Boletín Criminolóxico

Número 11 *Ano 2009*

Director: José Manuel Rebolo Sánchez

Publicado por : Instituto de Criminoloxía
Universidade de Santiago de Compostela
Edificio da Facultade de Dereito, 2º andar
15782 Santaigo de Compostela

Los delitos Informáticos

Traballo presentado por: Sara Rivera Panizo (alumna de Graduado en Ciencias Criminolóxicas e da Seguridade Pública)

Los Delitos Informáticos

Sara Rivera Panizo

Contenido

1. INTRODUCCIÓN

Debido a la necesidad que el ser humano tiene de transmitir información, a lo largo de la historia se han creado diferentes mecanismos para su procesamiento, transmisión y almacenamiento.

Así nace la informática como un "conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores"[1].

En 1969 aparece Internet al establecerse la primera conexión entre ordenadores , denominada ARPANET entre universidades de Utah y California.

Esto produjo un gran impacto en los ámbitos de ocio, trabajo y conocimiento en todo el mundo, debido a la facilidad de acceso a la información.

Hoy en día, es algo común el leer noticias, ver el tiempo, trabajar o comunicarnos con personas de todo el mundo a través de Internet.

Pero no todo son aspectos positivos.

La gran expansión que ha sufrido en los últimos tiempos hace que la información que circula a través de la red llegue a ser algo incontrolable, haciendo que aparezcan conductas antisociales e incluso delictivas entre algunos de sus usuarios.

A lo largo de este trabajo, se pondrán de manifiesto los diferentes tipos de delitos informáticos y sus principales características, las entidades que los combaten y la legislación vigente, no dejando por ello de hacer referencia al delincuente y la víctima, partes fundamentales en cualquier hecho delictivo.

1.1. LA PRIVACIDAD EN INTERNET

La privacidad es el interés que el individuo tiene en mantener un espacio personal, esto es, sin interferencias de ningún tipo por parte de otras personas u organizaciones.

La privacidad en internet, puede dividirse en diferentes materias de estudio:

[1] Término acuñado por la RAE(Real Academia Española)

1.1.1. LA CRIPTOGRAFÍA

Proceso consistente en alterar los datos de un mensaje con una clave de manera que ésta quede ilegible y sólo pueda ser recuperado mediante la introducción de esa clave.

Su función es garantizar el secreto de la comunicación entre dos entidades, ya sean personas u organizaciones.

1.1.2. EL ANONIMATO

Es una forma de no desvelar la identidad de la persona que transmite la información, por ejemplo en el caso de los correos electrónicos.

1.1.3. EL EMAIL O CORREO ELECTRÓNICO

Es un servicio que permite a los usuarios enviar y recibir información privada rápidamente mediante Internet.

1.1.4. LA ESTEGANOGRAFÍA

Es una disciplina en la que se aplican y estudian métodos que permiten ocultar mensajes u objetos dentro de otros que se denominan portadores, de modo que su existencia no sea percibida.

2. CONCEPTO

Con delito informático se define todo acto ilícito penal que ha sido llevado a cabo a través de medios informáticos y que está ligado a los bienes jurídicos relacionados con las tecnologías de la información o que tiene como fin estos bienes.

Por otro lado, cabe hacer referencia al Convenio de Ciberdelincuencia del Consejo de Europa[2], que los define como “actos dirigidos contra la confidencialidad, la

[2] Celebrado en Budapest el 23 de Noviembre de 2001.

integridad y la disponibilidad de los sistemas informáticos, así como el abuso de dichos sistemas, medios y datos".

3. TIPOS

El Código Penal, contempla como delitos informáticos los siguientes actos[3]:

3.1. ATAQUES CONTRA EL DERECHO A LA INTIMIDAD

Se refiere al delito de revelación y descubrimiento de secretos a través de la difusión y la incautación de datos registrados en soportes informáticos.

Se regula en los artículos del 197 al 201 del Código Penal[4].

3.2. INFRACCIONES A LA PROPIEDAD INTELECTUAL

Tratándose de la copia y la distribución de forma no autorizada de programas de ordenador, así como de tenencia de medios para eliminar los dispositivos utilizados para proteger esos programas.

Regulado en el artículo 270 del Código Penal.

3.3. SABOTAJES INFORMÁTICOS

Se trata de delitos de daños que se realizan mediante la destrucción o la alteración de datos, documentos o programas que estén contenidos en redes o sistemas informáticos.

