



RESUMEN

En la actualidad la informatización se ha implantado tanto en la organización y administración de empresas y administraciones públicas como en la investigación científica, en la producción industrial o en el estudio e incluso en el ocio, el uso de la informática es en ocasiones indispensable y hasta conveniente. Sin embargo, junto a las incuestionables ventajas que presenta comienzan a surgir algunas facetas negativas, como por ejemplo, lo que ya se conoce como “criminalidad informática”.

La delincuencia informática se comete en el ciberespacio, y no se detiene en las fronteras nacionales convencionales. En principio, puede perpetrarse desde cualquier lugar y contra cualquier usuario de ordenador del mundo. Se necesita una acción eficaz, tanto en el ámbito nacional como internacional, para luchar contra la delincuencia informática. En los países, las reacciones frente a la delincuencia informática se centran en el derecho nacional, descuidando medidas alternativas de prevención, no hay respuestas globales, a pesar de los esfuerzos de las organizaciones internacionales y supranacionales, las diversas leyes nacionales de todo el mundo ponen de manifiesto considerables diferencias, especialmente en las disposiciones del derecho penal sobre piratería informática, protección del secreto comercial y contenidos ilícitos. También existen diferencias en cuanto al poder coercitivo de los organismos investigadores, la jurisdicción en materia penal, y con respecto a la responsabilidad de los proveedores de servicios intermediarios por una parte y los proveedores de contenidos por otra.

De lo anteriormente anotado podemos concluir preguntándonos, ¿Está nuestro país preparado para detectar y enfrentar a la delincuencia informática?, ¿Cuenta nuestro país con una legislación apropiada para enfrentar los delitos informáticos?

PALABRAS CLAVES: Delitos informáticos, criminalidad informática, seguridad informática, cadena de custodia, delito informático.



ÍNDICE

LA CRIMINALIDAD INFORMÁTICA: PROPUESTA PARA LA TIPIFICACIÓN DE LOS DELITOS INFORMÁTICOS EN LA LEGISLACIÓN ECUATORIANA

INTRODUCCIÓN	9
CAPÍTULO I	
ANTECEDENTES HISTÓRICOS	12
1. Enfoque internacional sobre la criminalidad informática	12
Delimitación del fenómeno	17
Las víctimas de los delitos informáticos	26
Sujeto Activo	29
Sujeto Pasivo	29
Tipos de delitos informáticos reconocidos por las Naciones Unidas	30
Legislación Internacional sobre los delitos informáticos	33
<i>Alemania</i>	33
<i>Austria</i>	35
<i>Francia</i>	36
<i>Gran Bretaña</i>	37
<i>Holanda</i>	37
<i>España</i>	37
<i>Estados Unidos de Norteamérica</i>	39
<i>Chile</i>	40
<i>Perú</i>	41
<i>Bolivia</i>	42
<i>Unión Europea</i>	42
Responsabilidades entregadas a los Organismos Policiales Extranjeros	44
INTERPOL	44
FBI	44
CUERPO NACIONAL DE POLICIA ESPAÑOLA	45
POLICIA NACIONAL DE LA REPÚBLICA DE FRANCIA	45
DRA. GRACIELA ENCALADA OCHOA	2



2. Los delitos informáticos en la legislación ecuatoriana	46
Análisis de las infracciones informáticas en la legislación ecuatoriana	52
<i>Vulneración de claves o sistemas de seguridad</i>	52
<i>Obtención de datos personales para su utilización fraudulenta</i>	56
<i>Destrucción o supresión maliciosa y fraudulenta de sistemas de datos contenidos en un sistema de información o red electrónica</i>	58
<i>Falsificación electrónica</i>	59
<i>Daños informáticos</i>	61
<i>Apropiación ilícita</i>	63
<i>Estafa</i>	64

CAPÍTULO II

RIESGOS Y VULNERABILIDADES QUE OCASIONAN LOS DELITOS INFORMÁTICOS.	66
---	-----------

1. Introducción y problemas jurídicos de la criminalidad informática	66
Problemas de persecución. Delitos a distancia y competencia territorial	68
a) Problemática con la concepción tradicional de tiempo y espacio	69
b) Anonimato del sujeto activo	72
Criterios de selección de los nuevos tipos penales	73
El Convenio del Cibercrimen (Budapest 23.11.01)	74
Individualización de responsabilidad penal	77

2. Problemas de política criminal y persecución penal asociados a la informática	78
Globalización y sistema penal	79
Delitos informáticos y otros delitos relativos a la tecnología de la informática: XV Congreso Internacional de Derecho Penal (1994, Brasil: Río de Janeiro)	81

3. Las vulnerabilidades de los sistemas operativos y la no actualización por parte de los usuarios finales de los PARQUES concernientes a la seguridad de los mismos	87
La vulnerabilidad de los sistemas informáticos	89



Los sistemas operativos	89
Objetivos para la creación de los sistemas operativos	90
Funciones de los sistemas operativos	91
Características de los sistemas operativos	91
¿Cuáles son las vulnerabilidades de un sistema?	92
Factores que hacen a un sistema más vulnerable	95
Clasificación	98
Métodos de protección	112
Parche (Informática)	113
<i>Tipos según el código</i>	113
<i>Tipos según su propósito</i>	115
La importancia de actualizar	116
4. Seguridad de la información y seguridad informática	119
Seguridad de la información	119
Principios Básicos	120
Conceptos Importantes	121
Tecnologías	123
Estándares de seguridad de la información	124
Otros estándares relacionados	124
Certificaciones	124
Certificaciones independientes en seguridad de la información	124
Seguridad en Internet	125
Ataques pasivos	126
Ataques activos	127
Medidas de seguridad en la red	128
Seguridad y protección en computación	131
Casos famosos	132
Otras amenazas y ataques posibles	133
Principios básicos para la seguridad	134
Mecanismos de autorización	134
Dominios de protección	134
Matriz de acceso	135



Listas de acceso	136
Capacidades	136
Mecanismos de autenticación	137
Claves	137
Identificación física	138
Algunas medidas básicas	138
Criptografía	138
Política de seguridad	141
Algunas afirmaciones erróneas comunes acerca de la seguridad	142
Seguridad Informática y Normativa	143
Organismos Oficiales de seguridad informática	145

CAPÍTULO III

PRESERVACION DE EVIDENCIA DIGITAL NECESARIA PARA UN PROCESO LEGAL.

	147
1. Importancia	147
2. Principios Básicos	148
3. Reconocimiento de la Evidencia Digital	149
Características de la evidencia digital	151
Hechos Informáticos que pueden ser probados en juicios	152
Informática aplicada a la Investigación Forense	153
Valoración de la pericia informática	155
Herramientas para la recolección de evidencia	156
Técnicas Forenses en una máquina individual	159
Técnicas Forenses en una red	159
Regulación Internacional	160
<i>International Organization on Computer Evidence (IOCE)</i>	161
<i>Comunidad Europea</i>	163
<i>Regulación en Estados Unidos</i>	164
Limitaciones	164
Ministerio Público del Ecuador	166



4. Acciones a realizar en la Escena del Delito	173
Rastreo de correo electrónico	179
Peritos informáticos	183
CAPITULO IV	
CONCEPTUALIZACIÓN DE LA NATURALEZA DE LOS DELITOS INFORMÁTICOS SEGÚN LA LEGISLACION ECUATORIANA: PROPUESTA PARA SU TIPIFICACIÓN.	187
Planteamiento del problema	187
Conductas susceptibles de ser tipificadas como delitos informáticos en nuestro Código penal	189
Uso de medios informáticos para la comisión de delitos comunes, como circunstancia agravante de la infracción	199
CONCLUSIONES Y RECOMENDACIONES	202
BIBLIOGRAFÍA	207
ANEXOS	216



UNIVERSIDAD DE CUENCA

FACULTAD DE JURISPRUDENCIA Y CIENCIAS POLÍTICAS Y SOCIALES

**MAESTRÍA EN DERECHO INFORMÁTICO.
MENCIÓN EN COMERCIO ELECTRÓNICO**

**“LA CRIMINALIDAD INFORMÁTICA: PROPUESTA PARA LA
TIPIFICACIÓN DE LOS DELITOS INFORMÁTICOS EN LA LEGISLACIÓN
ECUATORIANA”**

Tesis previa a la obtención del
Grado Académico de Magíster en
Derecho Informático. Mención en
Comercio Electrónico.

AUTORA: DRA. GRACIELA ENCALADA OCHOA

DIRECTOR: DR. JUAN PEÑA AGUIRRE

CUENCA-ECUADOR

2010



RESPONSABILIDAD

Los criterios e ideas expuestas en esta tesis,
son de responsabilidad de la autora.

Dra. Graciela Encalada Ochoa



LA CRIMINALIDAD INFORMÁTICA: PROPUESTA PARA LA TIPIFICACIÓN DE LOS DELITOS INFORMÁTICOS EN LA LEGISLACIÓN ECUATORIANA

INTRODUCCIÓN

En la actualidad las computadoras se utilizan no solo 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, procesamiento, almacenamiento y transmisión de datos.

Para nadie es desconocida la enorme influencia que ha alcanzado la informática en la vida diaria de las personas y organizaciones y la importancia que tiene su progreso para el desarrollo de un país. Las transacciones comerciales, la comunicación, los procesos industriales, las investigaciones, la seguridad, la sanidad, etc. son todos aspectos que dependen cada día más de un adecuado desarrollo de la tecnología informática. La informática está hoy presente en casi todos los campos de la vida moderna. Con mayor o menor rapidez todas las ramas del saber humano se rinden ante los progresos tecnológicos, y comienzan a utilizar los sistemas de información para ejecutar tareas que en otros tiempos realizaban manualmente.

El progreso cada día más importante y sostenido de los sistemas computacionales permite hoy procesar y poner a disposición de la sociedad una cantidad creciente de información de toda naturaleza, al alcance de millones de interesados y de usuarios. Las más diversas esferas del conocimiento humano, en lo científico, en lo técnico, en lo profesional y en lo personal están siendo incorporados a sistemas informáticos que en la práctica cotidiana, de hecho sin limitaciones, entrega con facilidad a quien lo desee un conjunto de datos que hasta hace unos años solo podían ubicarse luego de largas búsquedas y selecciones en que el hombre jugaba un papel determinante y las máquinas existentes tenían el rango de equipos auxiliares para imprimir los resultados. En la actualidad, en cambio, ese enorme caudal de conocimiento puede obtenerse, además en segundos o minutos, transmitirse incluso documentalmente y llegar al



receptor mediante sistemas sencillos de operar, confiables y capaces de responder casi toda la gama de interrogantes que se planteen a los archivos informáticos.

Puede sostenerse que hoy las perspectivas de la informática no tienen límites previsible y que aumentan en forma que aún puede impresionar. Este es el panorama de este nuevo fenómeno científico-tecnológico en las sociedades modernas. Por ello ha llegado a sostenerse que la informática es hoy una forma de poder social. Las facultades que el fenómeno pone a disposición de Gobiernos y de particulares, con rapidez y ahorro consiguiente de tiempo y energía, configuran un cuadro de realidades de aplicación y de posibilidades de juegos lícitos e ilícitos, en donde es necesario el derecho para regular los múltiples efectos de una situación, nueva y de tantas potencialidades en el medio social.

En la actualidad la informatización se ha implantado tanto en la organización y administración de empresas y administraciones públicas como en la investigación científica, en la producción industrial o en el estudio e incluso en el ocio, el uso de la informática es en ocasiones indispensable y hasta conveniente. Sin embargo, junto a las incuestionables ventajas que presenta comienzan a surgir algunas facetas negativas, como por ejemplo, lo que ya se conoce como “criminalidad informática”. El espectacular desarrollo de la tecnología informática ha abierto las puertas a nuevas posibilidades de delincuencia antes impensables. La manipulación fraudulenta de los ordenadores con ánimo de lucro, la destrucción de programas o datos y el acceso y la utilización indebida de la información que puede afectar la esfera de la privacidad, son algunos de los procedimientos relacionados con el procesamiento electrónico de datos mediante los cuales es posible obtener grandes beneficios económicos o causar importantes daños materiales o morales. Pero no solo la cuantía de los perjuicios así ocasionados es a menudo infinitamente superior a la que es usual en la delincuencia tradicional, sino que también son mucho más elevadas las posibilidades de que no lleguen a descubrirse. Se trata de una delincuencia de especialistas capaces muchas veces de borrar toda huella de los hechos.



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

La delincuencia informática se comete en el ciberespacio, y no se detiene en las fronteras nacionales convencionales. En principio, puede perpetrarse desde cualquier lugar y contra cualquier usuario de ordenador del mundo. Se necesita una acción eficaz, tanto en el ámbito nacional como internacional, para luchar contra la delincuencia informática. En los países, las reacciones frente a la delincuencia informática se centran en el derecho nacional, descuidando medidas alternativas de prevención, no hay respuestas globales, a pesar de los esfuerzos de las organizaciones internacionales y supranacionales, las diversas leyes nacionales de todo el mundo ponen de manifiesto considerables diferencias, especialmente en las disposiciones del derecho penal sobre piratería informática, protección del secreto comercial y contenidos ilícitos. También existen diferencias en cuanto al poder coercitivo de los organismos investigadores, la jurisdicción en materia penal, y con respecto a la responsabilidad de los proveedores de servicios intermediarios por una parte y los proveedores de contenidos por otra.

De lo anteriormente anotado podemos concluir preguntándonos, ¿Está nuestro país preparado para detectar y enfrentar a la delincuencia informática?, ¿Cuenta nuestro país con una legislación apropiada para enfrentar los delitos informáticos?.



CAPÍTULO I

ANTECEDENTES HISTÓRICOS

1. Enfoque internacional sobre la criminalidad informática.

El fenómeno informático es una realidad incuestionable e irreversible, está presente entre nosotros. La tecnología y la informática han alcanzado tal desarrollo que la mayor parte de nuestras actividades laborales están dirigidas o controladas por la computadora por lo que es de suma importancia considerar que dentro de este conjunto social se encuentra comprendida también la criminalidad, la cual se encuentra incluso mejor adaptada a estos cambios, es ahí en donde radica la importancia del estudio de estas nuevas formas de criminalidad en el ámbito de la informática.

Francisco Lancho Pedrera en su artículo *“La criminalidad informática en el Código Penal de 1995”* considera importante referirse a la denominación de “delito informático” en sentido estricto, puesto que, por delito se entiende las conductas tipificadas como tales en la ley penal; pero, el concepto de “delito informático” también se usa en referencia a las infracciones administrativas e incluso para los ilícitos civiles, por tanto esta variedad de supuestos hacen que sea más correcto usar el concepto “criminalidad informática” que el de “delito informático”, toda vez que dentro del concepto de criminalidad informática se pueden considerar correctamente supuestos tanto incluidos en el ilícito penal, así como también supuestos que no entran técnicamente dentro del concepto de delito pero que, sin embargo, son reprochables por el ordenamiento jurídico, aunque se puede aceptar el uso de “delito informático” por convencionalismo.

Rubdiazm escribió: “Por criminalidad se entiende el volumen de infracciones cometidas sobre la ley penal, por individuos o una colectividad en un momento determinado y en una zona determinada, la criminalidad es un término que tiene muchas variantes, por ejemplo: los americanos no manejan el término criminalidad sino delincuencia. La delincuencia es un producto también a priori y de observación. La criminalidad como delincuencia es una forma peculiar de



recabar todos los hechos criminales, los hechos punibles ocurridos y fijados por las vías estadísticas.”

El autor Gabriel Andrés Cámpoli en su obra *Delitos Informáticos en la Legislación mexicana*, manifiesta que es necesario definir cuáles son las características especiales que se presentan en la criminología y la victimología debido a las nuevas tecnologías informáticas y a partir de ellas fundar el estudio teórico que se las debe aplicar.

Manifiesta el autor que, en la sociedad se busca siempre el estudio del crimen y los criminales y que estos temas le corresponden a la criminología, manifiesta asimismo, que en la antigüedad se pensaba que el delito nacía de los defectos físicos y mentales y que era el producto de los rasgos hereditarios, pero que hoy esas teorías han sido dejadas de lado pues se ha llegado a la conclusión que el delito se aprende y no se hereda, por lo que considera que el verdadero desafío, es aplicar las reglas vigentes de la criminología actual a las conductas desarrolladas por los individuos que se podría considerar desviados dentro de esta subcultura informatizada.

El autor se plantea la pregunta: ¿Cuáles son entonces los caracteres que describen a los integrantes de este grupo? y se responde: “Como primera medida, podemos decir que son del estrato social de clase media en adelante, ya que los equipos necesarios para acceder a la conectividad necesaria no están al alcance de las clases más bajas o marginadas económicamente a pesar de que el acceso a Internet por ejemplo, se ha abaratado mucho desde la aparición de los conocidos *café internet* u otros sitios similares.

Por otro lado, los conocimientos necesarios para el acceso, si bien día a día se reducen, implican al menos saber leer y escribir, más algunos conocimientos mínimos de computación al menos para poder operar los programas de navegación web, correo electrónico y FTP (File Transfer Protocol), o protocolos de transferencia de archivos en español. Esto reduce notablemente los sujetos posibles como podemos ver. Los conocimientos técnicos necesarios se integran por un sublenguaje que debe ser conocido para la pertenencia al grupo. Estas son al menos las características generales de los individuos que integran la subcultura tecnologizada.”



Siguiendo con el criterio Gabriel Campoli, las armas que hoy en da se usan para el cometimiento del delito, son “las bombas de numeros y los programas de cracking”. La unica diferencia notoria entre los tiempos antiguos y hoy es la edad de los contrincantes en este “duelo informatico”, pues la mayora de los hackers son menores de edad que buscan abrirse paso y ganarse una reputacion ingresando y violando, un sistema protegido, y el problema esta en que al ser menor de edad, no se le puede aplicar pena alguna pues los sistemas penales en su mayora se encuentran impedidos de ello. Uno de los mayores problemas que enfrenta el legislador y el jurista en esta clase de delitos es la edad de los posibles infractores de las normas penales, a esto se suma el hecho de la internacionalidad de la red y la disparidad de los sistemas juridicos a aplicar.

Otra caracteristica en los delitos informaticos es la despersonalizacion, lo que permite evadir la accion de la justicia por la dificultad de determinar al autor material del delito. Otro aspecto de gran importancia es la responsabilidad civil a asumir los danos causados a terceros por efectos del delito, este es un problema por la inimputabilidad casi absoluta de los menores involucrados, la solucion resulta disimil segun el sistema juridico de que se trate, existiendo en algunos de ellos responsabilidad objetiva de los padres u tutores de los menores y en otros, la irresponsabilidad absoluta tanto de unos como de otros.

Hasta la fecha, no existe un sistema penal especifico que contemple la situacion de los menores ante los delitos informaticos, sumado al hecho que son pocas las legislaciones que cuentan con normativa especifica en la materia, por lo que considerando que en la situacion actual, debido a la falta de reglas orales y legales claras, mas la impunidad por el dificil rastreo de los sujetos activos y el anonimato producto de la despersonalizacion informatica hace de la red un sitio propicio para la realizacion de toda clase de delitos. Situacion que se incrementa por la competencia intelectual de los jovenes que para demostrar que son los mejores, intentan violar cuanto sistema de seguridad este a su alcance. Campoli plantea como posibles soluciones:

- “Una normativa penal adecuada y adaptada a las condiciones personales y sociales de las subculturas informatizadas.



- Una acción formativa sobre los agentes del poder punitivo del Estado para disminuir los efectos de la victimización secundaria.
- Aunado a esto, sistemas alternativos de solución de conflictos que cumplan la doble finalidad de reducir la victimización secundaria y además, evitar la estigmatización social del delincuente, a lo cual se pueden agregar sistemas compulsivos de reparación del daño que, no impliquen penas privativas de la libertad.
- Una fuerte acción educativa de parte de los Estados para reducir las posibles víctimas enseñándolos a conducirse en los sistemas informáticos con las mismas precauciones de seguridad que lo hacen en todas sus otras actividades.”

Es cierto y sabemos, que el crimen existe desde que existe el hombre; sin embargo, el progreso tecnológico hace más dificultoso su control y penalización. Esa dificultad radica, en las sofisticadas formas que adquiere el delito con ayuda de la tecnología. En este sentido, los sistemas informáticos logran potencializar las posibilidades de las distintas modalidades delictivas denominadas tradicionales, y aún dar sustento al origen de nuevas ilicitudes que solo se conciben con esta hermenéutica informática.

Mariana Gómez Pérez considera, que aunque no existe diferenciación clara en la manera de abordar estos problemas, en estrecha correspondencia con el grado de desarrollo de los países y del objetivo de la protección de su legislación, sí existe consenso en la necesidad del tratamiento, prevención y penalización de las conductas delictivas generadas por el uso de sistemas informáticos en la sociedad.

Manifiesta asimismo que una ley aprobada en el Japón en el año 1988, dispuso la imposición de multas de hasta cien mil yens a quien incumpla las regulaciones para la protección de datos o realice otros actos ilícitos relacionados con el procesamiento de datos; y que, ya desde 1979, Luxemburgo tenía también reguladas sanciones de multa y de privación de libertad hasta un año, para varios



supuestos típicos relacionados con la obtención y procesamiento ilegal de datos.

En igual sentido manifiesta Mariana Gómez Pérez, que se realizaron disposiciones jurídicas de mayor rango, aprobadas durante las décadas del 70 y del 80 en Francia, Noruega y Suecia y que en todas ellas se establecen sanciones de multa y de privación de libertad hasta un año, para los incumplidores de las disposiciones relacionadas con la obtención, almacenamiento y procesamiento de datos por medios informáticos.

Asimismo señala Gómez Pérez, que la Ley de Protección de Datos Personales Informatizados de 29 de abril de 1991, prevé en Portugal penas de multa y privación de libertad para los que utilicen datos ilegalmente, consigan acceso no autorizado a las bases de datos, realicen interconexiones ilegales y otras conductas; y, que en Chile se aprobó en abril de 1993 una Ley para regularlas.

A criterio de la autora antes citada los ejemplos quizá más relevantes de la legislación que sobre este tema existe en el mundo en los momentos actuales, por su nivel de actualización y detalle, los tengamos en el Acta de Comunicaciones Electrónicas Privadas, aprobada en los Estados Unidos en 1986, la española Ley Orgánica para la Regulación del Tratamiento Automatizado de Datos (LORTAD), y más recientemente el Código Penal Español, pero que también existen muchos más ejemplos de legislaciones que han previsto sanciones para el incumplimiento de las regulaciones relacionadas con el tratamiento de los datos que se procesan por medios automatizados, con diferentes grados de severidad y diferentes matices en la protección, ya que unas hacen más énfasis en la protección de los datos estratégicos y económicos y otras en la protección de la intimidad de las personas; pero que por encima de similitudes y diferencias, lo fundamental es la existencia de consenso en la necesidad de la protección.¹

¹ Revista de Derecho Informático Alfa-Redi. No. 10, mayo de 1999, "Criminalidad Informática: un fenómeno de fin de siglo". Mariana Gómez Pérez.



Un análisis de las legislaciones que se han promulgado en diversos países demuestra que las normas jurídicas que se han puesto en vigor están dirigidas a proteger la utilización abusiva de la información reunida y procesada mediante el uso de computadoras, e incluso en algunas de ellas se ha previsto formar órganos especializados que protejan los derechos de los ciudadanos amenazados por los ordenadores.

Desde hace algunos años la mayoría de los países europeos han hecho todo lo posible para incluir dentro de la ley, la conducta punible penalmente, como el acceso ilegal a sistemas de cómputo o el mantenimiento ilegal de tales accesos, la difusión de virus o la interceptación de mensajes informáticos.

En la mayoría de las naciones occidentales existen normas similares a los países europeos. Todos estos enfoques están inspirados por la misma preocupación de contar con comunicaciones electrónicas, transacciones e intercambios tan confiables y seguros como sea posible.

Delimitación del Fenómeno.

Según criterio de Claudio Magliona y Macarena López existe una confusión terminológica y conceptual en el campo de la informática, especialmente, dicen ellos, en lo que hace relación con sus aspectos criminales, por eso es necesario “desenmarañar el intrincado debate doctrinario acerca del real contenido de lo que se ha dado en llamar los delitos informáticos”², según estos autores, desde esta perspectiva, debe reinar la claridad más absoluta respecto de las materias, acciones y omisiones sobre las que debe recaer la seguridad social que aporta el aparato punitivo del Estado.

Antonio Enrique Pérez Luño, en su libro "Ensayos de Informática Jurídica" señala que se pueden distinguir seis aspectos peculiares de la criminalidad informática, éstas son:

² HUERTA MIRANDA, Marcelo y LÍBANO MANZUR Claudio, Los Delitos Informáticos, Editorial Jurídica Cono Sur. Obra citada por Dr. Santiago Acurio Del Pino, en su obra “Delitos Informáticos: Generalidades”



1. En el plano de la dogmática jurídico penal, la criminalidad informática puede suponer una nueva versión de delitos tradicionales o la aparición de nuevos delitos impensables antes del descubrimiento de las nuevas tecnologías; por ejemplo la posibilidad de que existan fraudes en los que el engaño se realiza sobre una máquina y no sobre una persona; de robos de servicios de ordenador, que es realizado en las cosas, o de hurtos de tiempo de ordenador sin que exista un ánimo de lucro, sino el mero propósito lúdico por quién realiza, y sin que se prive al titular de la cosa de su posesión.
2. Por tratarse de un sector sometido a constantes fluctuaciones e innovaciones tecnológicas, sus categorías son asimismo efímeras y cambiantes.
3. La criminalidad informática se caracteriza por las dificultades que entraña descubrirla, probarla y perseguirla. Es decir la dificultad de descubrir las conductas informáticas delictivas, además de la facilidad de penetrar en algunos sistemas informáticos y la personalidad especial de algunos de los delincuentes que pueden considerarse como un subtipo de la delincuencia de cuello blanco.
4. La propia precariedad y anacronismo del sistema jurídico penal refuerza la tendencia a no denunciar estos delitos, para evitar la alarma social o el desprestigio que de su conocimiento podría derivarse, lo que dificulta el conocimiento preciso del número de delitos perpetrados y la planificación de las adecuadas medidas legales sancionadoras o preventivas.
5. La insuficiencia de los instrumentos penales del presente para evitar y castigar las distintas formas de criminalidad informática, lo que supone un reto para la política criminal de criminalidad de los próximos años.
6. La dificultad de tipificar penalmente situaciones sometidas a un constante cambio tecnológico, la manifiesta insuficiencia de las sanciones en relación con la gravedad y el daño de los crímenes informáticos y la propia



inadecuación de los medios penales tradicionales para remediar esta situación, determinan que, el Derecho penal informático sea un ejemplo manifiesto de Derecho penal simbólico. Los delitos informáticos han marcado una nueva era en las relaciones humanas y han desbordado el Derecho Penal.

Miguel Angel Davara Rodríguez, manifiesta al igual que el profesor mexicano Julio Téllez Valdés, que no le parece adecuado hablar de delito informático ya que, como tal, no existe, si consideramos la necesidad de una tipificación en la legislación penal para que pueda existir un delito. “Ni el nuevo Código Penal español de 1995 introduce el delito informático, ni admite que exista como tal un delito informático, si bien admite la expresión por conveniencia, para referirse a determinadas acciones y omisiones dolosas o imprudentes, penadas por la Ley, en las que ha tenido algún tipo de relación en su comisión, directa o indirecta, un bien o servicio informático”.³

Dar un concepto sobre delitos informáticos no es una labor fácil y esto en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de “delitos” en el sentido de acciones tipificadas o contempladas en textos jurídico-penales, se requiere que la expresión “delitos informáticos” esté consignada en los códigos penales, lo cual en nuestro país, al igual que en muchos otros, no ha sido objeto de tipificación aún; sin embargo, muchos especialistas en derecho informático emplean esta alusión a los efectos de una mejor conceptualización.

El autor mexicano Julio Téllez Valdés señala que los delitos informáticos son “*actitudes ilícitas en que se tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin (concepto típico)*”. Por su parte el tratadista penal italiano Carlos Sarzana, sostiene que los delitos informáticos son “*cualquier comportamiento criminal en que la computadora está involucrada como material, objeto o mero símbolo*”.

³ DAVARA RODRÍGUEZ, Miguel Angel, Análisis de la Ley de Fraude Informático, Revista de Derecho de UNAM. 1990.



Según Téllez Valdés, este tipo de acciones presentan las siguientes características principales:

- “Son conductas criminales de cuello blanco, en tanto que sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden llegar a cometerlas.
- Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se halla trabajando.
- Son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.
- Provocan serias pérdidas económicas, ya que casi siempre producen “beneficios” de más de cinco cifras a aquellos que las realizan.
- Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.
- Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.
- Son sofisticados y relativamente frecuentes en el ámbito militar.
- Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.
- En su mayoría son imprudenciales y no necesariamente se cometen con intención.
- Ofrecen facilidades para su comisión a los menores de edad.
- Tienden a proliferar cada vez más, por lo que requieren una urgente regulación.
- Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley”.

Asimismo, este autor clasifica a estos delitos, de acuerdo a dos criterios:

- a) Como instrumento o medio
- b) Como fin u objetivo.



a) Como instrumento o medio.

En esta categoría se encuentran las conductas criminales que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito, por ejemplo: Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etc.)

- Variación de los activos y pasivos en la situación contable de las empresas.
- Planeamiento y simulación de delitos convencionales (robo, homicidio, fraude, etc.)
- Lectura, sustracción o copiado de información confidencial.
- Modificación de datos tanto en la entrada como en la salida.
- Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas.
- Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa.
- Uso no autorizado de programas de cómputo.
- Introducción de instrucciones que provocan “interrupciones” en la lógica interna de los programas.
- Alteración en el funcionamiento de los sistemas, a través de los virus informáticos.
- Obtención de información residual impresa en papel luego de la ejecución de trabajos.
- Acceso a áreas informatizadas en forma no autorizada.
- Intervención en las líneas de comunicación de datos o teleproceso.

b) Como fin u objetivo

En esta categoría, se enmarcan las conductas criminales que van dirigidas contra las computadoras, accesorios o programas como entidad física, como por ejemplo:

- Programación de instrucciones que producen un bloqueo total al sistema.



- Destrucción de programas por cualquier método.
- Daño a la memoria.
- atentado físico contra la máquina o sus accesorios.
- Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.
- Secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje (pagos de rescate, etc.)

Por otra parte, existen diversos tipos de delito que pueden ser cometidos y que se encuentran ligados directamente a acciones efectuadas contra los propios sistemas como son:

Acceso no autorizado: Uso ilegítimo de passwords y la entrada de un sistema informático sin la autorización del propietario.

Destrucción de datos: Los daños causados en la red mediante la introducción de virus, bombas lógicas, etc.

Infracción al copyright de bases de datos: Uso no autorizado de información almacenada en una base datos.

Interceptación de e-mail: Lectura de un mensaje electrónico ajeno.

Estafas electrónicas: A través de compras realizadas haciendo uso de la red.

Transferencias de fondos: Engaños en la realización de este tipo de transacciones.

Por otro lado, la red internet permite dar soporte para la comisión de otro tipo de delitos:

Espionaje: Acceso no autorizado a sistemas informáticos gubernamentales y de grandes empresas e interceptación de correos electrónicos.

Terrorismo: Mensajes anónimos aprovechados por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional.

Narcotráfico: Transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas.



Otros delitos: Las mismas ventajas que encuentran en la internet los narcotraficantes pueden ser aprovechadas para la planificación de otros delitos como el tráfico de armas, proselitismo de sectas, propaganda de grupos extremistas y cualquier otro delito que pueda ser trasladado de la vida real al ciberespacio o al revés.

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

Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que lo que los diferencia entre sí es la naturaleza de los delitos cometidos. De esta forma, la persona que “ingresa” en un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes⁴.

Al respecto, según un estudio publicado en el Manual de las Naciones Unidas en la prevención y control de delitos informáticos (Nros. 43 y 44), el 90% de los delitos realizados mediante la computadora fueron ejecutados por empleados de la propia empresa afectada. Asimismo, otro reciente estudio realizado en América del Norte y Europa indicó que el 73% de las intrusiones cometidas eran atribuibles a fuentes interiores y solo el 23% a la actividad delictiva externa.

El nivel típico de aptitudes del delincuente informático es tema de controversia ya que para algunos el nivel de aptitudes no es indicador de delincuencia informática en tanto que otros aducen que los posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un

⁴ Delitos informáticos. <http://www.fing.uach.mx//MatDidactivo/Legislacion/deliinfo.htm>



reto tecnológico, características que pudieran encontrarse en un empleado del sector de procesamiento de datos”.

Sin embargo, teniendo en cuenta las características ya mencionadas de las personas que cometen los “delitos informáticos”, los estudiosos en la materia los han catalogado como “delitos de cuello blanco” término introducido por primera vez por el criminólogo norteamericano Edwin Sutherland en el año de 1943. Este criminólogo estadounidense dice que tanto la definición de los “delitos informáticos” como la de los “delitos de cuello blanco” no están de acuerdo al interés protegido, como sucede en los delitos convencionales sino de acuerdo al sujeto activo que los comete. Entre las características en común que poseen ambos delitos tenemos que: el sujeto activo del delito es una persona de cierto estatus socioeconómico, su comisión no puede explicarse por pobreza ni por mala habitación, ni por carencia de recreación, no por baja educación, no por poca inteligencia, ni por inestabilidad emocional.

Es difícil elaborar estadísticas sobre ambos tipos de delitos. Sin embargo, la cifra es muy alta; no es fácil descubrirlo y sancionarlo, en razón del poder económico de quienes lo cometen, pero los daños económicos son altísimos; existe una gran indiferencia de la opinión pública sobre los daños ocasionados a la sociedad; la sociedad no considera delincuentes a los sujetos que cometen este tipo de delitos, no los desprecia, ni los desvaloriza, por el contrario, el autor o autores de este tipo de delitos se consideran a sí mismos “respetables” otra coincidencia que tienen estos tipos de delitos es que, generalmente, son objeto de medidas o sanciones de carácter administrativo y no privativos de la libertad.

Este nivel de criminalidad se puede explicar por la dificultad de reprimirla en forma internacional, ya que los usuarios están esparcidos por todo el mundo y, en consecuencia, existe una posibilidad muy grande de que el agresor y la víctima estén sujetos a leyes nacionales diferentes. Además, si bien los acuerdos de cooperación internacional y los tratados de extradición bilaterales intentan remediar algunas de las dificultades ocasionadas por los delitos informáticos, sus posibilidades son limitadas.

En lo que se refiere a delitos informáticos, Olivier Hance en su libro “Leyes y Negocios en Internet”, considera tres categorías de comportamiento que pueden



afectar negativamente a los usuarios de los sistemas informáticos. Las mismas son las siguientes:

Acceso no autorizado: Es el primer paso de cualquier delito. Se refiere a un usuario que, sin autorización, se conecta deliberadamente a una red, un servidor o un archivo (por ejemplo, una casilla de correo electrónico), o hace la conexión por accidente pero decide voluntariamente mantenerse conectado.

Actos dañinos o circulación de material dañino: Una vez que se conecta a un servidor, el infractor puede robar archivos, copiarlos o hacer circular información negativa, como virus o gusanos. Tal comportamiento casi siempre es clasificado como piratería (apropiación, descarga y uso de la información sin conocimiento del propietario) o como sabotaje (alteración, modificación o destrucción de datos o de software, uno de cuyos efectos es paralizar la actividad del sistema o del servidor en Internet).

Interceptación no autorizada: En este caso, el hacker detecta pulsos electrónicos transmitidos por una red o una computadora y obtiene información no dirigida a él.

Las leyes estadounidense y canadiense, lo mismo que los sistemas legales de la mayoría de los países europeos, han tipificado y penalizado estos tres tipos de comportamiento ilícito cometidos a través de las computadoras.

Por su parte, el Manual de las Naciones Unidas para la Prevención y Control de Delitos Informáticos señala que cuando el problema se eleva a la escena internacional, se magnifican los inconvenientes y las insuficiencias, por cuanto los delitos informáticos constituyen una nueva forma de crimen transnacional y su combate requiere de una eficaz cooperación internacional concertada. Asimismo, la ONU resume de la siguiente manera a los problemas que rodean a la cooperación internacional en el área de los delitos informáticos:

- Falta de acuerdos globales acerca de qué tipo de conductas deben constituir delitos informáticos.
- Ausencia de acuerdos globales en la definición legal de dichas conductas delictivas.



- Falta de especialización de las policías, fiscales y otros funcionarios judiciales en el campo de los delitos informáticos.
- No armonización entre las diferentes leyes procesales nacionales acerca de la investigación de los delitos informáticos.
- Carácter transnacional de muchos delitos cometidos mediante el uso de computadoras.
- Ausencia de tratados de extradición, de acuerdos de ayuda mutuos y de mecanismos sincronizados que permitan la puesta en vigor de la cooperación internacional.

En síntesis, es destacable que la delincuencia informática se apoya en el delito instrumentado por el uso de la computadora a través de redes telemáticas y la interconexión de la computadora, aunque no es el único medio. La criminalidad informática constituye un reto considerable tanto para los sectores afectados de la infraestructura crítica de un país, como para los legisladores, las autoridades policiales encargadas de las investigaciones y los funcionarios judiciales.

En nuestro país, en materia penal no hemos tenido avances a diferencia de otras legislaciones por lo que se hace necesario que para enfrentar a la llamada criminalidad informática, los tipos penales tradicionales sean actualizados puesto que el avance tecnológico es acelerado y el uso de la computadora es un medio para la comisión de delitos que en muchas ocasiones quedan impunes por desconocimiento o por falta de las herramientas adecuadas para investigar y perseguir esta clase de infracciones.

Las víctimas de los delitos informáticos.

Es necesario definir cuáles serían los bienes jurídicos que se pueden afectar mediante el uso indebido de equipos informáticos.

A continuación citamos al menos tres: Patrimonio, Intimidad e Integridad física y/o lógica de los equipos de cómputo y/o páginas Web cuando ello no implique los dos anteriores.



Violaciones al patrimonio:

Las posibilidades de acciones ilícitas que pueden llevarse a cabo en menosprecio del patrimonio ajeno por medio de equipos informáticos, no son más que una modalidad de los tipos penales ya tipificados como el robo, el hurto, el fraude u otros similares. Por ejemplo si mediante una computadora, página web o correo electrónico se induce al sujeto pasivo a entregar por medio de ardid o engaño una parte de su patrimonio, sin importar el medio utilizado, sigue siendo o cumpliendo con los elementos del fraude, por lo que no es necesario crear otro tipo penal puesto que lo único que haría es confundir y superponer los delitos existentes. En el caso de la utilización de equipos informáticos como medio para la comisión del delito, se produce una indefensión debido a la diferencia de conocimientos entre víctima y victimario y al anonimato que pueden ofrecer los medios telemáticos, por ello, según Cápoli, en los casos en que se cometan delitos contra el patrimonio aprovechándose de la inexperiencia de la víctima o del anonimato a través de las nuevas tecnologías, se puede decir con certeza que se trata de un agravante por el medio, más no un nuevo tipo de delito.

Violaciones a la intimidad:

En este punto, es necesario definir dos conceptos que suelen confundirse, estos son: intimidad y privacidad.

Cápoli manifiesta que según parte de la doctrina, ambos conceptos son equivalentes, pero bajo un análisis un poco más detallado, surgen ciertas diferencias.

En el ámbito civil, existe la propiedad privada (privativa de su titular), mas no la propiedad íntima, lo cual deja ver que los dos conceptos no tienen el mismo significado, por tanto se puede definir a la propiedad privada como la potestad que tiene el titular sobre el uso exclusivo de un bien determinado, la cual puede ceder únicamente ante orden fundada del Estado en beneficio público (expropiación) pero que en sí, para su ejercicio, es conocida y reconocida por un grupo de personas sobre las cuales se ejerce esa exclusividad, con el Estado como garante del goce del derecho. Cápoli por analogía define a la **Información privada** en los siguientes términos: *“Es aquella sobre la cual el titular posee un derecho exclusivo de uso o conocimiento pero que en mayor o*



menor medida es conocida por un grupo de personas a su alrededor y por el Estado respondiendo a fines de garantía de los derechos del ciudadano". En este grupo tenemos por ejemplo los datos filiatorios, los económicos, los políticos y muchos otros.

En lo referente a qué se representa con información íntima, hace la siguiente reflexión: "la esfera de la intimidad se encuentra ligada expresamente según su raíz etimológica a lo que tiene que ver con el fuero interno de la persona, lo cual lo separa expresamente de la información privada.

El autor antes citado, define a la **Información íntima**, en los siguientes términos: "*Es aquella sobre la cual el titular tiene la absoluta exclusividad de su conocimiento y divulgación, que se encuentra ligada a sus procesos internos de selección y no puede ser conocida ni aún en circunstancias especiales por persona alguna ni por el Estado*". Dentro de este grupo en cambio tenemos la orientación sexual, las decisiones morales, los valores internos, etc. Ahora la pregunta que se hace Cámpoli es, ¿sobre cuál de las dos debe existir la protección penal? Sobre la información íntima, no existe discusión alguna, puesto que ésta debe ser protegida desde todos los puntos de vista posibles ya que está compuesta o integrada por lo que en doctrina se llaman datos sensibles y cualquier conocimiento o divulgación no autorizada produce necesariamente un daño, al menos moral en el sujeto pasivo. En cambio sobre la información privada, el asunto es más discutido, puesto que además del titular, existen otras personas con derecho a su conocimiento y divulgación, deberá entonces tomarse como parámetro, la lesión al bien jurídico. Por tanto, "se constituirá en delito aquella acción para la cual el sujeto activo no tenga derecho expreso y en este caso en particular, constituirá acción típica cualquier conocimiento o divulgación no autorizada de información a terceros.

Es claro el hecho que, como el conocimiento de información de un tercero resulta imposible de probar, lo que debe pensarse es cualquier acción que implique que el sujeto activo esté en posesión de información del sujeto pasivo a la cual no



tenía derecho, sea esta manifestación a través de la divulgación o de cualquier otro medio.”⁵

Violaciones a la integridad física y/o lógica de los equipos de cómputo y/o páginas web cuando ello no implique los dos anteriores:

La integridad física de los equipos podría verse protegida por el delito de daños, en razón de que se produce un deterioro o detrimento de un bien, pero se debe también reconocer que no siempre estos menoscabos en la operabilidad de los equipos se cometen por los tradicionales medios de empleo de la fuerza que caracterizan a este tipo delictual.

De todo lo anotado, se concluye que en este tipo de delitos, según su modalidad, se pueden apreciar dos tipos de víctimas:

Víctimas conscientes de su estado.

Víctimas no conscientes de su estado.

Sujeto activo:

En este tipo de delitos, el sujeto activo debe tener conocimientos técnicos de informática, es decir, en cierto modo, una persona con nivel de instrucción elevado, para poder manipular información o sistemas de computación.

Sujeto pasivo:

En el caso del delito informático pueden ser: individuos, instituciones de crédito, gobiernos, en fin entidades que usan sistemas automatizados de información.

⁵ CÁMPOLI, Gabriel. Delitos informáticos en la legislación mexicana. Página 65.



TIPOS DE DELITOS INFORMÁTICOS RECONOCIDOS POR NACIONES UNIDAS

Fraudes cometidos mediante manipulación de computadoras

Manipulación de los datos de entrada.

Este tipo de fraude informático, conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.

Manipulación de programas.

Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

Manipulación de los datos de salida.

Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían a base de tarjetas bancarias robadas; sin embargo, en la actualidad se usan ampliamente equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.



Manipulación informática aprovechando repeticiones automáticas de los procesos de cómputo.

Es una técnica especializada que se denomina “técnica del salchichón” en la que “rodajas muy finas” apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.

Falsificaciones informáticas.

COMO OBJETO: Cuando se alteran datos de los documentos almacenados en forma computarizada.

COMO INSTRUMENTOS: Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color a base de rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer copias de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.

Daños o modificaciones de programas de datos computarizados.

Sabotaje informático.

Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son:

VIRUS. Es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya.

GUSANOS. Se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los



datos, pero es diferente del virus porque no puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.

BOMBA LÓGICA O CRONOLÓGICA. Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba.

ACCESO NO AUTORIZADO A SERVICIOS Y SISTEMAS INFORMÁTICOS. Por motivos diversos; desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.

PIRATAS INFORMÁTICOS O HACKERS. El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.



REPRUDUCCIÓN NO AUTORIZADA DE PROGRAMAS INFORMÁTICOS DE PROTECCIÓN LEGAL. Esta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas. Al respecto, consideramos, que la reproducción no autorizada de programas informáticos no es un delito informático, debido a que el bien jurídico a tutelar es la propiedad intelectual.⁶

LEGISLACIÓN INTERNACIONAL SOBRE DELITOS INFORMÁTICOS

Según el Proyecto de criminalística informática, realizado por Carabineros de Chile, algunos casos de abusos relacionados con la informática deben ser combatidos con medidas jurídico-penales. Pero, para aprehender ciertos comportamientos merecedores de pena con los medios del Derecho penal tradicional, existen, al menos en parte, ciertas dificultades que se deben en buena medida, a la prohibición jurídico-penal de analogía y en ocasiones, son insuperables por la vía jurisprudencial. Surge entonces la necesidad de adoptar medidas legislativas.

Pocos son los países que disponen de una legislación adecuada para enfrentarse con el problema sobre el particular, sin embargo con objeto de que se tomen en cuenta las medidas adoptadas por ciertos países, se presenta los siguientes casos:

Alemania:

En Alemania, para hacer frente a la delincuencia relacionada con la informática y con sus efectos a partir del 1 de agosto de 1986, se adoptó la

⁶ REALIDAD ALTERNATIVA. <http://realidadalternatia.wordpress.com/2008/01/25/los-tipos-de-delitos-informaticos-reconocidos-por-nacines-unidas/>



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

- Espionaje de datos (202 a)
- Estafa informática (263 a)
- Falsificación de datos probatorios(269) junto a modificaciones complementarias del resto de falsedades documentales como el engaño en el tráfico jurídico mediante la elaboración de datos, falsedad ideológica, uso de documentos falsos(270, 271, 273)
- Alteración de datos (303 a) es ilícito cancelar, inutilizar o alterar datos inclusive la tentativa es punible.
- Sabotaje informático (303 b).destrucción de elaboración de datos de especial significado por medio de destrucción, deterioro, inutilización, eliminación o alteración de un sistema de datos. También es punible la tentativa.
- Utilización abusiva de cheques o tarjetas de crédito (266b)

Por lo que se refiere a la estafa informática, la formulación de un nuevo tipo penal tuvo como dificultad principal el hallar un equivalente análogo al triple requisito de acción engañosa, causación del error y disposición patrimonial, en el engaño del computador, así como en garantizar las posibilidades de control de la nueva expresión legal, quedando en la redacción que el perjuicio patrimonial que se comete consiste en influir en el resultado de una elaboración de datos por medio de una realización incorrecta del programa, a través de la utilización de datos incorrectos o incompletos, mediante la utilización no autorizada de datos, o a través de una intervención ilícita.

Sobre el particular, cabe mencionar que esta solución en forma parcialmente abreviada fue adoptada en los Países Escandinavos y en Austria.

