

# DIVISION DE INVESTIGACION CRIMINAL



## UNA BREVE RESEÑA DEL DELITO INFORMATICO

HELDER CAPATINTA SUMIRE

*“HAY DOS MANERAS FACILES DE CONDUCIRSE EN LA  
VIDA: CREERLO TODO Y DUDAR DE TODO. AMBAS NOS  
AHORRAN TENER QUE PENSAR”*

*Alfred Korzybski*

*Expreso mi gratitud al Sr. Coronel PNP José Luis BOJORQUEZ BUSTAMANTE, al “Detective” GAMBOA, a mis compañeros de la DIVINCRI-Cusco; por su amistad y colaboración.*

*A mis hijos Diego Fernando y Camila Fernanda, por ser la fuente de mi inspiración.*

## **INTRODUCCION**

El fenómeno informático es una realidad incuestionable e irreversible; definitivamente, la informática se ha instalado entre nosotros para no marcharse jamás. En consecuencia, la invasión de la informática en todos los ámbitos de las relaciones socioeconómicas ha motivado que muchos hablen ya de una auténtica “era informática”. En la actualidad con el avance de la tecnología y la globalización mundial, pocas dimensiones de nuestra vida no se ven afectadas, dirigidas o controladas por una –computadora-, ya sea de manera directa o indirecta, en actividades –licitas- o –ilícitas- (*buscando el bien o el mal*). Incluso, en determinados eventos, las computadoras no sólo son utilizadas como medios de archivo y procesamiento de información; sino que, además, se les concede la capacidad de adoptar automáticamente decisiones.

En este entender la –*investigación*- definido como el proceso metodológico, continuo, organizado, especializado, preciso de análisis y síntesis, que el ‘*pesquisa*’ desarrolla respecto a los diversos aspectos que expliquen la perpetración de un delito. En esta etapa, la investigación tiene por objeto la búsqueda de indicios y pruebas que sirvan para acreditar la existencia de un delito y la responsabilidad que pueda tener en él una o más personas.

## **ANTECEDENTES**

### **¿CUAL ES LA HISTORIA DE LOS DELITOS INFORMÁTICOS?**

Se podría decir que los Delitos Informáticos surgen antes de que existiese la Informática, tal como la concebimos hoy.

### **ORÍGENES DE INTERNET**

El 4 de Octubre de 1957 la antigua Unión Soviética puso en órbita el primer satélite artificial, llamado SPUTNIK, adelantándose a los Estados Unidos de América que dos años antes había anunciado el inicio de una carrera inter-espacial.

Un año después, el presidente Dwight Eisenhower ordenó la creación de la Advanced Research Projects Agency (ARPA) creado por el Departamento de Defensa de los EUA así como la NASA.

Este importante hecho marca el comienzo del uso de las comunicaciones globales.

Entre 1962 y 1968 se trabajó el concepto de intercambio de paquetes, desarrollado por Leonard Kleintock y su origen, y uso fue meramente militar. La idea consistía en que varios paquetes de información pudiesen tomar diferentes rutas para uno o más determinados destinos, consiguiendo con ello una mejor seguridad en el transporte de la información.

Se siguieron conectando computadores rápidamente a la ARPANET durante los años siguientes y el trabajo continuó para completar un protocolo host a host funcionalmente completo, así como software adicional de red.

En Diciembre de 1970, el Network Working Group (NWG) liderado por S.Crocker acabó el protocolo host a host inicial para ARPANET, llamado Network Control Protocol (NCP). Cuando en los modos de ARPANET se completó la implementación del NCP durante el periodo 1971-72, los usuarios de la red pudieron finalmente comenzar a desarrollar aplicaciones.

1991 - El Gopher es creado por la Universidad de Minnesota. El Gopher provee al usuario de un método basado en un menú jerárquico, que es capaz de localizar información en la Internet. Esta herramienta facilita enormemente el uso de la Internet.

1992 - Se funda la Internet Society.

1993 - El European Laboratory for Particle Physics in Switzerland (CERN) libera el World Wide Web (WWW), desarrollado por Tim Berners-Lee. El WWW usa el protocolo de transferencia de hipertexto (HTTP) y encadena hipertextos muy fácilmente, cambiando así la ruta o camino de la información, la cual entonces puede ser organizada, presentada y accedida en la Internet.

## **LOS VIRUS, LOS PRIMEROS DELITOS**

Desde la aparición de los virus informáticos en 1984 y tal como se les concibe hoy, han surgido muchos mitos y leyendas acerca de ellos. Esta situación se agravó con el advenimiento y auge de Internet.

### **1939-1949 LOS PRECURSORES.-**

En 1939, el famoso científico matemático John Louis Von Neumann, de origen húngaro, escribió un artículo, publicado en una revista científica de New York, exponiendo su "Teoría y organización de autómatas complejos", donde demostraba la posibilidad de desarrollar pequeños programas que pudiesen tomar el control de otros, de similar estructura.

Cabe mencionar que Von Neumann, en 1944 contribuyó en forma directa con John Mauchly y J. Presper Eckert, asesorándolos en la fabricación de la ENIAC, una de las computadoras de Primera Generación, quienes construyeron además la famosa UNIVAC en 1950.

### **JOHN LOUIS VON NEUMANN (1903-1957).-**

En 1949, en los laboratorios de la Bell Computer, subsidiaria de la AT&T, 3 jóvenes programadores: Robert Thomas Morris, Douglas Mcllory y Victor Vysotsky, a manera de entretenimiento crearon un juego al que denominaron CoreWar, inspirados en la teoría de John Von Neumann, escrita y publicada en 1939.

Robert Thomas Morris fue el padre de Robert Tappan Morris, quien en 1988 introdujo un virus en ArpaNet (precursora de Internet).

Puesto en la práctica, los contendores del CoreWar ejecutaban programas que iban paulatinamente disminuyendo la memoria del computador y el ganador era el que finalmente conseguía eliminarlos totalmente. Este juego fue motivo de concursos en importantes centros de investigación como el de la Xerox en California y el Massachusetts Technology Institute (MIT), entre otros.

Sin embargo durante muchos años el CoreWar fue mantenido en el anonimato, debido a que por aquellos años la computación era manejada por una pequeña élite de intelectuales

A pesar de muchos años de clandestinidad, existen reportes acerca del virus Creeper, creado en 1972 por Robert Thomas Morris, que atacaba a las famosas IBM 360, emitiendo periódicamente en la pantalla el mensaje: "I'm a creeper... catch me if you can!" (soy una enredadera, agárrenme si pueden). Para eliminar este problema se creó el primer programa antivirus denominado Reaper (segadora), ya que por aquella época se desconocía el concepto de los software antivirus.

En 1980 la red ArpaNet del Ministerio de Defensa de los Estados Unidos de América, precursora de Internet, emitió extraños mensajes que aparecían y desaparecían en forma aleatoria, asimismo algunos códigos ejecutables de los programas usados sufrían una mutación. Los altamente calificados técnicos del Pentágono se demoraron 3 largos días en desarrollar el programa antivirus correspondiente.

### **1981 LA IBM PC.-**

En Agosto de 1981 la International Business Machine lanza al mercado su primera computadora personal, simplemente llamada IBM PC. Un año antes, la IBM habían buscado infructuosamente a Gary Kildall, de la Digital Research,

para adquirirle los derechos de su sistema operativo CP/M, pero éste viajó a Miami ignorando las llamadas de los ejecutivos del "gigante azul".

