EL COSTE DEL DELITO INFORMATICO

ANSELMO DEL MORAL TORRES
Capitán de la Guardia Civil
Comisión Europea
Oficina de lucha contra el fraude

LA informática en general y las redes de telecomunicaciones en particular constituyen la gran revolución de finales de siglo XX y principio del nuevo milenio.

La sociedad de la información, hace tiempo que se ha instalado en nuestras vidas y hoy en dia sería muy difícil imaginarla, sin ordenadores en los supermercados, cajeros automáticos, farmacias, gasolineras, centros de estudio, etc.

No sólo las necesidades más básicas del hombre se encuentran ya gestionadas por el ordenador, sino que las grandes infraestructuras de todos los países, de las que dependen para subsistir millones de personas quedan en manos de la precisión de estos equipos. Pensemos en los ordenadores que gestionan el tráfico ferroviario, los aeropuertos, las centrales nucleares, las presas, las centrales eléctricas, etc. Todos estos sistemas se encuentran gestionados, por supuesto con la oportuna intervención del hombre, por equipos informáticos y/o electrónicos.

Las redes de comunicaciones globales se han socializado y se encuentran a disposición del gran público lo cual ha supuesto una revolución social intelectual y económica.

A través de la pantalla de un ordenador podemos comunicarnos fácilmente y a un bajo coste económico con personas que se encuentran a miles de kilómetros, se pueden realizar compras en cualquier país del mundo, hacer una reserva de hotel o de un billete de avión e incluso acceder a nuestro banco, ver la televisión y escuchar una emisora de radio que se encuentra en otro continente.

Si pasamos del ordenador al teléfono móvil, podríamos dibujar un panorama similar, la expansión de su uso en la sociedad en la década de los noventa a finales del siglo XX

ha sido brutal. Todos intuimos que en los años 80, casi nadie usaba en España teléfono móvil y hoy en día es una herramienta básica para muchas familias, comerciantes, y todo tipo de profesionales.

Pero volvamos a los ordenadores y a las redes informáticas. A principios del siglo XXI, encontramos alrededor de 3 millones de internautas en nuestro país de un población cercana a los 40 millones de habitantes. Podemos pensar que es una cifra pequeña, incluso si comparamos la cifra de personas que usan internet a nivel mundial, cuyo número no me atrevo a dar por quedar en ese mismo instante desfasado, con el total de la población mundial posiblemente hablaremos de un número ínfimo de personas.

Sin embargo, lo significativo es el crecimiento exponencial del número de personas, familias, empresas o instituciones que se introducen cada día en la red por cualquier razón. Este fenómeno mundial afecta a más de 100 países en los 7 continentes de tal forma que Internet se ha convertido en el sistema informático interconectado más grande del mundo.

Esta revolución tecnológica, sin la cual no entenderíamos los tiempos en los que vivimos, no ha hecho nada más que empezar. Como suele comentar el Profesor Sanromá (1), al hablar de Internet nos encontramos como en una situación similar a la del lejano oeste. La mayoría entra en este mundo buscando nuevos horizontes. Aparecen los primeros buscadores de oro, las primeras ciudades sin ley, no faltan algunos forajidos y comienzan a existir algunos destacamentos de caballería aislados..."

Pensemos que ocurriría con el número de millones de personas que usan actualmente internet, si los procedimientos de conexión se hiciesen mucho más fáciles y asequibles a profanos de la informática. Por ejemplo si las redes de comunicaciones en general, permitiesen accesos ágiles a través a Internet por medio de la televisión, a la cual podría asociarse una unidad de almacenamiento de datos.

No existen ordenadores en todos los hogares pero si encontraremos en la mayoría de ellos, un televisor y una conexión a la red telefónica. Que ocurriría si el teclado del ordenador se sustituye por el mando de la televisión y cualquier persona desde su domicilio pudiera a través del televisor y de internet realizar la compra en el supermercado, consultar su saldo en el banco, remitir la declaración de la renta o comprobar como se encuentra su hijo en la guardería a través de videoconferencia... La verdad es que el futuro más cercano es maravilloso pero da un poco de vértigo.

Casi con toda seguridad a lo largo del nuevo milenio, cada uno de nosotros llegará a utilizar varios ordenadores en el día a día. Tendremos ordenadores en la casa, en lo teléfonos televisores, oficinas y automóviles. Esta posibilidad incrementará enormemente la calidad de vida de los hogares.