Regulado en los artículos 263 y siguientes del Código Penal.

[3] Según el CNP (Cuerpo Nacional de Policía).

[4] En el apartado número 6 titulado "legislación nacional" se explicarán con más detenimiento los artículos señalados a lo largo de este punto.

3.4. FALSEDADES

Cabe comenzar definiendo qué se entiende por documento. Así, podría decirse que es un soporte material que incorpora o expresa datos.

Se trata en concreto de la falsificación de tarjetas de crédito y la fabricación o tenencia de programas que permitan cometer delitos de falsedad.

Se regula en los artículos 386 y siguientes del Código Penal.

3.5. FRAUDES O ESTAFAS INFORMÁTICAS

Son delitos de estafa cometidos a través de programas o datos para la obtención de un lucro que no es lícito.

Regulados en los artículos 248 y siguientes del Código Penal.

3.6. AMENAZAS

Consisten en el anuncio de un mal futuro ilícito mediante cualquier medio de comunicación.

Su finalidad es causar miedo o inquietud en la persona amenazada.

Se regula en los artículos 169 y siguientes del Código Penal.

3.7. CALUMNIAS E INJURIAS

Conviene definir previamente que se entiende por calumnia y por injuria.

Puede definirse la calumnia como aquella "imputación falsa a una persona de la comisión de un hecho que la ley califique como delito, a sabiendas de que éste no existe o de que el imputado no es el que lo cometió"[5]

Por otro lado, una injuria es un delito producido contra la buena fama o el honor de la persona.

[5] Fuente: http://es.wikipedia.org/wiki/Calumnia

Así, serán delitos cuando se propaguen por cualquier medio que se asemeje a la imprenta o a la radio.

Se regulan en los artículos 205 y siguientes del Código Penal.

3.8. PORNOGRAFÍA INFANTIL

Es uno de los delitos relativos a la prostitución, utilizando a menores o personas incapaces con fines pornográficos o exhibicionistas.

Se regula en los artículos 187 y 189 del Código Penal.

4. CARACTERÍSTICAS

Los delitos informáticos son acciones de tipo ocupacional, ya que en la mayoría de los casos, se realizan cuando el sujeto está trabajando o en su puesto de trabajo.

Cabe mencionar que en la mayor parte de las ocasiones, presentan grandes dificultades a la hora de comprobar quien cometió el ilícito debido a la gran expansión de Internet y a al carácter técnico de estos hechos.

Hasta hace poco, no se producían apenas denuncias en este ámbito, lo que dificultaba su persecución.

También su perpetración es relativamente fácil en cuanto a tiempo y espacio se refiere, ya que pueden llegar a consumarse en poco tiempo y sin necesidad de presencia física del delincuente.

Son delitos que provocan grandes pérdidas económicas para los afectados y grandes "beneficios"[6] para el que comete el delito.

Por último, señalar que en su mayoría, sólo pueden ser cometidos por personas con unos determinados conocimientos técnicos.

[6] De carácter económico.

5. SUJETOS

5.1. TIPOS

5.1.1. SUJETO PASIVO

Son sujetos activos las personas que comenten el delito, en este caso, de índole informático.

Generalmente son personas con especiales habilidades para el manejo de los sistemas informáticos y en muchos casos trabajan en lugares en los que se maneja información.

Ya en el año 1943 el norteamericano Edwin Sutherland introdujo el término de "delitos de cuello blanco" refiriéndose a aquellos que precisan unos determinados conocimientos para su realización.

Algunos autores, sin embargo, afirman que estas habilidades no son indicadoras de la delincuencia informática.

Por último destacar que la única forma de diferenciar a los distintos delincuentes informáticos es a partir del acto que han cometido.

5.1.2. SUJETO ACTIVO

Es la víctima del delito, que puede ser una persona tanto física[7] como jurídica[8] que utilice sistemas automatizados de información, normalmente a través de Internet.

En la mayoría de los casos, no denuncia los delitos informáticos, por lo que su persecución se hace más que complicada.

[7] Toda persona susceptible de adquirir derechos y contraer obligaciones.

[8] Ente al que al que las normas jurídicas reconocen la capacidad para ser titular de derechos y contraer obligaciones. Puede ser una empresa, una organización, el Gobierno…

5.2. PERFIL CRIMINOLÓGICO

Como se expuso anteriormente, las personas que cometen delitos informáticos, o el sujeto activo de dichos delitos, en el mayor número de los casos suelen ser verdaderos expertos en informática que entran sin ningún tipo de permiso a redes y ordenadores ajenos.

