante cualquier medio, de la información, de esas publicaciones; este delito tiene una punibilidad de 6 meses a 4 años de prisión. Asimismo, se castiga el hecho de realizar la instalación de equipo con el fin anterior.-

Falsificación informática. Es la alteración, modificación o borrado del contenido de documentos o comunicaciones informáticas o telemáticas. En este caso, se presupone la existencia de un documento escrito (aunque se debate doctrinariamente si los documentos electrónicos o virtuales pueden considerarse documentos escritos). En este caso, la doctrina italiana tiene muy clara la noción de "documento informático", al cual define como cualquier soporte informático que contenga datos, informaciones o programas específicamente destinados a elaborarlos.

Espionaje Informático.- Es la revelación del contenido de documentos informáticos secretos o su uso para adquirir beneficios propios, ocasionado daño a otro.

Violencia sobre bienes informáticos. Es el ejercicio arbitrario, con violencia, sobre un programa, mediante la total o parcial alteración, modificación o cancelación del mismo o sobre un sistema telemático, impidiendo o perturbando su funcionamiento.

Abuso de la detentación o difusión de Códigos de acceso (contraseñas).

Violación de correspondencia electrónica, la cual tiene agravantes si causare daños." (Seguridad de la Información, 2012)

IV CONCLUSIONES Y RECOMENDACIONES.-

Dentro del objetivo específico N°1 "Conocer que se entiende por *Phishing*, como delito informático y su relevancia jurídica" se llegaron a las siguientes conclusiones:

Los avances que se han experimentado en el marco de la información y la tecnología en los últimos años, han proporcionado a las personas nuevos medios para desarrollar sus actividades generando beneficios tanto en lo individual como en lo colectivo.

Del mismo modo que muchas actividades, aplicaciones y funciones se han trasladado al mundo de la Internet, creando facilidades y comodidades para el usuario, lamentablemente este mismo desarrollo tecnológico específicamente en el campo de la Internet, ha supuesto un nuevo entorno para la delincuencia.

Justamente al otorgar facilidades y ventajas para el usuario, ha ayudado a potencializar los nuevos métodos delincuenciales, produciendo un avance y una evolución de las estafas tradicionales bajo una nueva perspectiva más sofisticada. Este es el caso del *Phishing*.

Es en ese sentido que la proliferación de los delitos informáticos se ha producido en gran escala en esta última década.

Según el Instituto de Investigación Nacional de Tecnologías de la Información- INTECO, en Madrid España, la mayor parte de los juristas consideran necesaria una tipificación específica de estos delitos, siendo el camino seguido no sólo por el ordenamiento penal español, sino por la mayoría de los correspondientes penales de los demás países.

El impacto de delitos como el *Phishing* es grave, no solo por las pérdidas que ocasiona a la víctima, sino por el hecho de generar desconfianza hacia la Internet e inseguridad de sus usuarios, afectando los movimientos de la economía digital.

Dentro del objetivo específico N°2 "Determinar las diferencias entre *Phishing,* Estafa y Manipulación Informática" se llegaron a las siguientes conclusiones:

Sus características son muy particulares ya que para poder consumarse el tipo penal, se deben combinar cuatro elementos fundamentales:

- Generar un procedimiento conocido como ingeniería social, que consiste en explotar las debilidades de los usuarios de la Internet, haciendo que actúen contra sus propios intereses.

- Realizar esta operación a través de un software o programa especializado para desarrollar este tipo de ataques de forma masiva y haciéndolo automatizado por este programa.
- Se debe usar un medio de comunicación, especialmente la Internet o los mensajes de texto en el celular.
- Finalmente requiere que los delincuentes suplanten la identidad de una empresa legítima o una organización gubernamental.

Los partes que componen el tipo penal son:

- **Sujeto Activo:** El ciberdelicuente que realiza la estafa electrónica o programa algún software para la captación y pesca *(phishing)* que son necesarios para culminar la estafa.
- **Sujeto Pasivo:** La entidad bancaria u organización gubernamental cuya imagen es tomada por el delincuente para llevar adelante la acción fraudulenta.
- El mulero como elemento esencial que coopera sin saberlo y se convierte en víctima.
- El cliente o usuario afectado que ha sido engañado.

