# EL DELITO DE ESTAFA EN LA MODALIDAD "PHISHING" A TRAVÉS DE INTERNET Y SUS MEDIOS PROBATORIOS EN VENEZUELA

**UNIVERSIDAD DE CARABOBO**
**FACULTAD DE CIENCIAS JURIDICAS Y POLITICAS**
**DIRECCION DE POSTGRADO**
**ESPECIALIZACION EN DERECHO PENAL**

# EL DELITO DE ESTAFA EN LA MODALIDAD "PHISHING" A TRAVÉS DE INTERNET Y SUS MEDIOS PROBATORIOS EN VENEZUELA

**AUTOR: Abog. Juan Carlos Zapata Marcó**
**TUTOR: Dr. Ángel Jurado Machado**

**Bárbula, abril de 2009**

**UNIVERSIDAD DE CARABOBO**
**FACULTAD DE CIENCIAS JURIDICAS Y POLITICAS**
**DIRECCION DE POSTGRADO**
**ESPECIALIZACION EN DERECHO PENAL**

# EL DELITO DE ESTAFA EN LA MODALIDAD "PHISHING" A TRAVÉS DE INTERNET Y SUS MEDIOS PROBATORIOS EN VENEZUELA

**TUTOR: Dr. Ángel Jurado Machado**

**Trabajo de Especialización presentado ante la Dirección de Postgrado de la Universidad de Carabobo para optar al Título de Especialista en Derecho penal**

**Bárbula, abril de 2009**

## DEDICATORIA

-

- A mi hijo **Juan Carlos** por ser lo más grande de mi existencia, la continuación de la vida.
- A **Yesenia Rodríguez**, por estar en mi ser y en mis momentos más difíciles.
- A **mis Padrinos** quienes me dieron todo lo que soy, a mi hermano **Alex**. A la memoria de ellos.
- A **mis padres y hermanos** por su apoyo.

## AGRADECIMIENTOS

- A Dios YHVH Omnipresente, quien siempre dirige mis pasos.
- A la Profesora **Miriam González**, por su valiosa colaboración y sus enseñanzas.
- A la Lic. **Carmen Aquino**, por su comprensión e insistencia para la culminación del trabajo.
- Al Doctor **Ángel Jurado Machado**, quien con su apoyo hizo posible la culminación de este trabajo.
- A mis compañeros y profesores de la especialidad, gracias por conocerlos.

**INDICE**


**PAG.**

**RESUMEN**

**INTRODUCCION**

**CAPITULO I**
**EL PROBLEMA**
Planteamiento del Problema **12**
Formulación del Problema **18**
**OBJETIVOS DE LA INVESTIGACIÓN** **19**
Objetivo General **19**
Objetivos Específicos **19**
**JUSTIFICACION DE LA INVESTIGACION** **20**

**CAPITULO II**
**MARCO TEORICO REFERENCIAL**
Antecedentes de la Investigación **21**
Antecedentes Históricos **23**
Bases Teóricas **30**
¿Cómo funciona el Phishing? **33**
Fines y proceso del Delito de Estafa Informática **34**
Medios de Pruebas **35**
La Prueba electrónica **38**
Prueba Pericial Informática **42**
La Inspección Judicial **42**
El Reconocimiento y la Inspección **43**
Experticias sobre Mensajes de Datos y Correo Electrónico **44**
Procedimientos de Obtención y Resguardo de Medios Probatorios **46**
Peritos Informáticos **49**
Los Indicios en el Derecho Informático **50**
Los Rastros o Soportes Electrónico como Prueba Documental **50**
Principios de Identificación de las Actividades en Internet **52**
La Dirección IP **53**
Los Mensajes de Datos **54**
Correo Electrónico (Email) **54**
Auditoria del Mensaje del Correo Electrónico **55**
Existencia de una Cuenta de Correo Determinada **56**
Titularidad de las Cuentas de Correo **57**
Repercusión Social y Económica **59**
Bases Normativas **60**
Código Penal de España **63**

Código Penal de Colombia **65**
Código Penal de Costa Rica **65**
Definición de Términos Básicos **66**
Matriz de Variables **69**

**CAPITULO III**
**MARCO METODOLOGICO**
Nivel y modalidad de la investigación **70**
Técnicas e instrumentos para la recolección de información **71**
Observación **71**
Revisión documental **72**
Procedimiento **72**

**CAPITULO IV**
Análisis e Interpretación del Contenido **75**

**CAPITULO IV**
**CONCLUSION Y RECOMENDACIONES**
Conclusión **87**
Recomendaciones **88**

**REFERENCIAS BIBLIOGRAFICAS**

**REFERENCIAS NORMATIVAS**

**ANEXOS**

## RESUMEN

La descripción de diversas formas que asume el delito de Estafa Informática en su modalidad de Phishing permitirá, en este trabajo de investigación, efectuar un análisis de dicha forma. Dado que los mensajes y los sitios Web que envían estos usuarios parecen oficiales, logran engañar a muchas personas haciéndoles creer que son legítimos. La persona confiada, normalmente responde a estas solicitudes de correo electrónico con sus números de tarjeta de crédito, contraseñas, información de cuentas u otros datos personales. Estas nuevas y variadas posibilidades pueden tener algún efecto en las explicaciones sobre la estafa. El mensaje puede integrar un formulario para enviar los datos requeridos, aunque lo más habitual es que incluya un enlace a una página donde actualizar la información personal. Existen diversos instrumentos normativos que permiten ser el soporte a la investigación. El artículo in comento es norma de Derecho Internacional, la cual recomienda tomar medidas para tipificar el delito de fraude en los derechos internos de los países. Un componente importante en el Delito de Phishing es la captación de datos sobre personas. Número de tarjeta de crédito y de documentos de identidad y contraseñas para manejarlas, todos estos datos suelen residir en computadoras personales conectadas a la red. Los usuarios, creyendo que estaban conectados a la página Web de su banco, abrieron un formulario y lo rellenaron con sus datos, incluyendo, en muchos casos, su contraseña secreta. Envía la información deseada a un destino oculto, y se autodestruye para que el usuario no se de cuenta de que su información confidencial ha sido espiada. Posteriormente, la información obtenida se puede

utilizar para vaciar cuentas bancarias o acceder a servidores protegidos con contraseña. La información contenida en un mensaje de datos, reproducida en formato impreso, tendrá la misma eficacia probatoria atribuida en la ley a las copias o reproducciones fotostáticas.

# ABSTRACT

The description of diverse forms that assumes the crime of Computer science Swindle in its modality of Phishing will allow, in this work of investigation, to carry out an analysis of this form. Since the messages and the Web sites that these users send seem officials, they manage to deceive many people being done to them to think that they are legitimate. The trusted person normally responds to these requests of electronic mail with her numbers of password, credit card, personal information of accounts or other data. These new ones and varied possibilities can have some effect in the explanations on the swindle. The message can integrate a form to send the required data, although most habitual it is than it includes a connection to a page where to update the personal information. Diverse normative instruments exist that allow to be the support the investigation. The article in comment is norm of the Right International, which recommends taking, measures to typify the crime of fraud in the internal rights of the countries. An important component in the Crime of Phishing is the pick up of data on people. Number of identity card and credit card and passwords to handle them, all these data usually resides in connected personal computers to the network. The users, thinking that they were connected to the page Web of its bank, opened a form and they filled up it with its data, including, in many cases, its secret password. It sends the wished information to an hidden destiny, and self destroyer so that the account user not of which its confidential information has been spied on. Later, the obtained data can be used to drain banking accounts or to accede to servants protected with password. The information contained in a message of data, reproduced in printed format, will have the same probatory effectiveness attributed in the law to copies or reproductions.

**Descriptores**: Delitos Informáticos, Derecho Penal, Phishing, Fraude, Estafa, phisher

# INTRODUCCIÓN

En la actualidad las computadoras se utilizan no sólo como herramientas auxiliares de apoyo a diferentes actividades humanas, sino como medio eficaz para obtener y conseguir información, lo que las ubica también como un nuevo medio de comunicación fundado en la informática, tecnología cuya esencia se resume en la creación, procesamiento, almacenamiento y transmisión de datos.

La motivación que lleva a realizar esta investigación es por los acontecimientos que a nivel mundial se están sucediendo en el ciberespacio, como son los delitos informáticos y de ellos la Estafa. Miles de personas han sido defraudadas a través del uso de la Internet, casos de estafas millonarias a bancos o a personas. La investigación está delimitada a la Estafa Informática en la modalidad de Phishing por Internet en Venezuela y sus Medios Probatorios.

El presente trabajo de Especialización en Derecho Penal, versa sobre el Phishing a través de la Internet, percepción que se ha ido desarrollando muy por detrás de la realidad de los alcances de los llamados ciberdelitos, pero que ha generado acciones claras y evidentes de una necesidad de control por parte de los organismos competentes; es por ello que las experiencias desarrolladas por la Organización de las Naciones Unidas, la Comunidad Europea, los Estados Unidos de

Norteamérica, se han dirigido hacia la creación de los organismos necesarios para plantear que el problema del cibercrimen y sus consecuencias en la seguridad de las personas y en sus respectivas economías es un hecho grave y que requiere de urgentes medidas de todo tipo, tanto en el ámbito legislativo, tecnológico y social.

La investigación es de suma importancia, ya que la situación actual de vulnerabilidad de datos, en el área de la protección legal de los derechos de las personas naturales o jurídicas, no ha detenido el avance de otros medios, provenientes de la misma área tecnológica, para los resguardos de bienes jurídicos principalmente las patrimoniales.

Este proyecto de investigación se justifica, por el auge que ha tenido la Internet a nivel mundial, sobre todo en Venezuela, ya que el delincuente va a la par del desarrollo de la sociedad, y quizás, con un paso hacia delante de diferencia con respecto a la misma sociedad.

# CAPÍTULO I

# EL PROBLEMA

## Planteamiento del problema

Hoy, por la "autopista de la información" (término acuñado por el vicepresidente norteamericano Al Gore, 1994), circulan millones de personas, desde ciudadanos comunes: amas de casa, niños y adolescentes, empresas, partidos políticos, científicos; pero también hacen uso de la Internet delincuentes, terroristas, mafias organizadas y los llamados Hackers o piratas informáticos. Como en toda vía pública, en las autopistas de la información también existe la inseguridad.

La Estafa por Internet esta comprendida por Phishing, Subastas, Compras on line y los Juegos de Azar, de los delitos cometidos a través de Internet es el "phishing", o como se conoce en la voz inglesa fishing - pescar, es el que más auge ha tenido, pues, parte de la suplantación de identidad (en Internet, pero también por teléfono) con la finalidad de apropiarse de datos confidenciales de los usuarios, haciéndoles caer en error para tener un provecho injusto.

En la Red se utiliza el envío masivo de correos electrónicos que simulan proceder de entidades de prestigio y apremian al internauta a actualizar datos

personales (nombres de usuario y contraseña de cuentas bancarias, números de tarjeta de crédito, etc.) a través de una página que imita a la original. Al introducir los datos en la página falsa, éstos son 'pescados' por los ciberdelicuentes para utilizarlos de forma fraudulenta.

Comprar a través de Internet está revolucionando la manera en que los consumidores alrededor del mundo adquieren bienes y servicios. El número de transacciones electrónicas ha aumentado dramáticamente en años recientes. Durante las épocas navideñas, millones de personas visitan sitios de compras en la Internet. Sin embargo, hay un lado oscuro de la conveniencia y libertad del comercio electrónico; la incidencia de robo de identidad y la Estafa a través de la Internet también ha aumentado dramáticamente. Según estimados de la Industria Nacional de Crédito (EEUU), el número de quejas sobre estafa de identidad se ha incrementado desde menos de 60,000 en 1999 hasta unos 750,000 en 2.006.

En el año 2006 una investigación efectuada por el Buró de Investigaciones Federales de los Estados Unidos (FBI), reveló hasta qué punto el delito ha penetrado los espacios cibernéticos en el país más avanzado tecnológicamente del mundo. Según dicha investigación, más del 90 % de las grandes empresas reconoció constantes fallas y brechas de seguridad en sus sistemas; este estudio también refiere que se perdieron más de 155 millones de dólares por el delito de estafa en el año 2006.

A partir del año 2000, en Venezuela se registró un significativo incremento del número de usuarios en Internet. Actualmente, aproximadamente el 30% de los venezolanos tienen acceso a este servicio. La empresa encuestadora Datanálisis reportó que Venezuela tendría un crecimiento mayor al 40% para el año 2009 en el uso de la Internet.

La Superintendencia de Bancos y otras instituciones Financieras (SUDEBAN), planteó en el año 2000 ante la Asamblea Nacional, el preocupante incremento del número de Delitos Electrónicos en Venezuela durante los últimos años. Debido a la importancia y la necesidad de crear una legislación sobre la Estafa Informática y demás delitos informáticos, la Asamblea Nacional de Venezuela creó el 21 de septiembre del año 2000, una Subcomisión Especial, dependiente de la Comisión de Finanzas, a la que le encargó la tarea de investigar las Estafas Informáticas en el Sistema Financiero venezolano y proponer un proyecto de ley para atender esta problemática.

El número de usuarios de Internet se cuenta en miles de millones, y es el mercado más grande para Estafas jamás cometidas. Un ejemplo de Estafa clásica, (antes realizada por correo postal), es el ofrecimiento de participación en una herencia o una gran fortuna, previo pago de unos gastos necesarios. El engaño lleva más de un siglo de existencia, y fue realizado masivamente en los Estados Unidos después de la guerra contra España en 1898, cuando un presunto noble español,

prisionero de guerra en tierras americanas, ofreció participación en su gran fortuna a quien le ayudase con un poco de dinero para poder sobornar a las autoridades y salir de la cárcel. Sin embargo, habría que escribir muchas cartas a mano para conseguir una sola víctima de este engaño. Con la Internet, el envío de correo masivo es relativamente gratis, y ofertas poco plausibles de este tipo se pueden enviar a cientos de miles de personas. Este tipo de Estafa, denominada Cartas Nigerianas, ha tenido bastante éxito.

Con relación a los Medios de Prueba los casos de Estafa Informática a través de Internet en Venezuela, el obstáculo para la admisibilidad y apreciación de elementos de convicción distintos de las pruebas tradicionales o que estén contenidos dentro de un soporte distinto del documento escrito, ya no radica en restricciones establecidas por el Ordenamiento Jurídico Venezolano puesto que, el régimen Procesal Penal Venezolano le otorga cabida a cualquier elemento de convicción que cumpla con los requisitos de legalidad, licitud, idoneidad y utilidad; la resistencia hacia su incorporación en una investigación radica más bien en la nula o en el mejor de los casos, muy incipiente Cultura Tecnológica que ha impedido o retardado la familiarización de todos los sujetos procesales con este tipo de elementos probatorios.

Es evidente el natural rechazo que recaerá hacia cualquier elemento que luzca ininteligible para quien, aun cuando tenga la potestad de conducir una investigación, carezca de conocimientos especializados para comprenderlo, interpretarlo y discernir

acerca de su relevancia; por ello, al margen del necesario auxilio de los expertos para la "traducción" específica del significado de un rastro contenido en soportes lógicos y no físicos, es necesario identificar y familiarizarse *in abstracto* con todo el espectro probatorio que puede derivarse de los nuevos modos de almacenar, transmitir, conservar y manejar la información, independientemente de la calificación jurídica que puedan merecer los hechos objeto de investigación penal y el grado de responsabilidad penal involucrado.

Otro grave obstáculo al enjuiciamiento por delitos cibernéticos o informáticos es el hecho de que los delincuentes pueden destruir fácilmente las pruebas cambiándolas, borrándolas o trasladándolas. Si los agentes del orden operan con más lentitud que los delincuentes, se pierde gran parte de las pruebas; o puede ser que los datos estén cifrados, una forma cada vez más popular de proteger tanto a los particulares como a las empresas en las redes de computadoras. Tal vez la criptografía estorbe en las investigaciones penales, pero los Derechos Humanos podrían ser vulnerados si los encargados de hacer cumplir la ley adquieren demasiado poder técnico. Las empresas electrónicas sostienen que el Derecho a la Intimidad es esencial para fomentar la confianza del consumidor en el mercado de la Internet, y los grupos defensores de los Derechos Humanos desean que se proteja el cúmulo de datos personales archivados actualmente en ficheros electrónicos. Las empresas también recalcan que la información podría caer en malas manos, especialmente en países con problemas de corrupción, si los gobiernos tienen acceso a los mensajes en código.

Si los gobiernos tienen la clave para descifrar los mensajes en código, ésto significa que también personas no autorizadas, pueden obtenerlas y utilizarlas.

