Delitos informáticos

Mendoza Huarahuara Marisel Matilde
Universidad Mayor De San Andrés
Carrera De Informática
Simulación de Sistemas
mary_sel_mendoza@hotmail.com

RESUMEN

En este artículo se encuentra una revisión sobre lo que son los delitos informáticos, los tipos que existen de estos, a quienes afecta y a quienes beneficia, es decir la victima y el delincuente, respectivamente, las consecuencias legales y las estadísticas.

Palabras clave

Internet, informática, ordenador, tecnología, virus, , software, hardware.

1. INTRODUCCIÓN

La humanidad no ha cesado en la creación de métodos para procesar información, con ése fin nace la informática, como ciencia encargada del estudio y desarrollo de máquinas y métodos, y además con la idea de ayudar al hombre en aquellos trabajos rutinarios y repetitivos. Luego nace Internet como una tecnología que pondría la cultura, la ciencia y la información al alcance de millones de personas de todo el mundo. Junto al avance de la informática y su influencia en casi todas las áreas de la vida social, ha surgido una serie de comportamientos ilícitos denominados, de manera genérica.

El delito informático se refiere a actividades ilícitas realizadas por medio de o del , que tienen como objetivo la destrucción y el daño de ordenadores, medios electrónicos y redes de Internet. Los delitos también se pueden referir a las conductas que incurren sobre herramientas informáticas como hardware o software; como aquellas que empleando estos medios perjudican intereses jurídicamente tutelados como la intimidad, el patrimonio económico, la fe pública, entre otros.

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 creado la necesidad de regulación por parte del derecho.

El delito informático incluye una amplia variedad de categorías de crímenes. Generalmente este puede ser dividido en dos grupos:

Crímenes que tienen como objetivo redes de computadoras, por ejemplo, con la instalación de códigos, gusanos y archivos maliciosos (o correos electrónicos no solicitados para propósito comercial), ataque masivo a servidores de Internet y generación de virus.

Crímenes realizados por medio de ordenadores y del Internet, por ejemplo, espionaje por medio del Internet, fraudes y robos, pornografía infantil, pedofilia Internet, etc.

El término delito informático se acuñó a finales de los años noventa, a medida que Internet se expandió por toda Norteamérica.

El delito informático se aplica a nuevos tipos de criminalidad, tales como la pornografía cibernética o la distribución de imágenes pornográficas que violaban algunas (pero no todas) leyes de los países con respecto a la pornografía inaceptable o al material utilizado para explotar. El hecho de que Internet no tenga fronteras, facilitó a las personas la distribución de materiales a escala internacional, en ocasiones sin dejar rastros sobre su autor.

Una nueva forma de delito es también la penetración ilegal en los sistemas computarizados o piratería informática, que en muchos países aún no constituía un delito penal. Uno de los propósitos del Tratado sobre Delito Informático fue establecer y acordar las disposiciones que debían aparecer en las legislaciones de los signatarios con el objetivo de luchar contra la nueva actividad delictiva con más coordinación.

2. CARACTERISTICAS DE LOS DELITOS

Los delitos informáticos presentan las siguientes características principales:

a) Conductas criminales de cuello blanco (white collar crime), en tanto que sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos) puede llegar a cometerlas.

b) Ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se halla trabajando.

c) De oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de y del tecnológico y económico.

d) Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" de más de cinco cifras a aquellos que las realizan.

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

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

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

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

i) 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.

3. TIPOS DE DELITOS INFORMÁTICOS

3.1. Fraudes Cometidos Mediante Manipulación de Computadoras

3.1.1 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 de 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.

3.1.2 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.

3.1.3 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.

3.1.4 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.

3.2. Falsificaciones Informáticas

3.2.1. Como Objeto

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

3.2.2. 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.

3.3. Daños o Modificaciones de Programas o Datos Computarizados

3.3.1. 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.

3.3.2. 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.