La conducta específica de este delito es:

"L a persona que mediante engaños y a través de medios informáticos com0 son emails, spam, y todo tipo de software que parecen auténticos remita a los usuanos a páginas web fraudulentas, para conseguir que proporcionen información personal como nombres de usuario contraseñas números de cuenta, direcciones, números de identificación personal (PIN), con el fin de usurpar la identidad de la víctima y sacar dinero de su cuenta bancaria, organizar subastas online, solicitar tarjetas de crédito, pedir préstamos, blanquear dinero y llevar a cabo diferentes actividades ilegales online."

Son estas sus características particulares del *Phishing,* que ayudan a diferenciarlo de delitos como la Estafa o la Manipulación Informática, que se encuentran tipificados dentro de nuestra normativa.

Dentro del objetivo específico N° 3 "Analizar las soluciones normativas que las legislaciones de distintos países, así como los convenios internacionales ofrecen para prevenir los daños que provoca el *Phishing* como delito informático" se llegaron a las siguientes conclusiones:

Haciendo un análisis comparativo con otras legislaciones, así como la normativa internacional, podemos ver que existen gran cantidad de países como Alemania, Argentina, Austria, Chile, Estados Unidos, Francia, Inglaterra e Italia,

entre otros, que ya han regulado en sus normativas internas la figura del tipo penal del *Phishing,* considerándolo como un nuevo medio de fraude o estafa, que afecta a los intereses de sus ciudadanos.

También podemos tomar en cuenta la Resolución N°55/63 de las Naciones Unidas emitida en el año 2000, donde en busca de generar un carácter preventivo y cubrir las necesidades de los Estados miembros, sugiere entre otras cosas:

- Los Estados deben asegurarse de que su ordenamiento y práctica jurídicos eliminen los resquicios seguros para los delincuentes informáticos.
- Los ordenamientos jurídicos deben proteger la confidencialidad, integridad y disponibilidad de los datos y los sistemas de información frente a los ataques y asegurarse de que los delitos son perseguidos.
- Los ordenamientos jurídicos deben permitir el mantenimiento y el acceso rápido a los datos relativos a investigaciones criminales en curso.
- Hasta donde sea posible, las Tecnologías de la Información y las Comunicaciones deben ser diseñadas de forma que permitan prevenir y detectar el uso delictivo, perseguir al criminal y recopilar pruebas.

Tenemos el Convenio de Cibercriminilad adoptado por el Comité de Ministros del Consejo de Europa en el año 2001, que cuenta con 47 miembros y

8 observadores al día de la fecha) y abierta a otros países como Australia, Japón, Canadá, Sudáfrica y los EE.UU. Este acuerdo internacional tiende a regular todas las áreas relevantes de la legislación sobre ciberdelincuencia (derecho penal, derecho procesal y cooperación internacional), tratando con carácter prioritario la construcción de una política penal de cooperación internacional contra la ciberdelincuencia.

A diferencia de otras legislaciones, así como lo establecido por la normativa internacional, nuestras leyes se encuentran totalmente desactualizadas y existen vacíos normativos donde se debería regular normas que sancionen delitos como el *Phishing*.

En base a lo establecido en el objetivo general "Proponer mecanismos normativos para la introducción del *Phishing* como delito informático en Bolivia" se establecen las siguientes recomendaciones:

En base a lo establecido por el principio de Legalidad "*Nullum crimen nullum poena sine previa lege"* (No ha crimen, no hay sanción sin ley previa). Cualquier sujeto que cometa *Phishing* en Bolivia, se encuentra totalmente libre de recibir cualquier sanción en su contra. y menos aún se puede pretender sancionar este tipo de delitos con las normas ya establecidas porque violaría otro principio universal en materia penal

como es el de *"Nullum crimen, nulla poena, sine lege stricta"* (Los delitos y las penas deben estar determinadas exclusivamente por la Ley).