Así mismo, existe otro escollo, la penalización del delito cometido en contra de un residente en Venezuela por un delincuente informático, utilizando la Internet desde el exterior; ésto debido a que las normas que rigen en Venezuela, pueden ser diferentes o en su defecto inexistentes para el país desde donde se está cometiendo el delito de Estafa.

**Formulación del problema**

En Venezuela, los Delitos Informáticos están contemplados en la legislación vigente, específicamente en la Ley Especial Contra los Delitos Informáticos (2001); pero el problema que encuentra el juzgador es que, los Medios de Prueba no están establecidos para el delito de Estafa Informática, debiendo ser tomados de otras leyes.

Otro punto a tratar es lo referente a cómo éste delito (phishing) repercute en la sociedad, así como sus consecuencias legales. En razón de lo expuesto surgen las siguientes interrogantes:

¿En qué consiste el delito de “Phishing” cometido a través de Internet, en Venezuela?

¿Cuales son los Medios de Prueba contemplados en la Legislación Procesal Venezolana y Comparada?

¿Cuales son las repercusiones sociales y económicas?

**Objetivos de la investigación**

**Objetivo general**

Analizar el delito de Phishing a través del uso de la Internet, a la luz de la Legislación Penal Venezolana y Comparada, con la finalidad de identificar los medios de prueba derivados de las nuevas tecnologías de la Información, y las repercusiones legales, sociales y económicas de este delito.

**Objetivos específicos**

- Analizar el Delito de Estafa en la Modalidad de Phishing a través de Internet, en Venezuela.
- Determinar los Medios de Pruebas y su licitud de acuerdo al ordenamiento jurídico venezolano.

- Indagar las repercusiones sociales y económicas de este delito para poder enfrentarlo.
- Examinar la legislación extranjera para tipificar y penalizar los delitos de Estafa por Internet.

## JUSTIFICACION DE LA INVESTIGACION

El presente trabajo de investigación se justifica debido a la masificación de este delito, como lo es el Phishing a través de Internet, por cuanto en Venezuela hay denuncias efectuadas a la Asamblea Nacional y al Cuerpo de Investigaciones Científicas, Penales y Criminalísticas (CICPC), vinculadas sobre todo al Sistema Financiero. Por causa de este delito, se pierden millones de Bolívares al año en nuestro país, muchos de los afectados no denuncian, sobre todo las entidades financieras debido a la posible pérdida de clientes de la institución, o personas que consideran a los organismos encargados poco confiables e incapaces de dar respuestas eficientes a los casos.

# CAPITULO II

# MARCO TEORICO REFERENCIAL

## Antecedentes de la Investigación

En el año 2001, la Subcomisión de Delitos Informáticos de la Asamblea Nacional, dirigida por el Diputado Carlos Tablante, presentó una propuesta legal para enfrentar las amenazas de los Delitos en el ciberespacio. Este estudio ofreció una herramienta para controlar los peligros de la globalización; en el mismo se hizo un esbozo sobre las leyes que rigen la materia, incluyendo un Proyecto de Ley sobre Delitos Informáticos, vigente en la actualidad, como lo es la Ley Especial contra los Delitos Informáticos, la cual permite encuadrar los Delitos Informáticos en un marco legal en Venezuela y por ende en el trabajo de investigación. (Tablante, 2001)

Stangeland (2004), realizó un trabajo sobre la explicación y control de la Estafa Informática; él señala que a largo plazo van a dominar los delitos con fines de lucro, como los "robos" y la estafa a través de la Internet. Su trabajo determina cuales son los factores que coinciden para facilitar estos delitos: conocimientos suficientes de informática, el anonimato idóneo ofrecido por la Internet, mientras que la seguridad en redes temáticas es muy deficiente. El planteamiento que el autor hace en su trabajo se vincula con el presente estudio en lo referente a la explicación de los factores considerados para perpetrar el delito de Estafa a través de la Internet.

Por otro lado, la investigación de Gabaldon (2004) sobre la Estafa Electrónica y la Cultura Corporativa, expone una síntesis de la historia de la estafa y su penalidad a través de los tiempos, así como, su conceptualización y forma de efectuarlo. También hace referencia a su tipificación en las normas y la legislación vigente, modalidades y conducta del delincuente y sus proposiciones teóricas para la explicación de la Estafa Electrónica. Con este trabajo se dió a conocer algunas formas como operan los delincuentes en las corporaciones financieras. Su aporte a esta investigación es la descripción y la conceptualización del delito, así como las formas de perpetración.

Gutiérrez (2004), abogado especialista en Derecho Mercantil, profesor de postgrado de la Universidad Católica Andrés Bello (UCAB), refiere que las herramientas electrónicas también han sido utilizadas como medio para la comisión del delito informático de Estafa. Señala que el delincuente después que ha interceptado la información que le interesa, la utiliza para inducir al error con el ánimo de engañar o sorprender la buena fe de otra persona, y procurarse un provecho injusto; el medio o canal para realizar o cometer el delito es casi siempre un Email (correo electrónico), mediante la usurpación de la identidad; se utilizan, ilícitamente, datos tales como números de cuentas bancarias, claves secretas, número de tarjetas de crédito y débito, con la finalidad de girar instrucciones para enviar dinero al destino que desea el estafador. La descripción de diversas formas que asume este delito permitirá, en este trabajo de investigación, efectuar un análisis de dichas formas.

Arteaga (2004), en su trabajo "El Crimen Electrónico" define el Fraude Electrónico como todo acto que infringe la ley y que se realiza aplicando algún medio de procesamiento electrónico. Este autor presenta varios ejemplos: El robo a un Banco, violando la seguridad de algún medio de procesamiento electrónico de información, es constituido de crimen electrónico. No se considera Crimen Electrónico que el mismo Banco sea robado utilizando como medio artefactos electrónicos de alta tecnología que permita la comisión del delito. Seria bueno recordar que todo delito necesita determinados elementos objetivos y subjetivos para su identificación y diferenciación de acuerdo al sujeto activo, su modo de operar y los medios que utiliza en su acción. Un ejemplo sencillo: El HURTO se diferencia de la ESTAFA porque en este último es imprescindible el elemento subjetivo: engaño, mientras en aquel no. Otro elemento diferenciador es que en el HURTO el bien se sustrae o se apoderan de él, mientras en la ESTAFA el bien se entrega tácita o expresamente. Se vincula con elementos subjetivos y objetivos del trabajo, su forma de operar y medios para la comisión del delito.

**Antecedentes Históricos**

La Estafa, vinculada a la idea de engaño con fines lucrativos, tiene larga data como conducta penalizada. El Código de Hammburabí ( 1750 a.c) contempla varias formas, tales como la entrega en préstamo de granos y plata en distinta medida de lo

acordado, castigada con la perdida total de lo prestado (art 94). La apropiación de grano o forrajes cedidos para la siembra o cría, castigada con la pérdida de la mano (art. 253).

En el Derecho Romano (150 a.c)., la acción para perseguir las Estafas era de naturaleza privada y auxiliar al procedimiento civil, aunque mediante la práctica de los tribunales se extendió como auxiliar al procedimiento acusatorio, revistiendo entonces carácter penal, El *stellionatus (estelionato),* nombre genérico para la Estafa, fue precedido en la criminalización por la adulteración de testamentos y de monedas y por la corrupción de funcionarios y, aún antes, desde la Ley de la XII Tablas (450 a.c), por el falso testimonio, el cohecho de jurados y la compra de votos.

El Estelionato (Estafa) en la Edad Media, se diferenció notablemente del romano y de la Estafa actual, porque al surgir la doctrina de un nuevo *falsum* en el cual se incluyeron las formas de fraude patrimonial, pasó a ser una especie subsidiaria del estelionato, confundiéndose las dos figuras delictuales. Se ha dicho que los estatutos y las constituciones italianas reprodujeron los errores de la doctrina. En el Derecho Canónico sólo se encuentran disposiciones que imponían la excomunión, en los casos de una que otra norma relativa a eventos auténticos de Estafa (Núñez Tenorio, 1997: p. 25).

La ley Francesa de Policía Municipal del 22 de julio de 1791, en su artículo 35 del título segundo establecía:

> *"Quienes por dolo, o con ayuda de falsos nombres o de falsas empresas, o de un crédito imaginario, o de esperanzas o temores quiméricos, hayan abusado de la credulidad de algunas personas, estafando la totalidad o parte de sus bienes, serán perseguidos ante los Tribunales de Distrito, después de haber pronunciado las restituciones y daños y perjuicio, está autorizado para condenar por vía de policía correccional, a una multa que no podrá exceder de 5.000 libras, y a una prisión que no podrá exceder de dos años; y en caso de reincidencia la pena será el doble".*

El artículo 405 del Código Penal francés de 1810 (Código de Napoleón), tipificaba este delito en la siguiente forma:

> *"…Cualquiera que, ya haciendo uso de nombre supuesto o de supuestas cantidades, ya empleando maquinaciones fraudulentas para persuadir de la existencia de falsas empresas, de un poder o de un crédito imaginario, para hacer nacer la esperanza o el temor de un buen éxito, de un accidente o de cualquiera otro acontecimiento quimérico, o hubiese intentado hacerse remitir o entregar fondos muebles u obligaciones, disposiciones , billetes, promesas, recibos o descargos, y hubiese por uno de estos medios, estafado o intentado estafar, la totalidad o parte de la fortuna de otro, será condenado a un mínimum de uno y un máximum de cinco años de prisión y una multa mínima de 50 y máxima de 3.000 libras".*

En la actualidad, la Informática, es el "medio de comisión", favorecido por el desarrollo de la tecnología de la información, la cual implica la revolución más importante del siglo XX, quizás la única que ha marcado o ha significado un cambio irreversible en nuestro modo de ver y de actuar, que ha operado en forma silenciosa, universal y cotidiana, y que ha incorporado en forma asombrosa a una gran cantidad de personas a redes de comunicación.

La rápida extensión de computadoras y el crecimiento exponencial de usuarios de la Internet ha causado la impresión de que hemos entrado en una nueva era de la información con mejor acceso a ella y posibilidades ilimitadas de comunicación para todos. Sin embargo, estas proclamaciones han estado basadas en un optimismo técnico mal fundamentado en las realidades sociales y económicas del mundo. La Informática se encuentra todavía fuera del alcance de gran parte de la población mundial, donde una cuarta parte de la población todavía vive sin electricidad ni línea telefónica. Un resentimiento al dominio americano sobre la informática y la economía está detrás de muchos intentos de destrozar las redes telemáticas.

En los primeros años de la informática, los abusos de los sistemas eran menos graves. Primaron las bromas infantiles y, de vez en cuando, las venganzas personales. Dominaba la curiosidad y ganas de mostrar conocimientos y el desafío personal de poder romper sistemas. Se distinguió entre los que llamaban "Hackers", que se

metían en sistemas ajenos sin causar daños, y "Crackres" que causaban destrozos. El "Hackeo" exigía altos conocimientos de informática, y estas personas tenían una carrera profesional bien remunerada, y la utilización de estas técnicas para fines ilícitos les habría bloqueado las oportunidades de ganancias legales como analistas de sistemas en compañías prestigiosas. Por eso, en su infancia se limitaron a, mostrar excelencia y a gastar bromas, sin fines lucrativos.

Una de las causas del cambio en la ética profesional de los "Hackers" es la amplia divulgación de conocimientos informáticos. Algoritmos y trucos son ya conocidos y están al alcance de más personas. Los códigos fuente para crear un virus, troyano o gusano están disponibles en múltiples sitios. El umbral para los que quieren ser intrusos es más barato y requiere menos conocimientos. Una vez inventado un truco, se copia fácilmente y las herramientas de robo son más accesibles.

El término *phishing* fue creado a mediados de los años 90, por los piratas electrónicos mejor conocidos como crackers quienes procuraban robar las cuentas de American On Line (AOL). Un atacante se presentaría como empleado de AOL y enviaría un mensaje inmediato a una víctima potencial. El mensaje pedía que la víctima revelara su contraseña, con variadas excusas como la verificación de la cuenta o confirmación de la información de la facturación. Una vez que la víctima

entregara la contraseña, el atacante podría tener acceso a la cuenta de la víctima y utilizarla para cualquier otro propósito.

En esta modalidad de fraude, el usuario malintencionado envía millones de mensajes falsos que parecen provenir de sitios Web reconocidos o de su confianza, como su banco o la empresa de su tarjeta de crédito.

Dado que los mensajes y los sitios Web que envían estos usuarios parecen oficiales, logran engañar a muchas personas haciéndoles creer que son legítimos. La gente confiada, normalmente responde a estas solicitudes de correo electrónico con sus números de tarjeta de crédito, contraseñas, información de cuentas u otros datos personales.

Para que estos mensajes parezcan aun más reales, el estafador suele incluir un vínculo falso que parece dirigir al sitio Web legítimo, pero en realidad lleva a un sitio falso o incluso a una ventana emergente que tiene exactamente el mismo aspecto que el sitio Web oficial. Estas copias se denominan "sitios Web piratas". Una vez que el usuario está en uno de estos sitios Web, introduce información personal sin saber que se transmitirá directamente al delincuente, que la utilizará para realizar compras, solicitar una nueva tarjeta de crédito o robar su identidad.

Se puede afirmar, que la expansión tecnológica comunicacional parece haber multiplicado la escala cuantitativa de las Estafas mediante el incremento de las oportunidades que se ofrecen para acceder cómodamente, incluso sin contacto directo con la víctima, a blancos atractivos para esta actividad delictiva.

El número de usuarios de Internet se cuenta en miles de millones, y es el mercado más grande de estafa jamás concebido. Con Internet, el envío de correo masivo es gratis, y ofertas poco plausibles de este tipo se pueden enviar a cientos de miles de personas.

Probablemente la Estafa vinculada estrictamente a lo que se conoce como banca electrónica (operaciones a través de Internet), constituye a nivel nacional, un área de criminalidad todavía relativamente limitada, si bien en perspectiva de expansión, considerando el grado de incorporación de usuarios a la red.

Para 1998 la tasa de conexión a la red por cada mil habitantes fluctuaba, en los países industrializados de Europa, Asia y Norteamérica, entre 6,22 y 107,51, mientras que para América Latina fluctuaba entre 2,03 y 0,54, con Venezuela muy cerca del tope inferior, con una tasa de 0,61 (IESA, 2000:31).

Estas nuevas y variadas posibilidades pueden tener algún efecto en las explicaciones sobre la estafa. Por otro lado, el desarrollo legislativo, cada vez más estandarizado a nivel internacional, indica la tendencia de una criminalización legal anticipatoria, que no requiere, en el tipo legal, la consumación del perjuicio económico, sino la creación de la situación de riesgo.

Las modalidades de fraude a las que están expuestos los usuarios de la banca electrónica, el Phishing es una de las más utilizadas hoy en día.

**Bases Teóricas**

Las bases teóricas del presente trabajo de investigación se sustentan sobre un enfoque técnico-jurídico, y sobre el estudio de las repercusiones sociales y económicas del Delito de Estafa Informática en la modalidad "Phishing"

La informatización de las transacciones financieras, comerciales y bancarias, así como la generalización del pago a través de procedimientos electrónicos y el desarrollo de la gestión y de los procesos contables mediante sistemas de esta naturaleza, ha abierto formas inéditas de comisión de delitos a los fines patrimoniales y económicos que hasta hace poco no habían merecido ni doctrinal ni legalmente el interés que por su importancia merecían.

Igualmente, las redes de transmisión de datos, facilitan aún más la posibilidad de delinquir, al permitir que el autor pueda efectuar las modificaciones desde su propio domicilio, si dispone de un terminal y un instrumento de transferencia de datos adecuado.

El ilustre penalista Cuello (2002), mencionado por Gutiérrez, define:

> *"El delito informático como toda acción (acción u omisión) culpable, realizada por un ser humano, que cause un perjuicio a personas, sin que necesariamente beneficie al autor o que, por el contrario, produce un beneficio ilícito a su autor aunque no perjudique de forma directa o indirectamente a la víctima, tipificado por la ley, que se realiza en el entorno informático y que está sancionado con una pena*."

Por otro lado, el autor mexicano Téllez (2003) señala que los delitos informáticos son:

> "A*ctitudes 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)*".