Este invento maravilloso no escapa al lado oscuro de la vida. En realidad existen pocos obstáculos para la comisión de delitos a través de medios informáticos. La gente que ha informatizado sus negocios, empresas, etc., no tiene normalmente en consideración algunos requisitos de seguridad necesarios para salvaguardar la información contenida en los ordenadores, o los responsables técnicos no alcanzan a entender los riesgos a fondo para fundamentar sus esfuerzos.

Un insuficiente aprendizaje sobre seguridad, y métodos de ingeniería del software inapropiados pueden contribuir a la inseguridad.

Desafortunadamente el masivo uso de los ordenadores y las redes de telecomunicaciones no nos han dado demasiado tiempo para desarrollar y unas defensas apropiadas para los sistemas.

En este nuevo campo las fuerzas y cuerpos de seguridad necesitan adaptarse para poder operar. Los investigadores necesitan obtener conocimientos sobre los nuevos métodos y técnicas de investigación.

Los miembros de las fuerzas y cuerpos de seguridad, las autoridades judiciales y Ministerio Fiscal deben adaptarse a este tipo de investigaciones, no solo para proteger los intereses y recursos de la sociedad sino también para preservar muchas de las libertades y derechos que como ciudadanos deseamos tener.

Por otro lado la experiencia demuestra, lo importante que es la formación y la preparación en este campo, ya que los excesos y los daños causados durante una investigación de este tipo, ya sean accidentales o no, puede

conducir a una perdida de medios de prueba en fases posteriores del procedimiento judicial.

Para la protección de la sociedad se deben desarrollar nuevas técnicas de investigación. La sociedad no puede permitir conductas antisociales o comportamientos ilegales simplemente porque estos ocurren a través del intangible mundo de las redes informáticas. El hecho de que un mensaje sea transmitido a través de un cable por medio de electrones, en lugar de usar tinta sobre papel no da derecho a intromisiones en la vida privada de las personas, o porque una información este almacenada en un disco magnético, en lugar de un archivador, no quiere decir que por eso pueda violarse la documentación personal de un individuo.

¿Cuales son los costes de estas actividades antisociales denominadas delitos informáticos?

Para poder hacer una mediana aproximación a este parámetro deberiamos empezar por definir qué se considera "delito informático".

Si intentamos buscar la expresión "delito informático" en el Código Penal español o en las leyes procesales casi con toda seguridad no tendremos éxito. Tampoco encontraremos otras acepciones del término como "delito de alta tecnología" o "delito digital".

Estas expresiones provienen de la traducción de los conceptos anglosajones "Computer Crime", "High-Tech Crime", o "Digital Crime" ampliamente utilizados en las legislaciones de países como Estados Unidos de América o el Reino Unido.

En cualquier diccionario podemos encontrar la definición de la palabra delito como:

> *"Las acciones u omisiones culpables, antijurídicas, tipificadas y penadas por la ley".*

Si a esta definición, le añadimos el apelativo "informático", restringimos el concepto a aquellas acciones u omisiones delictivas donde el denominador común es el uso de medios informáticos para alcanzar el fin deseado.

No obstante profundizando en la bibliografía existente sobre la materia podemos ver que existen dos grandes corrientes en cuento a la definición y consideración de los denominados delitos informáticos

Una más clásica, que considera los delitos informáticos como un grupo cerrado de actividades ilícitas prácticamente ligadas a la copia ilegal de programas informáticos o el fraude cometido a través de estos medios y otra cada vez más entendida que realiza una clasificación de este tipo de ilícitos penales de acuerdo con un uso más general de medios informáticos para obtener el resultado final.

Esta segunda clasificación de los delitos informáticos aceptada principalmente por organismos policiales internacionales como la Oficina Internacional de Policía Criminal (OIPC-Interpol) diferencia no obstante estas acciones en:

Delitos informáticos puros.

Surgen en la mayoría de los ordenamientos jurídicos con la aparición desarrollo de los medios tecnológicos interconectados por ordenador y la realización de un uso ilícito de los mismos, agrupándose bajo los tipos:

- Copia ilegal de datos y software.
- Manipulación fraudulenta de hardware.
- Interceptación ilegal de las telecomunicaciones.
- Accesos ilegales a ordenadores.
- Daños a sistemas informáticos.
- Fraude electrónico.
- Fraude en las telecomunicaciones.