Es cuando aparece Bill Gates, de la Microsoft Corporation y adquiere a la Seattle Computer Products, un sistema operativo desarrollado por Tim Paterson, que realmente era un "clone" del CP/M. Gates le hizo algunos ligeros cambios y con el nombre de PC-DOS se lo vendió a la IBM. Sin embargo, Microsoft retuvo el derecho de explotar dicho sistema, bajo el nombre de MS-DOS.

El nombre del sistema operativo de Paterson era "Quick and Dirty DOS" (Rápido y Rústico Sistema Operativo de Disco) y tenía varios errores de programación (bugs).

La prisa con la cual se lanzó la IBM PC impidió que se le dotase de un buen sistema operativo y como resultado de esa imprevisión todas las versiones del llamado PC-DOS y posteriormente del MS-DOS fueron totalmente vulnerables a los virus, ya que heredaron muchos de los conceptos de programación del antiguo sistema operativo CP/M, como por ejemplo el PSP (Program Segment Prefix), una rutina de apenas 256 bytes, que es ejecutada previamente a la ejecución de cualquier programa con extensión EXE o COM.

### **1983 KENETH THOMPSON.-**

Este ingeniero, que en 1969 creó el sistema operativo UNIX, resucitó las teorías de Von Neumann y la de los tres programadores de la Bell y en 1983 siendo protagonista de una ceremonia pública presentó y demostró la forma de desarrollar un virus informático.

### **1984 FRED COHEN.-**

El Dr. Fred Cohen al ser homenajeado en una graduación, en su discurso de agradecimiento incluyó las pautas para el desarrollo de un virus. Este y otros hechos posteriores lo convirtieron en el primer autor oficial de los virus (*aunque hubieron varios autores más que actuaron en el anonimato*).

El Dr. Cohen escribió su libro "Virus informáticos: teoría y experimentos", donde además de definirlos los califica como un grave problema relacionado con la Seguridad Nacional. Posteriormente este investigador escribió "El evangelio según Fred" (The Gospel according to Fred), desarrolló varias especies virales y experimentó con ellas en un computador VAX 11/750 de la Universidad de California del Sur.

La verdadera voz de alarma se dio en 1984 cuando los usuarios del BIX BBS, un foro de debates de la ahora revista BYTE reportaron la presencia y propagación de algunos programas que habían ingresado a sus computadoras en forma subrepticia, actuando como "caballos de troya", logrando infectar a otros programas y hasta el propio sistema operativo, principalmente al "Sector de Arranque".

Al año siguiente los mensajes y quejas se incrementaron y fue en 1986 que se reportaron los primeros virus conocidos que ocasionaron serios daños en las IBM PC y sus clones.

### **1986 EL COMIENZO DE LA GRAN EPIDEMIA.-**

En ese año se difundieron los virus "(c) Brain", "Bouncing Ball" y "Marihuana" y que fueron las primeras especies representativas de difusión masiva. Estas 3 especies virales tan sólo infectaban el sector de arranque de los diskettes.

Posteriormente aparecieron los virus que infectaban los archivos con extensión EXE y COM.

El 2 de Noviembre de 1988 Robert Tappan Morris (hijo de uno de los precursores de los virus), recién graduado en Computer Science en la Universidad de Cornell, difundió un virus a través de ArpaNet, (precursora de Internet) logrando infectar 6,000 servidores conectados a la red. La propagación la realizó desde uno de los terminales del MIT (Instituto Tecnológico de Massashussets).

Cabe mencionar que el ArpaNet empleaba el UNIX, como sistema operativo. Robert Tappan Morris al ser descubierto, fue enjuiciado y condenado en la corte de Syracuse, estado de Nueva York, a 4 años de prisión y el pago de US \$ 10,000 de multa, pena que fue conmutada a libertad bajo palabra y condenado a cumplir 400 horas de trabajo comunitario. Actualmente es un experto en Seguridad y ha escrito innumerables obras sobre el tema.

### **1991 LA FIEBRE DE LOS VIRUS.-**

En Junio de 1991 el Dr. Vesselin Bontchev, que por entonces se desempeñaba como director del Laboratorio de Virología de la Academia de Ciencias de Bulgaria, escribió un interesante y polémico artículo en el cual, además de reconocer a su país como el líder mundial en la producción de virus da a saber que la primera especie viral búlgara, creada en 1988, fue el resultado de una mutación del virus “Vienna”, originario de Austria, que fuera desensamblado y modificado por estudiantes de la Universidad de Sofía. Al año siguiente los autores búlgaros de virus, se aburrieron de producir mutaciones y empezaron a desarrollar sus propias creaciones.

En 1989 su connacional, el virus "Dark Avenger" o el "vengador de la oscuridad", se propagó por toda Europa y los Estados Unidos haciéndose terriblemente famoso por su ingeniosa programación, peligrosa y rápida técnica de infección, a tal punto que se han escrito muchos artículos y hasta más de un libro acerca de este virus, el mismo que posteriormente inspiró en su propio país la producción masiva de sistema generadores automáticos de virus, que permiten crearlos sin necesidad de programarlos.

### **1991 LOS VIRUS PERUANOS.-**

Al igual que la corriente búlgara, en 1991 apareció en el Perú el primer virus local, autodenominado 'Mensaje' y que no era otra cosa que una simple mutación del virus "Jerusalem-B" y al que su autor le agregó una ventana con su nombre y número telefónico. Los virus con apellidos como Espejo, Martínez y Aguilar fueron variantes del Jerusalem-B y prácticamente se difundieron a nivel nacional.

Continuando con la lógica del tedio, en 1993 empezaron a crearse y diseminarse especies nacionales desarrolladas con creatividad propia, siendo alguno de ellos sumamente originales, como los virus Katia, Rogue o F03241 y los polimórficos Rogue II y Please Wait (que formateaba el disco duro). La creación de los virus locales ocurre en cualquier país y el Perú no podía ser la excepción.

### **1995 LOS MACRO VIRUS**

A mediados de 1995 se reportaron en diversas ciudades del mundo la aparición de una nueva familia de virus que no solamente infectaban documentos, sino que a su vez, sin ser archivos ejecutables podían auto-

copiarse infectando a otros documentos. Los llamados macro virus tan sólo infectaban a los archivos de MS-Word, posteriormente apareció una especie que atacaba al Ami Pro, ambos procesadores de textos. En 1997 se disemina a través de Internet el primer macro virus que infecta hojas de cálculo de MS-Excel, denominado Laroux, y en 1998 surge otra especie de esta misma familia de virus que ataca a los archivos de bases de datos de MS-Access.

### **1999 LOS VIRUS ANEXADOS (ADJUNTOS)**

A principios de 1999 se empezaron a propagar masivamente en Internet los virus anexados (adjuntos) a mensajes de correo, como el Melisa o el macro virus Melissa. Ese mismo año fue difundido a través de Internet el peligroso CIH y el ExploreZip, entre otros.

A fines de Noviembre de 1999 apareció el BubbleBoy, primer virus que infecta los sistemas con tan sólo leer el mensaje de correo, el mismo que se muestra en formato HTML. En Junio del 2000 se reportó el VBS/Stages.SHS, primer virus oculto dentro del Shell de la extensión .SHS.