Así, los Hackers, que podrían ser los nuevos piratas.

Son personas expertas "en varias o alguna rama técnica relacionada con la informática: programación, redes de computadoras, sistemas operativos, hardware de red/voz, etc. Se suele llamar hackeo y hackear a las obras propias de un hacker"[9].

Por otro lado, los crackers, son personas que "violan la seguridad de un sistema informático de forma similar a como lo haría un hacker, sólo que a diferencia de este último, el cracker realiza la intrusión con fines de beneficio personal o para hacer daño"[10].

Veamos algunos casos reales:

-Kevin Mitnick empezó desde que era un niño a sentir un gran deseo por investigar cosas y lograr objetivos que en principio le parecían imposibles, hasta que llegó a tener una gran habilidad para entrar sin autorización en servidores, robar información, crear virus…

En el año 1992 el Gobierno de Estados Unidos lo acusó de sustraer información del FBI así como de haber entrado sin autorización de ningún tipo en ordenadores militares, convirtiéndose así en un símbolo entre la comunidad internacional de crackers.

Después de una persecución por parte del FBI de 3 años, fue capturado en el año 1995 y condenado a 5 años de prisión.

-Vladimir Harkonen es un joven español que se especializó en diferentes disciplinas como lurker[11], phreaker[12], hacker y cracker.

[9] Fuente: http://es.wikipedia.org/wiki/Dark_heats.
[10] Fuente: http://es.wikipedia.org/wiki/Cracker.
[11] Nombre dado a los participantes de comunidades virtuales que tiene una actividad solamente receptiva, sin contribuir activamente aportando ficheros, escribiendo en grupos de discusión...(fuente: http://es.wikipedia.org/wiki/Lurker)

Se le atribuyen ataques a diferentes empresas de entre las que destaca Sony.

Fue juzgado en la Audiencia provincial de Madrid y sentenciado a 4 años de prisión como culpable de asalto, copia, sustracción y libre distribución de documentación e imágenes consideradas de seguridad nacional.

-Robert Tappan Morris fue uno de los precursores de los virus. En el año 1988 difundió un virus a través de Internet e infectó más de 6000 servidores conectados.

Fue condenado a 4 años de prisión y al pago de 10000 dólares de multa.

El principal objetivo de estos sujetos es extenderse a lo largo del mundo, poniendo siempre por delante la calidad, no la cantidad.

Están sujetos a determinados sistemas de valores y conductas que llegan a constituir una verdadera cultura.

Tienen incluso sus propias reglas de conducta y reglas de status.

No aparecen como grupos antisociales, sino disociales, esto es, realizan conductas transgresoras de las normas sociales, de carácter negativo y destructivas.

Estas personas adoptan un vocabulario propio y característico, incluyendo numerosos términos técnicos.

Así, tienden al uso de reglas gramaticales particulares.

En algunas ocasiones llegan a crear un vocabulario propio con la única intención de no dejar ver lo que dicen y de diferenciarse del resto, logrando obtener de este modo cierto poder.

De este modo, utilizan palabras o frases que literalmente significan una cosa y quieren decir otra, para lograr confundir al que las recibe, de forma que esa persona ejecute un programa cuando en realidad ejecutará lo que el hacker desea.

En cuanto a su nombre, nunca utilizan los verdaderos, sino que se esconden tras pseudónimos.

Estas personas aborrecen ser comparados con los nerds[13]

[12] Persona que investiga los sistemas telefónicos, mediante el uso de tecnología por el placer de manipular un sistema tecnológicamente complejo y en ocasiones también para poder obtener algún tipo de beneficio como llamadas gratuitas(fuente: http://es.wikipedia.org/wiki/Phreaker).

[13] Personas que persiguen actividades intelectuales. Son solitarias y excluidas del resto. Normalmente se asocian con personas de su mismo estilo de vida.

Normalmente huyen de trabajos de oficina, en los que probablemente deberían cambiar sus formas de vestir, al estar obligados a llevar traje.

En cuanto a la televisión, optan por los dibujos animados o series manga, huyendo de lo común.

En la mayoría de los casos son personas agnósticas, aunque algunos hackers profesen religiones como el Budismo zen[14] o el Taoismo[15].

Suelen decantarse por estudiar carreras de especialización como Ingenierías Informáticas, Física o Matemáticas.