Delitos clásicos cometidos través de medios informáticos y/o electrónicos.

No son considerados delitos informáticos, y consisten en tipos penales tradicionales recogidos en la mayoría de los ordenamientos jurídicos a nivel internacional, en los que el medio electrónico o informático es cada vez más empleado como vía de comunicación o difusión de información relacionada con la actividad delictiva. No obstante, en este caso, su presencia no es esencial a diferencia de lo que ocurre en el caso de los delitos informáticos puros para que se produzca el tipo delictivo. Estos pueden ser:

- Terrorismo.
- Apología.

- Pornografía infantil.
- Amenazas y coacciones.
- Calumnias e injurias.
- Tráfico ilegal de datos personales.
- Tráfico de armas, drogas, seres humanos.
- Apuestas ilegales.
- Contrabando de obras de arte.
- Falsificación de documentación.
- Espionaje industrial.
- Etcétera.

Las primeras conclusiones sobre los hechos expuestos nos ponen de manifiesto que no encontramos en el ordenamiento jurídico español, al igual que en otros de nuestro entorno cultural, una definición exhaustiva y concreta del denominado "delito informático" sino que este concepto corresponde a un conjunto de acciones u omisiones delictivas recogidas de forma dispersa o no, en los ordenamientos jurídicos consistentes en la comisión de actos ilícitos a través de medios electrónicos y/o informáticos.

Para ser más explicito, y avanzar un poco en la comprensión de este fenómeno podemos observar que en la mayoría de los denominados delitos informáticos se producen una serie de vulneraciones de la denominada "seguridad informática", es decir, son los diferentes procedimientos que afectan a la seguridad de los medios informáticos, los que son comprometidos en la realización de este tipo de actividades ilícitas.

Esta seguridad tiene diversas facetas, ya que el delito puede desarrollarse de formas muy complejas, como por ejemplo, a través de la vulneración de las comunicaciones de datos entre bancos por medio de sofisticados programas informáticos o simplemente vulnerando la seguridad relativa al personal que afecta a dichas redes a través del soborno de un empleado del banco para que facilite su palabra de acceso a la red de datos bancaria.

En este sentido hay que tener en cuenta que estas vulneraciones no se dan de forma aislada sino que aparecen de forma combinada en la mayoría de los casos y podrían clasificarse en vulneraciones relativas a la:

- Seguridad física.
- Seguridad relativa al personal.
- Seguridad del software y los datos.
- Seguridad de las comunicaciones.
- Seguridad de los medios de pago electrónicos.

En relación a lo comentado sobre los delitos clásicos y los usos cada vez más frecuentes de las nuevas tecnologías, que duda cabe que el conocimiento de estas tecnologías no se encuentra al alcance de todas las personas. Este fenómeno se produce por diversas razones entre las que se encuentran, el hecho de que en algunos casos no son productos asequibles económicamente, no es fácil entender su funcionamiento y somos normalmente reacios a aprender el uso de nuevas técnicas aferrándonos a lo conocido.

No obstante, la delincuencia organizada en todos sus ámbitos y espectros, siempre se ha destacado por "estar a la última" en el uso de medios tecnológicos ya que suelen contar con amplios recursos económicos para adquirirlos y en la mayoría de los casos les facilita la posibilidad de eludir la acción de la justicia debido a que:

- Es muy simple realizar comunicaciones a nivel internacional.
- No es fácil que las fuerzas y cuerpos de seguridad cuenten de forma generalizada, con los últimos adelantos tecnológicos para afrontar los nuevos usos de estos medios por parte de los delincuentes.
- Es necesario una especialización judicial y policial para entender los métodos y medios empleados.
- Pueden fácilmente contratar a técnicos que aseguren su perfecto funcionamiento.

Quizás un simple ejemplo termine de aclarar lo que supone el uso de la telecomunicaciones por las bandas organizadas.

En 1930, Alfonso Capone fue detenido en la ciudad de Chicago (EEUU) y condenado por delito fiscal por no declarar a la Hacienda Pública, sus supuestas actividades comerciales.

En este caso, para los investigadores fue esencial localizar y asegurar como evidencias los libros relativos a la contabilidad de dichas actividades confeccionados por el necesario contable contratado por el capo italiano.

