# UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

## FACULTAD DE INGENIERIA

# CIBERDELITO

**T E S I S**

**QUE PARA OBTENER EL TÍTULO DE:**

**INGENIERO EN TELECOMUNICACIONES**

**P R E S E N T A N:**

**LARIOS ESCAMILLA JORGE ADAIR**
**SÁNCHEZ GONZÁLEZ RODRIGO JULIÁN**

**DIRECTOR DE TESIS: ING. JESÚS REYES GARCÍA**

**MÉXICO, D.F., 2014**

***Jorge Adair Larios Escamilla***

**A mi familia**

Por las enseñanzas y el apoyo

brindado en el transcurso de la vida.

**A mis amigos y compañeros**

Por las tantas buenas

experiencias compartidas.

**A la Universidad Nacional Autónoma de México**

Por formarme como persona

y como profesionista.

**Al Ing. Jesús Reyes García**

Por hacerse cargo de la dirección de

este trabajo, por su apoyo y dedicación

en la realización del mismo.

***Rodrigo Julián Sánchez González.***

***A mi madre.***

Este logro es tuyo, y de nadie más. ¡Muchas gracias!

***A mi hermana.***

Siempre querer ir un paso adelante, me llevó hasta aquí.

***A mi novia, Blanca Iris.***

Ese apoyo al final de todo esto, me dio el ánimo y la energía para terminar.

***A mi compañero de tesis, Adair.***

Amigo, hermano. Mi compañero durante toda la carrera.

***A los profesores de la carrera***.

En especial, al Ing. Jesús Reyes García, por aceptar la dirección de la tesis.

***A mis jefes*.**

Dr. Víctor García Garduño, por darme la oportunidad de tomar experiencia laboral en el depto. De Telecomunicaciones.

Al Ing. Miguel Ángel Fuentes, por la confianza que me dio para desarrollarme y aprender mucho durante mi Servicio Social en la STPS.

***A mis amigos***.

Adair, David, Luis Omar, Iván, Sergio, Juan Pablo, Mauricio, Jairo, Julio César, Rafael, Gustavo. Fue divertido trabajar con ustedes, y gracias por sacarme de uno que otro problema.

***A la Universidad Nacional Autónoma de México, a la Facultad de Ingeniería***.

Muchas gracias por ser la parte fundamental de mi formación profesional.

***Y a todos aquellos que creyeron en mí*.**

Pero mucho más, en los que no creyeron en mí. Me hicieron querer demostrarles que si se puede.

***INDICE.***

***Índice de tablas.***

***Índice de figuras***

# ***INTRODUCCION.***

Internet se ha vuelto una de las herramientas más útiles, complejas y usadas de la historia, ya que permite brindar una cantidad enorme de productos y servicios que no sólo se enfocan a un sector, es decir se encuentra utilidad a esta en el sector gobierno, militar, económico, en el sector privado, salud etc.

Su creación y desarrollo no se llevó a cabo en un día; en este primer capítulo se aprecia ese complejo desarrollo y se muestran los acontecimientos más importantes para que esta herramienta llegara a la complejidad y utilidad que se tiene hoy día desde aquellos primeros conceptos y primeros nodos pasando por la apertura a la sociedad hasta la actualidad.

La seguridad informática ha tomado gran auge, debido a las cambiantes condiciones y nuevas plataformas tecnológicas disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes a las empresas para mejorar su productividad y poder explorar más allá de las fronteras nacionales, lo cual lógicamente ha traído consigo, la aparición de nuevas amenazas para los sistemas de información.

En este sentido, las políticas de seguridad informática surgen como una herramienta organizacional para concientizar a los colaboradores de la organización sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la empresa crecer y mantenerse competitiva, asegurando el buen uso de los recursos informáticos y la información como activos de una organización, manteniéndolos libres de peligros, daños o riesgos.

La seguridad informática se puede clasificar en seguridad lógica y seguridad física, y busca con la ayuda de políticas y controles mantener la seguridad de los recursos y la información manejando los riesgos.

El objetivo de este trabajo es brindar un panorama de lo que es la seguridad de la información. El primer tema que se toca es la evolución de las comunicaciones entre computadoras, iniciando con el porqué de ésta necesidad, es decir los primeros modelos militares los cuales tenían como objetivo descentralizar toda la infraestructura, esto con el objetivo de poder operar y poder coordinarse aun después de un gran ataque.

Conforme pasó el tiempo este concepto dejo de ser exclusivamente militar, abriéndose a las universidades, a las empresas y por ende a la sociedad en general; todos estos sucesos, toda esta evolución es mostrada en el primer capítulo de este trabajo, resaltando fechas importantes así como los nombres de algunos personajes que permitieron este cambio, también se destacan datos importantes como los primeros navegadores, servicios populares que brinda Internet y hasta algunos proyectos como Minitel, que se puede considerar alternativo. Por último se habla

sobre el primer ataque informático (pues es el nacimiento de esta área) y se muestran datos con los que se consideran los 10 softwares más peligrosos de la historia de la informática.

En el capítulo dos se describe una base de lo que son los diversos ataques a sistemas informáticos, para esto se habla desde la diferencia entre hacker y cracker, además se muestra que en el mundo de la seguridad informática existen más niveles y más nombres para referiste a las personas que tienen conocimientos en esta área.

Después de aclarar los nombres y las características de los personajes que se pueden encontrar en este mundo, se habla sobre los ataques a un equipo, ya sea de modo local o de modo remoto. Lo anterior, sin hacer distinción entre el tipo de equipo que se pueda vulnerar, es decir si es equipo de red o una simple estación de trabajo, y se muestra que no importa el sistema operativo se tenga ya que cualquiera puede ser violado.

A lo largo del capítulo dos, se tocan ataques más finos, es decir, que se pueden hacer dentro de la misma red local obteniendo todos los datos que se envían por la red, o ataques aún más peligrosos hechos a servidores en Internet. En esta parte se mencionas algunas tácticas para evitar estos incidentes, así como algunas recomendaciones para tener un mejor manejo de la información en la red.

En el capítulo tres, se habla sobre los delitos relacionados en contenido, es decir, cuando se usa la tecnología como herramienta para cometer otros delitos, ya sean fraudes, pornografía infantil, o violaciones a los derechos de autor entre muchos otros.

En el capítulo cuatro de este trabajo, se habla sobre lo que se conoce como derecho informático, que no es más que cómo se debe legislar ante estas acciones, ya sea con la tecnología como herramienta para cometer un ilícito, o cuando se han dañado los sistemas informáticos impactando a un negocio económicamente, o en algunos otros casos cuando se ha robado información.

En este apartado no sólo se enfoca en lo que se ha trabajado en México, se muestran leyes y convenios internacionales que pueden servir de referencias en nuestro país para la mejora continua de la legislación en este tema; algunas leyes, convenios, o legislaciones que se muestran son la estadounidense, la británica y la española, que son de las más completas que se pueden encontrar en el mundo, esto en gran parte por que el estallido de la popularidad del uso de Internet se ha dado primero en estos sitios lo que ha dado lugar a que toda esta problemática de ilícitos se haya presentado mucho antes que en México.

# *1. HISTORIA DEL SURGIMIENTO DE INTERNET*

## ***1.1. Primeras redes de comunicaciones.***

Antes de la Segunda Guerra Mundial, las redes telegráficas y las redes telefónicas, además de las transmisiones de radio y posteriormente de televisión, eran las más utilizadas en todo el mundo. Las primeras computadoras, cuando tenían la necesidad de comunicarse entre ellas, lo tenían que hacer desde un medio centralizado, en este caso, la red telefónica pública conmutada.

El sistema telefónico de conmutación consiste en un conjunto de centrales telefónicas enlazadas por medio de canales. La función de las centrales consiste en establecer un circuito o canal ininterrumpido entre los dos aparatos que sostiene una conversación. Es evidente que no es posible tener un canal de comunicaciones entre cualquier par de usuarios del servicio telefónico. La solución que se instrumentó para resolver este problema es la siguiente: considerando que se requiere un enlace dedicado entre todas las posibles parejas de usuarios, para hacer llegar la llamada proveniente de ese usuario desde su hogar u oficina hasta la red telefónica, se establece un canal entre el usuario y la central más cercana. Entre las diferentes centrales existen suficientes canales para que un buen número de usuarios puedan sostener conversaciones simultáneamente. Estos canales se asignan a conversaciones, de acuerdo con el orden solicitado por los usuarios.

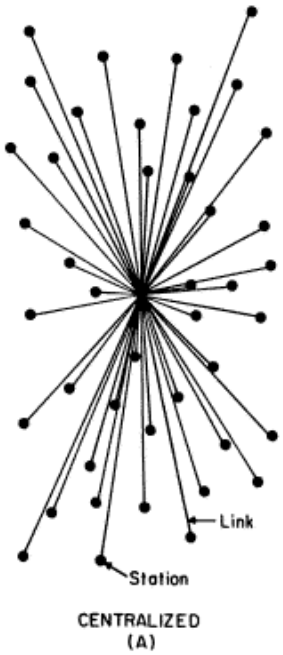



Figura 1. Primeros desarrollos de redes centralizadas.

### ***1.2. Experimentos militares.***

En 1946, los científicos estadounidenses John Presper Eckert y John William Mauchly construyeron la ENIAC (Electronic Numerical Integrator And Computer) en la Universidad de Pennsylvania, la cual tenía el propósito de calcular la trayectoria de proyectiles para el laboratorio de balística del ejército. El 2 de octubre de 1955, la ENIAC es desactivada para siempre.

En 1948, como una de las tantas consecuencias de la Segunda Guerra Mundial, surgió un proyecto denominado RAND (Research and Development), cuyo propósito, desde su fundación y hasta la actualidad, es fomentar y promover con fines científicos, educativos y de caridad el bienestar público, y sobre todo, mantener a la vanguardia a los E.U.A. en materia de avances científicos, priorizando de esta forma su seguridad nacional. El proyecto RAND fue desarrollado para facilitar el intercambio entre investigadores en inteligencia artificial.

Como consecuencia de la naciente Guerra Fría, la Unión Soviética, en 1957, lanza el Sputnik, el primer satélite artificial. En respuesta a este hecho, Estados Unidos, con Eisenhower de presidente, crea el ARPA (Organismo de proyectos de Investigación Avanzada) en 1958, dentro del Ministerio de Defensa (DOD) con el fin de establecer su liderazgo en el área de la ciencia y la tecnología aplicadas a las fuerzas armadas.

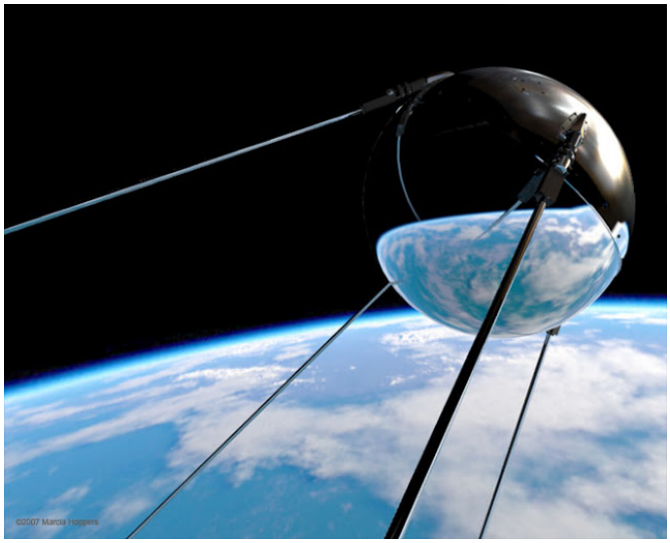


Figura 2. Satélite artificial Sputnik 1.

### ***1.3 El porqué de Internet. Primeras ideas.***

E.U.A. y la antigua U.R.S.S. estaban en plena guerra fría en el año de 1960. La RAND Corporation americana, dentro de sus funciones, se formuló una cuestión que iba tomando más relevancia conforme avanzaban los días: ¿Cómo se podrían comunicar con éxito las autoridades norteamericanas tras una guerra nuclear?

La América postnuclear necesitaría una red de comando y control enlazado de ciudad a ciudad, estado a estado, base a base. ¿Cómo sería controlada esa red? Cualquier autoridad central, cualquier núcleo de red centralizado, como las comunicaciones por red telefónica, o las radio bases utilizadas hasta entonces, serían un objetivo obvio e inmediato para un misil enemigo. El centro de la red sería el primer lugar a derribar.

La RAND le dio muchas vueltas a este difícil asunto en secreto militar y llegó a una solución atrevida.

La propuesta de la RAND se hizo pública en 1964. En primer lugar, la red "no tendría autoridad central". Además, sería "diseñada desde el principio para operar incluso hecha pedazos".

Todos los nodos en la red serían iguales entre sí, cada nodo con autoridad para crear, pasar y recibir mensajes. Los mensajes se dividirían en paquetes, cada paquete dirigido por separado. Cada paquete saldría de un nodo fuente específico y terminaría en un nodo destino. Cada paquete recorrería la red según unos principios particulares. La ruta que tome cada paquete no tendría importancia. Solo contarían los resultados finales.

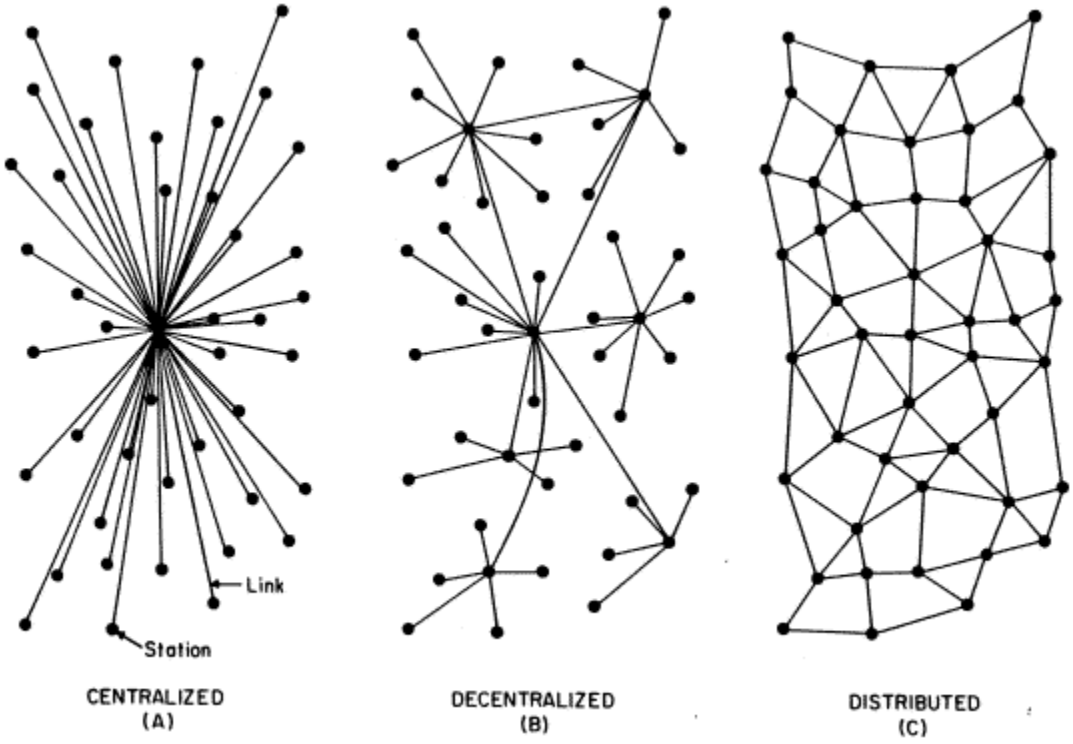



Figura 3. Redes centralizadas, descentralizadas y redes distribuidas.

En 1962, J.C.R. Licklider escribe un ensayo sobre el concepto de Red Intergaláctica, donde todo el mundo está interconectado haciendo posible acceder a programas y a datos desde cualquier lugar del planeta. En octubre de ese año, Lickider es el primer Director de ARPA, al cual denomina: IPTO Information Processing Techniques Office.

En ese mismo año, las Fuerzas Aéreas de Estados Unidos pidieron a un reducido grupo de investigadores que creara una red de comunicaciones militares que pudiera resistir un ataque nuclear. El concepto de esta red se basaba en un sistema descentralizado, de manera que la red pudiera seguir funcionando aunque se destruyeran uno o varios equipos.

### ***1.4 El modelo Baran***

Paul Baran es considerado como una de las figuras clave de la creación de Internet; en 1964, tuvo la idea de crear una red con la forma de una enorme telaraña. Se había dado cuenta de que un sistema centralizado era vulnerable, ya que si se destruía su núcleo, se podían cortar todas las comunicaciones. Por tal motivo, creó un modelo híbrido al utilizar la topología de estrella y de malla, en el que los datos viajarían dinámicamente "buscando" la ruta más clara y "esperando" en caso de que todas las rutas estuvieran bloqueadas. Esta tecnología se denominó "conmutación de paquetes"

### ***1.5 Primeros avances.***

Un año más tarde, un comité industria-gobierno desarrolla el código ASCII, por American Standard Code for Information Interchange y primer estándar universal para computadoras. Este es un paso fundamental pues permite que máquinas de todo tipo y marca intercambien datos.

En el año de 1965 las computadoras TX-2, en el laboratorio Lincoln del MIT y el AN/FSQ-32 de la System Development Corporation (Santa Mónica, California) quedan vinculadas directamente (sin conmutación por paquetes) por medio de una línea telefónica dedicada de 1 200 bps; más tarde se agrega la computadora de la Digital Equipment Corporation en ARPA y así conforma la red.