Generalmente tienen un alto coeficiente intelectual, y se sienten estimulados con las novedades de tipo intelectual.

Son anticonformistas e individualistas.

Así, muestran interés por cualquier cosa que les permita aprender, esto es, desarrollar su capacidad intelectual.

Refiriéndonos a sus motivaciones, al contrario que la mayor parte de las personas, no se motivan con dinero u otras gratificaciones.

Para ellos el mejor premio es lograr lo que se proponen en un primer momento.

Por último, es necesario destacar que en muchas ocasiones pueden llegar a experimentar adicción.

Así, cuando estas personas se sientan frente a un ordenador suelen experimentar una pérdida de la noción del tiempo acompañado de un olvido de alimentarse.

Suelen renunciar a actividades de tipo social y/o laboral y si no pueden estar delante del ordenador pueden tener incluso síndrome de abstinencia.

6. LEGISLACIÓN NACIONAL

Los delitos informáticos, a pesar de no estar reconocidos como un tipo de delito específico en la legislación española, se encuentran regulados en numerosas normas[16].

[14] Religión en la que las técnicas de meditación son de gran importancia y protagonismo.
[15] Religión cuyo objetivo fundamental es alcanzar la inmortalidad.

Entre ellas, destacan las siguientes:

-Ley 59/2003, de 19 de diciembre de Firma Electrónica; Se encarga de la regulación de la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación.

-Ley 32/2003, de 3 de noviembre General de Telecomunicaciones; "*El objeto de esta Ley es la regulación de las telecomunicaciones, que comprenden la explotación de las redes y la prestación de los servicios de comunicaciones electrónicas y los recursos asociados, de conformidad con el artículo 149.1.21 de la Constitución*"[17].

- Real Decreto Legislativo 1/1996, de 12 de abril, Ley de Propiedad Intelectual: Así, cabe destacar que "l*a propiedad intelectual está integrada por derechos de carácter personal y patrimonial, que atribuyen al autor la plena disposición y el derecho exclusivo a la explotación de la obra, sin más limitaciones que las establecidas en la Ley*"[18].

-Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal; "*tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar*"[19].

- Ley 34/2002 de 11 de Julio de Servicios de la Sociedad de la Información y Comercio Electrónico; cuyo objeto será "*la regulación del régimen jurídico de los servicios de la sociedad de la información y de la contratación por vía electrónica, en lo referente a las obligaciones de los prestadores de servicios incluidos los que actúan como intermediarios en la transmisión de contenidos por las redes de telecomunicaciones, las comunicaciones comerciales por vía electrónica, la información previa y posterior a la celebración de contratos electrónicos, las condiciones relativas a su validez y eficacia y el régimen sancionador aplicable a los prestadores de servicios de la sociedad de la información*"[20].

[16] Según el CNP.
[17] Artículo 1.1 de la ley 32/2003 General de Telecomunicaciones.
[18] Artículo 2 de la ley 1/1996, de 12 de abril.
[19] Artículo 1 de dicha LO 15/1999, de 13 de diciembre.
[20] Artículo 1 de la ley 34/2002, de 11 de Julio.

-Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

Aparte de estas normas, el Código Penal hace referencia a conductas relacionadas con los delitos informáticos en numerosos artículos.

De entre ellas, las más importantes son las mencionadas en los siguientes artículos:

-Artículo 186; Se hace alusión al que, por cualquier medio directo, venda, difunda o exhiba material pornográfico entre menores de edad o incapaces. El castigo será la pena de prisión de seis meses a un año o multa de 12 a 24 meses.

-Artículo 189; Hace referencia a las medidas que se impondrían a quien utilice menores de edad o personas incapaces con fines exhibicionistas o pornográficos, y quien produzca, venda o distribuya, exhiba o facilite la producción, venta, distribución o exhibición de material pornográfico en cuya elaboración se hayan utilizado menores de edad o incapaces.

-Artículo 197; contempla las penas con las que se castigará a quien con el fin de descubrir los secretos o vulnerar la intimidad de otro, se apodere de cualquier documentación o efecto personal, intercepte sus telecomunicaciones o utilice artificios de escucha, transmisión, grabación o reproducción de cualquier señal de comunicación.

A quien acceda por cualquier medio, utilice o modifique, en perjuicio de terceros, a datos reservados de carácter personal o familiar, registrados o almacenados en cualquier tipo de soporte.