En opinión de estudiosos de la materia, el legislador alemán ha introducido un número relativamente alto de nuevos preceptos penales, pero no ha llegado tan lejos como los Estados Unidos.



En el caso de Alemania, se ha señalado que a la hora de introducir nuevos preceptos penales para la represión de la llamada criminalidad informática el gobierno tuvo que reflexionar acerca de dónde radicaban las verdaderas dificultades para la aplicación del Derecho penal tradicional a comportamientos dañosos en los que desempeña un papel esencial la introducción del proceso electrónico de datos, así como acerca de qué bienes jurídicos merecedores de protección penal resultaban así lesionados.

Fue entonces cuando se comprobó que, por una parte, en la medida en que las instalaciones de tratamiento electrónico de datos son utilizadas para la comisión de hechos delictivos, en especial en el ámbito económico, pueden conferir a éstos una nueva dimensión, pero que en realidad tan sólo constituyen un nuevo modus operandi, que no ofrece problemas para la aplicación de determinados tipos.

Sin embargo, la protección fragmentaria de determinados bienes jurídicos ha puesto de relieve que éstos no pueden ser protegidos suficientemente por el Derecho vigente contra nuevas formas de agresión que pasan por la utilización abusiva de instalaciones informáticas.

En otro orden, las diversas formas de aparición de la criminalidad informática propician además, la aparición de nuevas lesiones de bienes jurídicos merecedoras de pena, en especial en la medida en que el objeto de la acción puedan ser datos almacenados o transmitidos o se trate del daño a sistemas informáticos. El tipo de daños protege cosas corporales contra menoscabos de su sustancia o función de alteraciones de su forma de aparición.

Austria:

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

Esta ley contempla los siguientes delitos:

- Destrucción de datos (126). En este artículo se regulan no sólo los datos personales sino también los no personales y los programas.



- Estafa informática (148). En este artículo se sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el curso del procesamiento de datos. Además contempla sanciones para quienes cometen este hecho utilizando su profesión.

Francia:

Ley número 88-19 de 5 de enero de 1988 sobre el fraude informático.

- Acceso fraudulento a un sistema de elaboración de datos(462-2).- En este artículo se sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la sanción correspondiente si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema.
- Sabotaje informático (462-3).- En este artículo se sanciona a quien impida o falsee el funcionamiento de un sistema de tratamiento automático de datos.
- Destrucción de datos (462-4).- En este artículo se sanciona a quien intencionadamente y con menosprecio de los derechos de los demás introduzca datos en un sistema de tratamiento automático de datos o suprima o modifique los datos que éste contiene o los modos de tratamiento o de transmisión.
- Falsificación de documentos informatizados (462-5).- En este artículo se sanciona a quien de cualquier modo falsifique documentos informatizados con intención de causar un perjuicio a otro.

Uso de documentos informatizados falsos (462-6) En este artículo se sanciona a quien conscientemente haga uso de documentos falsos haciendo referencia al artículo 462-5.



Gran Bretaña:

Debido a un caso de hacking en 1991, comenzó a regir en este país la Computer Misuse Act (Ley de Abusos Informáticos). Mediante esta ley el intento, exitoso o no, de alterar datos informáticos es penado con hasta cinco años de prisión o multas.

Esta ley tiene un apartado que especifica la modificación de datos sin autorización. Los virus están incluidos en esa categoría.

El liberar un virus tiene penas desde un mes a cinco años, dependiendo del daño que causen.

Holanda:

El 1º. de marzo de 1993 entró en vigencia la Ley de Delitos Informáticos, en la cual se penaliza el hacking, el preacking (utilización de servicios de telecomunicaciones evitando el pago total o parcial de dicho servicio), la ingeniería social (arte de convencer a la gente de entregar información que en circunstancias normales no entregaría), y la distribución de virus.

La distribución de virus está penada de distinta forma si se escaparon por error o si fueron liberados para causar daño.

España:

Ley Orgánica N°. 10 de 1995, de fecha 23 de Noviembre de 1995.
Dentro de la legislación española, podemos distinguir la aplicación de las siguientes medidas en el ámbito penal.

- **Ataques que se producen contra el derecho a la intimidad.** Artículos del 197 al 201 del Código Penal)
- **Infracciones a la Propiedad Intelectual a través de la protección de los derechos de autor.**



- Artículos 270 y otros del Código Penal
- **Falsedades**, Artículos 386 y ss. del Código Penal
- **Sabotajes informáticos.**
- Delito de daños mediante la destrucción o alteración de datos, programas o documentos electrónicos contenidos en redes o sistemas informáticos. (Artículo 263 y otros del Código Penal)
- **Fraudes informáticos.**
- Delitos de estafa a través de la manipulación de datos o programas para la obtención de un lucro ilícito.
- (Artículos 248 y ss. del Código Penal)
- **Amenazas.**
- Realizadas por cualquier medio de comunicación. (Artículos 169 y ss. del Código Penal)
- **Calumnias e injurias.**
- Cuando se propaguen por cualquier medio de eficacia semejante a la imprenta o la radiodifusión. (Artículos 205 y ss. del Código Penal)
- **Pornografía infantil.**
- Entre los delitos relativos a la prostitución al utilizar a menores o incapaces con fines exhibicionistas o pornográficos.
 - La inducción, promoción, favorecimiento o facilitamiento de la prostitución de una persona menor de edad o incapaz. (art. 187)
 - La producción, venta, distribución, exhibición, por cualquier medio, de material pornográfico en cuya elaboración hayan sido utilizados menores de edad o incapaces, aunque el material tuviere su origen en el extranjero o fuere desconocido. (art. 189)
 - El facilitamiento de las conductas anteriores (*El que facilitare la producción, venta, distribución, exhibición.*). (art. 189)
 - La posesión de dicho material para la realización de dichas conductas. (art. 189)



Estados Unidos de Norteamérica:

La adopción en los Estados Unidos en 1994 del Acta Federal de Abuso Computacional (18 U.S.C. Sec.1030) que modificó al Acta de Fraude y Abuso Computacional de 1986.

Con la finalidad de eliminar los argumentos hipertécnicos acerca de qué es y qué no es un virus, un gusano, un caballo de Troya, etc. y en qué difieren de los virus, la nueva acta proscribire la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, al sistema informático, a las redes, información, datos o programas.(18 U.S.C.: Sec. 1030 (a) (5) (A). La nueva ley es un adelanto porque está directamente en contra de los actos de transmisión de virus.

El Acta de 1994 diferencia el tratamiento a aquellos que de manera temeraria lanzan ataques de virus de aquellos que lo realizan con la intención de hacer estragos. El acta define dos niveles para el tratamiento de quienes crean virus estableciendo para aquellos que intencionalmente causan un daño por la transmisión de un virus, el castigo de hasta 10 años en prisión federal más una multa y para aquellos que lo transmiten sólo de manera imprudencial la sanción fluctúa entre una multa y un año en prisión.

El Acta de 1994 aclara que el creador de un virus no puede aducir el hecho que no conocía que con su actuar iba a causar daño a alguien o que él solo quería enviar un mensaje.

En opinión de los legisladores estadounidenses, la nueva ley constituye un acercamiento más responsable al creciente problema de los virus informáticos, específicamente no definiendo a los virus sino describiendo el acto para dar cabida en un futuro, a la nueva era de ataques tecnológicos a los sistemas informáticos en cualquier forma en que se realicen. Diferenciando los niveles de delitos, la nueva ley da lugar a que se contemple qué se debe entender como acto delictivo.



En el Estado de California, en 1992 se adoptó la Ley de Privacidad en la que se contemplan los delitos informáticos pero en menor grado que los delitos relacionados con la intimidad que constituyen el objetivo principal de esta Ley.

Es importante destacar las enmiendas realizadas a la Sección 502 del Código Penal relativas a los delitos informáticos en la que, entre otros, se amplían los sujetos susceptibles de verse afectados por estos delitos, la creación de sanciones pecuniarias de \$10, 000 por cada persona afectada y hasta \$50,000 el acceso imprudencial a una base de datos.

El objetivo de los legisladores al realizar estas enmiendas, era el de aumentar la protección a los individuos, negocios y agencias gubernamentales de la interferencia, daño y acceso no autorizado a las bases de datos y sistemas computarizados creados legalmente. Asimismo, los legisladores consideraron que la proliferación de la tecnología de computadoras ha traído consigo la proliferación de delitos informáticos y otras formas no autorizadas de acceso a las computadoras, a los sistemas y las bases de datos y que la protección legal de todos sus tipos y formas, es vital para la protección de la intimidad de los individuos así como para el bienestar de las instituciones financieras, de negocios, agencias gubernamentales y otras relacionadas con el estado de California que legalmente utilizan esas computadoras, sistemas y bases de datos.

Es importante mencionar que en uno de los apartados de esta ley, se contempla la regulación de los virus (computer contaminant), conceptualizándolos aunque no los limita a un grupo de instrucciones informáticas comúnmente llamados virus o gusanos sino que contempla a otras instrucciones designadas a contaminar otros grupos de programas o bases de datos, modificar, destruir, copiar o transmitir datos o alterar la operación normal de las computadoras, los sistemas o las redes informáticas.

Chile:

Chile fue el primer país latinoamericano en sancionar una Ley contra delitos informáticos, la cual entró en vigencia el 7 de junio de 1993.



Según esta ley, la destrucción o inutilización de los datos contenidos dentro de una computadora se castigaba con penas desde un año y medio a cinco años de prisión. Dentro de esas consideraciones estaba también los virus.

En esta Ley se contempla el tipo legal vigente de una conducta maliciosa tendiente a la destrucción o inutilización de un sistema de tratamiento de información o de sus componentes o que dicha conducta impida, obstaculice o modifique su funcionamiento. En esta ley se encuentra también tipificada la conducta maliciosa que altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información.⁷

Perú:

Ley N° 27.309, promulgada el 15 de julio de 2000 y publicada el 17 de julio de 2000, incorporó los delitos informáticos al Código Penal.

Artículo 207^o-A. 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 cincuenta y dos 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.

Artículo 207^o-B. 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.

⁷ Legislación sobre delitos informáticos. <http://www.elrinconcito.com/articulos/DelitosInf/legisdelinf.htm>



Artículo 207^o-C. En los casos de los artículos 207^o-A y 207^o- 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.⁸

Bolivia:

En Bolivia, en el año de 1989, se consideró el análisis y tratamiento sobre legislación informática concerniente a contratación de bienes y servicios informáticos, flujo de información computarizada, modernización del aparato productivo nacional mediante investigación científico-tecnológica en el país y la incorporación de nuevos delitos emergentes del uso y abuso de la informática.

Este conjunto de acciones tendientes a desarrollar de manera integral la informática, se tradujo en el trabajo de especialistas y sectores involucrados, representantes en el campo industrial, profesionales abogados y especialistas informáticos, la elaboración del Proyecto de Ley Nacional de Informática, concluido en febrero de 1991.

UNION EUROPEA:

La Comunidad Europea, en los cursos de acción desarrollados para la prevención y control de delitos informáticos ha generado una importante gama de políticas, en el ámbito judicial, político y policial, dando como principio el que Europa se ha caracterizado por pasar de una sociedad industrial a la sociedad de la información, esto ha dado grandes progresos en todos los aspectos de la vida humana: el trabajo, la educación y el ocio, el gobierno, la industria y el comercio. Las nuevas tecnologías de información y comunicación están teniendo un impacto

⁸ DelitosInformaticos.com -- PROYECTO DE CRIMINALISTICA INFORMATICA
<http://www.delitosinformaticos.com/tesis.htm> (25 de 72) [20/08/2001 17:12:34]



revolucionario y fundamental en sus economías y sociedades. Consideran que el éxito de la sociedad de la información es importante para el crecimiento, la competitividad y las posibilidades de empleo de Europa, y tiene repercusiones económicas, sociales y jurídicas de gran envergadura.

Para el logro de estos objetivos de crecimiento, competitividad y posibilitar la creación de nuevos empleos, se han volcado en las siguientes actividades legislativas. En diciembre de 1999, la Comisión puso en marcha la iniciativa eEuropa, con el fin de garantizar que Europa se beneficie de las tecnologías digitales, y que la nueva sociedad de la información sea socialmente inclusiva. En junio de 2000, el Consejo Europeo de Feira, adoptó el Plan de acción eEuropa, y solicitó que se aplicara antes de finales de 2002. El plan de acción resalta la importancia de la seguridad de las redes y de la lucha contra la delincuencia informática, en atención a que las infraestructuras de información y comunicación se han convertido en una parte crucial de las economías de los países miembros de la Comunidad.

La Unión Europea ha tomado ya diversas medidas para luchar contra los contenidos ilícitos y nocivos en Internet, para proteger la propiedad intelectual y los datos personales, para promover el comercio electrónico y el uso de la firma electrónica y para aumentar la seguridad de las transacciones. En abril de 1998, la Comisión presentó al Consejo los resultados de un estudio sobre la delincuencia informática, llamado estudio "COMCRIME". En octubre de 1999, la cumbre de Tampere del Consejo Europeo concluyó que la labor para acordar definiciones y sanciones comunes debe incluir la delincuencia de alta tecnología. El Parlamento Europeo también realizó un llamamiento para que se establezcan definiciones comúnmente aceptables de los delitos informáticos y se aproximen las legislaciones, en especial en el ámbito del derecho penal. El Consejo de la Unión Europea ha adoptado una posición común respecto a las negociaciones del Convenio del Consejo de Europa sobre delincuencia en el ciberespacio y ha adoptado varios elementos iniciales como parte de la estrategia de la Unión contra la delincuencia de alta tecnología.



La delincuencia informática se comete en el ciberespacio, y no se detiene en las fronteras nacionales convencionales. En principio, puede perpetrarse desde cualquier lugar y contra cualquier usuario de ordenador del mundo. Se necesita una acción eficaz, tanto en el ámbito nacional como internacional, para luchar contra la delincuencia informática.

A escala nacional, en muchos casos no hay respuestas globales y con vocación internacional frente a los nuevos retos de la seguridad de la red y la delincuencia informática. En la mayoría de los países, las reacciones frente a la delincuencia informática se centran en el derecho nacional (especialmente el derecho penal), descuidando medidas alternativas de prevención.

RESPONSABILIDADES ENTREGADAS A LOS ORGANISMOS POLICIALES EXTRANJEROS

INTERPOL:

La INTERPOL Internacional, a través de los últimos años se ha dedicado a la investigación de delitos y fraudes computacionales, ante lo cual participa en la creación de un organismo Internacional de cooperación con otros miembros de INTERPOL a través de Europa, África, Asia y América, dando origen a Crímenes de Tecnologías de la información (ITC: Information Technology Crime); abocadas a la investigación y persecución de los delitos de este tipo en todas las áreas del planeta que requieran cooperación.

Para ello, se ha editado el Manual del Crimen Computacional 2001.

<http://www.interpol.com>

FBI:

INTERNET FRAUD COMPLATION CENTER (FBI/NW3C)

El Servicio de Investigaciones de FBI, ante la creciente demanda de Instituciones, Empresas y Personas, afectadas por la acción de delitos



informáticos se une en la implementación con el “Centro de Delitos de Cuello Blanco” (National White Collar Crime Center (NW3C)), a fin de realizar las acciones tendientes para la prevención y control de los fraudes y delitos informáticos.

<http://www.fbi.gov>

CUERPO NACIONAL DE POLICIA ESPAÑOLA:

UNIDAD DE INVESTIGACIÓN DE DELINCUENCIA EN TECNOLOGÍAS DE LA INFORMACIÓN:

La Unidad de Investigación de la Delincuencia en Tecnologías de la Información nace en el transcurso del año 2000 con el propósito de impulsar, coordinar y realizar investigaciones relacionadas con la criminalidad de las nuevas tecnologías y las comunicaciones en España, estrechar las relaciones con las demás policías de la Comunidad Europea. Dependiente del Ministerio del Interior del Reino de España.

<http://www.mir.es/policia/>

POLICIA NACIONAL DE LA REPUBLICA DE FRANCIA

OFICINA CENTRAL DE LUCHA CONTRA LA CRIMINALIDAD LIGADA A LAS TECNOLOGIAS DE LA INFORMACIÓN Y LAS COMUNICACIONES.

A raíz de los altos requerimientos para la investigación de los ciberdelitos, el Primer Ministro Don Lionel Jospin, determina la creación de un organismo centralizado, estructurado y especializado en estas nuevas fuentes de información, ante lo cual, por decreto de fecha 15 de Mayo del 2000, entra en actividades la “**Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (O.C.L.C.T.I.C.)**” con la finalidad de cooperar al servicio de judicatura, en las nuevas técnicas tecnológicas, cooperar y asistir al Poder Judicial en delitos de graves costos sociales. Haciéndose asesorar por expertos en todas las áreas de la informática, penal y social.

<http://www.interieur.gouv.fr/police/ocltic/index.htm>



2. Los delitos informáticos en la legislación ecuatoriana.

El rápido desarrollo de las nuevas tecnologías hizo que el Ecuador busque integrarse en la nueva sociedad de la información y busque nuevas alternativas comerciales para poder comerciar sus productos con el resto del mundo es así como surgió el interés por el Comercio Electrónico y con el incremento de los negocios virtuales, muchos proveedores de servicios de Internet ecuatorianos buscaron ponerse al día con la tecnología de punta necesaria para ofrecer a sus clientes los servicios de comercio electrónico seguro.

Con este primer gran paso cumplido, surge también la necesidad de que el Estado impulse el desarrollo de las tecnologías y promueva masivamente el uso de los nuevos medios para comercializar productos y servicios con el fin de impulsar la economía ecuatoriana, por tanto, haciéndose necesario crear un marco jurídico acorde con una nueva realidad de comercio electrónico creciente en el país.

Producto de esto, manifiesta José Luis Barzallo, que es la Fundación de la Corporación Ecuatoriana de Comercio Electrónico CORPECE www.corpece.net la que impulsó el proyecto de Ley de Comercio Electrónico, Firma electrónica y Mensaje de datos. Para su elaboración y estructuración invitó a una amplia base de sectores involucrados y contó con la participación de importantes empresas del medio. Partieron de la legislación ecuatoriana y se apoyaron en proyectos de leyes como la Ley modelo UNCITRAL, diversas propuestas de la Organización de las Naciones Unidas; Directivas Europeas sobre comercio electrónico y firma digital, proyectos y anteproyectos de leyes de países europeos como Italia, España, Alemania, Luxemburgo; El acta de UTAH, de los Estados Unidos de Norteamérica; Estudios y proyectos latinoamericanos de Chile, Argentina, Uruguay, Colombia y Perú; Investigaciones y publicaciones sobre el derecho de las nuevas tecnologías, principalmente de universidades, entre otros, así como contaron con la opinión de importantes tratadistas del tema.

El sentido jurídico de dicho proyecto según José Luis Barzallo, fue el incluir dentro del comercio electrónico las diversas relaciones que se pueden dar en un



mundo de tecnología, sea en los negocios como en la vida diaria, con el propósito de enmarcar las diversas actividades jurídico-tecnológicas en los conceptos técnicos que se exponen y así proteger tanto al empresario como al usuario de estos servicios.

El proyecto de Ley ecuatoriana estaba compuesto de tres Títulos, conteniendo cada uno varios capítulos y artículos.

Respecto de las nuevas formas del delito, éstas son incluidas como reformas al Código Penal, a fin de tipificarse puntualmente estos delitos y actualizar al Código Penal respecto de estas nuevas formas de delinquir. Los nuevos delitos son: a). Fraude informático; b). Delito de daños informáticos; c). Falsificación electrónica; d). Intromisión indebida a los sistemas de información o telemáticos; e). Recopilación de información por medios fraudulentos. f). Violación al derecho a la privacidad en los términos de la misma ley.

Finalmente en el proyecto se dispone que el Estado vele porque se incentive, se difundan las posibilidades y conocimientos sobre el comercio electrónico y se protejan los derechos de las empresas que intervienen en el mercado de la informática y las telecomunicaciones, ramas indispensables para la ejecución del Comercio Electrónico. Por mandato se señala que la Ley entrará en vigencia a partir de su publicación en el Registro Oficial.

Este proyecto de Ley fue presentado en el H. Congreso Nacional para análisis de las nuevas formas jurídicas que se proponen para dinamizar el mercado ecuatoriano. Muchos de los conceptos propuestos llevan la creatividad misma que le impone al jurista el progreso desenfrenado al que lleva la tecnología.⁹

En abril de 2002, se aprueba en el Congreso Nacional, el texto definitivo de la Ley de Comercio Electrónico, Mensaje de Datos y Firmas Electrónicas, y en consecuencia las reformas al Código Penal con lo cual se da lugar a las llamadas Infracciones Informáticas.

El Título V versa sobre las infracciones informáticas, que se consideran aquellas

⁹ Dr. José Luis Barzallo. Ecuador: El Comercio Electrónico en el Ecuador, Desafío frente al Nuevo Siglo.



de carácter administrativo y que se encuentran detalladas mediante reformas en el Código Penal. Entre estas infracciones están: **violentar los sistemas de seguridad para acceder a información protegida** lo que es sancionado con prisión de seis meses a un año y una multa de quinientos a mil dólares de los Estados Unidos de Norteamérica. Si la información obtenida se refiere a seguridad nacional o secretos comerciales o industriales la sanción será de uno a tres años de prisión y multa de mil a mil quinientos dólares. La divulgación o utilización fraudulenta de la información protegida se sanciona con pena de reclusión menor ordinaria de tres a seis años y multa de dos mil a diez mil dólares. Si la divulgación o utilización fraudulenta lo realizan personas encargadas de la custodia o utilización legítima de la información serán sancionadas con pena de reclusión menor de seis a nueve años y multa de dos mil a diez mil dólares; **destrucción o supresión de documentos**, títulos, programas, datos o bases de datos que serán sancionados con un período de tres a seis años de reclusión menor; **falsificación electrónica, alteración o daño de programas, bases de datos**, información relacionada con sanción de seis meses a tres años de prisión y multa de sesenta a ciento cincuenta dólares; **apropiación ilícita** para facilitar la apropiación de un bien ajeno y violación del derecho de intimidad serán reprimidos con prisión de seis meses a cinco años y multa de quinientos a mil dólares de los Estados Unidos.

A continuación me permito transcribir las disposiciones de la Ley de Comercio Electrónico, Mensaje de Datos y Firmas Electrónicas lo referente a las infracciones informáticas.

Art. 57.- Infracciones informáticas.- Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente ley.

Reformas al Código Penal

Art. 58.- A continuación del artículo 202, inclúyanse los siguientes artículos innumerados:



"Art. ...- El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica.

Si la información obtenida se refiere a seguridad nacional, o a secretos comerciales o industriales, la pena será de uno a tres años de prisión y multa de mil a mil quinientos dólares de los Estados Unidos de Norteamérica.

La divulgación o la utilización fraudulenta de la información protegida, así como de los secretos comerciales o industriales, será sancionada con pena de reclusión menor ordinaria de tres a seis años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Si la divulgación o la utilización fraudulenta se realiza por parte de la persona o personas encargadas de la custodia o utilización legítima de la información, éstas serán sancionadas con pena de reclusión menor de seis a nueve años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Art. ...- Obtención y utilización no autorizada de información.- La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares, serán sancionadas con pena de prisión de dos meses a dos años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica."

Art. 59.- Sustitúyase el artículo 262 por el siguiente:

"Art. ...- 262.- Serán reprimidos con tres a seis años de reclusión menor, todo empleado público y toda persona encargada de un servicio público, que hubiere maliciosa y fraudulentamente, destruido o



suprimido documentos, títulos, programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, de que fueren depositarios, en su calidad de tales, o que les hubieren sido encomendados sin razón de su cargo".

Art. 60.- A continuación del artículo 353, agréguese el siguiente artículo innumerado:

"Art. ...- Falsificación electrónica.- Son reos de falsificación electrónica la persona o personas que con ánimo de lucro o bien para causar un perjuicio a un tercero, utilizando cualquier medio; alteren o modifiquen mensajes de datos, o la información incluida en éstos, que se encuentre contenida en cualquier soporte material, sistema de información o telemático, ya sea:

- 1.- Alterando un mensaje de datos en alguno de sus elementos o requisitos de carácter formal o esencial;
- 2.- Simulando un mensaje de datos en todo o en parte, de manera que induzca a error sobre su autenticidad;
- 3.- Suponiendo en un acto la intervención de personas que no la han tenido o atribuyendo a las que han intervenido en el acto, declaraciones o manifestaciones diferentes de las que hubieren hecho.

El delito de falsificación electrónica será sancionado de acuerdo a lo dispuesto en este Capítulo."

Art. 61.- A continuación del artículo 415 del Código Penal, inclúyanse los siguientes artículos innumerados:

"Art. ...- Daños informáticos.- El que dolosamente, de cualquier modo o utilizando cualquier método, destruya, altere, inutilice, suprima o dañe, de forma temporal o definitiva, los programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, será reprimido con



prisión de seis meses a tres años y multa de sesenta a ciento cincuenta dólares de los Estados Unidos de Norteamérica.

La pena de prisión será de tres a cinco años y multa de doscientos a seiscientos dólares de los Estados Unidos de Norteamérica, cuando se trate de programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, destinada a prestar un servicio público o vinculada con la defensa nacional.

Art. ...- Si no se tratare de un delito mayor, la destrucción, alteración o inutilización de la infraestructura o instalaciones físicas necesarias para la transmisión, recepción o procesamiento de mensajes de datos, será reprimida con prisión de ocho meses a cuatro años y multa de doscientos a seiscientos dólares de los Estados Unidos de Norteamérica."

Art. 62.- A continuación del artículo 553 del Código Penal, añádanse los siguientes artículos innumerados:

"Art. ...- Apropiación ilícita.- Serán reprimidos con prisión de seis meses a cinco años y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, los que utilizaren fraudulentamente sistemas de información o redes electrónicas, para facilitar la apropiación de un bien ajeno, o los que procuren la transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de ésta o de un tercero, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensajes de datos.

Art. ...- La pena de prisión de uno a cinco años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica, si el delito se hubiere cometido empleando los siguientes medios:

1. Inutilización de sistemas de alarma o guarda;



2. Descubrimiento o descifrado de claves secretas o encriptadas;
3. Utilización de tarjetas magnéticas o perforadas;
4. Utilización de controles o instrumentos de apertura a distancia; y,
5. Violación de seguridades electrónicas, informáticas u otras semejantes."

Art. 63.- Añádase como segundo inciso del artículo 563 del Código Penal, el siguiente:

"Será sancionado con el máximo de la pena prevista en el inciso anterior y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, el que cometiere el delito utilizando medios electrónicos o telemáticos."

Art. 64.- A continuación del numeral 19 del artículo 606 añádase el siguiente:

"... Los que violaren el derecho a la intimidad, en los términos establecidos en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos".

Análisis de las Infracciones Informáticas en la Legislación Ecuatoriana.

1. VULNERACIÓN DE CLAVES O SISTEMAS DE SEGURIDAD (primer artículo añadido al Art. 202 del Código Penal.

a. Bien Jurídico protegido.

Según la ubicación en la que se incluyó este delito en nuestro Código Penal, se puede determinar que el bien jurídico protegido es la "inviolabilidad del secreto", conforme la nominación del Capítulo V, que a su vez se encuentra



dentro del Título II, denominado “De los delitos contra las garantías constitucionales y la igualdad racial”.

b. El verbo rector o nuclear de la infracción.

La acción se encuentra identificada con el verbo “violentar”, que, según el Diccionario de la Academia Española de la Lengua, significa “romper”, “forzar” o “vulnerar”; es decir, es el acto ingresar o introducirse, violentando seguridades a un determinado lugar; en el presente caso, la acción consistiría en violentar claves o sistemas de seguridad informáticos, para acceder y obtener información protegida. Por lo tanto, al tratarse de sistemas virtuales, es decir no materiales, resulta incorrecto el verbo “violentar”, pues tal violencia física no existe ni puede existir, razón por la cual, el verbo rector de esta infracción para tipificarla en forma correcta, debería ser sustituido por los siguientes verbos: “desactivar” claves o “inhabilitar” sistemas de seguridad para acceder a información protegida.

Además, esta acción violenta debe realizarse empleando algún medio electrónico, informático o afín, lo cual refuerza aún más el argumento de que no corresponde a este delito el verbo “violentar”, aplicable solo a los medios físicos empleado en contra de las personas o la fuerza en las cosas.

Y debe tener un objetivo: vulnerar el secreto, confidencialidad o reserva que tenga dicha información; o, simplemente, vulnerar la seguridad. Es decir, el simple acceso de cualquier información protegida, sin ningún otro acto que le signifique beneficio posterior al autor, ya es objeto de sanción de seis meses a un año de prisión y multa de quinientos a mil dólares.

Esta pena se agrava si la información “violentada” es sobre seguridad nacional o secretos comerciales o industriales; en estos casos, se sanciona con prisión de uno a tres años y multa de un mil a un mil quinientos dólares. Este agravamiento de la pena, tiene su razón de ser en la mayor importancia de la información contenida en los medios virtuales.

Es importante insistir que esta acción delictiva se limita a “violentar” claves o sistemas de seguridad por medios electrónicos, informáticos o afines, sin que



se requiera ningún otro acto posterior que cause beneficio al infractor y perjuicio al ofendido; basta con llegar a la información protegida, para que se perfeccione este delito.

El ir más allá del simple acceso a la información protegida tiene una pena mayor y el legislador utiliza los siguientes verbos rectores: “divulgar” o “utilizar”, en forma fraudulenta la información protegida, así como los secretos comerciales o industriales.

Según esta redacción empleada por el legislador, esta conducta correspondería a otro tipo penal contenido en el mismo artículo: el primero, el simple acceso a la información protegida y, el segundo, la divulgación y la utilización fraudulenta de dicha información. Sin embargo, no resulta claro el explicar cómo, en este segundo caso, el autor divulga y utiliza la información si es que en primer lugar no accedió a ella, “violentando” las claves y los sistemas de seguridad; si una persona es la que accede a la información y luego la envía a otra persona, este envío ya sería una forma fraudulenta de “utilizar” tal información, lo que implica que ya habría cometido el segundo delito. Por lo tanto, la deficiente redacción del legislador crea graves confusiones; lo correcto hubiese sido que se utilicen los tres verbos de la siguiente manera: “acceder” en forma fraudulenta a una información protegida, para luego “divulgarla” o “utilizarla” en cualquier forma, en perjuicio del propietario, poseedor o propietario de la información.

Otra circunstancia agravante con razonable lógica, ocurre cuando la divulgación o utilización fraudulenta es realizada por la persona encargada de la custodia o utilización legítima de la información; esta agravante tiene su razón de ser en que el custodio o encargado de su utilización legítima, revela más peligrosidad al faltar a su deber de fidelidad laboral para la institución o persona para la cual presta sus servicios. En este caso la pena es de reclusión menor de seis a nueve años y multa de dos mil a diez mil dólares.



c. Sujetos activos y pasivos de esta infracción.

El sujeto activo de este delito, puede ser cualquier persona; pero en el último caso, en el que se agrava la pena, sólo puede ser el custodio o encargado de la utilización legítima de la información.

El sujeto pasivo u ofendido por el delito, es el propietario de la información vulnerada y, en el caso de la seguridad nacional, sería el Estado.

d. Tipo subjetivo.

Este delito es esencialmente doloso, es decir, debe existir el designio de causar daño; y este daño se produce por el simple acceso a la información protegida, sin ningún permiso o consentimiento, sin que se requiera ninguna otra finalidad, pues ya se lesionó la privacidad o la garantía de protección de un secreto. Al respecto, el tratadista Miguel Polaino Navarrete manifiesta: “todo acceso cognitivo no autorizado al correspondiente banco de datos reservados, implica lesión del bien jurídico de la intimidad garantizada al titular de datos reservados”.¹⁰

No cabe, por lo tanto, el delito culposo, es decir, el que se comete por falta de previsión o de precaución, ni el delito inintencional, en el cual no existe la intención de causar daño, o preterintencional, cuando el resultado va más allá de la intención.

También es necesario considerar que la pena se agrava cuando la información se refiere a la seguridad del Estado, o a secretos industriales o comerciales; y, aún más, cuando se utiliza o divulga esa información.

e. Consumación y tentativa.

El delito se consuma en el momento en el que el autor ingresa a la información protegida y, en la forma agravada, cuando utiliza o divulga esa información.

¹⁰ POLAINO NAVARRETE, Miguel, Curso de Derecho Penal Español, Madrid, 1996, p. 402.



Cabe la tentativa cuando se practican actos idóneos conducentes de manera inequívoca al ingreso a la información reservada utilizando medios electrónicos, informáticos o similares, pero la acción no se consuma por causas extrañas; por ejemplo, cuando es sorprendido utilizando un sistema informático con la clara intención de ingresar a la información reservada, lo cual correspondería a la tentativa del delito básico, pero no necesariamente a su forma agravada, la que se consuma en el momento de la utilización o divulgación no autorizada, a menos de que se trate de la persona encargada de la custodia o de la utilización legítima de la información, en cuyo caso podría darse la tentativa si realiza actos encaminados a esos fines, pero no se consuma el delito por causas ajenas a su voluntad.

2. OBTENCIÓN DE DATOS PERSONALES PARA SU UTILIZACIÓN FRAUDULENTO. (segundo artículo añadido al Art. 202 del Código Penal).

a. Bien jurídico protegido.

Al igual que el delito anterior, es la inviolabilidad del secreto y, en forma específica, la garantía de la reserva de los datos personales, que no pueden ser publicados o transferidos sin la autorización de su titular.

b. El verbo rector o nuclear de la infracción.

En el presente caso, la acción está definida con el verbo “obtener” información sobre datos personales. Lo cual, en forma necesaria, implica que debe existir un archivo en el que consten datos referentes a una determinada persona, sin definir si tales datos deben constar en un archivo virtual o material; al respecto, es preciso observar que este delito se incorpora al Código Penal en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, lo cual permitiría suponer que se trataría de un sistema informático de datos personales; sin embargo, el Art. 4 del Código Penal prohíbe la interpretación extensiva y obliga al Juez a atenerse estrictamente a la letra de la ley y solo cuando exista duda, se la interpretará en el sentido más favorable al reo. Por lo tanto, se debe considerar para esta infracción a cualquier archivo o base de datos, entre los que se incluyen los informáticos o virtuales.



Pero no basta la simple obtención de tales datos, la cual por sí sola no constituiría delito, sino deben obtenerse los datos para utilizarlos, con las finalidades definidas por los siguientes verbos: ceder, publicar o transferir dichos datos a cualquier título, sin la autorización de su titular.

c. Sujetos activos y pasivos

El sujeto activo de esta infracción puede ser cualquier individuo que obtenga, por cualquier medio, los datos de otra persona, para utilizarlos cediéndolos, publicándolos o transfiriéndolos a cualquier título, sin la autorización de su titular.

El sujeto pasivo de este delito, es el titular de esos datos, es decir, la persona a quien le pertenecen y cuya autorización se requiere para que la utilización sea legal.

d. Elemento subjetivo.

Para la consumación de este delito, se requiere del dolo directo, es decir, de la intención de utilizar los datos obtenidos para cederlos, publicarlos o transferirlos a cualquier título.

e. Consumación y tentativa.

Este delito se consuma cuando la persona que obtuvo los datos personales, los utiliza sin la autorización de su titular.

Podría darse la figura de la tentativa, si se practican actos idóneos para la consumación del delito, pero ésta no se realiza por causas ajenas a la voluntad del autor, como ocurriría cuando es sorprendido tratando de utilizar los datos personales sin la autorización de su titular.



3. DESTRUCCIÓN O SUPRESIÓN MALICIOSA Y FRAUDULENTO DE SISTEMAS DE DATOS CONTENIDOS EN UN SISTEMA DE INFORMACIÓN O RED ELECTRÓNICA. (Art. 262 del Código Penal).

a. Bien jurídico protegido.

En este delito, sin lugar a dudas, el bien jurídico protegido es la calidad del servicio público que el Estado debe garantizar a toda la población, requiriéndose, como características mínimas, que sea seguro, confiable y eficiente. Es por esta razón que se sanciona la violación de los deberes de un funcionario público o de una persona encargada de un servicio público, que tenga en su poder, en razón de su cargo o empleo, sistemas de información o redes electrónicas en los que consten datos, cuya protección y vigilancia les corresponde.

b. Sanción.

Este delito es sancionado con una pena de tres a seis años de reclusión menor.

c. El verbo rector o nuclear de la infracción.

Como verbo rector de esta infracción, se encuentra el “destruir” o “suprimir” documentos, títulos, programas, datos, bases de datos, información o cualquier mensaje de datos contenidos en sistemas de información o redes electrónicas. Parecería que el verbo correcto para este delito sería “eliminar” o “borrar” datos contenidos en sistemas informáticos, pues en especial el verbo “destruir” no sería aplicable, en forma correcta, a un sistema virtual. El legislador ha limitado la acción a la destrucción o supresión de documentos, títulos, programas, datos, bases de datos, información o cualquier mensaje de datos, pero no amplía la figura delictiva a la alteración de los mismos.

d. Sujetos activos y pasivos.

El sujeto activo de esta infracción, no puede ser cualquier persona. Tiene necesariamente que tener la calidad de funcionario público o encargado de un servicio público, que tenga acceso al sistema informático en razón de su cargo, es decir, que se ha encomendado por las funciones que ejerce.



e. Elementos subjetivos.

No toda destrucción o supresión de programas, documentos y datos constantes en un sistema informático o en una red electrónica, puede ser sancionado. Es necesario que la acción se la realice en forma maliciosa y fraudulenta; es decir, es necesario que exista el dolo directo, que según el Art. 14 del Código Penal es “el designio de causar daño”, faltando, de esta manera, en forma grave a los deberes intrínsecos que tienen los funcionarios públicos o cualquier persona encargada de un servicio público.

f. Consumación y tentativa.

Este delito se consuma cuando se han destruido o suprimido algún programa, documento o dato que se encuentre en algún soporte informático o red electrónica, cuando se actúan dolosamente.

También puede ocurrir que el autor realice actos idóneos conducentes a la comisión del delito, pero éste no se consuma por causas ajenas a la voluntad del autor.

4. FALSIFICACIÓN ELECTRÓNICA (artículo añadido a continuación del Art. 353 del Código Penal)

a. Bien jurídico protegido.

En este delito, el bien jurídico protegido es la fe pública, que se lesiona cuando se alteran la información o los datos contenidos en un soporte material, informático o telemático, es decir, se hacen aparecer como verdaderos información y datos falsos.

b. Sanción.

La sanción para este delito, se determina de modo general con la frase: “será sancionado de acuerdo a lo dispuesto en este capítulo”; de lo que se puede concluir que si se trata de un instrumento público, un instrumento privado o un certificado o registro, será aplicable las penas determinadas para la falsificación de estos documentos.



c. El verbo rector o nuclear de la infracción.

Los verbos rectores son “alterar” o “modificar” mensajes de datos o la información contenida en éstos, utilizando cualquier medio y con el ánimo de lucro o de causar perjuicio a otro, en las circunstancias detalladas que a su vez tienen otros verbos, de la siguiente manera: “alterar” una base de datos en cualquiera de sus elementos o requisitos de carácter formal o esencial; “simular” un mensaje de datos, en todo o en parte, que induzca a error sobre su autenticidad; o “suponer” en un acto la intervención de personas que no han intervenido, o atribuyendo a las que han intervenido declaraciones o manifestaciones diferentes a las que hubieran hecho.

d. Sujetos activos y pasivos.

Sujeto activo de este delito podría ser cualquier persona que tenga acceso legítimo a una base de datos o que fraudulentamente accediere a ella, a excepción del empleado público que desnaturalizare la esencia en la redacción de piezas correspondientes a su empleo, bien sea escribiendo estipulaciones diferentes a las acordadas, o estableciendo como verdaderos hechos que no lo son; o el médico que confiere certificaciones falsas; o los posaderos u hoteleros que hubieren registrado con nombres falsos a las personas alojadas en sus locales o alteraren dichos registros. Salvo estas excepciones, cualquier persona puede ser el sujeto activo de este delito.

Como sujeto pasivo, se encuentra el titular de esos datos o la persona a quien perjudique la falsificación.

e. Elementos subjetivos

La finalidad de estas acciones que consiste en el ánimo de lucro o la intención de perjudicar a otro, nos llevan a la conclusión de que se requiere del dolo para que se configure este delito, que, por lo tanto, no puede ser culposos.

f. Consumación y tentativa

Este delito se consuma cuando se ha alterado o modificado un mensaje de datos o la información contenida en éstos.



Cabe también la tentativa cuando se practican actos idóneos, conducentes de manera inequívoca a la realización del delito, el que no se consuma por causas ajenas a la voluntad del autor.

5) DAÑOS INFORMÁTICOS (dos artículo añadidos a continuación del Art. 415 del Código Penal)

a. Bien jurídico protegido

Según la ubicación de este artículo, el bien jurídico protegido es la “seguridad pública”, la cual se lesiona cuando se destruyen o modifican sistemas informáticos, en forma especial cuando se trata de servicios públicos o vinculados con la defensa nacional, en cuyo caso la sanción establecida es mayor.

Sin embargo, cuando los daños o el sabotaje se realizan en sistemas informáticos privados, el bien jurídico protegido sería más bien el patrimonio o la propiedad privada, pues si se alteran o suprimen, por ejemplo, los datos de una empresa, su funcionamiento regular se alterará en forma grave, lo cual traerá como consecuencia pérdidas económicas. Entonces la intención del autor así como el resultado de la acción, va a afectar, en forma directa, los intereses económicos o patrimoniales de una persona natural o jurídica; tratándose de empresas, es muy posible que la acción la realice alguien vinculado con la competencia comercial o industrial.

b. El verbo rector o nuclear de la infracción.

Los verbos rectores de este delito son varios: destruir, alterar, inutilizar, suprimir o dañar programas, datos, bases de datos, información o cualquier sistema de mensaje de datos contenidos en un sistema de información o red electrónica. Estas acciones, por lo tanto, constituyen sabotaje cuando se las realiza en un sistema virtual o software.

En cambio, el otro delito es destruir, alterar o inutilizar la infraestructura o instalaciones físicas necesarias para la transmisión, recepción o procesamiento de mensajes de datos. Es decir, estas acciones deben realizarse en la parte física



del sistema o hardware, o en las instalaciones o edificaciones en las que se encuentre instalado dicho sistema.

Este último delito es subsidiario, es decir, se lo aplica siempre y cuando no se trate de un delito mayor; es decir, si la acción cometida constituye otro delito, como por ejemplo el incendio de instalaciones, que revela una mayor peligrosidad del autor y es más severamente castigado, se lo juzgará por éste último.

c. Sanción

Las sanciones establecidas para este tipo de infracciones, son las siguientes:

- El sabotaje o daños al software en general, es sancionado con prisión correccional de seis meses a tres años y multa de sesenta a ciento cincuenta dólares; y, si es destinado a la prestación de un servicio público o utilizado en la defensa nacional, es de tres a cinco años de prisión y multa de doscientos a seiscientos dólares.
- El daño al hardware o a las instalaciones físicas, es sancionado con prisión correccional de ocho meses a cuatro años y multa de doscientos a seiscientos dólares.

d. Sujetos activos y pasivos

El sujeto activo de este delito, es cualquier persona que haya tenido acceso al software, al hardware y a las instalaciones físicas y cause daños.

El sujeto pasivo es el titular, propietario, poseedor o arrendatario del sistema informático, bien sea una persona natural o una personal natural o jurídica.

e. Elementos subjetivos

Se trata de un delito doloso, es decir, debe existir la intención de causar daño, sin que pueda cometerse en forma inintencional o culposa.

f. Consumación y tentativa

Este delito se perfecciona con la irrogación del daño, pudiendo quedar en el grado de tentativa, si el autor practica actos idóneos conducentes de modo



inequívoco a su realización, pero ésta no culmina por razones extrañas a su voluntad.

6) APROPIACIÓN ILÍCITA (dos artículos agregados a continuación del Art. 553 del Código Penal)

a. Bien jurídico protegido

Es delito de apropiación ilícita protege el bien jurídico “propiedad”; es decir, el dueño es privado de su derecho de propiedad de sus bienes, cuando el autor utiliza fraudulentamente sistemas informáticos o redes electrónicas.

b. El verbo rector o nuclear de la infracción

Son dos los verbos rectores principales: El primero es “utilizar” en forma fraudulenta redes informáticas o electrónicas para desapropiar a una persona de sus bienes. El otro, “procurar la transferencia no consentida de bienes, valores o derechos de una persona” en su perjuicio o de un tercero, en beneficio del autor o de otra persona, “alterando, manipulando o modificando” redes, programas o sistemas informáticos, telemáticos o mensajes de datos.

Con una pena mayor se reprime el delito cuando se utilizan sistemas de alarma, tarjetas magnéticas o perforadas, controles o instrumentos de apertura a distancias, descubriendo o descifrando claves o violando seguridades.

c. Sanción

La pena para este delito en general, es de seis meses a cinco años de prisión correccional y multa de quinientos a mil dólares.

La pena para el delito agravado, es de uno a cinco años de prisión correccional y multa de un mil a dos mil dólares.

d. Sujetos activos y pasivos

Sujeto activo es todo individuo que se apropie de bienes ajenos utilizando medios electrónicos o telemáticos, o alterando, manipulando o modificando dichos sistemas.



Y sujeto pasivo es la persona que sufre la privación de la propiedad de sus bienes, con la utilización de los referidos métodos.

e. Elementos subjetivos

Este delito sólo puede ser realizado en forma fraudulenta, es decir, con dolo, con el designio de causar daño a otra persona, al apropiarse ilícitamente de sus bienes. No cabe, por lo tanto, la culpa o la inintencionalidad.

f. Consumación y tentativa

El delito se consuma con la desapropiación de sus bienes que sufre una persona. Y, como los otros delitos informáticos, puede quedar en el grado de tentativa, si se practican actos idóneos conducentes de manera inequívoca a su realización, al que no culmina por causas ajenas a la voluntad del autor.

7) ESTAFA (Art. 563 del Código Penal, tercer inciso)

a. Bien jurídico protegido

El bien jurídico que protege este delito es la propiedad, la cual resulta seriamente lesionada cuando una persona entrega fondos, muebles, obligaciones, finiquitos o recibos, con su voluntad viciada por los manejos fraudulentos, es decir, cuando se ha abusado de la confianza y de la credulidad de su titular.

b. El verbo rector o nuclear de la infracción

La acción que caracteriza a este delito es “hacerse entregar” algo, que puede consistir en fondos, muebles, obligaciones, finiquitos o recibos, mediante la utilización de manejos fraudulentos, haciendo creer en cualquier acontecimiento quimérico o abusando, de otro modo, de la confianza y de la credulidad. Estos términos empleados por el legislador: “cualquier acontecimiento quimérico” o abusar “de otro modo” de la confianza y la credulidad, llevan a considerar que se trata de un tipo penal parcialmente en blanco, pues no se especifica, de manera exacta y precisa, cuáles son esas otras formas de cometer la infracción.

En su segundo inciso, el referido artículo agrava la pena cuando se hayan utilizado medios informáticos o telemáticos.



c. Sanción

Para reprimir las estafas en general, la pena es de seis meses a cinco años de prisión correccional y multa de ocho a ciento cincuenta y seis dólares.