Dos años después, en 1967 El Laboratorio Nacional de Física en Middlesex, Inglaterra, desarrolla la red NPL Data Network, supervisada por Donald Watts Davies, quien introdujo el término "paquete". La red NPL, un experimento en conmutación por paquetes, utilizaba líneas telefónicas de 768 Kbps.

En ese mismo año, Wesley Clark, quien era un experto de la ARPA, sugirió que la red fuese administrada por dispositivos llamados IMP, 'Interface Message Processors' ubicados enfrente de los grandes computadores, dando lugar a los "ruteadores" actuales.

En 1968, el Laboratorio Nacional de Física de Gran Bretaña preparó la primera red de prueba basada en estos principios. Poco después, la Agencia de Proyectos de Investigación Avanzada del Pentágono (ARPA) decidió financiar un proyecto más ambicioso y de mayor envergadura en los Estados Unidos.

Los nodos de la red iban a ser supercomputadoras de alta velocidad (o lo que se llamara así en aquel momento). Eran máquinas poco usuales, de mucho valor, y que necesitaban de un buen entramado de red para proyectos nacionales de investigación y desarrollo.

### *1.6 Primeros nodos. Surgimiento de ARPANET.*

En la siguiente tabla, se muestra la distribución de los primeros 4 nodos que entraron en operación por ARPANET; los 4 nodos, estaban ubicados en diferentes universidades del occidente de los E.U.A.

| Nodo | Fecha (año de 1969) | Función |
|---|---|---|
| Universidad de Los Ángeles, California. | 30 de Agosto | Centro de evaluación de redes. |
| Instituto de Investigaciones de Stanford. | 1 de Octubre | Centro de Información de Redes |
| Universidad de California Santa Barbara | 1 de Noviembre | Matemática Interactiva de Culler - Fried. |
| Universidad de Utah. | Diciembre | Gráficos. |

Tabla 1. Distribución de los primeros nodos de ARPANET.


Figura 4. Primeros 4 nodos de ARPANET, diciembre de 1969.

Los primeros paquetes se enviaron en la UCLA tratando de conectarse al SRI (centro de investigación de Stanford).

En 1970, ARPANET comienza con un proceso de expansión, la cual consistía en implementar un nuevo nodo por mes; un año más tarde, la red ya contaba con 15 nodos y 23 servidores.

Los servidores de ARPANET comienzan a utilizar los Protocolos de Control de Redes (NCP) Primer protocolo "servidor-a-servidor ", AT&T instala el primer vínculo costa a costa entre la UCLA y BBN (Bolt, Beranek y Newman) a 56 kbps. Está línea fue reemplazada más tarde por otra entre BBN y RAND. Se agrega una segunda línea entre el MIT (Massechussetts Institute of Technology) y la Universidad de Utah.

### ***1.7 Nacimiento del correo electrónico.***

Entre 1971 y 1972, nace el correo electrónico: Ray Tomlinson de BBN inventa un programa de correo electrónico para mandar mensajes en redes distribuidas. El programa original es producto de otros dos: un programa interno de correo electrónico (SENDMSG) y un programa experimental de transferencia de archivos (CPYNET) con lo que nace el e-Mail. Ray Tomlinson modifica el programa de correo electrónico para ARPANET, donde se transforma en un éxito. Se elige el signo @ entre los signos de puntuación de la máquina de teletipos Tomlinson Modelo 33 para representar el "en".

### ***1.8 Primeros protocolos y servicios basados en ARPANET.***

Entre 1975 a 1978, la DARPA continuó haciendo pruebas con base a lo que ya habían desarrollado, llegando a dividir a TCP (Transmission Control Protocol) en éste último año, en lo que hasta el día de hoy se conoce como el protocolo TCP/IP.

Para 1979, la ISO (International Organization for Standardization) definió un esquema de funciones de comunicaciones para el intercambio de información entre sistemas de computadoras que se llama **MODELO DE REFERENCIA DE INTERCONEXIÓN DE SISTEMAS ABIERTOS (O.S.I. OPEN SYSTEMS INTERCONECTION)**

El modelo OSI provee un conjunto detallado de estándares que describen una red. Es una plataforma de desarrollo de estándares para protocolos de redes.

Este modelo, usa capas operacionalmente bien definidas, que describen que ocurre en cada paso del procesamiento de datos para la transmisión.

El principio de división en capas:

- Se crea una capa para cada nivel de abstracción diferente.
- Cada capa debe tener una función bien definida.
- Estas funciones corresponden a estándares internacionales
- Es mínimo el flujo de información entre interfaces.
- Se genera una arquitectura conceptualmente manejable.

Cada capa consta de 2 partes:

- Definición de un servicio (definición abstracta de QUÉ provee la capa).
- especificación del protocolo (especificación exacta de CÓMO la capa provee el servicio (describe las reglas que implementan un servicio en particular))

Desde que éste modelo fue presentado, se propuso utilizar una gama de protocolos, algunos de estos protocolos se mencionan a continuación.

Protocolos propuestos para ARPANET

- Connectionless Network Protocol (CLNP)
- Connection-Oriented Network Protocol (X.25)
- Network Fast Byte Protocol
- End System to Intermediate System Routing Exchange Protocol (ES-IS)
- Intermediate System to Intermediate System Intra-domain Routing Protocol (IS-IS)
- End System Routing Information Exchange Protocol (SNARE)
- Transport Protocol Class 0, 1, 2…4 (TP0, TP1, ..., TP4)
- Transport Fast Byte Protocol

Mientras que las 7 capas del actual modelo OSI siguen siendo una referencia e incluso algunos de sus protocolos como el X.400, X.500 y IS-IS han tenido mucho impacto, los demás protocolos dejaron de ser utilizados como consecuencia de la entrada de los protocolos TCP e IP.

### ***1.9 De ARPANET a Internet: periodo 1975-1989.***

En la siguiente tabla, se muestra la cronología de aparición de protocolos y servicios durante el periodo 1981-1989.

| Año | Protocolo/servicio | Usos principales |
|---|---|---|
| **1979** | newsgroups | Aplicación cliente-servidor en la cual los usuarios se conectan mediante discado telefónico con un servidor de newsgroups requiriendo que se les envíen los últimos mensajes de determinados grupos. |
| **1981** | BitNet | Because it's time NETwork: Provee correo electrónico y servidores listserv que distribuyen información así como también transferencia de archivos. |
| | CSNET | Computer Science Network: su objetivo fue prestar servicios de red (especialmente de correo electrónico) a los científicos que carecían de acceso a la ARPANET. Más tarde la CSNET se conocerá como la Red de Computación y Ciencia. |
| **1982** | TCP, IP, TCP/IP | Surge Protocolo de Control de Transmisión (TCP) y el Protocolo de Internet (IP) como el conjunto de protocolos, conocido comúnmente como TCP/IP, para ARPANET. |
| | EGP | Exterior Gateway Protocol para el acceso entre redes (de diferentes arquitecturas). |
| **1983** | DNS | Aparece Domain Name System (DNS), Sistema de Nombre de Dominios, recomendando el uso del sistema de direccionamiento |

| | | |
|---|---|---|
| | | actual user@host.domain. El servidor de nombres fue desarrollado en la Universidad de Wisconsin; con este sistema ya no se requiere que el usuario conozca la ruta exacta para acceder a otros sistemas. |
| **1984** | dominios de Internet | .gov, .mil, .edu, .org, .net y .com. El dominio denominado .int, para identificar entidades internacionales, no es usado en ese momento. Se pone en marcha el código de dos letras para identificar a los países. |
| **1985** | symbolics.com | Primer dominio registrado el 15 de Marzo. Otros: cmu.edu, purdue.edu, rice.edu, ucla.edu (Abril); css.gov (Junio); mitre.org, .uk. |
| **1987** | backbone T1 | Backbone de alta velocidad T1 (1.544 Mbps) conectando sus súper centros. La idea es tan exitosa que ya se comienza a pensar en instrumentar una versión T3 (45Mbps). |
| **1988** | IANA | Autoridad de Asignación de Números de Internet: entidad que supervisa la asignación global de direcciones IP, sistemas autónomos, servidores raíz de nombres de dominio DNS y otros recursos relativos a los protocolos de Internet. |
| | IRC | Jarkko Oikarinen desarrolla el Internet Relay Chat (IRC) (Difusora de charlas en Internet). |

Tabla 2. Protocolos creados por ARPANET.

### *1.10 Surgimiento de Internet. ARPANET desaparece.*

- Para 1989 el número de hosts se incrementa de 80,000 en enero a 130,000 en julio y a 160,000 en noviembre. A partir de éste punto de inflexión positiva comienza la explosión del fenómeno Internet.
- Australia, Alemania, Israel, Italia, Japón, México, Holanda, Nueva Zelandia y el reino Unido se unen a Internet.
- La velocidad crece: NSFNET va a T3. En las LAN, Local Area Networks, Redes Locales, se opera a 100Mbps.
- Las compañías telefónicas comienzan a trabajar en sus propias WAN, Wide Area Networks, Redes Extendidas, con tecnología de paquetes a mayores velocidades.
- ARPANET deja de existir en el año de 1990.
- World se pone en línea (world.std.com) y de esta manera se convierte en el primer proveedor comercial de acceso telefónico a Internet.
- Aparecen en Internet instituciones tales como la Biblioteca del Congreso de los Estados Unidos, la Biblioteca Nacional de Medicina (USA), Dow Jones, y Dialog.
- En el año de 1991 Nace la Commercial Internet eXchange Association Inc., después de que la NSF eliminara las restricciones comerciales que regían sobre el uso de la Red.
- Brewster Kahle inventa los Wide Area Information Servers (WAIS), (Servidores de Información de área amplia. Permite indexar y acceder a la información de Internet) Asienta las bases de la manipulación e indexación de información de hoy en día en la WWW.

### ***1.11 Aparece la WWW. Internet para todos.***

En 1992, Paul Linder y Mark P. McCahill de la Universidad de Minessota lanzan Gopher, que es un servicio de Internet consistente en el acceso a la información a través de menús. Mientras tanto, la CERN lanza la World-Wide Web (WWW) creada por Tim Berners.

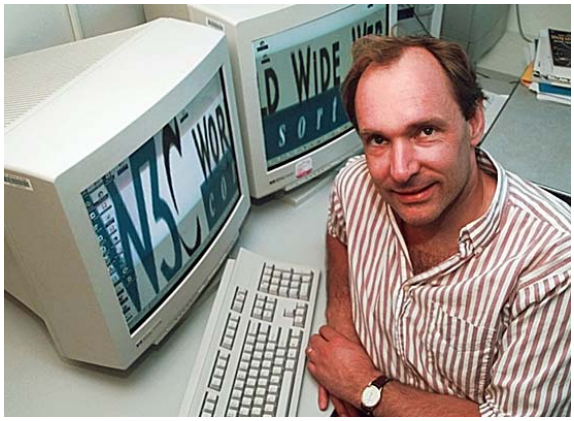


Figura 5. Tim Berners, creador de la WWW.

Berners comenzó a escribir un programa que le permitiera almacenar información. De modo magistral dio forma y aplicación a un par de conceptos que ya habían sido formulados anteriormente de forma más o menos vaga y genérica: el hipervínculo, que conducía directamente al concepto de hipertexto, de ahí al de páginas HTML (páginas Web) que a su vez, darían origen a un nuevo servicio de Internet que acabaría arrasando, y a un nuevo paradigma de arquitectura de la información: Los "Hipermedia".

Las páginas de hipertexto, con sus hipervínculos enlazando información en cualquier parte del mundo, tejen una telaraña mundial, de ahí el nombre que recibió, Telaraña Mundial, "World Wide Web", abreviadamente "La Web".

Tras varios años de desarrollo, Tim Berners mejora la implementación del hipertexto liberándolo al uso público.

### ***1.12 Un proyecto diferente: Minitel.***

En 1982, en Francia, surge un sistema que es el servicio en línea más exitoso antes del surgimiento de la World Wide Web: Minitel.

Minitel era una terminal tonta, la cual constaba de un teclado (AZERTY), una pantalla y un puerto de comunicaciones (MODEM) conectado a la línea telefónica. La capacidad gráfica de la pantalla era limitada ya que solo podía representar textos y semigráficos, similares al teletexto actual de la televisión. Todo los que los usuarios tenían que hacer era marcar un número en el teclado y seguir las instrucciones.

Desde sus primeros días, los usuarios podían realizar compras en línea, reservas de tren, buscar productos, recibir correo electrónico, y chatear de una manera similar a la que luego fue posible gracias a Internet.

En 1982, el servicio Minitel tuvo un éxito masivo. A partir de 1993 su expansión fue eclipsada por la rápida expansión de Internet. Durante 1995, sin embargo, en Francia existían cerca de 7 millones de terminales operando; este servicio fue dado de baja completamente el 30 de junio de 2012.


Figura 6. Proyecto Minitel

### ***1.13 Apertura del Internet a la sociedad civil.***

Para 1991, la expansión de los servidores y el aumento en la cantidad de hosts en forma exponencial se volvió inminente; no había ya un control como tal de las personas que instalaban un servidor; Internet creció más allá de sus principales raíces de investigación para incluir una amplia comunidad de usuarios y un aumento en las actividades comerciales; no existía una organización que uniformara la cantidad de nuevos protocolos y servicios que se le podrían dar a Internet en un futuro; todo esto, sumado a que ningún gobierno podía tener el control absoluto de Internet y de sus usuarios, y una necesidad reconocida de tener apoyo comunitario en Internet, llevó a la creación de una organización que fuera el centro de cooperación y coordinación global para el desarrollo de protocolos y estándares compatibles. El resultado de esos trabajos, fue la ISOC (Internet Society).

### ***ISOC***

Fue creada por Vinton Cerf, y es una organización no gubernamental sin fines de lucro que se dedica exclusivamente al desarrollo mundial de Internet; promueve el desarrollo abierto, la evolución y el uso de Internet para el beneficio de todas las personas del mundo.

Entre sus principales funciones están: que facilita el desarrollo abierto de normas, protocolos, administración e infraestructura técnicos del Internet, además de que fomenta el entorno de cooperación internacional, comunidad y una cultura que crea un autogobierno que funciona.

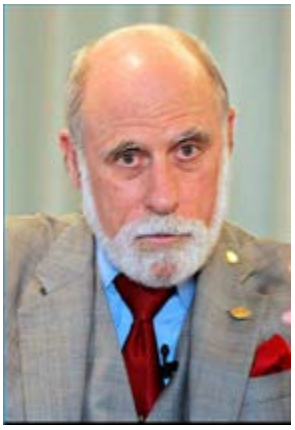


Figura 7. Vinton Cerf, creador de la ISOC.

***NIC (Network Information Center).***

En 1993 el sorprendente crecimiento de la red forzó a IANA (Internet Assigned Numbers Authority) a crear InterNIC, entidad que se hizo cargo de mantener y organizar la creciente demanda por el registro de nombres de dominio. Después de 1995, la fundación nacional de ciencia fue incapaz de continuar subsidiar el proceso de adquisición de dominios pues la red Internet se había vuelto demasiado grande. InterNIC empezó a cobrar 100 dólares por el registro de un dominio por 2 años.

El Network Information Center, es la organización encargada de la administración del nombre de dominio territorial (ccTLD, country code Top Level Domain), como ejemplo se tiene .mx, .us, .ar, etc, que es el código de dos letras asignado a cada país según el ISO 3166. Entre sus funciones están el proveer los servicios de información y registro para esos dominios, así como la asignación de direcciones de IP y el mantenimiento de las bases de datos respectivas a cada recurso.

### *1.14 Primeros navegadores*

Viola, el primer navegador web gráfico, fue el precursor del popular navegador Mosaic que a su vez fue precursor del primer navegador comercial (Netscape).

Netscape fue creado por Pai Wei que apenas era un estudiante de la universidad de California en Berkeley, quien lo público en mayo de 1992. El navegador se construyó sobre el lenguaje Viola que Wei desarrolló para computadoras UNIX. Violawww tenía algunas funciones avanzadas que incluían la habilidad para mostrar gráficos y descargar applets.

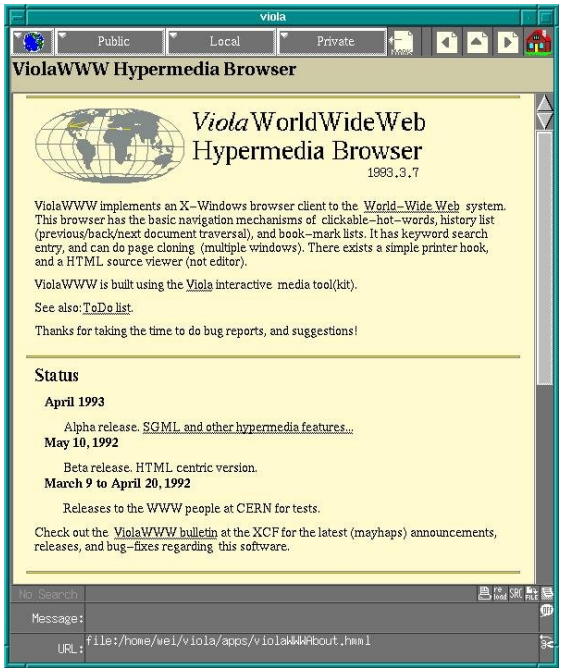



Figura 8. Viola, el primer navegador web gráfico.

## ***Mosaic***

El 22 de abril de 1993 es lanzado el NCSA Mosaic 1.0, creado por Marc Andreessen y Eric Bina quienes más tarde abandonarían este proyecto para dar paso a la creación de Netscape Navigator; fue el primer navegador de Internet en adquirir popularidad entre el público general.