También se castiga a quien difunda, revele o ceda a terceros los datos o hechos descubiertos.

-Los artículos 248 y 249; tratan de las estafas. El artículo 248 se centra en las estafas llevadas a cabo mediante manipulación informática o artificios semejantes a esta. Prisión de 3 meses a 6 años.

-Los artículos 255 y 256; recogen las penas que se impondrán a quienes comentan defraudaciones utilizando, entre otros medios, las telecomunicaciones. Multa de 3 a 12 meses.

-Artículo 264.2; hace referencia a las penas que se impondrán al que por cualquier medio destruya, altere, inutilice o de cualquier modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos. Prisión de uno a tres años y multa de doce a veinticuatro meses

-Artículo 278.1; se refiere a las penas con las que se castigará a quien, por cualquier medio destruya, altere, inutilice o de cualquier modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos, con el fin de descubrir secretos de empresa. Prisión de dos a cuatro años y multa de doce a veinticuatro meses.

-Artículo 270; pone de manifiesto las penas con las que se castigará a quienes reproduzcan, distribuyan o comuniquen públicamente, una parte o la totalidad de una obra literaria, artística o científica, con ánimo de lucro y perjuicio de terceros. Prisión de seis meses a dos años y multa de 12 a 24 meses.

-Artículo 273; establece las penas que se impondrán a quienes sin consentimiento del titular de una patente, fabrique, importe, posea, utilice, ofrezca o introduzca en el comercio, objetos que estén bajo el amparo de esos derechos, con fines comerciales o industriales. Prisión de seis meses a dos años y multa de 12 a 24 meses.

8. ENTIDADES PARA COMBATIR LOS DELITOS INFÓRMATICOS

Cabe hacer referencia, en primer lugar a la Guardia Civil;

Existe un organismo especializado en la investigación de los delitos que se realizan contando con las nuevas tecnologías o de Internet, es el llamado Grupo de Delitos Telemáticos.

Este grupo, se encuentra dentro de la Unidad Central Operativa de la Guardia Civil y sus principales funciones son la identificación y detección de los delitos informáticos en la red así como la realización de investigaciones que tengan que ver con el ámbito de la delincuencia informática.

Por otro lado, está la Policía Judicial;

Cuenta con la BIT[21]. Esta brigada se encuentra dentro de la Unidad de Delincencia Especializada y Violenta, y está destinada principalmente a la investigación de las nuevas formas de delincuencia.

La Brigada de Investigación Tecnológica, está formada por siete grupos operativos especializados. Estos grupos son los siguientes:

-Dos grupos de protección al menor que se encargan de perseguir los delitos que estén relacionados con la pornografía infantil.

-Dos grupos de fraudes en Internet. Uno de ellos está especializado en subastas y ventas fraudulentas por internet, y el otro en pishing[22]

-Un grupo de seguridad lógica que se dedica a la investigación del robo de datos, el hacking y las intrusiones.

-Un grupo de fraude en el uso de las telecomunicaciones, que se centra en investigar las amenazas, calumnias o injurias que se realizan a través de Internet.

-Un grupo de propiedad intelectual que se dedica a la investigación de los delitos de piratería.

Aparte de esta Brigada de Investigación Tecnológica, el CNP cuenta también con el apoyo de los Grupos especializados en delincuencia tecnológica, los cuales están incluidos en Jefaturas Superiores.

9. ESTADÍSTICAS

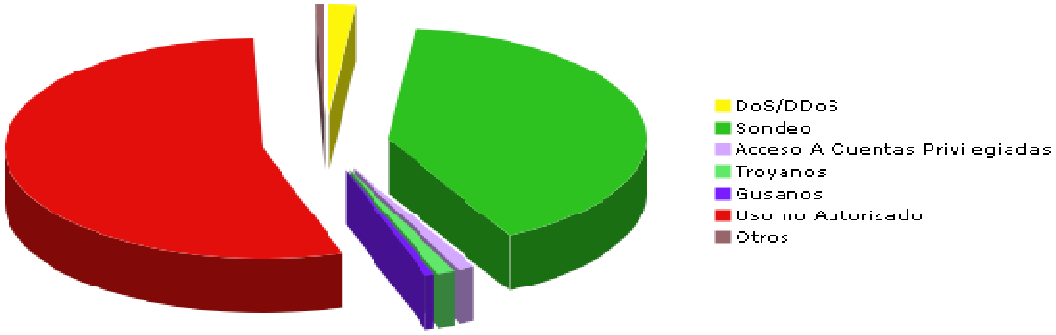
Francisco Canals, presidente del Observatorio Español de Internet, emitió un informe en el que se ponía de manifiesto que 24000 españoles habían sufrido estafa o fraude a través de Internet durante el año 2002.