3.3.3. 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.

3.3.4. Bomba Lógica o Cronológica

Exige conocimientos especializados ya que requiere la

programación de la destrucción o modificación de datos en un momento 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 de 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.

3.4. Acceso No Autorizado a Servicios y Sistemas Informáticos

Esta acción se realiza por varios motivos, desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.

3.4.1. 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.

3.4.2. Reproducción no Autorizado 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. Considerándose los siguientes aspectos.

En primer lugar, existe el nuevo delito de penetración del código, invasión o espionaje dentro de los sistemas informáticos de otras personas u organizaciones. Las opiniones diferían en cuanto a si el hecho de solo mirar constituía un delito, especialmente debido a que los primeros hackers detectaban a menudo fisuras en la seguridad y se consideraban ciudadanos honestos al informarlas. Naturalmente, penetrar un sistema con intensiones delictivas es otra cosa.

En segundo lugar, existen situaciones en las que el delito es viejo, pero el sistema es nuevo, como es el caso de las estafas fraudulentas por Internet. El fraude comercial ha existido durante miles de años, las estafas telefónicas han existido durante décadas y ahora tenemos las estafas por Internet. Esto también es válido para la pornografía y el fraude al derecho de autor.

El tercer elemento es el referido a la investigación, donde la computadora sirve como depósito de evidencias, necesarias para el procesamiento judicial exitoso de cualquier delito que se cometa. Lo que solía archivarse en expedientes de papel, prácticamente ya no se archiva de otra forma que no sea la digital y puede ser destruido y decodificado a distancia.

4. SUJETOS ACTIVOS Y PASIVOS

Muchas de las personas que cometen los delitos informáticos poseen ciertas características específicas tales como la habilidad para el manejo de los sistemas informáticos o la realización de tareas laborales que le facilitan el acceso a información de carácter sensible.

Muchos de los delitos informáticos encuadran dentro del concepto de , esta categoría requiere del sujeto activo (delincuente) y el sujeto pasivo (victima).

4.1. Sujeto Activo

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 hábiles 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 "entra" en un sistema Informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes.

Tanto la definición de los “delitos informáticos” como la de los delitos de cuello blanco no son 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 se tiene que: el sujeto activo del delito es una persona de cierto status socioeconómico, su comisión no puede explicarse por pobreza ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia,

ni por inestabilidad emocional.

4.2. Sujeto Pasivo

En primer término se tiene que distinguir que el sujeto pasivo o víctima del delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los delitos informáticos, mediante él podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos, que generalmente son descubiertos casuísticamente debido al desconocimiento del modus operandi.

El sujeto pasivo en el caso de los delitos informáticos, pueden ser individuos, instituciones crediticias, órganos estatales, etc. que utilicen sistemas automatizados de información, generalmente conectados a otros equipos o sistemas externos.

5. CONSECUENCIAS LEGALES

5.1. Aspecto Legal antes del año 2009

Existen leyes, en muchos países, que permiten tratar los mensajes electrónicos con el mismo rigor que los mensajes en papel. Sin duda estos mecanismos no eran garantía para sancionar correctamente a los delitos informáticos que día a día crecen en variedad y problemática.

Consideremos en este caso a un país vecino. En Colombia existe la ley 527/99 en el articulo 10º se menciona que hizo las siguientes consideraciones: "El mensaje de datos como tal debe recibir el mismo tratamiento de los documentos consignados en papel, es decir, debe dársele la misma eficacia jurídica, por cuanto el mensaje de datos comporta los mismos criterios de un documento".

5.2. Aspecto Legal año 2009 en Adelante

- Las penas anteriores pueden tener agravantes si los delitos se cometen:
- Sobre redes o sistemas informáticos de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
- Por servidor público en ejercicio de sus funciones.
- Aprovechando la confianza depositada por el poseedor de la información o por quien tuviera un vínculo contractual con este.
- Revelando o dando a conocer el contenido de la información en perjuicio de otro.
- Obteniendo provecho para si o para un tercero.
- Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
- Utilizando como instrumento a un tercero de buena fe.

Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

Tabla 1. Atentados informáticos con sus sanciones

Delito	Pena
Acceso abusivo a un sistema informático	48 a 96 meses de cárcel y de 100 a 1000 salarios mínimos legales vigentes
Obstaculización ilegítima de sistema Informático o red de telecomunicación	
Interceptación de datos informáticos	36 a 72 meses de carcel
Daño informático	48 a 96 meses de cárcel y de 100 a 10000 salarios mínimos legales vigentes
Uso de software malicioso	
Violación de datos personales	
Suplantación de sistios web para capturar datos personales	
Hurto por medios informáticos y semejantes	48 a 120 meses de cárcel y de 200 a 1500 salarios mínimos vigentes
Transferencia no consentida de archivos	48 a 120 meses de cárcel y de 200 a 1500 salarios mínimos vigentes

Cuando se imputa a una persona por un delito informático, generalmente el 363 bis Manipulación Informática (sólo este tiene pena de cárcel), la imputación incluye además otros delitos con más o menos años de cárcel, por ejemplo abuso de confianza, hurto, uso de instrumento falsificado, estafa agravada, etc. Esto se da porque si bien se pueden manipular los datos de entrada, el proceso o la salida de datos, estos datos en algún momento se reflejan en un papel firmado/rubricado o para causar el daño patrimonial establecido en el 363 bis, alguien deberá recibir el dinero físicamente.

6. ESTADÍSTICAS SOBRE DELITOS INFORMÁTICOS

Desde hace cinco años, en los Estados Unidos existe una institución que realiza un estudio anual sobre la y los crímenes cometidos a través de las computadoras. Esta entidad es El Instituto de Seguridad de Computadoras (CSI), quien anunció recientemente los resultados de su quinto estudio anual denominado "Estudio de Seguridad y Delitos Informáticos" realizado a un total de 273 principalmente grandes Corporaciones y Agencias del .

Entre lo más destacable del Estudio de Seguridad y Delitos Informáticos 2000 se puede incluir lo siguiente.

1.1. Violaciones a la Seguridad Informática

El 90% de los encuestados descubrió violaciones a la seguridad de las computadoras dentro de los últimos doce meses (ver Figura 1).

El 70% reportaron una variedad de serias violaciones de

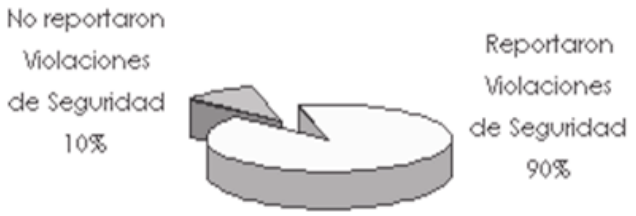

Figura 1. Violaciones de seguridad informática

seguridad de las computadoras, y que el más común de estas violaciones son los de computadoras, robo de computadoras portátiles o abusos por parte de los empleados -- por ejemplo, robo de información, fraude financiero, penetración del sistema por intrusos y sabotaje de datos o .

6.2. Perdidas Financieras

El 74% reconocieron pérdidas financieras debido a las violaciones de las computadoras.

61 encuestados cuantificaron pérdidas debido al sabotaje de datos o redes para un total de $US 27.148.000. Las pérdidas financieras totales debido al sabotaje durante los años anteriores combinados ascendido a sólo $US 10.848.850.

Como en años anteriores, las pérdidas financieras más serias, ocurrieron a través de robo de información (66 encuestados reportaron $US 66.708.000) y el fraude financiero (53 encuestados informaron $US 55.996.000) (ver Figura 2).