Si Al Capone viviera en hoy día, posible-

mente contrataría a un chico de 17 años, experto en informática, que realizaría los asientos correspondientes a las actividades ilegales de su jefe en un fichero informático encriptado, que ubicaría a través de internet en un servidor situado en un paraíso fiscal.

Una vez analizados los posibles usos de la informática y de las telecomunicaciones para la realización de hechos delictivos y establecida la distinción entre las diferentes vulnerabilidades de la denominada seguridad informática debemos realizar un esfuerzo de tipificación.

La propia definición del concepto delito y el principio de legalidad obliga a la tipificación de la conductas en hechos delictivos. En este sentido es preciso analizar los ordenamientos jurídicos penales para poder entender donde pueden entenderse comprendidas las diferentes vulneraciones de la seguridad relacionada con los medios tecnológicos.

Sobre la base de lo expuesto es necesario estudiar la legislación penal y procesal internacional en relación a los delitos cometidos a través de medios tecnológicos y al hacerlo podemos ver que, algunos países, como Holanda o el Reino Unido establecen legislaciones especiales para recoger sus descripciones delictivas relativas a este tipo de delitos. Sin embargo el legislador español ha optado, al igual que en otros países por incluir este tipo de delitos de forma dispersa en el Código Penal Español de 1995.

Por otro lado desde un punto de vista criminológico parece interesante analizar la finalidad de los presuntos autores de este tipo de acciones, ya que estas pueden ser muy diversas. Estas abarcan un abanico muy amplio desde la obtención un beneficio económico, la existencia de razones políticas o sociales o incluso como forma de eludir la acción de la justicia en el caso de bandas organizadas dada la dificultad de obtención de pruebas en el mundo de las nuevas tecnologías. Esta finalidad nos proporcionará claramente distintos perfiles de autores en el caso de los delitos informáticos.

En el caso de las víctimas, si analizados el resultado de estas acciones delictivas llegaremos a descubrir e identificar los diferentes tipos de víctimas que sufren este tipo de delitos.

En este sentido los denominados delitos informáticos pueden resultar casi inofensivos, como por ejemplo la modificación de una página WEB en Internet, o pueden venir acompañados de situaciones catastróficas.

Pensemos que, las centrales nucleares, los aeropuertos, las estaciones de tren, las presas o el sistema de impresión de billetes de un banco nacional se encuentran gestionados por redes de ordenadores que pueden ser vulnerados.

¿Cuál es el coste del delito informático en el caso de que por ejemplo un virus afecte al normal funcionamiento del sistema informático que coordina el tráfico aéreo de una determinada zona?

¿Qué daños ocasionaría para la economía de un país el bloqueo intencionado del sistema informático que controla el proceso de impresión de billetes?

Todo estos ejemplos y muchos más que podríamos imaginar ponen de manifiesto la importancia de la seguridad informática de los sistemas que gestionan las infraestructuras, los servicios y las comunicaciones básicas que afectan a los ciudadanos y la adopción de adecuadas políticas de prevención.

La realización de auditorías de seguridad informática en los organismos, empresas e instituciones es considerada en muchos casos de escaso interés, sin embargo, este tipo de actividad es esencial para evaluar la salud de la organización y realizar una optimización de los recursos donde se establezcan los oportunos procedimientos de seguridad.

No obstante, la realidad demuestra que pese al establecimiento de medidas preventivas, en algunos casos se producen violaciones de la seguridad en relación a medios tecnológicos y esto da lugar a la existencia de hechos delictivos que deben ser investigados y que producen unos costes directamente proporcionales al valor de la información comprometida por estas acciones ilegales.

Baste algunos ejemplos para entender que estas acciones pueden acarrear en determinadas situaciones unos costes demasiado elevados

En 1995 la BBA (2) estimaba que los fraudes cometidos a través de ordenador suponían anualmente unas pérdidas de 5 billones de libras al año.

El Ministerio de Defensa de Francia reconoció ese mismo año, que cinco ordenadores que contenía información confidencial habían sido sustraídos de la base naval de Toulon (Francia). Aunque la Marina francesa negó los hechos, intrusos informáticos informaron de que habían tenido acceso a los códigos de reconocimiento de aviones y submarinos.

El FBI (EEUU) tras una investigación acusó a Vladimir Levín, un hacker (3) ruso de transferir ilegalmente 10 millones de dólares en 6 meses desde diversas cuentas bancarias del Citibank en distintas sucursales del mundo hasta una cuenta del mismo banco en Helsinki (Finlandia).