Cuando se trate de estafas cometidas mediante la utilización de medios informáticos o telemáticos, este medio constituye una circunstancia agravante y es sancionado con el máximo de la pena señalada en el inciso anterior y multa de quinientos a mil dólares.

Y, por último, en caso de estafas en migraciones ilegales, la pena es de tres a seis años de reclusión menor ordinaria.

d. Sujetos activos y pasivos

El sujeto activo puede ser cualquier persona que desapropie a otra de sus bienes empleando manejos fraudulentos.

En cambio, el sujeto pasivo es el propietario que entrega el bien con su voluntad viciada por el engaño.

e. Elementos subjetivos

Como elemento subjetivo principal, tenemos que el autor debe hacerse entregar bienes de otra persona “con el ánimo de apropiarse” y utilizando el engaño o el fraude. Es decir, es una infracción esencialmente dolosa, sin que pueda cometerse en forma inintencional o culposa.

f. Consumación y tentativa

El delito se consuma con la desapropiación, es decir con la entrega del objeto, el que pasa a la esfera de custodia y de poder del autor, quien se lo ha hecho entregar con el ánimo de apropiarse, utilizando manejos fraudulentos.

Es posible la tentativa en este tipo de delitos, cuando se practican actos idóneos conducentes de manera inequívoca a la realización de la estafa, pero ésta no se consuma por circunstancias ajenas a la voluntad de su autor.



CAPÍTULO II

RIESGOS Y VULNERABILIDADES QUE OCASIONAN LOS DELITOS INFORMÁTICOS.

1. Introducción y problemas jurídicos de la criminalidad informática.

La dependencia cada vez mayor de la población a procedimientos automatizados e informatizados ocasionan también nuevos riesgos y la realización de ilícitos utilizando las nuevas tecnologías, convirtiéndose en habituales los fraudes en pagos electrónicos, la difusión prohibida de contenidos a través de la Red, el acceso ilegítimo a informaciones confidenciales contenidas en bases de datos, los ataques a sistemas informáticos que bloquean la prestación de determinados servicios o la difusión mundial de virus, pero a pesar de los perjuicios a causa de este tipo de hechos y la alarma que sin duda generan, debemos reconocer que formas de pago ilícitas, incluso mediante tarjetas de crédito, existían ya antes así como también, la difusión de material pornográfico se llevaba a cabo de forma precedente, la publicidad fraudulenta o engañosa no es un fenómeno que aparezca con las Nuevas Tecnologías, ni la falsificación documental se nos puede presentar como algo novedoso. En la práctica sabemos que no existe ningún campo del actuar humano en el que la seguridad esté garantizada plenamente.

La lucha frente a la criminalidad informática desborda naturalmente el campo exclusivo del Derecho Penal, pues se trata de un fenómeno cuyo control reclama además otros instrumentos más amplios y complejos (de tipo jurídico - no penal-, de tipo técnico, formativo, así como educativo)¹¹. Sin embargo, es necesario considerar la necesidad de un estudio profundo de las implicaciones penales de las tecnologías informáticas y de la comunicación. Una política criminal racional es imprescindible en este campo si se quiere obtener una respuesta legal adecuada y de largo alcance.

¹¹ REVISTA ÁMBITO JURÍDICO ®. "Problemas fundamentales de la criminalidad informática".



Es una constante histórica, la alarma que los avances científicos y técnicos producen en la sociedad que recibe su impacto. Con la novedad y las consecuencias prácticas de los instrumentos que la capacidad humana posibilita a lo largo de la historia surgen inmediatamente temores a su utilización. Pero en realidad ningún campo de la actividad humana está libre de riesgos frente a comportamientos peligrosos o perjudiciales. Con la aparición del comercio electrónico se abre la posibilidad de realizar pagos a través de Internet. Sin embargo existe una gran desconfianza –en cierta medida fundamentada- a realizar el pago con los datos de la tarjeta bancaria por la posible utilización fraudulenta de los mismos.

La revolución social y técnica que implican las nuevas tecnologías traen consigo también efectos en lo que al Derecho Penal respecta. Para esta disciplina jurídica aportan nuevos retos que necesariamente deberá abordar desde el punto de vista del derecho penal material. A pesar de que la mayoría de las conductas desarrolladas a través de internet no sean en esencia algo nuevo, la extraordinaria peculiaridad del medio dota a las mismas de una especial estructura que obliga a actualizar los tipos delictivos.

Al margen de las deficiencias en la construcción de los tipos penales, existen otros fenómenos que determinan graves obstáculos en la lucha contra esas formas de criminalidad, se trata de factores que dificultan la detección y persecución del delito cometido a través del Internet.

Según Javier Fernández Teruelo, entre esos factores se encuentra el **anonimato** potencial del autor y la **ejecución a distancia** propios del medio. Con relación al primero, las dificultades existentes para detectar la comisión de un delito ejecutado a través de internet pueden ser significativas. La tarea de delimitar quién es el autor de la acción presuntamente delictiva tampoco es siempre sencilla. El autor antes citado explica que cada ordenador tiene asignada una dirección IP en el momento de conectarse a internet. Su seguimiento y detección en muchos casos a priori no resulta complejo, incluidos los supuestos en que la misma tiene un carácter dinámico. Sin embargo, los actuales protocolos



IP no garantizan siempre la determinación de la dirección del emisor, ya que la misma puede ser manipulada.

En los primeros años de vida de internet la identificación de la máquina desde la cual se ejecutaba la conducta delictiva era compleja por las escasas obligaciones de control impuestas a los prestadores de servicios y el frecuente borrado de archivos log por parte de los proveedores de acceso. El log de visitas es un archivo creado por el servidor, donde se registran las acciones que los usuarios generan en la Web. En el mismo se contiene cuando menos la IP del usuario, la fecha, el archivo pedido, la ID de contestación, la página desde la que se pide el archivo, información sobre versión del navegador y terminal del usuario. El control de los archivos log es una de las principales herramientas con las que se cuenta para conocer los detalles de las tareas realizadas en el sistema, y por tanto, para la investigación de un eventual delito.¹²

Problemas de persecución. Delitos a distancia y competencia territorial.

Se presentan grandes dificultades por la ejecución de las conductas criminales a distancia. La conducta delictiva puede tener su origen en uno o varios países y los resultados producirse sin embargo en otro u otros. Incluso puede resultar difícil afirmar donde tiene lugar dicha acción, pues se dice que la conducta delictiva navega por la red. Esto ocasiona serios problemas para determinar la competencia jurisdiccional para su enjuiciamiento.

Para resolver este problema, en España se han formulado tres teorías: a) Teoría de la actividad, según ésta, se entiende cometido el delito donde el sujeto lleva a cabo externamente la conducta delictiva. b) la teoría del resultado; según esta teoría el delito se comete donde tiene lugar el resultado externo. c) La teoría de la ubicuidad, de acuerdo a esta teoría el delito se entiende cometido en donde se lleva a cabo la actividad o se manifiesta el resultado. En general la doctrina se ha manifestado favorable a la apreciación de la teoría del resultado. Sin embargo, esa solución no siempre será válida para los delitos cometidos a distancia y en

¹² Cibercrimen. Los delitos cometidos a través de internet. Javier Gustavo Fernández Teruelo.



concreto para los ejecutados a través de internet, para su enjuiciamiento según las autoridades españolas sería preciso acudir a la teoría de la ubicuidad, posibilidad que fue admitida por el Tribunal Supremo español considerando que tanto la acción como el resultado son elementos del tipo.

En el Documento “Delitos Informáticos: Generalidades” de la autoría del Dr. Santiago Acurio del Pino, encontramos lo siguiente con respecto a los problemas de persecución:

El citado autor manifiesta que, este tipo de infracciones son difícilmente descubiertas o perseguidas porque los sujetos activos actúan sigilosamente y poseen herramientas capaces de borrar todo rastro de intrusión o la consumación del delito, plantea que existen dos problemas principales: a) Problemática con la concepción tradicional de tiempo y espacio; b) Anonimato del Sujeto Activo.

a) Problemática con la concepción tradicional de tiempo y espacio.

Plantea que la característica de transnacional de la delincuencia informática es otro de los problemas de perseguibilidad. Dice el autor que tradicionalmente se ha considerado que la ley penal solo se aplica en el territorio de la República, hecho que constituye el llamado “principio de territorialidad de la ley”, este principio sostiene que la ley penal de un país es aplicable cuando la infracción ha sido cometida dentro del territorio, en el momento actual esto puede haber cambiado teniendo en cuenta que el nuevo escenario en donde mayormente se da este tipo de delitos es el Ciberespacio, un lugar donde no existen fronteras territoriales. Por lo expuesto dice el autor, se puede constatar que es difícil la persecución de estos delitos y su enjuiciamiento, ya que existe la posibilidad de preparar y cometer acciones delictivas informáticas en perjuicio de terceros en tiempo y espacio lejanos; pero que, los adelantos de las telecomunicaciones y la telemática, hace que las distancias reales o fronteras entre países no existan, ya que una persona puede realizar un acto delictivo en un lugar distinto del lugar de los hechos, como por ejemplo los creadores de MALWARE o de los VIRUS INFORMÁTICOS como el conocido: I LOVE YOU, el



cual fue diseñado y creado en Filipinas y causó daños a nivel mundial en cuestión de días.

La territorialidad de la ley es considerada como un principio de soberanía del estado y se resume al decir que no se puede aplicar al ecuatoriano delincuente otra ley que no sea la ecuatoriana, aclarando que no importa el lugar en donde se encuentre el delincuente, es decir, sin importar el país en donde se haya cometido el delito.

Según el Dr. Santiago Acurio, este principio denota algunas características:

- La ley penal es aplicable a los hechos punibles cometidos dentro del territorio del Estado, sin consideración a la nacionalidad del actor.
- No se toma en cuenta la nacionalidad del autor.
- Se toma en cuenta el lugar de comisión del delito. Nuestra legislación se inclina por la teoría del resultado, es decir que la infracción se entiende cometida en el territorio del Estado cuando los efectos de la acción u omisión deban producirse en el Ecuador o en los lugares sometidos a su jurisdicción.
- Se aplica al concepto jurídico de territorio por el Derecho Internacional: los límites del Estado, mar territorial, espacio aéreo.
- Se aplica también la teoría del territorio flotante o principio de la bandera: Naves o aeronaves de bandera nacional ya sea que se encuentren en alta mar, en su espacio aéreo y en lugares en que por la existencia de un convenio internacional, ejerzan jurisdicción. Este principio no se aplica cuando las naves o aeronaves mercantes estén sujetas a una ley penal extranjera.

El ámbito de aplicación de este principio está en:

1. Territorio Continental
2. Espacio Aéreo
3. Mar Territorial
4. Naves y aeronaves ecuatorianas de guerra o mercantes.
5. Infracciones cometidas en el recinto de una legación ecuatoriana en país extranjero.



Principios de extraterritorialidad.

Tres son los principios que constituyen el principio de extraterritorialidad y son los siguientes: a) el principio de la nacionalidad o personalidad; b) el principio de la defensa, y c) el principio de la universalidad y justicia mundial.

a) Principio de la nacionalidad o personalidad.

Según este principio, se debe aplicar al delincuente únicamente la ley que corresponde a su nacionalidad; es decir, la ley de país de su origen, sea el país que sea en el que haya cometido el delito. Este principio tiene dos divisiones:

1. **Principio de la nacionalidad activa.** Se funda en la obediencia que se exige al súbdito ecuatoriano con respecto a su legislación. Se toma en cuenta la nacionalidad del autor del delito.
2. **Principio de la nacionalidad pasiva.** El alcance espacial de la ley se extiende en función del ofendido o titular del bien jurídico protegido. Se aplicaría cuando está en juego la protección de los bienes jurídicos individuales.

b) Principio de la defensa.

Según este principio, es aplicable la ley del país donde los principios son atacados por el delito, sin tomar en cuenta la nacionalidad de los realizadores. SE toma en cuenta la nacionalidad del bien jurídico protegido; es decir, se aplica este principio cuando se afecta la integridad territorial. Quedando en juego la protección de los bienes nacionales. Ha sido tomado por algunos países, como por ejemplo el nuestro, el cual puede pedir la extradición de un delincuente informático que haya vulnerado bienes jurídicos protegidos en nuestro país como resultado de su acción delictiva. Claro que esta norma no puede ser aplicada en todos los países ya que algunos de ellos como el nuestro prohíbe la extradición de ecuatorianos que hayan cometido una infracción en otro país, en este caso se aplica un principio de equivalencia, es decir, si el delito cometido en el otro país se encuentra tipificado en el nuestro también puede seguirse el proceso penal por el cometimiento de dicho delito, pero en nuestro país.



c) Principio de la universalidad y justicia mundial.

Este principio se refiere a que es aplicable la ley del país que primero aprese al delincuente, sin considerar otro aspecto.

Este principio tiene una finalidad práctica para reprimir los delitos contra la humanidad, aquellos que han sido catalogados como tales en virtud de ser considerados como ofensores de toda la humanidad. Para ello es necesario firmar convenios internacionales y unilaterales con el fin de que cada país pueda sancionar al delincuente con su propia ley, sin importar el lugar donde el individuo haya cometido el acto ni tampoco la nacionalidad del mismo.

Se prescinde tanto de la nacionalidad del autor como del lugar de comisión del delito, se fundamenta en el principio de solidaridad de los estados en la lucha contra el delito.

En doctrina penal se concede en virtud de este principio eficacia extraterritorial a la ley penal; pero en el Derecho Internacional condiciona esta eficacia extraterritorial tomando en cuenta: a) La calidad del bien jurídico protegido, como bienes culturales supranacionales; b) Cuando los autores del delito sean peligrosos para todos los estados.

En cuando a los delitos informáticos de carácter transnacional, en especial en el ciberterrorismo es necesario aplicar este principio por cuanto la peligrosidad de este tipo de ataques puede causar más daño que el terrorismo convencional.

b) Anonimato del Sujeto Activo.

El sujeto activo de esta clase de infracciones puede ser totalmente anónimo y usar este anonimato como forma de evadir su responsabilidad, ya que éste no necesariamente puede usar su propio sistema informático, sino que se puede valer de un tercero, como por ejemplo en el caso del envío de correo no deseado o spam, en el cual se puede usar a una máquina zombi, es decir una



computadora que está bajo el control del spammer y que le permite usarla como una estación de trabajo de su propia red de máquinas zombis, las cuales pertenecen a usuarios desatentos que no tienen al día sus medidas de seguridad y que son fáciles presas de los hackers y crackers para cometer este tipo de infracciones. También existen programas de enmascaramiento o que no permiten ver la verdadera dirección ya sea de correo electrónico o del número IP.

Criterios de selección de los nuevos tipos penales.

Con la aparición del fenómeno de los hechos ilícitos cometidos mediante la informática o sobre los medios informáticos, inmediatamente se plantea la posibilidad del recurso al Derecho penal como medio de sancionar y combatir los mismos. La sanción penal, como se sabe, representa el medio jurídico más gravoso para los bienes e intereses de las personas por lo que únicamente debe ser empleado en los casos de ataques a los bienes más importantes de las personas y de la comunidad y cuando no existan otros medios jurídicos que pudieran solucionar satisfactoriamente este tipo de situaciones. Por ello se hace necesario determinar qué tipo de hechos vinculados a la informática alcanzan la gravedad y los requisitos mínimos para poder ser objeto de sanción penal. Desde el punto de vista dogmático los criterios de selección de cualquier conducta como hecho penalmente relevante hacen referencia al desvalor de resultado y desvalor de acción que las mismas representen¹³.

La conducta merecedora de sanción penal destaca fundamentalmente a través de dos datos: desvalor de acción y desvalor de resultado. El desvalor de resultado se concibe como la lesión o puesta en peligro de un bien jurídico-penalmente relevante (vida, libertad, patrimonio, medio ambiente, etc.). Por su parte el desvalor de acción se determina en relación a las propiedades materiales de la acción que la hacen peligrosa para el bien jurídico protegido.

Se considera que los medios informáticos representan en sí mismos una conducta con un elevado desvalor de acción, por su carácter insidioso y

¹³ REVISTA ÁMBITO JURÍDICO ®. "Problemas fundamentales de la criminalidad informática".



clandestino. Así las características técnicas que generalmente se asignan a los sistemas y medios informáticos son:

- Gran potencialidad para el almacenamiento de datos
- Gran velocidad de sus operaciones, pues procesa los datos a tiempo real.
- Exactitud y fiabilidad de sus operaciones.
- Extraordinaria adaptabilidad a las exigencias humanas.
- No perceptibilidad directa de las operaciones -sino a través del ordenador- (ejecución basada en los elementos lógicos de los sistemas informáticos).
- No presencia directa ni de autor ni de la víctima (aparente anonimato)

Las enormes potencialidades que se abren para el tratamiento automatizado de datos, para las telecomunicaciones y el acceso a la información, tienen un reverso que son los riesgos que se introducen para facilitar la realización de hechos que afecten a los intereses fundamentales de las personas. Desde este punto de vista aparece la informática como factor criminógeno: permite el acceso y el manejo de bases de datos, realización de operaciones desde lugares lejanos y no visibles directamente, siendo más costosa por novedosa y compleja técnicamente la averiguación del autor y la prueba de los hechos.

Pero además, como ya se ha puesto de relieve, es preciso conectarlas al peligro o lesión de un bien jurídico de relevancia penal para que nos encontremos ante un comportamiento merecedor de incriminación y sanción penal.

El Convenio de Cibercrimen (Budapest 23.11.01).

La necesidad de cooperación internacional para el caso de estos delitos que traspasan con gran facilidad los límites nacionales se hace evidente. Por ello distintos grupos de trabajo dirigen su esfuerzo a conseguir instrumentos internacionales aptos para la lucha contra una forma de delincuencia claramente transnacional. El Convenio de Cibercrimen, redactado en el marco de la actividad del Consejo de Europa –pero abierto a la firma de cualquier país- representa el instrumento internacional más válido frente a la cibercriminalidad. Sin embargo se

DRA. GRACIELA ENCALADA OCHOA



dice que pese a estar firmado por muchos países, no cuenta en este momento con el número suficiente de ratificaciones como para su entrada en vigor. Pese a ello debe ser objeto de atención en las distintas materias en las que aborda, entre ellas la de la armonización de los hechos punibles vinculados a la informática que deben estar penalizados en los países firmantes. El Convenio de Cibercrimen propone entonces en esta materia varias infracciones que deberán ser incorporadas a las legislaciones nacionales y que clasifica en cuatro grandes grupos de ilícitos penales.

Un primer grupo de infracciones lo constituyen los hechos contrarios a la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos.

Dentro de este grupo se incluyen las conductas de acceso ilegal injustificado a todo o parte de un sistema informático. La legislación penal española actual – a diferencia de lo que sucede en otros países, como Portugal – no conoce una auténtica infracción de mero acceso o mero intrusismo informático, de todas formas el Convenio permite que las partes firmantes modulen la incriminación de este supuesto mediante diferentes formas. Así es posible vincular la punibilidad de este hecho a la violación de medidas de seguridad, la existencia en el autor de determinadas intenciones a la hora de realizar el hecho o la presencia de conexión entre distintos sistemas informáticos. También se abarcan los supuestos de Interceptación ilegal de comunicaciones entre sistemas informáticos o en el interior de un mismo sistema, mediante el empleo de medios técnicos, tenemos también los atentados a la integridad de los datos, consistentes en el daño, borrado, deterioro, alteración o supresión intencional de datos informáticos. Este supuesto se puede condicionar a la producción de daños de carácter grave.

Mayor novedad para el sistema español representa el caso de los atentados a la integridad de los sistemas, consistente en el entorpecimiento grave de un sistema informático mediante las conductas anteriores de introducción, transmisión de daño, borrado, deterioro o supresión de datos informáticos. Finalmente en este primer grupo de infracciones se consideran como hechos dignos de castigo por las legislaciones nacionales todo tipo de conductas

DRA. GRACIELA ENCALADA OCHOA



abusivas relativas a los dispositivos informáticos (desde la producción y venta hasta la obtención para su utilización) que permitan la realización de los hechos delictivos anteriores. También se incriminan las mismas conductas respecto a palabras clave o códigos de acceso de un sistema informático.

El segundo grupo de conductas las denomina el Convenio Infracciones informáticas, y en ellas se incluye la falsedad informática y el fraude informático. Falsificación informática que resulta de la producción de datos informáticos no auténticos para su utilización con fines legales como si de datos genuinos se tratara. El Fraude informático hace referencia a las conductas de introducción, alteración, borrado o supresión de datos informáticos o cualquier forma de atentado al funcionamiento de un sistema informático con la intención de obtener un beneficio económico para si mismo o para otro. Se vincula entonces este supuesto a las actuaciones fraudulentas en los sistemas informáticos que persiguen el enriquecimiento injusto.

En el tercer grupo tenemos las Infracciones relativas al contenido incriminan múltiples conductas realizadas por el autor sobre materiales de pornografía infantil. Se incluyen conductas de producción, ofrecimiento, difusión o transmisión o procurar para otro por medio de un sistema informático pornografía infantil. Se extiende la incriminación a la obtención para si mismo de estos materiales mediante un sistema informático o la mera posesión del material en un sistema informático o de almacenamiento de datos informáticos. La convención se detiene en la determinación del concepto de material de pornografía infantil de manera que establece un concepto claramente amplio del mismo. Así considera pornografía infantil todo material pornográfico que represente de manera visual un menor desarrollando un comportamiento sexual explícito, representando una persona que aparezca como un menor desarrollando un comportamiento sexual explícito, o las imágenes realistas representando a un menor desarrollando un comportamiento sexual explícito. Es decir, incluye, tanto el material pornográfico realizado efectivamente con menores, como aquellos otros casos en los que los menores que figuran en el material no son auténticos, pero las imágenes puedan considerarse realistas (pornografía técnica).



En el cuarto grupo la propiedad intelectual y los derechos conexos son objeto de protección penal mediante lo dispuesto en la Convención. Se pretende incriminar los atentados a la propiedad intelectual y derechos conexos definidos en los Acuerdos Internacionales cometidos deliberadamente con fines comerciales por medio de sistemas informáticos, el Convenio deja a salvo la posibilidad de que alguno de los países firmantes no incriminen estas conductas a condición de que dispongan de otros recursos eficaces para su tutela y que tal falta de incriminación no supongan el incumplimiento de obligaciones internacionales que incumban a esa parte.

Individualización de la responsabilidad penal.

Desde los primeros momentos en los que aparecen las nuevas tecnologías y particularmente todo el mundo de Internet se plantean los límites y posibles responsabilidades derivadas de un uso irregular o ilícito de estos medios. Dentro del debate general sobre la regulación de estos nuevos mecanismos de comunicación y difusión uno de los aspectos más complejos y delicados es el de la concreta determinación de posibles responsabilidades para cada uno de los sujetos intervinientes en una compleja amalgama de partes que se suman e interactúan en el proceso total.

Efectivamente esta necesidad de determinación individualizada de responsabilidades por hechos ilícitos se ve dificultada por tratarse de un campo con características muy específicas. Por lo reciente y también por la complejidad en muchas ocasiones estamos ante un ámbito en el que no existe regulación – regulación jurídica general, no exclusivamente penal- o sólo se encuentra parcialmente regulado. Por la propia naturaleza de Internet es un medio que no cuenta con autoridades centrales e implica efectos transnacionales de su actividad. Realmente no sólo rebasa las fronteras nacionales, sino que además puede relacionar puntos del planeta distantes en lo geográfico, en lo cultural y en lo jurídico, lo que añade sin duda mayores inconvenientes a la existencia de una normativa aplicable y eficaz. Ya se ha mencionado cómo, a la hora de seleccionar ámbitos de responsabilidad, surgen inmediatamente dificultades suplementarias debido a la confluencia de plurales agentes en Internet con papeles diversos

DRA. GRACIELA ENCALADA OCHOA



(entre usuario y destinatarios existe un amplio abanico de intermediarios). Además hay que señalar que la actividad de prestación de servicios en internet se realiza por empresas, por entidades que desde el punto de vista jurídico poseen personalidad individualizada, y no por personas físicas, aunque en último extremo las tareas deban ser aplicadas por singulares sujetos. Esto genera un nuevo punto de mayor complejidad pues en aquellos casos en los que se aprecie un hecho ilícito deberá determinarse la responsabilidad personal en el entramado organizativo de la empresa e incluso la posible aplicación de sanciones a la persona jurídica.

En esta situación de relevantes singularidades y dificultades se plantea el modelo de responsabilidad a seguir en este nuevo terreno que permita una mayor confianza de los usuarios y una más clara aplicación de los hechos ilícitos por los Tribunales. Surgen dificultades ante la ausencia de regulación específica que se adapte a las características de las nuevas tecnologías.

2. Problemas de política criminal y persecución penal asociados a la informática¹⁴.

“El trabajo de la Asociación Internacional de Derecho Penal (AIDP) a favor de la profundización y extensión de la cooperación internacional en materia penal ha sido intenso, habiendo liderado científicamente el proyecto de creación de la Corte Penal Internacional. En el marco de sus Congresos Internacionales de Derecho Penal, de celebración quinquenal, la AIDP se ha ocupado de los fenómenos criminales que más preocupan en el mundo globalizado, ofreciendo un conjunto de resoluciones con propuestas específicas en cuanto apropiada para cada uno de ellos. En todo caso, y con carácter general, frente al riesgo creciente de generalización de una cooperación penal exclusivamente urgida por criterios punitivos y de seguridad ciudadana, la AIDP propugna y continúa propugnando la

¹⁴ JOSE LUIS DE LA CUESTA. Presidente de la Asociación Internacional de Derecho Penal (AIDP), Director del Instituto Vasco de Criminología. UPV-EHU.



necesidad de construcción y refuerzo de una cultura de justicia penal compartida, sin la cual resulta imposible una perdurable y eficaz colaboración”.

Globalización y sistema penal.

“Como es bien sabido, la proliferación e intensidad de las comunicaciones e intercambios más allá de las fronteras nacionales facilita el desarrollo de todo tipo de actividades transnacionales y, entre ellas, obviamente, de las propias actividades criminales. Estas se benefician, además, de la estructura y límites de los sistemas de justicia penal, lo que dificulta en gran manera su persecución¹⁵ .

Tanto a través de la acción bilateral como por el impulso de las agencias y organizaciones regionales e internacionales, son muchos los esfuerzos dirigidos a superar las dificultades indicadas mediante la firma y ratificación de instrumentos internacionales dirigidos a potenciar la colaboración entre las jurisdicciones nacionales y hasta al impulso de la jurisdicción penal internacional.

Ahora bien, aun cuando los términos internacionalización, mundialización, globalización se utilicen con frecuencia como sinónimos, en un sentido estricto, globalización no es lo mismo que internacionalización. Los teóricos de la globalización entienden que lo característico del fenómeno globalizador es esa interconectividad entre personas e instituciones que permite un funcionamiento global, muy particularmente en el marco económico y de la gobernanza: esto es, como una unidad, en tiempo real y a escala mundial¹⁶. Desde este prisma ni el desarrollo del Derecho Penal Internacional, ni la creación o establecimiento de instituciones internacionales, por muy importante que éstas sean (pensemos en la

¹⁵ J.L.de la Cuesta, “Retos y perspectivas del sistema penal en un mundo globalizado”, *Revista Académica. Facultad de Derecho de la Universidad de La Salle*, IV, 7, julio 2006, pp. 265 ss. Obra citada por José Luis de la Cuesta en su artículo “Problemas de política criminal y persecución penal asociados a la informática.

¹⁶ M.Castells, *The Information Age: Economy, Society and Culture*, vol. I: *The Rise of the Network Society*, Oxford, 1996, p.92.
J.L.DE LA CUESTA, *Principales lineamientos político-criminales de la AIDP en un mundo globalizado*. Obra citada por José Luis de la Cuesta en su artículo “Problemas de política criminal y persecución penal asociados a la informática.



propia Corte Penal Internacional) suponen *per se* una globalización del sistema penal¹⁷; ésta se encuentra todavía muy alejada de los propios sistemas penales internos y de la realidad de un sistema penal, que continúa viéndose a nivel mundial como una de las últimas manifestaciones de la soberanía estatal.

Que no exista un sistema penal globalizado no quiere, sin embargo, decir que la delincuencia no lo esté cada vez más. Y es que las oportunidades ofrecidas para la generalización y profundización de los intercambios internacionales por la desaparición de las barreras fronterizas (por lo menos en cuanto a la circulación de los bienes) y el desarrollo de las redes de comunicaciones¹⁸ resultan ampliamente aprovechadas por las redes criminales organizadas, que ven potenciadas las posibilidades abiertas para sus tráfico ilícitos, así como de penetración en los sistemas institucionales a través de la corrupción; algo similar ocurre con la cibercriminalidad y el terrorismo.

La delincuencia organizada, la corrupción, la cibercriminalidad, el terrorismo constituyen destacadas manifestaciones de una criminalidad transnacional que siempre ha preocupado internacionalmente; pero no coinciden con el núcleo duro de los crímenes internacionales en sentido estricto, tradicionalmente centrados en la agresión, los crímenes de guerra, el genocidio y los crímenes contra la humanidad. Es, con todo, en aquellas áreas, y no en el seno de los crímenes internacionales más tradicionales, donde la preocupación de las organizaciones internacionales se ha traducido, a través de la acción de las agencias globalizadas especializadas, en verdaderos esfuerzos globalizadores”.

¹⁷ S.Parmentier, “Cultural Integration and Globalization of Criminal Justice”, *Eguzkilore, Cuaderno del Instituto Vasco de Criminología*, 17, 2003, p.101. Obra citada por José Luis de la Cuesta en su artículo “Problemas de política criminal y persecución penal asociados a la informática

¹⁸ G.Picca, “Globalization and criminality”, *Annales Internationales de Criminologie*, 38, 1-2, 2000, p.93. Obra citada por José Luis de la Cuesta en su artículo “Problemas de política criminal y persecución penal asociados a la informática.



Delitos informáticos y otros delitos relativos a la tecnología de la informática: XV Congreso Internacional de Derecho Penal (1994, Brasil: Río de Janeiro)

Este artículo es de la autoría de José Luis de la Cuesta, Presidente de la Asociación Internacional de Derecho Penal y por considerarlo de mucha importancia he transcrito textualmente para no alterar el sentido del tema tratado.

“Ya 1994 los delitos informáticos fueron objeto de la Sección II del XV Congreso Internacional de Derecho Penal celebrado en Río de Janeiro (Brasil). Tras repasar un largo listado de medidas no penales, imprescindibles para una adecuada prevención de este fenómeno delictivo, las resoluciones aprobadas se ocuparon de los aspectos sustantivos (con una particular atención a la protección de la esfera privada), procesales e internacionales de la cuestión.

En el plano del *derecho penal sustantivo* a la vista de las lagunas que los nuevos modos de actuación ponen de manifiesto en el Derecho penal tradicional, el Congreso se manifestó a favor de la inclusión de nuevas disposiciones penales con objeto de hacer frente a esas insuficiencias (principio de subsidiaridad), destacando la necesidad de evitar la sobrecriminalización y asegurar su incriminación con precisión y claridad. Desde esta perspectiva, y siguiendo el contenido de la Recomendación núm. R(89)9, adoptada por el Consejo de Europa el 13 de septiembre de 1989, se entendió que el listado mínimo de actos a criminalizar vendría constituido por los siguientes:

- fraude en el campo de la informática,
- falsificación en materia informática,
- daños causados a datos o programas informáticos,
- sabotaje informático,
- acceso no autorizado,
- interceptación no autorizada,
- reproducciones no autorizadas (de un programa informático protegido, de una topografía). Al lado de los anteriores, y en una lista opcional, se incluían: 1) la alteración de datos o de programas informáticos, 2) el espionaje informático, 3) la utilización no autorizada de un ordenador, y 4) la utilización no autorizada de



un programa informático protegido.

En todo caso, se recomendaba que “algunas de las definiciones de la lista del Consejo de Europa -como la del acceso no autorizado- sean objeto de aclaración y perfeccionamiento a la luz del progreso de la tecnología de la información y de los cambios en la percepción de la delincuencia” y, al mismo tiempo, la inclusión de “otros tipos de abuso que no constan expresamente en las listas, tales como el tráfico de claves (*password*) obtenidas ilegalmente y de otras informaciones sobre posibilidades de obtener un acceso no autorizado a sistemas informáticos y la distribución de virus o de programas similares”.

Igualmente y, “en vista del daño potencial que pueden provocar los virus, gusanos y otros programas similares destinados o capaces de penetrar en un programa informático para causar daños, o interferir en datos informáticos”, se observaba la necesidad de fomentar “mayores debates científicos e investigaciones” en la materia, al tiempo que se entendía que debía prestarse una especial atención “al uso de normas penales que incriminen la imprudencia o la creación de riesgos, así como a los problemas prácticos de su ejecución”, así como “a la cuestión de saber si el delito resultante debe considerarse como delito de sabotaje”.

La sección II del Congreso abordó el debatido (y necesitado de mayor estudio y profundización) papel que corresponde al derecho penal en lo que concierne a la posible colisión de la *esfera privada*, con los nuevos cambios generados por la tecnología informática. Se afirmó aquí el carácter subsidiario del derecho penal y la prioridad de las medidas preventivas no penales, entendiéndose que principios básicos de la intervención penal, en la línea de la Recomendación (89) 9 del Consejo de Europa, han de ser:

- Su focalización en los casos intencionales y graves, “especialmente en aquellos que involucran datos altamente sensibles o información confidencial tradicionalmente protegida por ley”;
- El respeto del principio de taxatividad y la evitación del “uso de cláusulas vagas o generales;



- La distinción entre los diversos “niveles de gravedad de las infracciones” y el respeto de “las exigencias de la culpabilidad”;
- La toma en consideración por parte de las autoridades de enjuiciamiento de “la voluntad de la víctima en cuanto al ejercicio de la acción penal”.

También se entendió que en el plano de la *investigación del delito informático* han de buscarse los correspondientes equilibrios entre el “interés de una defensa social eficaz” y la “apropiada y equilibrada protección de los derechos humanos y de la intimidad”. Principio fundamental a respetar en este plano es el de legalidad, pues corresponde únicamente a la ley (y en el marco de las normas internacionales de derechos humanos) el establecimiento de disposiciones claras y precisas autorizadas de “cualquier restricción de los derechos humanos requerida para la investigación de estos delitos”, debiendo sancionarse con nulidad las pruebas obtenidas con violación no autorizada de los derechos humanos (esto, con independencia de la posible responsabilidad criminal del agente que infringió la ley). A través de la ley deberían, por tanto, definirse con claridad:

- “a. Los poderes para efectuar la búsqueda y aprehensión de pruebas en el ámbito de la tecnología de la información, en especial cuando se trata de la aprehensión de bienes intangibles y la investigación de un conjunto de sistemas;
- b. Los deberes de cooperación activa de las víctimas, testigos y demás usuarios de la tecnología de la información, con excepción del sospechoso (en particular para hacer que la información sea accesible a efectos judiciales); y
- c. Los poderes que permitan la interceptación de comunicaciones en el interior de un sistema de ordenadores o entre diferentes sistemas de ordenadores y los poderes de utilización de las pruebas obtenidas en procesos ante los tribunales”.

En todo caso, “la aplicación de poderes coercitivos debe hacerse en forma proporcional a la gravedad del delito cometido y de modo que interrumpen o afecten lo menos posible las actividades lícitas de la persona” y “el umbral a partir del cual deben comenzar las investigaciones debería tener en consideración

DRA. GRACIELA ENCALADA OCHOA 83



todos los valores inherentes al ámbito de la tecnología, como la pérdida de una oportunidad económica, el espionaje, la violación de la intimidad, la pérdida o el riesgo de privación económica y el costo de la reconstrucción de la integridad de los datos informáticos”.

El Congreso subrayó la importancia de la *cooperación internacional* en la prevención y persecución de los delitos informáticos, acentuada por “la movilidad de los datos informáticos en los sistemas de telecomunicación internacionales y la naturaleza altamente interrelacionada de la sociedad de información moderna”, a cuyo efecto, es clara la necesidad de una adecuada armonización del derecho penal material y el otorgamiento de poderes coercitivos adecuados en todos los Estados miembros. A juicio de la AIDP, la cooperación internacional debería igualmente alcanzar a otros ámbitos, como:

- la elaboración de “normas internacionales de seguridad para los sistemas informáticos”;
- la aplicación de “medidas adecuadas para la resolución de las cuestiones relativas a la competencia jurisdiccional en el ámbito de los delitos informáticos transfronterizos, así como otros delitos informáticos internacionales”;
- el logro de “acuerdos internacionales entre los Estados que se sirven de la nueva tecnología de la información para hacer sus investigaciones más efectivas; esto incluye acuerdos que prevean medidas transfronterizas de investigación y aprehensión efectivas, inmediatas y legales en el campo de los sistemas informáticos interconectados, así como otras formas de cooperación internacional, protegiendo al mismo tiempo los derechos y libertades individuales”.

Las resoluciones del Congreso se cerraron con una referencia final a las *tareas futuras* a desarrollar en este campo:

- difusión del contenido de las recomendaciones;
- desarrollo -por parte de la comunidad académica y científica, y por



los gobiernos- de investigaciones sobre los delitos de la tecnología de la información (en particular, “sobre las incidencias de los delitos de ordenadores, la extensión de las pérdidas, los métodos de comisión de las infracciones y las características de los delincuentes”), así como implantación de “nuevas medidas alternativas que permitan la utilización de las sanciones penales sólo como último recurso”;

- profundización en el estudio del derecho de la información por parte de la teoría y política jurídica, “teniendo en cuenta las características específicas de la información, frente a los objetos tangibles y examinando los cambios que suponen en los principios y paradigmas del derecho penal”;
- refuerzo de la coordinación (y colaboración con las asociaciones de industriales de material para ordenadores y de tratamiento de datos informáticos) en el combate contra el delito informático con el fin de “alcanzar una protección global eficaz”;
- mantenimiento al día del “manual sobre delitos relacionados con la informática, elaborado por iniciativa y bajo el auspicio de las Naciones Unidas”.

El aprovechamiento de las ventajas de la globalización por parte de la criminalidad provoca cada vez más la demanda de intervenciones internacionales coordinadas, que permitan hacer frente a las amenazas del crimen globalizado, algunas de cuyas manifestaciones más destacadas son, sin duda, el terrorismo, la criminalidad organizada, la cibercriminalidad, de la corrupción. La internacionalización del sistema penal, a pesar de su evidente progreso, no tiene mucho que ver con la construcción de un modelo globalizado, si por tal entendemos aquel sistema capaz de trabajar como una unidad en tiempo real y a escala planetaria; con todo, y a pesar de la resistencia de los Estados, es claro el esfuerzo de las agencias internacionales especializadas en la línea de la creación de redes globales que permitan la aplicación eficaz de programas mundiales de actuación y la promoción e impulso de todas las vías de cooperación (fundamentalmente policial, pero también judicial) en las áreas mencionadas.



Desde sus orígenes, la Asociación Internacional de Derecho Penal se ha mostrado siempre decididamente a favor de la profundización y extensión de la cooperación internacional en materia penal y hasta ha liderado científicamente el proyecto de creación de la Corte Penal Internacional que con la entrada del nuevo siglo pasó ya “de la utopía a la realidad”¹⁹. A través de sus trabajos ha constatado frecuentemente el riesgo de que la acción internacional se centre fundamentalmente en el aseguramiento de la cooperación de cara a la represión y persecución de los hechos delictivos, olvidando las tareas preventivas de carácter no punitivo, y con escasa sensibilidad por el aseguramiento del respeto de los derechos humanos.

Frente al riesgo de generalización de una cooperación penal exclusivamente urgida por criterios punitivos y de seguridad ciudadana²⁰, la AIDP propugna la construcción y refuerzo de esa “cultura de justicia penal”²¹ compartida, sin la cual resulta imposible una perdurable y eficaz colaboración. En este sentido, partiendo de la plena legitimidad de la lucha contra las formas más graves de criminalidad, la AIDP insiste, así, en primer lugar, en la necesidad de articulación de políticas criminales racionales que, con base en un adecuado conocimiento de la realidad de los fenómenos criminales (y de los factores personales y sociales que los mismos), prioricen la prevención a partir de los tres niveles criminológicos ya clásicos²² -criminalidad (fenómeno criminal), delito (concretas manifestaciones delictivas) y delincuente-, así como desde la perspectiva victimológica.

En este marco, el recurso al derecho penal constituye igualmente un instrumento imprescindible; un instrumento no prioritario, sino de carácter

¹⁹ R.Ottenhof, “L’Association... », *cit.*, pp. 15 ss. Obra citada por José Luis de la Cuesta.

²⁰ J.L.Díez Ripollés, “De la sociedad del riesgo a la seguridad ciudadana: un debate desenfocado”, *Revista electrónica de ciencia penal y criminología*, 2005, 07:01. Obra citada por José Luis de la Cuesta.

²¹ S.Parmentier, “Cultural Integration...”, *cit.*, pp.101 ss. Obra citada por José Luis de la Cuesta.

²² J.Pinatel, *Criminología*, 2ª ed. (trad. X.Rodríguez de Canestri), Caracas, 1974, pp. 93 ss. Obra citada por José Luis de la Cuesta.



subsidiario que encuentra su verdadero sentido y legitimidad en el servicio a favor de una justicia, cada vez más humana y eficaz, y de la paz²³. Esto exige trabajar permanentemente en el refuerzo de sus perfiles democráticos, de modo que en la defensa de los bienes jurídicos fundamentales, junto al “axioma fundamental” de humanidad²⁴, se asegure plenamente la garantía y defensa de los derechos y postulados penales y procesales básicos en todos los niveles de la intervención punitiva.”

3. Las vulnerabilidades de los sistemas operativos y la no actualización por parte de los usuarios finales de los PARCHES concernientes a la seguridad de los mismos.

Con las nuevas tecnologías no es extraño que desde la tranquilidad de un hogar, se esté entrelazado por medio de la tecnología digital con información proveniente desde los puntos más lejanos del mundo, o tener el acceso a nuestras cuentas corrientes, o simplemente encontrarnos leyendo las noticias nacionales e internacionales, sin necesidad de recurrir al diario de papel o estar en contacto con nuestros familiares en todo momento, ubicación y situación posible.

El desarrollo de toda esta infraestructura en las comunicaciones, informaciones y negocios lastimosamente también ha permitido cometer diversas actividades delictivas. Estas acciones perturbadoras de la convivencia social han surgido al amparo de las nuevas herramientas tecnológicas, ante lo cual en el ámbito mundial, se ha generado una percepción de la seguridad informática, y de una evidente necesidad de control por parte de los organismos de control social formal; 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

²³ J.L.de la Cuesta, “Mundialización”, *cit.*, p.77. Obra citada por José Luis de la Cuesta.

²⁴ A.Beristain, “Axiomas fundamentales de la Criminología ante la globalización y la multiculturalidad”, *Eguzkilore, Cuaderno del Instituto Vasco de Criminología*, 17, 2003, pp. 93 ss. Obra citada por José Luis de la Cuesta.



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, de tecnologías y de socialización.

Esta situación de vulnerabilidad a que nos vemos enfrentados 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 nuestros bienes jurídicos, tales como la privacidad, bienestar, derechos de autor y tantos otros; como son la aparición en el ámbito privado de servicios que mediante el uso de nuevas tecnologías o metodologías permiten un ambiente de tranquilidad relativa, especialmente en el desarrollo del comercio electrónico.

La infraestructura de la información se ha convertido en una parte vital de nuestras economías y los usuarios deberíamos poder confiar en la disponibilidad de los servicios informativos y tener la seguridad de que las comunicaciones y los datos están protegidos pues el desarrollo del comercio electrónico y su efectiva utilización dependen de la seguridad que se nos brinde, por ello es necesario utilizar medios jurídicos y prácticos eficaces para prevenir la comisión de acciones delictivas.

Se dice que el enfoque clásico de la seguridad exige una compartimentación organizativa, geográfica y estructural estricta de la información, según su sensibilidad y su categoría pero esto es casi posible en la práctica en el mundo digital, puesto que el tratamiento de la información se distribuye, se prestan servicios a usuarios móviles, y la interoperabilidad de los sistemas es una condición básica. Los enfoques tradicionales de la seguridad se han sustituido por soluciones innovadoras basadas en las nuevas tecnologías que implican el uso del cifrado y las firmas digitales, de nuevos instrumentos de autenticación y de control del acceso, y de filtros de software de todo tipo. Muchos de estas tecnologías existen ya, pero los usuarios no estamos conscientes de su existencia, de la manera de utilizarlas, o de las razones por las que pueden ser necesarias, esta última circunstancia está muy fuertemente arraigada en la cultura



nacional, de no enfrentar esta situación con la debida anticipación, negándonos la oportunidad de tener una clara percepción sobre esta grave problemática.

La Vulnerabilidad de los Sistemas Informáticos²⁵.

Sistemas Operativos.

Un sistema operativo es un programa que actúa como intermediario entre el usuario y el hardware de una computadora y su propósito es proporcionar un entorno en el cual el usuario pueda ejecutar programas. El objetivo principal de un sistema operativo es lograr que el sistema de computación se use de manera cómoda, y el objetivo secundario es que el hardware de la computadora se emplee de manera eficiente.

Un sistema Operativo es en sí mismo un programa de computadora, muy especial, quizá el más complejo e importante. El Sistema Operativo despierta a la computadora y hace que reconozca a la CPU, la memoria, el teclado, el sistema de vídeo y las unidades de disco. Además, proporciona la facilidad para que los usuarios se comuniquen con la computadora y sirve de plataforma a partir de la cual se corran programas de aplicación.

Cuando se enciende una computadora, lo primero que ésta hace es llevar a cabo un autodiagnóstico llamado auto prueba de encendido. Durante este autodiagnóstico, la computadora identifica su memoria, sus discos, su teclado, su sistema de vídeo y cualquier otro dispositivo conectado a ella. Lo siguiente que la computadora hace es buscar un Sistema Operativo para arrancar (boot).

Una vez que la computadora ha puesto en marcha su Sistema Operativo, mantiene al menos parte de éste en su memoria en todo momento. Mientras la computadora esté encendida, el Sistema Operativo tiene 4 tareas principales:

²⁵ <http://www.monografias.com/trabajos14/sisteinform/sisteinform.shtml> . Artículo enviado por [cjinicolini](#)



Proporcionar ya sea una interfaz de línea de comando o una interfaz gráfica al usuario, para que este último se pueda comunicar con la computadora.

- Interfaz de línea de comando: Se introducen palabras y símbolos desde el teclado de la computadora, ejemplo, el MS-DOS.
- Interfaz gráfica del Usuario (GUI): Se seleccionan las acciones mediante el uso de un Mouse para pulsar sobre figuras llamadas iconos o seleccionar opciones de los menús.

Administrar los dispositivos de hardware en la computadora. El Sistema Operativo sirve de intermediario entre los programas y el hardware.