La primera versión funcionaba sobre sistemas Unix, pero fue tal su éxito que en agosto del mismo año se crearon versiones para Windows y Macintosh.


Figura 9. Mosaic, el primer navegador popular entre el público.

***Netscape Navigator***

Fue el navegador más conocido de la primera época de Internet, junto a Internet Explorer. Nació en 1994. Sin casi nadie más que le hiciese frente, Netscape consiguió en sus primeras versiones un éxito rotundo: estaba solo. Incluía el navegador y el programa de correo.

Mientras Microsoft intentaba recuperar el terreno perdido, Nestcape Navigator marcaba el ritmo de cómo había que hacer las webs: qué podían tener, los plug-ins que debían existir y a los que había que adaptarse.

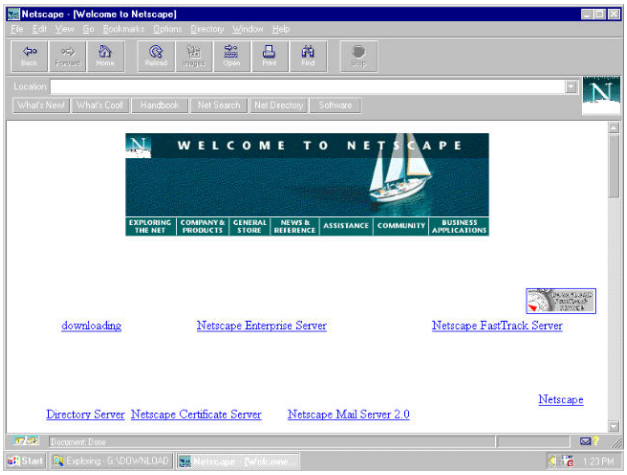



Figura 10. Netscape.

***1.15 SERVICIOS QUE BRINDA INTERNET.***

1995 nace Yahoo.

Yahoo! comenzó como un pasatiempo estudiantil. Los dos fundadores David Filo y Jerry Yang crearon listas de sus sitios preferidos en Internet como pasatiempo, con el tiempo, las listas de Jerry y David se hicieron demasiado largas y difíciles de manejar, y las colocaron en categorías, cuando las categorías eran demasiadas, desarrollaron subcategorías... y el concepto central detrás de Yahoo! nació. El sitio web comenzó como "La Guía de Jerry para la World Wide Web". Poco después este nombre se cambió con ayuda de un diccionario.


Figura 11. Yahoo!

***Ventas por Internet. Amazon.***

Amazon.com cuyo nombre está inspirado en Amazonas.

El primer sitio web de Amazon.com fue inaugurado el 16 de julio de 1995, iniciándose de inmediato un crecimiento exponencial de la compañía y su presencia en la red. Después de 30 días de salir Amazon.com a la red y sin promoción en los medios, Amazon.com estaba vendiendo libros en los 50 estados de EEUU y en 45 países.

En 1996, el sitio web amazon.com tenía más de 2.000 visitantes al día. Un año después los había multiplicado por 25. Justo hace un año, en diciembre de 1999, la revista Time nombró a Jeff Bezos, fundador y director ejecutivo de Amazon, Personaje del Año y le aclamaban como "el rey del cibercomercio".

Figura 12. Amazon

***ebay***

eBay es un sitio web destinado a la subasta de productos a través de Internet. Es uno de los pioneros en este tipo de transacciones, puesto que su presencia en la comunidad online es de varios años.

eBay fue fundada el 3 de septiembre de 1995 por Pierre Omydiar en San Jose, California, y el primer artículo vendido fue un puntero láser inservible, por un precio de 13.83 dólares. Asombrado, Omydiar contactó al ganador de la subasta con el fin de averiguar si realmente éste entendía lo que había comprado. La respuesta fue más asombrosa aún: "Me gusta coleccionar punteros láser inservibles."

Figura 13. eBay.

***Correo electrónico.***

*Hotmail*

En Julio de 1996 es cuando comienza la verdadera historia de Hotmail, en aquella época apareció un servicio de correo en la web llamado HoTMaiL (el nombre es lo único que se tiene de aquella versión, aunque esta ha cambiado y sólo la primera letra es en mayúsculas).


Figura 14. Hotmail.

Como lo indica el sitio web www.outlookiniciar**correo**.com/etiqueta/**jack**-**smith**, aquella versión del visualizador de correo electrónico fue creada y diseñada por Sabeer Bhatia y Jack Smith, el nombre de Hotmail lo eligieron por la unión de Hot y Mail (Hot Mail) y lo que querían dar a entender era un "correo que se utilizaba tanto que está que arde". Y como se puede observar, las letras mayúsculas de esta palabra son HTML que es el protocolo de Internet (HyperText Markup Language)

Este servicio creció rápidamente  y un año después ya contaba con millones de usuarios registrados. A finales del 1997 Microsoft compra la plataforma y cambia su nombre a MSN Hotmail.

***Primeras interacciones sociales. Los "blogs".***

Se sabe que el primer blog, Links.net, fue realizado por un estudiante del Swarthmore College, llamado Justin Hall. En ese momento no era llamado blog, sino que era una página personal.

No fue hasta 1997 cuando el término "weblog" fue acuñado. La creación de la palabra se ha atribuido a Jorn Barger, el término fue creado para reflejar el proceso de "registro de la web" (logging in the web). 1998 marca el primer ejemplo conocido de un blog en un sitio de noticias tradicional cuando Jonathan Dube blogueó "El Huracán Bonnie" para The Charlotte Observer.


Figura 15. Blogger, una de las web de blogs más grandes.

***La evolución de los buscadores; aparece Google.***

Larry y Sergey se dan cuenta de que el motor de búsqueda BackRub necesita un nuevo nombre. Tras una sesión de lluvia de ideas, se deciden por Google, haciendo un juego de palabras con el término matemático "gúgol", cuya pronunciación en inglés es similar a la de "Google" y que se refiere al número uno seguido de 100 ceros. La elección del término se basa en su objetivo de organizar una cantidad aparentemente infinita de información en la Web.


Figura 16. Google, el buscador más importante en la actualidad.

***Banca en línea***

El boom de Internet ocurrido entre fines de 1998 y abril del 2000 llevó a los bancos a incorporar el concepto que se había estado masificando, el Portal Financiero Horizontal. Incluso algunos bancos llevaron más allá sus apuestas, reemplazando o complementando sus marcas para tener una presencia diferenciada en Internet. Existía la creencia de que la agregación de valor podía ser “cualquier cosa” colocada en la Web.


Figura 17. Banca en línea.

***Servicios P2P; Napster.***

Napster, sistema que permite compartir música de forma gratuita a través de la Red fue creado por Shawn Fanning y liberado al mundo de la red en junio de 1999.

La mayor parte de sus usuarios eran jóvenes menores de 25 años que tan sólo tenían que teclear el nombre de la canción que buscaban y recibían la versión digital en el formato denominado MP3.

En el año 2000 Napster tuvo una gran cantidad de usuarios, logrando en tan solo un año 20 millones de usuarios. En ese mismo año, el grupo musical "Metallica" los demanda, y en una respuesta inmediata Napster bloquea a 300,000 usuarios que descargaron música de este grupo musical.

Las demandas siguieron para Napster, y a inicios del 2001, la Corte de Apelaciones los obliga a poner fin al intercambio de canciones con derecho de autor.

Finalmente Napster deja de funcionar y acuerda pagar 26 millones de dólares a las discografías cuando pueda relanzar el servicio como portal de pago.

Figura 18. Napster

***Servicios de mensajería instantánea; ICQ, Messenger.***

ICQ es un juego de palabras, que toma su origen en la pronunciación en ingles de estas tres letras. Su pronunciación literal es aproximadamente “ai si qiu” que suena prácticamente igual que “I seek you” en español “Te busco”, y eso es precisamente lo que hace el programa, busca en Internet a la gente que tú tienes registrada y te permite ponerte en contacto con ellas.

ICQ fue el primer sistema de mensajería instantánea para computadoras con sistema operativo distinto de UNIX/LINUX en noviembre de 1996; ICQ fue lanzado como primer programa de mensajería instantánea por una compañía hasta entonces desconocida, Mirabilis.


Figura 18. ICQ

Enciclopedias on-line: Wikipedia.

Wikipedia es una versión electrónica de las enciclopedias en papel. Los primeros pasos en la utilización de artilugios automáticos que superasen la imprenta como medio más ágil y práctico de acceso a los contenidos enciclopédicos se dan en la década de los años treinta con la novela de ficción de H. G. Wells, El cerebro del Mundo (1937), y la visión futurista Memex, de Vannevar Bush, de utilizar microfilms para almacenar toda la información relevante de una persona (idea expuesta posteriormente en su obra de 1945 As we may think). Otro hito importante fue el proyecto Xanadu (1960) de Ted Nelson.

En enero de 2001, Jimbo Wales, con la ayuda de Larry Sanger, inician el proyecto Wikipedia: una enciclopedia libre y poliglota basada en la colaboración. Toda persona con acceso a Internet puede modificar la gran mayoría de los artículos. Llegará a convertirse en la enciclopedia más gigantesca de la historia. Para mediados de 2008, supera los 10 millones de artículos en más de 250 idiomas. Según su propio sitio web, Wikipedia.org, al 16 de mayo de 2013, más de 37 millones de artículos en 284 idiomas (cantidad que incluye idiomas artificiales como el esperanto, lenguas indígenas o

aborígenes como el náhuatl, el maya y las lenguas de las islas Andamán, o lenguas muertas, como el latín, el chino clásico o el anglosajón).


Figura 20. Wikipedia, la enciclopedia on-line más grande en la actualidad.

### ***1.16 REDES SOCIALES.***

*-Facebook.*

Facebook se creó como una versión en línea de los "facebooks" de las universidades americanas. Los "facebooks" son publicaciones que hacen las universidades al comienzo del año académico, que contienen las fotografías y nombres de todos los estudiantes y que tienen como objetivo ayudar a los estudiantes a conocerse mutuamente. Facebook llevó esta idea a Internet, primero para los estudiantes americanos y abrió sus puertas a cualquier persona que cuente con una cuenta de correo electrónico.

Facebook nació en 2004 como un hobby de Mark Zuckerberg, en aquél momento estudiante de Harvard, y como un servicio para los estudiantes de su universidad.

En su primer mes de funcionamiento Facebook contaba con la suscripción de más de la mitad de los estudiantes de Harvard, y se expandió luego a las universidades MIT, Boston University y Boston College y las más prestigiosas instituciones de Estados Unidos.

En 2006 Facebook se "hizo público" permitiendo que no sólo los estudiantes de determinadas universidades o escuelas americanas participaran en él, sino que todas las personas que tengan correo electrónico puedan formar parte de su comunidad. Facebook se convirtió entonces en una comunidad de comunidades, en él se conectan estudiantes, empresas y gente que puede elegir participar en una o más redes. Es una comunidad creada por y en función de sus miembros.

*-Twitter.*

Twitter es un servicio gratuito de microblogging, que hace las veces de red social y que permite a sus usuarios enviar micro-entradas basadas en texto, denominadas "tweets", de una longitud máxima de 140 caracteres.

Twitter nació en el año 2006, una serie de jóvenes emprendedores que trabajaban para la compañía de Podcasts Odeo, Inc., de San Francisco, Estados Unidos, se vieron inmersos en un día completo de lluvia de ideas.

Una vez iniciado el proyecto probaron varios nombres. El nombre original durante un tiempo fue "Status" (Stat.us), pasando por twitch (tic) a causa del tipo de vibraciones de los móviles, pero se quedaron con Twitter. Que en palabras de Dorsey era perfecta, y la definición era "una corta ráfaga de información intrascendente", el "pio de un pájaro", que en inglés es twitt. Si recibes muchos mensajes, estás "twitterpated".

*-Youtube.*

YouTube, es un sitio web que permite a los usuarios subir, bajar, ver y compartir vídeos. Fundado en febrero de 2005 por 3 ex-empleados de PayPal: (Chad Hurley, Steve Chen y Jaweb Karim).

La corta historia de YouTube registra el mayor crecimiento exponencial que se recuerde. Chad Hurley pagó con su tarjeta de crédito la primera factura por la conexión de banda ancha que necesitaba para lanzar su web de vídeos online. La facilidad para alojar videos personales de hasta 10 minutos de duración lo hacen extremadamente popular y a veces, polémico. Desde entonces, la demanda ha sido tan explosiva (100 millones de visitas mensuales) que el costo de infraestructura ha subido a dos millones de dólares por mes.


Figura 21. Interacción de las redes sociales con otras redes.

## ***1.17 VENTAJAS Y DESVENTAJAS DE INTERNET.***

A continuación, la tabla 3 muestra una comparativa acerca de las principales ventajas de Internet, y las consecuentes desventajas que el incorrecto uso de éste conlleva.

| **VENTAJAS DE INTERNET** | **DESVENTAJAS DE INTERNET** |
|---|---|
| **Fácil acceso a información de todo tipo, de forma libre y gratuita.** | Fácil acceso a servicios de dudosa calidad educativa, ética y/o moral. |
| **Acceso anónimo a la información y a determinados servicios, que aumenta la sensación de libertad y autonomía completa.** | Fácil establecimiento de relaciones interpersonales en las que se omite o falsea la auténtica personalidad aprovechando el anonimato. |
| **Conexiones prolongadas con un costo muy reducido.** | Hay una posibilidad de que nos volvamos dependientes de Internet, es decir, que nos veamos obligados a entrar muy seguido para ver actualizaciones de algún tema en especial, por ejemplo, saber si alguien nos " twitteó" en la red social Twitter. |
| **Fácil y rápida transmisión de la información aprovechando la infraestructura de comunicaciones proporcionada por Internet.** | Internet puede resultar muy inseguro ya que nos pueden robar datos en la nube, por ejemplo cuando utilizamos Facebook sin privacidad, o cuando alguien se infiltra en nuestra computadora. Esta es quizá la peor desventaja. |
| **Fácil intercambio de información entre usuarios, a menudo desconocidos.** | Hay mucha gente que coloca información falsa en Internet para confundir a los lectores. Hay que tener cuidado e investigar si la fuente es confiable. |
| **Es la fuente de contenidos más grande de todo el mundo. En Internet hay muchísima información** | Fácil acceso a páginas web con contenido ilegal, tan solo buscando en la Deep Web |
| **Se puede estar en contacto con las personas todo el tiempo; esto facilita el proceso de socialización a través del uso de servicios como son los chats, juegos en red, participación en ciertas redes sociales, etcétera.** | Se puede ser víctima de un fraude de una manera muy sencilla, al desconocer la identidad de algún comprador, o si se es víctima de un ataque cibernético |
| **Facilita el acceso a la ciencia, cultura y ocio favoreciendo y completando así la educación fuera del ámbito de la escuela.** | Las personas empiezan a pensar más superficialmente cuando leen algo en Internet, porque no se concentran en lo que están leyendo. Simplemente leen ideas básicas o principales y no se enfocan en estudiar más lo leído porque con ello ya están satisfechos. |
| **Mejora los resultados académicos, según muestran estadísticas realizadas sobre estos temas.** | En Internet hay que tener cuidado con las Páginas Web en las que entramos porque puede haber malware que se dirija a las computadoras. |
| **Internet ofrece la posibilidad de ganar dinero Online. Mucha gente se pregunta si esto es posible.** | En Internet hay muchísimo uso del spam, y esto puede generar inconvenientes utilizando la web, porque por ejemplo aquel usuario puede hacer clic en alguna ventana emergente y le puede infectar la computadora con malware. |

Tabla 3. Ventajas y desventajas del uso de Internet.

### ***1.18 INTERNET 2.0.***

Desde octubre de 1996 34 universidades de los Estados Unidos se reunieron para definir los objetivos de Internet2, trataba de una red de alta velocidad y centrada en la comunicación académica. Para el 2006 esta red ya contaba con 200 universidades y medio centenar de empresas de tecnología.

Con el término Web 2.0, Internet abandona la marcada unidireccionalidad y se orienta más a facilitar la máxima interacción entre los usuarios y el desarrollo de redes sociales (tecnologías sociales) donde puedan expresarse y opinar, buscar y recibir información de interés, colaborar y crear conocimiento (conocimiento social), compartir contenidos, etc. Algunos ejemplos son:

Aplicaciones para expresarse/crear y publicar/difundir: blog, wiki...

Aplicaciones para publicar/difundir y buscar información: podcast, YouTube, Flickr, SlideShare…

Redes sociales: Facebook, Twitter...

Otras aplicaciones on-line.

El termino Web 2.0 (2004-presente) está comúnmente asociado con un fenómeno social, basado en la interacción que se logra a partir de diferentes aplicaciones web, que facilitan el compartir información, la interoperabilidad, el diseño centrado en el usuario y la colaboración en la World Wide Web ...es.wikipedia.org/wiki/Web_2.0

La web 2.0 proporciona soluciones tecnológicas altamente complejas para facilitar sencillez y facilidad de uso a los usuarios. Esto permite abrir unas perspectivas extraordinariamente interesantes para la educación. No obstante urge convertir estas potencialidades en el terreno educativo. Surgen cuestiones que van desde la nueva psicología y pedagogía educativa hasta la propia validación del conocimiento que se deriva de este modelo.

### ***1.19 VIRUS INFORMÁTICOS***

Un virus informático es un programa que es capaz de «infectar» otros programas para que incluyan una copia de sí mismo. Así pues, es un programa como cualquier otro, con la peculiaridad de que consigue reproducir su código cuando se ejecuta un programa infectado. El nombre de virus se debe a su parecido con los virus biológicos, pues se introducen en la computadora (cuerpo humano), infectan los programas y archivos (las células) y se reproducen, propagando la infección por el propio sistema, y contagiando a otros sistemas que tengan contacto con el original. El primero en haberlos llamado virus fue Len Adleman.