> El Tribunal Constitucional Plurinacional al respecto se pronunció en la Sentencia Constitucional 0034/2006, donde menciona lo siguiente:
> "No se puede recurrir a la analogía para extraer de su aplicación consecuencias desfavorables, aun cuando el comportamiento que se trata de incriminar sea similar al previsto en la ley penal.
>
> El fundamento de la prohibición de analogía radica en que, debido a la gravedad de la sanción contenida en la norma penal, ésta sólo debe responder a los supuestos que los representantes de la soberanía popular (legisladores) han establecido a través de la ley, vedándose de esta manera la extensión de la arbitrariedad del juzgador, exigiéndose, en cambio, la sujeción de éste a la Ley."(Tribunal Constitucional Plurinacional,2006)

En base a principios universales reflejados en nuestra Constitución Política del Estado como son el de garantizar el bienestar, el desarrollo, la seguridad y la protección e igual dignidad de las personas, ser protegido oportuna y efectivamente por los jueces y tribunales en el ejercicio de sus derechos e intereses legítimos, así como tener una justicia pronta y oportuna se recomienda la creación de una norma que tipifique el phishing como delito informático en Bolivia, pensando en respaldar la seguridad informática y patrimonial de las personas.

Asimismo se recomienda la creación de una división especializada dentro de la fiscalía destinada a perseguir los delitos informáticos. Para ello se debe

capacitar a los fiscales que compondrían la división, así como los peritos, investigadores y todo el personal que compone una división especializada en la fiscalía.

Esta capacitación debe consistir en prepararlos e ilustrarlos en todo el conocimiento necesario respecto a los delitos informáticos, en el *software* o programa utilizado en el caso del *phishing,* su manejo y las distintas técnicas utilizadas para la persecución y sanción de este tipo de delitos.

Imprescindiblemente la norma que regule el *phishing* como delito informático debe contener todas sus características particulares, como son la ingeniera social, la automatización a través de un software especializado, la suplantación de identidad y la multiplicidad de víctimas, con el fin de establecer claramente la conducta que se prohíbe y que en caso de cometerse el ílicito, el Ministerio Público tenga todos los elementos necesarios y clarificados para poder iniciar la investigación.

Finalmente se recomienda que para la creación de una norma que regule al *phishing* como delito informático se tome en cuenta como marco referencial lo establecido por las legislaciones de otros países que ya lo regularon, así como lo establecido por los distintos Convenios Internacionales, y lo establecido por los

especialistas en informática, con el fin de poder tipificar el delito de phishing de la forma más clara y precisa.

ANEXO 1 CASO BANCO NACIONAL DE BOLIVIA SOBRE PHISHING

Caso estafa cibernética en Bolivia.-

BNB detecta 600 débitos dudosos y recibe quejas.

El Banco Nacional de Bolivia (BNB) recibió hasta ayer alrededor de 200 denuncias de retiros indebidos de dinero de las cuentas de usuarios de sus tarjetas de débito; la entidad también detectó 600 transacciones sospechosas, desde el 11 de junio. (IBCE, 2012)

El Banco Nacional de Bolivia reportó según lo establecido por el Instituto Boliviano de Comercio Exterior (IBCE) que el 15 de junio de 2011 se detectaron 600 débitos dudosos y por lo tanto recibieron quejas de sus clientes. Según lo reportado los montos extraídos iban desde los 1.730 bolivianos hasta 2.250 bolivianos.

Por el robo a más de 600 clientes del Banco Nacional de Bolivia, tanto sus clientes que fueron víctimas de la sustracción del dinero de sus cuentas, como la institución bancaria y las aseguradores que tuvieron que hacer el rembolso, sufrieron considerables pérdidas económicas.

El banco informó que los días 10 y 11 de junio la mayoría de estas personas hicieron transacciones y consultas de saldo por internet y posteriormente se estableció que los clientes fueron víctimas de estafas cibernéticas.

ANEXO 2 ARTÍCULO LA AMENAZA PHISHING ESCRITO POR JOHN LACOUR DIRECTOR DE MARK MONITOR

La amenaza PHISHING.-

Escrito por John LaCour. Director de Soluciones Antiphising de MarkMonitor Cómo adoptan los ciberdelincuentes las mejores prácticas de TI para estafar online con más facilidad.