Sieber (2004), cita como ejemplo de esta modalidad el siguiente caso tomado de la jurisprudencia alemana:

> *"Una empleada de un banco del sur de Alemania transfirió, en febrero de 1983, un millón trescientos mil marcos alemanes a la cuenta de una amiga - cómplice en la*

> *maniobra - mediante el simple mecanismo de imputar el crédito en una terminal de computadora del banco. La operación fue realizada a primera hora de la mañana y su falsedad podría haber sido detectada por el sistema de seguridad del banco al mediodía. Sin embargo, la rápida transmisión del crédito a través de sistemas informáticos conectados en línea (on line), hizo posible que la amiga de la empleada retirara, en otra sucursal del banco, un millón doscientos ochenta mil marcos unos minutos después de realizada la operación informática."*

El criminólogo norteamericano Sutherland (1996) postuló nueve proposiciones teóricas para la explicación de la delincuencia. Cuatro (4) de ellas tienen que ver con los mecanismos de incorporación al repertorio conductual del sujeto: el comportamiento criminal se aprende; dicho aprendizaje se da por el contacto con grupos íntimos; y lo más importante, en el aprendizaje se incluyen tanto técnicas como motivos, impulsos, racionalizaciones y actitudes. Otras tres (3) guardan relación con la dinámica del aprendizaje sobre leyes: cuando hay un exceso de exposición a definiciones favorables a la violación de la ley es más probable la delincuencia, y la exposición a estas definiciones favorables a la violación de la ley varían en frecuencia, duración, prioridad e intensidad. Hay otras dos proposiciones vinculadas a lo inespecífico del aprendizaje del comportamiento criminal: una y otra implican mecanismos equivalentes, como imitación o identificación; y no existen motivaciones específicamente criminales frente a las no criminales, pues

motivaciones como el lucro, la búsqueda de la felicidad, la persecución del estatus social o la frustración son comunes a la conducta ilícita y a la lícita.

El Enfoque Técnico sobre la Estafa Electrónica, en su modalidad de Phishing, abarca la manipulación y creación de Paginas Web, relacionadas a su vez con el envío de correos electrónicos a su futura víctima. El delincuente, hace creer a la víctima que ese correo pertenece, por ejemplo a un banco, donde la víctima tiene su dinero, pero el Site o sitio es creación del victimario, donde los datos falsos de la pagina permiten, bajo un engaño, introducir por parte de la víctima datos personales con el propósito de obtener ganancias indebidas para el delincuente. Los distintos métodos para realizar estas conductas se deducen, fácilmente, de la forma de trabajo de un sistema informático: alterar datos, omitir e ingresar datos verdaderos o introducir datos falsos, en un computador.

**¿Cómo funciona el Phishing?**

El usuario recibe un e-mail de un banco, entidad financiera o tienda de Internet en el que se le explica que por motivos de seguridad, mantenimiento, mejora en el servicio, confirmación de identidad, advertencia de fraude o cualquier otro, debe actualizar los datos de su cuenta, además de informar que la cuenta será bloqueada si no realiza la actualización de los datos en un tiempo determinado. El mensaje

imita exactamente el diseño (logotipo, firma, etc.) utilizado por la entidad para comunicarse con sus clientes. El mensaje puede integrar un formulario para enviar los datos requeridos, aunque lo más habitual es que incluya un enlace a una página donde actualizar la información personal. Si se rellenan y se envían los datos de la página, caerán directamente en manos del estafador, quien puede utilizar la identidad de la víctima para operar en Internet.

**Fines y proceso del Delito de Estafa en la modalidad de Phishing**

Un componente importante en el Delito de Phishing es la captación de datos sobre personas. Número de tarjeta de crédito y de documentos de identidad, números de cuentas bancarias y contraseñas para manejarlas, todos estos datos suelen residir en computadoras personales conectadas a la red. En muchas ocasiones se puede conseguir que el usuario mismo lo facilite. Un ejemplo de Estafa de este tipo consistió en el envío de un Email, presuntamente de una asociación de consumidores dedicada a mejorar la seguridad bancaria, invitando a los usuarios a conectarse a su banco para realizar una averiguación. Ofrecieron en el Email un enlace a varios bancos. Sin embargo, un clic en esta dirección llevó a los usuarios a otro lugar. Los usuarios, creyendo que estaban conectados a la página Web de su banco, abrieron un formulario y lo rellenaron con sus datos, incluyendo, en muchos casos, su contraseña

secreta. Lo que se expuso anteriormente de ejemplo es lo que se denomina en el argot de la informática “Phishing”, variante del verbo “Fishing” pescando.

Un procedimiento más sofisticado es la instalación de un programa espía en la computadora personal. A través de un programa espía, se vigila la actividad del usuario, por ejemplo la contraseña tecleada cuando se conecta con su banco. Se instala en la computadora a través de un anexo a un correo electrónico, o escondido en un archivo de fotos o de música descargada gratuitamente de la web. Este programa espía, gusano electrónico programa troyano, puede ser capaz de mutarse para evitar la detección de un programa antivirus, y pasar desapercibido durante mucho tiempo. Envía la información deseada a un destino oculto, y se autodestruye para que el usuario no se de cuenta de que su información confidencial ha sido espiada. Posteriormente, la información obtenida se puede utilizar para vaciar cuentas bancarias o acceder a servidores protegidos con contraseña.

**Medios de Prueba**

El mayor obstáculo para la admisibilidad y apreciación de elementos de convicción distintos de las pruebas tradicionales -o que estén contenidos dentro de un soporte distinto del documento escrito- ya no radica en restricciones establecidas por el ordenamiento jurídico puesto que, como se verá más adelante, el régimen procesal penal venezolano le otorga cabida a cualquier elemento de convicción que cumpla

con los requisitos de legalidad, licitud, idoneidad y utilidad; la resistencia hacia su incorporación en una investigación radica más bien en la nula o -en el mejor de los casos- muy incipiente cultura tecnológica que ha impedido o retardado la familiarización de todos los sujetos procesales con este tipo de elementos probatorios. Es evidente el natural rechazo que recaerá hacia cualquier elemento que luzca ininteligible para quien, aun cuando tenga la potestad de conducir una investigación, carezca de conocimientos especializados para comprenderlo, interpretarlo y discernir acerca de su relevancia; por ello, al margen del necesario auxilio de los expertos para la "traducción" específica del significado de un rastro contenido en soportes lógicos y no físicos, es necesario identificar y familiarizarse *in abstracto* con todo el espectro probatorio que puede derivarse de los nuevos modos de almacenar, transmitir, conservar y manejar la información, independientemente de la calificación jurídica que puedan merecer los hechos objeto de investigación penal y el grado de responsabilidad penal involucrado.

En Venezuela, aparte de las disposiciones de la Constitución de 1999 que se refieren al uso de la informática por parte del Estado (Arts. 60 y 108), ya se cuenta, desde 2001, con algunas referencias legales concretas que aproximan la equiparación de los soportes informáticos con los documentos escritos:

1. **Decreto-Ley sobre Mensajes de Datos y Firma Electrónica (LMDFE), publicado el 28 de febrero de 2001.**

En materia de eficacia probatoria de mensajes de datos señala lo siguiente:

> **Artículo 4**. Los mensajes de datos tendrán la misma eficacia probatoria que la ley otorga a los documentos escritos, sin perjuicio de lo establecido en la primera parte del artículo 6 de este Decreto-Ley. Su promoción, control, contradicción y evacuación como medio de prueba, se realizará conforme a lo previsto para las pruebas libres en el Código de Procedimiento Civil.
>
> La información contenida en un mensaje de datos, reproducida en formato impreso, tendrá la misma eficacia probatoria atribuida en la ley a las copias o reproducciones fotostáticas.

Esta precariedad probatoria se subsana y la validez y eficacia son plenas cuando dicho mensaje de datos cuenta con una firma electrónica que permita atribuirle la autoría al signatario, siempre que la firma reúna determinados requisitos previstos en la ley. Así lo disponen los artículos 16 y 18 en los siguientes términos:

> **"Artículo 16**. La firma electrónica que permita vincular al signatario con el mensaje de datos y atribuir la autoría de éste, tendrá la misma validez y eficacia probatoria que la ley otorga a la firma autógrafa. A tal efecto, salvo que las partes dispongan otra cosa, la firma electrónica deberá llenar los siguientes aspectos:
>
> 1 Garantizar que los datos utilizados para su generación pueden producirse sólo una vez y asegurar, razonablemente, su confidencialidad.
>
> 2 Ofrecer seguridad suficiente de que no pueda ser

falsificada con la tecnología existente en cada momento.

3 No alterar la integridad del mensaje de datos.

A los efectos de este artículo, la firma electrónica podrá formar parte integrante del mensaje de datos o estar inequívocamente asociada a éste; enviarse o no en un mismo acto."

"**Artículo 18.** La firma electrónica, debidamente certificada por un proveedor de servicios de certificación conforme a lo establecido en este Decreto-Ley, se considerará que cumple los requisitos señalados en el artículo 16."

En cambio, cuando la firma electrónica carece de los requisitos exigidos, sólo podrá ser apreciada como un elemento de convicción valorable conforme a las reglas de la sana crítica (art. 17).

**2. Código Orgánico Tributario (publicado el 17 de octubre de 2001).**

Establece, en materia de notificaciones, el uso válido del correo electrónico como medio para practicarlas siempre que se deje constancia de su recepción en el expediente (art. 162, ord. 3º).

Si bien estas leyes contribuyen decisivamente a facilitar la demostración de las obligaciones asentadas en medios electrónicos -o contraídas a través de ellos- cuando éstas han cumplido con los requisitos establecidos en esas normas -en concordancia

con el artículo 395 del Código de Procedimiento Civil, que adoptó desde 1986 el sistema de libertad probatoria-, sus efectos no siempre son aplicables o transferibles a todo un universo de situaciones desvinculadas completamente de la esfera de sus disposiciones. Precisamente, es ese el caso de la mayor parte del tráfico de datos o de información que circula en las redes o que, simplemente, está contenida dentro de un computador. La eventual inutilidad o irrelevancia de estas disposiciones, surge cuando lo que está en juego es el despliegue de conductas dañinas, prevalidas justamente del uso indebido de la tecnología de información para lesionar bienes jurídicos dignos de protección, es decir, para cometer delitos.

**La Prueba Electrónica**

Es el elemento de convicción que está contenido dentro de sistemas o dispositivos que funcionan mediante la tecnología de información y al cual sólo puede accederse a través del uso de esta tecnología. Website: Alfa-redi, Nº 046 (2002)

Es un elemento de convicción, porque, de su apreciación depende el convencimiento del juzgador acerca del objeto de debate. En este sentido, hasta la discusión que contrapone las afirmaciones a los hechos como objeto de prueba resultaría irrelevante en este caso, puesto que cualquier elemento que proporcionara certeza sobre algo e influyese en la opinión de quien está llamado a apreciarlo

perfectamente podría referirse, en forma indistinta, tanto a hechos como a afirmaciones.

Está contenida en sistemas o dispositivos que funcionan mediante la tecnología de información:

Al incluir en la definición tanto a los sistemas como a los dispositivos como fuentes de prueba, se pretende abarcar todo el universo posible de fuentes de prueba electrónica, puesto que todos los elementos y recursos relativos al uso de la tecnología de información pueden presentarse, dentro de una investigación penal, sólo de dos maneras posibles: en forma de varios componentes integrados para cumplir una función (sistema) o, simplemente como dispositivos, es decir, como elementos que se encuentran aislados o desincorporados de un sistema y que requieren de su integración a éste para conocer su contenido o la carencia de tal. Es conveniente aclarar que esta acepción que adoptamos para el vocablo dispositivo toma en cuenta, exclusivamente, las características que tienen relevancia jurídica desde el punto de vista probatorio y no necesariamente coinciden con la definición tecnológica del término, a la cual nos referiremos más adelante. Pero examinemos separadamente ambos términos.

La definición de **Sistema** prevista en el artículo 2 de la Ley Especial contra los Delitos Informáticos (LEDI), expresa:

> Artículo 2.- (omissis)
>
> "b. Sistema: cualquier arreglo organizado de recursos y procedimientos diseñados para el uso de tecnologías de información, unidos y regulados por interacción o interdependencia para cumplir una serie de funciones específicas, así como la combinación de dos o más componentes interrelacionados, organizados en un paquete funcional, de manera que estén en capacidad de realizar una función operacional o satisfacer un requerimiento dentro de unas especificaciones previstas".

Se observa que esta disposición legal es aplicable al propio computador concebido desde el punto de vista estructural y también a las redes, cuya existencia como tales deriva, precisamente, de la interconexión de varios computadores entre sí, por lo que constituyen un sistema por excelencia.

En cuanto al dispositivo, es un elemento o recurso que forma o puede formar parte de un sistema de Tecnología de Información. Desde el punto de vista tecnológico, los dispositivos pueden dividirse en simples (como un CD) -constituidos por un solo componente o por varios que no interactúan entre sí- y complejos, considerados como subsistemas, cuya estructura integra varios elementos que poseen interacción (un ratón, por ejemplo).

También se puede hablar de dispositivos dependientes, cuyo funcionamiento se encuentra totalmente subordinado a un sistema (caso de una tarjeta gráfica insertada dentro de un computador) y dispositivos independientes, que pueden realizar algunas funciones por su cuenta, separados del sistema principal (tal como ocurre con una cámara digital). Por ejemplo, las unidades extraíbles de almacenamiento de información (CD, diskette, pendrive) son dispositivos, puesto que han sido fabricados para que formen parte de un sistema y sólo a través de su interacción con éste es que pueden funcionar como medio para guardar y recuperar información; sin embargo, es posible que estos elementos –relevantes en una investigación penal- se presenten en forma aislada, sin que el sitio del hallazgo los vincule con un sistema específico que indique de manera inmediata su uso en la comisión de delito alguno. Sin embargo, el posterior examen de estos dispositivos –aún cuando el sistema o sistemas específicos de los que formaron parte no aparezcan jamás- podría aportar elementos reveladores de la comisión de delitos. De allí que, desde el punto de vista probatorio, al margen de la clasificación tecnológica de los dispositivos, su relevancia jurídica nace de la circunstancial separación del sistema al cual estaban o podrían estar integrados y del cual habrían sido considerados como parte si se hubiesen presentado unidos a él.

**Prueba pericial informática**

Es el Medio de Prueba, de suma importancia para cualquier actuación judicial y/o arbitraje que precisen conocimientos científicos o técnicos especializados. En lo que

se refiere a pericias informáticas, hay que tener en cuenta, que no siempre se relaciona con delitos informáticos exclusivamente, es decir, no siempre que la informática forma parte de un asunto judicial es con motivo de un delito. La informática puede verse implicada, por ejemplo:

- Cuando es utilizada como medio de un delito.
- Cuando la informática es el objeto propio del delito (ejemplo: compra de software ilegal)
- Cuando tiene lugar en el conflicto de forma colateral, pero en ocasiones, determinante.
- Los incumplimientos de contratos de programación y desarrollo.

**La Inspección Judicial**

El juez podrá percibir con sus propios sentidos mensajes de datos, contenidos de páginas web, ver imágenes, percibir sonidos y observar todos los fenómenos multimedia para incorporarlos al expediente.

El aspecto negativo de este medio es el que las partes que no estén interesadas en la prueba pueden procurar el cambiar los contenidos o borrarlos a efectos de que no queden incorporados por este medio en el proceso. En los casos en que se trate de utilizar la jurisdicción voluntaria, se sabe que puede estar supeditada a la ratificación de las inspección de este tipo dentro del proceso, momento para el cual puede haber

cambiado o desaparecido los documentos informáticos. Aunque los buscadores o motores de búsqueda guardan versiones de las páginas para poder indexarlas, existen varios sitios páginas web encargadas de archivar las diversas versiones de otros sitios lo cual puede ser un recurso alterno probatorio. Lo ideal es que la inspección se haga directamente sobre el sitio, pero en caso de que no sea posible se podrá captar cualquier tipo de información archivada en diversos tipos de servidores y se puede considerar captación y registro como indicio de la existencia de sitios o su contenido.

Los inventarios de equipos, la identificación de máquinas, con su hardware y el software instalado deben ser verificados por esta vía.

Los jueces o funcionarios también pueden dejar constancia por este medio de la existencia de mensajes de datos en computador o computadores tanto del emisor, así como del destinatario y terceros a los que se haya copiado o reenviado el mensaje.

**El reconocimiento y la inspección como medios de prueba electrónica**

La autora española Sanchis (1999) niega a los soportes informáticos cualquier posibilidad de ser objeto de la prueba de reconocimiento puesto que, en su criterio, "dicha prueba estaría circunscrita a la apreciación de sus exterioridades, por lo que su verdadera relevancia pasaría inadvertida para el juez". Esta afirmación se sustentaría en la identificación que hace la autora de la incompatibilidad manifiesta entre la característica más resaltante del soporte informático -que es la imperceptibilidad de

su contenido- y la naturaleza de la prueba de reconocimiento –que radica en la percepción directa a través de los sentidos-.