Los siguientes datos y gráficas[23] han sido extraídos de www.rediris.es.
RedIRIS es la Red española para Interconexión de los Recursos Informáticos de las universidades y los centros de investigación. Fue fundada en el año 1988 como un proyecto del Ministerio de Educación y Ciencia en colaboración con Telefónica.

[21] Brigada de Investigación Tecnológica.
[22] Tipo de delito de estafa que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta. Fuente: http://es.wikipedia.org/wiki/Carding).
[23] Del año 2007.

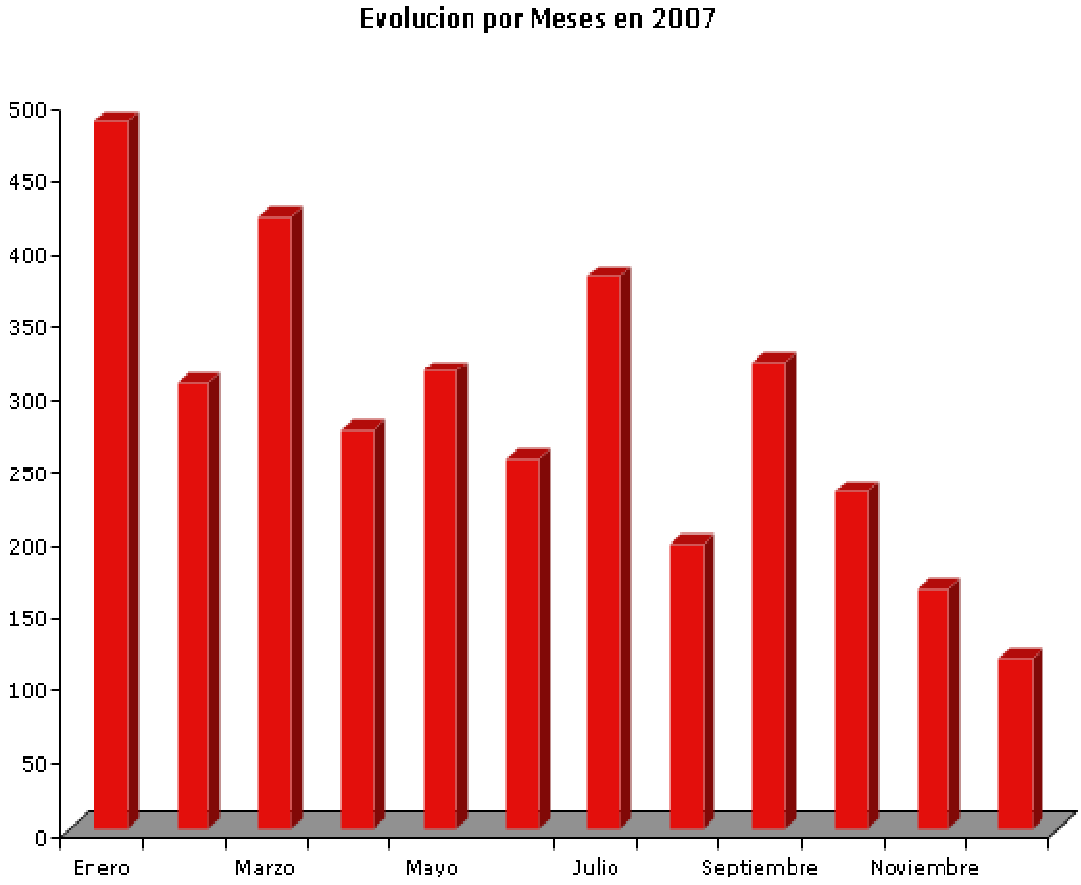
En la actualidad está gestionada por la Entidad Pública empresarial Red.es y financiada por el Plan Nacional de I+D+i.