Los delitos electrónicos cometidos por el Grupo Rock Phish se están expandiendo rápidamente. Ha llegado el momento de que las empresas renueven sus iniciativas contra la delincuencia electrónica para responder a esta creciente amenaza, sobre todo los bancos, que han de esforzarse por fomentar la seguridad personal en Internet entre sus clientes.

La delincuencia electrónica es una amenaza cada vez mayor para la sociedad, especialmente el tipo de fraude online conocido como phishing. Las estadísticas no sólo revelan un aumento constante de los ataques de tipo phishing, sino que además estas estafas son cada vez más elaboradas y más difíciles de eliminar. Curiosamente, el éxito de las mismas reside en muchas de las mejores prácticas de las Tecnologías de la Información (TI) utilizadas por empresas legítimas para garantizar la continuidad de su negocio. Parece que ahora los estafadores están empleando dichas prácticas para aumentar el éxito de sus estafas online y escapar de las estrategias de mitigación utilizadas por aquellos que tratan de acabar con el phishing

El phishing es una estafa online que consiste en remitir engañosamente a los usuarios a páginas web fraudulentas, principalmente mediante e-mails que parecen auténticos, y en pedirles que proporcionen información personal como nombres de usuario, contraseñas, números de cuenta, direcciones, números de identificación personal (PIN), etc. Después, el

estafador utiliza esa información para usurpar la identidad de la víctima y sacar dinero de su cuenta bancaria, organizar subastas online, solicitar tarjetas de crédito, pedir préstamos, blanquear dinero y llevar a cabo diferentes actividades ilegales online. Aunque el blanco de estas estratagemas son los consumidores individuales, las entidades por las que se hacen pasar los estafadores también son víctimas: se está atentando contra su marca y la buena reputación que tanto les ha costado conseguir. Los bancos son el objetivo más común de los ataques de tipo phishing, aunque cada vez se producen más ataques contra todo tipo de empresas.

El phishing se ha convertido en una realidad desafortunada. El número de páginas únicas de phishing detectado por el (www.antiphishing.org) ascendió a 55.643 en abril de 2007, lo que supone un aumento radical respecto a las 20.871 que existían en marzo. Un modo más preciso de medir las actividades de estos estafadores es contar el número de marcas corporativas que han sido atacadas. Según el estudio de MarkMonitor® recogido en el Brandjacking Index™ del verano de 2007, el número de marcas al mes víctimas del phishing alcanzó en mayo de 2007 la cifra de 240, un hecho sin precedentes.

En un ataque habitual de phishing, el estafador envía cantidades ingentes de correo "spam", con links a páginas web fraudulentas cuyo control está en sus manos. Los links remiten a páginas que aparentan pertenecer a la empresa verdadera y normalmente se encuentran en servidores de páginas web legales en las que el estafador entra. Ante esta situación, el éxito del estafador depende de su capacidad para conseguir la recepción satisfactoria de los e-mails falsos que envía, entrar en un servidor web e introducir en él páginas falsas. En la actualidad, las empresas especializadas en operaciones antiphishing normalmente pueden mitigar sin demora estos ataques. Lo consiguen proporcionando inmediatamente direcciones de páginas web a las compañías antispam y contactando con los proveedores de web hosting o con el

propietario legítimo de la web para eliminar de la misma las páginas web fraudulentas. Por ello, muchos estafadores han optado por nuevas tácticas para incrementar la efectividad de sus operaciones.

Hoy en día, los profesionales de TI han adoptado una serie de mejores prácticas diseñadas para mejorar la seguridad y disponibilidad de los sistemas de información corporativa.

Desafortunadamente, los ciberdelincuentes se están adaptando a estas mismas tácticas para diseñar sus ataques. En particular, durante los dos últimos años, un grupo conocido como Grupo Rock Phish ha estado empleando estos métodos para robar una suma que se cree que alcanza cientos de millones de euros a bancos de todo el mundo mediante técnicas de phishing más avanzadas. Es más, el grupo Rock y sus secuaces han construido una arquitectura de red elaborada con varios niveles formada por varias capas únicas con el fin de poder llevar a cabo sus estafas.