### **2000 EN ADELANTE.-**

El 18 de Septiembre del 2001 el virus Nimda amenazó a millones de computadoras y servidores, a pocos días del fatídico ataque a las Torres Gemelas de la isla de Manhattan, demostrando no solo la vulnerabilidad de los sistemas, sino la falta de previsión de muchos de los administradores de redes y de los usuarios.

Los gusanos, troyanos o la combinación de ellos, de origen alemán como MyDoom, Netsky, etc. revolucionaron con su variada técnica.

No podemos dejar de mencionar la famosa "Ingeniería Social", culpable de que millones de personas caigan en trampas, muchas veces ingenuas. Los BOT de IRC y a finales del 2005 los temibles Rootkit.

Resultará imposible impedir que se sigan desarrollando virus en todo el mundo, por ser esencialmente una expresión cultural de "graffiti cibernético", así como los crackers jamás se detendrán en su intento de "romper" los sistemas de seguridad de las redes e irrumpir en ellas con diversas intencionalidades. Podemos afirmar que la eterna lucha entre el bien y el mal ahora se ha extendido al ciber espacio.

## **MODALIDADES**

### **PHISHING.-**

Consistente en falsificar una página o portal web que simula el servicio de una entidad bancaria o financiera, donde el usuario, previo mensajes de correo electrónico es convencido a ingresar a un link re-direccionado (hosting falso), en muchas ocasiones le solicitan ingresar o actualizar sus datos de su tarjeta de crédito, contraseñas o datos personales, a causa de un supuesto error o averías en el sistema de Internet. Obviamente que estos datos ingresados serán utilizados para realizar transferencias o desvíos electrónicamente vía Internet.

### **KEYLOGGER.-**

Son dispositivos para “registrar las acciones del teclado”, es una herramienta que se descarga en nuestro servidor para realizar el registro de las pulsaciones que ejecuta el teclado, siendo almacenado en un fichero (carpeta), para luego ser extraído a través de Internet.

### **SCAMMING.-**

Son correos electrónicos fraudulentos, que pretenden estafar económicamente por medio del "engaño", generalmente ofrecen oportunidades de viaje, premios, préstamos, donaciones, lotería, ofertas, promociones, cursos, becas, etc.; logrando convencer ilícitamente a un usuario para proporcionar sus datos personales, lugar de residencia, número de teléfono, cuentas bancarias, etc.; existe una variedad de estafas vía Internet, precisando los siguientes:

- a) Oportunidad de cobro de una suma de dinero en algún país lejano como resultado de una resolución judicial.
- b) Una persona "amiga" en el extranjero lo refirió para el sorteo de un viaje en crucero durante 7 días, para dos personas.
- c) Préstamos de dinero o refinanciamiento de deudas a muy bajo interés.

- d) Comunicación de haber ganado un premio en una Lotería.
- e) Apelar al dolor humano para contribuir a una causa noble. Puede estar combinado con el PHISHING.
- f) Venta de software por Internet, supuestamente legal y licenciado.

### **SPYWARE.-**

Son pequeños programas que se instalan en nuestro sistema u ordenador, con la finalidad de rastrear nuestros datos y espiar nuestros movimientos por la red. Luego envían esa información a otro servidor para fines ilícitos. Se instalan o cuelgan, cuando:

- a) Al visitar sitios de Internet que nos descargan su código malicioso (ActiveX, JavaScripts o Cookies), sin nuestro consentimiento.
- b) Acompañando de algún virus o llamado un Troyano.
- c) Estando ocultos en un programa gratuito (Freeware) los cuales al aceptar sus condiciones de uso (casi siempre en inglés y que no leemos), estamos aceptando que cumplan sus funciones de espía.

### **VIRUS INFORMÁTICOS.-**

Son ataques perniciosos, dañinos y destructivos, sí son realizados totalmente a través de las computadoras y en casos especiales con la complicidad de terceros, en forma física en determinadas eventualidades; podríamos citar las siguientes:

- a) La propagación de virus informáticos destructivos.
- b) Envío masivo de correo no deseado o SPAM.
- c) Suplantación de los remitentes de mensajes con la técnica Spoofing.
- d) Envío o ingreso subrepticio de archivos espías o Keloggers
- e) Uso de Troyanos / Backdoors para el control remoto de los sistemas o la sustracción de información.
- f) Uso de archivos BOT del IRC y Rootkits, para el control remoto de sistemas, sustracción de información y daños irreversibles.
- g) Ataques a servidores con el objeto de sabotearlos.

### **PHARMING.-**

Es la explotación de una vulnerabilidad en el software de los servidores DNS (Domain Name System) o en el de los equipos de los propios usuarios, que permite a un atacante redireccionar un nombre de dominio (domain name) a otra máquina distinta. De esta forma, un usuario que introduzca un determinado nombre de dominio que haya sido redireccionado, accederá en su explorador de internet a la página web que el atacante haya especificado para ese nombre de dominio.

### **SPAM.-**

Es el correo electrónico denominado “basura” o “sms basura”, habitualmente de tipo “publicitario”, enviados en grandes cantidades (incluso masivas), que perjudican al receptor. La más utilizada en la web, es mediante el envío de música, protector de pantalla, etc.

### **ADWARE.-**

Un programa adware es cualquier programa que automáticamente se ejecuta, muestra o baja publicidad al computador después de instalado el programa o mientras se está utilizando la aplicación.

### **ZOMBIES.-**

Es la denominación que se asigna a computadoras que tras haber sido infectadas por algún tipo de malware, pueden ser usadas por terceras personas para ejecutar actividades hostiles. Este uso se produce sin la autorización o conocimiento del usuario. El nombre procede de los zombis o muertos vivientes esclavizados, figuras legendarias surgidas de los cultos vudú.

### **INGENIERIA SOCIAL.-**

La ingeniería social es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Es una técnica que pueden usar

ciertas personas, tales como investigadores privados, criminales o ciberdelincuentes (conocidos como “hackers”, aunque el termino correcto es “cracker”) para obtener información, acceso o privilegios que les permitan realizar algún acto que perjudique o exponga la fuente accedida a riesgo o abusos.

### **SKIMMING.-**

Son dispositivos colocados en cajeros, monederos electrónicos, saldo-maticos, pin pad, POS, skimmer, puertas de acceso, etc. para obtener en forma fraudulenta la banda magnética y el PIN de una tarjeta electrónica, para luego ser clonado o copiado.

### **CARDADO.-**

Son registros que utilizan los –skimmers- o clonadores vía Internet o cajeros automáticos, con el fin de verificar el saldo de las tarjetas electrónicas clonadas, mediante compras con montos pequeños para que el usuario o cliente no se alerte de la pérdida, retiro o transferencia.

### **CHEXTING.-**

Extraído del termino ingles “cheat” (engañar) y “texting” (escribir mensajes), son mensajes de texto (MSM) o chats enviados desde un celular o Internet que intimidan o comprometen al usuario.

### **NUMERATI.-**

Son correos electrónicos o programas aplicativos que se descargan en nuestro servidor con el fin de rastrear nuestros movimientos por la red, para luego ser comercializados a empresas de servicios, publicidad o estadística. Para disuadir a los usuarios a visitar sitios o paginas web re-direccionados, con fines comerciales.