Administrar y mantener los sistemas de archivo de disco. Los SO agrupan la información dentro de compartimientos lógicos para almacenarlos en el disco. Estos grupos de información son llamados archivos. Los archivos pueden contener instrucciones de programas o información creada por el usuario. El SO mantiene una lista de los archivos en un disco, y nos proporciona las herramientas necesarias para organizar y manipular estos archivos.

Apoyar a otros programas. Por ejemplo, listar los archivos, grabarlos en el disco, eliminar archivos, revisar espacio disponible, etc.

Objetivos para la creación de los Sistemas Operativos.

El objetivo fundamental de los sistemas de computación es ejecutar los programas de los usuarios y facilitar la resolución de sus problemas. El hardware se construye con este fin, pero como este no es fácil de utilizar, se desarrollan programas de aplicación que requieren ciertas operaciones comunes.

Otros objetivos son:

Transformar el complejo hardware de una computadora a una máquina accesible al usuario.

Lograr el mejor uso posible de los recursos.

Hacer eficiente el uso del recurso.



Funciones de los Sistemas Operativos.

Aceptar todos los trabajos y conservarlos hasta su finalización.

Interpretación de comandos: Interpreta los comandos que permiten al usuario comunicarse con el ordenador.

Control de recursos: Coordina y manipula el hardware de la computadora, como la memoria, las impresoras, las unidades de disco, el teclado o el Mouse.

Manejo de errores: Gestiona los errores de hardware y la pérdida de datos.

Secuencia de tareas: El sistema operativo debe administrar la manera en que se reparten los procesos. Definir el orden. (Quien va primero y quien después).

Protección: Evitar que las acciones de un usuario afecten el trabajo que está realizando otro usuario.

Multi acceso: Un usuario se puede conectar a otra máquina sin tener que estar cerca de ella.

Contabilidad de recursos: establece el costo que se le cobra a un usuario por utilizar determinados recursos.

Características de los Sistemas Operativos.

En general, se puede decir que un Sistema Operativo tiene las siguientes características:

Conveniencia. Un Sistema Operativo hace más conveniente el uso de una computadora.

Eficiencia. Un Sistema Operativo permite que los recursos de la computadora se usen de la manera más eficiente posible.

Habilidad para evolucionar. Un Sistema Operativo deberá construirse de manera que permita el desarrollo, prueba o introducción efectiva de nuevas funciones del sistema sin interferir con el servicio.



Encargado de administrar el hardware. El Sistema Operativo se encarga de manejar de una mejor manera los recursos de la computadora en cuanto a hardware se refiere.

Relacionar dispositivos. El Sistema Operativo se debe encargar de comunicar a los dispositivos periféricos, cuando el usuario así lo requiera.

Organizar datos para acceso rápido y seguro.

Manejar las comunicaciones en red. El Sistema Operativo permite al usuario manejar con alta facilidad todo lo referente a la instalación y uso de las redes de computadoras.

Facilitar las entradas y salidas. Un Sistema Operativo debe hacerle fácil al usuario el acceso y manejo de los dispositivos de Entrada/ Salida de la computadora.

¿Cuáles son las vulnerabilidades en un Sistema?²⁶

Muchas veces nos hemos preguntado: ¿Cómo puedo defenderme, de algo que no conozco?

Para poder defendernos, debemos conocer cuáles son las principales vulnerabilidades en un Sistema de Cómputo, comprendiendo como Sistema de Cómputo, todo aquel dispositivo que integra las comunicaciones, las estaciones de trabajo, las redes, los firewalls, servidores, módems, gente, etc.

Una vez que sabemos cuáles son los componentes del Sistema de Cómputo, daremos una serie de recomendaciones y puntos de debilidad que podemos reforzar, con herramientas, mejores prácticas, políticas, procedimientos y sobre todo la conciencia de que la seguridad solamente puede ser segura, a través de Políticas y procedimientos, de la tecnología y sobre todo del elemento

²⁶ Clemente Topete Contreras



más importante: los recursos humanos, ya que es la principal vulnerabilidad en cualquier Sistema.

1. Cuando tenemos un control de acceso inadecuado, hacia los dispositivos de entrada, como lo son los ruteadores, podemos reforzar este control de acceso con el uso de un ACL (Authorization Control List, por sus siglas en inglés), para no permitir filtraciones de información a través de ICMP (Internet Control Message Protocol por sus siglas en inglés), IP NetBIOS y bloquear accesos no autorizados a determinados servicios en los servidores de la DMZ (Demilitarized zone por sus siglas en inglés).

2. Cuando tenemos puntos de acceso remoto a nuestra red, es muy probable que nosotros tengamos la creencia de que son seguros; y nos tenemos que hacer la pregunta: ¿Realmente son seguros los puntos de acceso remoto a nuestra red? Debemos reforzar los accesos remotos, con la ayuda de tecnologías de autenticación de usuarios, creando una VPN (Virtual Private Network, por sus siglas en inglés) o usando módems del tipo call back.

3. Los sistemas operativos, son una fuente constante de vulnerabilidades, ya que si no aplicamos parches a nuestros sistemas operativos, una persona ajena a nuestro entorno, puede obtener información de usuarios, aplicaciones, servicios compartidos, información del DNS, etc. Para contrarrestar esta vulnerabilidad es necesario aplicar los diferentes parches, que los fabricantes de los sistemas operativos publiquen.

4. Los hosts que ejecutan servicios que no son necesarios, como son: RPC, FTP, DNS, SNTTP), ya que pueden ser fácilmente atacados.

5. Una de las principales vulnerabilidades, son las contraseñas de las estaciones de trabajo, ya que por lo regular usamos una contraseña sencilla, fácilmente adivinable, ya usada con anterioridad. Para contrarrestarla debemos de usar contraseñas de 7 caracteres o más, que tengan letras mayúsculas y minúsculas combinadas con números.



- 6.** Las claves de acceso que tienen exceso de privilegios, ya que se puede tener acceso a los servidores de información.

- 7.** Servidores en la zona DMZ, mal configurados, especialmente en archivos de comandos CGI en servidores Web y FTP anónimos, con directorios en los que cualquier persona cuente con privilegios de escritura.

- 8.** Una vez que se ha comprometido un servidor de la zona DMZ, se puede tener acceso a los ruteadores para tener acceso a los sistemas internos de nuestra red.

- 9.** Las aplicaciones que no se hayan parchado convenientemente, o que no estén actualizadas, o dejen su configuración predeterminada, se vuelven un dolor de cabeza y un apetitoso manjar para los hackers.

- 10.** No es recomendable tener excesivos controles de acceso a archivos y directorios, cuando hacemos exportaciones de un sistema NT o XP mediante NFS en Unix.

- 11.** Cuando contamos con relaciones de confianza, como son los Dominios de confianza de NT y los archivos.rhost y hosts.equiv de Unix, ya que a través de ellos se puede tener acceso a sistemas sensibles.

- 12.** Servicios no autenticados, tales como rastreadores de la red (sniffers), ya que a través de ellos se puede obtener información privilegiada y así poder penetrar a las diferentes aplicaciones con que cuenta nuestra empresa.

- 13.** Es importante revisar las bitácoras de acceso a nuestra red, ya que podemos vigilar y detectar intentos de acceso a nuestra red, deberán estar implantadas en dos niveles, el de la red y el del host.

- 14.** Cuando en una empresa no se tienen políticas de seguridad, así como procedimientos y falta de capacitación a su personal, se dice que es una "empresa vulnerable", ya que el personal se vuelve la parte más débil, por su ignorancia y falta de control.



Espero que con estos pequeños concejos, la seguridad de la información y de los Sistemas se vuelva menos vulnerable y estar menos expuesta a ataques positivos y que personas no autorizadas accedan a uno de los activos más importantes de las empresas: "**La Información**".

Factores que hacen a un sistema más vulnerable.

Existen varios factores que hacen a un sistema más vulnerable:

Código sin confirmar - Un código en un diskette, en CD-ROM o USB, se puede ejecutar por la irresponsabilidad o ignorancia del usuario.

Defectos - La mayoría de los sistemas contienen errores que se pueden aprovechar por el malware, mientras no se ponga el parche correspondiente.

Homogeneidad - Cuando todas las computadoras en una red funcionan con el mismo sistema operativo, sí pueden corromper ese SO, podrán afectar cualquier computadora en el que funcione.

Sobre-privilegios del código - La mayoría de los sistemas operativos permiten que el código sea ejecutado por un usuario con todos los derechos.

Sobre-privilegios del usuario - Algunos sistemas permiten que todos los usuarios modifiquen sus estructuras internas.

Bugs:

La mayoría de los sistemas contienen bugs (errores) que pueden ser aprovechados por el malware. Los ejemplos típicos son los desbordamiento de búfer (buffer overflow), en los cuales la estructura diseñada para almacenar datos en un área determinada de la memoria permite que sea ocupada por más datos de la que le caben, sobre escribiendo áreas anexas. Esto puede ser utilizado por el malware para forzar al sistema a ejecutar su código.

Nota histórica: La palabra BUG se utiliza para referirse a fallos, pero una de las connotaciones históricas más comentada es "un error computacional causado por una polilla que se interpuso entre los contactos de un relé probablemente



debido al calor que desprendían las primeras computadoras", hay otra historia, que suele suceder en contadas ocasiones, es que animales de compañía se coman el cableado. Curiosamente en el mundo de la informática, se ha venido utilizando para errores software, cuando originalmente era para referirse a errores hardware.

Discos de inicio:

Los PCs tenían que ser booteadas (iniciadas) con un diskette, y hasta hace poco tiempo era común que fuera el dispositivo de arranque por defecto. Esto significó que un diskette contaminado podría dañar la computadora durante el arranque, e igual se aplica a CDs y llaves USB.

Aunque eso es menos común ahora, sigue siendo posible olvidarse de que el equipo se inicia por defecto, en un medio removible, y por seguridad normalmente no debería haber ningún diskette, CD, etc, al encender el computador.

Para solucionar esto basta con entrar en la BIOS del ordenador y cambiar el modo de arranque del ordenador a HDD/CDROM/USB/Floppy, aunque para volver a instalar el sistema operativo hay que revertir los cambios a Floppy/CDROM/USB/HDD.

Homogeneidad:

Una causa no citada de la vulnerabilidad de redes, es la homogeneidad del software multiusuario. En particular, Microsoft Windows-tiene una gran parte del mercado que al concentrarse en él permitirá a crackers derribar una gran cantidad de sistemas.

Sobre-privilegios de usuario:

En algunos sistemas, los usuarios no-administradores son sobre-privilegiados por diseño, en el sentido que se les permite modificar las estructuras internas del sistema.



En algunos ambientes, los usuarios son sobre-privilegiados porque les han concedido privilegios inadecuados de administrador o el estado equivalente. Éste es sobre todo una decisión de la configuración, pero en los sistemas de Microsoft Windows la configuración por defecto es sobre-privilegiar al usuario.

Esta situación existe debido a decisiones tomadas por Microsoft para priorizar la compatibilidad con viejos sistemas sobre la necesidad de una nueva configuración de seguridad y porque las aplicaciones típicas fueron desarrollados sin tomar en cuenta a los usuarios sin privilegios.

Muchas aplicaciones existentes que requieren exceso de privilegio (código sobre-privilegiado) pueden tener problemas con la compatibilidad con Vista. Sin embargo, la característica del control de la cuenta del usuario de Vista procura remediar las aplicaciones no diseñados para los usuarios no privilegiados, actuando como apoyo para resolver el problema del acceso privilegiado inherente en las aplicaciones heredadas.

Sobre-privilegio de código:

Los malware, funcionando como código sobre-privilegiado, pueden utilizar estos privilegios para cambiar el sistema. Casi todos los sistemas operativos populares, y también muchas aplicaciones escritas no prohíben algunos códigos también con muchos privilegios, generalmente en el sentido que cuando un usuario ejecuta el código, el sistema no limita ese código a los derechos del usuario. Esto hace a los usuarios vulnerables al malware en la forma de anexos de E-mail, que pueden o no pueden ser disfrazados. Dado esta situación, se advierte a los usuarios que abran solamente archivos solicitados, y ser cuidadosos de archivos recibidos de fuentes conocidas o desconocidas que no han solicitado.

Es también común para los sistemas operativos que sean diseñados de modo que reconozcan más dispositivos de los diversos fabricantes y cuenten con drivers de estos hardwares, aún algunos que pueden no ser muy confiables.



Clasificación:

Existen muchísimos tipos de malware, aunque algunos de los más comunes son los virus informáticos, los gusanos, los troyanos, los programas de spyware/adware o incluso ciertos bots.

Dos tipos comunes de malware son los *virus* y los *gusanos informáticos*, este tipo de programas tienen en común la capacidad para auto replicarse, es decir, pueden contaminar con copias de sí mismos y en algunas ocasiones mutando, la diferencia entre un gusano y un virus informático radica en la forma de propagación, un gusano opera a través de una red, mientras que un virus lo hace a través de ficheros a los que se añade.

Los virus informáticos utilizan una variedad de portadores. Los blancos comunes son los archivos ejecutables que son parte de las aplicaciones, los documentos que contienen macros (Virus de macro), y los sectores de arranque de los discos de 3 1/2 pulgadas y discos duros (Virus de boot, o de arranque). En el caso de los archivos ejecutables, la rutina de infección se produce cuando el código infectado es ejecutado, ejecutando al primero el código del virus. Normalmente la aplicación infectada funciona correctamente. Algunos virus sobrescriben otros programas con copias de ellos mismos, el contagio entre computadoras se efectúa cuando el software o el documento infectado van de una computadora a otra y es ejecutado.

Cuando un software produce pérdidas económicas en el usuario del equipo, también se clasifica como **software criminal o Crimeware**, término dado por Peter Cassidy, para diferenciarlo de los otros tipos de software malignos, en que estos programas son encaminados al aspecto financiero, la suplantación de personalidad y el espionaje, al identificar las pulsaciones en el teclado o los movimientos del ratón o creando falsas páginas de bancos o empresas de contratación y empleo para con ello conseguir el número de cuenta e identificaciones, registros oficiales y datos personales con el objetivo de hacer fraudes o mal uso de la información. También es utilizando la llamada Ingeniería social, que consiste en conseguir la información confidencial del propio usuario mediante engaños, como por ejemplo, mediante un correo en donde mediante



engaños se solicita al usuario enviar información privada o entrar a una página falsificada de Internet para hacerlo.

Adware:

Este software muestra o baja anuncios publicitarios que aparecen inesperadamente en el equipo, pudiendo hacerlo simultáneamente o cuando se está utilizando la conexión a una página Web o después de que se ha instalado en la memoria de la computadora.

Algunas empresas ofrecen software "gratuito" a cambio de publicitarse en su pantalla, otras al instalar el programa, se instalan junto con Spyware sin que lo note.

También existen algunos programas "a prueba" (shareware), que mientras no son pagados, no permiten algunas opciones como puede ser imprimir o guardar y además en ocasiones cuentan con patrocinios temporales que al recibir la clave libera de tales mensajes publicitarios y complementan al programa.

El adware es una aplicación que muestra publicidad y que suele acompañar a otros programas. Si bien esto puede hacerse, en algunas oportunidades, bajo el conocimiento del usuario, el problema radica en los casos en los cuales se recoge información sin consultar.

También pueden ser fuente de avisos engañosos. Por lo general los programas adware tiene la capacidad de conectarse a servidores en línea para obtener publicidades y enviar la información obtenida. Cabe aclarar que no toda aplicación que muestra algún tipo de publicidad incluye adware y esto, en muchos casos, se ha transformado en una controversia para determinar cuando un elemento se encuadra dentro de estas características.

Backdoor:

Una puerta trasera (también conocidos como *Backdoor*) es un software que permite el acceso al sistema de la computadora ignorando los procedimientos normales de autenticación o facilita la entrada a la información de un usuario sin



su permiso o conocimiento. Como es el caso de e-mail, que aparentan ser enlaces a actualizaciones y que al pulsarla nos conecta a páginas similares a las originales, descargando archivos backdoor que al instalarlos, abrirá un puerto del equipo, dejándolo a expensas del autor del **malware** o para poder descargar otros códigos maliciosos.

Según como trabajan e infectan a otros equipos, existen dos tipos de puertas traseras. El primer grupo se asemeja a los Caballo de Troya, es decir, son manualmente insertados dentro de algún otro software, ejecutados por el software contaminado e infecta al sistema para poder ser instalado permanentemente. El segundo grupo funciona de manera parecida a un gusano informático, el cuál es ejecutado como un procedimiento de inicialización del sistema y normalmente infecta por medio de gusanos que lo llevan como carga.

Badware Alcalinos:

Este es un tipo de Malware mitad spyware, mitad backdoor, suele residir en las ventanas del sistema observando incesantemente hasta que se lanza al acecho de un usuario.

Bomba fork:

Programa que se autoreplica velozmente para ocupar toda la memoria y capacidad de proceso del ordenador donde se ejecutan, debido a que su forma de ataque es del tipo denegación de servicio (DoS) que es un ataque al servidor o a la red de computadoras para producir la in conectibilidad a una red debido a que consume el ancho de banda atacado, al crear programas y procesos simultáneos muy rápidamente, saturando el espacio disponible e impidiendo que se creen procesos reales del usuario.

Bots:

Es un programa robot que se encarga de realizar funciones rutinarias, pero que también pueden ser usados para, por ejemplo, crear cuentas en los diferentes sitios que otorgan e-mail gratuitos, para con estas cuentas realizar daños.



En algunos casos este bot, puede encargarse de fingir ser un humano dando contestación a preguntas como es el caso de supuestos adivinos que dan el futuro a aquellos que pagan por este servicio o fingir ser una mujer u hombre con quien se esta teniendo una candente conversación, pero también pueden ser juegos de Internet programados para jugar contra supuestamente una serie de contrincantes que lo son en forma virtual, pudiendo pedir cantidades de dinero para poder participar y con ello además poder tener datos de cuentas de tarjetas de crédito.

También son programas que a través de órdenes enviadas desde otra computadora controlan el equipo personal de la víctima, es decir convirtiéndola en un "Zombi".

Caballo de Troya:

Un **programa caballo de Troya** (también llamado Troyano) cuyo nombre está relacionado con la conocida historia del Caballo de Troya, es un intruso informático, software dañino disfrazado de software legítimo. Los caballos de Troya no son capaces de replicarse por sí mismos y pueden ser adjuntados con cualquier tipo de software por un programador y contaminar a los equipos por medio del engaño, usando un programa funcional para encubrirse y permanecer dentro del computador.

Su nombre es dado en alusión al popular caballo de madera con que los aqueos (griegos) engañaron a los troyanos. De modo similar este software actúa entrando en la computadora, oculto en otros programas aparentemente útiles e inofensivos pero que al activarse crean problemas al desarrollar la acción de estos archivos infecciosos.

Se considera que el primer troyano aparece a finales de los años 1980, pero eran poco comunes al ser necesario que el programa se distribuyera casi manualmente, fue hasta que se generalizó la comunicación por Internet, que se hizo más común y peligroso al entrar ocultos e instalarse cuidadosamente sin que se percatara el usuario del equipo, con lo que sean considerados una de las más



temibles invasiones ilegales en las estaciones de trabajo, servidores y computadoras personales.

Cookies:

- 1.- El buscador pide una página Web.
- 2.- El servidor envía la página + la cookie.
- 3.- El buscador pide otra página.

La cookie es el tipo de almacenamiento de información guardado en el propio equipo que puede hacer normalmente el seguimiento de las preferencias en Internet dándole una clave que su creador podrá identificar para con ello tener una referencia de visitas con la finalidad de medir preferencias de mercado. Pero también por lo mismo puede ser usada por hackers para analizar qué páginas consulta un usuario regularmente, quitándole privacidad. Estos cookies se pueden aceptar o evitar en nuestros equipos, por medio de la configuración de privacidad de las opciones del navegador de Internet.

Crackers:

Son programas que monitorean las contraseñas en las aplicaciones de la máquina.

Además de referirse a hackers con malas intenciones, a los que se les conocen también como ladrones de contraseñas, se considera que lo hacen para demostrar su habilidad y satisfacer su vanidad, dañando la relativa seguridad del cifrado, en algunos casos dejando hasta su rúbrica, para hacer más palpable su osadía.

Cryptovirus, Ransomware o Secuestradores:

Es el programa que entra a la computadora y se instala, registra su estancia en dispositivos de almacenamiento extraíble (flash disks, pendrives, etc.) buscando y cifrando los archivos del registro del disco infectado, después borran los originales en forma inadvertidamente para el usuario, haciéndolos inaccesibles para el dueño y cuando se intenta abrir algún documento, a través de un archivo de texto que forma parte de este malware informa, como en el AIDS.exe: **"Si**



quiere obtener una clave para liberar el documento, ingrese 378 dólares a la cuenta en la ciudad de Panamá número X", o también se le solicita que se envíe el pago vía Internet (rescate), para obtener la clave de dicha codificación (la liberación del rehén). o bien simplemente impide el ingreso del usuario a su unidad de almacenamiento extraíble ocasionando el bloqueo temporal del sistema hasta la desconexión del dispositivo de la PC. Como en el "Cn911.exe" (aplicación encubierta como ejecutable que se instala en el registro de usuario y lo modifica.) La codificación es de claves simétricas simples, es decir son aquellas que utilizan la misma clave para cifrar y descifrar un documento lo que ocasiona la reducción de la capacidad de almacenamiento del disco extraíble, sin embargo algunos usuarios con conocimientos informáticos avanzados, descifran, cuáles son dichas claves y pueden llegar a recuperar la capacidad real del dispositivo, trucada por el malware.

Dialers:

Los dialers son programas que llaman a un número telefónico de larga distancia, o de tarifas especiales, para, a través del módem, entrar de forma automática y oculta para el usuario y sin su consentimiento, principalmente a páginas de juegos, adivinación o pornográficas, que van a reeditar en beneficio económico a los creadores del malware, pero que además al usuario le crean la obligación de pagar grandes tarifas por el servicio telefónico.

Existen en Internet páginas preparadas para descargar, instalar y ejecutar dialers de conexión y virus informáticos capaces de llevar a cabo todo lo anterior, con la desventaja de su rápida propagación.

Actualmente las conexiones por medio de banda ancha, han evitado estos problemas.

Exploit:

Exploit que evade a la mayoría de antivirus.

Un exploit es aquel software que ataca una vulnerabilidad particular de un sistema operativo. Los exploits no son necesariamente maliciosos –son



generalmente creados por investigadores de seguridad informática para demostrar que existe una vulnerabilidad. Y por esto son componentes comunes de los programas maliciosos como los gusanos informáticos.

Falso antivirus:

Hacen creer que es un antivirus gratuito y que la computadora ha sido detectada infectada, pero que para deshacerse de la infección deberá comprar la versión completa, y si trata de eliminar esta instalación del supuesto antivirus le informan que debe tener la clave de desinstalación, la cual deberá comprar.

Hijacker:

Programa que realiza cambios en la configuración de la página de inicio del navegador, que lo redirige a otras páginas de características indeseables como son las pornográficas y más peligrosamente a copias casi fieles de las bancarias.

Hoaxes, Jokes o Bulos:

Son bromas que semejan ser virus, pero que, ciertamente no lo son. Normalmente una persona conocida nuestra recibe una "alarma" de un supuesto virus y nos "hace el favor" de notificarnos para que tomemos precauciones en nuestro equipo.

El objetivo de la persona que inició el rumor o hoax se ha cumplido, al preocupar al usuario con la broma y que, en muchos casos, puede hacer al usuario auto eliminar algún supuesto archivo contaminado, lo cual podría afectar realmente al funcionamiento del sistema, llegando incluso a tener que reinstalarlo.

Keystroke o keyloggers:

Son programas espías, que toman el control de los equipos, para espiar y robar información, monitorea el sistema, registrando las pulsaciones del teclado, para robar las claves, tanto de páginas financieras y correos electrónicos como cualquier información introducida por teclado, en el equipo utilizado para saber lo que la víctima ha realizado como conversaciones que la misma tuvo, saber donde ha entrado, qué ha ejecutado, qué ha movido, etc.



Pueden ser también aparatos o dispositivos electrónicos colocados intencionalmente en equipos, que se intercalan entre el dispositivo y el computador.

Ladilla virtual:

Conocido como (virtual crab). Este tipo de programa maligno que, como analogía al parásito de transmisión sexual, entra en una computadora a través del sexo virtual, sitios pornográficos o cualquier aplicación relacionada. Los sitios web pornográficos suelen ser un gran caldo de cultivo para estos Malware virtuales.

Leapfrog:

Las ranas como también se conocen en español son programas que entran a los equipos para conocer las claves de acceso y las cuentas de correo almacenadas en la libreta de direcciones para ser utilizadas en la replicación de estos, a través de enviar copias del gusano.

Parásito Informático:

Este tipo de malware es el que se adhiere a archivos (especialmente ejecutables), como lo haría un parásito. Ese archivo ejecutable es denominado portador (o Host) y el parásito lo utiliza para propagarse. Si el programa es ejecutado, lo primero que se ejecuta es el parásito informático, y luego, para no levantar sospechas, se ejecuta el programa original. Muchas veces es aquí donde los parásitos fallan, porque hay programas que detectan estas modificaciones y lanzan errores (incluso errores de advertencias de presencia de malware).

Pharming:

Es el software maligno que suplanta el DNS, en el archivo host local, para conducirnos a una página Web falsa, con lo cual, al intentar entrar a un determinado nombre de dominio en nuestro navegador nos redirecciona al que el cracker, ha cambiado.

Por ejemplo la página de un banco pudiera ser www.bankito.com (xxx.156.24.196), nos lo cambia por www.banquita.com (YYY.132.30.60), con lo



que al parecerse, no nos percatamos normalmente que nos está enviando a otra página controlada por el bandido cibernético.

Para poder instalarnos la página que realizará el direccionamiento, se instalará en nuestro sistema algunos programas malware ejecutables, que recibimos a través de un correo electrónico, descargas por Internet, programas P2P, etc.

Siendo en este momento el más común el envío de una supuesta tarjeta de Gusanito.com, que al entrar en el vínculo contenido en el correo electrónico, no solo nos da la sorpresa de la tarjeta, sino que ha realizado la descarga correspondiente que se encargará de auto ejecutarse creando el host que redirecciona nuestro navegador a las IP de las páginas falsas administradas por el hacker.

Phishings:

Del inglés "fishing" (pescando), se utiliza para identificar la acción fraudulenta de conseguir información confidencial, vía correo electrónico o página web, con el propósito de que los usuarios de cuentas bancarias lo contesten, o entren a páginas aparentemente iguales a la del banco o de los portales con ingreso por contraseña.

El phishing se basa en el envío por parte de un estafador de un mensaje electrónico o enlace de una empresa supuestamente respetable. Éstas a menudo conducen a una página Web falsificada que han creado, y engañan al usuario para que introduzca su contraseña y su información personal. Así lo convierten en un blanco fácil del robo de información personal o financiera de manera electrónica utilizando el nombre de un tercero (banco) y últimamente las páginas del acceso a e-mails de compañías como Yahoo!.

Nunca debe darse información de cuentas bancarias por otros medios que no sea en las sucursales correspondientes al banco, ya que por medio de correos electrónicos con enlaces falsos, supuestamente del banco, pueden solicitar los números de cuentas y contraseña privados, con lo que se les está dando todo para que puedan cometer el fraude.



En falsas cartas bancarias:

- Se presiona al cliente con supuestas fallas en su información o en los servidores que es urgente atender.
- El documento puede contar con faltas de acentos ortográficos en palabras como línea, dirección, activación, cámbiela, etc.
- Para dar confianza al usuario se colocan botones e imágenes que le son conocidos por la página real y las advertencias usuales de la página de acceso normal.
- Para completar el engaño, advierte del envío de e-mails falsos, siendo en sí mismo uno de ellos.
- El medio para entrar a la página web suplantada puede ser "http://" (en lugar del real "https://")+ nombre de la página web (siendo ésta la dirección real a la que entramos normalmente) + "@" + dirección del sitio al que nos redirige.

Generador de claves dinámicas:

El método de entrar a las páginas Web de los diferentes Bancos de algunos países, es usando el generador de claves dinámicas de las compañías Aladdin y el RSA SecurID, con lo que se espera terminar con los Phishing.

Por lo tanto ahora el ataque de los pescadores de datos (fishing), es pidiéndole que sincronice su generador de claves, con lo que inmediatamente entran a la cuenta del usuario sacando lo que puedan y cambiando hasta las claves de acceso.

También Yahoo da protección por medio de la creación del llamado sello de acceso personalizado, que consiste en colocar una imagen o texto, el cual debe aparecer cada vez que se inicie sesión en Yahoo, en la computadora en que se ha colocado, pues se vincula a ella y no al usuario del correo. Si el sello de acceso **NO** está, es probable que sea una página falsificada creada por un estafador para robar los datos personales.



Pornware:

Describe programas que usan el Módem de la computadora para conectarse a servicios de pago por evento pornográfico o para bajar contenidos pornográficos de la Web. Es un caso particular de Dialers.

Es un auténtico fraude mediante información engañosa, manifiestan que es completamente gratuito, el sitio a visitar es en efecto sin costo, pero solo se tiene acceso por vía telefónica (MODEM), que resulta con una alta tarifa por minuto que se refleja en el recibo telefónico (por lo regular utilizan una clave de larga distancia internacional (900) con un cargo aproximado de \$20.00 USD por minuto). Esta técnica fraudulenta se utiliza también usando como señuelo videojuegos, salva pantallas, programas o cualquier otra falacia que requiera acceso mediante un MODEM telefónico.

Primero se descarga desde algún sitio que ofrece todo absolutamente gratis un pequeño programa ejecutable, que coloca en el escritorio de la PC un llamativo ícono para que cualquier incauto con un simple click haga el enlace mencionado, aparecen insistentes mensajes sugiriendo de que todo es completamente gratis y sin límite de tiempo.

Sin embargo, se están extinguiendo por dejarse de lado los Módems convencionales de 56Kbps, y usarse Tarifas Planas en Red Ethernet de Banda ancha o ADSL.

Rabbit o conejos:

Reciben este nombre algunos gusanos informáticos, cuyos códigos malignos llenan el disco duro con sus reproducciones en muy poco tiempo y que también pueden saturar el ancho de banda de una red rápidamente además de poder mandar un número infinito de impresiones del mismo archivo, colapsando la memoria de la impresora al saturarla.



Riskware:

Programas originales, como las herramientas de administración remota, que contienen agujeros usados por los crackers para realizar acciones dañinas.

Rootkit:

Los rootkits son programas que son insertados en una computadora después de que algún atacante ha ganado el control de un sistema. Los rootkit generalmente incluyen funciones para ocultar los rastros del ataque, como es borrar los log de entradas o encubrir los procesos del atacante. Los rootkit pueden incluir puertas traseras, permitiendo al atacante obtener de nuevo acceso al sistema o también pueden incluir exploits para atacar otros sistemas y evitan ser desinstalados o eliminados a toda costa, pues cuenta con protección para no permitirlo, con lo cual se convierte en un programa indeseable y molesto. Los rootkit se volvieron famosos a partir de uno que estaba incluido en un mecanismo anticopia en algunos CD de música de la empresa Sony.

Scumware o escoria:

Scumware o escoria es cualquier software que hace cambios significativos en la apariencia y funciones de las páginas Web sin permiso del Administrador (Webmaster) o propietarios. Por ejemplo, un número de productos sobreponen la publicidad de los banners con otros anuncios, a veces para los productos de la competencia. El Scumware puede agregar hyperlinks desautorizados a la sección opinión de una página Web - a veces usar de un usuario acoplamiento a los sitios posiblemente desagradables. Tales programas pueden interferir con hipervínculos (hyperlinks) existentes agregando otros destinos a los previstos. A veces, el Scumware es conocido como thiefware.

Spam:

Se le llama spam a los e-mails basura, que son enviados masivamente a direcciones electrónicas compradas por empresas con la finalidad de vender sus productos.



Últimamente han surgido páginas con mensajes que aparecen en un corto instante de tiempo (efecto *flash*) tratando de producir en el inconsciente de la mente la necesidad de comprar el producto anunciado como si de un mensaje subliminal se tratara.

Actualmente existen filtros que bloquean los spam en la mayoría de los servidores de correo, además de existir ya legislación contra los spam, México cuenta desde el 2000, con una ley en donde se prohíben las prácticas comerciales no solicitadas por correo electrónico, además de artículos en la Ley Federal de Protección al Consumidor, que regulan el comercio electrónico, aunque los spam son enviados desde otros países para evadir éstas y otras restricciones mundiales.

Se calcula que alrededor del 75% del correo electrónico que circula en la red son spam, pero podemos observar que tiene variaciones mensualmente. Sophos, en su lista "Dirty dozen spam relaying countries", incluye una categoría de generación de spam por país con estos porcentajes: United States 23.2%, China (inc. Hong Kong) 20.0%, Corea 7.5%, Francia 5.2%, España 4.8%, Polonia 3.6% , Brasil 3.1%, Italia 3.0%, Alemania 2.5%, Inglaterra 1.8%, Taiwán 1.7%, Japón 1.6%, Otros 22.0%.

Spyware:

Los Spywares o Programa espía, son aplicaciones que se dedican a recopilar información del sistema en el que se encuentran instaladas ("husmean" la información que está en nuestro equipo) para luego enviarla a través de Internet, generalmente a alguna empresa de publicidad en algunos casos lo hacen para obtener direcciones de e-mail. Todas estas acciones se enmascaran tras confusas autorizaciones al instalar programas de terceros, por lo que rara vez el usuario es consciente de ello. Estos agentes espía, pueden ingresar a la PC por medio de otras aplicaciones. Normalmente trabajan y contaminan sistemas como lo hacen los Caballos de Troya.



Ventanas emergentes/POP-UPS:

Son, generalmente, ventanas muy molestas que aparecen al navegar y muestran publicidad o información que es difícil de eliminar y que aparece constantemente.

Son una forma en línea de publicidad en el World Wide Web, que aumentan el tráfico de la red o que son también usadas para capturar direcciones de e-mail. Trabaja cuando ciertos sitios abren una ventana del buscador para exhibir los anuncios.

La ventana pop-up que contiene un anuncio es generada normalmente por JavaScript, pero se puede generar por otros medios también.

Una variante en las ventanas pop-up es hacer aparecer el anuncio debajo de la ventana activa o en direcciones fuera del área visual, normalmente en la parte inferior derecha, y suelen aparecer como intentos de abrir una página nueva durante unos milisegundos, hasta cargarse y cumplir su cometido, cerrándose inmediatamente, con lo cual el usuario no se percató cuando surge, sino hasta que cierra su navegación, con lo que difícilmente puede identificar junto a que página surgió, sobre todo en aquellas sesiones en que se tienen varios documentos abiertos.

Worms o gusanos:

Los **gusanos** informáticos son similares a los virus, pero los gusanos no dependen de archivos portadores para poder contaminar otros sistemas. Estos pueden modificar el sistema operativo con el fin de auto ejecutarse como parte del proceso de inicialización del sistema. Para contaminar otros sistemas, los gusanos explotan vulnerabilidades del objetivo o utilizan algún tipo de ingeniería social para engañar a los usuarios y poderse ejecutar.

El caso más conocido es el del gusano Blaster que se distribuyó por internet rápidamente gracias a una vulnerabilidad de Windows, que reiniciaba al ordenador al cabo de 1 minuto, e intentaba infectar a una infinidad de



computadores cercanos a la máquina (en redes locales) y lejanos (en internet) de forma aleatoria.

Métodos de protección.

- Usar sistemas operativos más seguros, mejores y efectivos que windows como GNU/Linux, Mac OS o FreeBSD.
- Utilizar una cuenta de usuario con pocos privilegios (no administrador) en su equipo, solo utilizar la cuenta de administrador cuándo se deba cambiar una configuración o instalar un software de confianza. De todas maneras, se debe ser cauteloso con lo que se ejecuta.
- Cada vez que se transfiera un archivo desde o hacia Internet se debe tener la precaución de revisarlo contra virus, crimeware o malwares, pero lo más importante saber de dónde proviene.
- Se debe comprobar todos y cada uno de los medios magnéticos (Diskettes, ya en desuso), soportes ópticos (CDS, DVD, Blu-ray) o tarjetas de memoria (SD, MMC, XD, compact Flash), que se introduzcan en el ordenador.
- Comprobar los archivos comprimidos (ZIP, RAR, ACE, CAB, 7z..).
- Hacer copias de respaldo de programas y documentos importantes, pueden ser guardados en un Pendrive, CD, DVD, entre otros medios externos.
- No instalar programas de dudoso origen.
- Evitar navegar por sitios potencialmente dañinos buscando cosas como "pornografía", "programas gratis", "mp3 gratis", claves, licencias o cracks para los programas comerciales.
- Evita descargar programas, archivos comprimidos o ejecutables, desde redes peer-to-peer ya que no se sabe el real contenido de la descarga.
- Crear una contraseña de alta seguridad.
- Mantener las actualizaciones automáticas activadas, como por ejemplo el Windows Update.
- Tener un programa antivirus y un firewall (también llamados cortafuegos) instalados en el ordenador, un anti-espías como SpywareBlaster, Spybot - Search & Destroy, y un filtrador de IP' maliciosas como el PeerGuardian. que eventualmente también frena troyanos.



- También es importante tener actualizados estos programas ya que cada día aparecen nuevas amenazas.
- Desactivar la interpretación de Visual Basic VBS y permitir JavaScript JS, ActiveX y cookies sólo en páginas web de confianza.
- Seguir las políticas de seguridad en cómputo

PARCHE (INFORMÁTICA)²⁷

En informática, un **parche** es una sección de código que se introduce a un programa. Dicho código puede tener varios objetivos; sustituir código erróneo, agregar funcionalidad al programa, aplicar una actualización, etc.

Los parches suelen ser desarrollados por programadores ajenos al equipo de diseño inicial del proyecto (aunque no es algo necesariamente cierto). Como los parches se pueden aplicar tanto a un binario ejecutable como al código fuente, cualquier tipo de programa, incluso un sistema operativo, pueden ser objeto de un parche.

El origen del nombre probablemente se deba a la utilidad de Unix llamada **patch** creada por Larry Wall.

Tipos según el código

Parches a archivos binarios.

A menudo un parche consiste en una actualización del archivo ejecutable de un programa. En este caso, el archivo binario es modificado para añadir los cambios o completamente reemplazado.

El tamaño de los parches es variable. Algunos parches solamente modifican un archivo binario de la aplicación pero otros alteran mucho más contenido. Si el parche sólo modifica el ejecutable, puede ser muy pequeño (por debajo del megabyte). La instalación de parches solía ser una tarea tediosa, y con

²⁷ Wikipedia. Enciclopedia libre "[http://es.wikipedia.org/wiki/Parche_\(inform%C3%A1tica\)](http://es.wikipedia.org/wiki/Parche_(inform%C3%A1tica))"



mucha posibilidad de error. Un error solía significar tener que reinstalar la aplicación y el parche. Hoy en día, la instalación de parches se realiza en muchos casos por programas especiales de forma automática.

Históricamente, los parches eran distribuidos en cintas o en tarjetas perforadas, que se debía cortar la cinta original y reemplazar ese pedazo de programa con el nuevo. La similitud de este proceso con el que pueda usar un costurero a la hora de remendar una pieza es lo que dio el nombre de parche.

Después de esto se distribuyeron en cintas magnéticas, disquetes o más tarde en CD-ROM. Con un acceso cada vez más común en Internet, la mayoría de los parches se distribuyen y pueden ser descargadas de las páginas web de los desarrolladores de las aplicaciones.

Varias compañías de software han desarrollado herramientas para ayudar en la tarea de aplicar un parche a una aplicación binaria. Pocket Soft desarrolló RTPatch. WinZip tiene una utilidad de autoextracción que lanza un programa capaz de aplicar un parche.

Algunos programas pueden actualizarse ellos mismos por medio de Internet con muy poca o nula intervención del usuario. Es muy popular que el mantenimiento de los sistemas operativos se haga de esta manera. En situaciones donde los administradores de sistemas controlan un cierto número de computadoras, esta manera de automatización ayuda a mantener la consistencia. La aplicación de parches de seguridad comúnmente ocurre de esta forma.

Parches al código fuente.

Estos parches se aplican directamente al código fuente del que constan las aplicaciones en vez de a la versión compilada de las mismas, por lo tanto un programador podrá saber qué nuevas características añade el parche.

Por ejemplo, en el desarrollo del sistema operativo Linux, que publica todo su código libremente, Linus Torvalds, su autor original, recibe cientos de miles de parches desde muchos programadores para que los aplique en su versión. En estos proyectos de código libre, es común que los autores reciban parches o que



mucha gente publique parches de forma autónoma que arreglan ciertos problemas o añaden ciertas funcionalidades.

El servidor web más usado en la actualidad, Apache, evolucionó como un conjunto de parches que los encargados de páginas web creaban para añadir cierta funcionalidad. Además, su nombre deriva del hecho de que sea un conjunto de parches.

Tipos según su propósito

Parches de depuración.

El objetivo de este tipo de parches es reparar bugs, o errores de programación que no fueron detectados a tiempo en su etapa de desarrollo. Se dice que un programa que se lanza con una alta probabilidad de contener este tipo de errores se le llama versión beta.

Parches de seguridad.

Los parches de seguridad solucionan agujeros de seguridad y, siempre que es posible, no modifican la funcionalidad del programa. Los parches de seguridad son especialmente frecuentes en aplicaciones que utilizan la red.

Parches de actualización.

Consiste en modificar un programa para convertirlo en un programa que utilice metodologías más nuevas. Por ejemplo, optimizar en tiempo cierto programa, utilizar algoritmos mejorados, añadir funcionalidades, eliminar secciones obsoletas de software, etc.



La importancia de actualizar²⁸

Muchos sostienen que la creación del software es más un arte que una técnica. Esto era especialmente cierto hace unas décadas donde se carecía de las herramientas tecnológicas y metodologías existentes hoy en día para el desarrollo de software. Lo cierto es que en este llamado “arte” de crear software la seguridad no figuraba como un objetivo a seguir y finalmente lo que se buscaba era una aplicación funcional que le sirviera al usuario.

Esta manera de desarrollar aplicaciones funcionales (y no forzosamente seguras) permaneció por mucho tiempo en el mundo del desarrollo de software, no sólo en las aplicaciones creadas por y para una empresa en particular, sino en el software comercial como lo son los sistemas operativos, aplicaciones de ofimática, navegadores o reproductores de música digital. Actualmente las metodologías y herramientas tecnológicas empiezan a considerar cada vez más el factor de seguridad dado que para muchos desarrolladores de software ya no es suficiente codificar programas funcionales sino también seguros. Lo anterior obedece a que cada vez más la seguridad en las aplicaciones es vista como un valor agregado apreciado por los clientes.

En nuestros días, el auge del comercio electrónico y la posibilidad de hacer transacciones financieras en línea ha hecho mucho más necesario que tanto el sistema operativo como las aplicaciones que corren en él sean lo más seguras posibles. Y es que en la práctica resulta difícil desarrollar software seguro, por lo que los fabricantes de software han optado por crear actualizaciones o parches a

²⁸ [Fausto Cepeda](#) ingeniero en Sistemas Computacionales por el ITESM, CCM. Es Maestro de Seguridad de la Información por la Universidad de Londres en el Reino Unido. Ha sido Consultor de Seguridad y actualmente es Analista de Sistemas en la Oficina de Seguridad Informática del Banco de México. También cuenta con la certificación de seguridad CISSP (Certified Information Systems Security Professional).

<http://blog.netmedia.info/index.php/2008/02/27/la-importancia-de-actualizar/>



sus sistemas operativos y aplicaciones con el fin de resolver problemas de seguridad (vulnerabilidades).

Para los usuarios, dos de los principales problemas inherentes a un esquema de “parchado” son:

- * saber de la existencia de la actualización para poder aplicarla.
- * disponer del parche antes de que existan ataques que afecten la seguridad.

Para el primer caso, un usuario se enfrenta a la problemática de seguirle la pista a varias decenas de aplicaciones instaladas en su equipo con el fin de informarse sobre las últimas actualizaciones de seguridad. Si corremos con suerte, la aplicación notificará automáticamente sobre la existencia de un nuevo parche para que efectuemos su instalación (como lo es el caso de por ejemplo Adobe Reader para leer documentos tipo PDF). Algunos sistemas operativos como Windows Vista y Windows XP inclusive se pueden configurar para que se actualicen sin notificación previa y llevan a cabo la instalación del o los parches sin más intervención del usuario. Sin embargo existen muchos programas que no tienen estas funcionalidades, dejando al usuario la responsabilidad de estar al tanto de nuevas actualizaciones. Lo recomendable es ingresar al menos una vez al mes a sitios como www.cert.org, www.cert.org.mx o www.secunia.com, donde se listan las últimas actualizaciones de parches para varias aplicaciones (junto con la liga para descargar el parche y un análisis del impacto de la debilidad). Otra opción más sencilla es ingresar a sitios gratuitos como www.f-secure.com/healthcheck/ donde después de analizar el equipo, se informa de las actualizaciones que hacen falta. Es una tarea tediosa pero es necesaria si es que deseamos eliminar las inseguridades de nuestro equipo de cómputo y minimizar el riesgo de que un atacante aproveche una vulnerabilidad que resulte en diversas consecuencias indeseables.

Para el segundo problema que se refiere a disponer de un parche antes de que exista un ataque, los usuarios se enfrentan a la difícil situación de que se conozca públicamente una debilidad y que el fabricante no emita ningún parche de seguridad, dejando indefenso al usuario a la merced de posibles ataques. Al



respecto, la empresa eEye publica un listado de todos aquellos programas que tienen un problema de seguridad públicamente conocido y que no cuentan con una solución (<http://research.eeye.com/html/alerts/zeroday/index.html>). Ante esta realidad, seguir las llamadas “mejores prácticas” puede ser de mucha utilidad, como lo es tener un firewall personal, un antivirus actualizado y una actitud preventiva ante los ataques que nos tratan de engañar (phising).

La problemática del esquema de “parchado” anteriormente descrita se puede ilustrar de manera muy clara con un ejemplo que recientemente se publicó en diversos sitios especializados en Internet. Entre diciembre del año pasado y enero del presente empezaron a circular diversos correos electrónicos diciendo que nos habían enviado una tarjeta de felicitación virtual; una variante también llegó por correo ofreciendo la lectura de una noticia importante de un periódico de México. Ambos correos solicitaban al usuario hacer “click” en una liga proporcionada en el correo ya sea para ver la tarjeta o la noticia en cuestión. Una vez hecho esto, la próxima vez que deseáramos ingresar a la banca en línea en el sitio financiero www.banamex.com, seríamos dirigidos automáticamente a un sitio fraudulento. ¿Cómo es esto posible? Aún teniendo el sistema operativo y aplicaciones actualizadas, el ataque era exitoso.

La razón es que los defraudadores habían encontrado una vulnerabilidad en el módem inalámbrico de la marca “2Wire”, que en México ofrece el servicio Prodigy Infitum a sus clientes. Al hacer “click” en la liga de los correos ya mencionados, se llevaba a cabo un cambio en la configuración del módem. Esta debilidad permite a una persona mal intencionada atacar a este dispositivo, lo cual significa que aunque el usuario escriba en su navegador correctamente un sitio como lo es “www.banamex.com”, se mostrará el contenido de un sitio falso que en apariencia es similar al original. Una vez que el usuario ingresaba al sitio falso, se intentaba descargar un virus para robar las contraseñas de acceso al sitio bancario. Otros ataques podrían haber solicitado simplemente las contraseñas de acceso en el sitio falso sin intentar la infección con un virus. Aunque el ataque se centró en Banamex, no se descartó que se aprovechara este tipo de vulnerabilidad para otros sitios.