El resultado de estas tácticas es que las páginas web que este grupo usa para estafar duran un 61% más de media, a veces hasta unas tres semanas. La efectividad de estas nuevas tácticas de phishing ha provocado que un conjunto de bancos deleguen sus actividades antiphishing en compañías de seguridad como MarkMonitor, que se dedican a controlar la complejidad de estas redes y enfrentarse a estas tácticas novedosas. (La Amenaza Phishing, 2012)

ANEXO 3 TÉRMINOS INFORMÁTICOS UTILIZADOS EN EL PRESENTE TRABAJO RELACIONADOS AL PHISHING Y SU PROCEDIMIENTO.

INFORMACIÓN.- Según Julio Téllez Valdés

"La palabra 'información' del latín in-formare (poner en forma) es una noción abstracta, no obstante que posee una connotación vinculada a una de nuestras más grandes libertades; la opinión y expresión de informaciones e ideas por cualquier medio que sea. De aquí que la información se haya considerado como un elemento susceptible de ser transmisible por un signo o combinación de signos, o como un proceso físico mecánico de transmisión de datos, teniendo como dato al elemento referencial acerca de un hecho. En sentido general un conjunto de datos constituye una información". (Téllez Valdez, 1996, pág. 2)

DERECHO INFORMÁTICO.- Para Oscar Fernando Orozco Muñiz el Derecho Informático se define como

"Un conjunto de principios y normas que regulan los efectos jurídicos nacidos de la interrelación entre derecho y la informática.

Se considera que el derecho informático es un punto de inflexión del derecho, puesto que todas las aéreas del derecho se han visto afectadas por la aparición de la denominada sociedad de la información, cambiando de este modo los procesos sociales y por tanto los procesos políticos y jurídicos. Es aquí donde hace su aparición el derecho informático, no tanto como una rama sino como un cambio".

DELITO INFORMÁTICO.- Para Julio Téllez Valdés existen dos clasificaciones del Delito Informático, que parten de lo típico y lo atípico.

Típico, "los Delitos Informáticos son las conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin".

Atípico, "los Delitos Informáticos son actitudes ilícitas en que se tiene a las computadoras como instrumento o fin".(Téllez Valdez,1996, pág.81)

SPAM.- Spam es todo aquel correo electrónico que contiene publicidad que no ha sido solicitada por el propietario de la cuenta de e-mail. La actividad de los spammers-aquellos sujetos que se encargan de generar el spam- es considerada poco ética e inclusoilegal en muchos países. Aquellas aplicaciones y herramientas encargadas de detectar o eliminar el spam son llamadas programas antispam.

1. El spam puede clasificarse como un tipo de correo electrónico no deseado

2. Por extensión, spam también se aplica a todo tipo de método de publicidad engañosa, no solicitada u oculta. (Diccionario Informático, 2012)

DIRECCIÓN IP.- Serie de números asociadas a un dispositivo (generalmente una computadora), con la cual es posible identificarlo dentro de una red configurada específicamente para utilizar este tipo de direcciones (una red configurada con el protocolo IP - Internet Protocol). Internet es un ejemplo de una red basada en protocolo IP version 4.

Como Internet es una red basada en el protocolo IP, por lo tanto, toda computadora o dispositivo conectados a esta deben ser asociados a una dirección IP. Esta dirección identifica a ese dispositivo unívocamente y puede permanecer invariable en el tiempo o cambiar cada vez que se reconecte a la red. Una dirección IP es estática cuando no varía, y es dirección IP dinámica cuando cambia en cada reconexión. (Diccionario Informático, 2012)

MALWARE.- Programa maligno. Cualquier programa creado con intenciones de molestar, dañar o sacar provecho en las computadoras infectadas. (Diccionario Informático, 2012)

HOST.- Utilizado a veces como sinónimo de mainframe, en realidad identifica al ordenador central en un sistema informático complejo.