## **DESCRIPCION TIPICA**

En nuestro Código Penal aprobado mediante Decreto Legislativo Nro. 635 (08ABR1991), se pretendió hacer frente al problema desde una visión patrimonialista incorporando delitos que estén acordes con las nuevas formas de criminalidad informática (Art. 186 Num. 3). Con fecha 17JUL2000 se promulgo la Ley Nro. 27309, que incorpora los típicos delitos informáticos a nuestro Código Penal. Los mismos que en doctrina también se les conoce con las denominaciones de “delitos electrónicos”, “delitos relacionados con la computadora”, “crímenes por computadora”, “delitos de cuello blanco”, “delitos relacionados con el ordenador” o “delitos a través de medios informáticos”; descritos con el siguiente detalle:

### **ARTICULO 207-A DELITO INFORMÁTICO.-**

El que utiliza o ingresa indebidamente a una base de datos, sistema o red de computadoras o cualquier parte de la misma, para diseñar, ejecutar o alterar un esquema u otro similar, o para interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos, será reprimido con pena privativa de libertad no mayor de dos años o con prestación de servicios comunitarios de cincuentidós a ciento cuatro jornadas.

Si el agente actuó con el fin de obtener un beneficio económico, será reprimido con pena privativa de libertad no mayor de tres años o con prestación de servicios comunitarios no menor de ciento cuatro jornadas.

**ARTICULO 207-B ALTERACIÓN, DAÑO Y DESTRUCCIÓN DE BASE DE DATOS, SISTEMA, RED O PROGRAMA DE COMPUTADORAS.-**

El que utiliza, ingresa o interfiere indebidamente una base de datos, sistema, red o programa de computadoras o cualquier parte de la misma con el fin de alterarlos, dañarlos o destruirlos, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años y con setenta a noventa días multa.

**ARTICULO 207-C DELITO INFORMÁTICO AGRAVADO.-**

En los casos de los Artículos 207-A y 207-B, la pena será privativa de libertad no menor de cinco ni mayor de siete años, cuando:

1. El agente accede a una base de datos, sistema o red de computadora, haciendo uso de información privilegiada, obtenida en función a su cargo.
2. El agente pone en peligro la seguridad nacional.

## **DELITOS CONCORDANTES**

El delito informático puede ser definido como aquella conducta típica, antijurídica, culpable y punible en la que la computadora o algún medio informático, sus técnicas y funciones desempeñan un papel trascendente, ya sea como método, medio o fin en el logro de los objetivos ilícitos (perjuicio de tipo patrimonial). En términos más sencillos se puede definir como *–el uso de cualquier medio informático para obtener un beneficio indebido en perjuicio de otro–*. Existiendo en nuestro Código Penal diversos artículos que tipifican o tienen aplicación directa en la investigación de los delitos informáticos.

### **A. COACCION.-**

El Artículo 151 del Código Penal, describe “El que, mediante amenaza o violencia, obliga a otro a hacer lo que la ley no manda o le impide hacer lo que ella no prohíbe”. Esta tipificación es concordante con el Art. 2 Inc. 3, 4, 8, 15 y 24 de la Constitución Política del Perú, los mismos que son vulnerados mediante el uso de un medio informático (computadora, aparato celular, video-filmación, cámara fotográfica, radio-transmisión, USB, Internet, e-mail, msm, etc).

### **B. VIOLACIÓN DE LA INTIMIDAD.-**

El Artículo 154 del Código Penal detalla lo siguiente: “El que viola la intimidad de la vida personal y familiar ya sea observando, escuchando o registrando un hecho, palabra, *escrito o imagen*, valiéndose de

*instrumentos, procesos técnicos u otros medios...* “Si utiliza algún medio de comunicación social...”

Asimismo en el Artículo 157 del Código Penal precisa lo siguiente: “El que indebidamente, organiza, proporciona o emplea *cualquier archivo* que tenga datos referentes a las convicciones políticas o religiosas y otros aspectos de la vida íntima de una o más personas...”

### **C. TURISMO SEXUAL INFANTIL.-**

El Código Penal describe en el Artículo 181-A “El que promueve, publica, favorece o facilita el turismo sexual, a través de cualquier *medio escrito, folleto, impreso, visual, audible, electrónico, magnético o a través de Internet*, con el objeto de ofrecer relaciones sexuales de carácter comercial de personas de catorce y menos de dieciocho años de edad...”

### **D. PORNOGRAFIA INFANTIL.-**

Previsto en el Artículo 183-A del Código Penal, “El que posee, promueva, fabrique, distribuya, exhiba, ofrece, comercializa o publica o exporta por cualquier medio incluido la Internet... en los cuales se utilice personas de catorce y menores de dieciocho años de edad...” En la actualidad los actos de *PEDOFILIA*, son cometidos a partir de la soledad de los niños, causada por diversos motivos (conflicto entre padres, falta de diálogo, abandono o uso indebido de Internet), esto conlleva que los niños acudan a las cabinas públicas de Internet para entablar amistad o comunicación con personas desconocidas. Es allí donde, principalmente a través del Chat (Twitter, Facebook, Mirc, Messenger, etc) los pedófilos

encuentran el camino y la forma más fácil para ganarse la confianza, luego seducirlos y finalmente convencerlos a sus bajos instintos (*dejando un trauma imborrable en sus pequeñas e inocentes víctimas*).

#### **E. HURTO DEL ESPECTRO ELECTROMAGNETICO.-**

El Artículo 185 del Código Penal, establece “El que, para provecho, se apodera ilegítimamente de un bien mueble, total o parcialmente ajeno, sustrayéndolo del lugar donde se encuentra...” “Se equiparan a bien mueble... *el espectro electromagnético*”. Con el avance de la informática diversas empresas informales vienen sustrayendo y comercializando los servicios de Internet inalámbrico, televisión de cable y telefonía móvil, colgándose de los servicios autorizados (con licencia), clonando los códigos de usuario o servicio. Esto se observa en grifos, supermercados, cajeros, agentes financieros, cabinas o domicilios (incluso fabrican sus antenas en forma artesanal).

#### **F. HURTO AGRAVADO POR TRANSFERENCIA ELECTRÓNICA DE FONDOS, TELEMÁTICA EN GENERAL Y EMPLEO DE CLAVES SECRETAS.-**

El Artículo 186 del Código Penal, segundo párrafo numeral 3 (modificado por la Ley Nro. 26319), el cual dispone “... si el hurto es cometido mediante la utilización de sistemas de transferencia electrónica de fondos, de la telemática en general, o la violación del empleo de claves secretas”. En la actualidad es el ilícito mas utilizado por el cibercrimen denominados: “*phishers*”, “*hackers*” o “*crackers*” (sujetos que consiguen las contraseñas y cuentas bancarias), “*cashing*” (sujetos que maniobran, operan y generan los fraudes), “*droppers*” (sujetos que

consiguen a las personas -muchas veces engañadas-, con cuentas en los bancos, conocidos como “*drops*”, receptores del fraude). En muchos casos son sujetos que tienen amplio conocimiento de informática o avance tecnológico (ex-empleados de entidades financieras, soporte técnico, seguridad informática, estudiantes de sistemas o informática, redes sociales), empleando diversos programas aplicativos (*scamming*, *keylogger*, *spyware* o *troyanos –espías- y spam*); que se disfrazan mediante software gratuitos (música, caricaturas o e-mail –basura-), soportes que se instalan y trabajan en forma “*secreta*” y “*automáticamente*” en un servidor (espiando nuestros movimientos en la red). Su metodología se resume a registrar todos los datos escritos a través del teclado. Para luego ser trasladados fuera de la computadora del usuario para ser almacenados en bases de datos externas y utilizados en forma indebida para realizar transferencias bancarias.