Ese año un empleado de banco japonés y dos operadores fueron detenidos y acusados de haber transferido ilegalmente por medios informáticos 140.000.000 de yens desde el Takain Bank Ltd a otra cuenta bancaria.

En 1996 Julio César Ardita, un joven de nacionalidad argentina, accedió desde su domicilio a través de Internet a los ordenadores de la Universidad de Harvard en EEUU. Tras suplantar la personalidad de alumnos y profesores realizó nuevas conexiones no autorizadas a ordenadores de instituciones militares de EEUU y empresas de Méjico, Corea, Taiwan y Brasil.

Ese año William Gaede un ingeniero de software fue condenado como sospechoso de sustraer información privilegiada contenida en ordenadores de la compañía Intel valorada en unos 15.000.000 de dólares.

En 1997, Carlos Felipe Salgado de 36 años un hacker venezolano consiguió acceder a través de Internet de forma no autorizada a datos de 100.000 tarjetas de crédito. Salgado intentó vender estos datos a una agente encubierto del FBI (EEUU) por 260.000 dólares unos 50.000.000 de pesetas.

Ese año un estudio realizado por Deloitte and Touche LLP para la Comisión Europea estimó que el fraude internacional ha costado a la Unión Europea alrededor de 33 billones de ecus destacando por su volumen los fraudes cometidos a través de Internet.

En 1998 Sakura unos de los mayores bancos japoneses reconoció que varios ciberdelincuentes habían obtenido de forma no autorizada datos confidenciales de 20.000, de sus 15 millones de clientes y confirmaron que al menos datos referidos a 37 personas habían sido ya vendidos a través de e-mail a un comprador de Tokio.

La encuesta realizada por Price Waterhouse Coopers en 1998, sobre seguridad de la información global muestra que entre los encuestados que fueron capaces de identificar sus pérdidas debido a problemas de seguridad en los últimos 12 meses, el 84 por 100 estimó sus pérdidas entre 1.000 y 100.000 dólares y otro 16 por 100 estimaba sus pérdidas en más de 100.000 dólares.

En 1999, 51 personas fueron arrestadas en China por introducirse ilegalmente en el sistema informático de la red ferroviaria china y modificar el sistema de emisión de billetes lo que afectó a 8.000 billetes valorados en unos 450.000 yuan, unos 10.500.000 pesetas.

A finales de ese año, la Guardia Civil española detuvo en Madrid a un ingeniero acusado de acceso ilegal a través de Internet a la red informática de la Universidad de Utrech (Holanda) y a la copia ilegal de la obra multimedia Champollion sobre los tesoros egipcios en Europa valorada en 6.000.000 de euros.

Todos estos casos muestran una vez más que los delitos informáticos no deben ser considerados cuestión baladí. Hemos podido ver como ya existen ejemplos de que estas actividades ilícitas pueden ocasionar pérdidas millonarias tanto en el sector público como en el privado.

No existen datos fehacientes y expuestos de una forma coordinada sobre los incidentes de seguridad informática conocidos anualmente en España entre otras razones debido a la inexistencia de una coordinación global entre los diferentes centros españoles que pueden contar mayoritariamente con esta información como son: RedIRIS (4), la DIT-UPM (5), el CERT-UPC (6) y el Grupo de Seguridad-Universidad de Sevilla.

No existe tampoco ningún estudio coordinado sobre incidentes de seguridad informática y su coste en Europa, por lo que tenemos que acudir a EEUU y al informe anual de CSI (7) para hacernos una idea de los daños económicos que ocasionan determinados incidentes de seguridad informática en base a encuestas realizadas con la mayoría de los ISP,s (8) estadounidenses desde 1997 hasta 1999.