La vulnerabilidad del módem inalámbrico era públicamente conocida e inclusive existían ataques que se aprovechaban de ella, sin embargo eran pocas las personas que conocían de este problema y el fabricante no tenía disponible un parche o actualización, dejando a miles de usuarios de este servicio de banda ancha indefensos. Afortunadamente el fabricante publicó los parches correspondientes y Prodigy Infinitum confirmó que se distribuirían durante el mes de febrero de manera automática para varios de los modelos de la marca en cuestión.

Este ejemplo del módem inalámbrico ilustra claramente la problemática de mantenerse al día en cuestiones de parches de seguridad no sólo del sistema operativo y aplicaciones, sino hasta del módem inalámbrico que se usa. Seguir ciertas precauciones de seguridad pueden ser de utilidad para evitar estos riesgos. Para este caso específico del módem puede no ser suficiente el hecho de contar con un antivirus o firewall personal, sino que se deberán seguir medidas adicionales como lo puede ser la verificación de la validez del certificado digital de los sitios bancarios que se visiten, comprobando que el certificado esté a nombre de Banamex y que no muestre ningún error. Esto último se logra al hacer doble “click” en el candado cerrado que se habilita en el navegador antes de enviar las contraseñas de acceso a la banca en línea.

Independientemente de este ataque al módem inalámbrico, es una buena práctica siempre efectuar esta verificación en sitios que involucren transacciones financieras.

4. Seguridad de la información y seguridad informática.

SEGURIDAD DE LA INFORMACIÓN²⁹

Seguridad de la Información tiene como fin la protección de la información y de los sistemas de la información del acceso, uso, divulgación, interrupción o destrucción no autorizada.

²⁹ http://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n



El término Seguridad de Información, Seguridad informática y garantía de la información son usados con frecuencia y aunque su significado no es el mismo, persiguen una misma finalidad al proteger la **Confidencialidad, Integridad y Disponibilidad** de la información; Sin embargo entre ellos existen algunas diferencias sutiles. Estas diferencias radican principalmente en el enfoque, las metodologías utilizadas, y las zonas de concentración.

La Seguridad de la Información se refiere a la **Confidencialidad, Integridad y Disponibilidad** de la información y datos, independientemente de la forma los datos pueden tener: electrónicos, impresos, audio u otras formas.

Principios Básicos.

Los Gobiernos, entidades militares, instituciones financieras, los hospitales y las empresas privadas acumulan una gran cantidad de información confidencial sobre sus empleados, clientes, productos, investigación y su situación financiera. La mayor parte de esta información es recolectada, tratada, almacenada y puesta a la disposición de sus usuarios, en computadoras y transmitida a través de las redes entre los ordenadores.

En caso de que la información confidencial de una empresa, sus clientes, sus decisiones, su estado financiero o nueva línea de productos caigan en manos de un competidor; se vuelva pública de forma no autorizada, podría ser causa de la pérdida de credibilidad de los clientes, pérdida de negocios, demandas legales o incluso la quiebra de la misma.

Por lo que proteger la información confidencial es un requisito del negocio, y en muchos casos también un imperativo ético y una obligación legal.

Para el individuo común, la Seguridad de la Información tiene un efecto significativo respecto a su privacidad, la que puede cobrar distintas dimensiones dependiendo de la cultura del mismo.



Conceptos Importantes.

Por más de veinte años la Seguridad de la Información ha declarado que la confidencialidad, integridad y disponibilidad (conocida como la Tríada CIA, del inglés: "**C**onfidentiality, **I**ntegrity, **A**vailability") son los principios básicos de la seguridad de la información.

La correcta Gestión de la Seguridad de la Información busca establecer y mantener programas, controles y políticas, que tengan como finalidad conservar la confidencialidad, integridad y disponibilidad de la información.

Confidencialidad:

La confidencialidad es la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados.

Por ejemplo, una transacción de tarjeta de crédito en Internet requiere que el número de tarjeta de crédito a ser transmitida desde el comprador al comerciante y el comerciante de a una red de procesamiento de transacciones. El sistema intenta hacer valer la confidencialidad mediante el cifrado del número de la tarjeta y los datos que contiene la banda magnética durante la transmisión de los mismos. Si una parte no autorizada obtiene el número de la tarjeta en modo alguno, se ha producido una violación de la confidencialidad.

La pérdida de la confidencialidad de la información puede adoptar muchas formas. Cuando alguien mira por encima de su hombro, mientras usted tiene información confidencial en la pantalla, cuando se publica información privada, cuando un laptop con información sensible sobre una empresa es robado, cuando se divulga información confidencial a través del teléfono, etc. Todos estos casos pueden constituir una violación de la confidencialidad.

Integridad:

Para la Seguridad de la Información, la integridad es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. (No es igual a integridad referencial en bases de datos.) La violación de integridad se presenta



cuando un empleado, programa o proceso (por accidente o con mala intención) modifica o borra los datos importantes que son parte de la información.

Disponibilidad:

La Disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

En el caso de los sistemas informáticos utilizados para almacenar y procesar la información, los controles de seguridad utilizados para protegerlo, y los canales de comunicación protegidos que se utilizan para acceder a ella deben estar funcionando correctamente. La Alta disponibilidad sistemas objetivo debe seguir estando disponible en todo momento, evitando interrupciones del servicio debido a cortes de energía, fallos de hardware, y actualizaciones del sistema.

Garantizar la disponibilidad implica también la prevención de ataque Denegación de servicio.

Otros conceptos relacionados son:

- **Auditabilidad:** Permitir la reconstrucción, revisión y análisis de la secuencia de eventos
- **Identificación:** verificación de una persona o cosa; reconocimiento.
- **Autenticación:** Proporcionar una prueba de identidad; puede ser algo que se sabe, que se es, se tiene o una combinación de todas.
- **Autorización:** Lo que se permite cuando se ha otorgado acceso
- **No repudio:** no se puede negar un evento o una transacción.
- **Seguridad en capas:** La defensa a profundidad que contenga la inestabilidad
- **Control de Acceso:** limitar el acceso autorizado solo a entidades autenticadas
- **Métricas de Seguridad, Monitoreo:** Medición de actividades de seguridad
- **Gobierno:** proporcionar control y dirección a las actividades
- **Estrategia:** los pasos que se requieren para alcanzar un objetivo
- **Arquitectura:** el diseño de la estructura y las relaciones de sus elementos



- **Gerencia:** Vigilar las actividades para garantizar que se alcancen los objetivos
- **Riesgo:** la explotación de una vulnerabilidad por parte de una amenaza
- **Exposiciones:** Áreas que son vulnerables a un impacto por parte de una amenaza
- **Vulnerabilidades:** deficiencias que pueden ser explotadas por amenazas
- **Amenazas:** Cualquier acción o evento que puede ocasionar consecuencias adversas
- **Riesgo residual:** El riesgo que permanece después de que se han implementado contra medidas y controles
- **Impacto:** los resultados y consecuencias de que se materialice un riesgo
- **Criticidad:** La importancia que tiene un recurso para el negocio
- **Sensibilidad:** el nivel de impacto que tendría una divulgación no autorizada
- **Análisis de impacto al negocio:** evaluar los resultados y las consecuencias de la inestabilidad
- **Controles:** Cualquier acción o proceso que se utiliza para mitigar el riesgo
- **Contra medidas:** Cualquier acción o proceso que reduce la vulnerabilidad
- **Políticas:** declaración de alto nivel sobre la intención y la dirección de la gerencia
- **Normas:** Establecer los límites permisibles de acciones y procesos para cumplir con las políticas
- **Ataques:** tipos y naturaleza de inestabilidad en la seguridad
- **Clasificación de datos:** El proceso de determinar la sensibilidad y Criticidad de la información

Tecnologías .

Las principales tecnologías referentes a la seguridad de la información son:³

- Cortafuegos
- Administración de cuentas de usuarios
- Detección y prevención de intrusos
- Antivirus
- Infraestructura de llave pública
- Capas de Socket Segura (SSL)



- Conexión única "Single Sign on- SSO"
- Biometría
- Cifrado
- Cumplimiento de privacidad
- Acceso remoto
- Firma digital
- Intercambio electrónico de Datos "EDI" y Transferencia Electrónica de Fondos "EFT"
- Redes Virtuales Privadas "VPNs"
- Transferencia Electrónica Segura "SET"
- Informática Forense
- Recuperación de datos
- Tecnologías de monitoreo

Estándares de seguridad de la información

- [ISO/IEC 27000-series](#)
- [ISO/IEC 27001](#)
- [ISO/IEC 17799](#)

Otros estándares relacionados

- [COBIT](#)
- [ISACA](#)
- [ITIL](#)

Certificaciones

- CISM - CISM Certificaciones : Certified Information Security Manager
- CISSP - CISSP Certificaciones : Security Professional Certification
- [GIAC](#) - GIAC Certificaciones : Global Information Assurance Certification

Certificaciones independientes en seguridad de la información

- CISA- Certified Information Systems Auditor , [ISACA](#)
- CISM- Certified Information Security Manager, [ISACA](#)



- **Lead Auditor ISO27001** - Lead Auditor ISO 27001, **BSI**
- **CISSP** - Certified Information Systems Security Professional, **ISC2**
- **SECURITY+**, **COMPTia** - Computing Technology Industry Association
- **CEH** - Certified Ethical Hacker
- **PCI DSS** - PCI Data Security Standard

SEGURIDAD EN INTERNET³⁰.

Intentar comunicar un secreto en un entorno con millones de testigos potenciales como Internet es difícil, y la probabilidad de que alguien escuche una conversación entre dos interlocutores se incrementa conforme lo hace la distancia que las separa. Dado que Internet es verdaderamente global, ningún secreto de valor debería ser comunicado a través de ella sin la ayuda de la criptografía.

En el mundo de los negocios, información como números de tarjetas de crédito, autenticaciones de clientes, correos electrónicos e incluso llamadas telefónicas acaba siendo enrutada a través de Internet. Ya que gran parte de esta información corporativa no debe ser escuchada por terceras personas, la necesidad de seguridad es obvia.

Sin embargo, la **Seguridad en Internet** no es sólo una preocupación empresarial. Toda persona tiene derecho a la privacidad y cuando ésta accede a Internet su necesidad de privacidad no desaparece. La privacidad no es sólo confidencialidad, sino que también incluye anonimato. Lo que leemos, las páginas que visitamos, las cosas que compramos y la gente a la que hablamos representan información que a la mayoría de las personas no les gusta dar a conocer. Si las personas se ven obligadas a exponer información que normalmente desean ocultar por el hecho de conectarse a Internet, probablemente rechazarán todas las actividades relacionadas con la red.

Los tipos de agresión a la seguridad de un sistema de computadores o de redes se caracterizan mejor observando la función del sistema como proveedor de información. En general, existe un flujo de información desde un origen, como

³⁰ http://es.wikipedia.org/wiki/Seguridad_en_Internet



puede ser un fichero o una región de memoria principal, a un destino, como otro fichero o un usuario.

Hay cuatro tipos de agresión:

Interrupción: un recurso del sistema se destruye o no llega a estar disponible o se inutiliza. Ésta es una agresión de disponibilidad. Ejemplos de esto son la destrucción de un elemento hardware (un disco duro), la ruptura de una línea de comunicación o deshabilitar el sistema de gestión de ficheros.

Intercepción: un ente no autorizado consigue acceder a un recurso. Ésta es una agresión a la confidencialidad. El ente no autorizado puede ser una persona, un programa o un computador. Ejemplos de agresiones a la confidencialidad son las intervenciones de las líneas para capturar datos y la copia ilícita de ficheros o programas.

Modificación: un ente no autorizado no solamente gana acceso sino que deteriora el recurso. Ésta es una agresión a la integridad. Algunos ejemplos son los cambios de valores en un fichero de datos, alterando un programa para que funcione de una forma diferente, y modificando el contenido de los mensajes que se transmiten en una red.

Fabricación: una parte no autorizada inserta objetos falsos en el sistema. Esta es una agresión a la autenticidad. Un ejemplo sería la incorporación de registros a un fichero.

ATAQUES PASIVOS.

Las agresiones pasivas son el tipo de las escuchas o monitorizaciones ocultas de las transmisiones. La meta del oponente es obtener información que está siendo transmitida. Existen dos tipos de agresiones: **divulgación del contenido de un mensaje** o **análisis del tráfico**.

La **divulgación del contenido de un mensaje** se entiende fácilmente. Una conversación telefónica, un mensaje de correo electrónico o un fichero transferido



pueden contener información sensible o confidencial. Así, sería deseable prevenir que el oponente se entere del contenido de estas transmisiones.

El segundo tipo de agresión pasiva, el **análisis del tráfico**, es más sutil. Suponga que tenemos un medio de enmascarar el contenido de los mensajes u otro tipo de tráfico de información, aunque se capturan los mensajes, no se podría extraer la información del mensaje. La técnica más común para enmascarar el contenido es el cifrado. Pero incluso si tenemos protección de cifrado, el oponente podría ser capaz de observar los modelos de estos mensajes. El oponente podría determinar la localización y la identidad de los computadores que se están comunicando y observar la frecuencia y la longitud de los mensajes intercambiados. Esta información puede ser útil para extraer la naturaleza de la comunicación que se está realizando.

Las agresiones pasivas son muy difíciles de detectar ya que no implican la alteración de los datos. Sin embargo, es factible impedir el éxito de estas agresiones. Así, el énfasis para tratar estas agresiones está en la prevención antes que la detección.

ATAQUES ACTIVOS.

La segunda categoría de agresiones es la de las agresiones activas. Estas agresiones suponen la modificación del flujo de datos o la creación de flujos falsos y se subdivide en 4 categorías: **enmascaramiento**, **repetición**, **modificación de mensajes** y **denegación de un servicio**.

Un **enmascaramiento** tiene lugar cuando una entidad pretende ser otra entidad diferente. Una agresión de enmascaramiento normalmente incluye una de las otras formas de agresión activa. Por ejemplo, se puede captar una secuencia de autenticación y reemplazarla por otra secuencia de autenticación válida, así se habilita a otra entidad autorizada con pocos privilegios a obtener privilegios extras suplantando a la entidad que los tiene.

La **repetición** supone la captura pasiva de unidades de datos y su retransmisión subsiguiente para producir un efecto no autorizado.



La **modificación de mensajes** significa sencillamente que alguna porción de un mensaje legítimo se altera, o que el mensaje se retrasa o se reordena para producir un efecto no autorizado.

La **denegación de un servicio** impide o inhibe el uso o gestión normal de las facilidades de comunicación. Esta agresión puede tener un objetivo específico: por ejemplo, una entidad puede suprimir todos los mensajes dirigidos a un destino particular. Otro tipo de denegación de servicio es la perturbación sobre una red completa, deshabilitándola o sobrecargándola con mensajes de forma que se degrade su rendimiento.

Las agresiones activas presentan características opuestas a las agresiones pasivas. Mientras que una agresión pasiva es difícil de detectar, existen medidas disponibles para prevenirlas. Por otro lado, es bastante difícil prevenir una agresión activa, ya que para hacerlo se requeriría protección física constante de todos los recursos y de todas las rutas de comunicación. Por consiguiente, la meta es detectarlos y recuperarse de cualquier perturbación o retardo causados por ellos. Ya que la detección tiene un efecto disuasivo, también puede contribuir a la prevención.

Medidas de seguridad en la red.

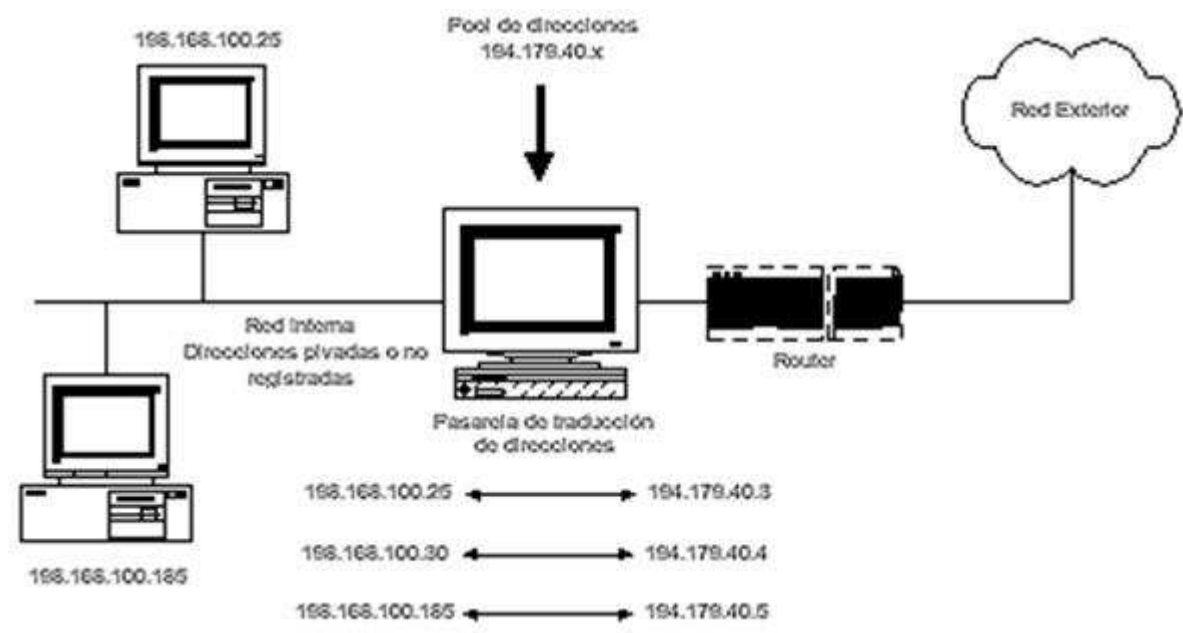
Existen numerosas técnicas para proteger la integridad de los sistemas. Lo primero que se debe hacer es diseñar una política de seguridad. En ella, definir quiénes tienen acceso a las diferentes partes de la red, poner protecciones con contraseñas adecuadas a todas las cuentas y preocuparse de hacerlas cambiar periódicamente (Evite las passwords “por defecto” o demasiado obvias).

Firewalls.

Existen muchas y muy potentes herramientas de cara a la seguridad de una red informática. Una de las maneras drásticas de no tener invasores es la de poner murallas. Los mecanismos más usados para la protección de la red interna de otras externas son los firewalls o cortafuegos. Estos tienen muchas aplicaciones, ente las más usadas está:

Packet filter (filtro de paquetes). Se basa en el tratamiento de los paquetes IP a los que aplica unas reglas de filtrado que le permiten discriminar el tráfico según nuestras indicaciones.

Normalmente se implementa mediante un router. Al tratar paquetes IP, los filtros que podremos establecer serán a nivel de direcciones IP, tanto fuente como destino.



Cortafuegos filtro de paquetes ejemplarizado en un router.

La lista de filtros se aplican secuencialmente, de forma que la primera regla que el paquete cumpla marcará la acción a realizar (descartarlo o dejarlo pasar). La aplicación de las listas de filtros se puede hacer en el momento de entrada del paquete o bien en el de salida o en ambos.

La protección centralizada es la ventaja más importante del filtrado de paquetes. Con un único enrutador con filtrado de paquetes situado estratégicamente puede protegerse toda una red.

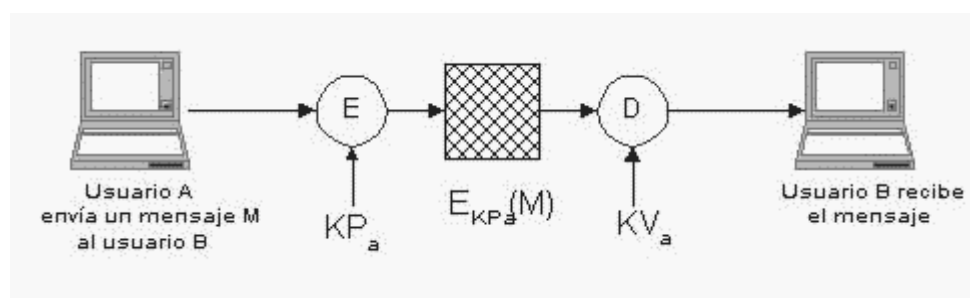
Firma digital.

El cifrado con clave pública permite generar firmas digitales que hacen posible certificar la procedencia de un mensaje, en otras palabras, asegurar que proviene de quien dice. De esta forma se puede evitar que alguien suplante a un usuario y envíe mensajes falsos a otro usuario, por la imposibilidad de falsificar la firma. Además, garantizan la integridad del mensaje, es decir, que no ha sido alterado durante la transmisión. La firma se puede aplicar a un mensaje completo o puede ser algo añadido al mensaje.

Las firmas son especialmente útiles cuando la información debe atravesar redes sobre las que no se tiene control directo y en consecuencia, no existe posibilidad de verificar de otra forma la procedencia de los mensajes.

Existen varios métodos para hacer uso de la firma digital, uno de ellos es el siguiente: “quien envía el mensaje lo codifica con su clave privada. Para descifrarlo, sólo puede hacerse con la clave pública correspondiente a dicha persona o institución. Si efectivamente con dicha clave se descifra es señal de que quien dice que envió el mensaje, realmente lo hizo”.

Firma digital formada encriptando con la clave privada del emisor:



Firma Digital y Autenticación

E: Encriptar / D: Desencriptar

KP: Encriptación utilizando la Clave Privada.

KV: Encriptación utilizando la Clave Pública.

M: Mensaje

Seguridad en WWW.



SEGURIDAD Y PROTECCIÓN EN COMPUTACIÓN³¹

Es necesario hacer una distinción entre seguridad y protección. El problema de la seguridad consiste en lograr que los recursos de un sistema sean, bajo toda circunstancia, utilizados para los fines previstos. Para eso se utilizan mecanismos de protección.

Los sistemas operativos proveen algunos mecanismos de protección para poder implementar políticas de seguridad. Las políticas definen qué hay que hacer (qué datos y recursos deben protegerse de quién; es un problema de administración), y los mecanismos determinan cómo hay que hacerlo. Esta separación es importante en términos de flexibilidad, puesto que las políticas pueden variar en el tiempo y de una organización a otra. Los mismos mecanismos, si son flexibles, pueden usarse para implementar distintas políticas.

Los mecanismos que ofrece el sistema operativo necesariamente deben complementarse con otros de carácter externo. Por ejemplo, impedir el acceso físico de personas no autorizadas a los sistemas es un mecanismo de protección cuya implementación no tiene nada que ver con el sistema operativo.

Un aspecto importante de la seguridad es el de impedir la pérdida de información, la cual puede producirse por diversas causas: fenómenos naturales, guerras, errores de hardware o de software, o errores humanos. La solución es una sola: mantener la información respaldada, de preferencia en un lugar lejano.

Otro aspecto importante de la seguridad, es el que tiene que ver con el uso no autorizado de los recursos:

Lectura de datos.

Modificación de datos.

Destrucción de datos.

Uso de recursos: ciclos de CPU, impresora, almacenamiento.

³¹ Francisco Armando Dueñas Rodríguez fduenas_farroba@hotmail.com



Aquí el sistema operativo juega un rol fundamental, ofreciendo mecanismos de autorización y autenticación.

Protección absoluta contra uso malicioso de los sistemas es imposible, pero si los costos de violar un sistema son superiores a los potenciales beneficios que se pueden obtener, entonces el sistema puede considerarse seguro. El problema es que esa protección no obstaculice el uso del sistema por parte de usuarios autorizados. Demasiada seguridad podría ser contraproducente si es muy engorrosa para los usuarios, pues éstos tenderán a eludir los procedimientos para facilitarse la vida.

Casos famosos:

Algunos de los Titanics y Hindenburgs de la seguridad en computadores son los siguientes:

En Unix `lpr -r` archivo imprime archivo y después lo elimina. En versiones antiguas de Unix se podía hacer `lpr -r /etc/passwd`, lo que terminaba con la eliminación del archivo donde se registran los usuarios.

El comando `mkdir xx` era un [programa](#) que ejecutaba en modo superusuario, creando un nodo-i para el directorio xx, y luego cambiando el dueño de xx de *root* al del usuario. Con un sistema lento y un poco de suerte, se podía modificar el nodo-i para que apuntara a cualquier archivo (por ejemplo, el `passwd`), justo antes de que `mkdir` fijara el nuevo dueño.

Otro ejemplo ilustrativo de lo fácil que es pensar que un sistema es seguro, cuando en realidad no lo es, es el del sistema operativo TENEX, usado en los DEC-10 de Digital. TENEX usaba memoria virtual, y para permitir al usuario monitorear el comportamiento de sus programas, éste podía especificar una rutina que el sistema ejecutaría cada vez que hay una falta de página. Al mismo tiempo, los archivos en TENEX estaban protegidos por una clave: cada vez que se abría un archivo, debía especificarse su clave. El sistema operativo chequeaba las claves de un caracter a la vez, deteniéndose apenas un caracter difiriera. Gracias a eso y a que era posible saber cuándo había una falta de página, se podía descubrir la clave de cualquier archivo, de la siguiente manera:



Poner primer caracter de posible clave en la última posición de una página p, y arreglárselas para que la siguiente (la p+1) estuviera inválida (no presente en memoria física). Tratar de abrir el archivo, usando esa posible clave. El resultado esperado es un mensaje diciendo "clave incorrecta", pero dependiendo de si hubo falta de página o no en p+1, podemos saber si el primer caracter era correcto o no. Después de unas pocas pruebas, se habrá descubierto el primer caracter, y es cosa de seguir la misma idea para descubrir el resto. Si hay 128 caracteres posibles, necesitaremos $128n$ intentos para descubrir una clave de n caracteres, en lugar de 128^n

Probablemente la violación más famosa de todos los tiempos ocurrió en 1988 cuando un estudiante lanzó un gusano por la internet que botó miles de máquinas en cosa de horas. El gusano tomaba el control de una máquina intentando diversos mecanismos. Uno de ellos era un bugo en el programa finger. Una vez obtenido el control, trataba de descubrir las claves de los usuarios de esa máquina intentando palabras comunes. Si descubría una, entonces tenía acceso a todas las máquinas en que ese usuario tuviera cuenta. El gusano no hacía ninguna acción dañina en sí, pero usaba tantos recursos de las máquinas infectadas que las botaba.

Aunque estos defectos han sido corregidos, todavía hay más. En Unix, algunos nunca serán corregidos (si se corrigen, dejaría de ser Unix).

Otras amenazas y ataques posibles.

Caza claves. Dejar corriendo en un terminal un programa que pida "login:" y luego "password:", para engañar a los usuarios de modo que estos revelen su clave.

Solicitar recursos como páginas de memoria o bloques de disco, y ver qué información contienen; muchos sistemas no los borran cuando se liberan, de modo que se puede encontrar información "interesante".



Principios básicos para la seguridad

Suponer que el diseño del sistema es público.

El defecto debe ser: sin acceso.

Chequear permanentemente.

Los mecanismos de protección deben ser simples, uniformes y contruidos en las capas más básicas del sistema.

Los mecanismos deben ser aceptados psicológicamente por los usuarios.

Mecanismos de autorización.

Un sistema de computación puede verse como una colección de objetos (procesos, procesadores, segmentos de memoria, discos, impresoras, archivos, semáforos). Cada objeto debe tener un nombre único para poder identificarlo, y un número finito de operaciones que los procesos pueden efectuar sobre él (leer y escribir en archivos, P y V en semáforos). Podemos ver a estos objetos como tipos abstractos de datos.

Obviamente, un proceso no debe poder acceder objetos sobre los que no tenga autorización. También debe ser posible restringir el uso de un objeto por parte de un proceso sólo a ciertas operaciones. Por ejemplo, un proceso podría tener autorización para leer, pero no para escribir un determinado archivo.

Dominios de protección.

Un dominio de protección es un conjunto de pares (objeto, operaciones); cada par identifica un objeto y las operaciones permitidas sobre él.

En cada instante, cada proceso ejecuta dentro de un dominio de protección. Los procesos pueden cambiar de un dominio a otro en el tiempo; el cómo depende mucho del sistema. En UNIX, se asocia un dominio a cada usuario+grupo; dado un usuario y el grupo al cual pertenece, se puede construir una lista de todos los objetos que puede acceder y con qué operaciones. Cuando un usuario ejecuta un programa almacenado en un archivo de propiedad de otro



usuario B, el proceso puede ejecutar dentro del dominio de protección de A o B, dependiendo del bit de dominio o *SETUSERID bit* del archivo. Este mecanismo se usa con algunos utilitarios. Por ejemplo, el programa `passwd` debe tener privilegios que un usuario común no tiene, para poder modificar el archivo donde se guardan las claves. Lo que se hace es que el archivo `/bin/passwd` que contiene el programa es propiedad del superusuario, y tiene el `SETUSERID` encendido. Este esquema es peligroso: un proceso puede pasar de un estado en que tiene poco poder a otro en que tiene poder absoluto (no hay términos medios). Cualquier error en un programa como `passwd` puede significar un gran hoyo en la seguridad del sistema. Cuando se hace una llamada al sistema también se produce un cambio de dominio, puesto que la llamada se ejecuta en modo protegido.

Matriz de acceso.

Ahora bien, ¿cómo se las arregla el sistema para llevar la cuenta de quién puede acceder qué objetos y con qué operaciones? Conceptualmente al menos, podemos ver este modelo de protección como una gran matriz de acceso.

Los cambios de dominio que un proceso puede hacer también podemos integrarlos a la matriz, tratando a los dominios como otros objetos, con una operación: entrar.

Una política de protección involucra decidir cómo se va a llenar esta matriz. Normalmente el usuario que crea un objeto es quién decide cómo se va a llenar la columna de la matriz correspondiente a ese objeto. La matriz de acceso es suficientemente general como para apoyar diversas políticas. Por ejemplo:

La capacidad para copiar o transferir un derecho de un objeto a otro dominio.

Capacidad de un dominio para modificar los derechos en otros dominios (todos, o para un recurso específico).

El problema es cómo almacenar esta matriz. Como es una matriz poco densa (muchos de los elementos son vacíos), no resulta práctico representarla como matriz propiamente. Podríamos usar una tabla con triples (dominio, objeto,



derechos). Si un proceso dentro de un dominio D intenta efectuar una operación M sobre un objeto O, se busca (D, O, C), y se verifica si M pertenece a C. De todas maneras, la tabla es grande, y el esquema no es muy eficiente. Además, si un objeto puede ser, por ejemplo, leído por todo el mundo, debe tener entradas para cada dominio.

Listas de acceso.

Alternativamente, podemos guardar la matriz por columnas (descartando las entradas vacías). Es decir, a cada objeto se le asocia una lista de pares (dominio, derechos). Es lo que se conoce como lista de acceso o ACL. Si pensamos en archivos de Unix, podemos almacenar esta lista en el nodo-i de cada archivo, y sería algo así como

((Juan, *, RW), (Pedro, Profes, RW), (*, Profes, R))

En la práctica, se usa un esquema más simple (y menos poderoso), pero que puede considerarse aún una lista de accesos, reducida a 9 bits. 3 para el dueño (RWX), 3 para el grupo, y 3 para el resto del mundo.

Windows NT usa listas de accesos con todo el nivel de detalle que uno quiera: para cualquier usuario o grupo, se puede especificar cualquier subconjunto de derechos para un archivo, de entre {RWDPO}.

Capacidades.

La otra posibilidad es almacenar la matriz por filas. En este caso, a cada proceso se le asocia una lista de capacidades. Cada capacidad corresponde a un objeto más las operaciones permitidas.

Cuando se usan capacidades, lo usual es que, para efectuar una operación M sobre un objeto O, el proceso ejecute la operación especificando un puntero a la capacidad correspondiente al objeto, en vez de un puntero al objeto. La sola *posesión* de la capacidad por parte del proceso quiere decir que tiene los derechos que en ella se indican. Por lo tanto, obviamente, se debe evitar que los procesos puedan "falsificar" capacidades.



Una posibilidad es mantener las listas de capacidades dentro del sistema operativo, y que los procesos sólo manejen punteros a las capacidades, no las capacidades propiamente. Otra posibilidad es cifrar las capacidades con una clave conocida por el sistema, pero no por el usuario. Este enfoque es particularmente adecuado para sistemas distribuidos, y es usado en Amoeba.

Un problema de las capacidades es que puede ser difícil revocar derechos ya entregados. En Amoeba, cada objeto tiene asociado un número al azar, grande, que también está presente en la capacidad. Cuando se presenta una capacidad, ambos números deben coincidir. De esta manera, para revocar los derechos ya otorgados, se cambia el número asociado al objeto. Problema: no se puede revocar selectivamente. Las revocaciones con ACL son más simples y más flexibles.

Mecanismos de autenticación.

La autenticación, que consiste en identificar a los usuarios que entran al sistema, se puede basar en posesión (llave o tarjeta), conocimiento (clave) o en un atributo del usuario (huella digital).

Claves.

El mecanismo de autenticación más ampliamente usado se basa en el uso de claves o *passwords*; es fácil de entender y fácil de implementar. En UNIX, existe un archivo `/etc/passwd` donde se guarda los nombres de usuarios y sus claves, cifradas mediante una función *one-way* F. El programa login pide nombre y clave, computa F(clave), y busca el par (nombre, F(clave)) en el archivo.

Con claves de 7 caracteres tomados al azar de entre los 95 caracteres ASCII que se pueden digitar con cualquier teclado, entonces las 95^7 posibles claves deberían desincentivar cualquier intento por adivinarla. Sin embargo, una proporción demasiado grande de las claves escogidas por los usuarios son fáciles de adivinar, pues la idea es que sean también fáciles de recordar. La clave



también se puede descubrir mirando (o filmando) cuando el usuario la digita, o, si el usuario hace login remoto, interviniendo la red y observando todos los paquetes que pasan por ella. Por último, además de que las claves se pueden descubrir, éstas también se pueden "compartir", violando las reglas de seguridad. En definitiva, el sistema no tiene ninguna garantía de que quien hizo login es realmente el usuario que se supone que es.

Identificación física

Un enfoque diferente es usar un elemento físico difícil de copiar, típicamente una tarjeta con una banda magnética. Para mayor seguridad este enfoque se suele combinar con una clave (como es el caso de los cajeros automáticos). Otra posibilidad es medir características físicas particulares del sujeto: huella digital, patrón de vasos sanguíneos de la retina, longitud de los dedos. Incluso la firma sirve.

Algunas medidas básicas

Demorar la respuesta ante claves erróneas; aumentar la demora cada vez. Alertar si hay demasiados intentos.

Registrar todas las entradas. Cada vez que un usuario entra, chequear cuándo y desde dónde entró la vez anterior.

Hacer chequeos periódicos de claves fáciles de adivinar, procesos que llevan demasiado tiempo corriendo, permisos erróneos, actividades extrañas (por ejemplo cuando usuario está de vacaciones).

Para los más paranoicos: poner trampas para descubrir intentos de uso no autorizado.

Criptografía.

Los mecanismos de protección que hemos visto hasta ahora muchas veces no son suficientes para mantener información confidencial adecuadamente resguardada. Con el uso masivo de las redes de computadores, más y más información se transmite por ella, y nadie puede estar seguro de que no hay



mirones en el alambre. Los métodos criptográficos son los más comúnmente usados para proteger información confidencial. Lo que se envía por la red no es la información original, sino la información codificada, que carece de sentido salvo para el receptor, que puede decodificarla.

Criptografía simétrica.

La criptografía simétrica se basa en un algoritmo general de codificación C , un algoritmo general de decodificación D , y una clave secreta k , tales que

$$D_k(C_k(m)) = m.$$

C_k y D_k son computables eficientemente.

La seguridad depende sólo de que la clave --no los algoritmos-- sea secreta.

Un esquema ampliamente usado es el DES (data encryption standard), creado por la NSA.

El inconveniente de la criptografía simétrica es la distribución de la clave. Si quiero enviar un texto confidencial por la red, lo envío cifrado, pero ¿cómo le comunico la clave a mi interlocutor? Por otra parte, se requiere una clave por cada par de usuarios.

Criptografía de clave pública.

La criptografía de clave pública es asimétrica. Se basa en [métodos](#) que requieren una clave pública para cifrar, y otra, distinta y privada, para descifrar. Supongamos que los procedimientos para cifrar y descifrar de los usuarios A y B, son, respectivamente C_A , D_A , C_B y D_B .

Para que B envíe mensaje m a A:

B averigua la clave pública de A, en un directorio público.

Envía $C_A(m)$

A descifra el mensaje con su clave: $m=D_A(C_A(m))$. Sólo A puede hacerlo, pues es el único que conoce la clave.



Los métodos de criptografía de clave pública tienen la interesante propiedad

$$m=C_A(D_A(m))$$

que permite implementar también firmas digitales. Una firma digital debe ser dependiente del firmador y del mensaje que está firmando.

Un mensaje m firmado por B es

$$s=(D_B(m))$$

Si se lo quiere mandar privadamente a B , además lo cifra, enviando $C_A(s)$, pero esto es sólo para privacidad.

A primero recupera s , descifrando el mensaje como antes, si viene cifrado, y luego obtiene el mensaje original con

$$m=C_B(s)$$

Y ahora A posee el par (m,s) que equivale a un documento firmado por B , puesto que:

B no puede negar que envió m , pues nadie más que B puede haber creado $s=(D_B(m))$.

A puede convencer a un juez que $m=C_B(s)$.

A no puede modificar m , pues la firma habría sido otra.

En particular, RSA opera de la siguiente manera:

La clave pública de cifrado es un par (c,n) , y la clave privada un par (d,n) . Cada mensaje se representa como un número entre 0 y $n-1$.

Los procedimientos para cifrar y descifrar con esas claves son:

$$C(m) = m^c \text{ mod } n = w$$

$$D(w) = w^d \text{ mod } n$$

El problema es escoger las claves. n es el producto de dos números primos grandes (100 dígitos) p y q . d se escoge al azar como un número grande



relativamente primo con $(p-1)(q-1)$. Finalmente c se computa como el inverso de d en módulo $(p-1)(q-1)$, o sea:

$$c \cdot d \pmod{(p-1)(q-1)} = 1$$

A pesar de que n es público, p y q no lo son, y todo se basa en la suposición de que es difícil factorizar un número grande.

Criptografía híbrida.

Los métodos de criptografía de clave pública resuelven el problema del intercambio de claves, pero son bastante más lentos (100 a 1000 veces) que los métodos de criptografía simétrica. Se puede obtener lo mejor de ambos mundos con un esquema híbrido: se usa criptografía de clave pública para acordar una clave privada, y el grueso de la comunicación se cifra con esa clave usando criptografía simétrica.

¿Es posible hacer un formulario seguro?

Para hacer un formulario se debe tener un servidor seguro.

En primer lugar los formularios pueden tener “agujeros” a través de los que un hacker hábil, incluso poco hábil, puede “colar” comandos.

La red es totalmente pública y abierta, los paquetes pasan por máquinas de las que no se tiene conocimiento y a las que puede tener acceso la gente que le guste humear el tráfico de la red. Si es así (y no tienen que ser necesariamente hackers malintencionados, algunos proveedores de servicio lo hacen) sólo se puede recurrir a encriptar el tráfico por medio, en WWW, de servidores y clientes seguros.

Política de seguridad.

Proveer acceso a los servicios de la red de una empresa y proveer acceso al mundo exterior a través de la organización, da al personal e institución muchos beneficios. Sin embargo, a mayor acceso que se provea, mayor es el peligro de que alguien explote lo que resulta del incremento de vulnerabilidad.



De hecho, cada vez que se añade un nuevo sistema, acceso de red o aplicación se agregan vulnerabilidades potenciales y aumenta la mayor dificultad y complejidad de la protección. Sin embargo, si se está dispuesto a enfrentar realmente los riesgos, es posible cosechar los beneficios de mayor acceso mientras se minimizan los obstáculos. Para lograr esto, se necesitará un plan complejo, así como los recursos para ejecutarlo. También se debe tener un conocimiento detallado de los riesgos que pueden ocurrir en todos los lugares posibles, así como las medidas que pueden ser tomadas para protegerlos.

En algunos aspectos, esto puede parecer una carga abrumadora, y podría muy bien serlo, especialmente en organizaciones pequeñas que no tienen personal experto en todos los temas. Alguien podría estar tentado para contratar un consultor de seguridad y hacerlo con él; aunque esto puede ser una buena manera para outsourcing, todavía necesita saber lo suficiente y observar la honestidad del consultor. Después de todo, se le va a confiar a ellos los bienes más importantes de la organización.

Para asegurar una red adecuadamente, no solamente se necesita un profundo entendimiento de las características técnicas de los protocolos de red, sistemas operativos y aplicaciones que son accesadas, sino también lo concerniente al planeamiento. El plan es el primer paso y es la base para asegurar que todas las bases sean cubiertas.

Algunas afirmaciones erróneas comunes acerca de la seguridad.

- *Mi sistema no es importante para un cracker.* Esta afirmación se basa en la idea de que no introducir contraseñas seguras en una empresa no entraña riesgos pues ¿quién va a querer obtener información mía?. Sin embargo, dado que los métodos de contagio se realizan por medio de programas *automáticos*, desde unas máquinas a otras, estos no distinguen buenos de malos, interesantes de no interesantes, etc. Por tanto abrir sistemas y dejarlos sin claves es facilitar la vida a los virus.



- *Estoy protegido pues no abro archivos que no conozco.* Esto es falso, pues existen múltiples formas de contagio, además los programas realizan acciones sin la supervisión del usuario poniendo en riesgo los sistemas.
- *Como tengo antivirus estoy protegido.* En general los programas antivirus no son capaces de detectar todas las posibles formas de contagio existentes, ni las nuevas que pudieran aparecer conforme los ordenadores aumenten las capacidades de comunicación, además los antivirus son vulnerables a desbordamientos de búfer que hacen que la seguridad del sistema operativo se vea más afectada aún.
- *Como dispongo de un firewall no me contagio.* Esto únicamente proporciona una limitada capacidad de respuesta. Las formas de infectarse en una red son múltiples. Unas provienen directamente de accesos al sistema (de lo que protege un firewall) y otras de conexiones que se realizan (de las que no me protege). Emplear usuarios con altos privilegios para realizar conexiones puede entrañar riesgos, además los firewalls de aplicación (los más usados) no brindan protección suficiente contra el spoofing.
- *Tengo un servidor web cuyo sistema operativo es un unix actualizado a la fecha:* Puede que esté protegido contra ataques directamente hacia el núcleo, pero si alguna de las aplicaciones web (PHP, Perl, Cpanel, etc.) está desactualizada, un ataque sobre algún script de dicha aplicación puede permitir que el atacante abra una shell y por ende ejecutar comandos en el unix.

Seguridad Informática y Normativa.

Con el fin de evitar los ataques por parte de la delincuencia informática ya sea nacional o transnacional se debe contar con dos variables importantes:



- a) **La seguridad informática**, que es el conjunto de técnicas y métodos que se utilizan para proteger tanto la información como los equipos informáticos en donde ésta se encuentra almacenada ya sean éstos individuales o conectados a una red frente a posibles ataques accidentales o intencionados.

La seguridad informática a su vez está dividida en cinco componentes:

- **Seguridad Física:** Es aquella que tiene relación con la protección del computador mismo, vela porque las personas que lo manipulan tengan la autorización para ello, proporciona todas las indicaciones técnicas para evitar cualquier tipo de daños físicos a los equipos informáticos.
- **Seguridad de Datos:** Es la que señala los procedimientos necesarios para evitar el acceso no autorizado, permite controlar el acceso remoto de la información, en suma protege la integridad de los sistemas de datos.
- **Back Up y Recuperación de datos:** Proporciona los parámetros básicos para la utilización de sistemas de recuperación de datos y Back Up de los sistemas informáticos. Permite recuperar la información necesaria en caso de que ésta sufra daños o se pierda.
- **Disponibilidad de los Recursos:** Este procura que los recursos y los datos almacenados en el sistema puedan ser rápidamente accedidos por la persona o personas que lo requieren. Permite evaluar constantemente los puntos críticos del sistema para así poderlos corregir de manera inmediata.
- **La Política de Seguridad:** Conjunto de normas y criterios básicos que determinan lo relativo al uso de los recursos de una organización cualquiera.
- **Análisis Forense:** Este surge como consecuencia de la necesidad de investigar los incidentes de seguridad informática que se producen en las entidades. Persigue la identificación del autor y del motivo del ataque.



Igualmente, trata de hallar la manera de evitar ataques similares en el futuro y obtener pruebas periciales.

- b) **Seguridad Normativa**, derivada de los principios de legalidad y seguridad jurídica, se refiere a las normas jurídicas necesarias para la prevención y sanción de las posibles conductas que puedan ir en contra de la integridad y seguridad de los sistemas informáticos.

Para que exista una adecuada protección a los sistemas informáticos y telemáticos se deben conjugar tanto la seguridad informática como la seguridad legal y así poder brindar una adecuada protección y tutela tanto técnica como normativa.

Algunas compañías o entidades gubernamentales siguen creyendo o tienen la idea errónea que sus sistemas y redes informáticos no son blancos idóneos de un ataque, en razón de que no generan ningún tipo de información relevante, por tanto se creen inmunes a cualquier ataque informático porque no tienen una presencia visible y preponderante en la red, situación que no es así, ya que si bien su información no podría ser el blanco de un delincuente informático, si lo podrían ser los recursos de que dicho sistema informático posee, por ejemplo, su capacidad de procesamiento, su capacidad de almacenamiento y de interconexión, en esta situación hace atractiva la idea de tomar dicho sistema como un medio para descifrar o romper claves de acceso utilizando sistemas zombis. El deseo del agresor puede consistir únicamente en un lugar en donde almacenar su compendio de números de tarjetas de crédito, o sus programas ilegalmente obtenidos, sus crackeadores, o pornografía.

Existe una falta de conciencia en el uso de las TICs dentro de la Sociedad de la Información por parte de los usuarios, quienes no tienen un nivel de capacitación suficiente o directivas claras de lo que implica el manejo, creación y transmisión de información importante, no solo personal, sino también profesional y corporativa y de sus posibles vulnerabilidades.



Organismos oficiales de seguridad informática.

Existen organismos oficiales encargados de asegurar servicios de prevención de riesgos y asistencia a los tratamientos de incidencias, tales como el **CERT/CC** (*Computer Emergency Response Team Coordination Center*) del SEI (Software Engineering Institute) de la Carnegie Mellon University el cual es un centro de alerta y reacción frente a los ataques informáticos, destinados a las empresas o administradores, pero generalmente estas informaciones son accesibles a todo el mundo.³²

³² http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica



CAPÍTULO III

PRESERVACION DE EVIDENCIA DIGITAL NECESARIA PARA UN PROCESO LEGAL.