Computador central o principal en un entorno de procesamiento distribuido. Por lo general se refiere a un gran computador de tiempo compartido o un computador central que controla una red. (Diccionario Informático, 2012)

LINKS- Un enlace o link es texto o imágenes en un sitio web que un usuario puede pinchar para tener acceso o conectar con otro documento. Los enlaces son como la tecnología que conecta dos sitios web o dos páginas web. En el navegador se ven como palabras subrayadas (como Ir al índice de FAQ's al final de ésta página). (Más Adelante, 2012)

DNS.- (Domain Name System). Sistema de Nombres de Dominio. Conjunto de protocolos y servicios para la identificación/conversión de una dirección de internet expresada en lenguaje natural por una dirección IP. (Diccionario Informático, 2012)

PHISHING.- Es la capacidad de duplicar una página web para hacer creer al visitante que se encuentra en el sitio web original, en lugar del falso. Normalmente, se utiliza con fines delictivos enviando SPAM e invitando acceder a la página señuelo. El objetivo del engaño es adquirir información confidencial del usuario como contraseñas, tarjetas de crédito o datos financieros y bancarios. (Diccionario Informático, 2012)

PHARMING.-Una de las modalidades más peligrosas del phishing es el pharming. Esta técnica consiste en modificar el sistema de resolución de nombres de dominio (DNS) para conducir al usuario a una página web falsa. (Diccionario Informático, 2012)

V.- FUENTES

(26 de Octubre de 2012). Obtenido de Seguridad de la Información: http://www.segu-info.com.ar/delitos/estadosunidos.htm

Delitos Informáticos. (26 de Octubre de 2012). Obtenido de http://delitos-infor.blogspot.com/2010/04/delitos-informaticos.html

Delitos Informáticos. (27 de Marzo de 2012). Obtenido de http://www.delitosinformaticos.com/03/2012/delitos/fraudes/informacion-sobre-phishing-ofertas-de-trabajo-falsas-y-blanqueo-de-capitales.#.ULRdUDBIGhM

Delitos Informáticos. (26 de Octubre de 2012). Obtenido de http://www.delitosinformaticos.com/03/2012/delitos/fraudes/informacion-sobre-phishing-ofertas-de-trabajo-falsas-y-blanqueo-de-capitales

Derecho Informático. (26 de Octubre de 2012). Obtenido de http://www.elderechoinformatico.com/publicaciones/mtemperini/JAIIO_DI_Phishing_Camera_Ready.pdf

Diccionario Informático. (5 de Mayo de 2012). Obtenido de La Web del Programador: http://www.lawebdelprogramador.com/diccionario/buscar.php?letra=&cadena=link.

La Amenaza Phishing. (3 de Abril de 2012). Obtenido de Iberfinanzas: http://www.iberfinanzas.com/index.php/Articulos-especiales/La-amenaza-phishing.html

Mas Adelante. (15 de Mayo de 2012). Obtenido de http://www.masadelante.com/faqs/enlace

Modalidades de Phishing - Pharming. (3 de Abril de 2012). Obtenido de Iberfinanzas: http://www.iberfinanzas.com/index.php/Articulos-especiales/La-amenaza-phishing.html

Peritaje Informática. (26 de Octubre de 2012). Obtenido de http://www.peritajeinformatica.com.ar/delitos-informaticos-reconocidos-por-las-naciones-unidas

Seguridad de la Información. (26 de Octubre de 2012). Obtenido de http://www.segu-info.com.ar/delitos/inglaterra.htm

Carrion, H. D. (2001). *Tesis "Presupuestos para la Punibilidad del Hacking".*

IBCE. (2 de Abril de 2012). *BNB detecta 600 débitos dudosos y recibe quejas*. Obtenido de Instituto Boliviano de Comercio Exterior: http://www.ibce.org.bo/principales_noticias_bolivia/15062011/noticias_la_razon_bolivia.asp?id=20730

Lima de la Luz, M. (1984). *"Delitos Electrónicos" en Criminalia.* México: Porrúa.

Sarzana, C. (2000). Delitos Informáticos. En *Delitos Informáticos* (pág. 37). Buenos Aires: AD-HOC.

Téllez Valdez, J. (1996). Derecho Informático.

Wikter, J. (1995). Cómo Elaborar un Tesis en Derecho. En *Pautas y Técnicas para el Estudiante o Investigador del Derecho* (pág. 10). Civitas.

Witker, J., & Larios, R. (1997). Metodología Jurídica. México D.F.: Mc Graw Hill - UNAM.