#### ***Historia***

Su origen se remonta a 1959, en los laboratorios de la BELL Computer, subsidiaria de AT&T, en Nueva Jersey, donde se inventó un juego que se denominó Core Wars, inspirado en las teorías sobre programas con capacidad de autorreplicación de Von Neuman. El fundamento de este juego consistía en que dos programadores desarrollaban dos programas, que compartían un espacio de

memoria común, de modo que los programas pudiesen reproducirse dentro de este ecosistema digital e ir «conquistando» zonas de memoria. Ganaba el programador del virus que hubiese consumido más espacio de memoria o hubiese conseguido aniquilar al contrario.

El desarrollo de los códigos malignos ha evolucionado desde simples intentos de demostración de conocimiento informático, por parte de programadores individuales hasta formar verdaderos negocios, con jugosas ganancias llevados a cabo por mafias con objetivos precisos.

A comienzos de 1984, la revista Scientific American, publicó la información completa sobre esos programas, con guías para la creación de virus. Es el punto de partida de la vida pública de estos programas, y naturalmente de su difusión sin control en las computadoras personales.

Por esa misma fecha, 1984, el Dr. Fred Cohen, en su tesis para Doctor en Ingeniería Eléctrica, presentada en la Universidad del Sur de California, hace una demostración de cómo se podía crear un virus y presentó un virus informático residente en una computadora. Al Dr. Cohen se le conoce hoy como "el padre de los virus". Cohen es reconocido como el primero en definir los virus informáticos: "Se denomina virus informático a todo programa capaz de infectar a otros programas, a partir de su modificación para introducirse en ellos".

Con posterioridad, los virus se multiplicaron con gran rapidez. Cada día creció el número de virus existentes y hoy son tantos que es imposible registrarlos todos. Aunque cientos de ellos son prácticamente desconocidos, otros gozan de gran popularidad, debido a su extensión y daños causados.

***Primer ataque cibernético.***

El primer virus reconocido como tal, atacó a una máquina IBM Serie 360. Fue llamado Creeper, creado en 1972. Este programa emitía periódicamente en la pantalla el mensaje: «I'm a creeper... catch me if you can!» (¡Soy una enredadera... agárrame si puedes!). Para eliminar este problema se creó el primer programa antivirus denominado Reaper (cortadora).

http://www.tudiscovery.com/Internet/nace-arpa-el-abuelo-de-Internet.shtml

***Los 10 virus de mayor impacto en la historia.***

La tabla número 4, muestra los 10 virus que son considerados los de mayor impacto en la historia de la informática.

| ***NOMBRE*** | ***AÑO*** | ***DESCRIPCIÓN*** |
|---|---|---|
| **1.Flame** | 2012 | Tenía por objetivo conseguir datos desde Irán, el Líbano, Siria, Sudán y otros países de Medio Oriente y el Norte de África. Con capacidad de propagarse a través de la red de área local LAN o mediante memorias USB, y una vez dentro podía grabar audio, capturas de pantalla, |

| | | |
|---|---|---|
| | | pulsaciones de teclado, tráfico de red, grabar conversaciones de Skype y controlar Bluetooth para obtener información. |
| **2.Stuxnet** | 2007 | Gusano informático que apunta a los sistemas industriales de control que se utilizan para controlar instalaciones industriales como plantas de energía eléctrica, represas, sistemas de procesamiento de desechos, entre otras operaciones industriales. |
| **3.Duqu** | 2011 | Su finalidad era actuar como backdoor para facilitar el robo de información privada. Expertos en seguridad han captado más de una docena de incidentes que involucran a Duqu, y la gran mayoría de las víctimas están localizadas en Irán.<br><br>Un análisis de sus actividades muestra que el principal objetivo de los ataques era robar información sobre los sistemas de control utilizados en varias industrias, así como la recopilación de información acerca de las relaciones comerciales de una amplia gama de organizaciones iraníes |
| **4.I love you** | 2000 | Afectó de forma masiva a miles de computadoras y sistemas de todo el mundo. Y marcó un antes y un después en la seguridad informática. Causó la primera infección masiva a nivel mundial, y marcaría la manera de actuar posterior para los creadores de 'malware', así como su profesionalización. Se trataba de un correo electrónico cuyo gancho era su título, 'I Love You', así como el nombre del documento de texto asociado a él 'Love-Letter-For-You.txt.vbs'. Al ejecutar el archivo, el gusano modificaba los archivos de la computadora infectada y se auto enviaba por correo electrónico a todas las direcciones de la víctima. Afectó a cerca de 50 millones de computadoras en todo el planeta una semana después de su aparición, es decir, el 10% de las máquinas conectadas a la Red de redes, provocando pérdidas de más de 5,500 millones de dólares. |
| **5.Melissa** | 1999 | Infectó alrededor de 1 millón de computadoras y causó daños valorados en más de 80 millones de dólares. Se propagó globalmente horas después de ser descubierto y lo hizo más rápidamente que cualquier virus anterior. El funcionamiento de Melissa produjo una caída masiva de los sistemas de correo electrónico a lo largo de Internet (Microsoft llegó a cerrar todo el sistema de correo electrónico para evitar propagarlo). |
| **6.Chernobyl** | 1999 | Es un virus residente que se activa cada 26 de abril. Borra todo el contenido del disco duro e impide el arranque de computadoras con Windows NT, Windows 98 o Windows 95. También infecta archivos con extensión EXE, aunque sólo en computadoras con Windows 98 y |

| | | |
|---|---|---|
| | | Windows 95. Además, en el caso de equipos con microprocesador Pentium de Intel, borra el contenido de la BIOS. |
| **7.DNS Changer** | 2007 | Se trata de un troyano que modifica la configuración DNS para que los equipos afectados utilicen servidores DNS no legítimos y controlados por un atacante. A partir de ahí, intenta acceder al router al que está conectado el equipo utilizando las credenciales por defecto. Si consigue el acceso, cambia los servidores DNS utilizados por el mismo por los servidores DNS no legítimos. El FBI tuvo que apropiarse de todos los servidores DNS que fueron utilizados por este troyano. Dichos servidores fueron deshabilitados el día 8 de marzo de 2012. |
| **8.Conficker** | 2008 | Es un gusano que permite ejecutar remotamente código arbitrario. Si la fecha del sistema es mayor que el 1 de enero de 2009, intenta conectarse a cierta página web para descargar y ejecutar otro tipo de malware en el equipo afectado. |
| **9.Zafiro** | 2003 | Se demoró apenas 10 minutos en recorrer el globo convirtiéndose en el virus informático que más rápido se ha propagado por la Red hasta ahora. Casi impidió el acceso a la Red en Corea del Sur y paralizó algunos cajeros automáticos de Estados Unidos, duplicó el número de computadoras infectadas cada 8,5 segundos en el primer minuto de su aparición. |
| **10.Storm** | 2007 | Provoca ataques zombis, que son ataques realizados con máquinas infectadas por un troyano, contra el sitio de Microsoft. Infecta sistemas que ejecutan Internet Information Server 4 y 5 (IIS) vulnerables. Se copiará a cada máquina encontrada en esas condiciones, cada una de las cuáles ejecutarán entonces automáticamente el gusano, repitiendo el ciclo. cada uno de estos sistemas infectados también se convierte en zombis, todos ellos programados para lanzar ataques de negación de servicio contra el dominio de Microsoft |

Tabla 4. Top-10 de los virus más significativos en la historia de la informática.

# *2. DELITOS CONTRA SISTEMAS INFORMÁTICOS*

La gran y compleja herramienta de la que se trata el Internet, ha sido usada para educación a distancia, para telemedicina, y para un sinfín de actos de ayuda a personas en sitios remotos, pero como muchas herramientas ésta es usada para provocar daños a terceros.

En este capítulo, se muestra como el Internet y las computadoras se pueden usar para robo de información, suplantación de identidad y una gran cantidad de ataques informáticos que afectan a personas y empresas en general.

Esta parte tiene un enfoque en su mayoría técnico ya que se llegan a detallar la estructura, los conceptos y los procesos mediante los cuales se puede llevar a cabo un ataque, así como algunos métodos con los cuales se puede hacer frente a estos.

El ciberdelito, es el término que se utiliza para describir al crimen genérico o crimen electrónico, que agobia con operaciones ilícitas realizadas por medio de Internet o que tienen como objetivo destruir y dañar computadoras, medios electrónicos y redes de Internet. Sin embargo, las categorías que definen un delito informático son aún mayores y complejas y pueden incluir delitos tradicionales como el fraude, el robo, chantaje, falsificación y la malversación de caudales públicos, en los cuales computadoras y redes han sido utilizados.

## ***2.1 Hacker.***

El término “hacker” suele ir acompañado por un aura de misterio, desde el genio informático, hasta el perverso creador de virus.

Actualmente suelen confundirse los términos hacker y cracker; antes de iniciar este capítulo donde se explicarán los detalles técnicos de los diversos ataques informáticos, se hará una breve distinción entre estos dos términos.

Se puede entender por hacker a:

- Gente apasionada por la seguridad informática.
- Una comunidad de entusiastas programadores y diseñadores de sistemas originada en los sesenta alrededor del Instituto Tecnológico de Massachusetts (MIT), el Tech Model Railroad Club (TMRC) y el Laboratorio de Inteligencia Artificial del MIT. Esta comunidad se caracteriza por el lanzamiento del movimiento de software libre. La World Wide Web e Internet en sí misma son creaciones de hackers.
- Según el RFC 1392: "persona que se disfruta de un conocimiento profundo del funcionamiento interno de un sistema, en particular de computadoras y redes informáticas"
- En la actualidad se usa de forma corriente para referirse mayormente a los criminales informáticos.

Los hackers del software libre consideran la referencia a intrusión informática como un uso incorrecto de la palabra, y se refieren a los que rompen los sistemas de seguridad como "crackers" (analogía de "safecracker", que en español se traduce como "un ladrón de cajas fuertes").

**White hat y black hat**

Un hacker de sombrero blanco se refiere a un hacker ético que se centra en asegurar y proteger los sistemas de Tecnologías de información y comunicación.

Por el contrario, un hacker de sombrero negro es el villano, también conocidos como "crackers" muestran sus habilidades en informática rompiendo sistemas de seguridad de computadoras, colapsando servidores, entrando a zonas restringidas, infectando redes o apoderándose de ellas, entre otras muchas cosas utilizando sus destrezas en métodos hacking.

**Wannabe**

Generalmente son aquellos a los que les interesa el tema de hacking y/o phreaking pero que por estar empezando no son reconocidos por la elite.

**Lammer o script-kiddie**

Es un término para una persona falta de habilidades técnicas, generalmente no competente en la materia, que pretende obtener beneficio del hacking sin tener los conocimientos necesarios.

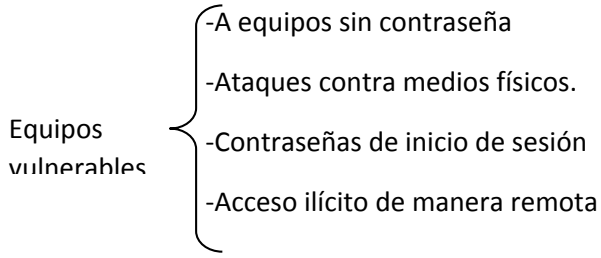
**Newbie**

Newbie es un término utilizado comúnmente para describir a un novato, en esta área, es el que no posee muchos conocimientos en el tema.

### ***2.2 Acceso ilícito a sistemas privados***

Se define como el acceso a un equipo computacional, a un equipo de red, o incluso a un teléfono inteligente, sin el consentimiento del dueño. Su complejidad varía ya que puede ir desde entrar a la pc de un compañero de oficina sin su consentimiento, hasta la invasión de un servidor web en el otro lado del mundo. Este tipo de delito es muy común, debido a su complejidad variable ya que va desde lo muy fácil, como acceso a una cuenta sin contraseña, pasando por el uso de software especializado de fácil manipulación para romper medidas de seguridad en los sistemas, hasta ataques complejos a sistemas remotos que en muchas ocasiones debido a su dificultad se llevan a cabo por grupos de crackers experimentados.

### ***2.2.1 Descripción de los ataques más comunes***




### ***2.2.2 Ataque a equipos sin contraseña.***

El acceso ilícito más sencillo a un equipo es simplemente cuando éste ***carece de alguna contraseña***; esto se puede lograr encendiendo el equipo, o haciendo uso de éste cuando está encendido, y el usuario de éste se ha apartado por algún motivo. De igual modo se puede tener la desventaja de que el equipo haya sido robado o extraviado, y jamás se hayan tomado las medidas de seguridad adecuadas para el resguardo de la información.

De aquí se pueden derivar otros delitos como lo son: espionaje de datos, intervención y manipulación de información confidencial, entre otros, los cuales se describirán más tarde.

### ***2.2.3 Medios físicos. Usuarios malintencionados.***

Los 2 aspectos más importantes que se deben de tener en cuenta son: el lugar en que se encuentra ubicado el servidor y las personas que tienen acceso físico al mismo. Los especialistas en seguridad llevan mucho tiempo sosteniendo que si usuarios malintencionados tienen acceso físico, los controles de seguridad son inútiles y dicha afirmación es totalmente cierta. Salvo raras excepciones, casi todos los sistemas de computación son vulnerables a ataques *in situ.*

Como lo explica Michel Ruiz Tejeda en su manual de Administración de Servidores Linux, un ataque puede significar muchas cosas en este contexto. "*Por ejemplo, imagine que ha dejado a algún usuario malintencionado sólo con sus servidores durante 10 segundos, es muy probable que estos sufran daños importantes en ese intervalo de tiempo. El usuario podría realizar un rudimentario ataque de denegación de servicio desconectando cables, desconectando hardware de red o reiniciando los servidores.*

*La mayor preocupación deben de ser los usuarios locales autorizados, aquellos que solo tienen al menos autorización limitada para acceder al sistema. Se ha estimado que el 80% de las intrusiones provienen del personal interno. El motivo es que este personal tiene acceso a información que los agresores remotos a menudo no pueden obtener".*

Otra de las ventajas que tiene el personal interno es la confianza. Los empleados de confianza, deambulan libremente sin temor a que les hagan preguntas. Después de todo, se supone que están en su sitio y a nadie se le ocurre cuestionar su presencia, a menos que entren en un área restringida.

***Defensa.***

**Centro de operaciones de red (NOC)**

Un NOC es un área restringida en la que se encuentran los servidores. Éstos suelen estar asegurados por pernos, fijados a bastidores o asegurados de alguna otra manera, junto con el hardware de red esencial.

Idealmente un NOC debería de ser una oficina independiente, a la que tuviesen acceso muy pocas personas. Aquellas personas que estén autorizadas deberían tener claves. (Un buen método es el uso de tarjetas de acceso que incluso restrinjan el acceso de los usuarios autorizados a ciertas horas del día). Por último, merece la pena llevar un registro escrito de acceso y ordenar que incluso el personal autorizado firme al entrar y salir.

También, se debe de asegurar que el NOC cumpla con los siguientes requisitos:

- Debe encontrarse dentro de otro espacio de la oficina y alejado del público; es preferible que no se encuentre en la planta baja.
- La sala y los pasillos que conducen a ella deben ser totalmente opacos: sin puertas de cristal.
- Las puertas de acceso deben tener un blindaje que incluya el cerco de la puerta. Esto evita que los intrusos fuercen la cerradura.
- Si se emplea vigilancia (circuito cerrado de TV o imágenes instantáneas secuenciales), dirija la señal desde la cámara a un VCR (video cassette recorder) remoto. Esto le garantiza que aunque los atacantes dañen el equipo y se lleven la cinta, seguirá teniendo pruebas.
- Mantenga todos los dispositivos de almacenamiento en un lugar seguro, o aún mejor, en un lugar distinto.

Además, hay que promulgar estrictas normas escritas que prohíban al usuario medio entrar al NOC. Dichas normas deberían incluirse como clausulas en los contratos de trabajo. De esta forma, todos los empleados las conocerán y sabrán que si las violan pueden enfrentarse a un despido.

### *2.2.4 Ruptura de contraseñas en los medios físicos.*

La mayoría de las arquitecturas (como x86, PPC o Sparc) utilizan contraseñas de BIOS-PROM (basic input/output system – programable read-only memory), contraseñas de consola, o ambas. Los fabricantes de hardware incluyen estos sistemas de contraseñas como una capa extra de seguridad, un obstáculo para disuadir a los usuarios esporádicos de “fisgonear”.

Uno de los métodos más comunes de protección de la información que existe en una computadora, es configurarle una contraseña al disco duro del equipo; así, al encender la computadora, el sistema básico de inicio requerirá de una contraseña para poder pasar a la ejecución del sistema operativo instalado.

Las contraseñas de BIOS o de la PROM evitan que los usuarios malintencionados accedan a la configuración del sistema, mientras que las contraseñas de consola suelen proteger los perfiles de

usuario de la estación de trabajo. En cualquier caso, estos sistemas de contraseñas son parcialmente efectivos y es conveniente usarlos siempre que sea posible.

Actualmente las teclas y contraseñas predeterminadas de configuración de la BIOS de casi todos los fabricantes son muy conocidas, por lo cual deben cambiarse al configurar el sistema. Se debe de asegurar que la contraseña no coincida con otras que utilice la red, lo que garantiza que si rompen la contraseña de la BIOS o de la consola, las aplicaciones o las restantes maquinas no estarán expuestas a ningún ataque.