La prueba de reconocimiento o inspección tiene un alcance limitado; sin embargo, jamás se debe descartar la posibilidad de que pueda resultar útil en un momento dado, sobre todo cuando pueda desarrollarse en combinación con los otros medios de prueba. Ese podría ser el caso de la comisión de delitos contra la propiedad intelectual realizados mediante el uso de tecnología de información, en los que la identificación "a primera vista" de copias no autorizadas de una obra del intelecto podría establecerse perfectamente a través del reconocimiento de los propios dispositivos de almacenamiento (CDs o DVDs) sin perjuicio de la utilidad de combinarlo con cualquier otra diligencia probatoria que estuviere orientada hacia un cauce procesal distinto.

**Experticias sobre Mensajes de Datos y Correo Electrónico**

Para este tipo de experticias muchas veces es necesario, que se le de acceso al perito al computador en donde se ha recibido el mensaje de datos. Debe hacerse un análisis detallado de la meta data o datos ocultos que guardan la información, tales como la Dirección IP del remitente, la información sobre el programa o aplicación utilizado para enviarlo, su versión, información sobre el proveedor de servicios de correo o agentes de mensajes de datos.

Es posible que una vez conocidos los datos ocultos del mensaje de datos, sea necesario requerir al proveedor de servicios de Internet (ISP[), los datos relacionados con esa dirección IP en una fecha y hora determinada. Los expertos también pueden dirigirse a verificar la información en los computadores que han servido como canal para el envío de los mensajes, como los servidores de correo a efectos de verificar las bitácoras o registros internos de estos conmutadores en los que queda registrada la actividad de los usuarios. Es muy probable, que se promueva experticias del computador o computadores del presunto emisor, donde se puede tratar de ubicar el mensaje en los archivos de elementos o mensajes de datos enviados.

En muchas oportunidades, la parte a la que no le interesa este tipo de prueba, puede realizar maniobras de cambio o eliminación de la Evidencia Digital, cambio de equipos, borrado de información puntual o formateo de discos duros y otro tipo de recursos dolosos (que pueden ser ilícitos), para evitar se prueben hechos. Los peritos deberán comunicar sus evaluaciones y resultados en base a la información que encuentren.

Uno de los primeros casos famosos relacionados con este tipo de experticia sobre mensajes de datos fue el del escándalo de los Irán Contras en los Estados Unidos, donde el indiciado era el militar norteamericano Oliver North, quien había borrado mensajes de datos de su computador, pero la evidencia fue encontrada en los respaldos o backups alojados en los servidores destinados a este efecto.

**Procedimientos de obtención y resguardo de medios probatorios**

La volatilidad de los datos en lo que a prueba informática se refiere exige las máximas precauciones a la hora de obtener el *corpus instrumentorum* - aquellos medios o instrumentos que utilizó el imputado o indiciado para cometer un hecho delictuoso-. Dicha actividad comienza desde el momento del allanamiento mismo. Los métodos tradicionales de búsqueda y el hallazgo de la prueba en todas las investigaciones, no resultan suficiente para el éxito en los procedimientos por delitos informáticos. Aquello que se halló en el lugar del hecho, debe ser exactamente lo que llegue al ámbito del perito, para su análisis y dictamen**.**

No escapa a la lógica más simple suponer que, al procederse el diligenciamiento de una orden de allanamiento, quienes resultan afectados y, de alguna manera se saben partícipes de una actividad delictual, intentarán por todos los medios evitar que los funcionarios intervinientes obtengan elementos probatorios que pudieren incriminarlos. Partiendo de esta natural reticencia a que prospere la medida judicial, debe tenerse en cuenta que, cuando aquello que resulta de interés se halla almacenado en computadoras, por lo general, sus operadores conocen las rutinas que deben llevarse a cabo rápidamente para eliminar los registros comprometedores o bien inutilizar completamente los sistemas.

A fin de no echar por tierra la labor investigativa previa es menester como primera medida disponer el alejamiento de toda persona que se halle en presencia de los computadores, servidores o tableros de suministro eléctrico, para proceder, inmediatamente a desconectar la totalidad de los teclados hasta que cada uno de los terminales sea examinado por los expertos.

Dada la increíble diversidad de aplicaciones, utilidades, sistemas operativos, etc., normalmente, el perito ha de utilizar "herramientas" consistentes en *software* específico que permita acceder a la información almacenada en los computadores. El idóneo que asesora a las autoridades que realizan el allanamiento debe explicar claramente a los testigos cada una de las tareas que realiza y la finalidad de las aplicaciones que utiliza, velando por la exacta transcripción de sus especificaciones en el acta respectiva.

La labor de asegurar la prueba consiste fundamentalmente en establecer que el contenido de las unidades de almacenamiento (discos rígidos, CD, diskettes u otros) al momento de procederse a su secuestro a fin de que, eventualmente se pueda confirmar que éste es idéntico al que se sometió a dictamen pericial posterior.

Las operaciones deben realizarse, en consecuencia, en presencia de los testigos y de los imputados, el operador debe explicar paso a paso las tareas que realiza.

Atento el carácter preponderantemente escrito de nuestra tradición judicial y a la carencia de medios técnicos para permitir la visualización del material secuestrado en cada oportunidad que el juzgador o las partes lo requieran, es imprescindible trasladar a papel el contenido de los soportes de almacenamiento a secuestrar, para evitar luego que se pretenda argüir adulteraciones en los mismos. Para ello han de listarse todos los directorios o carpetas, según el sistema operativo de que se trate, de modo que quede expresamente consignado el nombre del archivo, su extensión, su tamaño ("peso"), fecha y hora de su última modificación y atributos de accesos. Es conveniente, además que los listados se realicen sobre el denominado papel continuo ya que abreviará el trámite posterior, requiriendo solo la rúbrica de los intervinientes en la primera y última hoja, siendo conveniente asegurar los troquelados con cinta adhesiva o elemento similar. Este material formará anexos del acta de allanamiento que revisten su mismo carácter instrumental.

Hecho esto, se procede al secuestro de las unidades. Es importante tener en cuenta que, en principio carece de relevancia el traslado de la totalidad de monitores y teclados, toda vez que ellos no intervienen en el almacenamiento de información de interés para la causa, la cual si se halla en las unidades de control o CPU. No obstante ello, en función a la gran variedad de marcas, modelos, clones, etc. es conveniente que el experto determine si resulta necesario trasladar tales elementos a fin de permitir su puesta en funcionamiento en laboratorio a los fines periciales.

Básicamente, el tratamiento que debe darse al computador consiste en franjado de todas las conexiones de entrada y salida, ya sea de datos, periféricos o energía y los accesos a unidades de discos flexibles, rígidos removibles, o unidades de back-ups. Finalmente, se debe franjar toda la periferia, evitando la posibilidad de que se desmonten sus partes componentes, todo ello con la rúbrica de funcionarios y testigos.

Idéntico tratamiento se aconseja para los discos extraíbles o elementos menores que deberán ser colocados preferentemente en cajas debidamente aseguradas para su traslado. En tanto todos los elementos permanezcan así conservados, no se albergarán dudas sobre su contenido actual. Finalmente, de resultar técnicamente factible es conveniente contar con una filmación continua de la diligencia de allanamiento y secuestro o, en su defecto del audio directo donde se identifiquen claramente las indicaciones de lo peritos sobre los trabajos realizados y los testigos puedan, eventualmente identificar sus voces.

**Peritos Informáticos**

Con respecto a las características de los peritos, un perito informático debe ser un profesional del peritaje informático, no un experto en una sola área de la informática. Es decir, un informático preparado, idóneo en varias disciplinas, y sobre todo, eficaz "perito en la materia".

**Los Indicios en el Derecho Informático**

Todos los hechos que indirectamente orienten al juez hacia la convicción de que un hecho jurídico informático se ha producido, o si bien se ha producido de una forma determinada podrán ser evaluados bajo las normas de valoración de la Sana Critica aunque no se puede probar su existencia directamente. En muchas ocasiones se presentaran solo indicios de hechos informáticos, dada la posibilidad de que varíe o desaparezca las pruebas digitales.

La conducta procesal de las partes también podrá constituirse en un indicio en su contra. Si se designan peritos para la práctica de una experticia de un computador o una red o sobre servidores y se impide el acceso a los equipos o bien se bloquea, cambia o borra la información contenida en los mismos, podría constituirse en un indicio de la pre-existencia de documentos electrónicos. Un conjunto de indicios de hechos jurídicos informáticos podrían ser valorados conforme a la Sana crítica a efectos de establecer la convicción sobre un punto de hecho con sus consecuencias jurídicas respectivas.

**Los rastros o soportes electrónicos como prueba documental**

Sostiene Bacigalpo (2002), que la posibilidad de creación electrónica de documentos no ha modificado el concepto de documento en sí mismo. El autor afirma que "lo que ha cambiado son las maneras en las que se llevaban a cabo las funciones

tradicionales del documento, básicamente el tipo de soporte en el cual se perpetúa la declaración de la voluntad que se documenta, la forma de garantizar la imputación del contenido de la declaración a quien la realizó y la prueba de la autenticidad mediante una certificación de determinados signos, análoga a una certificación de carácter notarial, a través de un servicio de certificación electrónico.

El problema dentro del proceso penal nos lo resuelve la referencia que aporta la Ley de Especial de contra los Delitos Informáticos (LEDI), que define al documento -dentro del ámbito de la tecnología de información- como un "registro incorporado en un sistema en forma de escrito, video, audio o cualquier otro medio, que contiene datos o información acerca de un hecho o acto capaces de causar efectos jurídicos" (art. 2, lit. e), es decir, que equipara al documento escrito a cualquier soporte o rastro que reúna los requisitos de fidelidad y perdurabilidad sobre los cuales se sustente la seguridad o certeza de su contenido.

La **fidelidad** consiste en la seguridad de que lo representado coincide con lo que efectivamente se realizó y que, al quedar plasmado, no puede quedar comprometido por la acción del tiempo sobre la memoria humana.

La **perdurabilidad** la proporciona la constante disponibilidad de lo representado tal y como acaeció: en cualquier momento puede acreditarse la existencia del derecho o que las cosas sucedieron de determinada manera.

Para ilustrar lo dicho, se toma como ejemplo el caso de la comisión de dos hechos punibles que pueden cometerse mediante el uso de la tecnología de información –aunque no estén categorizados como delitos informáticos-, como podrían ser la difamación o la instigación a delinquir perpetradas desde un dominio (sitio web). En estos casos, la prueba documental constituiría el medio por excelencia para la demostración de su comisión e inclusive de su autoría, ya que los proveedores de servicios de INTERNET, así como los verificadores de registros de dominios suelen guardar y poner a disposición de quien los solicite, los registros acerca de los contenidos puestos en línea y también, los datos de identificación de los administradores, contactos técnicos y pagadores de los dominios desde donde se hubiesen generado los contenidos considerados delictivos.

**Principios de Identificación de las Actividades en Internet**

Todo usuario que tiene acceso a Internet necesita de los servicios de los llamados Proveedores de Servicios de Internet (ISP), que dan acceso a particulares a la llamada súper autopista de la información. Los usuarios son identificados por el proveedor, por lo que en manos de estos está información fundamental para el establecimiento de la verdad de los hechos informáticos relacionados con este tema. Cada vez que un usuario del servicio se conecta a Internet, comienza lo que desde el punto de vista informático se denomina una sesión de acceso. Las sesiones de acceso son controladas por los servidores del proveedor de servicios, que registran en las

llamadas *bitácoras* (Logs), datos esenciales para la investigación de los hechos informáticos. Cuando la conexión a Internet se hace vía telefónica (Dial Up), el servidor correspondiente del ISP registra el número de teléfono desde el cual se esta haciendo la conexión, lo que sirve a su vez para ubicar la sede física o lugar desde el cual se realizó el acceso para navegación, envío de mensajes de datos, etc. Los computadores relacionados con hechos informáticos también poseen la información y configuración de acceso a los proveedores, para que se pueda establecer contacto entre proveedor y los usuarios, lo cual puede constatarse preferiblemente por vía de inspección o experticia.

**La Dirección IP**

Cada vez que se comienza una sesión de acceso a Internet, se le asigna al usuario un número de identificación único a nivel mundial denominado Dirección IP. Los proveedores de servicios de Internet poseen un gran rango de números de identificación disponibles, que son asignados a los usuarios durante las diversas sesiones de acceso. La dirección IP asignada al usuario es guardada también en las bitácoras de los servidores del proveedor y es capturada por la mayoría de los programas de telecomunicación informática, tales como programas o aplicaciones Web de correo electrónico servidores de Internet y navegadores. De lo antes expuesto podemos deducir que al enviarse y recibirse los mensajes de datos, los receptores de la dirección IP del emisor puede ser extraída de estos mensajes.

Existen Proveedores de Servicios de Internet, que asignan direcciones IP fijas a sus usuarios. Es común que estos casos sean los de servicios de televisión por acceso combinados de televisión por cable. El servicio de acceso a Internet por Banda Ancha (ADSL), por sus características técnicas, hace posible que un mismo usuario use o detente una sola dirección IP, por días o meses lo que hace posible una identificación rápida de los usuarios. Las direcciones IP en estos casos pueden variar un mismo día.

**Los Mensajes de Datos**

Mensaje de Datos es toda información inteligible en formato electrónico o similar que pueda ser almacenada o intercambiada por cualquier medio. La característica principal del mensaje de datos es la posibilidad de intercambio de información. Dentro de este concepto legal amplio entrarían las páginas Web, toda vez que el propietario, administrador y muchas veces los usuarios de páginas Web pueden publicar información subiéndola al servidor Web. Una vez que se encuentra la información en el servidor y que por ende la misma es publica, terceros pueden acceder a ella, con lo que se configuraría el intercambio.

**Correo Electrónico (Email)**

Uno de los medios de intercambio de información más comunes donde existen aplicaciones o programas que sirven para redactar y leer mensajes de datos que por lo

privados porque se generan por un usuario llamado Emisor, para ser recibidos por una o mas personas usuarios de cuentas de correo llamados receptores o destinatarios. Los mensajes de datos de este tipo pueden ser enviados a una o más personas. Los mensajes de datos de este tipo cuando se trata de aplicaciones o programas (software), después de ser escritos, se envían a través de los llamados Agentes de Transmisión de Correo, que son programas ubicados en servidores que sirven como especie de oficinas postales dirigiendo los mensajes de datos de este tipo o bien a otros Agentes de Transmisión de Correo o bien a su destinatario final. Los mensajes de datos vía correo también pueden ser generados por programas que se activan desde los navegadores Web, tales como el Explorer, Netscape o otros. Los sitios como Hotmail.com permiten que en un computador se genere un mensaje de datos tipo correo-e, se envíe a otra cuenta de correo-e que posteriormente puede ser visto por otro usuario en un mismo computador.

**Autoría del Mensaje del Correo Electrónico**

El envío de un mensaje de datos vía correo electrónico por técnicas universalmente aceptadas implica la captura de la dirección IP del usuario que lo envía, la hora en que se realiza el envío, la hora en que el mensaje pasa los por Agentes de Transferencia de los Mensajes (MTA) de datos. Los Agentes de transferencia de mensajes de datos juegan un papel fundamental probatorio, por cuanto van agregando datos de horas de envío y recepción a las llamadas cabeceras

de los mensajes de datos, que podemos comparar imaginaria y analógicamente con los sellos que van colocando las oficinas de correo postal a los sobres que procesan.

**Existencia de una cuenta de correo determinada**

Para establecer si una cuenta de correo existe o si la misma ha sido falsificada o inventada, existe por supuesto la posibilidad de dirigirse al administrador del servidor o de la empresa encargada del mismo a efectos de que se suministren los datos del usuario. Si no se tiene acceso directo a la misma su pueden realizar pruebas de experticia o de experimentos, en los cuales se pueden enviar mensajes de prueba y establecer el comportamiento del sistema para determinar si son retornados o no para demostrar la actividad o vigencia de una cuenta de correo determinada, lo que puede indicar o ser indicio de la posibilidad de emisión de un mensaje de datos. El hecho de que un mensaje de prueba rebote de una cuenta no significa que la cuenta no ha existido. Las cuentas de correo electrónico pueden ser creadas y borradas por los administradores de los servidores de correo y es por ello que pueden obtener pruebas dentro del servidor como logs de ejecución de este tipo de comandos. Pueden existir también pruebas indiciarias que indiquen la existencia de direcciones de correo determinadas y la relación con sus presuntos autores.