El delito de hurto agravado por transferencia electrónica de fondos tiene directa importancia en la actividad informática, así como en el sistema de transferencia de fondos, se refiere a la totalidad de las instituciones y prácticas bancarias que permiten y facilitan las transferencias interbancarias de fondos; uno de los medios de transferencia electrónica de fondos se refiere a colocar sumas de dinero de una cuenta a otra, ya sea dentro de la misma entidad financiera o una cuenta en otra entidad de otro tipo, ya sea pública o privada. Cuando se refiere a “empleo de claves secretas” se está incluyendo la vulneración de password, de niveles de seguridad, de códigos o claves secretas.

#### **G. DELITO DE ESTAFA.-**

El delito de estafa, previsto en el Art. 196 del CP, se define como el perjuicio patrimonial ajeno, causado mediante engaño, astucia, ardid u

otra forma fraudulenta, induciendo o manteniendo prendida por el delito de estafa. En primer lugar, y en cuanto al engaño que se requiere en la estafa, éste se refiere de manera directa a una persona física, aunque últimamente algunos autores indican que puede estar dirigido a una persona jurídica. Sin embargo, el problema principal estriba en si la introducción de datos falsos en una máquina equivale al engaño sobre una persona. La opinión unánime de la doctrina, -y a la que nos adherimos-, rechaza tal identificación, puesto que, mientras en un extremo se encuentra el delincuente informático, en el otro existe una computadora. En realidad, para que exista engaño, es requisito la participación de dos personas.

Es indudable que en algunas conductas de manipulación fraudulenta sí se podrá configurar el delito de estafa, por ejemplo, cuando el delincuente informático engaña mediante una computadora a otra persona que se encuentra en el otro terminal; en este caso, al haber dos personas, podrá sustentarse el engaño, en donde el medio empleado para conseguirlo es una computadora.

También en la actualidad se puede plantear el engaño a una persona jurídica, como en el caso en que se solicita un préstamo al banco, falseando la situación económica real, o en el que ante una compañía de seguros se miente sobre el verdadero estado de salud de la persona.

Desde el punto de vista del Derecho Penal, se niega la posibilidad de engañar a una máquina. En este sentido, la computadora es sólo una máquina, un instrumento creado por el hombre.

En cuanto al error, como elemento de la estafa, se requiere la concurrencia de dos personas, lo cual se deduce de la descripción del tipo en el Art. 196 del CP, donde se indica "induciendo o manteniendo

en error al agraviado mediante engaño". Además, el error es entendido como el estado psíquico que padece el agraviado como consecuencia del engaño. Por estas razones es que en la manipulación de computadoras, tal y como está concebida y establecida en el Código Penal, no es posible sustentar que existe un engaño. De otro lado, no puede sostenerse que la computadora incurre en un error, dado que actúa conforme a los mandatos o datos de las instrucciones manipuladas.

Por tanto, no hay estafa en los casos de manipulación de máquinas automáticas, pues no se puede hablar ni de error ni de engaño; sólo podrá plantearse hurto en el caso que se obtenga un bien mueble, pero será un hecho impune cuando se trata de prestación de servicios. Un problema semejante tiene lugar con la manipulación de computadoras a través de la introducción y alteración de programas.

En referencia al acto de disposición patrimonial en el delito de estafa, éste ha de realizarlo la persona engañada, quien se encuentra en una situación de error, de ahí que siempre se entienda en la estafa que el acto de disposición es un acto humano, es decir, realizado por una persona. En el caso de las manipulaciones informáticas fraudulentas el acto de disposición lo realiza la computadora, con lo cual se rompe el esquema planteado en el delito de estafa.

Finalmente, en cuanto al perjuicio en el delito de estafa, éste no ofrece mayor problema para comprenderlo dentro de la manipulación de una computadora, puesto que en ambos casos normalmente se causa un perjuicio a la persona.

En conclusión, en la legislación peruana, la casi totalidad de supuestos de manipulación de computadoras no puede acogerse dentro del delito de estafa. La única manera sería creando un tipo especial defraudatorio

donde se prescinda de los elementos básicos de la estafa, -el engaño a una persona y la subsiguiente provocación del error.

Entre las conductas defraudatorias cometidas mediante computadora y las defraudaciones en general, -dentro de las cuales se encuentra la estafa- existe una afinidad o proximidad en los conceptos. Pero al examinar más exhaustivamente los elementos típicos de la estafa, se acaba concluyendo que el fraude informático y el delito de estafa prácticamente sólo tienen en común el perjuicio patrimonial que provocan.

Dentro de las manipulaciones informáticas se distingue:

- a) La fase input o entrada de datos en la cual se introducen datos falsos o se modifican los reales añadiendo otros, o bien se omiten o suprimen datos.
- b) Las manipulaciones en el programa que contiene las órdenes precisas para el tratamiento informático.
- c) La fase output o salida de datos, donde no se afecta el tratamiento informático, sino la salida de los datos procesados al exterior, cuando van a ser visualizados en la pantalla, se van a imprimir o registrar.
- d) Las manipulaciones a distancia, en las cuales se opera desde una computadora fuera de las instalaciones informáticas afectadas, a las que se accede tecleando el código secreto de acceso, con la ayuda de un modem y de las líneas telefónicas.

El punto medular de la delincuencia informática es la manipulación de la computadora. La conducta consiste en modificaciones de datos, practicados especialmente por empleados de las empresas perjudicadas, con el fin de obtener un enriquecimiento personal, por ejemplo, el pago de sueldos, pagos injustificados de subsidios, manipulaciones en el balance, etc.

**H. FRAUDE EN LA ADMINISTRACIÓN DE PERSONAS JURÍDICAS EN LA MODALIDAD DE USO DE BIENES INFORMÁTICOS.-**

Puesto que en el patrimonio de la persona están incluidos tanto bienes materiales (hardware) como inmateriales (software, información, base de datos, etc), esta figura delictiva puede aplicarse al campo informático según interpretación del Artículo 198º Inciso 8 del Código Penal, establece que: "... en su condición de fundador, miembro del directorio o del consejo de administración o del consejo de vigilancia, gerente, administrador o liquidador de una persona jurídica, realiza, en perjuicio de ella o de terceros, cualquiera de los actos siguientes: Usar en provecho propio o de otro, el patrimonio de la persona (Inciso 8)..." Esta figura podría aplicarse, en este orden de ideas, tanto al uso indebido de software, información, datos informáticos, hardware u otros bienes que se incluyan en el patrimonio de la persona jurídica.

**I. DELITO DE DAÑOS.-**

Se encuentra tipificado en el Artículo 205º del Código Penal, el comportamiento consiste en dañar, destruir o inutilizar un bien. En el sistema informático, el delito de daños existirá si usuarios, carentes de autorización, alteran o destruyen archivos o bancos de datos a propósito. Es importante precisar que, si los daños se producen de manera negligente, quedarán impunes dado que el delito de daños sólo puede cometerse de manera dolosa. Estos hechos se conocen como "sabotaje", hechos que resultan ser favorecidos gracias a la concentración de información en un mínimo espacio. La destrucción total de programas y datos puede poner en peligro la estabilidad de una empresa e incluso de la economía nacional. El modus operandi de estos actos se viene perfeccionando con el tiempo; en primer lugar, se

realizaban con la perpetración de incendios, posteriormente, con la introducción de los denominados “programas crasch”, virus, time bombs (la actividad destructiva comienza luego de un plazo), cancer roudtine (los programas destructivos tienen la particularidad de que se reproducen por sí mismos), que borran grandes cantidades de datos en un cortísimo espacio de tiempo.