	Incidentes			Pérdidas totales en dólares			
	1997	1998	1999	1997	1998	1999	97-99
Robo de información contenida en ordenadores	21	20	23	20.048.000	33.545.000	42.496.000	96.089.000
Sabotaje de redes informáticas	14	25	27	4.285.850	2.142.000	4.421.000	10.848.850
Interceptación de emanaciones electromagnéticas procedentes de ordenadores	8	10	10	1.181.000	562.000	765.000	2.508.000
Intrusiones en sistema informático desde el exterior	22	19	28	2.911.700	1.637.000	2.885.000	12.302.750
Abuso de redes informáticas por empleados	55	67	81	1.006.750	3.720.000	7.576.000	12.302.750
Fraude electrónico	26	29	27	24.892.000	11.239.000	39.706.000	75.837.000
Denegación de servicio (bloqueo de sistemas)	D*	36	28	D	2.787.000	3.255.000	6.042.000
Spoofing (9)	4	D	D	512.000	D	D	512.000
Virus	165	143	116	12.498.150	7.874.000	5.274.000	25.646.150
Accesos no autorizados por empleados	22	18	25	3.991.605	50.565.000	3.567.000	58.123.605
Fraude en las telecomunicaciones	35	32	29	22.660.300	17.256.000	773.000	40.689.300
Intervención no autorizada de las comunicaciones	D	5	1	D	245.000	20.000	265.000
Robo de ordenadores	160	162	150	6.132.200	5.250.000	13.038.000	24.420.200

Fuente: Computer Securily Institute.

1997: 391 ISP responden 69%.
1998: 515 ISP responden 99%.
1999: 512 ISP responden 98%.

* Desconocido.

Estas estadisticas ponen de manifiesto claramente que la mayoría de incidentes de seguridad en los sistemas informáticos son causados desde el interior de las organizaciones.

Esta claro que una adecuada politica de seguridad informática debe prestar un marcado interés por el factor personal y por las vulnerabilidades de los sistemas informáticos ocasionadas desde el interior de las organizaciones, empresas e instituciones.

Muchas empresas han emprendido campañas de contratación de técnicos de alto nivel que provienen de compañías competidoras en el sector de la informática o las telecomunicaciones. Estos técnicos suelen aportar conocimientos elevados e incluso se valora en gran medida su conocimiento sobre las vulnerabilidades de la empresa de origen, incluidas las de su sistema informático.

Todo este razonamiento nos conduce inequívocamente a pensar que no nos valdrá de nada realizar una fuerte inversión en la adquisición e instalación de equipos y programas para reforzar la seguridad de nuestro sistema informático si antes no hemos analizado y tomado las medidas necesarias para disminuir los riesgos procedentes de los ataques deslealtades, y descuidos provocados por los empleados o miembros de una institución.

Finalmente cabría decir que cada vez más organizaciones políticas; militares, empresariales, etc., estructuran su flujo de información interior y exterior en torno a un sistema informático que permite al menos el acceso a una intranet y a un sistema de correo electrónico. Al mismo tiempo estas organizaciones proporcionan como es lógico el acceso de sus miembros a Internet donde podrán comunicarse con el resto del mundo de una manera ágil y apor-

tarán un valor añadido a esa organización ya que obtendrán información y gestionarán recursos de una forma más eficaz.

Esta situación es imparable y la organización, empresa o institución que no adapte su estructura a esta tipología quedará pronto desfasada y fuera de la denominada "revolución tecnológica del siglo XXI"

Cuando esta situación se encuentre razonablemente extendida, no existirá apenas información que no se encuentre almacenada o sea transmitida por medios informáticos. A nadie se le escapa que el "coste del delito informático" aumentará proporcionalmente al incremento del uso de los medios informáticos y tecnológicos por parte del hombre. No obstante que duda cabe, que serán prácticamente imposible de evaluar los daños causados por ataques o intromisiones en sistemas informáticos que gestionen infraestructuras básicas para el hombre.

Esperemos que nunca lleguemos a verlo.

NOTAS

(1) Manuel Sanromá. Jefe del Dpto. de Ingeniería Electrónica de la Universidad Rovira i Virgili de Tarragona. fundador de TINET (Tarragona Internet) y miembro del Consejo de Administración de la ISOC (Internet Society) de EEUU.

(2) British Banking Association (Asociación británica de banca).

(3) Intruso informático.

(4) Red académica y de investigación nacional, patrocinada por el Plan Nacional de I+D+I y gestionada por el Consejo Superior de Investigaciones Científicas.

(5) Departamento de Ingeniería de Sistemas Telemáticos Universidad Politécnica de Madrid

(6) Centro para Emergencias en Redes Telemáticas de la Universidad Politécnica de Cataluña.

(7) CSI Computer Security Institute-Instituto de seguridad informática. San Francisco (EEUU).

(8) ISP: Internet Server Provider-Proveedor de Servicios de Internet.

(9) Intrusiones en sistemas informáticos enmascarando técnicamente la personalidad del usuario.

(10) Red informática interna.