La configuración del programa de correo, hace que cuando se configura un programa para el uso de una cuenta de correo, se coloque el nombre del usuario, lo

cual constituirá un indicio de la titularidad de la cuenta. El Login o nombre de usuario de la cuenta puede ser también otro indicio de hecho, al igual que la coincidencia de iníciales o de silabas que formen parte del nombre y apellidos de una persona, o bien la combinación de números. En una caso donde no se impugne o desconozca una mensaje de datos debe tenerse como aceptada la existencia de la cuenta del emisor.

Cuando se investiga una cuenta de correo relacionada presuntamente con un Dominio o nombre web tipo www.dominio.com, pueden realizarse estudios periciales a efectos de establecer si efectivamente ese dominio esta apuntado a un servidor con servicios de correo activos. La tecnología permite el que existan nombres de Dominio activos que apunten o dirija en navegador a un servidor sin que necesariamente se tenga activado el servicio de correo en el mismo. Esto es posible gracias que los propietarios de dominios puede utilizar servicios de redireccionamiento, que hacen por ejemplo que cualquier correo-e enviado a una dirección propia determinada se reenvíen automáticamente a otra cuenta de correo, funcionando similar a un servicio telefónico de transferencia de llamadas. Existen gran cantidad de variables desde el punto de vista técnico que deben ser verificadas por expertos o peritos a efectos de que se establezca el origen o procedencia de los mensajes de datos, su emisor y destinatario.

**Titularidad de las cuenta de correo**

**Correo Gratuito:** La información sobre la titularidad de una la cuenta de correo electrónico en servidores gratuitos, como por ejemplo, Hotmail.com, es resguardada por políticas de privacidad. Leyes de algunos países regulan el control y resguardo de este tipo de información, por lo que el acceso a la misma deberá principalmente realizarse por requerimiento judicial.

Uno de los problemas típicos de este tipo de cuentas es el anonimato que buscan muchos usuarios, suministrando datos falsos en las planillas de inscripción y registro de estos servicios. A todo evento debemos mencionarse que lo mas seguro es que la mayoría de los servicios resguarden otros datos como la dirección IP del usuario al momento de registro lo que puede generar indicios y elementos de prueba susceptibles de ser utilizados en juicio.

***Correo Privado***: En los casos de cuentas de correo de servidores privados, se puede requerir información al administrador o al propietario del sitio Web. La dirección y datos del administrador de un sitio Web puede ser obtenida vía Inspección Ocular con asistencia de práctico, toda vez que al realizarse el registro de un dominio es indispensable el que se coloquen los datos del propietario, administradores y responsables lo cual es por lo general de acceso público a través de diversas páginas web.

Adicionalmente pueden practicarse experticias e inspecciones en computadores que se sospechan como los que dieron origen a los mensajes de datos o como aquellos donde fueron recibidos, en donde se puede revisar su configuración para determinar si en los programas destinados a la redacción y lectura se encuentran datos relacionados con las cuentas de correo involucradas en un caso. La configuración de equipos para la conexión a Internet y las de uso de cuentas de correo pueden ser elementos importantes para el establecimiento del uso de cuentas de correo, así como del envío y recepción de mensajes de datos.

**Repercusión Social y Económica**

La proliferación de los delitos informáticos ha hecho que nuestra sociedad sea cada vez más escéptica a la utilización de Tecnologías de la Información, las cuales pueden ser de mucho beneficio para la sociedad en general. Este hecho puede obstaculizar el desarrollo de nuevas formas de hacer negocios, por ejemplo el comercio electrónico puede verse afectado por la falta de apoyo de la sociedad en general. También se observa el grado de especialización técnica que adquieren los delincuentes para cometer éste tipo de delitos, por lo que personas con conductas maliciosas cada vez más están ideando planes y proyectos para la realización de actos delictivos, tanto a nivel empresarial como a nivel global. También se observa

que las empresas que poseen activos informáticos importantes, son cada vez más celosas y exigentes en la contratación de personal para trabajar en éstas áreas, pudiendo afectar en forma positiva o negativa a la sociedad laboral de nuestros tiempos. Aquellas personas que no poseen los conocimientos informáticos básicos, son más vulnerables a ser víctimas de un delito, que aquellos que si los poseen. En vista de lo anterior aquel porcentaje de personas que no conocen nada de informática (por lo general personas de escasos recursos económicos) pueden ser engañadas si en un momento dado tienen acceso a recursos tecnológicos y no han sido asesoradas adecuadamente para la utilización de tecnologías como la Internet, correo electrónico, etc. La falta de cultura informática puede impedir de parte de la sociedad la lucha contra los delitos informáticos, por lo que el componente educacional es un factor clave en la minimización de esta problemática.

**Bases Normativas**

Existen diversos instrumentos normativos que permiten ser el soporte a la investigación.

El Consejo de Europa suscribió el Convenio sobre la Cibernética (Budapest, 23.XI.2001), donde establece en su cuerpo normativo:

> **"Artículo 8 - Fraude informático.** Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos

> deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante:
>
> a) cualquier introducción, alteración, borrado o supresión de datos informáticos;
>
> b) cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona.”

El artículo in comento es norma de Derecho Internacional, la cual recomienda tomar medidas para tipificar el delito de fraude en los derechos internos de los países.

La Constitución de la República Bolivariana de Venezuela (CRBV, 1999), consagra el derecho a la privacidad y establece:

> **“Artículo 48**. Se garantiza el secreto e inviolabilidad de las comunicaciones privadas en todas sus formas. No podrán ser interferidas sino por orden de un tribunal competente, con el cumplimiento de las disposiciones legales y preservándose el secreto de lo privado que no guarde relación con el correspondiente proceso.”

Este artículo de la norma fundamental refiere, como lo expresa claramente, no podrán ser violentadas la comunicación privada, y es entendible que un correo electrónico, a parte de ser un medio de comunicación, es privado, y como tal es secreto y debe ser protegido por el Estado.

También la Carta Magna establece:

> **"Artículo 60.** Toda persona tiene derecho a la protección de su honor, vida privada, intimidad, propia imagen, confidencialidad y reputación. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y ciudadanas y el pleno ejercicio de sus derechos."

Este artículo expone que las personas tienen derecho a la protección de su privacidad, reputación etc. así como la ley regula el uso de la informática, con el fin mismo de protección a la vida privada de las personas y su entorno familiar

La Ley Especial contra los Delitos Informáticos (2001) señala:

> **"Artículo 14.- Fraude.** El que, a través del uso indebido de tecnologías de información, valiéndose de cualquier manipulación en sistemas o cualquiera de sus componentes o en la data o información en ellos contenida, consiga insertar instrucciones falsas o fraudulentas que produzcan un resultado que permita obtener un provecho injusto en perjuicio ajeno, será penado con prisión de tres a siete años y multa de trescientas a setecientas unidades tributarias."

Este artículo de la ley, es el más reciente que penaliza a este tipo de delitos, la cual establece que cualquier persona que logre insertar algún tipo de información falsa para un provecho injusto para si o para otro será sancionado penalmente con privación de libertad y sancionado pecuniariamente.

> **"Artículo 3. Extraterritorialidad.** Cuando alguno de los delitos previstos en la presente ley se cometa fuera del territorio de la República, el sujeto activo quedará sujeto a

> sus disposiciones si dentro del territorio de la República se hubieren producido efectos del hecho punible y el responsable no ha sido juzgado por el mismo hecho o ha evadido el juzgamiento o la condena por tribunales extranjeros.”

El artículo anterior de la ley in comento, hace mención cuando el delito es cometido fuera de nuestras fronteras, el delincuente queda sujeto a las normativas de nuestro país si se produce algún efecto nocivo y no ha sido juzgado por el mismo hecho o evadido la condena.

El Código Penal Venezolano (2005) expresa que:

> **“Artículo 462**. El que, con artificios o medios capaces de engañar o sorprender la buena fe de otro, induciéndole en error, procure para sí o para otro un provecho injusto con perjuicio ajeno, será penado con prisión de uno a cinco años. La pena será de dos a seis años si el delito se ha cometido:
>
> 1. En detrimento de una administración pública, de una entidad autónoma en que tenga interés el Estado o de un instituto de asistencia social.
>
> 2. Infundiendo en la persona ofendida el temor de un peligro imaginario o el erróneo convencimiento de que debe ejecutar una orden de la autoridad.
>
> El que cometiere el delito previsto en este artículo, utilizando como medio de engaño un documento público falsificado o alterado, o emitiendo un cheque sin provisión de fondos, incurrirá en la pena correspondiente aumentada de un sexto a una tercera parte.”

**Código Penal de España**

El Artículo 197 Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, establece que:

> **"**1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.
>
> 2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.
>
> 3. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.
>
> Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.
>
> 4. Si los hechos descritos en los apartados 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, se impondrá

la pena de prisión de tres a cinco años, y si se difunden, ceden o revelan los datos reservados, se impondrá la pena en su mitad superior.

5. Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o un incapaz, se impondrán las penas previstas en su mitad superior.

6. Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado 5, la pena a imponer será la de prisión de cuatro a siete años."

Asimismo, el artículo 248 expresa:

"También se consideran reos de estafa los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero. La misma pena se aplicará a los que fabriquen, introdujeren, poseyeren o facilitaren programas de ordenador específicamente destinados a la comisión de estafas previstas en este artículo"

**Código Penal de Colombia**

Ley 1273, por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado "De la Protección de la información y de los datos":

**Artículo 269G**.

**"Suplantación de sitios web para capturar datos personales.** El que con objeto ilícito y sin estar facultado

> para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.”

Este artículo es muy preciso y se podría pensar que los delitos informáticos orientados a capturar datos personales no siempre se harán por suplantación de páginas ya que con el pasar del tiempo nuevas técnicas pueden ser implementadas para el mismo fin.

**Código Penal de Costa Rica**

Ley No. 8148, Adición al Código Penal, Ley Nº 4573, el artículo 217 bis, el cual establece:

> "**Fraude informático.** Se impondrá pena de prisión de uno a diez años a la persona que, con la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero, influya en el procesamiento o el resultado de los datos de un sistema de cómputo, mediante programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema."

**Definición de Términos Básicos**

En el presente trabajo de investigación se encuentran definiciones básicas, las cuales permitirán una mejor compresión del tema planteado.

**Datos**

Informaciones no elaboradas y que una vez procesadas (ordenadas, sumadas, comparadas, etc.) constituyen lo que se denomina información útil.

**Criptografía**

(Del griego kryptos (ocultar) y grafos (escribir), literalmente escritura oculta, la criptografía es el arte o ciencia de cifrar y descifrar información).

**Estafa**

Es un delito que se caracteriza, frente a los demás delitos contra la propiedad o el patrimonio, porque la conducta activa del autor consiste en un engaño que contribuye a su propio enriquecimiento.

Existen diferentes modalidades de Estafa, ya que se entiende que el engaño se puede producir tanto de un modo activo (lo más frecuente) como de un modo pasivo (el supuesto clásico es el de la persona que abandona un hotel sin pagar).

**Estafa Informática**

Consistente en la manipulación a través de un computador o artificio similar, con ánimo de lucro para inducir al error y se consiga una transferencia de cualquier activo patrimonial en perjuicio de tercero.

**Fraude**

(lat. fraudem). Acto realizado para eludir una disposición legal en perjuicio del Estado o de terceros, o para burlar los derechos de una persona o de una colectividad.

**Internet**

Red de datos ideada para transmitir imagen y voz.

**Phishing**

Es la capacidad de duplicar una página web para hacer creer al visitante que se encuentra en la página original en lugar de la copiada. Normalmente se utiliza con fines delictivos duplicando páginas web de bancos conocidos y enviando indiscriminadamente correos para que se acceda a esta página a actualizar los datos de acceso al banco.

En ocasiones, el término "*phishing*" se dice que es la contracción de "*password harvesting fishing*" (cosecha y pesca de contraseñas), aunque esto probablemente es un acrónimo retroactivo.

De forma más general, el nombre *phishing* también se aplica al acto de adquirir, de forma fraudulenta y a través de engaño, información personal como contraseñas o detalles de una tarjeta de crédito, haciéndose pasar por alguien digno de confianza

con una necesidad verdadera de tal información en un e-mail parecido al oficial, un mensaje instantáneo o cualquier otra forma de comunicación. Es una forma de ataque de la ingeniería social.

**Matriz de Variables**

**Analizar el Delito de Estafa Informática en la modalidad de Phishing**

| Objetivos Específicos | Variables | Dimensiones | Indicadores |
|---|---|---|---|
| **Determinar los medios probatorios y su licitud** | **Medios de Prueba** | **Tecnológica**<br>**Normativa**<br>**Tipos** | **Computadoras**<br>**Legislación Procesal penal** |
| **Indagar el la repercusión del Delito de Phishing en la vida social y económica para enfrentarlo legalmente** | **Impacto del Phishing** | **Social**<br>**Económico** | **Edad, clase social, sexo** |
| **Examinar la legislación comparada para tipificar y penalizar los delitos de Phishing** | **Legislación Comparada** | **País**<br>**Tipificación**<br>**Pena** | **Localidad**<br>**Delito**<br>**Legislación Penal Comparada** |

# CAPÍTULO III

# MARCO METODOLOGICO

## Nivel y Modalidad de la Investigación

La investigación es de nivel descriptivo-informativa porque permitió reseñar y reconocer los diferentes elementos que se interrelacionan para llevar a cabo la investigación. Según, Hernández, Batista (1991) el estudio descriptivo conlleva **"**el propósito que tiene el investigador de descubrir situaciones o eventos, es decir, como es y como se manifiesta determinado fenómeno; los estudios descriptivos buscan especificar las propiedades importantes de personas, grupos, comunidades o cualquier otro fenómeno que sea sometido a análisis**"**.

De esta manera, el estudio descriptivo identifica características del universo de la investigación, señala formas de conducta y actitudes de lo investigado, establece, descubre y comprueba asociaciones entre variables de investigación.

La investigación se ubica dentro de la modalidad específica de recopilaciones documentales y bibliográficas, que intentará establecer los efectos legales, sociales y económicos generados por el Phishing perpetrado a través de la Internet. Para ello, se

recopiló información actualizada, que permitió esbozar algunas conclusiones sobre la problemática planteada.

Según Alfonso (1995), la investigación documental es un procedimiento científico, un proceso sistemático de indagación, recolección, organización, análisis e interpretación de información o datos en torno a un determinado tema. Al igual que otros tipos de investigación, éste es conducente a la construcción de conocimientos.

**Técnicas e Instrumentos para la Recolección de Información**

Los datos empleados en la investigación han sido recolectados mediante documentos escritos, por esta razón el diseño del presente trabajo es de tipo documental, por ello, para llevar a cabo esta investigación se recurrió a las siguientes técnicas:

**Observación,** permitió revisar la documentación pertinente a la investigación. Según, Sabino, Carlos (1992), **"**como el uso sistemático de nuestros sentidos en la búsqueda de los datos que se necesitan para resolver un problema de investigación. Dicho de otro modo, observar es percibir activamente la realidad exterior con el propósito de obtener los datos que, previamente, han sido definidos de interés para la investigación**"**.

**Revisión documental,** Permitió el reconocimiento del material de texto de varios autores destacados en el tema que se investiga, es decir, se utilizó la revisión documental, la cual trató de la verificación de los textos referentes al tema, para su clasificación. Se utilizó la lectura de trabajos de grado, ponencias, (obtenidas a través de internet), textos, que guardan relación con el tema a investigar. Por otro lado se utilizó el subrayado el cual consiste en resaltar las ideas más importantes de los documentos utilizados; así como, también se elaboraron resúmenes de dicho documento.

Los instrumentos que se utilizaron en la recolección de datos estuvo constituidos por: Cuaderno de notas, Pendrive y Computadora, lo cual permitió el análisis de información, se utilizó el análisis descriptivo, para establecer y clasificar con claridad la información recolectada.

El programa computarizado de uso comercial, que se empleó fue el procesador de palabras Microsoft Word 2007, el cual permitió la transcripción de la información recolectada.

**Procedimiento**

De acuerdo al tipo de diseño investigativo, ya mencionado, y para lograr alcanzar los objetivos propuestos, se procedió de la siguiente manera:

a) Se acopió de manera sistemática los textos, leyes pertinentes con el tema investigado atendiendo al criterio de autenticidad e integridad de fuentes primarias; tratando de cubrir el universo epistemológico**.** Realizando, a posteriori, una organización de las mismas, indicando las respectivas referencias bibliográficas de los documentos consultados.

b) Seguidamente, se procedió a una clasificación detallada para extraer de ellas todos los datos indispensables, acumulándolos para la cabal sustentación teórica del planteamiento del tema y que tendría incidencia directa en la conclusión. Realizando, para ello, una lectura comprensiva, analítica y discriminatoria que permitió organizar los distintos títulos y subtítulos planteados.

c) Todo lo anterior conllevó a los resultados explanados en la conclusión de la investigación y permitió hacer las recomendaciones subsecuentes.