Es indudable que estos comportamientos producen un daño en el patrimonio de las personas, por lo que no hay inconveniente en sancionar penalmente dichas conductas. Pero es necesario indicar que con el delito de daños sólo se protege un determinado grupo de conductas que están comprendidas en el delito informático, quedando fuera otras, como por ejemplo, el acceso a una información reservada sin dañar la base de datos. De ahí que el delito de daños será de aplicación siempre que la conducta del autor del hecho limite la capacidad de funcionamiento de la base de datos.

#### **J. CONTRA LOS DERECHOS INTELECTUALES Y CONTRA LOS DERECHOS DE AUTOR DE SOFTWARE.-**

Tipificados en el Artículo 216° del Código Penal, el comportamiento consiste en copiar, reproducir, exhibir o difundir al público, en todo o en parte, por impresión, grabación, fonograma, videograma, fijación u otro medio, una obra o producción literaria, artística, científica o técnica, sin la autorización escrita del autor o productor o titular de los derechos. A esta conducta los autores asimilan lo que se conoce como “piratería de software” frente a la copia ilícita. Estos hechos han alcanzado en la realidad una especial gravedad dada la frecuencia con la que abundan copias piratas de todo tipo de programas de computadoras. En nuestro país se promueve la creación de una fiscalía especializada en la

persecución de todas las conductas relativas a la defraudación del derecho de autor. Por tanto, el delito contra los derechos intelectuales sólo comprenderá un grupo de comportamientos incluidos en el delito informático, básicamente, los referidos contra los derechos de autor, por su creación científica en el campo del software.

El Decreto Legislativo 822, modificó el Código Penal, y se han aumentado las penas, con respecto a la legislación peruana anterior, así tenemos:

**F.1. Artículo 217º del CP.-**

Establece "...el que con respecto a una obra o una grabación audiovisual o una imagen fotográfica expresada en cualquier forma, realiza cualquiera de los siguientes actos, sin la autorización previa y escrita de autor o titular de los derechos". Este artículo garantiza la protección de los derechos patrimoniales de los contratos de licencia de uso de software, que contemplan el respeto de estos derechos y también en la Ley de Derecho de Autor. La autorización previa y escrita del titular, generalmente en la actividad empresarial se instrumenta en una licencia de uso de software.

**F.2. Artículo 218º del CP.-**

Dispone los supuesto tratados en este artículo se refieren tanto a derecho morales como patrimoniales, que por su gravedad (atentar contra el derecho de paternidad, comercializar o distribuir copias ilegales, registrar en forma indebida el software) llegando ha ampliar la pena hasta ocho años.

**F.3. Artículo 219º del CP.-**

Establece "...el que con respecto a una obra, la difunda como propia, en todo o en parte, copiándola o reproduciéndola textualmente, o tratando de disimular la copia mediante ciertas alteraciones, atribuyéndose o atribuyendo a otro, la autoría o titularidad ajena". La apropiación de autoría ajena, de reputarse una obra que no es de uno como propia, también se aplica al software, más aún con las opciones tecnológicas para su copia, que incluyen equipos de cómputo, cada vez más sofisticados y el uso de herramientas en Internet.

**F.4. Artículo 220º del CP.-**

- a) Quien se atribuya falsamente la calidad de titular originario o derivado, de cualquiera de los derechos protegidos en la legislación del derecho de autor y derechos conexos y, con esa indebida atribución, obtenga que la autoridad competente suspenda el acto de comunicación, reproducción o distribución de la obra, interpretación, producción, emisión o de cualquier otro de los bienes intelectuales protegidos.
- b) Si el agente que comete cualquiera de los delitos previstos... posee la calidad de funcionario o servidor público.

Una de las preocupaciones de los creadores de software, al registrar su obra en el Registro Nacional de Derecho de Autor de INDECOPI, es que se tiene que entregar, entre otros requisitos, el programa fuente, se cuestionan que sucede si lo copian sin su

consentimiento. Dado que el depósito es intangible, los funcionarios que cometieran estos delitos estarían dentro de este tipo penal y podrían ser pasibles de pena privativa de libertad hasta ocho años.

**K. DELITO CONTRA LA PROPIEDAD INDUSTRIAL.-**

El Artículo 222 del Código Penal en el numeral “C” detalla: “Un producto amparado por un diseño industrial registrado en el país”, así como en el numeral “F”, donde describe “Un producto o servicio que utilice una marca no registrada idéntica o similar a una marca registrada en el país” *(mediante la utilización de soportes informáticos -software o programas- para copiar, adulterar o falsificar marcas registradas)*.

Seguidamente el Artículo 222-A establece la penalización de la clonación o adulteración de terminales de telefonía celular, donde se detalla “El que altere, modifique, duplique o de cualquier modo modifique un número de línea, o un terminal celular, de modo tal que pueda ocasionar perjuicio al titular o usuario del mismo así como a terceros”. Esta adición muestra la actividad ilícita del *flasheo, desbloqueo, cambio de servidor* o empresa de telefonía.

**L. FALSEDAD DOCUMENTAL E INFORMÁTICA.-**

El Decreto Legislativo 681 modificado por la Ley 26612, es la norma que regula el valor probatorio del documento informático (incluyendo los conceptos de microforma y microduplicado tanto al microfilm como al documento informático). El Artículo 19 de esta norma establece que “la falsificación y adulteración de microformas, microduplicados y

microcopias sea durante el proceso de grabación o en cualquier otro momento, se reprime como delito contra la fe pública, conforme las normas pertinentes del Código Penal”.

Por tanto, esta modalidad delictiva puede aplicarse al delincuente informático siempre y cuando se supere la concepción tradicional de documento que mantiene la legislación penal peruana, anclada básicamente en un papel escrito, y que se acepten nuevas formas de expresión documental, sobre la base de disquetes, CD, discos duros, en cuanto sistemas actuales de expresión de información.

En el Código Penal, entre los delitos contra la fe pública, que son aplicables a la falsificación y adulteración de microformas digitales tenemos los siguientes:

### **C.1. FALSIFICACIÓN DE DOCUMENTOS.-**

“El que hace, en todo o en parte, un documento falso o adultera uno verdadero que pueda dar origen a derecho u obligación o servir para probar un hecho con el propósito de utilizar el documento...” (Artículo 427 del Código Penal). Tratándose de microformas digitales su falsificación y/o adulteración son sancionados con la misma pena.

### **C.2. FALSEDAD IDEOLÓGICA.-**

“El que inserta o hace insertar, en instrumento público, declaraciones falsas concernientes a hechos que deben probarse con el documento, con el propósito de emplearlo como si la declaración fuera conforme a la verdad...” (contemplado en el Artículo 428 del Código Penal). La microforma digital de un documento público tiene su mismo valor, por tanto puede darse el

caso de falsedad ideológica de instrumentos públicos contenidos en microformas digitales.