1. Importancia.

Somos parte de una sociedad en la cual las tecnologías de la información y de las comunicaciones se han extendido de manera considerable en el quehacer cotidiano del ser humano, existe un uso masivo de nuevos elementos que nos proporciona las nuevas tecnologías como son: correo electrónico, comunicaciones telefónicas, cajeros automáticos, pagos por Internet, mensajes de texto, filmaciones de cámaras de seguridad, entre otros.

Estos elementos pueden ser considerados como medios de prueba de situaciones con implicaciones legales: un contrato celebrado por correo electrónico, una filmación sobre un pedido de soborno, un mensaje de texto entre la víctima y un sospechoso de asesinato, en fin, nuevos elementos a ser incorporados a los procedimientos judiciales. Esto es de vital importancia, pues actualmente se mantiene el tradicional sistema de gestión de expedientes en soporte papel, con lo cual la forma de presentación de un elemento probatorio en medio electrónico es a través de copias en papel.

La forma en la cual el documento digital ha sido obtenido y conservado, las medidas de protección para la actualización de su formato, en su caso, las precauciones para garantizar que la copia en papel es idéntica al original electrónico, son cuestiones que deberán ser explicitadas en el juicio de modo de colaborar a formar la convicción del Juez. ¿Cómo se presenta un correo electrónico firmado digitalmente? ¿Cómo se demuestra que la firma digital de ese documento electrónico es válida? son cuestiones que comienzan a ser exploradas y necesitan ser manejadas correctamente para ello contamos con la Informática Forense que es un ciencia criminalística que actualmente está adquiriendo gran importancia; sin embargo no tiene un método estandarizado, es éste el motivo por el cual su admisibilidad dentro de un proceso judicial podría ser cuestionada, pero

DRA. GRACIELA ENCALADA OCHOA



esto no debe ser un obstáculo para no contar con esta importante herramienta, la cual debe ser manejada en base a rígidos principios científicos, normas legales y de procedimiento.³³

2. Principios Básicos

Partiendo del hecho que la prueba dentro del proceso penal es muy importante, puesto que a partir de ella se confirma o desvirtúa una hipótesis o afirmación precedente, se llega a la posesión de la verdad material y de esta manera se confirmará la existencia de la infracción y la responsabilidad de quienes aparecen en un inicio como presuntos responsables, es necesario tener en consideración algunos principios básicos sobre el manejo de la evidencia digital.³⁴

A continuación me permito transcribir los PRINCIPIOS BÁSICOS que se recomienda en el Manual de Manejo de Evidencias Digitales y Entornos Informáticos, elaborado por el Ministerio Público del Ecuador.

1. Ninguna acción debe tomarse por parte de la Policía Judicial, el Ministerio Público o por sus agentes y funcionarios que cambie o altere la información almacenada dentro de un sistema informático o medios magnéticos, a fin de que ésta sea presentada fehacientemente ante un tribunal.
2. En circunstancias excepcionales una persona competente puede tener acceso a la información original almacenada en el sistema informático objeto de la investigación, siempre que después se explique detalladamente y de manera razonada cual fue la forma en la que se produjo dicho acceso, su justificación y las implicaciones de dichos actos.
3. Se debe llevar una bitácora de todos los procesos adelantados en relación a la evidencia digital. Cuando se hace una revisión de un caso por parte de una tercera parte ajena al mismo, todos los archivos y registros de dicho caso y el

³³ Introducción a la Informática Forense. Dr. Santiago Acurio del Pino. Coordinador del Departamento Informático del Ministerio Público de Pichincha.

³⁴ Introducción a la Informática Forense. Dr. Santiago Acurio del Pino. Coordinador del Departamento Informático del Ministerio Público de Pichincha.



proceso aplicado a la evidencia que fue recolectada y preservada, deben permitir a esa parte recrear el resultado obtenido en el primer análisis.

4. El Fiscal del Caso y/o el Oficial a cargo de la investigación son responsables de garantizar el cumplimiento de la ley y del apego a estos principios, los cuales se aplican a la posesión y al acceso a la información almacenada en el sistema informático. De igual forma debe asegurar que cualquier persona que acceda a o copie dicha información cumpla con la ley y estos principios.

3. Reconocimiento de la Evidencia Digital.

Es muy importante antes de proceder a tratar sobre el reconocimiento de la evidencia digital, comenzar con una definición de lo que es evidencia digital **aunque no podemos** afirmar que exista una sola definición, uniforme y/o universal sobre evidencia digital. Sin embargo, la dada por el profesor Cano puede ser útil para entender a qué se refiere dicho concepto. Él, siguiendo la sugerencia de Eoghan Casey, la define como un **“tipo de evidencia física construida por campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales”**. También consideramos importante recordar la Conferencia Internacional de Crímenes de Alta Tecnología y Computación Forense celebrada en 1999, donde la IOCE (Internacional Organization Of Computer Evidence), convocó a una reunión de trabajo en la cual se revisaron los trabajos realizados por el Reino Unido y así mismo, los borradores del grupo Standard and Principles Scientific Working Group on Digital Evidence (SWEDGE), donde se presentaron principios generales y definiciones de evidencia digital, dentro de las cuales se destaca aquella que la establece como la “información de valor probatorio almacenada o transmitida en forma digital”. De acuerdo con este documento, la evidencia digital incluye, por ejemplo, la evidencia en computadores, videos, sonidos, teléfonos celulares, máquinas de fax, etc. No debe olvidarse entonces, que los medios electrónicos en



los que se soporta la evidencia digital son la “vía requerida para presentar pruebas de los hechos ocurridos en sistemas o dispositivos electrónicos”.³⁵

En este sentido puede mencionarse el estándar norteamericano (que se asemeja al australiano) que clasifica la evidencia digital en tres categorías, como son:

1. Registros generados por computador
2. Registros no generados en computadores pero almacenados en éstos.
3. Registros híbridos: Incluyen los generados por computador y almacenados en los mismos.

La principal diferencia entre estos tres aspectos radica en el factor humano, puesto que lo determinante es saber si fue una persona o un computador quien creó el contenido del registro.

La evidencia digital puede convertirse en un factor fundamental dentro de un proceso. Sin embargo, no puede omitirse que ésta es frágil y volátil, y que por lo tanto, puede tornarse en una desventaja para el sistema judicial que no tenga los mecanismos adecuados para su efectivo desarrollo.

Según el Dr. Santiago Acurio del Pino, en su documento Introducción a la Informática Forense, inicialmente el tipo de evidencia digital que se buscaba en los equipos informáticos era del tipo CONSTANTE o PERSISTENTE, es decir, aquella que se encontraba almacenada en un disco duro o en otro medio informático y que se mantenía preservada después que la computadora era apagada. Posteriormente gracias a las redes de interconexión, se dice que el investigador forense se ve obligado a buscar también evidencia del tipo VOLÁTIL, esto es, evidencia que se encuentra alojada temporalmente en la memoria RAM, o en el CACHE, y que por su naturaleza inestable se pierden cuando el

³⁵ Evidencia Digital en Colombia: Una reflexión en la práctica. Por Diana Bogota Prieto, Claudia Moreno Peña. <http://www.alfa-redi.org/rdi-articulo.shtml?x=9330>



computador es apagado, por ello este tipo de evidencias deben ser recuperadas casi de inmediato, por ello es muy importante y necesario utilizar los procedimientos técnicos legales y la rigurosidad científica que pone a disposición de los investigadores la ciencia forense informática a fin de descubrir a los autores y cómplices del delito cometido.

Características de la Evidencia Digital.³⁶

Tal como lo habíamos mencionado, la Evidencia Digital es un tipo de la evidencia física, que es menos tangible que otro tipo de evidencias, pero a diferencia de todas las demás evidencias físicas, ésta presenta ciertas ventajas, debido a que puede ser duplicada de una forma exacta, por lo que es posible peritar sobre copias, tal cual como si se tratara de la evidencia original, lo cual permite realizar diversos tipos de análisis y pruebas sin correr el riesgo de alterar o dañar la evidencia original.

En contraposición a lo que se piensa, es relativamente fácil determinar si una evidencia digital ha sido modificada o alterada a través de la comparación con su original o bien con el análisis de sus metadatos.

La evidencia digital no puede ser destruida fácilmente, tal como piensan los usuarios de ordenadores o computadoras, que creen que con ejecutar un comando de borrado (delete), ya ha desaparecido un documento o archivo objeto del mismo de la máquina. El disco duro de un sistema informático, guarda los datos en sectores creados en el momento del formateo del mismo, lo cual equivale a cuadricular una hoja de papel para insertar números y hacer operaciones matemáticas. Es posible que para guardar un archivo se necesiten varios sectores del disco. Los sistemas operativos y hardware o parte física de los ordenadores, trabajan en conjunto en la ubicación de los archivos y programas para su visualización o ejecución, siendo los responsables específicos del acceso a los archivos, otros archivos denominados Meta Archivos con funciones de

³⁶ **Informática Forense como medio de pruebas.** <http://www.dragonjar.org/informatica-forense-como-medio-de-pruebas.xhtml>



índice, que contienen la información necesaria para abrir o visualizar rápidamente datos específicos en el soporte magnético (Disco Duro). Lo que hace la ejecución de comando de borrado en la mayoría de los sistemas operativos es una eliminación de los datos de ubicación del archivo en el índice del disco duro sin borrar real y físicamente el archivo en si, por lo que el archivo objeto de la instrucción de borrado puede quedar en el disco duro sin que el usuario esté consciente de ello.

Hechos Informáticos que pueden ser probados en juicios.

En principio, todo hecho realizado en un sistema informático puede ser objeto de experticia y puede promoverse un medio probatorio a los efectos de su incorporación procesal. Los peritos en la materia, utilizan entre otros el método de la reconstrucción relacional, es decir, la ubicación en los ordenadores de los datos vinculados al caso, y de ser posible establecer el tiempo y concatenación de estos hechos a efectos de dar a conocer al sentenciador los elementos básicos de la investigación judicial, como lo son el ¿qué?, ¿cómo?, ¿cuándo?, ¿dónde? y el ¿por qué?. Una de las posibilidades, que parece en principio no viable a los ojos de los usuarios informáticos convencionales, es el que se pueden obtener resultados periciales, en los cuales se establezca el origen o procedencia de los mensajes de datos (correo electrónico), los anexos o archivos adjuntos que se envían con los mensajes de datos, pudiendo el experto determinar no solamente el país y/o ciudad de origen, sino que es posible también determinar e individualizar, entre varias máquinas de una misma marca, un mismo modelo, en cuál ha sido producido un archivo determinado.

Las actividades realizadas en el denominado espacio virtual o Internet, son de diversa naturaleza, pero es allí donde ocurren la mayoría de los nuevos delitos de violación de derechos de autor y contra la propiedad industrial más comunes. A través de la pericia informática es posible el rastreo y determinación de la propiedad, administración, y datos de contactos relacionados con un dominio en Internet y/o servidores de almacenamiento, así como la fecha de creación y modificaciones realizadas en página Web para establecer responsabilidades.



Debemos considerar dentro del ámbito de la Informática Forense, el análisis de los datos almacenados en todo tipo de artefactos electrónicos tales como: teléfonos móviles o celulares, agendas personales, grabadoras digitales, dispositivos de almacenamiento, cámaras, discos compactos en todas sus variedades, memorias no volátiles e inclusive fax.

La actividad en redes locales o externas puede ser igualmente analizadas a efectos de determinar las características y tráfico de datos, modus operandi, móviles y costumbre de los usuarios de informática.

Informática aplicada a la Investigación Forense.

La Evidencia Digital puede ser procesada conforme a los criterios de colección y manejo de evidencia que se manejan generalmente en Criminalística, por lo que el proceso se puede resumir en varias fases:

1. Reconocimiento.
2. Captura y Preservación.
3. Clasificación e Individualización.
4. Reconstrucción.

1. **Reconocimiento:** El reconocimiento de la Evidencia Digital incluye la fase de individualización del Hardware o equipos informáticos (cuando se pueda tener acceso físico a ellos), así como la descripción de sistemas operativos y aplicaciones instaladas en los mismos. La ubicación de los datos relevantes al caso es importante en esta fase, los cuales pueden ser de distinta naturaleza, dependiendo del programa que haya sido utilizado para realizar el hecho jurídico informático.

El perito o práctico en materia civil y afines, debe ser muy cauteloso en el ejercicio de sus funciones, regidas por el principio dispositivo, por cuanto la extralimitación en el encargo pericial puede traducirse fácilmente en un delito electrónico.



2. La captura y preservación de la Evidencia Digital en los casos penales, debe procurarse en su estado original. Para lograr efectivamente la preservación correcta de los datos, los expertos deben realizar copias exactas y fieles, a través del procedimiento conocido como copia bit a bit, el cual garantiza que los datos de un medio de almacenamiento, sean copiados de manera exacta desde su fuente de origen.

Los sistemas operativos instalados en los ordenadores utilizan en su mayoría los denominados archivos temporales, denominados también Memoria Virtual, que contienen trazas de las operaciones realizadas en los mismos, así como otro tipo de datos, imágenes y archivos susceptibles de ser recuperados, aún cuando se haya intentado borrarlos, por lo que el perito debe realizar las operaciones de copia con técnicas o herramientas especiales destinadas a tal efecto.

Las operaciones técnicas de análisis, nunca deben realizarse sobre los medios de almacenamiento originales sino sobre copias fieles y exactas.

Una de las garantías que debe ofrecer el perito a las partes y al juez, es la verificación de la identidad o correspondencia entre los archivos originales y sus duplicados, a través de la obtención de valores matemáticos de comprobación conocidos como "Hash", que son valores numéricos, resultado de la suma de números tomados de los datos objeto del señalado proceso. El Hash o valor de comprobación debe ser idéntico entre los archivos originales y los copiados.

3. Clasificación e Individualización: La clasificación de la Evidencia Digital, es el proceso a través del cual el perito ubica las características generales de archivos y datos, que son útiles a su vez para realizar comparaciones entre archivos similares o bien para individualizar la evidencia, por lo que de esta forma se establecerán los tipos de archivos.

La individualización juega un papel determinante en la experticia informática, la cual se logra a través de la ubicación y análisis de los metadatos (metadata), es decir, los datos sobre los datos, información ésta que se encuentra



en embebida de forma oculta dentro de los archivos, siendo los metadatos típicos los relacionados con el título, tema, autor y tamaño de los archivos, incluyéndose también en esta categoría las fechas de creación, modificación e impresión de un documento electrónico. Los metadatos son incorporados a los documentos automáticamente sin que el usuario tenga que realizar ninguna operación destinada a él. Algunos programas toman datos del Hardware o de los equipos donde se encuentran instalados, lo cual en casos determinados puede constituir prueba inequívoca de que un archivo ha sido realizado en un ordenador determinado.

4. Reconstrucción: La reconstrucción de los hechos informáticos incluye conceptualmente el establecimiento de la secuencia de producción de actividades en un computador o en redes. La recuperación de Evidencia Digital dañada entra también en esta categoría.

Es importante que en la pericia informática registre cada acción realizada durante su práctica a efectos de hacer posible la evaluación de los protocolos de manejo de evidencia o bien a efectos de confirmarse los resultados en ampliaciones y aclaratorias del dictamen.

La reconstrucción relacional de los hechos informáticos es importante a efectos de establecer su relación con otro tipo de evidencia del mismo caso. El perito debe tratar de hacer una especie de línea del tiempo cuando la complejidad de los hechos que está evaluando así lo requiera.

Valoración de la pericia informática.

Los hechos informáticos tienen su origen en procesos matemáticos por los cuales le son aplicables leyes científicas de carácter incuestionable, pero ello no significa en forma alguna que toda pericia informática sea certera y adecuada a las necesidades del proceso. Las pericias informáticas deben ser apreciadas siempre y cuando se desprenda del dictamen una estricta aplicación de las fases de preservación y manejo de evidencia, así como una correcta, sopesada y objetiva aplicación del método científico como garante único de la objetividad del



perito, el cual no solo tiene el reto de realizar su labor de por sí compleja, sino que además debe preocuparse por utilizar un lenguaje digerible por mentes de corte eminentemente humanístico en las que a veces existe una predisposición en contra de la informática o bien una desconfianza sobre los posibles resultados de este nuevo tipo de aplicación de los medios probatorios periciales.³⁷

Herramientas para la Recolección de Evidencia³⁸

Existen una gran cantidad de herramientas para recuperar evidencia. El uso de herramientas sofisticadas se hace necesario debido a:

1. La gran cantidad de datos que pueden estar almacenados en un computador.
2. La variedad de formatos de archivos, los cuales pueden variar enormemente, aún dentro del contexto de un mismo sistema operativo.
3. La necesidad de recopilar la información de una manera exacta, y que permita verificar que la copia es exacta.
4. Limitaciones de tiempo para analizar toda la información.
5. Facilidad para borrar archivos de computadores.
6. Mecanismos de encriptación, o de contraseñas.

- **EnCase**

ENCASE es un ejemplo de herramientas de este tipo. Desarrollada por Guidance Software Inc. Permite asistir al especialista forense durante el análisis de un crimen digital. Algunas de las características más importantes de encase se relacionan a continuación:

³⁷ <http://www.dragonjar.org/informatica-forense-como-medio-de-pruebas.xhtml>

³⁸ <http://html.rincondelvago.com/informatica-forense.html>



Copiado Comprimido de Discos Fuente.

Encase emplea un estándar sin pérdida (loss-less) para crear copias comprimidas de los discos origen. Los archivos comprimidos resultantes, pueden ser analizados, buscados y verificados, de manera semejante a los normales (originales). Esta característica ahorra cantidades importantes de espacio en el disco del computador del laboratorio forense, permitiendo trabajar en una gran diversidad de casos al mismo tiempo, examinando la evidencia y buscando en paralelo.

Búsqueda y Análisis de Múltiples partes de archivos adquiridos.

EnCase permite al examinador buscar y analizar múltiples partes de la evidencia. Muchos investigadores involucran una gran cantidad de discos duros, discos extraíbles, discos “zip” y otros tipos de dispositivos de almacenamiento de la información. Con Encase, el examinador puede buscar todos los datos involucrados en un caso en un solo paso. La evidencia se clasifica, si está comprimida o no, y puede ser colocada en un disco duro y ser examinada en paralelo por el especialista.

Diferente capacidad de Almacenamiento.

Los datos pueden ser colocados en diferentes unidades, como Discos duros IDE o SCSI, drives ZIP, y Jazz. Los archivos pertenecientes a la evidencia pueden ser comprimidos o guardados en CD-ROM manteniendo su integridad forense intacta, estos archivos pueden ser utilizados directamente desde el CD-ROM evitando costos, recursos y tiempo de los especialistas.

Varios Campos de Ordenamiento, Incluyendo Estampillas de tiempo.

EnCase permite al especialista ordenar los archivos de la evidencia de acuerdo a diferentes campos, incluyendo campos como las tres estampillas de tiempo (cuando se creó, último acceso, última escritura), nombres de los archivos, firma de los archivos y extensiones.



Análisis Compuesto del Documento. EnCase permite la recuperación de archivos internos y meta-datos con la opción de montar directorios como un sistema virtual para la visualización de la estructura de estos directorios y sus archivos, incluyendo el *slack* interno y los datos del espacio *unallocated*.

- **Herramientas para el Monitoreo y/o Control de Computadores.**

Algunas veces se necesita información sobre el uso de los computadores, por lo tanto existen herramientas que monitorean el uso de los computadores para poder recolectar información. Existen algunos programas simples como *key loggers* o recolectores de pulsaciones del teclado, que guardan información sobre las teclas que son presionadas, hasta otros que guardan imágenes de la pantalla que ve el usuario del computador, o hasta casos donde la máquina es controlada remotamente .

- **KeyLogger .**

“KeyLogger” es un ejemplo de herramientas que caen en esta categoría. Es una herramienta que puede ser útil cuando se quiere comprobar actividad sospechosa; guarda los eventos generados por el teclado, por ejemplo, cuando el usuario teclea la tecla de 'retroceder', esto es guardado en un archivo o enviado por *e-mail*. Los datos generados son complementados con información relacionada con el programa que tiene el foco de atención, con anotaciones sobre las horas, y con los mensajes que generan algunas aplicaciones.

Existen dos versiones: la registrada y la de demostración. La principal diferencia es que en la versión registrada se permite correr el programa en modo escondido. Esto significa que el usuario de la máquina no notará que sus acciones están siendo registradas.

- **Herramientas de Marcado de documentos**

Un aspecto interesante es el de marcado de documentos; en los casos de robo de información, es posible, mediante el uso de herramientas, marcar software para poder detectarlo fácilmente. El foco de la seguridad está centrado



en la prevención de ataques. Algunos sitios que manejan información confidencial o sensitiva, tienen mecanismos para validar el ingreso, pero, debido a que no existe nada como un sitio 100% seguro, se debe estar preparado para incidentes.

Técnicas forenses en una máquina individual.

Esta es probablemente la parte más común en las técnicas de forense digital. El examinador forense puede estar buscando evidencia de fraude, como hojas financieras dispersas, evidencia de comunicación con alguien más, e-mail o libretas de direcciones o evidencia de una naturaleza particular, como imágenes pornográficas. En los discos duros, se puede buscar tanto en los archivos del usuario como en archivos temporales y en caches. Esto permite al examinador forense reconstruir las acciones que el usuario ha llevado a cabo, que archivos ha accedido, y más.

Hay muchos niveles a los que puede ser examinado un disco duro, existen utilidades por ejemplo, observar que contenía un disco antes de una formateada. Muchos de los archivos que se detectan no pueden ser leídos inmediatamente, muchos programas tienen sus propios formatos de archivo; sin embargo, también existen utilidades que permiten saber cual tipo de archivo es.

Técnicas forenses en una red.

Las técnicas forenses en una red se usan para saber dónde se localiza un computador y para probar si un archivo particular fue enviado desde un computador particular. Estas técnicas son muy complicadas, pero se puede investigar utilizando dos herramientas básicas:

- Registros de firewalls
- Encabezados de correo



Post-Mortem

El análisis post-mortem se realiza mayoritariamente para la recuperación de datos con los cuales poder trabajar posteriormente, obviamente para no tener que acudir a éste recurso se aconsejan la copias de seguridad periódicas.

Se puede decir que un disco duro ha "muerto" cuando su parte mecánica interna no funciona correctamente o cuando se quema, moja, deforma, rompe, etc. Es decir, deja de ser operativo.

Cuando esto sucede no hay más que una solución posible, y esa es el análisis post-mortem. Para ello se lleva a cabo un volcado completo del soporte digital en una "cámara blanca". Los platos del disco antiguo se extraen y se insertan en un nuevo conjunto mecánico para su correcta lectura de datos.

Hay que tener claro que un volcado no es lo mismo que una simple transferencia de ficheros, si no que es una copia EXACTA de un soporte en otro, los mismos bits uno tras otro desde el principio hasta el fin. Para comprobar, una vez finalizado el volcado, de que las copias son idénticas, se pasa el algoritmo de hash MD5 de 128 bits cuyo resultado es un valor hexadecimal de 32 dígitos; si éste es el mismo en los dos podemos asegurar que el proceso ha sido completado con éxito, y de esta forma trabajar como si se tratara del mismo sistema justo antes de sufrir daños.

Regulación Internacional.³⁹

Existen procedimientos internacionalmente aceptados para recolección, aseguramiento, análisis y reporte de la evidencia digital, existen iniciativas como las de la IOCE, la Convención de Cybercrimen expuesta por la Comunidad

³⁹ Evidencia Digital en Colombia: Una reflexión en la práctica. Por Diana Bogota Prieto, Claudia Moreno Peña, <http://www.alfa-redi.org/rdi-articulo.shtml?x=9330>



Europea, el Digital Forensic Research Workshop-DFRWS 2001, etc., donde se establecen marcos de acción y lineamientos que cobijan la evidencia en medios electrónicos.

En el ámbito internacional, se ha tratado recurrentemente el tema de evidencia digital pues los crímenes por medios digitales han tenido tanto auge como la revolución tecnológica en sí. En consecuencia, los procedimientos que les permitan a los investigadores recuperar datos de computadores involucrados en actividades delictivas, para ser usados como evidencia en investigaciones criminales se han convertido en un tema fundamental para las agencias de policía internas de cada país. Así, el tema se traslada del ámbito interno al ámbito internacional por su naturaleza misma. Puede presentar un caso en el que el delito se origine en un país, pero se materialice en otro u otros, haciéndose necesario que la evidencia digital, sea recolectada de acuerdo a ciertos parámetros establecidos ¿Por quién? Y ¿Quién debe recolectarla? Esta clase de interrogantes se presentan a diario en casos que pueden aparentar ser sencillos. De esta forma, se hace evidente la necesidad de adoptar procedimientos y estándares, científicamente evaluados, para conducir investigaciones forenses en sistemas de computación.

Teniendo en cuenta este objetivo, se han realizado distintos estudios y el tema ha sido desarrollado eficazmente por distintas organizaciones internacionales y a nivel interno en unos países más que en otros. A continuación tenemos el trabajo que ha realizado al respecto la IOCE, la Comunidad Europea y la regulación interna de Estados Unidos.

International Organization on Computer Evidence (IOCE).

La IOCE es un organismo internacional que funciona desde abril de 1995 cuando adoptó su estatuto interno. Está compuesto por agencias gubernamentales que realizan investigaciones que involucran o contienen evidencia digital, cuando el Gobierno las ha acreditado debidamente y han sido invitadas por el Comité Ejecutivo de la Organización. De acuerdo con este estatuto, el propósito de este organismo es realizar un Foro Internacional donde



se reúnan distintas agencias internas de múltiples nacionalidades para intercambiar información concerniente a investigaciones de evidencia digital y a temas de computación forense. En esa medida, los objetivos que trazaron para este foro son los siguientes:

1. Identificar y discutir asuntos que sean de interés general.
2. Facilitar la diseminación internacional de la información.
3. Desarrollar recomendaciones que luego sean consideradas individualmente por cada agencia miembro.

Desde marzo de 1998, la función principal de la IOCE fue realizar una lista de principios internacionales de los procedimientos relacionados con la evidencia digital, buscando armonizar métodos y prácticas internas y garantizando la posibilidad de utilizar la evidencia digital recolectada por un Estado, en las Cortes de otro Estado. A partir de ahí, la IOCE desarrolló una lista de 6 principios que hoy en día corresponden al mayor avance de unificación internacional en la materia. Dichos principios son los siguientes:

- Cuando se maneje evidencia digital, deben ser aplicados todos los principios procedimentales y forenses generales.
- Al obtener evidencia digital, las acciones que se hayan tomado, no pueden modificar esta evidencia.
- Cuando sea necesario que una persona acceda a evidencia digital original, esa persona debe estar entrenada y calificada para este propósito.
- Todas las actividades relacionadas con obtención, acceso, conservación y transferencia de evidencia digital, deben estar completamente documentadas, preservadas y disponibles para revisión.
- El individuo es responsable por todas las acciones que realice con respecto al manejo de evidencia digital mientras ésta esté bajo su cuidado.
- Cualquier agencia gubernamental que sea responsable de obtener, acceder, conservar y transferir evidencia digital, es responsable de cumplir con estos principios.



La importancia del trabajo que han realizado las distintas agencias que trabajan conjuntamente dentro de la IOCE radica en que los principios generales para la recuperación de evidencia residente en computadores se han convertido en guías interdisciplinarias y estándares para la recuperación, preservación y examen de evidencia digital, incluyendo audio, imágenes y dispositivos electrónicos. Actualmente, es un trabajo que marca la pauta para la unificación de regulaciones internas a nivel mundial, por lo que facilita la lucha contra los delitos cometidos por medios digitales y permite aumentar la protección en la tecnología de la información.

Comunidad Europea.

En noviembre de 2001, la Comunidad Europea firmó la Convención contra el cybercrimen, adoptando medidas para la conservación de datos; producción, búsqueda y análisis de datos; recolección de evidencia en tiempo real e interceptación de contenidos de datos.

Este trabajo se realizó teniendo en cuenta la importancia de la cooperación internacional en la lucha contra el cybercrimen, y pretende ajustarse a los estándares internacionales y así lograr que la regulación funcione adecuadamente en los casos de delitos cibernéticos cometidos dentro y fuera de las fronteras de los países que la conforman.

Esta Convención se centra en la prevención de acciones en contra de la confidencialidad, integridad y disponibilidad de los sistemas digitales, y los datos contenidos en computadores; así como el mal uso que se le da a esos datos o sistemas. Adicionalmente, adopta poderes suficientes para combatir estas ofensas al facilitar su detección, investigación y persecución tanto a nivel doméstico como a nivel internacional.



Regulación en Estados Unidos.

En Estados Unidos, el Departamento de Justicia, ha desarrollado dos documentos que contienen principios básicos en materia de evidencia digital: “Forensic Examination of Digital Evidence: A Guide for Law Enforcement” y “Electronic Crime Scene Investigation: A Guide for First Responders”. Estos documentos, al igual que todo el desarrollo en materia de evidencia digital, surgen como una respuesta a la facilidad y velocidad con la que se cometen delitos utilizando computadores. Son el resultado del esfuerzo que se realiza junto con agencias de justicia, instituciones financieras y firmas inversoras que incorporan la computación forense a su infraestructura; para luchar contra esta nueva ola de crimen. Sin importar el delito, el área común es la evidencia, la prueba que le dará certeza al juez sobre la comisión de ese delito particular.

Así, estos documentos presentan una serie de procedimientos y protocolos que abarcan todo el proceso de investigación. Se extiende desde la escena del crimen, por todo el análisis y alcanza el proceso de juzgamiento. Es importante mencionar que estos documentos constituyen meras recomendaciones y no tienen fuerza vinculante o equivalen a mandatos legales. Por el contrario, éstas son recomendaciones que representan el consenso de distintos puntos de vista y experiencias de los miembros del TWGEDE (Technical Working Group for the Examination of Digital Evidence). Aclaran que no pretenden cubrir todos los casos posibles y que las recomendaciones pueden variar de acuerdo con el caso concreto. Por lo que las directrices que están consignadas en ellas, son una base para que los investigadores tengan una formación profesional uniforme, que promueva la cooperación y haga posible la interacción entre jurisdicciones en los casos en que se presenten delitos que abarquen varias de ellas.

Limitaciones.

Existen limitaciones que deberán ser tenidas en cuenta con miras a disminuir los efectos negativos que éstas puedan tener sobre la evidencia digital. Dichas limitaciones se componen por:



- **El factor humano.**

Determinante para generar conocimiento y avance. Se requiere una formación básica para orientar las actividades de los profesionales que se dedican a determinada área de la ciencia, con el fin de otorgar mayor certeza a sus resultados y mejorar la efectividad de los procesos. En este orden de ideas, las investigaciones forenses en informática no son la excepción.

- **Estrategias de recolección y análisis de evidencia.**

Usualmente se sustentan en herramientas de software, procedimientos aceptados a nivel internacional y la experiencia del investigador. Entre mayor sea la capacidad de las herramientas utilizadas, mejores resultados y controles podrán ser obtenidos.

- **Limitaciones Tecnológicas.**

Pese a que la tecnología, en la mayoría de los casos, tiene como objetivo facilitar y promover procedimientos, su gran avance hace que se convierta en una limitación, al no contar con los medios y el conocimiento adecuado para su óptimo desarrollo.

El investigador forense requiere de varias habilidades que no son fáciles de adquirir, es por esto que el usuario normal se encontrará con dificultades como las siguientes:

1. Carencia de software especializado para buscar la información en varios computadores.
2. Posible daño de los datos visibles o escondidos, aún sin darse cuenta.
3. Será difícil encontrar toda la información valiosa.
4. Es difícil adquirir la categoría de 'experto' para que el testimonio personal sea válido ante una corte.



5. Los errores cometidos pueden costar caro para la persona o la organización que representa.
6. Dificultad al conseguir el software y hardware para guardar, preservar y presentar los datos como evidencia.
7. Falta de experiencia para mostrar, reportar y documentar un incidente computacional.
8. Dificultad para conducir la investigación de manera objetiva.

Ministerio Público del Ecuador.

El Ministerio Público del Ecuador realiza un importante trabajo sobre el reconocimiento de la Evidencia Digital.

Comienza recordando la importancia que tiene el clarificar los conceptos y describir la terminología adecuada que nos señale el rol que tiene un sistema informático dentro del íter críminis o camino del delito. Esto con el fin de encaminar correctamente el tipo de investigación, la obtención de indicios y posteriormente los elementos probatorios necesarios para sostener nuestro caso. Asimismo se dice que el procedimiento de una investigación por homicidio que tenga relación con evidencia digital será totalmente distinto al que se utilice en un fraude informático, por tanto el rol que cumpla el sistema informático determinará “DONDE DEBE SER UBICADA Y COMO DEBE SER USADA LA EVIDENCIA”⁴⁰ con este propósito se han creado categorías a fin de hacer una necesaria distinción entre el elemento material de un sistema informático o hardware (evidencia electrónica) y la información contenida en éste (evidencia digital). Esta distinción es útil al momento de diseñar los procedimientos adecuados para tratar cada tipo de evidencia y crear un paralelo entre una escena física del crimen y una digital. En este contexto el hardware se refiere a todos los componentes físicos de un sistema informático, mientras que la información, se refiere a todos los datos, programas almacenados y mensajes de datos transmitidos usando el sistema informático.

⁴⁰ Manual de Manejo de Evidencias Digitales y Entornos Informáticos. Versión 2007. Ministerio Público del Ecuador.



Con el propósito de enfatizar el papel que juegan los sistemas informáticos en la comisión de delitos, así como para que el investigador criminal tenga un rumbo claro y preciso al buscar los elementos de convicción que aseguren el éxito dentro de un proceso penal, puesto que para efectos probatorios son objeto de examen tanto el hardware como la información contenida en él, ayudándonos de la ciencia informática y en particular la ciencia forense informática, en el Manual de Manejo de Evidencias Digitales y Entornos Informáticos se ha elaborado un cuadro sobre el Hardware o Elementos Físicos, el mismo que me permito transcribirlo:

Hardware o Elementos Físicos.

SISTEMA INFORMÁTICO	
HARDWARE (Elementos Físicos)	Evidencia Electrónica
. El hardware es mercancía ilegal o fruto del delito.	. El hardware es una mercancía ilegal cuando su posesión no está autorizada por la ley. Ejemplo: en el caso de los decodificadores de la señal de televisión por cable, su posesión es una violación a los derechos de propiedad intelectual y también un delito. . El hardware es fruto del delito cuando éste es obtenido mediante robo, hurto, fraude u otra clase de infracción.
. El hardware es un instrumento	. Es un instrumento cuando el hardware cumple un papel importante en el cometimiento del delito, podemos decir que es usado como un arma o herramienta, tal como una pistola o un cuchillo. Un ejemplo serían los sniffers y otros aparatos



	especialmente diseñados para capturar el tráfico en la red o interceptar comunicaciones.
. El hardware es evidencia	. En este caso el hardware no debe ni ser una mercancía ilegal, fruto del delito o un instrumento. Es un elemento físico que se constituye como prueba de la comisión de un delito. Por ejemplo el scanner que se usó para digitalizar una imagen de pornografía infantil, cuyas características únicas son usadas como elementos de convicción.

Información.

SISTEMA INFORMÁTICO	
INFORMACIÓN	Evidencia Digital
. La información es mercancía ilegal o el fruto del delito.	. La información es considerada como mercancía ilegal cuando su posesión no está permitida por la ley, por ejemplo en el caso de la pornografía infantil. De otro lado será fruto del delito cuando sea el resultado de la comisión de una infracción, como por ejemplo las copias pirateadas de programas de ordenador, secretos industriales robados.
. La información es un instrumento.	. La información es un instrumento o herramienta cuando es usada como medio para cometer una infracción



	penal. Son por ejemplo los programas de ordenador que se utilizan para romper las seguridades de un sistema informático, sirven para romper contraseñas o para brindar acceso no autorizado. En definitiva juegan un importante papel en el cometimiento del delito.
. El información es evidencia	. Esta es la categoría más grande y nutrida de las anteriores, muchas de nuestras acciones diarias dejan un rastro digital. Uno puede conseguir mucha información como evidencia, por ejemplo la información de los ISP's, de los bancos, y de las proveedoras de servicios las cuales pueden revelar actividades particulares de los sospechosos.

Clases de Equipos Informáticos y Electrónicos.

En el Manual elaborado por el Ministerio Público del Ecuador, se dice que algunas personas tienden a confundir los términos evidencia digital y evidencia electrónica, dichos términos pueden ser usados indistintamente como sinónimos, sin embargo es necesario distinguir entre aparatos electrónicos como los celulares y PDAs y la información digital que estos contengan. Esto es indispensable ya que el foco de nuestra investigación siempre será la evidencia digital aunque en algunos casos también serán los aparatos electrónicos.

Con el fin de que los investigadores forenses tengan una idea de dónde buscar evidencia digital, éstos deben identificar las fuentes más comunes de evidencia. Situación que brindará al investigador el método más adecuado para su posterior recolección y preservación.



Las fuentes de evidencia digital pueden ser clasificadas en tres grandes grupos:

1. SISTEMAS DE COMPUTACIÓN ABIERTOS, son aquellos que están compuestos de los llamados computadores personales y todos sus periféricos como teclados, ratones y monitores, las computadoras portátiles y los servidores. Actualmente estos computadores tienen la capacidad de guardar gran cantidad de información dentro de sus discos duros, lo que los convierte en una gran fuente de evidencia digital.
2. SISTEMAS DE COMUNICACIÓN, estos están compuestos por las redes de telecomunicaciones, la comunicación inalámbrica y el Internet. Son también una gran fuente de información y de evidencia digital.
3. SISTEMAS CONVERGENTES DE COMPUTACIÓN, son los que están formados por los teléfonos celulares llamados inteligentes o SMARTPHONES, los asistentes personales digitales PDAs, las tarjetas inteligentes y cualquier otro aparato electrónico que posea convergencia digital y que puede contener evidencia digital.

Dada la ubicuidad de la evidencia digital es raro el delito que no esté asociado a un mensaje de datos guardado y transmitido por medios informáticos. Un investigador entrenado puede usar el contenido de ese mensaje de datos para descubrir la conducta de un infractor, puede también hacer un perfil de su actuación, de sus actividades individuales y relacionarlas con sus víctimas.

Ejemplos de aparatos electrónicos e informáticos:

- Computador de escritorio
- Computador portátil
- Estación de Trabajo
- Hardware de Red
- Servidor – *aparato que almacena o transfiere datos electrónicos por el Internet*



- Teléfono celular
- Teléfono inalámbrico
- Aparato de identificar llamadas
- Localizador – *beeper*
- “GPS” – *aparato que utilizar tecnología satélite capaz de ubicar geográficamente a la persona o vehículo que lo opera.*
- Cámaras, videos
- Sistemas de seguridad
- Memoria “flash” – pequeño dispositivo que puede conservar hasta 4 gigabytes de datos o 4.000.000.000 bytes de información. Actualmente existen de más capacidad.
- “Palm” – *asistente personal electrónico que almacena datos y posiblemente tiene conectividad inalámbrica con el Internet.*
- Juegos electrónicos – en su unidad de datos se puede guardar, incluso, una memoria de otro aparato.
- Sistemas en vehículos – computadoras obvias y computadoras del sistema operativo del vehículo que registra cambios en el ambiente y el mismo vehículo
- Impresora
- Copiadora
- Grabadora
- Videograbadora, DVD
- Duplicadora de discos
- Discos, disquetes, cintas magnéticas



- Aparatos ilícitos – tales como los aparatos que capturan el número celular de teléfonos cercanos para después copiarlo en otros teléfonos, o los llamados sniffers, decodificadores, etc.

Incautación de Equipos Informáticos o Electrónicos.

Si el investigador presume que existe algún tipo de evidencia digital en algún aparato electrónico o en algún otro soporte material relacionado con el cometimiento de una infracción, éste debe pedir la correspondiente autorización judicial para incautar dichos elementos, de igual forma debe tener la autorización judicial para acceder al contenido guardado, almacenado y generado por dichos aparatos.

Antes de realizar un allanamiento e incautación de equipos informáticos o electrónicos se debe tomar en cuenta lo siguiente:

1. ¿A qué hora debe realizarse?
 - Para minimizar destrucción de equipos, datos
 - El sospechoso tal vez estará en línea
 - Seguridad de investigadores.
2. Entrar sin previo aviso
 - Utilizar seguridad
 - Evitar destrucción y alteración de los equipos, o la evidencia contenida en ésta
3. Materiales previamente preparados (Cadena de custodia)
 - Embalajes de papel
 - Etiquetas
 - Discos y disquetes vacíos
 - Herramienta
 - Cámara fotográfica
4. Realizar simultáneamente los allanamientos e incautación en diferentes sitios
 - Datos pueden estar en más de un lugar, sistemas de red, conexiones remotas.
 - Examen de equipos
 - Aparatos no especificados en el orden de allanamiento
5. Creación de respaldos en el lugar, creación de imágenes de datos.
 - Autorización para duplicar, reproducir datos encontrados (por ejemplo, un aparato contestador)



6. Fijar/grabar la escena
7. Cámaras, videos, etiquetas
8. Códigos/claves de acceso/contraseñas
9. Buscar documentos que contienen información de acceso, conexiones en redes, etc.
10. Cualquier otro tipo de consideración especial (consideraciones de la persona involucrada: médicos, abogados, información privilegiada, etc.)

La falta de una orden de allanamiento e incautación que ampare las actuaciones (sobre los equipos y sobre la información) de la Policía Judicial y el Ministerio Público puede terminar con la exclusión de los elementos probatorios por violación de las Garantías Constitucionales.⁴¹

4. Acciones a realizar en la Escena del Delito.

Los investigadores que llegan primero a una escena del delito tienen ciertas responsabilidades, las cuales se resumen en el siguiente cuadro:

- **OBSERVAR Y ESTABLEZCER LOS PARÁMETROS DE LA ESCENA DEL DELITO:** El primero en llegar a la escena, debe establecer si el delito está todavía en progreso, luego tiene que tomar nota de las características físicas del área circundante. Para los investigadores forenses esta etapa debe ser extendida a todo sistema de información y de red que se encuentre dentro de la escena. En estos casos dicho sistema o red pueden ser blancos de un inminente o actual ataque como por ejemplo uno de denegación de servicio (DoS).
- **INICIAR LAS MEDIDAS DE SEGURIDAD:** El objetivo principal en toda investigación es la seguridad de los investigadores y de la escena. Si uno observa y establece en una condición insegura dentro de una escena del delito, debe tomar las medidas necesarias para mitigar dicha situación. Se deben tomar las acciones necesarias a fin de evitar riesgos eléctricos, químicos o biológicos, de igual forma cualquier actividad criminal. Esto es

⁴¹ Manual de Manejo de Evidencias Digitales y Entornos Informáticos. Versión 2007. Ministerio Público del Ecuador.



importante ya que en una ocasión en una investigación de pornografía infantil en Estados Unidos un investigador fue muerto y otro herido durante la revisión de una escena del crimen.

- **FACILITAR LOS PRIMEROS AUXILIOS:** Siempre se deben tomar las medidas adecuadas para precautelar la vida de las posibles víctimas del delito, el objetivo es brindar el cuidado médico adecuado por el personal de emergencias y el preservar las evidencias.
- **ASEGURAR FÍSICAMENTE LA ESCENA:** Esta etapa es crucial durante una investigación, se debe retirar de la escena del delito a todas las personas extrañas a la misma, el objetivo principal es el prevenir el acceso no autorizado de personal a la escena, evitando así la contaminación de la evidencia o su posible alteración.
- **ASEGURAR FÍSICAMENTE LAS EVIDENCIAS:** Este paso es muy importante a fin de mantener la cadena de custodia de las evidencias, se debe guardar y etiquetar cada una de ellas. En este caso se aplican los principios y la metodología correspondiente a la recolección de evidencias de una forma práctica. Esta recolección debe ser realizada por personal entrenado en manejar, guardar y etiquetar evidencia.

La cadena de custodia es un sistema de aseguramiento que, basado en el principio de la "mismidad", tiene como fin garantizar la autenticidad de la evidencia que se utilizará como "prueba" dentro del proceso. La información mínima que se maneja en la cadena de custodia, para un caso específico, es la siguiente: a) Una hoja de ruta, en donde se anotan los datos principales sobre descripción de la evidencia, fechas, horas, custodios, identificaciones, cargos y firmas de quien recibe y quien entrega; b) Recibos personales que guarda cada custodio y donde están datos similares a los de la hoja de ruta; c) Rótulos que van pegados a los envases de las evidencias, por ejemplo a las bolsas plásticas, sobres de papel, sobres de manila, frascos, cajas de cartón, etc; d) Etiquetas que tienen la misma información que los rótulos, pero van atados con una cuerquita a bolsas de papel kraft, o a frascos o a cajas de



cartón o a sacos de fibra; e) Libros de registro de entradas y salidas, o cualquier otro sistema informático que se deben llevar en los laboratorios de análisis y en los despachos de los fiscales e investigadores.

- **ENTREGAR LA ESCENA DEL DELITO:** Después de que se han cumplido todas las etapas anteriores, la escena puede ser entregada a las autoridades que se harán cargo de la misma. Esta situación será diferente en cada caso, ya que por ejemplo en un caso penal será a la Policía Judicial o al Ministerio Público; en un caso corporativo a los Administradores del Sistema. Lo esencial de esta etapa es verificar que todas las evidencias del caso se hayan recogido y almacenado de forma correcta, y que los sistemas y redes comprometidos pueden volver a su normal operación.

- **ELABORAR LA DOCUMENTACIÓN DE LA EXPLOTACIÓN DE LA ESCENA:** Es indispensable para los investigadores documentar cada una de las etapas de este proceso , a fin de tener una completa bitácora de los hechos sucedidos durante la explotación de la escena del delito, las evidencias encontradas y su posible relación con los sospechosos. Un investigador puede encontrar buenas referencias sobre los hechos ocurridos en las notas recopiladas en la explotación de la escena del delito.

Qué hacer al encontrar un dispositivo informático o electrónico.

En el Manual elaborado por el Ministerio Público del Ecuador, encontramos algunas instrucciones de cómo proceder si se encuentra un dispositivo informático o electrónico en la escena del delito.

- No tomar los objetos sin guantes de hule, se podría alterar, encubrir o hacer desaparecer las huellas dactilares o adeníticas existentes en el equipo o en el área donde se encuentra residiendo el sistema informático.
- Asegurar el lugar.
- Asegurar los equipos. De cualquier tipo de intervención física o electrónica hecha por extraños.



- Si no está encendido, no lo encienda (*para evitar el inicio de cualquier tipo de programa de autoprotección*)
- Si está encendido, no lo apague inmediatamente (*para evitar la pérdida de información "volátil"*)
- Si es posible, llame a un técnico.