En cuanto a la revisión documental, se seleccionó lo que es relevante para el trabajo de investigación, a través de los textos normativos y doctrinarios Existentes, usando la técnica del subrayado, se realizó la clasificación, por autor, subtema y año de edición. Seguidamente se obtuvo, el conocimiento de las Bases Legales a través de la lectura a título informativo de las fuentes disponibles, entre las que se encuentran en la legislación venezolana tanto sustantiva como adjetiva, Para la interpretación de

los artículos legales aplicables, se utilizó el método de la hermenéutica jurídica, que permitió emplear la norma indagando su sentido, significado, estructura e intención del legislador.

En lo que respecta al tratamiento de la información, fue cotejada, subrayada, y fichada para su análisis, la cual es en forma descriptiva.

Por último se completó la fase interpretativa, la cual nos permitió llegar a las conclusiones buscadas, en esta etapa se realizó el análisis del contenido para lograr un informe final de investigación, de donde se concluyen las respuestas a las interrogantes planteadas en los objetivos del presente trabajo.

# CAPÍTULO IV

## ANALISIS DEL CONTENIDO

El delito de Estafa en su modalidad Phishing, consiste en suplantar la identidad de una persona o institución, a los efectos de obtener información sensible de un tercero. Actualmente esta práctica se le relaciona con medios electrónicos, ya que la principal forma de ejercerla es a través de Internet, pero su aplicación a través de llamadas telefónicas, sms y servicios postales se viene realizando desde hace mucho tiempo.

El estafador envía un correo desde la dirección "atencionalcliente@banco.com", este correo aunque posea al final un nombre de dominio valido no necesariamente demuestra que sea genuino ni que la institución fue el remitente, ya que existe software que disfrazan las direcciones de correo. Posteriormente en el contenido del correo, el cual posee logo y colores del Banco, le incluyen un enlace (link) que lo redirecciona a una página falsa, que es idéntica a la original del Banco donde le solicitan que reingrese sus datos privados. Una vez que se introducen los datos, se envía a una base de datos automatizada la cual los reenviará al estafador, poniéndolo en posesión de su login y password.

Un componente importante en el Delito de Phishing es la captación de datos sobre personas, números de tarjeta de crédito y de documentos de identidad, números de cuentas bancarias y contraseñas para manejarlas, todos estos datos suelen residir en computadoras personales conectadas a la red. En muchas ocasiones se puede conseguir que el usuario mismo lo facilite.

Un procedimiento más sofisticado es la instalación de un programa espía en la computadora personal. A través de un programa espía, se vigila la actividad del usuario, por ejemplo la contraseña tecleada cuando se conecta con el banco. Se instala en la computadora a través de un anexo a un correo electrónico, o escondido en un archivo de fotos o de música descargada gratuitamente de la web. Este programa espía, gusano electrónico programa troyano, puede ser capaz de mutarse para evitar la detección de un programa antivirus, y pasar desapercibido durante mucho tiempo. Envía la información deseada a un destino oculto, y se autodestruye para que el usuario no se de cuenta de que su información confidencial ha sido espiada. Posteriormente, la información obtenida se puede utilizar para vaciar cuentas bancarias o acceder a servidores protegidos con contraseña.

La cifra negra de la criminalidad, en materia de delitos informáticos, no puede seguir en la penumbra, de allí la necesidad imperiosa para el derecho penal y organismos gubernamentales la investigación de una nueva modalidad comisiva de amplias repercusiones sociales y económicas. Existe una necesidad urgente de incluir

en el derecho penal vigente una tipificación básica de los delitos informáticos que afecten el interés social y el patrimonio público. En primer término en lo que concierne a las conductas punibles, sería imprescindible crear nuevos tipos penales y en otros casos modificar los ya existentes.

Por ello, tanto los nuevos delitos incorporados a los distintos ordenamientos jurídicos en el mundo -incluida Venezuela desde noviembre de 2001-, como aquellos delitos tradicionales que simplemente se han visto "robustecidos" con la inclusión de un *modus operandi* más –el tecnológico- dentro de su elemento material, han generado la necesidad de afinar los procedimientos para su investigación y persecución penal, puesto que la visión tradicional y formal que muchas veces impregna los procesos jurídicos no hace más que acrecentar la natural ventaja del delincuente que sepa valerse de las nuevas tecnologías, frente a un funcionario que asuma la conducción del proceso penal desapercibido de las posibilidades de los recursos tecnológicos existentes y de la adecuada interpretación de las vías que puede ofrecer el propio ordenamiento jurídico para cumplir con los fines de la justicia ante estos nuevos retos.

Es importante insistir en que el legislador venezolano adoptó la postura de volcar dentro de nuestro ordenamiento penal las dos vertientes posibles de conductas consideradas universalmente como delitos informáticos: los delitos de resultado (de

fin), cometidos en perjuicio de la información como bien jurídico -delitos contra los sistemas que usan tecnologías de información- y los delitos de medio, en los cuales la lesión se produce contra otros bienes jurídicos ya reconocidos y consolidados con anterioridad en el derecho positivo -la propiedad, la privacidad de las personas y las comunicaciones, la protección de los niños y adolescentes y el orden económico- cuando la tecnología de información constituye el único medio de comisión posible para lograr el efecto dañoso que justifica la protección penal que se requiere; por consiguiente, no forman parte de la categoría de delitos informáticos aquellas conductas que vulneren bienes jurídicos tradicionales cuando el uso indebido de la tecnología de información constituye uno más de los medios de comisión posibles u ofrece similar efectividad en relación con cualquier otro a los efectos de producir el resultado. Es el caso de la difamación, la extorsión, el terrorismo, la legitimación de capitales, entre otros delitos, en los cuales la herramienta tecnológica dista mucho de superar o reemplazar a los diversos *modus operandi* tradicionales que coexisten con ella y que muchas veces compiten con éxito en eficacia delictiva.

Dentro del ámbito probatorio, el mayor obstáculo para la admisibilidad y apreciación de elementos de convicción distintos de las pruebas tradicionales -o que estén contenidos dentro de un soporte distinto del documento escrito- ya no radica en restricciones establecidas por el ordenamiento jurídico puesto que, el régimen procesal penal venezolano le otorga cabida a cualquier elemento de convicción que cumpla con los requisitos de legalidad, licitud, idoneidad y utilidad; la resistencia

hacia su incorporación en una investigación radica más bien en la nula o -en el mejor de los casos- muy incipiente cultura tecnológica que ha impedido o retardado la familiarización de todos los sujetos procesales con este tipo de elementos probatorios. Es evidente el natural rechazo que recaerá hacia cualquier elemento que luzca ininteligible para quien, aun cuando tenga la potestad de conducir una investigación, carezca de conocimientos especializados para comprenderlo, interpretarlo y discernir acerca de su relevancia; por ello, al margen del necesario auxilio de los expertos para la "traducción" específica del significado de un rastro contenido en soportes lógicos y no físicos, es necesario identificar y familiarizarse *in abstracto* con todo el espectro probatorio que puede derivarse de los nuevos modos de almacenar, transmitir, conservar y manejar la información, independientemente de la calificación jurídica que puedan merecer los hechos objeto de investigación penal y el grado de responsabilidad penal involucrado.

Pero en nuestro país, aparte de las disposiciones de la Constitución de 1999 que se refieren al uso de la informática por parte del Estado (arts. 60 y 108), ya contamos, desde 2001, con algunas referencias legales concretas que nos aproximan a la equiparación de los soportes informáticos con los documentos escritos, como es el **Decreto-Ley sobre Mensajes de Datos y Firma Electrónica**, publicado el 28 de febrero de 2001.

En materia de eficacia probatoria de mensajes de datos señala lo siguiente:

> "Artículo 4º.-Los mensajes de datos tendrán la misma eficacia probatoria que la ley otorga a los documentos escritos, sin perjuicio de lo establecido en la primera parte del artículo 6 de este Decreto-Ley. Su promoción, control, contradicción y evacuación como medio de prueba, se realizará conforme a lo previsto para las pruebas libres en el Código de Procedimiento Civil.
>
> "La información contenida en un mensaje de datos, reproducida en formato impreso, tendrá la misma eficacia probatoria atribuida en la ley a las copias o reproducciones fotostáticas."

Esta precariedad probatoria se subsana y la validez y eficacia son plenas cuando dicho mensaje de datos cuenta con una firma electrónica que permita atribuirle la autoría al signatario, siempre que la firma reúna determinados requisitos previstos en la ley. Así lo disponen los artículos 16 y 18 en los siguientes términos:

> "Artículo 16.- La firma electrónica que permita vincular al signatario con el mensaje de datos y atribuir la autoría de éste, tendrá la misma validez y eficacia probatoria que la ley otorga a la firma autógrafa. A tal efecto, salvo que las partes dispongan otra cosa, la firma electrónica deberá llenar los siguientes aspectos:
>
> 1. Garantizar que los datos utilizados para su generación pueden producirse sólo una vez y asegurar, razonablemente, su confidencialidad.
>
> 2. Ofrecer seguridad suficiente de que no pueda ser falsificada con la tecnología existente en cada momento.
>
> 3. No alterar la integridad del mensaje de datos.

> A los efectos de este artículo, la firma electrónica podrá formar parte integrante del mensaje de datos o estar inequívocamente asociada a éste; enviarse o no en un mismo acto".
>
> "Artículo 18.- La firma electrónica, debidamente certificada por un proveedor de servicios de certificación conforme a lo establecido en este Decreto-Ley, se considerará que cumple los requisitos señalados en el artículo 16."

En caso de delitos cometidos mediante el uso indebido de la tecnología de información, los límites que el Código Orgánico Procesal Penal (COPP) establece para el régimen probatorio aplicable al proceso penal son, al mismo tiempo, los principios que lo informan, a saber: la licitud, libertad, idoneidad y utilidad de la prueba y el hecho de que su apreciación se fundamenta en la sana crítica, realizada mediante la observación de las reglas de la lógica, los conocimientos científicos y las máximas de la experiencia (art. 22 COPP). Al quedar de manifiesto, entonces, que el régimen probatorio previsto para el proceso penal venezolano, en principio, no es restrictivo ni excluyente en relación con los medios de prueba, es menester familiarizarnos con las nuevas formas de evidencia provenientes del uso de la tecnología de información con el objeto de identificar el cauce más apropiado para su incorporación al proceso penal de modo que mantengan toda su eficacia jurídica como elementos de convicción.

Comprobar la comisión de delitos de Estafa Informática en la modalidad Phishing, puede volverse una actividad de muy compleja realización e, incluso, de difícil percepción; en casos como éstos, no existe medio más idóneo para incorporar

al proceso penal la evidencia de un ataque de esta naturaleza, que el **análisis del computador o red por parte del perito**, quien, mediante la aplicación de herramientas informáticas y la interpretación de sus resultados, estaría en capacidad de confirmar o descartar si el sistema resultó comprometido, cuál habría sido el *modus operandi* utilizado e, inclusive, la dirección IP.

Para ilustrar lo dicho, tomemos como ejemplo el caso de la comisión de dos hechos punibles que pueden cometerse mediante el uso de la tecnología de información –aunque no estén categorizados como delitos informáticos-, como podrían ser la difamación o la instigación a delinquir perpetradas desde un dominio (sitio web). En estos casos, la prueba documental constituiría el medio por excelencia para la demostración de su comisión e inclusive de su autoría, ya que los proveedores de servicios de INTERNET, así como los verificadores de registros de dominios suelen guardar y poner a disposición de quien los solicite, los registros acerca de los contenidos puestos en línea y también, los datos de identificación de los administradores, contactos técnicos y pagadores de los dominios desde donde se hubiesen generado los contenidos considerados delictivos.

Como consideración última, aplicable a todas las formas de prueba electrónica, debemos reafirmar que, además de todo lo dicho, la validez de la prueba electrónica requiere que su recabación, incorporación y valoración se realicen con respeto a la salvaguarda de los derechos y garantías constitucionales de los ciudadanos, y

descansa en la observancia de la disposición contenida en el artículo 197 del COPP que prohíbe conferir validez a cualquier actividad probatoria realizada mediante "tortura, maltrato, coacción, amenaza, engaño, indebida intromisión en la intimidad del domicilio, en la correspondencia, las comunicaciones, los papeles y los archivos privados", o que se obtenga por otro medio que menoscabe la voluntad o viole los derechos fundamentales de las personas, o que provenga directa o indirectamente de un medio o procedimiento ilícitos.

Los delitos informáticos han hecho que nuestra sociedad sea cada vez más escéptica a la utilización de tecnologías de la información, las cuales pueden ser de mucho beneficio para la sociedad en general. Este hecho puede obstaculizar el desarrollo de nuevas formas de hacer negocios, por ejemplo el comercio electrónico puede verse afectado por la falta de apoyo de la sociedad en general.

También se observa, que el grado de especialización técnica que adquieren los delincuentes para cometer éste tipo de delitos, por lo que personas con conductas maliciosas cada vez más están ideando planes para la realización de actos delictivos, tanto a nivel empresarial como a nivel global.

Cabe considerar, que las empresas que poseen activos informáticos importantes, son cada vez más celosas y exigentes en la contratación de personal para trabajar en

éstas áreas, pudiendo afectar en forma positiva o negativa a la sociedad laboral de nuestros tiempos.

Aquellas personas que no poseen los conocimientos informáticos básicos, son más vulnerables a ser víctimas de un delito, que aquellos que si los poseen. En vista de lo anterior aquel porcentaje de personas que no conocen nada de informática (por lo general personas de escasos recursos económicos) pueden ser engañadas si en un momento dado poseen acceso a recursos tecnológicos y no han sido asesoradas adecuadamente para la utilización de tecnologías como la Internet, correo electrónico, etc.

La falta de cultura informática puede impedir de parte de la sociedad la lucha contra los delitos informáticos, por lo que el componente educacional es un factor clave en la minimización de esta problemática

La repercusión en el orden económico, tenemos que el costo del impacto mundial de los ataques cibernéticos ha crecido constantemente, de 300 millones de dólares en 1997 a un monto estimado de 952.000 millones de dólares en 2007, según estudios del Computer Economics de Carlsbad, California (2008). Como resultado, la protección de las redes contra los intrusos se ha vuelto esencial.

En promedio, las empresas dedicaron 9% del presupuesto de TI a la seguridad de la red en 2007. La cifra se elevó a 11% en 2008 y se espera que llegue a 15% para el 2009.

Venezuela no escapa de esta situación, sobre todo en el campo financiero bancario, las medidas e inversiones en materia de seguridad son millonarias, pero son cifras irrisorias comparada con las perdidas anuales en lo que atañe a los delitos informáticos, por supuesto lo que respecta al delito Phishing, los banqueros no ponen de su parte porque ese delito es de carácter "privado", es decir, quien tiene que contratar o estar al día con la seguridad es el cliente de la entidad bancaria, ya que es por vía email que ocurre la Estafa.

Es probable que en los próximos años el enfoque del gasto en seguridad se oriente más hacia la implantación de herramientas nuevas o mejoradas de prevención de ataques y mitigación rápida de efectos de los ataques, en lugar del empleo de capas perimetrales de protección y detección de intrusión que resultan insostenibles conforme se habilitan más transacciones y comunicaciones electrónicas.

Pero el arma eficaz para prevenir este delito informático y otros, es el conocimiento, el cual debe ser divulgado por los medios de información, así como una normativa penal más acorde con los tiempos.

Para determinar la penalización y tipificación el delito de Estafa Informática en la modalidad de Phishing, a nivel de legislaciones foráneas, se pudo establecer, dentro de las normativas estudiadas, que el único país, que tipifica claramente el delito de Phishing, es la legislación colombiana, en su código penal, específicamente el artículo 269G , este artículo es muy preciso y se podría pensar que los delitos informáticos orientados a capturar datos personales no siempre se harán por suplantación de páginas ya que con el pasar del tiempo nuevas técnicas pueden ser implementadas para el mismo fin.

# CAPÍTULO V

# CONCLUSION Y RECOMENDACIONES

## Conclusión

Del Trabajo de investigación realizado con la finalizad de Analizar el Delito de Estafa en la Modalidad de Phishing a través de Internet, así como determinar los Medios de Pruebas y su licitud de acuerdo al ordenamiento jurídico venezolano, Indagar las repercusiones sociales y económicas de este delito para poder enfrentarlo y Examinar la legislación extranjera para tipificar y penalizar los delitos de Estafa por Internet, se concluye que:

Un componente importante en el Delito de Phishing es la captación de datos sobre personas, números de tarjeta de crédito y de documentos de identidad, números de cuentas bancarias y contraseñas para manejarlas.