Lo más recomendables es no fiarse de las contraseñas de las BIOS ni de la consola como una línea seria de defensa, ya que tienen defectos inherentes. Uno de ellos es que los agresores pueden anular las contraseñas de la BIOS con solo provocar un cortocircuito en la batería de la CMOS. En otros casos, ni siquiera necesitan hacerlo, ya que el fabricante de la placa base incluye un "jumper" que, colocado en el modo adecuado, borrará la CMOS.

Más aun, los agresores van armados frecuentemente con barrenadores de BIOS (programas que borran los ajustes de la BIOS), o con utilidades de captura de contraseña de BIOS. Algunas de esas herramientas se mencionan en la tabla número 5:

### *2.2.5 Utilidades de captura y barrenadores de BIOS.*

| ***HERRAMIENTAS*** | ***DESCRIPCIÓN*** |
|---|---|
| ¡BIOS de Bluefish | Este paquete es un conjunto de herramientas de propósito general para atacar a la BIOS que incluye barrenadores, utilidades de captura y herramientas de descifrado. ¡BIOS superará con facilidad la mayoría de las protecciones de contraseña de BIOS modernas. |
| AMIDECODE | Esta utilidad decodificará las contraseñas de la BIOS de los sistemas de American Megatrends. |
| AMI Password Viewer | Esta utilidad de KORT lee, descifra y muestra las contraseñas de la BIOS de AMI. |
| AW.COM | Esta utilidad de Falcon and Alex rompe las contraseñas de la BIOS de Award. |

Tabla 5. Utilidades para vulnerar el BIOS.

### ***2.2.6 Contraseñas de inicio de sesión.***

Superando ya los bloqueos de la BIOS, si es que en algún momento el usuario los configuró, el paso siguiente es romper la contraseña de inicio de sesión, dependiendo del sistema operativo que se esté utilizando.

Una de las formas más comunes de acceso a los sistemas sin conocer la contraseña, es mediante el uso de software especializado en la materia. ERD Commander, Hirens boot, Ophcrack, o simplemente el disco de instalación del sistema operativo bastarán para poder iniciar una sesión.

Comúnmente, estos programas operan cambiando la contraseña, dado que el software conocido para estos fines no puede desencriptar la contraseña del usuario.

Por ejemplo, el ERD Commander es una herramienta de reparación y recuperación que soluciona aquellos problemas que impiden a Windows arrancar, y restaura el sistema sin pérdida de datos críticos, pero entre sus funciones restablece contraseñas de usuarios del sistema operativo.

Al contar con estas características, el atacante no se arriesgará a dañar la información a la cual quiera tener acceso, y únicamente necesitará hacer del programa ERD Commander un programa "booteable".

Otra forma de vulnerar la contraseña de un usuario en el sistema operativo de Windows, es la que se describe a continuación:

1.- Ejecutar un live cd de un sistema operativo Linux.

2.- Entrar en el Shell y verificar cual es el disco y la partición que contiene el sistema operativo Windows (puede ser incluso Windows server) y montarla.

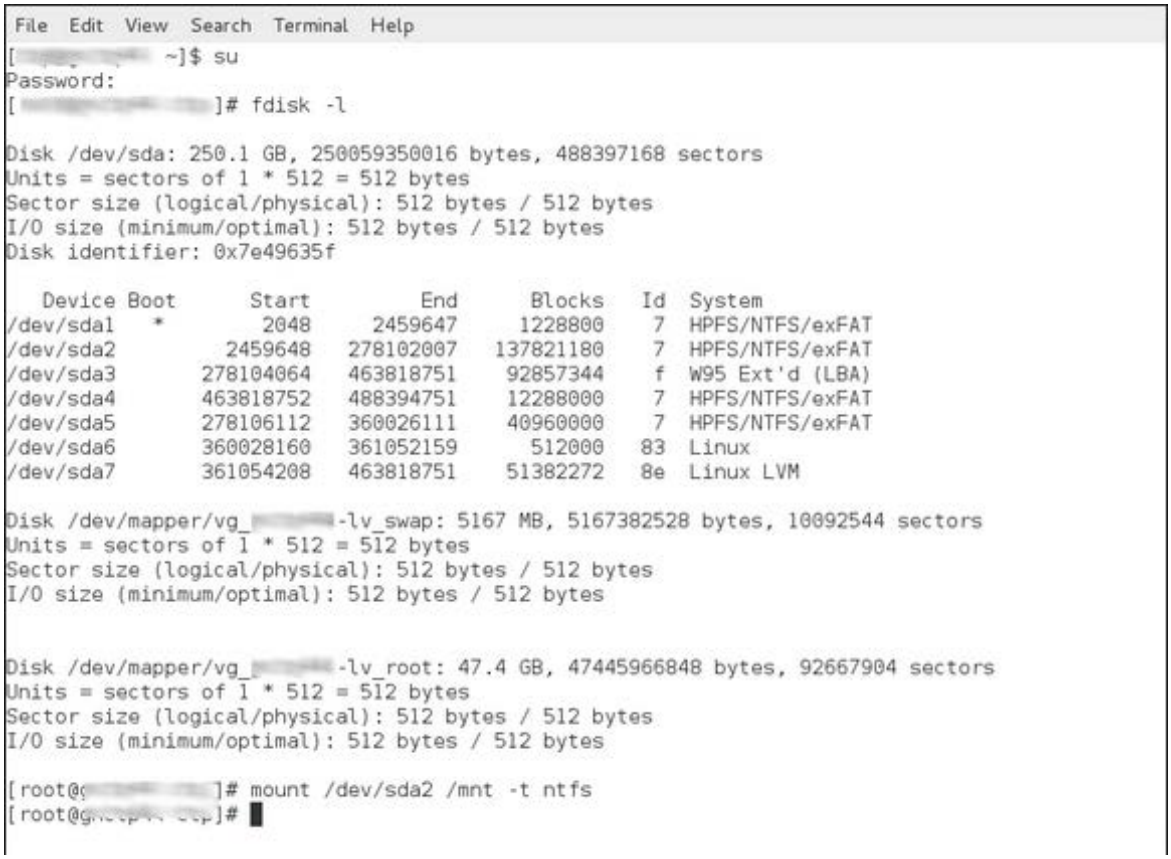



Figura 22. Shell en Debian, mostrando verificación de discos.

3.- Localizar la carpeta principal del sistema operativo, la cual es system32:

cd windows\system32

4.- Se debe ejecutar el siguiente comando:

copy cmd.exe sethc.exe

5.- Reiniciar el equipo.

Después de que ha reiniciado, presionar 5 veces shift; en la ventana que aparece escribir: control userpasswords2, y escribir la nueva contraseña.

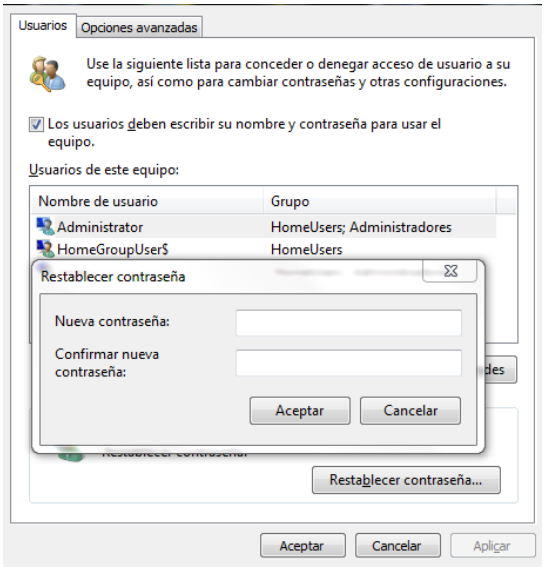



Figura 23. Ventana en Windows para cambiar contraseña.

Sí el método anterior no permite que se cambie la contraseña en la terminal en vez de escribir control userpasswords2 se deberá escribir net user:

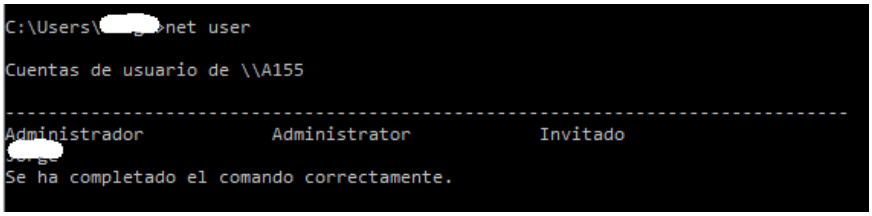



Figura 24. Cmd de Windows, comando net user.

Y una vez que se tiene el usuario objetivo se procede a escribir: net user usuario *

Donde * es para indicar que se quiere introducir una nueva contraseña

Para sistemas operativos diferentes, como Linux, también se puede usar un Live CD Linux y lo que se hace es lo siguiente:

1. Iniciar con el LiveCD

2. Abrir una consola

3. Montar la unidad principal de nuestro Linux (por ejemplo, /dev/sda5 , una ruta común de la unidad principal): sudo mount /dev/sda5

4. Hacer un chroot (cambia la raíz del sistema de archivos) en /mnt: sudo chroot /mnt

5. Cambiar la contraseña: passwd

6. Reiniciar el equipo: exit → sudo reboot

Bastará con reiniciar la computadora, introducir la contraseña nueva, y el acceso a este sistema operativo está garantizado.

Todos estos procesos son los más conocidos para romper la contraseña en la mayoría de los sistemas operativos; sin embargo, atacantes con mucha más experiencia podrán hacer este proceso mediante otras técnicas que suelen ser mucho más avanzadas que las anteriormente descritas.

Este proceso de romper contraseñas de inicio de sesión no es exclusivo de computadoras; con el avance de las tecnologías de la información, los teléfonos inteligentes han tomado una relevancia mucho mayor, que incluso los mismos equipos de cómputo; casi todos estos teléfonos tienen la opción de activar una contraseña, que impida que una persona ajena a la propietaria del teléfono acceda a información (que suele ser de una confidencialidad mayor que la almacenada en las PC´s.)

Sin embargo, aunque en mucho menor medida, existen formas de romper estas contraseñas y tener acceso a toda la información que se encuentre en el teléfono inteligente; en este caso, no es con cualquier programa que se distribuya de forma comercial o libre, puesto que los que existen de este tipo eliminan toda la información que se encuentra en el teléfono, cosa que por supuesto el atacante no desea.

Uno de los métodos efectivos para romper las contraseñas, en este caso para teléfonos con sistema operativo Android, es el que se describe a continuación:

1. Instalar el SDK (kit de desarrollo de software) de Android.
2. Configurar el path del SDK.

   Para trabajar cómodamente con los comandos que nos proporciona el SDK, ejecutaremos el siguiente comando (reemplazando la ruta del SDK por la que se tenga):

   Echo "export PATH=$PATH:/ruta/del/sdk/tools"

   source ~/.bashrc

3. Instalar la máquina virtual de Java.
4. Crear una regla en udev.

Debemos ahora crear una regla en udev para que al momento de conectar el dispositivo lo podamos usar con el SDK de Android. Así que creamos y editamos como root el archivo /etc/udev/rules.d/99-android.rules y dentro ponemos:

SUBSYSTEM=="usb", ATTRS{idVendor}=="El del teléfono", SYMLINK+="android_adb", MODE="0666"

5. Conectarse al dispositivo

Se conecta el smartphone y se selecciona la opción HTC Syn obteniendo un error que dice que no encontró el HTC Sync en el PC, con esto se activa el modo depuración del USB, el cual permitirá conectarse desde la terminal de Linux. Se debe comprobar si se reconoce el dispositivo ejecutando:

adb devices:

* daemon not running. starting it now *
* daemon started successfully *
List of devices attached
HT9A3LG11652 device

HT9A3LG11652 es el nombre del dispositivo en este caso; que nos permitirá referenciarlo al momento de ejecutar comandos sobre él desde CLI de Linux.

Una vez que se tiene el acceso podemos ejecutar entre otras:

adb -s HT9A3LG11652 shell #ejecutar una shell

adb -s HT9A3LG11652 push archivo_local archivo_destino #copiar un archivo al smartphone

adb -s HT9A3LG11652 pull archivo_remoto archivo_local #copiar un archivo desde el smartphone

adb -s HT9A3LG11652 shell rm -r /system/sd/archivo #borrar archivos del smartphone

adb -s HT9A3LG11652 install nombre_aplicacion.apk #instalar aplicaciones

adb -s HT9A3LG11652 uninstall nombre.paquete #desinstalar aplicaciones

Aquí se tiene acceso al teléfono.

Con la utilización del comando chmod se podrían agregar o quitar permisos a archivos y carpetas del teléfono, lo cual lograría evitar el uso de contraseña y así poder desconectar el teléfono de la computadora y tener acceso a este de un modo más cómodo.

Este método es muy largo; si se desea aplicar cuando el dueño de un teléfono se ha distraído se debe de contar con mucha experiencia y con todas las herramientas preparadas.

En cambio, si el teléfono fuera robado y se quisiera tener acceso a los datos contenidos en éste, es un método que se puede hacer de manera segura.

Este método se puede aplicar a otro tipo de Smartphone, considerando que se deben de hacer algunos cambios, dependiendo del sistema operativo en cuestión; el resultado sería muy similar.

### ***2.2.7. Acceso ilícito de manera remota.***

***Ataques remotos más comunes***

- -Ataques contra módems caseros
- -XSS
- -inyección SQL
- -Exploits
- -Troyanos

Otro tipo muy común de acceso ilícito a la información, es hacerlo de manera remota, esto es, que no es necesario estar manipulando la información desde el equipo que será víctima de este acceso; cualquier usuario desde cualquier parte puede realizar este tipo de ataques.

El objetivo sigue siendo el mismo: tener acceso a cuentas de usuario sin la autorización de éste, ya sea de inicio de sesión en un sistema operativo, o de cualquier otro de cuenta, como lo pueden ser de correo electrónico, de alguna red social, entre otros.

Actualmente la tecnología inalámbrica crece cada día, siendo de gran ayuda para trabajar de manera más cómoda o más eficiente. Se puede conectar con un teléfono a una red inalámbrica y poder trabajar desde este, por desgracia trae consigo algunas desventajas en cuanto a la parte de la seguridad.

En México, uno de los principales proveedores de Internet es Telmex, seguido por Cablevisión, los cuales brindan el equipo algunas veces pre-configurado para que el usuario estándar llegue y conecte este a la corriente y a la red telefónica y listo, se tiene Internet, pero uno de los descuidos que se ha vendió teniendo con esta práctica es que las claves para el acceso a la red tienen un sistema de cifrado WEP (Wired Equivalent Privacy, privacidad equivalente a cableado) el cual en muchos foros de Internet hablan sobre el modo de crackearlo, y además en muchos lados se proporcionan las herramientas para que de una manera muy sencilla se obtenga el acceso a éste; incluso existen herramientas para que se obtenga el mismo resultado desde un teléfono inteligente.

Cualquier usuario malintencionado que pueda tener acceso a la red que otros pagan, y que incluso pueda modificar la configuración de este y dejar fuera de la propia red es un problema muy grande, dada la facilidad con la que se “truenan” los cifrados WEP; si el problema quedará ahí, se podría resetear el modem, pedir un poco de asesoría y aumentar la seguridad para tratar de evitar que esto volviera a suceder, pero en ocasiones los atacantes pueden llevar a cabo acciones que podrían

repercutir de maneras grave en los trabajos, escuelas o cualquier otro aspecto de la vida sin que el usuario se dé cuenta.

Una de las formas comunes de atacar este problema, es cambiar el cifrado por uno que no sea tan inseguro, como lo es el WPA, WPA2, WPA2-PSK, los cuales son mucho más difíciles de crackear, ya que se necesitan más recursos y muchas herramientas. No es imposible, pero si mucho más complicado.

Para ataques que tienen como objetivo principal algún sitio web, o bases de datos, existen 2 métodos que son los más populares entre los atacantes, los cuales son: ataque de Cross-Site Scripting (XSS), y el ataque por inyección de código SQL.

#### ***2.2.7.1. Criptografía.***

El diccionario de la Real Academia Española define a la criptografía como "el arte de escribir con clave secreta o de un modo enigmático"

Tal definición da una idea, a grandes rasgos, de que la criptografía se utiliza para escribir de manera tal que el resultado de esa escritura pueda ser interpretado únicamente por quien conozca la clave secreta. Sin embargo esta definición es incompleta en la actualidad respecto de las técnicas usadas en sistemas informáticos.

La criptografía tiene diversos usos entre ellos la confidencialidad o privacidad de la información, que implica básicamente mantener en secreto una información determinada.

Autenticación, este es otro mecanismo, técnica o uso muy usado en la actualidad, hablar de autenticación implica hablar de la corroboración de la identidad de una entidad (persona, computadora, un sector de una compañía etc.).

Verificaciones de integridad, al hablar de comprobaciones o de verificaciones de integridad nos referimos a un uso o aplicación de técnicas criptográficas para el aseguramiento de que una información particular no haya sido alterada por personas no autorizadas o por cualquier otro método no conocido.

Algunas aplicaciones de la criptografía que se pueden derivar de las anteriores son:

- La autorización: Permiso concreto, a una parte o entidad, para dar acceso a un recurso.
- La validación: Medio de proveer una autorización puntual para el uso o manipulación de una información o recursos.
- Control de acceso: Restricción de acceso a la información o a los recursos para las partes o entidades con privilegios suficientes.
- Certificación: Respaldo de información por una parte o entidad de confianza.
- El fechado: Registro de la fecha de creación o de existencia de una información determinada.
- Algunas otras también: atestiguamiento, recibo, confirmación, propiedad, anonimato, revocación.

### *Criptografía simétrica*

La criptografía simétrica usa una misma clave para cifrar y descifrar mensajes. Las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar. Una vez que ambas partes tienen acceso a esta clave, el remitente cifra un mensaje usando la clave, lo envía al destinatario, y éste lo descifra con la misma clave.