Esta gráfica muestra la distribución de incidentes según el tipo:

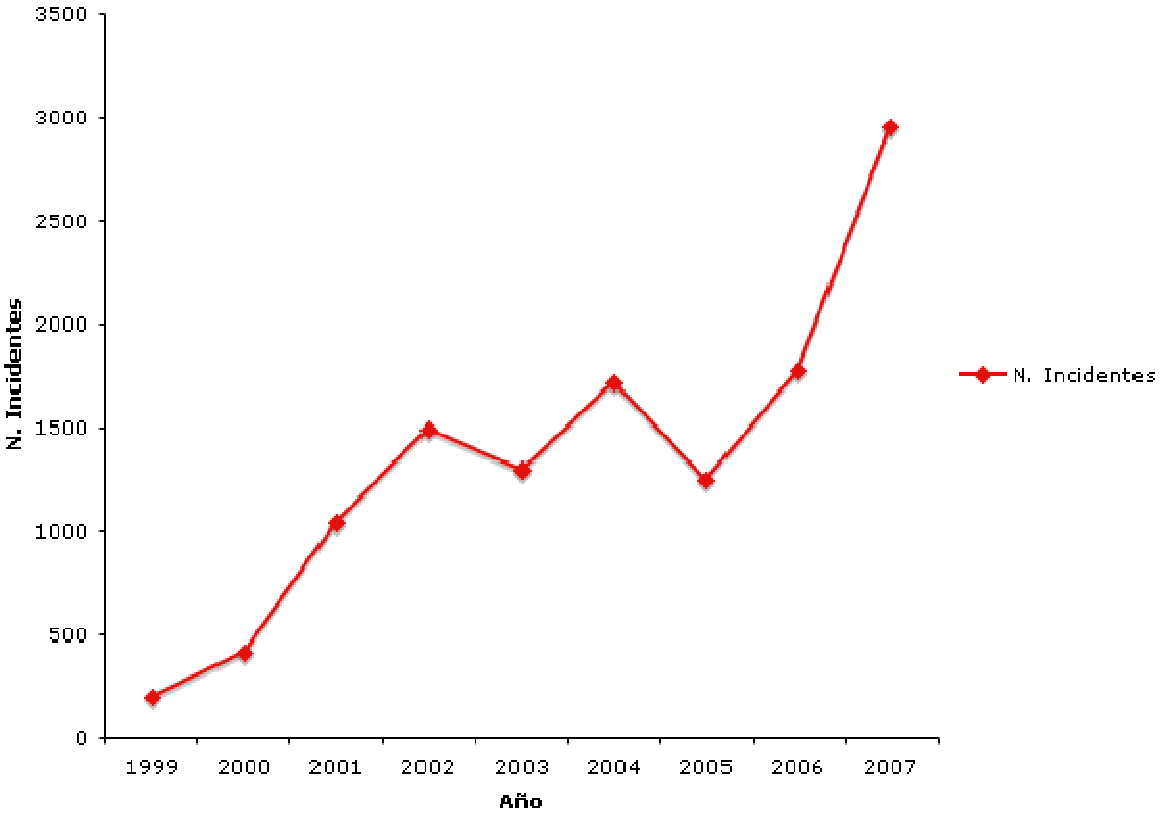


Los incidentes de uso no autorizado son los más elevados y en su mayoría corresponden a casos de pishing o problemas de inyección de código web.

A continuación se muestra la evolución de los delitos informáticos por meses a lo largo del año 2007:



Por último se muestra la evolución de este tipo de delitos a lo largo de los años:



Durante el año 2007 la web se eligió como el primer punto de ataque para el intento de infección de víctimas vulnerables (vulnerabilidades en los sistemas PHP instalados, y errores de programación y falta de concienciación de los programadores Web, vulnerabilidades conocidas en los navegadores más utilizados, inyección de código SQL, XSS…) Estos sitios, una vez están bajo el control de los atacantes se usan para lanzar otro tipo de ataques sobre todo de Pishing.

Los ataques de Pishing han seguido teniendo protagonismo durante el año 2007 y no han decrecido tampoco en los últimos años.

Para finalizar, es necesario decir que el patrón de ataque sigue siendo dirigido, silencioso e inteligente y siempre con algún trasfondo.

10. BIBLIOGRAFÍA

"Derecho Informático. Julio Téllez Valdés". McGrawHill.

"Delitos Informáticos y Delitos Comunes cometidos a través de la informática". Enrique Orts. Tirant lo Blanch, 2001.

"Cibercrimen. Los delitos cometidos a través de internet". Javier Gustavo Fernández. Constitutio Criminalis Carolina, 2007.

www.wikipedia.es

www.rediris.es