El régimen probatorio previsto para el proceso penal venezolano, en principio, no es restrictivo ni excluyente en relación con los medios de prueba, es menester familiarizarnos con las nuevas formas de evidencia provenientes del uso de la tecnología de información con el objeto de identificar el cauce más apropiado para su incorporación al proceso penal de modo que mantengan toda su eficacia jurídica como elementos de convicción.

Los delitos informáticos han hecho que nuestra sociedad sea cada vez más escéptica a la utilización de tecnologías de la información, las cuales pueden ser de mucho beneficio para la sociedad en general.

Para determinar la penalización y tipificación el delito de Estafa Informática en la modalidad de Phishing, a nivel de legislaciones foráneas, se pudo establecer, dentro de las normativas estudiadas, que el único país, que tipifica claramente el delito de Phishing, es la legislación colombiana, en su código penal, específicamente el artículo 269G, este artículo es muy preciso.

**Recomendaciones**

¿Cómo podemos evitar el Phishing? , la respuesta es estar informado acerca de esta nueva modalidad de fraude electrónico es la mejor arma para no convertirse en una victima. Se cuidadoso cuando se suministre información personal o financiera a través de Internet.

Nunca responder solicitudes de información personal a través de correos electrónicos. Si se tiene alguna duda, contactar con la entidad que supuestamente ha enviado el mensaje.

No accesar a la página del Banco a través de enlaces ubicados en otras páginas o **enlaces que reciba en correos.**

Notificar inmediatamente al banco cualquier sospecha de fraude o robo de cuentas, tarjetas o claves de acceso.

Consultar frecuentemente los saldos de las cuentas y los movimientos de las tarjetas de crédito.

Evitar ingresar a la página de los banco desde un cybercafé, o lugares públicos.

Además de lo mencionado, nunca se debe dirigir a sitios de finanzas desde enlaces facilitados en e-mail o direcciones de Internet cuyo origen es desconocido (aunque parezcan provenir de los sitios originales). Si se recibe un e-mail de este tipo, antes de introducir datos, es conveniente contactar a la entidad para confirmar la veracidad del mensaje. También es importante estar atento a que, en la página, aparezca la dirección **"httpS://"** en lugar de la habitual "**http://"**, lo cual indica que la página está alojada en un servidor seguro. Con estas sencillas medidas se puede reducir significativamente el riesgo de ser un "estafado virtual".

Lo importante es el medio masivo –Internet- en el que se comete el delito y las facultades del fiscal director de la investigación, quien puede ordenar al funcionario de Policía Judicial la búsqueda o la recuperación de la información, que luego será

verificada por el Juez de Control. Esta es una diligencia que nos permite agilizar la preservación de la evidencia. En estos casos de materia tecnológica hay que actuar en forma inmediata, toda vez que se podría perder la evidencia o ser modificada por las personas que manejan o tienen a su cargo el control de la información.

*“Inútil leyes debilitan las leyes necesarias."*

Montesquieu, 1.748

# ANEXO 1

# LEY ESPECIAL CONTRA LOS DELITOS INFORMATICOS

Gaceta Oficial Nº 37.313 del 30 de octubre de 2001

## LA ASAMBLEA NACIONAL DE LA REPUBLICA BOLIVARIANA DE VENEZUELA

**DECRETA** la siguiente,

### LEY ESPECIAL CONTRA LOS DELITOS INFORMATICOS

### TITULO I
### DISPOSICIONES GENERALES

**Artículo 1 Objeto de la Ley** La presente Ley tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualesquiera de sus componentes, o de los cometidos mediante el uso de dichas tecnologías, en los términos previstos en esta Ley.

**Artículo 2 Definiciones** A efectos de la presente Ley, y cumpliendo con lo previsto en el artículo 9 de la Constitución de la República Bolivariana de Venezuela, se entiende por:

a. **Tecnología de Información:** rama de la tecnología que se dedica al estudio, aplicación y procesamiento de datos, lo cual involucra la obtención, creación, almacenamiento, administración, modificación, manejo, movimiento, control, visualización, transmisión o recepción de información en forma automática, así como el desarrollo y uso del "hardware", "firmware", "software", cualesquiera de sus componentes y todos los procedimientos asociados con el procesamiento de datos.

b. **Sistema:** cualquier arreglo organizado de recursos y procedimientos diseñados para el uso de tecnologías de información, unidos y regulados por interacción o interdependencia para cumplir una serie de funciones específicas, así como la combinación de dos o más componentes interrelacionados, organizados en un paquete funcional, de manera que estén en capacidad de realizar una función operacional o satisfacer un requerimiento dentro de unas especificaciones previstas.

c. **Data (datos):** hechos, conceptos, instrucciones o caracteres representados de una manera apropiada para que sean comunicados, transmitidos o procesados por seres humanos o por medios automáticos y a los cuales se les asigna o se les puede asignar un significado.

d. **Información:** significado que el ser humano le asigna a la data utilizando las convenciones conocidas y generalmente aceptadas.

e. **Documento:** registro incorporado en un sistema en forma de escrito, video, audio o cualquier otro medio, que contiene data o información acerca de un hecho o acto capaces de causar efectos jurídicos.

f. **Computador:** dispositivo o unidad funcional que acepta data, la procesa de acuerdo con un programa guardado y genera resultados, incluidas operaciones aritméticas o lógicas.

g. ***Hardware:*** equipos o dispositivos físicos considerados en forma independiente de su capacidad o función, que conforman un computador o sus componentes periféricos, de manera que pueden incluir herramientas, implementos, instrumentos, conexiones, ensamblajes, componentes y partes.

h. ***Firmware:*** programa o segmento de programa incorporado de manera permanente en algún componente de *hardware*.

i. ***Software:*** información organizada en forma de programas de computación, procedimientos y documentación asociados, concebidos para realizar la operación de un sistema, de manera que pueda proveer de instrucciones a los computadores así como de data expresada en cualquier forma, con el objeto de que los computadores realicen funciones específicas.

j. **Programa:** plan, rutina o secuencia de instrucciones utilizados para realizar un trabajo en particular o resolver un problema dado a través de un computador.
k. **Procesamiento de Datos o de Información:** realización sistemática de operaciones sobre data o sobre información, tales como manejo, fusión, organización o cómputo.
l. **Seguridad:** condición que resulta del establecimiento y mantenimiento de medidas de protección, que garanticen un estado de inviolabilidad de influencias o de actos hostiles específicos que puedan propiciar el acceso a la data de personas no autorizadas, o que afecten la operatividad de las funciones de un sistema de computación.
m. **Virus:** programa o segmento de programa indeseado que se desarrolla incontroladamente y que genera efectos destructivos o perturbadores en un programa o componente del sistema.
n. **Tarjeta Inteligente:** rótulo, cédula o carnet que se utiliza como instrumento de identificación; de acceso a un sistema; de pago o de crédito, y que contiene data, información o ambas, de uso restringido sobre el usuario autorizado para portarla.
ñ. **Contraseña (*password*):** secuencia alfabética, numérica o combinación de ambas, protegida por reglas de confidencialidad, utilizada para verificar la autenticidad de la autorización expedida a un usuario para acceder a la data o a la información contenidas en un sistema.
o. **Mensaje de Datos:** cualquier pensamiento, idea, imagen, audio, data o información, expresados en un lenguaje conocido que puede ser explícito o secreto (encriptado), preparados dentro de un formato adecuado para ser transmitido por un sistema de comunicaciones.
**Artículo 3 Extraterritorialidad** Cuando alguno de los delitos previstos en la presente Ley se cometa fuera del territorio de la República, el sujeto activo quedará sometido a sus disposiciones si dentro del territorio de la República se hubieren producido efectos del hecho punible, y el responsable no ha sido juzgado por el mismo hecho o ha evadido el juzgamiento o la condena por tribunales extranjeros.
**Artículo 4 Sanciones** Las sanciones por los delitos previstos en esta Ley serán principales y accesorias. Las sanciones principales concurrirán con las penas accesorias y ambas podrán también concurrir entre sí, de acuerdo con las circunstancias particulares del delito del cual se trate, en los términos indicados en la presente Ley.
**Artículo 5 Responsabilidad de las Personas Jurídicas** Cuando los delitos previstos en esta Ley fuesen cometidos por los gerentes, administradores, directores o dependientes de una persona jurídica, actuando en su nombre o representación, éstos responderán de acuerdo con su participación culpable.
La persona jurídica será sancionada en los términos previstos en esta Ley, en los casos en que el hecho punible haya sido cometido por decisión de sus órganos, en el ámbito de su actividad, con sus recursos sociales o en su interés exclusivo o preferente.

## TITULO II DE LOS DELITOS

### Capítulo I De los Delitos Contra los Sistemas que Utilizan Tecnologías de Información

**Artículo 6 Acceso Indebido** Toda persona que sin la debida autorización o excediendo la que hubiere obtenido, acceda, intercepte, interfiera o use un sistema que utilice tecnologías de información, será penado con prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias.
**Artículo 7 Sabotaje o Daño a Sistemas** Todo aquel que con intención destruya, dañe, modifique o realice cualquier acto que altere el funcionamiento o inutilice un sistema que utilice tecnologías de información o cualesquiera de los componentes que lo conforman, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias.
Incurrirá en la misma pena quien destruya, dañe, modifique o inutilice la data o la información contenida en cualquier sistema que utilice tecnologías de información o en cualesquiera de sus componentes.
La pena será de cinco a diez años de prisión y multa de quinientas a mil unidades tributarias, si los efectos indicados en el presente artículo se realizaren mediante la creación, introducción o transmisión, por cualquier medio, de un virus o programa análogo.

**Artículo 8 Favorecimiento Culposo del Sabotaje o Daño** Si el delito previsto en el artículo anterior se cometiere por imprudencia, negligencia, impericia o inobservancia de las normas establecidas, se aplicará la pena correspondiente según el caso, con una reducción entre la mitad y dos tercios.

**Artículo 9 Acceso Indebido o Sabotaje a Sistemas Protegidos** Las penas previstas en los artículos anteriores se aumentarán entre una tercera parte y la mitad, cuando los hechos allí previstos o sus efectos recaigan sobre cualesquiera de los componentes de un sistema que utilice tecnologías de información protegido por medidas de seguridad, que esté destinado a funciones públicas o que contenga información personal o patrimonial de personas naturales o jurídicas.

**Artículo 10 Posesión de Equipos o Prestación de Servicios de Sabotaje** Quien importe, fabrique, distribuya, venda o utilice equipos, dispositivos o programas; con el propósito de destinarlos a vulnerar o eliminar la seguridad de cualquier sistema que utilice tecnologías de información; o el que ofrezca o preste servicios destinados a cumplir los mismos fines, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias. **Artículo 11 Espionaje Informático** Toda persona que indebidamente obtenga, revele o difunda la data o información contenidas en un sistema que utilice tecnologías de información o en cualesquiera de sus componentes, será penada con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.

La pena se aumentará de un tercio a la mitad, si el delito previsto en el presente artículo se cometiere con el fin de obtener algún tipo de beneficio para sí o para otro.

El aumento será de la mitad a dos tercios, si se pusiere en peligro la seguridad del Estado, la confiabilidad de la operación de las instituciones afectadas o resultare algún daño para las personas naturales o jurídicas, como consecuencia de la revelación de las informaciones de carácter reservado.

**Artículo 12 Falsificación de Documentos** Quien, a través de cualquier medio, cree, modifique o elimine un documento que se encuentre incorporado a un sistema que utilice tecnologías de información; o cree, modifique o elimine datos del mismo; o incorpore a dicho sistema un documento inexistente, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.

Cuando el agente hubiere actuado con el fin de procurar para sí o para otro algún tipo de beneficio, la pena se aumentará entre un tercio y la mitad.

El aumento será de la mitad a dos tercios si del hecho resultare un perjuicio para otro.

## Capítulo II
## De los Delitos Contra la Propiedad

**Artículo 13 Hurto** Quien a través del uso de tecnologías de información, acceda, intercepte, interfiera, manipule o use de cualquier forma un sistema o medio de comunicación para apoderarse de bienes o valores tangibles o intangibles de carácter patrimonial sustrayéndolos a su tenedor, con el fin de procurarse un provecho económico para sí o para otro, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

**Artículo 14 Fraude** Todo aquel que, a través del uso indebido de tecnologías de información, valiéndose de cualquier manipulación en sistemas o cualquiera de sus componentes, o en la data o información en ellos contenida, consiga insertar instrucciones falsas o fraudulentas, que produzcan un resultado que permita obtener un provecho injusto en perjuicio ajeno, será penado con prisión de tres a siete años y multa de trescientas a setecientas unidades tributarias. **Artículo 15 Obtención Indebida de Bienes o Servicios** Quien, sin autorización para portarlos, utilice una tarjeta inteligente ajena o instrumento destinado a los mismos fines, o el que utilice indebidamente tecnologías de información para requerir la obtención de cualquier efecto, bien o servicio; o para proveer su pago sin erogar o

asumir el compromiso de pago de la contraprestación debida, será castigado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

**Artículo 16 Manejo Fraudulento de Tarjetas Inteligentes o Instrumentos Análogos** Toda persona que por cualquier medio, cree, capture, grabe, copie, altere, duplique o elimine la data o información contenidas en una tarjeta inteligente o en cualquier instrumento destinado a los mismos fines; o la persona que, mediante cualquier uso indebido de tecnologías de información, cree, capture, duplique o altere la data o información en un sistema, con el objeto de incorporar usuarios, cuentas, registros o consumos inexistentes o modifique la cuantía de éstos, será penada con prisión de cinco a diez años y multa de quinientas a mil unidades tributarias.

En la misma pena incurrirá quien, sin haber tomado parte en los hechos anteriores, adquiera, comercialice, posea, distribuya, venda o realice cualquier tipo de intermediación de tarjetas inteligentes o instrumentos destinados al mismo fin, o de la data o información contenidas en ellos o en un sistema.

**Artículo 17 Apropiación de Tarjetas Inteligentes o Instrumentos Análogos** Quien se apropie de una tarjeta inteligente o instrumento destinado a los mismos fines, que se haya perdido, extraviado o que haya sido entregado por equivocación, con el fin de retenerlo, usarlo, venderlo o transferirlo a una persona distinta del usuario autorizado o entidad emisora, será penado con prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias.

La misma pena se impondrá a quien adquiera o reciba la tarjeta o instrumento a que se refiere el presente artículo.

**Artículo 18 Provisión Indebida de Bienes o Servicios** Todo aquel que, a sabiendas de que una tarjeta inteligente o instrumento destinado a los mismos fines, se encuentra vencido, revocado; se haya indebidamente obtenido, retenido, falsificado, alterado; provea a quien los presente de dinero, efectos, bienes o servicios, o cualquier otra cosa de valor económico será penado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

**Artículo 19 Posesión de Equipo para Falsificaciones** Todo aquel que sin estar debidamente autorizado para emitir, fabricar o distribuir tarjetas inteligentes o instrumentos análogos, reciba, adquiera, posea, transfiera, comercialice, distribuya, venda, controle o custodie cualquier equipo de fabricación de tarjetas inteligentes o de instrumentos destinados a los mismos fines, o cualquier equipo o componente que capture, grabe, copie o transmita la data o información de dichas tarjetas o instrumentos, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.

## Capítulo III
## De los Delitos Contra la Privacidad de las Personas y de las Comunicaciones

**Artículo 20 Violación de la Privacidad de la Data o Información de Carácter Personal** Toda persona que intencionalmente se apodere, utilice, modifique o elimine por cualquier medio, sin el consentimiento de su dueño, la data o información personales de otro o sobre las cuales tenga interés legítimo, que estén incorporadas en un computador o sistema que utilice tecnologías de información, será penada con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

La pena se incrementará de un tercio a la mitad si como consecuencia de los hechos anteriores resultare un perjuicio para el titular de la data o información o para un tercero.

**Artículo 21 Violación de la Privacidad de las Comunicaciones** Toda persona que mediante el uso de tecnologías de información, acceda, capture, intercepte, interfiera, reproduzca, modifique, desvíe o elimine cualquier mensaje de datos o señal de transmisión o comunicación ajena, será sancionada con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

**Artículo 22 Revelación Indebida de Data o Información de Carácter Personal** Quien revele, difunda o ceda, en todo o en parte, los hechos descubiertos, las imágenes, el audio o, en general, la data o información obtenidos por alguno de los medios indicados en los artículos 20 y 21, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Si la revelación, difusión o cesión se hubieren realizado con un fin de lucro, o si resultare algún perjuicio para otro, la pena se aumentará de un tercio a la mitad.