Dado que toda la seguridad está en la clave, es importante que sea muy difícil adivinar el tipo de clave. Esto quiere decir que el abanico de claves posibles, o sea, el espacio de posibilidades de claves, debe ser amplio.

Actualmente, los ordenadores pueden descifrar claves con extrema rapidez, y ésta es la razón por la cual el tamaño de la clave es importante en los criptosistemas modernos. El algoritmo de cifrado DES usa una clave de 56 bits, lo que significa que hay 256 claves posibles (72.057.594.037.927.936 claves). Esto representa un número muy alto de claves, pero un ordenador genérico puede comprobar el conjunto posible de claves en cuestión de días. Una máquina especializada puede hacerlo en horas. Algoritmos de cifrado de diseño más reciente como 3DES, Blowfish e IDEA usan claves de 128 bits, lo que significa que existen 2128 claves posibles. Esto equivale a muchísimas más claves, y aun en el caso de que todas las máquinas del planeta estuvieran cooperando, tardarían más tiempo en encontrar la clave que la edad del universo.

El principal problema con los sistemas de cifrado simétrico no está ligado a su seguridad, sino al intercambio/distribución de claves. Una vez que el remitente y el destinatario hayan intercambiado las claves pueden usarlas para comunicarse con seguridad, pero ¿qué canal de comunicación que sea seguro han usado para transmitirse las claves? Sería mucho más fácil para un atacante intentar interceptar una clave que probar las posibles combinaciones del espacio de claves.

Otro problema es el número de claves que se necesitan. Si tenemos un número n de personas que necesitan comunicarse entre sí, se necesitan en total n(n-1)/2 claves para todas las parejas de personas que tengan que comunicarse de modo privado. Esto puede funcionar con un grupo reducido de personas, pero sería imposible llevarlo a cabo con grupos más grandes.

Para solucionar estos problemas se podrían tener centros de distribución de claves simétricas. Esto podría funcionar por ejemplo para organizaciones militar. Aunque siempre habría un riesgo a posibles fugas de información de que claves son usadas en ciertas comunicaciones. Sin embargo su uso en el sector privado llevaría consigo inevitables fugas, atascos burocráticos y una constante amenaza de filtraciones.

### *Criptografía asimétrica*

La criptografía asimétrica usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona que ha enviado el mensaje. Una clave es pública y se puede entregar a cualquier persona, la otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso a ella. Los métodos criptográficos garantizan que esa pareja de claves sólo se puede generar una vez,

de modo que se puede asumir que no es posible que dos personas hayan obtenido casualmente la misma pareja de claves.

Si el remitente usa la clave pública del destinatario para cifrar el mensaje, una vez cifrado, sólo la clave privada del destinatario podrá descifrar este mensaje, ya que es el único que la conoce. Por tanto se logra la confidencialidad del envío del mensaje, nadie salvo el destinatario puede descifrarlo.

Si el propietario del par de claves usa su clave privada para cifrar el mensaje, cualquiera puede descifrarlo utilizando su clave pública. En este caso se consigue por tanto la identificación y autentificación del remitente, ya que se sabe que sólo pudo haber sido él quien empleó su clave privada (salvo que alguien se la hubiese podido robar). Esta idea es el fundamento de la firma electrónica.

Los sistemas de cifrado de clave pública o sistemas de cifrado asimétricos se inventaron con el fin de evitar por completo el problema del intercambio de claves de los sistemas de cifrado simétricos. Con las claves públicas no es necesario que el remitente y el destinatario se pongan de acuerdo en la clave a emplear. Todo lo que se requiere es que, antes de iniciar la comunicación secreta, el remitente consiga una copia de la clave pública del destinatario. Es más, esa misma clave pública puede ser usada por cualquiera que desee comunicarse con su propietario. Por tanto, se necesitarán sólo n pares de claves por cada n personas que deseen comunicarse entre sí.

La mayor ventaja de la criptografía asimétrica es que la distribución de claves es más fácil y segura ya que la clave que se distribuye es la pública manteniéndose la privada para el uso exclusivo del propietario, pero este sistema tiene bastantes desventajas:

- Para una misma longitud de clave y mensaje se necesita mayor tiempo de proceso.
- Las claves deben ser de mayor tamaño que las simétricas.
- El mensaje cifrado ocupa más espacio que el original.

#### ***2.2.7.2 XSS.***

XSS es un ataque de inyección de código malicioso para su posterior ejecución que puede realizarse a sitios web, aplicaciones locales e incluso al propio navegador.

Sucede cuando un usuario mal intencionado envía código malicioso a la aplicación web y se coloca en forma de un hipervínculo para conducir al usuario a otro sitio web, mensajería instantánea o un correo electrónico. Así mismo, puede provocar una negación de servicio (DDos).

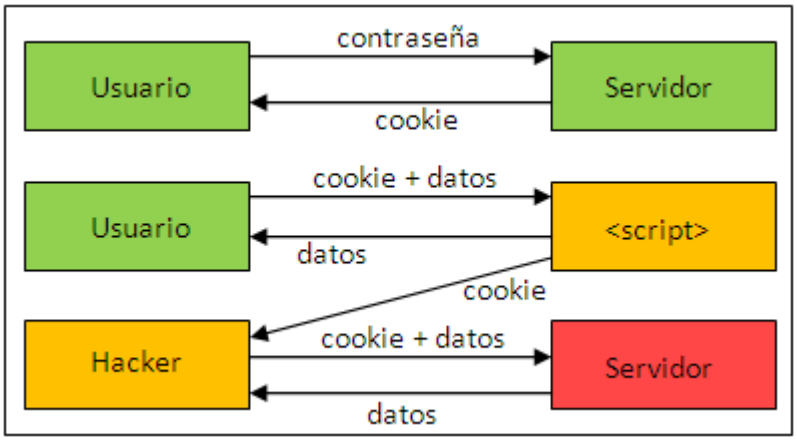



Figura 25. Ataque XSS. Descripción gráfica.

Generalmente, si el código malicioso se encuentra en forma de hipervínculo es codificado en HEX (basado en el sistema de numeración hexadecimal, base 16) o algún otro, así cuando el usuario lo vea, no le parecerá sospechoso. De esta manera, los datos ingresados por el usuario son enviados a otro sitio, cuya pantalla es muy similar al sitio web original.

De esta manera, es posible secuestrar una sesión, robar cookies y cambiar la configuración de una cuenta de usuario.

***Tipos de ataques***
- ***directo***
- ***indirecto o reflejado***

Las diversas variantes de esta vulnerabilidad pueden dividirse en dos grandes grupos: el primero se conoce como XSS persistente o directo y el segundo como XSS reflejado o indirecto.

**Directo o persistente**. Consiste en invadir código HTML mediante la inclusión de etiquetas <script> y <frame> en sitios que lo permiten.

**Local.** Es una de las variantes del XSS directo, uno de sus objetivos consiste en explotar las vulnerabilidades del mismo código fuente o página web. Esas vulnerabilidades son resultado del uso indebido del DOM (Modelo de Objetos del Documento, es un conjunto estandarizado de objetos para representar páginas web) con JavaScript, lo cual permite abrir otra página web con código malicioso JavaScript incrustado, afectando el código de la primera página en el sistema local. Cuando el XSS es local, ningún código malicioso es enviado al servidor. El funcionamiento toma lugar completamente en la máquina del cliente, pero modifica la página proporcionada por el sitio web antes de que sea interpretada por el navegador para que se comporte como si se realizara la carga

maliciosa en el cliente desde el servidor. Esto significa que la protección del lado del servidor que filtra el código malicioso no funciona en este tipo de vulnerabilidad.

**Indirecto o reflejado.** Funciona modificando valores que la aplicación web pasa de una página a otra, sin emplear sesiones. Sucede cuando se envía un mensaje o ruta en una URL, una cookie o en la cabecera HTTP.

#### ***2.2.7.3 ¿COMO DEFENDERSE DE UN ATAQUE XSS?***

La aplicación web que se desee implementar debe contar con un buen diseño. Posteriormente se deben realizar diversos tipos de pruebas, antes de su liberación, para detectar posibles fallos y huecos de seguridad, mediante el empleo de alguna herramienta automatizada. También es conveniente proporcionar mantenimiento a la aplicación y estar actualizado en las versiones de las herramientas que se emplean para su puesta en marcha.

Algunas recomendaciones para mitigar el problema, son:

- Emplear librerías verificadas, o algún framework que ayude a disminuir el inconveniente. Por ejemplo: la librería anti-XSS de Microsoft, el módulo ESAPI de codificación de OWASP, Apache Wicket, entre otros.
- Entender el contexto en el cual los datos serán usados, y la codificación de los mismos, este aspecto es importante cuando se envían datos de un componente a otro de la aplicación, o cuando se deben enviar a otra aplicación.
- Conocer todas las áreas potenciales donde las entradas no verificadas pueden acceder al software: parámetros o argumentos, cookies, información de la red, variables de entorno, resultados de consultas, búsqueda de DNS reversible, peticiones enviadas en las cabeceras, componentes de la URL, correos electrónicos, archivos, nombres de archivo, bases de datos o algún sistema externo que proporcione información a la aplicación.
- Las validaciones de datos de entrada, deben realizarse siempre del lado del servidor, no sólo en el lado del cliente. Los atacantes pueden evitar la validación realizada del lado del cliente modificando valores antes de realizar verificaciones o remover por completo esta validación.
- En caso de ser posible, emplear mecanismos automatizados para separar cuidadosamente los datos del código fuente: revisión de comillas, codificación y validación automática que muchas veces se escapan al desarrollador.
- Por cada página web generada, se recomienda emplear una codificación determinada de caracteres, ya que si no se especifica, el navegador puede dar un trato diferente a ciertas secuencias de caracteres especiales, permitiendo la apertura del cliente a posibles ataques.
- Para mitigar el problema de ataque contra el uso de cookies, es conveniente indicar que tiene el formato de HttpOnly. En los navegadores que lo soportan, puede prevenirse que la cookie sea usada por scripts maliciosos desde el lado del cliente.
- Se debe emplear una estrategia de validación de las entradas: rechazar aquellas que no cumplan con lo especificado, limpiar las que sean necesarias. Al validar, considérense las

características de cada entrada: longitud, tipo de dato, rango de valores aceptados, entradas pérdidas o adicionales, sintaxis, consistencia con otras entradas proporcionadas y seguimiento de las reglas del negocio.

- Cuando se construyan páginas web de forma dinámica (generadas de acuerdo a las entradas o solicitudes de los usuarios), es recomendable usar listas blancas estrictas. Todas las entradas deben ser limpiadas y validadas, incluidos cookies, campos ocultos, cabeceras y la propia dirección.
- Cuando una cantidad aceptable de objetos, como nombres de archivo o URL es limitada o conocida, es conveniente crear una conjunto de asignaciones de valores de entrada fijo a los nombres de archivo o URL y rechazar todos los demás.
- Se recomienda usar un firewall de aplicaciones capaz de detectar ataques cuando el código se genere dinámicamente, como medida de prevención, debe complementarse con otras para proporcionar defensa en profundidad.

Así como el desarrollador debe validar las entradas proporcionadas por parte del usuario, el encargado de diseñar e implementar la base de datos debe considerar la seguridad de la misma, pues en ella se guarda la información proporcionada por los usuarios y es manipulada mediante la aplicación web. Los datos que serán almacenados, también pueden ser validados mediante el uso de constraints (restricciones aplicables a los objetos de una base de datos: unique, default, not null, check) que restringen la entrada para cada campo.

#### ***2.2.7.4 ALGUNAS VARIANTES DEL ATAQUE XSS.***

***PDF XSS***

Es una vulnerabilidad ampliamente usada para afectar el Acrobat Reader de Adobe. En este caso, si se abusa de las características para abrir archivos en Acrobat, un sitio bien protegido se vuelve vulnerable a un ataque de tipo XSS si da alojamiento a documentos en formato PDF.

Esto afecta seriamente, a menos que se actualice el Reader o se cambie la forma en que el navegador maneja dichos documentos.

Una manera de combatirlo, si se cuenta con el servidor de aplicaciones web Apache, es llevar a cabo la correcta configuración de ModSecurity, ya que cuenta con directivas de protección para archivos en formato PDF.

***XSRF***

Un ataque Cross-Site Request Forgery (XSRF o también CSRF) explota la confianza que un usuario tiene hacia las entradas proporcionadas por un sitio.

Por ejemplo: un usuario se encuentra autenticado y navegando en un sitio, en ese momento un atacante obtiene el control de su navegador, con él realiza una solicitud a una tarea de una URL válida del sitio, por lo que el atacante tendrá acceso como si fuera el usuario previamente registrado.

Distintivamente, un atacante intercalará código HTML o JavaScript malicioso en un correo o en una tarea específica accesible desde una URL, que se ejecuta ya sea directamente o empleando un error de tipo XSS. También, es posible realizar inyección a través de lenguajes como el BBCode. Este tipo de ataques son difíciles de detectar.

Muchas de las funcionalidades de un sitio web son susceptibles de uso durante un ataque XSRF. Esto incluye información enviada tanto por GET como por POST.

También puede usarse como vector para explotar vulnerabilidades de tipo XSS en una aplicación. Ejemplos de ello son: una vulnerabilidad de tipo XSS en un foro donde un atacante puede obligar al usuario a publicar –sin que éste se dé cuenta- un gusano informático. Un atacante puede también usar XSRF para transmitir un ataque a algún sitio de su elección, así como realizar un DDos.

Sin embargo, las formas más comunes de realizar este tipo de ataque consisten en usar la etiqueta HTML o el objeto JavaScript empleados para imágenes. Distintivamente, el atacante infiltrará un email o sitio web en ellos, así cuando el usuario cargue la página o el correo electrónico, también estará realizando la petición a la URL que haya colocado el atacante.

Un atacante puede instalar su script dentro de un documento de Word, un archivo de flash, un clip de video, redifusión web RSS o Atom, o algún otro tipo de formato que pueda alojar el script.

Si un sitio web permite ejecutar sus funciones empleando una URL estática o peticiones POST, es posible que sea vulnerable, si la función se lleva a cabo mediante la petición GET, el riesgo es mayor. Si se realizan las mismas funciones, de la misma forma repetidamente, entonces la aplicación puede ser vulnerable.

Un ataque XSRF no puede evitarse mediante la verificación del referer de las cabeceras de la petición realizada, ya que puede “limpiarse” o modificarse mediante algún tipo de filtro. Las cabeceras pueden falsearse usando XMLHTTP, por ejemplo.

Una de las soluciones más conocidas, consiste en adjuntar un token no predecible y cambiante a cada petición. Es importante que el estado de éste vaya asociado con la sesión del usuario, de otra manera un atacante puede adjuntar su propio token válido y emplearlo en su beneficio. Adicionalmente, al ligarlo a la sesión del usuario es importante limitar el periodo durante el cual será válido.

### ***2.2.8 INYECCION DE CODIGO SQL.***

La inyección de código SQL es un ataque en el cual se inserta código malicioso en las cadenas que posteriormente se pasan a una instancia de SQL Server para su análisis y ejecución. Todos los procedimientos que generan instrucciones SQL deben revisarse en busca de vulnerabilidades de inyección de código, ya que SQL Server ejecutará todas las consultas recibidas que sean válidas desde el punto de vista de la sintaxis. Un atacante calificado y con determinación puede manipular incluso os datos con parámetros.

La forma principal de inyección de código SQL consiste en la inserción directa de código en variables especificadas por el usuario que se concatenan con comandos SQL y se ejecutan. Existe un ataque

menos directo que inyecta código dañino en cadenas que están destinadas a almacenarse en una tabla o como metadatos. Cuando las cadenas almacenadas se concatenan posteriormente en un comando SQL dinámico, se ejecuta el código dañino.

El proceso de inyección consiste en finalizar prematuramente una cadena de texto y anexar un nuevo comando. Como el comando insertado puede contener cadenas adicionales que se hayan anexado al mismo antes de su ejecución, el atacante pone fin a la cadena inyectada con una marca de comentario "--". El texto situado a continuación se omite en tiempo de ejecución.

Los ataques por inyección SQL permiten a los atacantes suplantar identidad, alterar datos existentes, causar problemas de repudio como anular transacciones o cambiar balances, permite la revelación de todos los datos en el sistema, destruir los datos o si no volverlos inasequibles, y convertirse en administradores del servidor de base de datos.

La inyección SQL es muy común con aplicaciones PHP y ASP debido a la prevalencia de interfaces funcionales obsoletas. Debido a la naturaleza de las interfaces programáticas disponibles, las aplicaciones J2EE y ASP.NET tienen menor probabilidad de ser fácilmente atacadas por una inyección SQL.

La gravedad de una inyección SQL está limitada por la habilidad e imaginación del atacante, y en menor medida a las contramedidas, como por ejemplo las conexiones con bajo privilegio al servidor de bases de datos, entre otras. En general, se considera a la inyección SQL de alto impacto.