### **C.3. OMISIÓN DE DECLARACIÓN EN DOCUMENTO.-**

“El que omite en un documento público o privado declaraciones que deberían constar o expide duplicados con igual omisión al tiempo de ejercer una función y con el fin de dar origen a un hecho u obligación...” (descrito en el Artículo 429 del Código Penal). Para que tenga valor probatorio y efecto legal una microforma digital tiene que cumplir requisitos formales y técnicos. El requisito formal consiste en que debe ser autenticado por depositario de la fe pública (fedatario juramentado o notario) el proceso técnico de micrograbación y que las copias de esos documentos deben ser certificados, por lo cual una omisión de las declaraciones que por ley deben incluirse podría configurar esta figura delictiva.

### **C.4. FALSIFICACIÓN DE SELLOS, TIMBRES Y MARCAS OFICIALES.-**

El Artículo 434 del Código Penal describe: “El que fabrica, fraudulentamente, o falsifica sellos o timbres oficiales de valor...” “Cuando el agente emplea como auténticos o todavía válidos los sellos o timbres oficiales de valor que son falsos, falsificados o ya usados...”

El Artículo 435 detalla: “El que fabrica, fraudulentamente, o falsifica marcas o contraseñas oficiales destinadas a hacer constar el resultado de un examen de la autoridad o la concesión de un permiso o la identidad de un objeto o el que a sabiendas de

su procedencia ilícita hace uso de tales marcas”. En nuestro medio la fabricación de sellos o timbres oficiales es mediante la utilización de software o programas que facilitan su creación o fabricación; siendo su empleo o expedición sin las respectivas normas de control.

**C.5. FALSEDAD GENERICA.-**

“El que de cualquier otro modo que no este especificado en los Capítulos precedentes, comete falsedad simulando, suponiendo alterando la verdad intencionalmente y con perjuicio de terceros, por palabras, hechos usurpando nombre, calidad o empleo que no le corresponde, suponiendo que viva a una persona fallecida o que no haya existido o viceversa”. Con el uso de la informática se ha facilitado la adulteración, modificación o edición de documentos.

# METODOLOGIA DE INVESTIGACION

## BENEFICIOS DE LA INFORMATICA



## ORGANIGRAMA ESTRUCTURAL

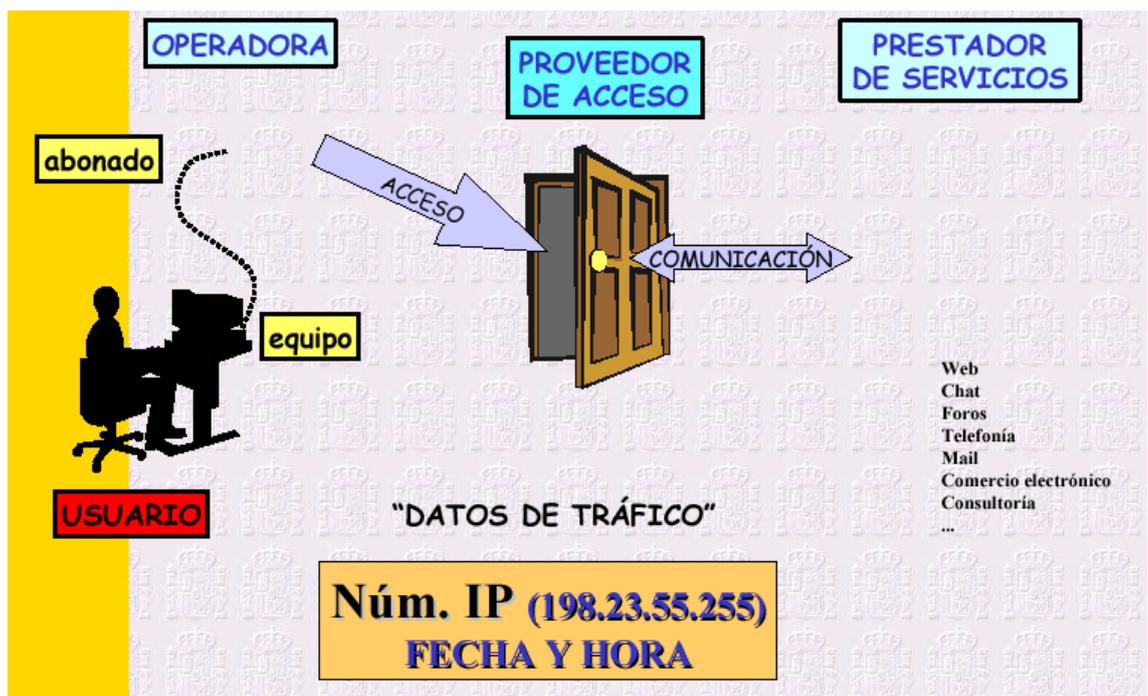
RD N° 1695-DIRGEN/EMG del 08AGO2005 crea la SEINDAT dentro de la estructura orgánica de la DIVINCRI, con la MISIÓN de investigar, denunciar y combatir el crimen organizado dentro del campo de la informática.



## LA INVESTIGACION POLICIAL



## LA INVESTIGACION TECNOLOGICA



## FASES DE LA INVESTIGACION

**¿cómo?** → **IDENTIFICACIÓN OBTENCIÓN DE PRUEBAS**

1. FASE PREVIA. ¿qué ha pasado?
1. FASE DE INVESTIGACIÓN. ¿cómo y quién lo ha hecho?
1. FASE DE INCRIMINACIÓN. Asegurar y presentar la prueba

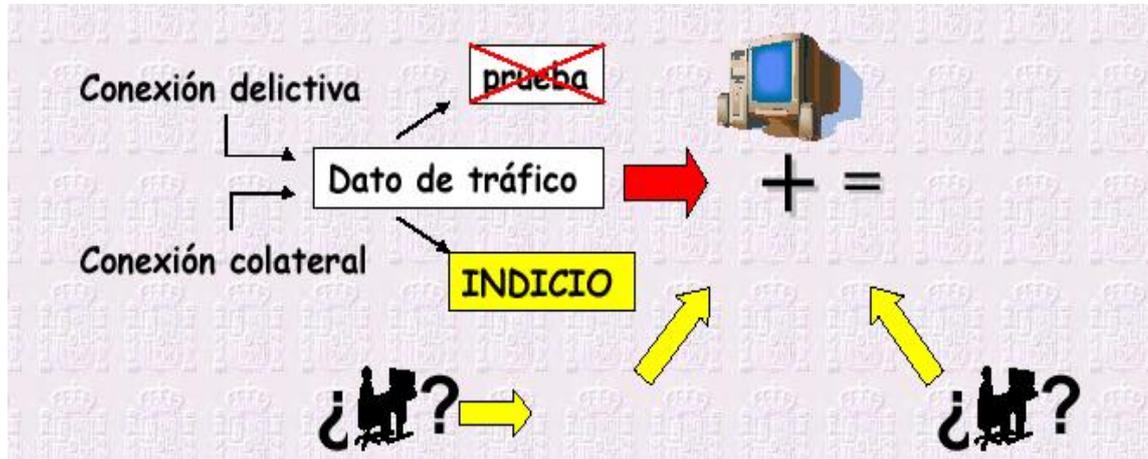
### 1. FASE PREVIA

- Denuncia - Conocimiento delito público
- Recogida de evidencias del delito (~inspección ocular)
  - Recuperación de logs, mensajes, backups, imágenes (volcado), ...
  - Penalidad añadida a la víctima.
  - Auxilio administradores de sistemas afectados.
  - Acreditar el delito.