Cuando no hay técnico:

- Si está encendido, no lo apague inmediatamente
- Si tiene un "Mouse", muévalo cada minuto para no permitir que la pantalla se cierre o se bloquee
- Si el aparato está conectado a una red, anote los números de conexión, (números IP).
- Fotografíe la pantalla, las conexiones y cables.
- Usar bolsas especiales antiestáticas para almacenar diskettes, discos rígidos y otros dispositivos de almacenamiento informáticos que sean electromagnéticos (si no se cuenta, pueden utilizarse bolsas de papel madera). Evitar el uso de bolsas plásticas, ya que pueden causar una descarga de electricidad estática que puede destruir los datos.
- Coloque etiquetas en los cables para facilitar reconexión posteriormente.
- Anote la información de los menús y los archivos activos (sin utilizar el teclado) *Cualquier movimiento del teclado puede borrar información importante.*
- Si hay un disco, un disquete, una cinta, un CD u otro medio de grabación en alguna unidad de disco o grabación, retírelo, protéjalo y guárdelo en un contenedor de papel.
- Bloquee toda unidad de grabación con una cinta, un disco o un disquete vacío aportado por el investigador (NO DEL LUGAR DE LOS HECHOS). *Al utilizar algún elemento del lugar del allanamiento o de los hechos, se contamina un elemento materia de prueba con otro.*
- Selle cada entrada o puerto de información con cinta de evidencia.
- De igual manera deben sellar los tornillos del sistema a fin de que no se puedan remover o reemplazar las piezas internas del mismo.
- Desconecte la fuente de poder.
- Quite las baterías (si funciona a base de baterías).



- Mantenga el sistema y medios de grabación separados de cualquier tipo de imán, o campo magnético.
- Al llevar aparatos, anote todo número de identificación, mantenga siempre la cadena de custodia.
- Lleve todo cable, accesorio, conexión.
- Lleve, si es posible, manuales, documentación, anotaciones.
- Tenga en cuenta que es posible que existen otros datos importantes en sistemas periféricos, si el aparato fue conectado a una red.

Si el equipo es una estación de trabajo (conectado en red) o está en un negocio, el desconectarla puede acarrear: Daño permanente el equipo, responsabilidad civil para la Policía Judicial y el Ministerio Público, interrupción ilegal del giro del negocio.

Otros aparatos electrónicos.

Teléfonos inalámbricos, celulares, smartphones

Se puede encontrar evidencia potencial contenida en los teléfonos inalámbricos tal como:

- Números llamados
- Números guardados en la memoria y en el marcado rápido.
- Identificador de llamadas, llamadas entrantes
- Otra información guardada en la memoria del teléfono
- Números marcados
- Nombres y direcciones
- Números personales de identificación (PIN)
- Número de acceso al correo de voz
- Contraseña del correo de voz
- Números de tarjetas de crédito
- Números de llamadas hechas con tarjeta
- Información de acceso al Internet y al correo electrónico
- Se puede encontrar valiosa información en la pantalla del aparato
- Imágenes. Fotos, grabaciones de voz



- Información guardada en las tarjetas de expansión de memoria.

REGLA DEL ENCENDIDO “ON” Y APAGADO “OFF”.

1. Si el aparato está encendido “ON”, no lo apague “OFF”.
 - Si lo apaga “OFF” puede iniciarse el bloqueo del aparato.
 - Transcriba toda la información de la pantalla del aparato y de ser posible tómese una fotografía.
 - Vigile la batería del aparato, el transporte del mismo puede hacer que se descargue. Tenga a mano un cargador.
 - Selle todas las entradas y salidas.
 - Selle todos los puntos de conexión o de admisión de tarjetas o dispositivos de memoria.
 - Selle los tornillos para evitar que se puedan retirar o reemplazar piezas internas.
 - Buscar y asegurar el conector eléctrico.
 - Colocar en una bolsa de FARADAY, (especial para aislar de emisiones electromagnéticas), si no hubiere disponible, en un recipiente vacío de pintura con su respectiva tapa.
2. Si el aparato está apagado “OFF”, déjelo apagado “OFF”.
 - Prenderlo puede alterar evidencia al igual que en las computadoras.
 - Antes del análisis del aparato consiga un técnico capacitado en el mismo.
 - Si no existe un técnico uso otro teléfono.
 - Es necesario que el investigador busque el manual del usuario relacionado con el aparato encontrado.

Aparatos de mensajería instantánea, beepers.

1. Beepers Numéricos (reciben solo números y sirven para transmitir números y códigos)
2. Beepers Alfanuméricos (reciben números y letras, pueden cargar mensajes completos en texto)
3. Beepers de Voz (pueden transmitir la voz y también caracteres alfanuméricos)
4. Beepers de dos vías (contienen mensajes de entrada y salida).
5. BUENAS PRÁCTICAS.



- Una vez que el beeper está alejado del sospechoso, éste debe ser apagado. Si se mantiene encendido los mensajes recibidos, sin tener una orden judicial para ello puede implicar una interceptación no autorizada de comunicaciones.
6. ¿Cuándo se debe buscar en el contenido del aparato?
- Cuando es la causa de la aprehensión del sospechoso
 - Cuando haya presunción del cometimiento de un delito flagrante.
 - Con el consentimiento del dueño o receptor de los mensajes.

Máquinas de fax

1. En las máquinas de fax podemos encontrar:
 - Listas de marcado rápido
 - Fax guardados (transmitidos o recibidos)
 - Bitácoras de transmisión de fax (transmitidos o recibidos)
 - Línea del encabezado
 - Fijación de la hora y fecha de la transmisión del fax..
2. BUENAS PRÁCTICAS.
 - Si la máquina de fax es encontrada prendida “ON”, el apagarla causaría la pérdida de la memoria del último número marcados así como de los facsímiles guardados.
3. Otras consideraciones:
 - Busque la concordancia entre el número de teléfono asignado a la máquina de fax y la línea de teléfono a la que está conectado.
 - De igual forma busque que el encabezado del mensaje y el número impreso coincidan con el del usuario y la línea telefónica.
 - Es necesario que el investigador busque el manual del usuario relacionado con el aparato encontrado.

Rastreo del correo electrónico.

El correo electrónico nos permite enviar cartas escritas con el computador a otras personas que tengan acceso a la Red. El correo electrónico es casi instantáneo, a diferencia del correo normal. Podemos enviar correo a cualquier



persona en el mundo que disponga de conexión a Internet y tenga una cuenta de correo electrónico.

Al enviar un correo electrónico, la computadora se identifica con una serie de números al sistema del proveedor de servicios de Internet (ISP). Enseguida se le asigna una dirección IP y es dividido en paquetes pequeños de información a través del protocolo TCP/IP. Los paquetes pasan por una computadora especial llamada servidor (server) que los fija con una identificación única (Message-ID) posteriormente los sellan con la fecha y hora de recepción (sello de tiempo). Mas tarde al momento del envío se examina su dirección de correo para ver si corresponde la dirección IP de alguna de las computadoras conectadas en una red local (dominio). Si no corresponde, envía los paquetes a otros servidores, hasta que encuentra al que reconoce la dirección como una computadora dentro de su dominio, y los dirigen a ella, es aquí donde los paquetes se unen otra vez en su forma original a través del protocolo TCP/IP (Protocolo de Control de Transferencia y Protocolo de Internet). Siendo visible su contenido a través de la interfase gráfica del programa de correo electrónico instalado en la máquina destinataria.

Hay que tomar en cuenta que los correos electrónicos se mantienen sobre un servidor de correo, y no en la computadora del emisor o del destinatario, a menos que el operador los guarde allí. Al redactarlos se transmiten al servidor de correo para ser enviados. Al recibirlas, nuestra computadora hace una petición al servidor de correo, para que los mensajes sean transmitidos luego a la computadora del destinatario, donde el operador lapuede guardar o leer y cerrar. Al cerrar sin guardar, la copia de carta visualizada en la pantalla del destinatario desaparece, pero se mantiene en el servidor, hasta que el operador solicita que sea borrada.

En algunas ocasiones es necesario seguir el rastro de los correos electrónicos enviados por el Internet. Los rastros se graban en el encabezamiento del e-mail recibido. Normalmente, el encabezamiento que aparece es breve. La apariencia del encabezamiento está determinada por el proveedor de servicios de Internet utilizado por nuestra computadora, o la de DRA. GRACIELA ENCALADA OCHOA



quien recibe el correo electrónico. Para encontrar los rastros, se requiere un encabezamiento completo o avanzado, posibilidad que existe como una opción en nuestro proveedor de servicios de Internet.

Para poder elegir la opción de un encabezamiento técnico, seleccione “encabezamiento completo o avanzado” por medio de **opciones** o **preferencias** en la barra de herramientas de la página Web de su proveedor de correo electrónico (YAHOO, GMAIL, HOTMAIL, etc.). El encabezamiento completo contiene información fácil y difícil de interpretar, por ejemplo: “TO”, “FROM” “CC”, datos fáciles de entender (el destinatario, el emisor, una copia enviada a, y el título del mensaje). Otros datos son más difíciles de entender, como los números IP: 148.235.52.34 o Message-id: NIBBLHGCOLIEFEEJKGEBCCAAA. abelardolopez98@prodigy.net.mx>. Esta información requiere interpretación.

Encabezado General.

Español	Inglés	Contenido
DE:	FROM:	Abelardo López <abelardolopez98@prodigy.net.mx>
ENVIADO:	SENT:	Miércoles, 11 de febrero, 2004 7:16 PM
PARA:	TO:	<kylegrimes@msn.com>
COPIA:	CC:	Gabriel Grimes <grimesgk@hotmail.com>
TÍTULO:	SUBJECT:	Hace mucho tiempo

El encabezamiento breve se lee desde arriba hacia abajo.

- **From o De**, emisor de la correspondencia, contiene el nombre del autor, Abelardo López, su identificación en el Internet, abelardolopez98, su nombre de dominio primario es un proveedor de servicios de Internet, prodigy, que tiene un dominio de red, .net, y que un dominio territorial, .mx, que pertenece a México.
- **Sent o Enviado**, es la fecha y hora de su envío, designado por la computadora de origen, Miércoles, 11 de Febrero, 2004, 7:16 PM.



- **To o Para**, destinatario de la correspondencia, contiene su identificación en el Internet, kylegrimes, su nombre de dominio primario es un proveedor de servicios de Internet, msn (Microsoft Network), que tiene un dominio de comercio, com.
- **CC**. Copia enviada a, contiene el nombre de otro destinatario secundario, Gabriel Grimes, su identificación en el Internet, grimesgk, su nombre de dominio primario es un proveedor de servicios de correspondencia electrónica, Hotmail, que tiene un dominio de comercio, com.
- **Subject o Título**, es el tema de la correspondencia escrita por el emisor, Hace mucho tiempo.

Los signos de puntuación, como los puntos, < >, y la @ son indicaciones para el protocolo de manejo en el Internet.

Encabezado Técnico.

MIME – Version: 1.0
Received: from [216.136.226.197] by Hotmail.com (3.2) with ESMTTP id MHotMailBD737B61008E4D888E2C506160; Thu, 20 Sep 2001 11:07:30-0700
Received: from [12.26.159.122] by web20808.mail.yahoo.com vía HTTP; Thu, 20 Sep 2001 11:07:29 PDT
From: Polaris99992001@yahoo.com Thu, 20 Sept 2001 11:07:58 -0700
Message-id: <20010920180729.36281.gmail@web20808.mail.yahoo.com>

El encabezamiento completo se lee desde abajo hacia arriba.

- Message-id, 20010920180729.36281.gmail@web20808.mail.yahoo.com, indica una identificación asignada al correo electrónico por el servidor que inicialmente procesó la correspondencia original. La identificación es única, y sirve para verificar la originalidad del mensaje.
- From, el emisor del mensaje y la fecha y hora de su envío (según la computadora que lo envió). Siempre se debe verificar el uso horario a fin de tener la hora correcta.
- Received from, muestra el número IP de la computadora del origen, 12.26.159.122, que puede ser un compuesto del número local y la red que procesa el mensaje, by, o por, el servidor que inicialmente procesó el



mensaje, web20808.mail.yahoo.com, vía, o por cual protocolo, http (protocolo de transferencia de hipertexto), fecha y hora del Internet, Thu, 20 Sep 2001 11:07:29 PDT (hora normal de la Zona del Pacífico).

- Received from, el número IP mencionado del destinatario, 216.136.226.197, by, o por, el servidor de HOTMAIL, Hotmail.com, with ESMTP id, una nueva identificación de mensaje asignado por el nuevo servidor, MHotMailBD737B61008E2C506160, la fecha y hora de su recepción, Thu, 20 Sep 2001 11:07:30-0700.
- MIME-Version: 1.0, es la versión de encabezado.

Con la información del encabezado técnico podemos verificar el origen del mensaje enviado, buscando con el número IP registrado el dominio de donde se originó el mensaje. Para eso se utiliza una interfaz, "WHOIS?" que significa "¿Quién es?", para determinar el servicio utilizado, ubicar la dirección geográfica de los servidores y los puntos de contacto, y localizar (a veces) la instalación donde se encuentra un computador.

Se puede poner la dirección IP en la página Web: <http://samspace.or> para averiguar los datos antes señalados, también se puede acudir a la página de INTERNIC. Podemos usar también meta buscadores como GOOGLE, ALTAVISTA, YAHOO, etc.⁴²

Peritos Informáticos.⁴³

Los peritos son personas que por disposición legal y encargo judicial o del Ministerio Público aportan con sus conocimientos los datos necesarios para que el Juez, el Fiscal o la Policía Judicial adquieran un grado de conocimiento para determinar las circunstancias en que se cometió una infracción. La presencia de los peritos en una diligencia es indispensable conforme lo preceptúa el Código de Procedimiento Penal.

⁴² Manual de Manejo de Evidencias Digitales y Entornos Informáticos. Departamento de Informática del Ministerio Fiscal Distrital de Pichincha. Versión 2007

⁴³ Introducción a la Informática forense. Dr. Santiago Acurio del Pino



Los requisitos que debe cumplir una persona para ser perito son:

- a. Ser profesional especializado y calificado por el Ministerio Público, poniendo a salvo un criterio, que es aquel de que no necesariamente el perito es un profesional en determinada rama, sino una persona experta o especializada en su respectivo campo de determinada materia. El Código de Procedimiento Penal faculta para que en ciertos casos de lugares donde se vaya a realizar una diligencia y no existan peritos habilitados, el Fiscal nombre a personas mayores de edad, de reconocida honradez y probidad que tengan conocimientos sobre la materia que van a informar.
- b. Mayores de edad, en nuestro país la mayoría de edad se fija en 18 años, considerando que a esa edad la persona ha alcanzado madurez psicológica necesaria para prestar esta clase de asesoramiento a la Administración de Justicia.
- c. Reconocida honradez y probidad, en cuanto a la calidad moral del perito, debe ser de proceder recto, íntegro y honrado en el obrar, el perito es un personaje esencialmente imparcial que cumple con su cometido y se desvincula del proceso.
- d. Conocimientos específicos en la materia sobre la que debe informar, es decir los necesarios y específicos para cumplir su cometido.

La pericia es un medio de prueba *“con el cual se intenta obtener para el proceso, un dictamen fundado en especiales conocimientos científicos, técnicos o artísticos, útil para el descubrimiento o valoración de un elemento de prueba”*⁴⁴.

El informe pericial no es definitivo ni concluyente, su valoración jurídica queda a criterio del Fiscal, del Juez Penal o Tribunal Penal, ellos pueden aceptarlo o no con el debido sustento o motivación.

El Perito Informático Forense según la opinión del profesor Jeimy Cano, citado por Santiago Acurio en su obra Introducción a la Informática Forense, requiere la formación de un perito informático integral que siendo especialista en

⁴⁴ Obra citada.



temas de tecnologías de información, también debe conocer sobre disciplinas jurídicas, criminalísticas y forenses, así se sugiere que el perito informático general debe tener una formación por lo menos en:

1. AREA DE TECNOLOGÍAS DE INFORMACIÓN Y ELECTRÓNICA:
 - Lenguajes de programación.
 - Teoría de sistemas operacionales y sistemas de archivo
 - Protocolos e infraestructuras de comunicación
 - Fundamentos de circuitos eléctricos y electrónicos
 - Arquitectura de computadores.
2. FUNDAMENTO DE BASES DE DATOS AREA DE SEGURIDAD DE LA FORMACIÓN:
 - Principios de Seguridad de la Información
 - Políticas estándares y procedimientos en seguridad de la información.
 - Análisis de vulnerabilidades de seguridad informática.
 - Análisis y administración de riesgos informáticos.
 - Recuperación y continuidad de negocio
 - Clasificación de la información.
 - Técnicas de hacking y vulneración de sistemas de información.
 - Mecanismos y tecnologías de seguridad informática
 - Concientización en seguridad informática.
3. ÁREA JURÍDICA:
 - Teoría General del Derecho
 - Formación básica en delito informático
 - Formación básica en protección de datos y derechos de autor
 - Formación básica en convergencia tecnológica.
 - Formación básica en evidencias digital y pruebas electrónicas
 - Análisis comparado de legislaciones e iniciativas internacionales
4. AREA DE CRIMINALÍSTICA Y CIENCIAS FORENSES:
 - Fundamentos de conductas criminales
 - Perfiles psicológicos y técnicos
 - Procedimientos de análisis y valoración de pruebas



- Cadena de custodia y control de evidencias
- Fundamentos de Derecho Penal y Procesal
- Ética y responsabilidades del perito
- Metodologías de análisis de datos y presentación de informes.

5. AREA DE INFORMÁTICA FORENSE:

- Esterilización de medios de almacenamiento magnético y óptico
- Selección y entrenamiento en software de recuperación y análisis de datos.
- Análisis de registros de auditoría y control
- Correlación y análisis de evidencias digitales
- Procedimientos de control y aseguramiento de evidencias digitales
- Verificación y validación de procedimientos aplicados en la pericia forense.



CAPITULO IV

CONCEPTUALIZACIÓN DE LA NATURALEZA DE LOS DELITOS INFORMÁTICOS SEGÚN LA LEGISLACION ECUATORIANA: PROPUESTA PARA SU TIPIFICACIÓN.

Planteamiento del Problema.

Los delitos informáticos han tenido un tratamiento tangencial en nuestra legislación, posiblemente debido al atraso tecnológico de nuestro país y a la tardía difusión masiva de los medios virtuales de información y comunicación, como la internet y el correo electrónico; la primera convertida en la gran autopista de la información, con la más grande cantidad de archivos de todos los tiempos en formatos de audio y de video, superior a todas las bibliotecas materiales juntas; y, el correo electrónico, considerado como el medio más eficaz de comunicación, desde y con cualquier lugar del mundo, transmitiendo información escrita, así como videos y música.

Esta enorme cantidad de información, ha generado la más grande revolución del conocimiento desde el surgimiento de la imprenta, que propició la difusión masiva de los textos escritos. Sin embargo, en forma concomitante a este desarrollo positivo, han surgido algunos actos atentatorios a ciertos derechos y garantías fundamentales, como la privacidad y la reserva de los datos personales, que no deben ser conocidos y difundidos sin autorización de su titular; o el grave atentado contra la moral colectiva, con la creación, distribución y comercialización de la pornografía infantil; o el peligro que representa la vulneración de secretos inherentes a la seguridad nacional, que podría atentar contra la supervivencia misma de un estado.

El problema se agrava aún más si se considera que los autores de dichos actos son, por lo general, personajes con estudios superiores, de un conocimiento tecnológico de tal naturaleza que les permite vulnerar claves y sistemas de seguridad para acceder a datos reservados contenidos en sistemas virtuales de información. Además, actúan en forma dolosa, es decir con un claro designio de



causar daño, aunque no se puede descartar su afán de divertirse participando en un juego perverso al invadir espacios reservados con el único afán de probar sus destrezas y habilidades. En todo caso, existe consenso en no considerarle al autor de una infracción informática como un delincuente común, sino más bien como un individuo con una formación y una capacidad intelectual superiores, que actúa sin peligro y a traición, escudado siempre en el presunto anonimato que le ofrece la posibilidad de vulnerar sistemas virtuales desde cualquier lugar del mundo, lo cual dificulta, aunque no imposibilita, su ubicación y, por ende, su posterior juzgamiento y sanción.

En nuestro país, recién con la expedición de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, publicada en el Registro Oficial No. 557 del 17 de abril del 2002, se incorporaron como infracciones penales algunas conductas que el legislador las ha considerado lesivas para ciertos bienes jurídicos. Así, por ejemplo, los delitos contra la información protegida; la destrucción maliciosa de documentos, títulos, programas, datos, base de datos, información o cualquier mensaje de datos contenidos en un sistema de información o red electrónica; la falsificación electrónica; los daños informáticos; la apropiación ilícita; y, la estafa.

Sin embargo, al tratar de individualizar algunos delitos informáticos que pueden ser absorbidos por la legislación penal común, se corre el riesgo ineludible de no poder cubrir todo el universo de infracciones, quedando en la impunidad algunas conductas dolosas. Y, lo adecuado sería no dejar resquicio alguno para la impunidad, es decir, que la ley penal tipifique como delitos a todas las conductas que puedan adoptar los infractores para lesionar bienes jurídicos protegidos, y determine su debida sanción, con una finalidad claramente disuasiva.

Por lo tanto, nuestro objetivo es formular una propuesta que englobe a una gran variedad de acciones susceptibles de ser reprimidas penalmente, y que se dividiría en dos grupos perfectamente diferenciados:

1. Los actos netamente virtuales, cuya tipificación se agruparía en un capítulo especial, cuya denominación podría ser: "Delitos Informáticos"; y,



2. Los delitos que ya se encuentran tipificados en la ley penal común, pero que se cometen mediante la utilización de medios virtuales, informáticos o similares; en este caso, no consideramos adecuado el detallarlos e imponer penas especiales para cada caso, pues, como se dijo anteriormente, van a quedar en la impunidad algunas acciones ante la dificultad de detallar todo el universo de delitos que pueden ser cometidos en esa forma. Para evitar esta posibilidad real, la utilización de medios virtuales para cometer delitos comunes, a nuestro criterio debería considerarse como circunstancias agravantes, que impedirían rebajar la sanción por circunstancias atenuantes y, al contrario, permitirían el incremento de la pena. Las justificaciones para este tratamiento, serían las siguientes: el utilizar medios virtuales, electrónicos o telemáticos aumenta la malicia del acto, la alarma ocasionada en la sociedad y revela la peligrosidad de sus autores, pues utilizan conocimientos tecnológicos avanzados, tienen una formación superior y actúan sin peligro, con evidente alevosía, al encontrarse protegidos por el anonimato que les proporcionan los sistemas virtuales para la comisión de un delito común.

CONDUCTAS SUSCEPTIBLES DE SER TIPIFICADAS COMO DELITOS INFORMÁTICOS EN NUESTRO CÓDIGO PENAL:

1.- ACCESO A LA INFORMACIÓN PROTEGIDA

a) Justificación.

Por información protegida se entiende toda base de datos o toda información restringida al conocimiento y uso de otras personas. Al conectarse a una red a través de la internet, se tiene acceso a otras redes y por lo tanto a otros sistemas informáticos; es por ello que se puede compartir información. Sin embargo, siempre existirán sistemas de datos de carácter confidencial y, en forma concurrente, la posibilidad de que personas inescrupulosas ingresen a esa información sin autorización de los titulares.



La información confidencial, puede ser pública o privada. De orden público cuando se refiera a sistemas de datos estatales, que pueden ser de uso civil o militar, de interés económico o de seguridad nacional. Y, también, existen datos e información reservada de uso particular, como, por ejemplo, los secretos de ciertas empresas que se los debe mantener en reserva de la competencia; o, los datos personales que no deben ser conocidos por el resto de la comunidad sin la autorización de su titular, para no vulnerar el derecho constitucional de protección a la intimidad.

El tratamiento que nuestra legislación penal proporciona a estos actos dolosos, es el adecuado. Sin embargo, puede organizarse de mejor manera la tipificación de las acciones y la determinación de las penas, ubicándolas en forma conjunta pero estableciendo diferentes penas según la gravedad del daño causado, en atención al principio de proporcionalidad consagrado en el Art. 76 numeral 6 de la Constitución, desde el simple acceso a la información, su divulgación o utilización fraudulenta, hasta la comisión de estos hechos por parte de los custodios o encargados del resguardo de la información.

b) Bien jurídico protegido.

Los bienes jurídicos protegidos son varios: La seguridad interior y exterior del Estado, cuando los datos son públicos; y la intimidad, en caso de datos privados, considerada como una garantía constitucional consagrada en nuestra Constitución. A su vez la información privada debe tener un tratamiento diferenciado, cuando, por ejemplo, se trate de secretos comerciales o industriales, cuyo conocimiento y divulgación causaría daños graves a sus titulares, o si concierne a intereses individuales, que merecen también sanción pero que, por ser tales, tienen una importancia menor.

Además, en el caso de la vulneración a la información protegida por parte de un custodio, es decir, por aquella persona que por obligación laboral o administrativa debe resguardar la información, el bien jurídico lesionado sería también la “fidelidad” que el empleado o trabajador debe a la institución, a la empresa o a la persona a quien presta sus servicios.



c) Verbo rector

El acto delictivo consiste en el “acceso” a la información protegida; es decir, el verbo nuclear es “acceder” a una base de datos confidencial, sin la autorización de su titular, que puede ser el Estado y sus instituciones, o una persona natural o jurídica de orden privado; la pena será mayor si el titular es una institución pública, intermedia si se trata de una persona jurídica privada y menor cuando sea una persona natural.

Otro de los verbos rectores que determinaría una circunstancia agravante constitutiva de la infracción, es “divulgar” o “utilizar” en forma fraudulenta la información a la que se tuvo un acceso ilegal.

Finalmente, estos actos son sancionados con una pena mayor si son cometidos por personas encargadas de su custodia, vulnerando, en forma grave, sus obligaciones.

d) Texto propuesto:

Art. ...: El que accediere a información protegida de cualquier tipo vulnerando claves o sistemas de seguridad con algún sistema electrónico, informático o similar, será reprimido con prisión correccional de seis meses a dos años y multa de quinientos a mil dólares. La divulgación o utilización fraudulenta de dicha información protegida, será sancionada con prisión correccional de uno a tres años y multa de mil a dos mil dólares. Si estos actos son realizados por el custodio o persona encargada del resguardo de la información, la pena será de prisión de dos a cinco años y multa de dos mil a cuatro mil dólares.

Si la información correspondiese a secretos comerciales o industriales, la pena será de prisión correccional de uno a tres años y multa de un mil a tres mil dólares. La divulgación o utilización fraudulenta de tales secretos, será sancionada con prisión de dos a cinco años y multa de dos mil a cuatro mil dólares. En caso de estos actos lo cometa el custodio de la información, la pena será de reclusión menor de tres a seis años y multa de tres mil a ocho mil dólares.



Si la información estuviere vinculada a intereses públicos o secretos de seguridad nacional, la pena será de reclusión menor ordinaria de tres a seis años y multa de tres a diez mil dólares. La divulgación o utilización fraudulenta de dicha información, será sancionada con reclusión menor ordinaria de seis a nueve años y multa de cinco a quince mil dólares. Si el autor de estos actos fuere el custodio de la información, la pena será de reclusión menor extraordinaria de nueve a doce años.

2.- OBTENCIÓN Y UTILIZACIÓN NO AUTORIZADA DE DATOS PERSONALES|

a) Justificación

La obtención de datos personales de un individuo, sin vulnerar claves o sistemas de seguridad como en el caso anterior, para su publicación o transferencia a cualquier título sin la autorización de su titular, sin lugar a dudas vulnera su derecho constitucional a la intimidad, a la reserva sobre sus datos y a su libre y voluntaria disponibilidad de acuerdo a sus propias, íntimas e inalienables conveniencias.

En este caso, la pena debe ser ostensiblemente menor, de acuerdo al principio consagrado en nuestra Constitución sobre la proporcionalidad que debe existir entre la pena y la infracción; es decir, mientras más grave sea el daño causado, más dura debe ser la sanción. Es así que nuestra legislación sanciona el caso propuesto de una manera adecuada y aceptable, con pena de prisión correccional, pues el ofendido es una persona natural, no se han vulnerado claves o sistemas de seguridad y el acto consiste en que no existió autorización para publicar o transferir los datos referidos a esa persona.

b) Bien jurídico protegido

El bien jurídico protegido es la intimidad, es decir el derecho que tiene un individuo a la libre disponibilidad de sus datos personales, utilizándolos como a bien tuviere o manteniéndolos en reserva a su libre criterio, derecho que se lesiona en forma grave si se los publica o transfiere sin la autorización de su titular.



c) Verbo rector

El Art. 202.2 de nuestro Código Penal tiene una redacción adecuada en su primera parte, pues en ella se tipifican las acciones fundamentales y concurrentes de este delito, que consisten en “obtener” los datos de una persona y “utilizarlos” sin la autorización de su titular; es decir que la simple obtención de dichos datos no agota el delito, pues, para que éste se configure, se requiere, además, que el autor de la infracción los publique o transfiera sin la autorización de su titular.

Sin embargo, en su segunda parte, su redacción es imprecisa y redundante, pues se utilizan los siguientes verbos: “ceder”, “publicar”, “utilizar” o “transferir a cualquier título”. Al respecto, sin ningún esfuerzo, se observa que la acción de ceder se encuentra subsumida en la transferencia a cualquier título, pues es evidente que la cesión de datos personales es una forma de transferencia. En igual sentido, el verbo “utilizar” subsume, a su vez, las acciones de publicar o transferir, que constituyen formas evidentes de utilización; en otras palabras, si alguien publica o transfiere esos datos, simplemente los está utilizando.

En definitiva, nuestra propuesta es que la acción debe tipificarse mediante el verbo rector “utilizar” los datos personales, en cualquier forma, para que se configure el delito, pues el “publicar”, “transferir” y “ceder” son evidentes formas de “utilización”. En conclusión, la innecesaria referencia a otros verbos, sólo provoca dificultad en la comprensión de la norma.

d) Texto propuesto

Art. ...: Quien obtuviere información sobre datos personales y los utilizare, en cualquier forma, sin autorización de su titular, será sancionado con prisión correccional de dos meses a dos años y multa de quinientos a dos mil dólares.



3.- ELIMINACIÓN MALICIOSA DE UNA BASE DE DATOS

a) Justificación

Es posible que las personas encargadas de un servicio público, sean o no funcionarios públicos, abusen de sus funciones en perjuicio del Estado o de los particulares. Si el abuso se perpetra sobre dineros o bienes que se encuentren en su poder en virtud o razón de su cargo, se configura el delito de peculado, tipificado en el Art. 257 y sancionado con ocho a doce años de reclusión mayor ordinaria. Y, si la persona encargada de un servicio público, en forma maliciosa, elimina una base de datos, será sancionado con reclusión menor de tres a seis años aplicando el Art. 262 del Código Penal.

Esta última norma, a pesar de estar bien concebida, tiene serias falencias pues su redacción es imprecisa, incorrecta, confusa e inadecuada, como lo veremos a continuación.

En primer lugar se refiere a los empleados públicos y a “toda persona encargada de un servicio público”; para evitar esta redundancia, el texto que propondremos podría correctamente limitarse, en forma sencilla, a “las personas encargadas de un servicio público”.

A continuación señala que la acción debe ser “maliciosa y fraudulenta”, sin reparar en que el un adjetivo contiene al otro, pues no existe fraude sin malicia; por lo tanto, para establecer el dolo, es suficiente referirse a la acción “maliciosa”.

En lo que concierne a la acción delictiva, se la tipifica con dos verbos: “destruir” y “suprimir”. Al respecto se observa que la “destrucción” de una base de datos debe referirse, necesariamente, al hardware o soporte material que lo contiene; en cambio la “supresión” correspondería a la manipulación del sistema informático para eliminar tales datos. Estas dos posibilidades podrían resumirse en una sola acción: “eliminar” una base de datos “en cualquier forma”, lo cual abarcaría todas las posibilidades imaginables.

También se hace una descripción de los elementos virtuales protegidos, especificando que pueden ser “documentos, títulos, programas, datos, base de



datos, información o cualquier mensaje de datos”; cuando bien podría haberse referido la norma a “cualquier elemento o dato contenido en sistemas de información o redes electrónicas”, lo que abarcaría no sólo a aquellos detallados por el legislador sino a cualquier elemento virtual sobre el que recaiga la acción delictiva.

Un delito similar lo encontramos en el Art. 415.1, en el que se utilizan los verbos “destruir, alterar, inutilizar, suprimir o dañar de forma temporal o definitiva”, programas, datos, base de datos, información “o cualquier mensaje de datos”, con la diferencia que este delito lo puede cometer cualquier persona. Las sanciones son las siguientes: seis meses a tres años de prisión y multa de 60 a 150 dólares; y, en caso de tratarse de una base de datos destinada a un servicio público o a la defensa nacional, prisión de tres a cinco años y multa de 200 a 600 dólares. Sobre este asunto, nuestra propuesta es que se unifiquen estos dos artículos, a fin de que una sola norma, clara y completa, abarque estas posibilidades; y que la acción delictiva se amplíe a la “alteración” de tales datos.

Por último, también se encuentra el Art. 415.2, que se refiere a la “destrucción, alteración o inutilización” de las instalaciones físicas necesarias para la “transmisión, recepción o procesamiento” de mensajes de datos, que, siempre que no se trate de un delito mayor, será reprimido con prisión de ocho meses a cuatro años y multa de 200 a 600 dólares. Consideramos que sería conveniente que esta disposición también se unifique en un solo artículo.

b) Bien jurídico protegido

Es indudable que con esta norma legal se pretende proteger, en primer lugar, el servicio público, que se verá lesionado si se eliminan los elementos o datos contenidos en un sistema informático, que el encargado de ese servicio lo tiene en su poder en razón de su cargo, es decir, para el cumplimiento de sus funciones.

En segundo lugar, se puede establecer como bien jurídico protegido la “fidelidad” que el encargado de un servicio público está obligado a observar con respecto a la entidad para la cual presta sus servicios.



Y, por último, también se verá afectado el interés público, cuando el servicio dirigido a la comunidad se vea eliminado o alterado por la acción dolosa del encargado de su custodia y funcionamiento.

c) Verbo rector

Los verbos rectores serían los siguientes: “eliminar” o “alterar” cualquier elemento o dato contenido en un sistema informático que el infractor tenga en su poder en razón de su cargo. Y, también, “destruir” las instalaciones físicas en las que se encuentren los soportes informáticos o sirvan para la transmisión o procesamiento de tales datos.

d) Texto propuesto

“Art. ... Quien, en forma maliciosa, elimine o altere elementos o datos contenidos en un sistema informático o **red electrónica**, será sancionado con seis meses a tres años de prisión y multa de cincuenta a doscientos dólares. Si se tratare de datos necesarios para un servicio público o la defensa nacional, la pena será de tres a seis años de reclusión menor. Si el autor es el encargado de un servicio público, que tuviere en su poder tales datos en razón de su cargo, será sancionado con cuatro a ocho años de reclusión mayor ordinaria.

Siempre que no se trate de un delito mayor, si se destruyeren las instalaciones físicas en la que se encuentren tales sistemas informáticos, o sirvan para su procesamiento o transmisión, la pena será de uno a cinco años de prisión. Si los datos estuvieren destinados a un servicio público o a la defensa nacional, la pena será de tres a seis años de reclusión menor. Y, si el autor de tales destrucciones es el encargado de su custodia o las instalaciones se encuentran en su poder en razón de su cargo, la pena será de cuatro a ocho años de reclusión mayor ordinaria.”

En conclusión, se eliminarían los Arts. 415.1 y 415.2.



4) FALSIFICACIÓN ELECTRÓNICA

a) Justificación

Además de las falsificaciones de documentos físicos, sean públicos o privados, es posible la falsificación informática, es decir, la alteración de los datos contenidos en un soporte informático con la finalidad de perjudicar a quien tenga derecho sobre tales datos o sea su beneficiario.

La falsificación siempre va a generar beneficios al autor; sin embargo, no se puede descartar la posibilidad de que su única finalidad sea causarle algún daño a su titular, bien sea por venganza, animadversión o cualquier otra causa.

La falsedad de un documento material público o privado, puede realizarse de diferentes maneras:

1. Alterando los datos de un documento auténtico, para lo cual se requiere la preexistencia de tal documento en el cual el autor de la falsificación altera los datos o firmas constantes en su texto. Se conoce como la falsedad material.
2. La segunda posibilidad es la falsedad ideológica, que ocurre al elaborar el documento, siendo el autor quien lo confecciona y coloca como verdaderos datos falsos, bien sea alterando firmas o frases, intercalando convenciones no reales o haciéndolas desaparecer. El tratadista Jorge Zavala Baquerizo, en obra "Delitos contra la Fe Pública, La Falsedad Instrumental", Tomo II, Pág. 181, textualmente señala: "En la falsedad ideológica el agente hace constar, en el momento de la formación del instrumento, como su contenido, un hecho, o una declaración de voluntad, o de conocimiento, como verdaderos, cuando el agente está consciente de que no lo son".
3. Por último, se encuentra la falsedad ideal, que, según el mismo tratadista, consiste en la "creación" total del instrumento, mediante la imitación o falsificación o el fingimiento o la forjadura.

Estas tres posibilidades, están contempladas en nuestra legislación.



Así tenemos se puede asimilar a la falsedad “material” la alteración de datos preexistentes contenidos en un soporte informático, con la finalidad de causar un perjuicio a su titular.

En cambio, si el agente infractor coloca datos falsos, suprime o inventa cláusulas o convenios, cometería un delito de falsedad ideológica.

Por último, si en un soporte informático se imita o forja una base de datos, con apariencia de verdadera pero conteniendo datos falsos, esa acción dolosa se encasillaría en la falsedad ideal.

En conclusión, en nuestra opinión se debe tipificar de mejor manera esas conductas dolosas susceptibles de lesionar bienes jurídicos protegidos, con la finalidad de que no queden en la impunidad. Mucho más aún si tomamos en consideración que las actuaciones judiciales y las notificaciones de decretos, autos y sentencias se realizan a través de correos electrónicos y que, en un futuro cercano, todos los archivos públicos constarán en soportes informáticos.

Además, nuestro Art. 353.1 del Código Penal nos remite a las penas establecidas para la falsificación de documentos en general, por lo que no es adecuado que se pretenda en dicha norma regular todos los casos. Basta, por lo tanto, referirse a cualquiera de las circunstancias establecidas en la ley, para abarcar las circunstancias posibles, sin caer en el riesgo de dejar en la impunidad algunas conductas que lesionan bienes jurídicos protegidos, como la utilización dolosa de datos falsos contenidos en un soporte informático, que no se encuentra prevista.

b) Bien jurídico protegido

El bien jurídico principal, sin lugar a dudas, es la fe pública, es decir la presunción de veracidad que tienen los instrumentos públicos o privados, que se hace extensivos a los que constan en soportes informáticos o electrónicos.

Pero también, con estos actos dolosos, se pueden lesionar otros bienes jurídicos protegidos como la propiedad, si con estos métodos alguien es despojado de sus bienes. O al buen nombre y buena fama, si se hacen constar



antecedentes o circunstancias que puedan lesionar la credibilidad y la honorabilidad de una persona.

c) Verbo rector

Como verbos rectores de esta infracción, podrían ser, según nuestra propuesta, los que definen las siguientes acciones, equiparables a la falsificación de documentos materiales:

1. Alterar una base de datos preexistente en alguno de sus elementos esenciales o formales, de tal manera que se desnaturalice en sus objetivos y, por lo tanto, se asimilaría a la falsedad material.
2. Crear una base de datos con apariencia de verdadera, pero con elementos no verdaderos, como la falsa intervención de personas o incluyendo acuerdos inexistentes o suprimiendo los verdaderos, que sería la falsedad ideológica.
3. Simular o forjar una base de datos inexistente, con apariencia de verdadera, que correspondería a la falsedad ideal.

d) Texto propuesto

“Art. ... Quienes cometieren una falsedad, imitación o forjamiento en cualquiera de los casos señalados en el CAPÍTULO III, del TÍTULO IV, del LIBRO II, del Código Penal, en una base de datos o mensajes contenidos en un soporte informático o electrónico, utilizando cualquier medio, serán reprimidos con las penas que constan en dicho capítulo para la falsificación de documentos en general; en igual forma se sancionará a quienes utilicen dolosamente la información falsa”.

USO DE MEDIOS INFORMÁTICOS PARA LA COMISIÓN DE DELITOS COMUNES, COMO CIRCUNSTANCIA AGRAVANTE DE LA INFRACCIÓN

a) Justificación

Hemos analizado que pueden existir delitos informáticos independientes del resto de delitos, es decir, delitos especiales que deben ser tratados en forma



separada, bien sea en un solo capítulo o en los capítulos que corresponda de acuerdo a los bienes jurídicos protegidos.

Los medios electrónicos o informáticos pueden ser utilizados para la comisión de delitos comunes, cuya descripción correría el riesgo de ser restrictiva, es decir, no alcanzar al detalle de todo el universo de delitos susceptibles de ser cometidos a través de tales medios. Así tenemos la apropiación ilícita de bienes, tipificada como delito independiente en los Arts. 553.1 y 553.2 del Código Penal. O la estafa con medios electrónicos o informáticos, que se la tipifica en el último inciso del Art. 563 del Código Penal. Sin embargo, también se pueden cometer otros delitos utilizando esos medios, sin que esta posibilidad se encuentre prevista en nuestra ley penal; por ejemplo, el delito de peculado, cohecho, concusión, estupro o injurias, por mencionar algunos de ellos, por lo que se requiere de una norma general que abarque todas estas posibilidades y se considere la utilización de medios informáticos o electrónicos como una circunstancia que aumenta la pena prevista para la infracción.

Se puede considerar el uso de medios informáticos o electrónicos como circunstancias agravantes, pues, al ser un medio en el que no se enfrenta el autor a la víctima y, eventualmente, puede ser muy difícil su detección, podría considerarse que se actúa a traición y sobre seguro, que son las formas que configuran la alevosía. Si a este análisis le añadimos que estos delitos son cometidos por personas que tienen conocimientos técnicos suficientes, es decir, no se trata de delincuentes comunes, podremos arribar a la conclusión de que este actuar taimado y mañoso aumenta la malicia del acto, la alarma que produce en la sociedad y la peligrosidad del autor.

Por último, al ser una circunstancia agravante bloquea la posibilidad de que se disminuya la pena por las circunstancias atenuantes, de acuerdo a las reglas contempladas en los Arts. 72, 73 y 74 del Código Penal.



d) Texto propuesto

Agregar otro artículo a continuación del Art. 30.1 del Código Penal, con el siguiente texto:

“Art. 30.2. Se considera circunstancia agravante especial, el ejecutar la infracción utilizando medios electrónicos o informáticos; en estos casos, el mínimo de las penas previstas para la infracción se aumentará en seis meses y no podrá rebajarse las penas con la aplicación de atenuantes.”



CONCLUSIONES Y RECOMENDACIONES

Es importante poner de relieve que la delincuencia cibernética, generalmente se basa en el delito instrumentado por el uso de la computadora a través de redes telemáticas y la interconexión de la computadora. Las ventajas y las necesidades del flujo nacional e internacional de datos, que aumenta de modo creciente en países donde la tecnología está más avanzada y en otros en donde se está desarrollando notablemente, conlleva también a la posibilidad creciente de estos delitos. Es por esta razón, que la criminalidad informática constituye un reto considerable, tanto para los sectores afectados, como para los legisladores, funcionarios judiciales y autoridades policiales encargadas de las investigaciones.

Resulta necesario alertar a los usuarios sobre la posibilidad de la ocurrencia de estos crímenes y delitos informáticos de los cuales la comunidad recién se está enterando que existen y animarlos a buscar y cerrar toda brecha de inseguridad que exista en sus sistemas computarizados. Gran parte de los problemas, se encuentra en la inacción de la víctima potencial. Las organizaciones que dependen cada vez más de las computadoras deben llegar a tener conciencia de que la implementación de medidas de seguridad son una inversión y no un gasto.

Dado el carácter transnacional de los delitos cometidos mediante el uso de las computadoras, es conveniente establecer tratados de extradición o acuerdos de ayuda mutua entre los países, que permitan fijar mecanismos sincronizados para la puesta en vigor de instrumentos de cooperación internacional y así contrarrestar eficazmente la incidencia de la criminalidad informática⁴⁵.

Como se ha dicho, con el desarrollo científico técnico, y el aumento del intercambio de información y la participación activa de nuestro país en el mundo, no estamos exentos de la aparición de nuevas modalidades delictivas que planteen variaciones en los elementos tradicionales del tipo legal y que conlleven

⁴⁵ El sabotaje o daño informático. Dra. María Cristina Vallejo.
<http://www.dlh.lahora.com.ec/paginas/judicial/PAGINAS/D.Informatico.28.htm>



por tanto la necesidad de ciertas modificaciones en la redacción de los preceptos para ajustarlos a las nuevas realidades.

Es evidente, que el Derecho Penal no puede estar ajeno al impacto que ha significado el desarrollo de las tecnologías informáticas en todas las esferas de la vida de la sociedad e, incluso, en otras ramas del Derecho.

La existencia de conductas tipificables, sobre todo por el daño que provocan sus resultados, no debe hacernos perder de vista, sin embargo, que en las mismas se involucran con mucha frecuencia jóvenes cuya motivación es ante todo lúdica, o de ofrecer demostraciones de inteligencia o retos a la misma, lo que supone, incluso, la participación de algunos profesionales informáticos en hechos de esta naturaleza. Ello indica la necesidad, más que de reprimir, de trabajar en la formación de valores en la ciudadanía.

Ecuador ha dado los primeros pasos en el desarrollo de iniciativas que permiten la investigación y sanción de los delitos informáticos, sin embargo, es preciso desarrollar, mejorar e implementar mecanismos que permitan que dichas investigaciones se desarrollen dentro de marcos regulados, controlados y mediante el uso de tecnología apropiada por parte los entes y profesiones dedicados a su investigación. Por ello considero necesario que se debe tipificar esta nueva conducta ilícita como delito en el Código Penal del Ecuador, y brindarle la importancia que merece este tipo de delito, tomando en consideración que en nuestro país existe un incremento en el uso de la tecnología en las diversas actividades del hombre.

Se debe promover la correcta aplicación de las pruebas electrónicas en los procesos penales, para garantizar el acceso a la justicia de las víctimas de estos nuevos delitos, se deben establecer cursos de capacitación para jueces, magistrados y personal judicial sobre estos tipos penales, buscando encaminarlas a que tomen las decisiones más ajustadas a derecho, garantizando de esta manera, el respeto a los derechos humanos fundamentales de los sujetos pasivos; se deben crear cuerpos de peritos judiciales en informática para que puedan colaborar y asesorar a las víctimas.



Se torna necesario aportar con investigaciones jurídicas en el área de la informática, para que, tanto abogados como personas interesadas tengan una fuente donde acudir, ya que sin lugar a dudas en un futuro cercano los asuntos en materia de Derecho Informático y las Nuevas Tecnologías de la Información serán tratados con más frecuencia.

Finalmente, debe destacarse el papel del Estado, que aparece como el principal e indelegable regulador de la actividad de control del flujo informativo a través de las redes informáticas.

Con el fin de tener una idea un poco más clara sobre el tratamiento y valoración dada a la evidencia digital en los órganos pertenecientes al aparato judicial, nuestro trabajo de campo se basó en conseguir información en las diferentes Salas de lo Penal y Tránsito de la Corte Provincial de Justicia del Azuay, así como en los Juzgados y Tribunales de Garantías Penales del Azuay, sobre: si desde el año 2002 en que está en vigencia la Ley de Comercio Electrónico, Firma Electrónica y Mensaje de Datos, se encuentran registrados procesos por delitos informáticos y el estado en que se encuentran dichos procesos; así como obtener información sobre los peritos acreditados en la Fiscalía del Azuay, en materia informática.