#### ***2.2.8.1 DEFENSA CONTRA INYECCION DE CODIGO SQL.***

Se deben validar siempre los datos especificados por el usuario mediante comprobaciones de tipo, longitud, formato e intervalo. A la hora de implementar medidas de precaución frente a la especificación de datos dañinos, tener en cuenta la arquitectura y los escenarios de implementación de la aplicación. Recordar que los programas diseñados para ejecutarse en un entorno seguro pueden copiarse en un entorno no seguro. Las sugerencias que se muestran a continuación deben considerarse prácticas recomendadas:

- No hacer suposiciones sobre el tamaño, tipo o contenido de los datos que recibirá la aplicación. Por ejemplo, debe hacer la siguiente evaluación:
- Cómo se comportará la aplicación si un usuario (malicioso o no) especifica un archivo MPEG de 10 megabytes cuando la aplicación espera un código postal.
- Cómo se comportará la aplicación si se incrusta una instrucción DROP TABLE en un campo de texto.
- Comprobar el tamaño y el tipo de los datos especificados y aplique unos límites adecuados. Esto puede impedir que se produzcan saturaciones deliberadas del búfer.
- Compruebe el contenido de las variables de cadena y acepte únicamente valores esperados. Rechazar las especificaciones que contengan datos binarios, secuencias de escape y caracteres de comentario. Esto puede impedir la inyección de scripts y puede servir de protección frente a explotaciones de saturación del búfer.
- Cuando se trabaje con documentos XML, valide todos los datos con respecto a su esquema a medida que se vayan indicando.

- No crear nunca instrucciones Transact-SQL directamente a partir de datos indicados por el usuario.
- Utilizar procedimientos almacenados para validar los datos indicados por el usuario.
- En entornos de varios niveles, todos los datos deben validarse antes de que se admitan en la zona de confianza. Los datos que no superen el proceso de validación deben rechazarse, y debe devolverse un error al nivel anterior.
- Implemente varias capas de validación. Las precauciones que se tomen contra usuarios malintencionados ocasionales pueden resultar ineficaces contra piratas informáticos con determinación. Lo más recomendable es validar los datos especificados por el usuario en la interfaz de usuario y, después, en todos los puntos posteriores en que atraviesen un límite de confianza.

  Por ejemplo, la validación de datos en una aplicación de cliente puede evitar la inyección de scripts. Sin embargo, si en el siguiente nivel se asume que ya se ha validado la entrada, cualquier usuario malintencionado que sea capaz de eludir un cliente puede disfrutar de un acceso sin restricciones a un sistema.

- No concatenar nunca datos especificados por el usuario que no se hayan validado. La concatenación de cadenas es el punto de entrada principal de una inyección de scripts.
- No aceptar las siguientes cadenas en campos a partir de los que puedan construirse nombres de archivo: AUX, CLOCK$, COM1 a COM8, CON, CONFIG$, LPT1 a LPT8, NUL y PRN.

Para ataques dirigidos a computadoras personales, existen 2 ataques que son los más comunes para obtener las contraseñas de acceso a éstas, todo de manera remota: exploits y troyanos.

### ***2.2.9 EXPLOITS.***

Son códigos maliciosos que intentan explotar las vulnerabilidades en las aplicaciones o sistemas operativos.

Son herramientas que utilizan los crackers para infiltrarse en sistemas desprotegidos o descuidados, los cuales muchas veces permiten accesos de Administrador en la máquina afectada.

Son programas o scripts que están escritos en diferentes lenguajes de programación para aprovecharse de vulnerabilidades y/o errores específicos dentro de un sistema para lograr acceder a él de forma ilegítima o causar otro tipo de problemas. Estos errores, comúnmente llamados bugs, pueden ser del tipo desbordamiento de búfer (buffer overflow), condición de carrera (race condition), errores de validación de variables, etc.

Por ejemplo, si se encontró un error en un software o en un sistema operativo un cracker escribirá un código que sirva para explotar esta vulnerabilidad y con un par de instrucciones más quizá sea

posible abrir un acceso remoto con permisos de administrador en el servidor afectado.

Podríamos catalogar a los exploits en dos tipos diferentes:

1.- 0-day

2.- Públicos

Los exploits de tipo 0-day son aquellos que los crackers mantienen ocultos al mundo y los utilizan para explotar los sistemas que quieren. De alguna manera son códigos privados.

Por otro lado los exploits públicos son aquellos que los crackers decidieron no utilizar más en su propio beneficio y los liberan públicamente. Muchas veces pueden pasar varios meses o años entre que el exploit pase de condición 0-day a ser público. Es por esto mismo que los primeros son más peligrosos, ya que al no conocerse la vulnerabilidad y no ser pública entonces existen muchos más servidores afectados cuyos administradores ni siquiera se enteran de que pueden ser atacados. Al hacerse públicos, normalmente se entrega la solución o bien los fabricantes de software reaccionan y sacan una actualización de seguridad crítica.

Esta es la razón por la cual hay que siempre tener dos cosas presentes:

1.- El tipo de software y la versión exacta que tenemos instalado en nuestras máquinas, ya sea como cliente (ejemplo Microsoft Outlook) o servidor (Exchange, Postfix, Sendmail, etc.)

2.- Nunca dejar de revisar los sitios de exploits mencionados anteriormente. Increíblemente hay gente que se dedica a estar atentos a estos exploits para inmediatamente cuando se publica comenzar a atacar sitios webs. Estos son los llamados script-kiddies. Pero por más despectivo que parezca el nombre, son igualmente peligrosos.

### ***2.2.10 TROYANOS.***

El nombre de esta amenaza proviene de la leyenda del caballo de Troya, ya que el objetivo es el de engañar al usuario. Son archivos que simulan ser normales e indefensos, como pueden ser juegos o programas, de forma tal de "tentar" al usuario a ejecutar el archivo. De esta forma, logran instalarse en los sistemas. Una vez ejecutados, parecen realizar tareas inofensivas pero paralelamente realizan otras tareas ocultas en la computadora.

Al igual que los gusanos (un malware que tiene la propiedad de duplicarse a sí mismo) no siempre son malignos o dañinos. Sin embargo, a diferencia de los gusanos y los virus, estos no pueden replicarse por sí mismos.

Los troyanos pueden ser utilizados para muchos propósitos, entre los que se encuentran, por ejemplo:

- Acceso remoto (o Puertas Traseras): permiten que el atacante pueda conectarse remotamente al equipo infectado.
- Registro de tipeo y robo de contraseñas.
- Robo de información del sistema.

Los "disfraces" que utiliza un troyano son de lo más variados. En todos los casos intentan aprovechar la ingenuidad del usuario explotando diferentes técnicas de Ingeniería Social. Uno de los casos más comunes es el envío de archivos por correo electrónico simulando ser una imagen, un archivo de música o algún archivo similar, legítimo e inofensivo. Además del correo electrónico, otras fuentes de ataque pueden ser las mensajerías instantáneas o las descargas directas desde un sitio web.

Al igual que los gusanos, se pueden encontrar los primeros troyanos a finales de los años ’80, principios de los años ’90, de la mano del surgimiento de la Internet.

**Tipos de troyanos**

Troyanos más comunes
- -Backdoors
- -Keyloggers
- -Banker
- -Password stealer

La tabla número 6, explica a detalle qué son y cómo funcionan cada uno de los troyanos más comunes.

| ***TROYANO*** | ***DESCRIPCION*** | ***USO*** |
|---|---|---|
| **Backdoors** | Otros nombres para estos tipos son troyanos de acceso remoto o puertas traseras. Un troyano de estas características, le permite al atacante conectarse remotamente al equipo infectado. Las conexiones remotas son comúnmente utilizadas en informática y la única diferencia entre estas y un backdoor es que en el segundo caso, la herramienta es instalada sin el consentimiento del usuario. | Una vez que el atacante accede a la computadora del usuario, los usos que puede hacer del mismo son variados, según las herramientas que utilice: enviar correos masivos, eliminar o modificar archivos, ejecución de archivos, reiniciar el equipo o usos más complejos como instalar aplicaciones para uso malicioso (por ejemplo: |

| | | |
|---|---|---|
| | | alojamiento de sitios web de violencia o pedofilia). |
| **Keyloggers** | (Del inglés Key = Tecla y Log = Registro) son uno de los tipos más utilizados para obtener información sensible de los usuarios. Los troyanos de este tipo, instalan una herramienta para detectar y registrar las pulsaciones del teclado en un sistema. La información capturada es enviada al atacante generalmente, en archivos de texto con la información. Estos troyanos, no son una amenaza para el sistema sino para el usuario y su privacidad. | Pueden capturar información como contraseñas de correos, cuentas bancarias o sitios web, entre otras, y por lo tanto atentar contra información sensible del usuario. Los datos recolectados, pueden ser utilizados para realizar todo tipo de ataques, con fines económicos o simplemente malignos como modificar las contraseñas de las cuentas de acceso a algún servicio. |
| **Banker** | Los troyanos bancarios tienen como principal objetivo robar datos privados de las cuentas bancarias de los usuarios. Utilizan diferentes técnicas para obtener los datos de acceso a todo tipo de entidades financieras, | Reemplazan parcial o totalmente el sitio web para enviar capturas de pantalla de la página bancaria (útiles cuando el usuario utiliza teclados virtuales) o incluso la grabación en formato de video de las acciones del usuario mientras accede al sitio web. Los datos son enviados al atacante, por lo general, por correo electrónico o alojándolos en sitios FTP |
| **Password stealer** | Los password Stealer se encargan de robar información introducida en los formularios en las páginas web. Estos datos pueden ser enviados por correo electrónico o almacenados en un servidor al que el delincuente accede para recoger la información robada. | Pueden robar información de todo tipo, como direcciones de correo electrónico, logins, passwords, PINs, números de cuentas bancarias y de tarjetas de crédito. En la mayoría de sus versiones, utilizan técnicas keyloggers para su ejecución y son similares a estos. |

Tabla 6. Descripción de los troyanos más comunes.

### ***2.3 ESPIONAJE DE DATOS.***

Una persona acostumbrada a navegar por la Red o utilizar correo electrónico ha podido ser víctima de espionaje, aunque en la mayoría de los casos, no se haya percatado de ello.

Bien, como sucede en todos los campos o materias de la vida, la tecnología avanza, y a pasos agigantados, lo que aporta grandes y notables beneficios a las comunicaciones y a la interacción de los distintos sectores de la economía. No obstante estos nuevos conocimientos pueden ser aprovechados por mentes maliciosas que los utilizan para fines menos éticos.

La aparición en el mercado de nuevas técnicas y programas, difundidos en su mayor parte a través de Internet, posibilitan la recopilación de información privada de un determinado usuario, sin dejar de mencionar aquellos programas que reconfiguran parámetros de las computadoras aprovechándose del desconocimiento de las personas en el campo de las nuevas tecnologías.

Existen diferentes técnicas, entre ellas:

Técnicas de espionaje de datos
- -Adware
- -Spyware
- -Programas de acceso remoto ilegales (backdoors)
- -Caballos de Troya
- -Sniffing

En la tabla número 7, se describen brevemente estas técnicas utilizadas para el espionaje de datos.

| ***TECNICA*** | ***DESCRIPCION*** |
|---|---|
| ***SPYWARE*** | El spyware es aquel software que transmite información fuera de nuestra computadora y sin nuestro conocimiento |
| ***ADWARE:*** | Está totalmente orientado a la publicidad, que suele llegar a ser hostil. Algunas aplicaciones de adware, utilizan información de los programas, o de las búsquedas que nosotros estamos haciendo en Internet; espían lo que buscamos, por lo que algunos de estos programas se pueden clasificar como spyware. |
| ***BACKDOORS:*** | Permiten el acceso de un tercero a su computadora para un posterior ataque o alteración de los datos. Son fácilmente reconocibles por los antivirus. |
| ***CABALLOS DE TROYA*** | Programa que una vez instalado en la computadora provoca daños o pone en peligro la seguridad del sistema |

| | |
|---|---|
| ***SNIFFING*** | Se trata de una técnica por la cual se puede "escuchar" todo lo que circula por una red. Esto que en principio es propio de una red interna o Intranet, también se puede dar en la red de redes: Internet.<br>Esto se hace mediante aplicaciones que actúan sobre todos los sistemas que componen el tráfico de una red, así como la interactuación con otros usuarios y equipos de cómputo. Capturan, interpretan y almacenan los paquetes de datos que viajan por la red, para su posterior análisis (contraseñas, mensajes de correo electrónico, datos bancarios, etc.). |

Tabla 7. Descripción de técnicas para espionaje de datos.

### ***2.3.1 SNIFFERS.***

***Cómo funcionan los Sniffers:***

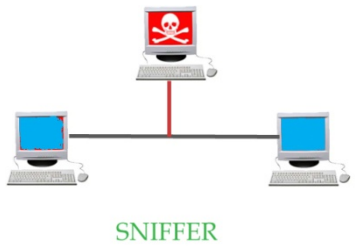



Figura 26. Funcionamiento básico de un Sniffer.

El modo más sencillo de comprender su funcionamiento, es examinándola forma en que funciona un sniffer en una red Ethernet. Se aplican los mismos principios para otras arquitecturas de red.

Un sniffer de Ethernet es un programa que trabaja en conjunto con la tarjeta de interfaz de red (NIC, Network Interface Card), para absorber indiscriminadamente todo el tráfico que esté dentro del umbral de audición del sistema de escucha. Y no sólo el tráfico que vaya dirigido a una tarjeta de red, sino a la dirección de difusión de la red 255.255.255.255 (a todas partes).

Para ello, el sniffer tiene que conseguir que la tarjeta entre en modo "promiscuo", en el que -como indica la propia palabra- recibirá todos los paquetes que se desplazan por la red. Así pues, lo primero que hay que hacer es colocar el hardware de la red en modo promiscuo; a continuación el software puede capturar y analizar cualquier tráfico que pase por ese segmento.

Esto limita el alcance del sniffer, pues en este caso no podrá captar el tráfico externo a la red (o sea, más allá de los routers y dispositivos similares), y dependiendo de dónde esté conectado en la Intranet, podrá acceder a más datos y más importantes que en otro lugar. Para absorber datos que

circulan por Internet, lo que se hace es crear servidores de correo o de DNS para colocar sus sniffers en estos puntos tan estratégicos.

#### 2.3.1.1 Programas Sniffers:

Hay una serie de aplicaciones que son las que principalmente se utilizan para este propósito del sniffing. A continuación, se mencionan algunas de éstas, así como su forma de actuar:

A) SpyNet

Es un programa shareware muy sencillo, incluye 2 programas en 1, "CaptureNet" y "PeepNet".

El primero es el que espía el tráfico en la red, guardando los paquetes de datos en formatos de bytes hexadecimales.

Mientras que el segundo analiza los datos recopilados, reconstruyendo los paquetes, o reproduciendo los correos incluso las contraseñas de los E-mail empleados (sólo la versión de pago); además muestra las direcciones de las computadorases que participan y el protocolo empleado (pop3, http, smtp, etc.), así como los programas empleados (navegadores, programas de ftp, de correo, etc.) incluso hasta el sistema operativo.

B) Wireshark

Muy aplaudido en el mundo Linux, y ya con una versión para Windows. Su funcionamiento es similar al anterior, pero menos gráfico, aunque informa de lo que encuentra según el uso del protocolo. Y por supuesto, cuando se trata de POP3 localiza rápidamente el usuario y la contraseña. Y para rematar es código abierto (open source) y además gratuito.

C) WinSniffer

Es un programa especialista en contraseñas. Busca en toda la red accesos de login (usuario) y contraseñas, mostrándolos en pantalla. En concreto en la versión de prueba muestra el usuario y en la de pago, además la contraseña.

#### ***2.3.1.2. Detección de los Sniffers:***

Para detectar estas amenazas de una forma rápida, en redes que no utilizan las contramedidas anteriormente citadas, podemos utilizar herramientas que detectan los adaptadores de red que están funcionando en modo promiscuo (modo necesario para el funcionamiento de los sniffers). Herramientas como:

*En Linux.*

**Sniffdet** es un sistema de pruebas para la detección remota de los sniffers de red. Usa las técnicas test ICMP, test ARP, test DNS y test de ping de latencia.

El proyecto del **Sentinel** es una puesta en práctica de las técnicas de detección de modo promiscuo. Necesita las bibliotecas: libpcap y libnet. Utiliza los métodos de: test DNS, test ARP, prueba ICMP Etherping, y ping de latencia.

*En Windows:*

**ProDETECT** es un explorador de sniffers, que utiliza una técnica de análisis del paquete ARP.

Promgry y PromgryUI son dos herramientas que detectan los adaptadores de red que están funcionando en modo promiscuo, la diferencia entre una y otra es que PromgryUI tiene interfaz gráfica y Promgry se ejecuta en consola de comandos.

PromiscDetect comprueba si su adaptador de red está funcionando en modo promiscuo, sirve para probar que un sniffers está funcionando en la máquina.

Un ejemplo de cómo es que se puede espiar información mediante un sniffer, es el siguiente:

Se utilizó el sniffer llamado NetworkMiner; de manera inalámbrica, se configuró la tarjeta de red de modo promiscuo, y sólo fue cuestión de esperar que la víctima visitara algún sitio de Internet; cabe destacar, que aquí se tomó el tráfico de toda la red inalámbrica, no sólo lo de una sola computadora, es decir, con este software no se puede especificar precisamente a quien se quiere atacar, sino que se recibe toda la información de la red inalámbrica.

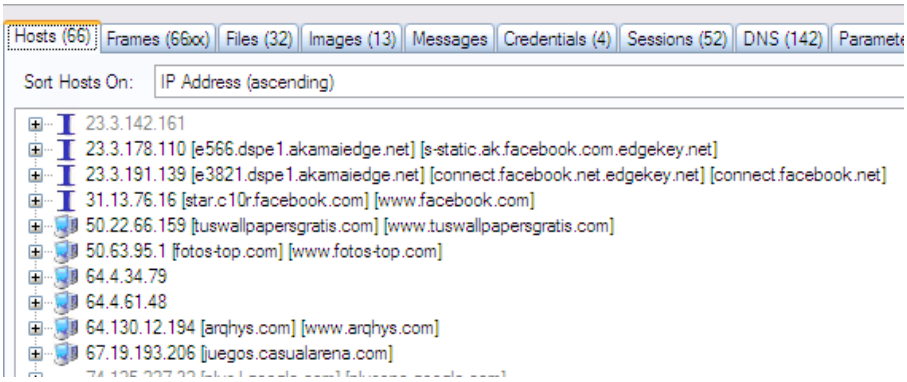



Figura 27. En esta imagen, se muestran las IP que la víctima visitaba al momento del ataque.