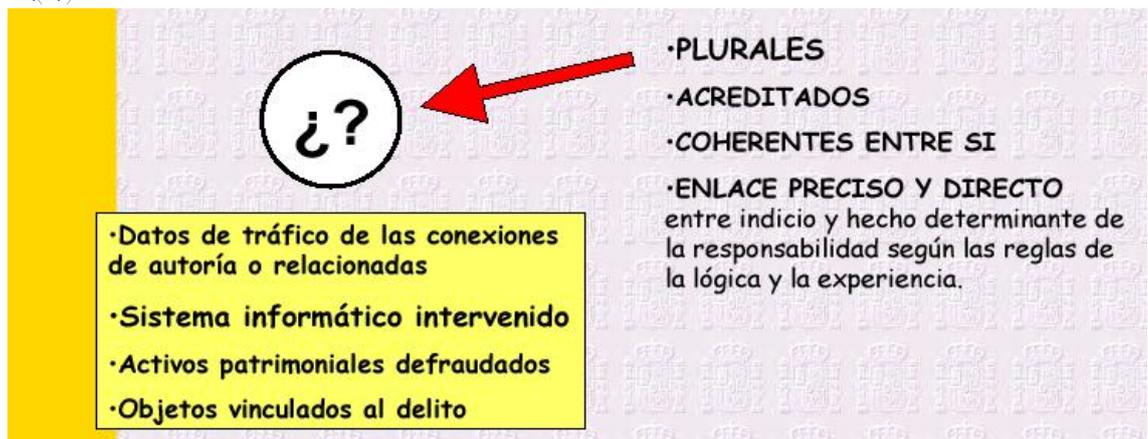
### 2. FASE DE INVESTIGACION

- Análisis de evidencias y búsqueda de indicios de autoría
- Búsqueda de información (ayudas externas) y referencias identificativas (vanidad)
- Resolución de "datos de tráfico" de indicios y referencias identificativas (ISP,s)
- Identificación y localización (teléfono)
- Vigilancia
- Interceptación de telecomunicaciones (teléfono, e-mail, sniffers, ADSL)

## (a) ¿Como y quien?



## (b) Prueba informática



## 3. FASE DE INCRIMINACION

- 1) Registro e incautación (protocolo validación de la prueba)
- 2) Análisis forense de sistema y soportes intervenidos
- 3) Informe policial incriminatorio

## (a) Objetivo del análisis

- Localización, identificación y aseguramiento de cuantas evidencias se hallen para construir la prueba de indicios.
- Localización, identificación y aseguramiento de cuantas evidencias se hallen que vinculen equipo informático, usuario e indicios .

## (b) Problemática del análisis

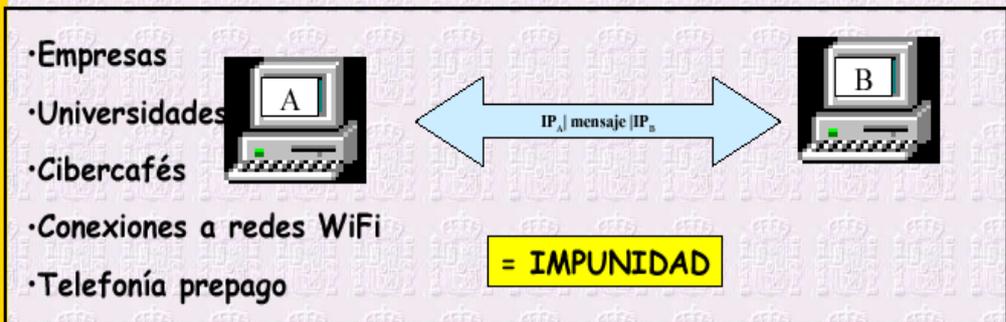
- Desconocimiento generalizado en el estamento judicial.
- Ausencia de protocolo de volcado y análisis homologados.
- Sistemas hardware, software, no homologados.
- Sistemas propietarios, no open source
- Sistemas lentos con elevadas incidencias. (Firma digital, Timestamping).
- Sistemas caros (HD). Se mantiene la identidad digital.
- Limitaciones por cifrado.
- Posibilidad de falsificación de indicios (coartadas).

## (c) El informe policial

- Descripción del conjunto de evidencias electrónicas que interrelacionadas conducen por un razonamiento lógico a una conclusión de culpabilidad.
- Traducción del lenguaje técnico informático a un lenguaje coloquial y comprensible para profanos en la materia.
- Descripción de los protocolos de actuación utilizados en el proceso de análisis.

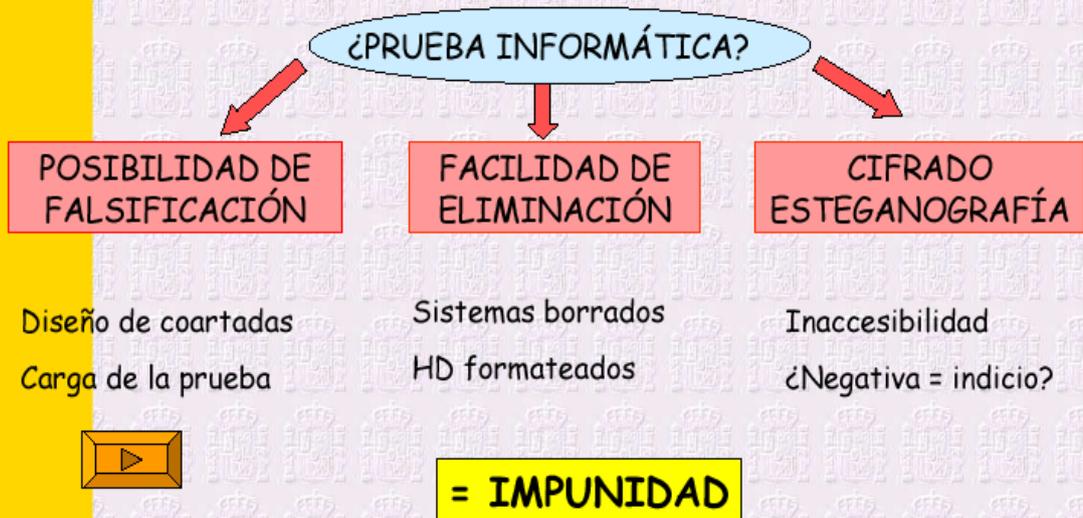
# PROBLEMATICA DE LA INVESTIGACION

## 1. IMPOSIBILIDAD DE IDENTIFICACIÓN DEL USUARIO



**AUSENCIA** de legislación administrativa sobre cibercafés, telefonía prepago, ...

## VIRTUALIDAD DE LA PRUEBA INFORMÁTICA



# HECHOS POLICIALES

















**Cualquier información ó denuncia escriba a nuestros correos:**  
[seindat\\_divincriusco@hotmail.com](mailto:seindat_divincriusco@hotmail.com)  
[detective355@hotmail.com](mailto:detective355@hotmail.com)

**Teléfonos:**  
084-222796  
084-984702511 ó 084-984346135

**Escribanos al Blog:**  
[http://detective\\_355.blogspot.com](http://detective_355.blogspot.com)