A continuación me permito realizar un resumen de los resultados obtenidos:

- PRIMERA SALA DE LO PENAL Y TRÁNSITO DE LA CORTE PROVINCIAL DE JUSTICIA DEL AZUAY:

Se encuentra inventariada la causa penal No. 474-09 seguida en contra de Johann Patricio Delgado Gárate por delitos contra la información protegida (Art. 202.1 Código Penal) en perjuicio de Marco Vinicio Bermeo Guambaña. El proceso fue resuelto por la Primera Sala Especializada de lo Penal y Tránsito en fecha 8 de septiembre del 2009, a las 09H00, revocándose el auto de llamamiento a juicio y dictándose a favor del procesado el Auto de Sobreseimiento Definitivo. (ANEXO 1).

- SEGUNDA SALA DE LO PENAL Y TRÁNSITO DE LA CORTE PROVINCIAL DE JUSTICIA DEL AZUAY:



En esta Sala Especializada, desde su especialización, NO se encuentra inventariada causa alguna por delitos informáticos. (ANEXO 2).

- JUZGADO PRIMERO DE GARANTÍAS PENALES DEL AZUAY:

En este Juzgado, desde hace DIEZ años **NO** se encuentra causa penal alguna por Delitos Informáticos. (ANEXO 3).

- JUZGADO SEGUNDO DE GARANTÍAS PENALES DEL AZUAY:

Desde el año 2002 a la fecha **NO** se encuentra inventariada causa penal alguna por Delitos Informáticos. (ANEXO 4).

- JUZGADO TERCERO DE GARANTÍAS PENALES DEL AZUAY:

Desde hace diez años hasta la fecha, **NO** se encuentra inventariada causa alguna por Delitos Informáticos. (ANEXO 5).

- PRIMER TRIBUNAL DE GARANTÍAS PENALES DEL AZUAY:

Desde el año 2002 **NO** se encuentran registrados procesos por Delitos Informáticos. (ANEXO 6)

- SEGUNDO TRIBUNAL DE GARANTÍAS PENALES DEL AZUAY:

NO se encuentra inventariada causas penales con respecto a delitos informáticos desde el año 2002 a la fecha. (ANEXO 7).

- TERCER TRIBUNAL DE GARANTÍAS PENALES DEL AZUAY:

NO se encuentra registrados procesos por delitos informáticos. (ANEXO 8).

- LA DIRECCIÓN PROVINCIAL DE AZUAY DEL CONSEJO DE LA JUDICATURA, certifica que, en el Registro de Peritos de la Fiscalía del Azuay, consta únicamente el Dr. Juan Peña Aguirre, como Perito en Informática-Documentología, desde el 27 de abril del 2005. (ANEXO 9).



Los resultados obtenidos en nuestra investigación de campo, evidencia que no existen causas presentadas por delitos informáticos en el Azuay, lo cual no podemos atribuir a que no se cometan este tipo de infracciones, sino a nuestro criterio creemos se debe a desconocimiento tanto de usuarios de las tecnologías como de los profesionales del Derecho, sobre este tema, por lo que consideramos que es imprescindible que las Facultades de Jurisprudencia de las Universidades del país, implementen en su pensum de estudios las asignaturas: Informática Jurídica y el Derecho Informático, con el fin de contar con una nueva generación de profesionales Abogados con conocimientos sobre la temática y que darán respuesta a la creciente necesidad de la sociedad de contar con asesores entendidos y capaces de brindar sustento y respaldo legal a cada una de las actividades que se desarrollan con soporte de las tecnologías de la información.



BIBLIOGRAFÍA

- ACURIO DEL PINO, Santiago. “*Delitos Informáticos: Generalidades*”. Material proporcionado en clase en la Maestría en Derecho Informático. Cuenca-Ecuador.
- ACURIO DEL PINO, Santiago. “*El Fraude y los Daños Informáticos*”. Material proporcionado en clase en la Maestría en Derecho Informático. Cuenca-Ecuador.
- ACURIO DEL PINO, Santiago. “*Introducción a la Informática Forense*”. Material proporcionado en clase en la Maestría en Derecho Informático. Cuenca-Ecuador.
- ACURIO DEL PINO, Santiago. “*La Delincuencia Informática Transnacional y la UDIMP*”.
- ACURIO DEL PINO, Santiago Martín. “*Análisis crítico del tipo penal de la Apropiación Ilícita en la Legislación Ecuatoriana*”. Revista de Derecho Informático. ISSN 1681-5726. Edita. Alfa-Redi.
- BARZALLO, José Luis. “*Ecuador: El Comercio Electrónico en el Ecuador, Desafío frente al Nuevo Siglo*”.
- BRAMONT-ARIAS TORRES, Luis Alberto. “*Delitos Informáticos*”. Publicado en Revista Peruana de Derecho de la Empresa “Derecho Informático y Teleinformática Jurídica” No. 51.
- CABANELLAS DE LAS CUEVAS, Guillermo (Director); MONTES DE OCA, Angel (Coordinador). “*Derecho de Internet*”. Heliasta.
- CAMPOLI, Gabriel Andrés. “*Delitos informáticos en la legislación mexicana*”. Instituto Nacional de Ciencias Penales. México, 2007.
- CODIGO PENAL DEL ECUADOR. Actualizado a marzo de 2009.



- DAVARA RODRÍGUEZ, Miguel Angel, “*Análisis de la Ley de Fraude Informático*”,
Revista de Derecho de UNAM. 1990”
- FERNÁNDEZ TERUELO, Javier Gustavo. “Cibercrimen. Los Delitos cometidos a
través de Internet.” editorial_ccc@telefonica.net. Librería Ojanguren. 2007.
- GÓMEZ PÉREZ, Mariana. Revista de Derecho Informático Alfa-Redi. No. 10,
mayo de 1999, “Criminalidad Informática: un fenómeno de fin de siglo”.
- GONZÁLEZ AGUILAR, Audilio; CARRASCOSA LÓPEZ, Valentin; BAUZA
REILLY, Marcelo. “*El Derecho de la prueba y la informática. Problemática y
perspectivas*”. Edita: Universidad Nacional de Educación a Distancia. Centro
Regional de Extremadura – Mérida. 1991.
- GONZÁLEZ RUS, Juan José
“*Protección Penal de Sistemas, Elementos, Datos, Documentos y Programas
Informáticos*”.
- HUERTA MIRANDA, Marcelo y LÍBANO MANZUR Claudio, Los Delitos
Informáticos, Editorial Jurídica Cono Sur. Obra citada por Dr. Santiago
Acurio Del Pino, en su obra “Delitos Informáticos: Generalidades”
- LANCHO PEDRERA, Francisco. “*La Criminalidad Informática en el Código Penal
de 1995*”.
- LANDAVERDE CONTRERAS, Melvin Leonardo; SOTO CAMPOS, Joaquín
Galileo; TORRES LIPE, Jorge Marcelo.
“*Delitos Informáticos*” (octubre de 2000)
- LEY DE COMERCIO ELECTRÓNICO, FIRMA ELECTRÓNICA Y MENSAJES DE
DATOS. Ley 67, Registro Oficial Suplemento 557 de 17 de Abril del 2002.
- LEGISLACIÓN NICARAGÜENSE ANTE LOS DELITOS INFORMATICOS. Corte
Suprema de Justicia Nicaragua. “*Delitos Informáticos. Legislación y el
Manejo de la Información en la era del conocimiento*”.



MANUAL DE MANEJO DE EVIDENCIAS DIGITALES Y ENTORNOS INFORMÁTICOS. Ministerio Público del Ecuador. Departamento de Informática del Ministerio Fiscal Distrital de Pichincha. Versión 2007.

PLAN NACIONAL DE POLÍTICA EXTERIOR. Ministerio de Relaciones Exteriores. República del Ecuador. “*Delincuencia Transnacional y el Crimen Organizado en el Ecuador*”.

POLAINO NAVARRETE, Miguel,

Curso de Derecho Penal Español, Madrid, 1996, p. 402.

Artículos publicados en Internet:

GUERRA CALDERÓN, Ramiro .

“Infracciones electrónicas en el Ecuador”.

<http://www.dlh.lahora.com.ec/paginas/judicial/PAGINAS/D.Informatico.37.htm>

Consulta: 02-Jul.2007

Universidad de El Salvador.

<http://www.e-libro.net/E-libro-viejo/gratis/delitoinf.pdf>

Consulta: 13-Nov.-2007

GREGORIO, Carlos G.; GRECO, Silvana; BALIOSIAN, Javier.

“*Impacto de las nuevas tecnologías de comunicación e información sobre los derechos de intimidad y privacidad*”.

<http://www.flacso.org.ec/docs/sfintgregorio.pdf>

Consulta: 13-Nov.-2007

CARRION, Hugo Daniel

“*Presupuestos para la incriminación del hacking*”

<http://delitosinformaticos.com/trabajos/hacking.pdf>

Consulta: 13-Nov.-2007

TOLEDO DUMENES, José Alfonso

DRA. GRACIELA ENCALADA OCHOA



“Delitos emergentes en internet y el desafío de carabineros de Chile en la prevención y control en la era informática”.

<http://www.delitosinformaticos.com/trabajos/criminalistica.pdf>

Consulta: 13-Nov.-2007

“Seguridades Informáticas y Delitos Informáticos”

CETID- Boletín Informativo – 2007

http://www.cetid.abogados.ec/index.php?p=boletin_mostrar&id=18&ide=6

Consulta: 13-Nov.-2007

YÁNEZ N., Pablo

“Infracciones electrónicas en el procedimiento penal”

Derechoecuador.com

<http://www.dlh.lahora.com.ec/paginas/judicial/PAGINAS/D.Informatico.36htm>

Consulta: 05-Oct.-2007

“Seguridades y Derecho Informático”

Cetid – Boletín informativo – 2007

http://www.cetid.abogados.ec/index.php?p=boletin_mostrar&id=100&ide=16

Consulta: 16-Oct.-2007

“Apuntes sobre delitos informáticos”

<http://www.monografias.com/trabajos14/delitos-informaticos/delitos-informaticos.shtml>

Consulta: 16-Oct.-2007

SOSA MEZA, Jorge, Ab.

“Aspectos generales y comparados de la Ley de Comercio Electrónico”

<http://www.dlh.lahora.com.ec/paginas/judicial/PAGINAS/D.Informatico.24.htm>

Consulta: 13-Nov.-2007

HUILCAPI PEÑAFIEL, Arturo Oswaldo

“El Delito Informático”

<http://www.dlh.lahora.com.ec/paginas/judicial/PAGINAS/D.Informatico.23.htm>

DRA. GRACIELA ENCALADA OCHOA



Consulta: 13-Nov.-2007

LAVENE, Ricardo; CHIARAVALLOTI, Alicia

“Introducción a los delitos informáticos, tipos y legislación”

<http://delitosinformaticos.com/delitos/delitosinformaticos.shtml>

Consulta: 13-Nov.-2007

BIDOT PELÁEZ, José

“Seguridad Informática en el Siglo XXI”

<http://tecnologiaedu.us.es/cvei/foros/bidot.htm>

Consulta: 14-Nov.-2007

CAMPOLI, Gabriel Andrés

“Hacia una correcta Hermenéutica Penal – Delitos Informáticos vs. Delitos Electrónicos”

<http://www.alfa-redi.org/rdi-articulo.shtml?x=1480>

Consulta: 14-Nov.2007

“Legislación y Delitos Informáticos”

<http://www.segu-info.com.ar/delitos/delitos.htm>

Consulta: 16-Oct.2007

“Legislación sobre delitos informáticos”

<http://www.monografias.com/trabajos/legisdelifn/legisdelifn.shtml>

Consulta: 16-Oct.-2007

“Delitos informáticos”

<http://www.monografias.com/trabajos6/delin/delin.shtml>

Consulta: 16-Oct.-2007

ARREGOITIA LÓPEZ, Siura Libertad. *“Los llamados delitos informáticos; su regulación penal en Cuba”*.



<http://www.fgr.cu/Biblioteca%20Juridica/Derecho%20y%20Delitos%20Informaticos/LOS%20LLAMADOS%20DELITOS%20INFORMATICOS%20SU%REGULACI%D3N%20PENAL%20EN%20CUBA.doc>

Consulta: 28-Abril-08

“Realidad Alternativa. Internet y delito informático: Nuevas formas de Criminalidad?”. Publicado en comutacion forence, derecho electrónico by Simón Bécquer on Enero 24th, 2008.

<http://realidadalternativa.wordpress.com/2008/01/24/internet-y-delito-infomatico-nuevas-formas-de-criminalidad/>

Consulta. 28-Abril-08

PEÑA ALONSO, Javier. Universidad de Burgos, España. *“Delitos en Internet”*.

<http://www.portaldeabogados.com.ar/noticias/derin03.htm>

Consulta. 28-Abril-08

PAZ MERAYO, Guillermo Augusto. *“Delitos Informáticos”*. Universidad de Costa Rica.

<http://www.derecho.ucr.ac.cr/gapmerayo/cursos/cursoDI/trabajosclase/delitoinf/delinfocap1.htm>

Consulta: 28-Abril-08

CORDOVES, Enrique. *“Características Generales de la Criminalidad Informática en Cuba”*. Revista de Derecho Informático. ISSN 1681-5726. Edita:Alfa-Redi

<http://www.alfa-redi.org/rdi-articulo.shtml?x=7178>

Consulta: 28-Abril-08

“Algunas consideraciones”.

<http://www.mailxmail.com/curso/informatica/delitosinformaticos/capitulo5.htm>

Consulta. 28-Abril-08

CUERVO, José. *“Delitos Informáticos: Protección Penal de la Intimidad”*.

<http://www.informatica-juridica.com/trabajos/delitos.asp>

Consulta: 28-Abril-08



“Los tipos de delitos informáticos reconocidos por Naciones Unidas”.

<http://realidadalternativa.wordpress.com/2008/01/25/los-tipos-de-delitos-informaticos-reconocidos-por-naciones-unidas/>

Consulta: 28-abril-08

<http://www.alfa-redi.org/rdi-articulo.shtml?x=6961>

Consulta: 28-Abril-08

“El bien jurídico y la nueva criminalidad. La criminalidad informática o computacional”.

<http://www.monografias.com/trabajos23/bien-juridico/bien-juridico.shtml>

Consulta: 28-Abril-08

ESTRADA GARAVILLA, Miguel. “Delitos Informáticos”.

<http://www.unifr.ch/ddp1/derechopenal/articulos/pdf/DELITOS.pdf>

Consulta: 28-Abril-08

“Legislación Nicaragüense ante los delitos Informáticos”.

<http://www.ictparliament.org/resources/DelitosInformaticos.pdf>

Consulta: 28-Abril-08

TINAJEROS ARCE, Erika Patricia. *“Criminalidad Informática en Bolivia”.*

http://www.informatica-juridica.com/trabajos/Criminalidad_informatica_en_Bolivia.asp

Consulta: 28-Abril-08

“Internet y Delito Informático: Nuevas formas de criminalidad?”

<http://vlex.com/vid/115525>

Consulta. 28-Abril-08

“Legislación y Delitos Informáticos- La Información y el Delito”.

<http://www.segu-info.com.ar/legislacion/>

Consulta. 28-Abril-08



“Legislación y Delitos Informáticos – El Delincuente y la Víctima”.

<http://www.segu-info.com.ar/delitos/delincuenteyvictima.htm>

Consulta: 28-Abril-08

“Legislación sobre delitos informáticos”.

<http://www.elrinconcito.com/articulos/DelitosInf/legisdelif.htm>

Consulta: 28-Abril-08

“Legislación sobre delitos informáticos. Panorama general”.

<http://www.mailxmail.com/curso/informatica/delitosinformaticos/capitulo34.htm>

Consulta: 28-abril-08

“Ciberdelincuencia en Ecuador, avanza sin parar”

<http://www.itecuador.com/2009/09/03/ciberdelincuencia-en-ecuador-avanza-sin-parar/>

Consulta: 05-Oct.-2009

“Delitos informáticos”.

<http://www.fing.uach.mx//MatDidactivo/Legislacion/deliinfo.htm>

REALIDAD

ALTERNATIVA.

<http://realidadalternatia.wordpress.com/2008/01/25/los-tipos-de-delitos-informaticos-reconocidos-por-naciones-unidas/>

“Legislación sobre delitos informáticos”.

<http://www.elrinconcito.com/articulos/DelitosInf/legisdelif.htm>

DelitosInformaticos.com -- PROYECTO DE CRIMINALISTICA INFORMATICA

<http://www.delitosinformaticos.com/tesis.htm> (25 de 72) [20/08/2001 17:12:34]

REVISTA ÂMBITO JURÍDICO ® . “Problemas fundamentales de la criminalidad informática”.

José Luis de la Cuesta Presidente de la Asociación Internacional de Derecho Penal (AIDP), Director del Instituto Vasco de Criminología.



Wikipedia.

Enciclopedia

libre

["http://es.wikipedia.org/wiki/Parche_\(inform%C3%A1tica\)"](http://es.wikipedia.org/wiki/Parche_(inform%C3%A1tica))

http://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n

Francisco Armando Dueñas Rodríguez fduenas_arroba@hotmail.com

http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica

Evidencia Digital en Colombia: Una reflexión en la práctica. Por Diana Bogota

Prieto, Claudia Moreno Peña. <http://www.alfa-redi.org/rdi-articulo.shtml?x=9330>

Informática Forense como medio de pruebas_____.

<http://www.dragonjar.org/informatica-forense-como-medio-de-pruebas.shtml>

<http://www.dragonjar.org/informatica-forense-como-medio-de-pruebas.shtml>

<http://html.rincondelvago.com/informatica-forense.html>



ANEXOS

Anexo 1

SEÑOR PRESIDENTE DE LA PRIMERA SALA DE LO PENAL Y
TRÁNSITO DE LA CORTE PROVINCIAL DE JUSTICIA DEL AZUAY:

Graciela Encalada Ochoa, me permito solicitar a usted de la manera más respetuosa, ordene que por Secretaría se me proporcione la siguiente información: si en el Juzgado a su cargo desde el año 2002 en que está en vigencia la Ley de Comercio Electrónico, Firma Electrónica y Mensaje de Datos, se encuentran registrados procesos por delitos informáticos y el estado en que se encuentran dichos procesos. La información que solicito servirá para la elaboración de mi tesis en la Maestría en Derecho Informático que se dictó en la Facultad de Jurisprudencia de la Universidad de Cuenca.

Atentamente,

Dra. Graciela Encalada Ochoa
Mat. C.A.A. 2570

Presentado en Cuenca a seis de noviembre del dos mil nueve a las diez y seis horas.
Certifico.

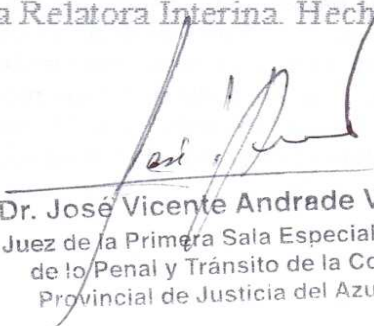
Dra. Ma. Lorena Palacios P.
Secretaria Relatora interina
de la Primera Sala Especializada





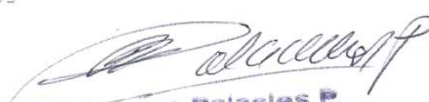
Cuenca, 6 de noviembre del 2009.- Las 10h10

Por secretaria confíerese a la peticionaria lo solicitado, En virtud de la acción de personal 172-09-DDCNJA, actúe la Dra. Lorena Palacios Palacios como Secretaria Relatora Interina. Hecho entréguese.


Dr. José Vicente Andrade Vélez
Juez de la Primera Sala Especializada
de lo Penal y Tránsito de la Corte
Provincial de Justicia del Azuay



RAZON: Siento como tal que revisados los libros correspondientes se encuentra inventariada la causa penal No. 474-09 seguida en contra de JOHANN PATRICIO DELGADO GARATE por delitos contra la información protegida (Art. 202. 1 Código Penal) en perjuicio de Marco Vinicio Bermeo Guambaña. El proceso fue resuelto por esta Primera Sala Especializada de lo Penal y Tránsito en fecha 8 de septiembre del 2009, a las 09h00, revocándose el auto de llanamiento a juicio y dictándose a favor del procesado el Auto de Sobreseimiento Definitivo. Adjunto copias de la resolución.
Cuenca, 9 de noviembre del 2009


Dra. Ma. Lorena Palacios P.
Secretaria Relatora interina
de la Primera Sala Especializada
de lo Penal y Tránsito de la Corte
Provincial de Justicia del Azuay





*42 doc
unoy*

JUEZ PROVINCIAL PONENTE: DR. JOSE VICENTE ANDRADE VELEZ
CORTE PROVINCIAL DE JUSTICIA DEL AZUAY: PRIMERA SALA DE LO PENAL
Y TRÁNSITO.- Cuenca, 08 de septiembre del 2009; las 09h00.- VISTOS: La Dra. Elizabeth Valarezo Loayza, Jueza Temporal encargada del Juzgado Segundo de Garantías Penales del Azuay, dicta el auto de llamamiento a juicio pues "considera que existen suficientes elementos de convicción que demuestran tanto la existencia material de la infracción como la responsabilidad de Johann Patricio Delgado Gárate de haber cometido el ilícito de utilización de secretos mediante información electrónica tipificado en el Art. 202-A, Inc., 4 del Código Penal".- De este auto interpone recurso de apelación el acusado (fs. 17), quien fundamenta su recurso en los siguientes términos: a) Que no se ha determinado la existencia material de la infracción, pues "en el auto de llamamiento a juicio se me acusa de haber cometido el delito de utilización de secretos mediante información electrónica", tipificada en el Art. 202-A inciso 4 del Código Penal y sancionada con seis a nueve años de reclusión menor, pero que dicha norma no establece dicha infracción, pues se requiere hacer un análisis jurídico de todo el artículo, con lo que se concluye que hace referencia a los "delitos contra la información protegida" y, en forma específica, en el inciso 4 "contenida en sistemas de información", pero no se ha demostrado que haya sido un "empleado de confianza" sino un simple vendedor con un contrato a plazo fijo, que debía conseguir clientes y que debía vender un mínimo de 8.000 dólares y luego 11.000 dólares, para tener un derecho a una remuneración de 350 dólares. b) Que en la denuncia se afirma que utilizó información contenida en el software para tomar contacto con la compañía taiwanesa TRANCED INFORMATION INC.; sin embargo, dicha empresa no consta en el referido software, conforme lo establece un informe pericial suscrito por el Dr. Juan Peña Aguirre. c) Que en cuanto a la falsa acusación de competencia desleal y perjuicio económico, tampoco han sido demostradas pues se ha excluido un informe realizado por el perito Dr. Germán Escandón. Y, d) Que tampoco se ha demostrado su responsabilidad pues no se ha demostrado que la supuesta información protegida "haya sido tomada de alguna manera por mi parte".- Encontrándose la causa en estado de resolver, en forma previa se considera: PRIMERO: En el trámite se han observado las solemnidades de ley, por lo que declara válido lo actuado.- SEGUNDO: La Sala es competente para conocer y resolver la apelación del auto de llamamiento a juicio, por el sorteo realizado y lo dispuesto en el Art. 29 Num. 1 del Código de Procedimiento Penal.- TERCERO: El auto impugnado es susceptible de ser apelado, conforme lo dispone el Art. 343 del Código de Procedimiento Penal; además, el recurso ha sido presentado, mediante escrito fundamentado, dentro de los tres días posteriores a su notificación, siendo admisible al trámite.- CUARTO: En la audiencia llevada a efecto, la defensa del imputado manifestó, en lo que la Sala considera principal para efectos de esta resolución, lo siguiente: 1) Que en la denuncia se afirma que Johann Patricio Delgado Gárate utilizó, en forma



fraudulenta, información protegida de carácter exclusivo y de propiedad del denunciante Marco Bermeo Guambaña, de manera específica con la compañía "Transcend Information Inc.", con la que ha realizado negocios en el mes de septiembre del 2008, adquiriendo a su nombre gran cantidad de suministros; pero que, sin embargo, tal empresa no consta en el software de CUENCA NET CIA. LTDA., según el informe pericial realizado por el Dr. Juan Peña Aguirre, por lo que no existe el presunto delito.

2) Que se ha pretendido utilizar una certificación del mismo presunto ofendido para establecer que dicha empresa, "Transcend Information Inc.", es proveedora de Cuenca Net Cía Ltda., lo cual no tiene valor alguno. 3) Que la dirección electrónica de "Transcend Information Inc.", consta en una memoria externa de computador de venta libre, que se la exhibe, con lo que se demuestra que dicha información no es reservada. 4) Que según consta en una certificación, Transcend Information Inc. tiene dos empresas que la representan en el Ecuador, sin que ninguna de ellas sea Cuenca Net Cía. Ltda., de propiedad del denunciante. 5) Que tampoco se ha demostrado el perjuicio causado, pues no se han podido justificar la no importación o la carencia de mercadería atribuibles al imputado. 6) Que Johann Delgado, según el contrato a plazo fijo celebrado, no tenía obligación de confidencialidad respecto al sistema informático y, siendo un agente vendedor, debía buscar por sí mismo a sus clientes. 7) Que la acusación vulnera el Art. 76 de la Constitución vigente, que en su numeral 6 garantiza la proporcionalidad entre infracción y sanción, pues siendo un simple agente vendedor, se acusa al imputado de un delito cuya pena rebasa a la de delitos como el prevaricato, el cohecho o la muerte de la mujer por maniobras abortivas. 8) Que el auto de llamamiento a juicio carece de la motivación suficiente. Y, 9) Que según el contrato de trabajo, el imputado estaba obligado a la reserva sólo de "la información que reciba" conforme consta en la Cláusula-Cuarta, y no tenía acceso a ningún otro tipo de información.- QUINTO: En la misma audiencia, la señora representante del Ministerio Público, en lo principal, manifestó lo siguiente: a) Que la resolución impugnada debe ser confirmada, pues en esta etapa procesal no se presentan "pruebas", como lo afirma la defensa del imputado, sino "elementos de convicción" y se requiere de "meras presunciones" para fundamentar un auto de llamamiento a juicio. b) Que se le contrató a Johann Delgado para que trabaje en forma exclusiva para su empleador, pero violó la reserva a la que estaba obligado por su relación contractual. c) Que el delito por el que acusa es la utilización fraudulenta del "listado de clientes" y no está tipificado en el inciso 4 del Art. 202-A del Código Penal, sino en el inciso 3 de dicha norma, cuya pena es de tres a seis años de reclusión. Y, d) Que si bien Transcend Information Inc. no está en los registros de la empresa del ofendido, si constan otras compañías con las que ha negociado el imputado, según información proporcionada por el SRI.- QUINTO: Tomando en consideración los fundamentos y alegaciones realizadas en la audiencia, la Sala llega a las siguientes conclusiones: 1) No existen presunciones de que el imputado haya utilizado o divulgado



13 de set
 2009

información protegida, pues no existe ningún elemento de convicción que lleve a presumir que recibió tal información; por lo tanto, no podía darle un uso indebido a una información que no tenía la calidad de reservada o protegida. 2) Tampoco existen presunciones de que era encargado de la custodia o utilización legítima de información protegida, pues según el contrato de trabajo suscrito entre las partes, el imputado era un simple vendedor de los productos de la empresa del denunciante. 3) Por lo tanto, no se puede presumir la existencia del delito tipificado en el inciso cuarto del Art. 202-A del Código Penal, acusado por el señor Agente Fiscal que actuó ante el señor juez a quo, ni el inciso tercero por el que acusó la señora Agente Fiscal en la audiencia ante esta Sala. 4) El Ministerio Público ha tenido una posición discordante respecto a la tipificación de la infracción, conforme se hace referencia anteriormente, y, además, la Sala considera que para fundamentar un auto de llamamiento a juicio no se requiere de "meras presunciones" sino de presunciones "graves y fundadas", inexistentes en el presente caso.- Por todo lo señalado, esta Primera Sala de lo Penal y Tránsito de la Corte Provincial de Justicia del Azuay, aceptando el recurso de apelación interpuesto por el imputado, revoca el auto de llamamiento a juicio dictado en contra de Johann Patricio Delgado Gárate y dicta el sobreseimiento definitivo del proceso y a su favor, conforme lo dispone el Art. 242 del Código de Procedimiento Penal.- A la denuncia presentada por Marco Vinicio Bermeo Guambaña, no se la califica ni de maliciosa ni de temeraria.- Adjuntando copia de esta resolución, devuélvase el expediente al juzgado de origen para los fines de ley.- En virtud de la acción de personal No. 172-DDCNJA-08, actúe la Dra. María Lorena Palacios como Secretaria Relatora Interina.- Notifíquese.

Dr. José Vicente Andrade Vélez
 Juez de la Primera Sala Especializada
 de lo Penal y Tránsito de la Corte
 Provincial de Justicia del Azuay

DR. JUAN PACHECO BARROS

DR. VICTOR LLERENA M.

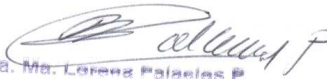
En CUENCA, ocho de Septiembre del dos mil nueve, a las nueve horas con cuatro minutos, notifiqué con la Providencia que antecede, por boletas a: BERMEO GUAMBANA MARCO VINICIO, en la casilla No: 150 de Dr.(a) LOYOLA POLO FERNANDO-RODAS ZUÑIGA CARLOS; a: DELGADO GARATE JOHANN PATRICIO, en la casilla No: 327 de Dr. (a) CRIOLLO PINTADO MARCELO ENRIQUE; a: DR. OSWALDO MARTINEZ, DEFENSOR PUBLICO, en la casilla No: 301 ; a: DR. PAUL VASQUEZ ILLESCAS, FISCAL, en la casilla No: 202 ; a: DRA. JULIA ELENA VAZQUEZ MORENO FISCAL PROVINCIAL, en la casilla No: 202 ; a: JOHANN PATRICIO DELGADO GÁRATE, PATROCINADO POR EL DR. DOGGO DELGADO JARA., en la casilla No: 327 ; - Certifico.

PALACIOSL

Dra. Ma. Lorena Palacios R.
 Secretaria Relatora Interina
 de la Corte Provincial de Justicia del Azuay
 Calle 10 de Agosto No. 1000
 Cuenca, Azuay, Ecuador



CERTIFICO: Que las copias fotostáticas que anteceden en dos fojas son iguales a su original del juicio penal No. 474-09 seguido en contra de JOHANN PATRICIO DELGADO GARATE por delitos contra la información protegida en perjuicio de marco Vinicio Guambaña.- Certifico
Cuenca, 9 de noviembre del 2009.


Dra. Ma. Lorena Palacios P.
Secretaria Relatora interina
de la Primera Sala Especializada
de lo Penal y Tránsito de la Corte
Provincial de Justicia del Azuay



Anexo 2

ANEXO 2

SEÑOR PRESIDENTE DE LA SEGUNDA SALA DE LO PENAL Y
TRÁNSITO DE LA CORTE PROVINCIAL DE JUSTICIA DEL AZUAY:

Graciela Encalada Ochoa, me permito solicitar a usted de la manera más respetuosa, ordene que por Secretaría se me proporcione la siguiente información: si en el Juzgado a su cargo desde el año 2002 en que está en vigencia la Ley de Comercio Electrónico, Firma Electrónica y Mensaje de Datos, se encuentran registrados procesos por delitos informáticos y el estado en que se encuentran dichos procesos. La información que solicito servirá para la elaboración de mi tesis en la Maestría en Derecho Informático que se dictó en la Facultad de Jurisprudencia de la Universidad de Cuenca.

Atentamente,

Dra. Graciela Encalada Ochoa
Mat. C.A.A. 2570

Presentado en Cuenca, nueve de Noviembre del dos mil nueve a las diez y seis horas.- Certifico.

Dr. Edgar Ávila Enderica
Secretario Relator

Cuenca, 23 de noviembre de 2009; las 09h00.

Confíerese la certificación requerida y entréguese.

CORTE PROVINCIAL DE JUSTICIA DEL AZUAY
SEGUNDA SALA ESPECIALIZADA DE LO PENAL

CUENCA-ECUADOR

Dr. Eduardo Makdonado Seade.

Juez Provincial Presidente de la Segunda Sala Especializada de lo Penal.



3 0x311A

Razón: Siento como tal que revisado el libro de inventario de causas de esta Segunda Sala Especializada de lo Penal, desde su especialización, **no se encuentra inventariada causa alguna por delitos informáticos.**

Certifico.- Cuenca, 24 de noviembre de 2009.

CORTE PROVINCIAL DE JUSTICIA DEL AZUAY
SEGUNDA SALA ESPECIALIZADA DE LO PENAL


Dr. Edgar Avila Enderica.

CUENCA-ECUADOR

Secretario Relator de la Segunda Sala Especializada de lo Penal.



Anexo 3

ANEXO 3

SEÑOR JUEZ PRIMERO DE GARANTÍAS PENALES DEL AZUAY:

Graciela Encalada Ochoa, me permito solicitar a usted de la manera más respetuosa, ordene que por Secretaría se me proporcione la siguiente información: si en el Juzgado a su cargo desde el año 2002 en que está en vigencia la Ley de Comercio Electrónico, Firma Electrónica y Mensaje de Datos, se encuentran registrados procesos por delitos informáticos y el estado en que se encuentran dichos procesos. La información que solicito servirá para la elaboración de mi tesis en la Maestría en Derecho Informático que se dictó en la Facultad de Jurisprudencia de la Universidad de Cuenca.

Atentamente,

Dra. Graciela Encalada Ochoa
Mat. C.A.A. 2570

Presentado en Cuenca, a los diecisiete días del mes de noviembre del año dos mil nueve, a las quince horas con catorce minutos. Certifico.


c.o.

Dr. Geovanny Peñafiel Calle
EL SECRETARIO
SECRETARIO DEL JUZGADO
PRIMERO DE GARANTIAS PENALES
DE CUENCA

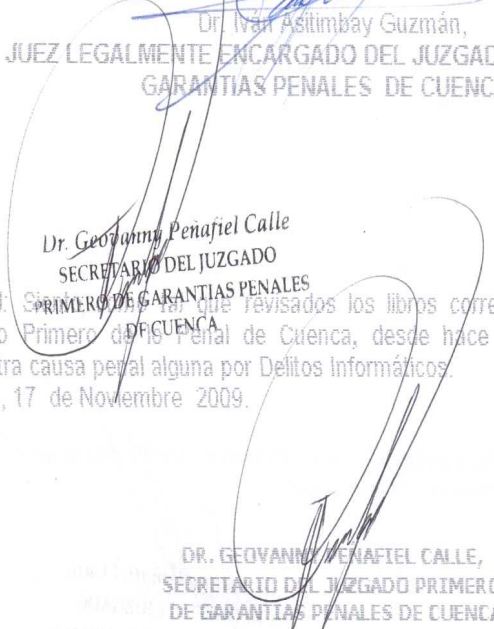


REPUBLICA DEL ECUADOR
JUZGADO PRIMERO DE GARANTIAS PENALES DE
CUENCA

Cuenca, a 17 de Noviembre de 2009.- Las 10h00
Confíerase lo solicitado y hecho devuélvase.


Dr. Ivan Asitimbay Guzmán,
JUEZ LEGALMENTE ENCARGADO DEL JUZGADO PRIMERO DE
GARANTIAS PENALES DE CUENCA

Lo Certifico.
El Secretario .-


Dr. Geovanny Peñafiel Calle
SECRETARIO DEL JUZGADO
PRIMERO DE GARANTIAS PENALES
DE CUENCA

RAZON: Se revisaron los libros correspondientes a este
Juzgado Primero de Penal de Cuenca, desde hace DIEZ años NO se
encuentra causa penal alguna por Delitos Informáticos.
Cuenca, 17 de Noviembre 2009.

DR. GEOVANNY PEÑAFIEL CALLE,
SECRETARIO DEL JUZGADO PRIMERO
DE GARANTIAS PENALES DE CUENCA





Anexo 4

ANEXO 4

SEÑOR JUEZ SEGUNDO DE GARANTÍAS PENALES DEL AZUAY:

Graciela Encalada Ochoa, me permito solicitar a usted de la manera más respetuosa, ordene que por Secretaría se me proporcione la siguiente información: si en el Juzgado a su cargo desde el año 2002 en que está en vigencia la Ley de Comercio Electrónico, Firma Electrónica y Mensaje de Datos, se encuentran registrados procesos por delitos informáticos y el estado en que se encuentran dichos procesos. La información que solicito servirá para la elaboración de mi tesis en la Maestría en Derecho Informático que se dictó en la Facultad de Jurisprudencia de la Universidad de Cuenca.

Atentamente,

Dra. Graciela Encalada Ochoa
Mat. C.A.A. 2570

Presentado en Cuenca el día diez de noviembre del dos mil nueve,
a las tres de la tarde con veinte minutos. Lo Certifico.

EL SECRETARIO

C.O.

JUZGADO SEGUNDO DE
GARANTIAS PENALES DE CUENCA



Cuenca - Ecuador

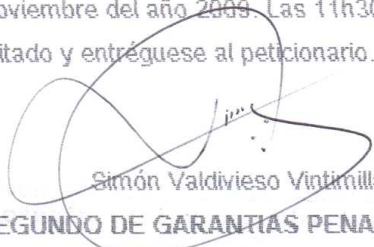


N 0230A



REPÚBLICA DEL ECUADOR
JUZGADO SEGUNDO DE GARANTIAS PENALES DE CUENCA

Cuenca, 11 de noviembre del año 2009. Las 11h30
Confírase lo solicitado y entréguese al peticionario.



Simón Valdivieso Vintimilla,
JUEZ SEGUNDO DE GARANTIAS PENALES DE CUENCA

Lo Certifico,
El Secretario



RAZON: Siento como tal que revisados los libros del Juzgado desde el año 2002 a la fecha **NO** se encuentra inventariada causa penal alguna por DELITOS INFORMATICOS. Certifico.

Cuenca, 11 de noviembre del año 2009.



Justo Velastegui Espinosa
SERETARIO

JUZGADO SEGUNDO DE
GARANTIAS PENALES DE CUENCA



Cuenca - Ecuador



Anexo 5

ANEXO 5

SEÑOR JUEZ TERCERO DE GARANTÍAS PENALES DEL AZUAY:

Graciela Encalada Ochoa, me permito solicitar a usted de la manera más respetuosa, ordene que por Secretaría se me proporcione la siguiente información: si en el Juzgado a su cargo desde el año 2002 en que está en vigencia la Ley de Comercio Electrónico, Firma Electrónica y Mensaje de Datos, se encuentran registrados procesos por delitos informáticos y el estado en que se encuentran dichos procesos. La información que solicito servirá para la elaboración de mi tesis en la Maestría en Derecho Informático que se dictó en la Facultad de Jurisprudencia de la Universidad de Cuenca.

Atentamente,

Dra. Graciela Encalada Ochoa
Mat. C.A.A. 2570

Presentado en Cuenca el diez de noviembre del dos mil nueve a las tres de la tarde con veinte minutos. Lo Certifico.

EL SECRETARIO

C.O.





8 0x34A

Cuenca, 13 de noviembre del 2009.- Las 09H53.-
De ser procedente confírase lo que solicita y entréguese a la interesada.-

Dra. SONIA CARDENAS CAMPOVERDE
JUEZA DE GARANTIAS PENALES
DEL JUZGADO TERCERO DE CUENCA

Lo Certifico
El Secretario

RAZON. Revisados los libros de inventarios de este Juzgado Tercero de lo Penal del Azuay, desde hace DIEZ años hasta la presente fecha, **NO** se encuentra inventariada causa alguna por delitos informáticos.- Certifico.-
Cuenca, 17 de Noviembre de 2009

Raúl Andrés Moscoso,
SECRETARIO DEL JUZGADO TERCERO
DE GARANTIAS PENALES DE CUENCA





Anexo 6

ANEXO 6

SEÑOR PRESIDENTE DEL PRIMER TRIBUNAL DE GARANTÍAS PENALES
DEL AZUAY:

Graciela Encalada Ochoa, me permito solicitar a usted de la manera más respetuosa, ordene que por Secretaría se me proporcione la siguiente información: si en el Juzgado a su cargo desde el año 2002 en que está en vigencia la Ley de Comercio Electrónico, Firma Electrónica y Mensaje de Datos, se encuentran registrados procesos por delitos informáticos y el estado en que se encuentran dichos procesos. La información que solicito servirá para la elaboración de mi tesis en la Maestría en Derecho Informático que se dictó en la Facultad de Jurisprudencia de la Universidad de Cuenca.

Atentamente,

Dra. Graciela Encalada Ochoa
Mat. C.A.A. 2570

Presentado en la Secretaría del Primer Tribunal Penal del Azuay, en Cuenca diez de noviembre del dos mil nueve a las dieciséis horas treinta minutos-Certifico.



Ab. Juan Manzano Crespo
SECRETARIO DEL TRIBUNAL

Cuenca, 11 de noviembre del 2009.- Las 11H15
Prevía la revisión de los libros correspondientes, confírase lo solicitado.

Dr. Rodrigo Dávila Vintimilla
PRESIDENTE DEL PRIMER TRIBUNAL
DE GARANTIAS PENALES DEL AZUAY

LO CERTIFICO.-

AB. Juan Manzano Crespo
SECRETARIO DEL TRIBUNAL

RAZON: Siento como tal que revisados los libros correspondientes desde el año 2002 NO SE ENCUENTRAN REGISTRADOS PROCESOS POR DELITOS INFORMÁTICOS
Cuenca, 11 de noviembre del 2002



Ab. Juan Manzano Crespo
SECRETARIO DEL TRIBUNAL



Anexo 7

ANEXO 7

SEÑOR PRESIDENTE DEL SEGUNDO TRIBUNAL DE GARANTÍAS PENALES
DEL AZUAY:

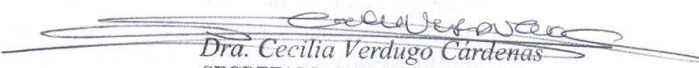
Graciela Encalada Ochoa, me permito solicitar a usted de la manera más respetuosa, ordene que por Secretaría se me proporcione la siguiente información: si en el Juzgado a su cargo desde el año 2002 en que está en vigencia la Ley de Comercio Electrónico, Firma Electrónica y Mensaje de Datos, se encuentran registrados procesos por delitos informáticos y el estado en que se encuentran dichos procesos. La información que solicito servirá para la elaboración de mi tesis en la Maestría en Derecho Informático que se dictó en la Facultad de Jurisprudencia de la Universidad de Cuenca.

Atentamente,

Dra. Graciela Encalada Ochoa
Mat. C.A.A. 2570

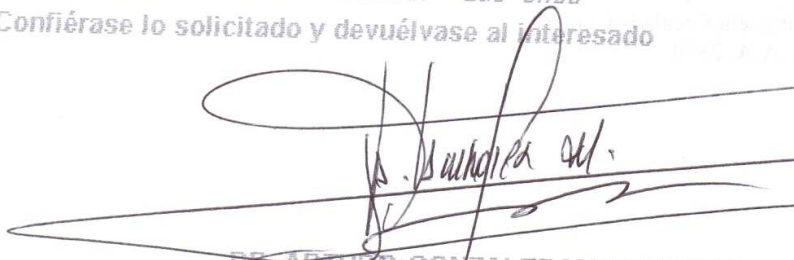


Presentado hoy once de Noviembre dos mil nueve, a las nueve horas
certifico.-


Dra. Cecilia Verdugo Cárdenas
SECRETARIA DEL II TRIBUNAL DE
GARANTIAS PENALES DEL AZUAY

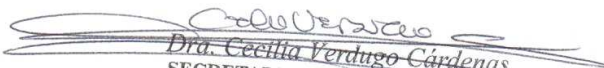
Cuenca, 12 de Noviembre del 2009.- Las 9h00
Confíerese lo solicitado y devuélvase al interesado




DR. ARTURO GONZALEZ MONTESINOS
PRESIDENTE DEL SEGUNDO TRIBUNAL
DE GARANTIAS PENALES DEL AZUAY

RAZON: Una vez revisados los libros correspondientes de este Tribunal
NO se encuentra inventariada causas penales con respecto a delitos
informaticos desde el año 2002 a la fecha
Cuenca, 12 de Noviembre del 2009.- certifico.-

L. 2


Dra. Cecilia Verdugo Cárdenas
SECRETARIA DEL II TRIBUNAL DE
GARANTIAS PENALES DEL AZUAY





Anexo 8

SEÑOR PRESIDENTE DEL TERCER TRIBUNAL DE GARANTÍAS PENALES
DEL AZUAY:

Graciela Encalada Ochoa, me permito solicitar a usted de la manera más respetuosa, ordene que por Secretaría se me proporcione la siguiente información: si en el Juzgado a su cargo desde el año 2002 en que está en vigencia la Ley de Comercio Electrónico, Firma Electrónica y Mensaje de Datos, se encuentran registrados procesos por delitos informáticos y el estado en que se encuentran dichos procesos. La información que solicito servirá para la elaboración de mi tesis en la Maestría en Derecho Informático que se dictó en la Facultad de Jurisprudencia de la Universidad de Cuenca.

Atentamente,

Dra. Graciela Encalada Ochoa
Mat. C.A.A. 2570

Presentado en Cuenca, en la secretaria del Tercer Tribunal de Garantías Penales del Azuay, hoy trece de noviembre del dos mil nueve, a las quince horas.-CERTIFICO.

Dra. Cecilia Crespo Ochoa
SECRETARIA

TERCER TRIBUNAL DE GARANTIAS PENALES DEL AZUAY.- Cuenca, 16 de noviembre del 2009. las 08h00. confíerese y devuélvase lo solicitado previa revisión de los archivos. CUMPLASE.

DR. Olmedo Feicán Garzón
PRESIDENTE ENCARGADO DEL TERCER TRIBUNAL



8 0230A

DE GARANTIAS PENALES DEL AZUAY

RAZON: Siento como tal, que una vez revisado los archivos y los libros correspondientes a este Tribunal Penal, NO se encuentra registrados procesos por delitos informáticos. Certifico.

Cuenca, 16 de noviembre del 2009

Dra. Cecilia Crespo Ochoa
secretaria





Anexo 9

ANEXO 9



REPUBLICA DEL ECUADOR

CONSEJO DE LA JUDICATURA
DIRECCION PROVINCIAL DEL AZUAY

**DRA. MARTHA ORELLANA PONCE, JEFE DE PERSONAL (E) DE
LA DIRECCION PROVINCIAL DE AZUAY DEL CONSEJO DE LA
JUDICATURA**

A petición verbal de parte interesada,

CERTIFICA:

Que, en el Registro de Peritos de la Fiscalía del Azuay, consta el Dr. Juan Peña Aguirre, como Perito en Informática-Documentología, desde el 27 de abril del 2005, hasta la presente fecha.

Cuenca, 9 de noviembre de 2009

**DRA. MATHA ORELLANA PONCE
JEFE DE PERSONAL (E) DE LA DIRECCION PROVINCIAL
DE AZUAY DEL CONSEJO DE LA JUDICATURA**