Los resultados del estudio ilustran que esa amenaza del crimen por computadoras a las grandes corporaciones y agencias del gobierno viene de ambos lados dentro y fuera de sus perímetros electrónicos, confirmando la tendencia en años anteriores.

6.3. Accesos No Autorizados

El 71% de los encuestados descubrieron acceso desautorizado por personas dentro de la empresa. Pero por tercer año consecutivo, la mayoría de encuestados (59%) mencionó su conexión de Internet como un punto frecuente de ataque, los que citaron sus sistemas interiores como un punto frecuente de ataque fue un 38% (ver Figura3).

Basado en contestaciones de 643 practicantes de seguridad de computadoras en corporaciones americanas, agencias gubernamentales, financieras, instituciones médicas y universidades, los hallazgos del Estudio de Seguridad y Delitos Informáticos 2000, confirman que la amenaza del crimen por computadoras y otras violaciones de seguridad de información continúan constantes y que el fraude financiero está ascendiendo.

Las tendencias que el estudio de CSI/FBI ha resaltado por años son alarmantes. Los "Cyber crímenes" y otros delitos de seguridad de información se han extendido y diversificado. El 90% de los encuestados reportaron ataques. Además, tales incidentes pueden producir serios daños.

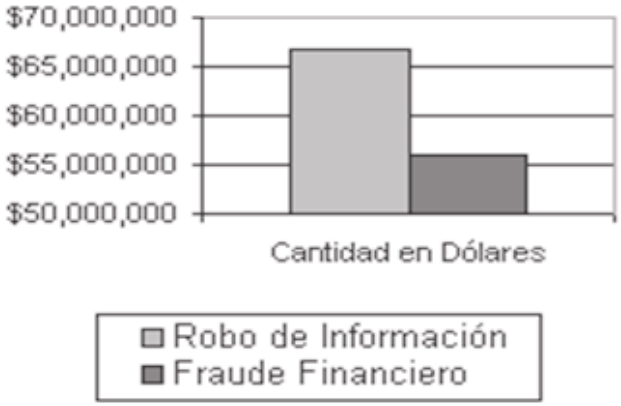

Figura 2. Pérdidas por sabotaje informático

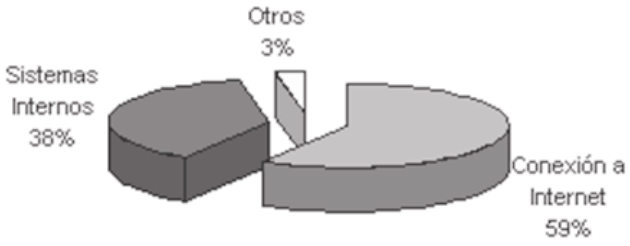

Figura 3. Puntos frecuentes de ataques informáticos

7. CONCLUSIONES

La falta de cultura informática es un factor crítico en el impacto de los delitos informáticos en la sociedad en general, cada vez se requieren mayores conocimientos en tecnologías de la información, las cuales permitan tener un marco de referencia aceptable para el manejo de dichas situaciones. Como consecuencia del desconocimiento de las nuevas tecnologías existe una excesiva dependencia que recae en los "Peritos Informáticos".

Los delitos informáticos en muchos casos no se castigan por defectos procesales, al igual que otro tipo de delitos, en este punto debemos resaltar la falta de capacitación del Personal de la fuerza de la Ley (policía y fiscales) en el secuestro de evidencia digital y la preservación de la cadena de custodia de la misma.

8. REFERENCIAS

[1]http://www.microsoft.com/.../delitos_informaticos.mspx

[2]http://www.delitosinformaticos.info/delitos_informaticos/tipos_delitos.html

[3]http://www.monografias.com/trabajos6/delin/delin.shtml

[4]http://www.rosalesuriona.com/spip.php?article395

[5]http://www.chiaravalloti_asociados.dtj.com.ar/links_1.htm

[6]http://web.presidencia.gov.co/leyes/2009/enero/ley127305012009.pdf