## Capítulo IV
## De los Delitos Contra Niños, Niñas o Adolescentes

**Artículo 23 Difusión o Exhibición de Material Pornográfico** Todo aquel que, por cualquier medio que involucre el uso de tecnologías de información, exhiba, difunda, transmita o venda material pornográfico o reservado a personas adultas, sin realizar previamente las debidas advertencias para que el usuario restrinja el acceso a niños, niñas y adolescentes, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

**Artículo 24 Exhibición Pornográfica de Niños o Adolescentes** Toda persona que por cualquier medio que involucre el uso de tecnologías de información, utilice a la persona o imagen de un niño, niña o adolescente con fines exhibicionistas o pornográficos, será penada con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias.

## Capítulo V
## De los Delitos Contra el Orden Económico

**Artículo 25 Apropiación de Propiedad Intelectual** Quien sin autorización de su propietario y con el fin de obtener algún provecho económico, reproduzca, modifique, copie, distribuya o divulgue un *software* u otra obra del intelecto que haya obtenido mediante el acceso a cualquier sistema que utilice tecnologías de información, será sancionado con prisión de uno a cinco años y multa de cien a quinientas unidades tributarias.

**Artículo 26 Oferta Engañosa** Toda persona que ofrezca, comercialice o provea de bienes o servicios, mediante el uso de tecnologías de información, y haga alegaciones falsas o atribuya características inciertas a cualquier elemento de dicha oferta, de modo que pueda resultar algún perjuicio para los consumidores, será sancionada con prisión de uno a cinco años y multa de cien a quinientas unidades tributarias, sin perjuicio de la comisión de un delito más grave.

# TITULO III
# DISPOSICIONES COMUNES

**Artículo 27 Agravantes** La pena correspondiente a los delitos previstos en la presente Ley se incrementará entre un tercio y la mitad:

1. Si para la realización del hecho se hubiere hecho uso de alguna contraseña ajena indebidamente obtenida, quitada, retenida o que se hubiere perdido.
2. Si el hecho hubiere sido cometido mediante el abuso de la posición de acceso a data o información reservada, o al conocimiento privilegiado de contraseñas, en razón del ejercicio de un cargo o función.

**Artículo 28 Agravante Especial** La sanción aplicable a las personas jurídicas por los delitos cometidos en las condiciones señaladas en el artículo 5 de esta Ley, será únicamente de multa, pero por el doble del monto establecido para el referido delito.

**Artículo 29 Penas Accesorias** Además de las penas principales previstas en los capítulos anteriores, se impondrán, necesariamente sin perjuicio de las establecidas en el Código Penal, las penas accesorias siguientes:

1. El comiso de equipos, dispositivos, instrumentos, materiales, útiles, herramientas y cualquier otro objeto que hayan sido utilizados para la comisión de los delitos previstos en los artículos 10 y 19 de la presente Ley.

2. El trabajo comunitario por el término de hasta tres años en los casos de los delitos previstos en los artículos 6 y 8 de esta Ley.
3. La inhabilitación para el ejercicio de funciones o empleos públicos; para el ejercicio de la profesión, arte o industria; o para laborar en instituciones o empresas del ramo por un período de hasta tres (3) años después de cumplida o conmutada la sanción principal, cuando el delito se haya cometido con abuso de la posición de acceso a data o información reservadas, o al conocimiento privilegiado de contraseñas, en razón del ejercicio de un cargo o función públicas, del ejercicio privado de una profesión u oficio, o del desempeño en una institución o empresa privada, respectivamente.
4. La suspensión del permiso, registro o autorización para operar o para el ejercicio de cargos directivos y de representación de personas jurídicas vinculadas con el uso de tecnologías de información, hasta por el período de tres (3) años después de cumplida o conmutada la sanción principal, si para cometer el delito el agente se hubiere valido o hubiere hecho figurar a una persona jurídica.

**Artículo 30 Divulgación de la Sentencia Condenatoria** El Tribunal podrá además, disponer la publicación o difusión de la sentencia condenatoria por el medio que considere más idóneo.

**Artículo 31 Indemnización Civil** En los casos de condena por cualquiera de los delitos previstos en los Capítulos II y V de esta Ley, el Juez impondrá en la sentencia una indemnización en favor de la víctima por un monto equivalente al daño causado. Para la determinación del monto de la indemnización acordada, el juez requerirá del auxilio de expertos.

## TITULO IV
## DISPOSICIONES FINALES

**Artículo 32 Vigencia** La presente Ley entrará en vigencia, treinta días después de su publicación en la Gaceta Oficial de la República Bolivariana de Venezuela.

**Artículo 33 Derogatoria** Se deroga cualquier disposición que colida con la presente Ley.

Dada, firmada y sellada en el Palacio Federal Legislativo, sede de la Asamblea Nacional, en Caracas a los cuatro días del mes de septiembre de dos mil uno. Año 191º de la Independencia y 142º de la Federación.

**ANEXO 2**

## Ejemplo de Código de Correo Phishing
## Banco Banesco

Received: on /h/8/C/T/r/juancarloszapata/Maildir at Wed Feb 7 12:27:56 2007
Return-Path: <nobody@earth.ehostone.net>
Received: from rs25s8.datacenter.cha.cantv.net (rs25s8.ric.cantv.net [10.128.131.130])
by rs26s7.datacenter.cha.cantv.net (8.13.8/8.13.0/1.0) with ESMTP id l17GRt9k029998
for <juancarloszapata@cantv.net>; Wed, 7 Feb 2007 12:27:55 -0400
Received: from earth.ehostone.net (earth.ehostone.net [70.84.105.84])
by rs25s8.datacenter.cha.cantv.net (8.13.8/8.13.0/3.0) with ESMTP id l17GRt9d026039
for <juancarloszapata@cantv.net>; Wed, 7 Feb 2007 12:27:55 -0400
X-Matched-Lists: []
Received: from nobody by earth.ehostone.net with local (Exim 4.63)
(envelope-from <nobody@earth.ehostone.net>)
id 1HEpWt-0003dZ-Hd
for juancarloszapata@cantv.net; Wed, 07 Feb 2007 08:20:19 -0800
To: juancarloszapata@cantv.net
Subject: Seguridad en su cuenta.
From: Banesco Banco Universal <soporte@banesco.ve>
Reply-To:
MIME-Version: 1.0
Content-Type: text/html
Content-Transfer-Encoding: 8bit
Message-Id: <E1HEpWt-0003dZ-Hd@earth.ehostone.net>
Date: Wed, 07 Feb 2007 08:20:19 -0800
X-EHostOne-MailScanner-Information: Please contact the ISP for more information
X-EHostOne-MailScanner: Found to be clean
X-EHostOne-MailScanner-SpamCheck:
X-EHostOne-MailScanner-From: nobody@earth.ehostone.net
X-AntiAbuse: This header was added to track abuse, please include it with any abuse report
X-AntiAbuse: Primary Hostname - earth.ehostone.net
X-AntiAbuse: Original Domain - cantv.net
X-AntiAbuse: Originator/Caller UID/GID - [99 99] / [47 12]
X-AntiAbuse: Sender Address Domain - earth.ehostone.net

X-Source:
X-Source-Args:
X-Source-Dir:
X-Virus-Scanned: ClamAV version 0.88.7, clamav-milter version 0.88.7 on 10.128.1.151
X-Virus-Status: Clean

## ANEXO 3

### Casos de Impacto de Delitos Informáticos

**Zinn, Herbert, Shadowhack.**

Herbert Zinn, (expulsado de la educación media superior), y que operaba bajo el seudónimo de "Shadowhawk", fue el primer sentenciado bajo el cargo de Fraude Computacional y Abuso en 1986. Zinn tenia 16 y 17 cuando violo el acceso a AT&T y los sistemas del Departamento de Defensa. Fue sentenciado el 23 de enero de 1989, por la destrucción del equivalente a US $174,000 en archivos, copias de programas, los cuales estaban valuados en millones de dólares, además publico contraseñas y instrucciones de cómo violar la seguridad de los sistemas computacionales. Zinn fue sentenciado a 9 meses de cárcel y a una fianza de US$10,000. Se estima que Zinn hubiera podido alcanzar una sentencia de 13 años de prisión y una fianza de US$800,000 si hubiera tenido 18 años en el momento del crimen.

**Smith, David.**

Programador de 30 años, detenido por el FBI y acusado de crear y distribuir el virus que ha bloqueado miles de cuentas de correo, "Melissa". Entre los cargos presentados contra él, figuran el de "bloquear las comunicaciones publicas" y de "dañar los sistemas informáticos". Acusaciones que en caso de demostrarse en el tribunal podrían acarrearle una pena de hasta diez años de cárcel.

Por el momento y a la espera de la decisión que hubiese tomado el juez, David Smith esta en libertad bajo fianza de 10.000 dólares. Melissa en su "corta vida" había conseguido contaminar a más de 100,000 ordenadores de todo el mundo, incluyendo a empresas como Microsoft, Intel, Compaq, administraciones públicas

estadounidenses como la del Gobierno del Estado de Dakota del Norte y el Departamento del Tesoro.

En España su "éxito" fue menor al desarrollarse una extensa campaña de información, que alcanzo incluso a las cadenas televisivas, alertando a los usuarios de la existencia de este virus. La detención de David Smith fue fruto de la colaboración entre los especialistas del FBI y de los técnicos del primer proveedor de servicios de conexión a Internet de los Estados Unidos, América On Line. Los ingenieros de América On Line colaboraron activamente en la investigación al descubrir que para propagar el virus, Smith había utilizado la identidad de un usuario de su servicio de acceso. Además, como otros proveedores el impacto de Melissa había afectado de forma sustancial a buzones de una gran parte de sus catorce millones de usuarios.

**Poulsen Kevin, Dark Dante.**

Diciembre de 1992 Kevin Poulsen, un pirata infame que alguna vez utilizo el alias de "Dark Dante" en las redes de computadoras es acusado de robar órdenes de tarea relacionadas con un ejercicio de la fuerza aérea militar americana. Se acusa a Poulsen del robo de información nacional bajo una sección del estatuto de espionaje federal y encara hasta 10 años en la cárcel.

Siguió el mismo camino que Kevin Mitnick, pero es más conocido por su habilidad para controlar el sistema telefónico de Pacific Bell. Incluso llegó a "ganar" un Porsche en un concurso radiofónico, si su llamada fuera la 102, y así fue.

Poulsen también crackeó todo tipo de sitios, pero él se interesaba por los que contenían material de defensa nacional.

Esto fue lo que lo llevó a su estancia en la cárcel, 5 años, fue liberado en 1996, supuestamente "reformado". Que dicho sea de paso, es el mayor tiempo de estancia en la cárcel que ha comparecido un hacker.

**Murphy Ian, Captain Zap.**

En julio de 1981 Ian Murphy, un muchacho de 23 años que se autodenominaba "Captain Zap", gana notoriedad cuando entra a los sistemas en la Casa Blanca, el Pentágono, BellSouth Corp. TRW y deliberadamente deja su currículum.

En 1981, no había leyes muy claras para prevenir el acceso no autorizado a las computadoras militares o de la casa blanca. En ese entonces Ian Murphy de 24 años de edad, conocido en el mundo del hacking como "Captain Zap,".

Mostró la necesidad de hacer mas clara la legislación cuando en compañía de un par de amigos y usando una computadora y una línea telefónica desde su hogar viola los accesos restringidos a compañías electrónicas, y tenia acceso a ordenes de mercancías, archivos y documentos del gobierno. "Nosotros usamos los a la Casa Blanca para hacer llamadas a líneas de bromas en Alemania y curiosear archivos militares clasificados" Explico Murphy. "El violar accesos nos resultaba muy divertido". La Banda de hackers fue finalmente puesta a disposición de la ley". Con cargos de robo de propiedad, Murphy fue multado por US $1000 y sentenciado a 2 ½ años de prueba.

**Morris Robert.**

En noviembre de 1988, Morris lanzo un programa "gusano" diseñado por el mismo para navegar en Internet, buscando debilidades en sistemas de seguridad, y que pudiera correrse y multiplicarse por sí solo. La expansión exponencial de este programa causó el consumo de los recursos de muchísimas computadoras y que más de 6000 sistemas resultaron dañados o fueron seriamente perjudicados. Eliminar al gusano de sus computadoras causo a las víctimas muchos días de productividad perdidos, y millones de dólares. Se creo el CERT (Equipo de respuesta de emergencias computacionales) para combatir problemas similares en el futuro. Morris fue condenado y sentenciado a tres años de libertad condicional, 400 horas de

servicio comunitario y US $10,000 de fianza, bajo el cargo de Fraude computacional y abuso. La sentencia fue fuertemente criticada debido a que fue muy ligera, pero reflejaba lo inocuo de las intenciones de Morris más que el daño causado. El gusano producido por Morris no borra ni modifica archivos en la actualidad.

**Referencias Bibliográficas**


ALFONZO, I. (1994). **Técnicas de investigación bibliográfica.** Caracas: Contexto Ediciones.

ARTEAGA, A. (2004). **El Crimen Electrónico**. Caracas, UCAB

BACIGALUPO Z., E**. "Documentos electrónicos y delitos de falsedad documental"**, http://criminet.ugr.es/recpc/recpc_04-12.pdf

BRANDT, L. (2001). **Página web condiciones, políticas y términos legales.** Caracas: Editorial Legislec Editores.

CAFFARO, M. **Pericias Informáticas.** http://publicaciones.derecho.org/redi/ No._32_- _Marzo_del_2001/6

GABALDON, L (2004). **Fraude Electrónica y Cultura Corporativa**. Caracas. UCAB

GUTIERREZ, L (2004). **La Estafa Electrónica.** Caracas, UCAB

HERNANDEZ, B (1991). **La investigación Descriptiva**. España.

MENDEZ, C. (1998). **Metodologia, guia para elaborar diseños de investigación.** Bogotá: Editorial Mcgraw-hill interamericana.

NUÑEZ, E. (1997). **El delito de Estafa. La Estafa por Computadora.** Caracas: Editorial Ediciones Librería Destino.

SABINO, C (1992) **Como hacer una tesis.** Editorial Panapo. Caracas.

SANCHIS, C. (1.999) **La prueba por soportes informáticos**. Valencia, España: Tirant Lo Blanch.

SIEBER, U. (1992). **Documentación para una aproximación al delito Informático, en "Delincuencia Informática".** BARCELONA. Revista: Traducción castellano de U. Joshi, pp. 83-89SIEBER (2004)

STANGELAND, P ( 2004) **El Fraude Telemático.** Caracas. UCAB.

SUTHERLAND, E. (1999). **El Delito de Cuello Blanco.** Madrid. Ediciones de la Piqueta.

TABLANTE, C. (2001). **Delitos Informáticos. Delincuente sin rostro**. Caracas: Editorial Encambio.

TELLEZ V., J. (2003). **Derecho informático**. Editorial: McGraw-Hill Interamericana

Delitos Infomaticos.com.(2002), Boletin informativo No. 4 del 26/01/2002 en "http//delitosinformactiocs.com/estafas/fraudes-FTC2002.shtml.

Alfa-Redi (2002), Revista de Derecho Informático. España. http://www.alfa-redi.org

ORTA M, Raymond, http:// www.informaticaforense.com/criminalistica/index.php

**Referencias Normativas**

Constitución de la República Bolivariana de Venezuela. (1999). Gaceta Oficial De la República Bolivariana de Venezuela, 5.453, Marzo 24 de 2000.

Ley Especial contra los Delitos Informáticos. (2001). Gaceta Oficial de la República Bolivariana de Venezuela, 37.313, octubre 30 de 2001.

Código Penal Venezolano. (2005). Gaceta Oficial de la la República Bolivariana de Venezuela, Extraordinario 5.768, abril 13 de 2005.

Código Orgánico Procesal Penal Venezolano. (2008). Gaceta Oficial de la República Bolivariana de Venezuela, Extraordinario 5.894, agosto 26 de 2008.

Código Orgánico Tributario Venezolano. (2001). Gaceta Oficial de la República Bolivariana de Venezuela, 37.305, octubre 17 de 2001.

Ley sobre Mensajes de Datos y Firma Electrónica. Gaceta Oficial de la República Bolivariana de Venezuela, 37.148, febrero 28 de 2001.

Ley Orgánica 10/1995, Código Penal Español. , 23 de noviembre de 1995.

Ley 1273, Código Penal Colombiano, 5 enero de 2009

Ley 4573, Código Penal de Costa Rica**,** 4 de mayo de 1970