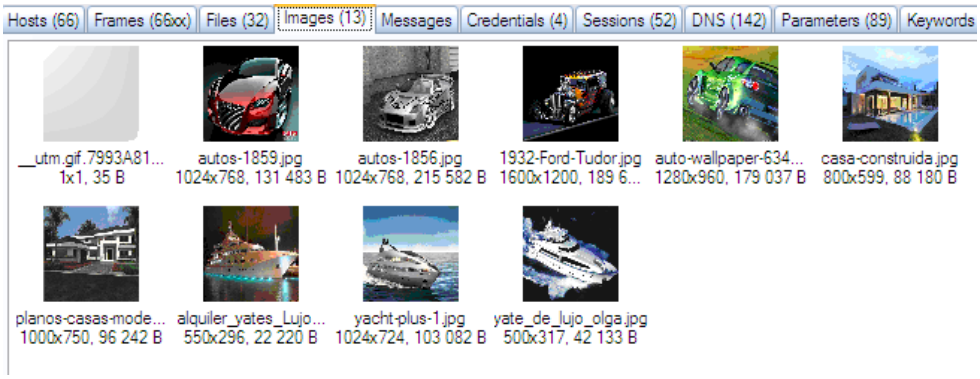



Figura 28. En esta imagen, se muestra lo que la víctima observaba:

También se pueden obtener contraseñas de sitios que tengan una seguridad deficiente:

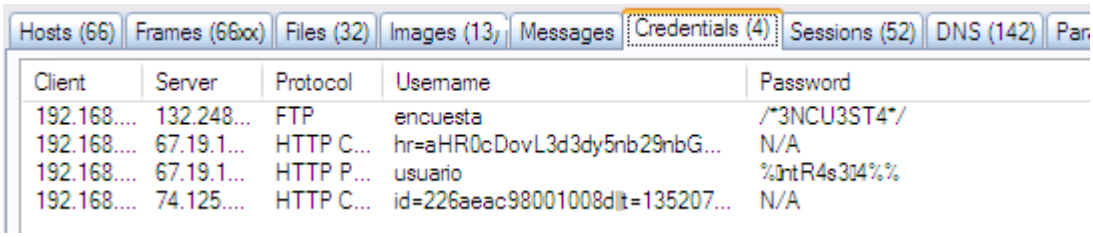



Figura 29. Contraseñas de sitios con una seguridad defectuosa.

Una compañía estadounidense, "Lover Spy", ofrece la forma de espiar a la persona deseada enviando una tarjeta postal electrónica, que se duplica en el sistema como un dispositivo oculto.

Según algunos expertos en seguridad informática, esta práctica parece violar la ley estadounidense.

Lo venden como una manera de poder saber qué es lo que está haciendo tu pareja, o cualquier otra persona cercana, como puede ser un hijo o similar. Su precio es de 89 dólares, y puede ser instalado hasta en cinco computadoras.

Desde que el programa se instala, todas las acciones llevadas a cabo en la computadora son registradas, desde un simple 'clic' de ratón. Esta información es posteriormente remitida a la persona que solicitó el servicio de espionaje.

No es este el único programa que sirve para espiar, hay otros como eBlaster de SpectorSoft, con la salvedad de que éste es instalado por el usuario en su propio equipo.

### ***2.3.2. Espionaje empresarial y gubernamental.***

En la actualidad se llevan a cabo acciones de espionaje por parte de gobiernos apoyados por instituciones privadas como se muestra en extracto del artículo periodístico siguiente llamado:

“Cinco preguntas sobre cómo nos espía EEUU a través de Apple y Microsoft”

Extraído de www.expansion.com Madrid 22.06.2013

http://www.expansion.com/2013/06/21/empresas/tmt/1371843239.html

“*El Gobierno de EEUU ha redoblado sus esfuerzos por evitar un nuevo ataque terrorista. ¿Cómo? La Agencia Nacional de Seguridad ha puesto en marcha varios programas para monitorizar las comunicaciones.*

*No sólo controlan metadatos de llamadas telefónicas (como el teléfono del que se hace la llamada, el tiempo de comunicación y el tipo de dispositivo empleado, entre otros datos), sino también, como desveló recientemente The Washington Post, el contenido de las comunicaciones online.*

*En concreto, la NSA y la CIA tendrían acceso a las conversaciones de personas no americanas sospechosas de querer atentar contra la seguridad de EEUU. Es decir, a las comunicaciones habladas o escritas que cualquier europeo realiza a través de una red telefónica o IP.*

*Todos los gigantes tecnológicos estadounidenses están involucrados: Google, Microsoft, Skype, Yahoo!, Facebook y Apple son la cara visible de un escándalo que podría afectar a las relaciones entre la Unión Europea y EEUU.*

*Empresas como Google, Facebook y Apple recaban datos de sus usuarios, incluida su ubicación geográfica, siempre que el usuario haya aceptado previamente los términos de privacidad que se despliegan, por ejemplo, al descargar una apps.*

*No obstante, según The Washington Post, la NSA puso en marcha en 2007 un programa de vigilancia electrónica de alto secreto (Prism), por el que el Gobierno de EEUU accede a correos electrónicos, chats, direcciones IP, perfiles de redes sociales o transferencias de archivos.*

*"Al tratarse de un programa confidencial, las empresas involucradas tienen terminantemente prohibido reconocer haber dado acceso a sus servidores a la NSA o haber interconectado sus centros de datos con los de estas agencias", explica Antonio Martínez Algora, director general de Netasq, propiedad de Cassidian Cybersecurity (la división de seguridad de EADS) para España y Portugal.*

*Por ahora, Apple ha afirmado únicamente haber recibido entre 4.000 y 5.000 peticiones de datos, tanto de la NSA como de otras agencias, en los últimos seis meses. Por su parte, Facebook asegura que, sólo en el segundo semestre de 2012, recibió entre 9.000 y 10.000 peticiones de datos, que afectan a 19.000 de sus usuarios, de las que respondió al 79%. En el caso de Microsoft, la NSA solicitó información de unos 31.000 de sus clientes.*

*Google ha hecho un llamamiento a la calma y ha solicitado al Gobierno norteamericano publicar el tipo de datos que ha proporcionado, con el fin de tranquilizar a la opinión pública.*

*"El programa Prism es confidencial, pero no ilegal", confirma Martínez Algora. Ante la magnitud de la polémica, el propio Barack Obama ha defendido públicamente la legalidad de las actuaciones de sus servicios de inteligencia. EEUU justifica que el programa Prism está orientado a la detección precoz de amenazas contra la seguridad nacional, como el espionaje y el terrorismo.*

*Como se ve en el artículo anterior una vez que somos usuarios de estas empresas nuestros datos no nos pertenecen y en cualquier momento se puede violar nuestra privacidad de manera "legal"".*

***Wikileaks***

WikiLeaks es una organización sin fines de lucro dentro de los medios de comunicación. Su objetivo es llevar noticias e información ofreciendo una forma innovadora, segura y anónima para las fuentes de fugas de información de sus periodistas. Una de sus actividades más importantes es publicar material original junto con sus noticias para que los lectores e historiadores por igual puedan ver la evidencia de la verdad. Es una organización joven que ha crecido muy rápidamente, basándose en

una red de voluntarios dedicados de todo el mundo. Desde 2007, cuando se puso en marcha oficialmente la organización, Wikileaks ha trabajado para informar y publicar información importante.

## ***2.4 MANIPULACION DE DATOS Y FALSIFICACIÓN INFORMÁTICA***

Los datos informáticos son esenciales para los usuarios privados, las empresas y las administraciones, lo que depende de la integridad y disponibilidad de los datos. La carencia de acceso a los datos puede causar daños (económicos) considerables.

Una vez dentro de los sistemas informáticos a los cuales haya accedido el atacante, éste puede hacer demasiadas cosas con la información, como publicarla en redes sociales, borrarla, sustraerla, alterarla, restringir su acceso o bien utilizarla para otros fines como lo son el fraude y el robo de identidad; éstas últimas, situaciones de las que se hablarán más adelante.

El siguiente cuadro nos presenta las formas más comunes de falsificación de datos con las cuales los usuarios de una computadora se pueden enfrentar.

- Supresión de información.
- Alteración o falsificación de datos.
- Restricción de información.

### ***2.4.1 SUPRESIÓN DE INFORMACIÓN.***

En la actual sociedad del conocimiento, las empresas y entidades generan información constantemente y a un ritmo creciente: se estima que en 2020 la cantidad de información será 44 veces mayor que la que había en 2009. Gracias a la tecnología, esta información se puede generar, copiar, enviar y recibir desde cualquier lugar y en cualquier momento, aspectos vitales para el funcionamiento de las empresas.

El conocimiento de la gestión del ciclo de vida de la información y el establecimiento de planes, normas y políticas de almacenamiento de la información y de seguridad de los datos, asegura un control y gestión de la información eficiente.

Se dice que se produce una pérdida de información o datos cuando se altera alguno de sus atributos de integridad, disponibilidad y confidencialidad y, específicamente en el proceso del almacenamiento, la disponibilidad es el atributo más crítico. Una información se pierde definitivamente cuando no se consigue el acceso a la misma o esta ha desaparecido.

### ***2.4.2 Causas de la pérdida de datos***

En la tabla número 8, se describen las principales causas por las que los datos en una computadora pueden llegar a pederse.

| ***CAUSA*** | ***DESCRIPCION*** |
|---|---|
| Fallos mecánicos en los dispositivos de almacenamiento | Causados bien por motivos externos (como cortes de suministro eléctrico o picos de tensión en la red eléctrica), o internos de los propios dispositivos (por ejemplo, por degradación de las piezas mecánicas al final de la vida útil de los mismos). |
| Errores humanos | Por borrado o formateo de las unidades de almacenamiento o por manipulación indebida de los dispositivos. A veces la mala preparación del personal y la toma de decisiones erróneas a la hora de intentar recuperar la información tras un incidente son las causas de estos errores. |
| Fallos en el software utilizado | Como fallos imprevistos en los sistemas operativos por reinicios inesperados o mal funcionamiento de las propias herramientas de diagnóstico. |
| Desastres naturales o estructurales | Como incendios e inundaciones que causan la destrucción de las instalaciones donde se encuentran los equipos. |
| Virus o software malicioso | Los programas instalados en las computadoras buscan causar un fallo en el sistema y/o robar información que envían a un equipo remoto. |

Tabla 8. Causas de la pérdida de datos.

### ***2.4.3 VIRUS INFORMATICOS.***

La causa más común y peligrosa de pérdida de datos, son los virus informáticos. Anteriormente, los virus informáticos se distribuían por dispositivos de almacenamiento, tales como disquetes, mientras que hoy en día los virus se distribuyen por Internet anexos a los mensajes de correo electrónico o a los archivos que descargan los usuarios de Internet. Estos nuevos y eficientes métodos de distribución han acelerado de manera generalizada la infección por virus y han

aumentado sobremanera el número de sistemas informáticos infectados. Según las estimaciones, el gusano informático SQL Slammer infectó el 90 por ciento de los sistemas informáticos vulnerables en los diez 10 minutos posteriores a su distribución.

La mayoría de los virus informáticos de primera generación se limitaban a borrar información o mostrar mensajes. Recientemente, los efectos se han diversificado. Los virus modernos son capaces de abrir puertas traseras por las que los piratas pueden tomar el control del computador o cifrar los archivos del mismo de modo que las víctimas no puedan acceder a sus propios archivos, a no ser que paguen para obtener la clave.

***Virus de archivo:*** Este tipo de virus infecta a archivos ejecutables como los del tipo EXE, COM, DLL, OVL, DRV, SYS, BIN, e incluso BAT. El virus se añade al principio o al final de los archivos. Su código se ejecuta antes que el del programa original, pudiendo ser o no residentes. Una vez en memoria, buscan nuevos programas a los cuales puedan trasladarse.

***Virus macro:*** Este tipo de virus ha destruido el concepto que hasta el momento se tenía de los virus en general. Infectan documentos de determinadas aplicaciones que dispongan o puedan hacer uso de un potente lenguaje de macros. Los primeros virus de este tipo aparecieron en el verano de 1995 y, ya a principios del siguiente año, se habían hecho tremendamente populares, hasta el punto de haber arrebatado el primer puesto en cuanto a porcentaje de infecciones a los viejos virus de sector de arranque.

La inmensa mayoría utilizan el lenguaje de macros WordScript de Word (si bien podemos encontrar algunos desarrollados en otros lenguajes como pueda ser LotusScript para Lotus SmartSuite), aunque la aparición de VBA (Visual Basic for Applications) que emplea Microsoft Office, posibilita la creación de virus genéricos efectivos en cualquier aplicación con soporte para OLE2. Esta característica está propiciando que los virus creados con VBA se les denominen virus de OLE2.

La infección comienza cuando se carga un documento, ya sea un texto de Word, una hoja de cálculo de Excel, etc. La aplicación además del documento carga cualquier macro que lo acompaña. Si alguna o algunas de esas macros son válidas, la aplicación las ejecuta, haciéndose éstas dueñas del sistema por unos instantes. Al tener el control, lo primero que hacen es copiarse al disco duro y modificar la plantilla maestra (NORMAL.DOT en Word), para que sean ejecutadas ciertas de ellas al iniciar la aplicación determinada. En cada documento que creemos o abramos, se incluirán a partir de ese momento las macros "malignas".

Si cualquiera de esos documentos es abierto en otro equipo, se repite el proceso y se propaga la infección. Las capacidades destructivas son virtualmente incluso mayores y, puesto que algunos paquetes están disponibles para distintos sistemas y plataformas, son mucho más versátiles. Asimismo, las macros pueden ser programadas como troyanos, siendo capaces de incluir un virus convencional, cambiar una DLL o ejecutable, etc., e instalarlo en el sistema.

## ***2.5 ALTERACIÓN O FALSIFICACIÓN DE DATOS.***

Se refiere a quién, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en archivos o

soportes informáticos, electrónicos o telemáticos, o cualquier otro tipo de archivo o registro público o privado, por ejemplo:

• crear un documento que parece provenir de una institución fiable;

• manipular imágenes electrónicas

• alterar documentos.

Estas alteraciones, se llevan a cabo cuando se modifican o falsifican datos de los documentos almacenados de forma computarizada, o bien, las computadoras pueden efectuar las alteraciones de documentos, ya sean de carácter personal o comercial.

Una parte muy importante de esto, es el sabotaje informático, el cual consiste en modificar o borrar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema, o en su defecto, atentando directamente contra el usuario de la computadora, alterando la información de los datos que ésta contenga de él, ya sea de carácter personal, público, comercial, escolar, entre otras.

Los delincuentes siempre han intentado manipular documentos. Con la falsificación informática, se puede ahora copiar documentos digitales sin ninguna pérdida de calidad y manipularlos fácilmente. A los expertos forenses les resulta difícil comprobar las manipulaciones digitales a menos que se apliquen medios técnicos de protección para evitar la falsificación de un documento.

### ***2.5.1 Man-in-the-Middle.***

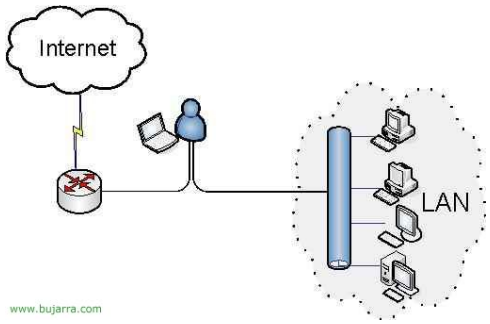



Figura 30. Funcionamiento básico de la técnica Man-in-the-Middle.

Uno de los ataques más comunes, es el denominado Man-in.the-Middle, el cual es un ataque en el que el enemigo adquiere la capacidad de leer, insertar y modificar a voluntad, los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado. El atacante debe ser capaz de observar e interceptar mensajes entre las dos víctimas. El ataque MitM es particularmente significativo en el protocolo original de intercambio de claves de Diffie-Hellman, cuando éste se emplea sin autenticación.

El ataque 'Man in the middle', traducido al español como 'El hombre en el medio', es un ataque PASIVO, que se lleva a cabo tanto en redes LAN como WLAN.

El ataque MitM puede incluir algunos de los siguientes subataques:

-Intercepción de la comunicación (eavesdropping), incluyendo análisis del tráfico y posiblemente un ataque a partir de textos planos (plaintext) conocidos.

-Ataques a partir de textos cifrados escogidos, en función de lo que el receptor haga con el mensaje descifrado.

-Ataques de sustitución.

-Ataques de repetición.

-Ataque por denegación de servicio (denial of service). El atacante podría, por ejemplo, bloquear las comunicaciones antes de atacar una de las partes. La defensa en ese caso pasa por el envío periódico de mensajes de status autenticados.

-MitM se emplea típicamente para referirse a manipulaciones activas de los mensajes, más que para denotar intercepción pasiva de la comunicación.

Un ejemplo para poner de manifiesto en qué consiste este ataque: suponer que se tienen 3 hosts dentro de una red, host A, host B, y host C. El host A quiere intercambiar información con el host B (éste host puede o no estar en la misma red), para ello, los paquetes deben enviarse a través del router que los dirige hacia B. Ahora, si el host C tiene intención de 'escuchar' el mensaje que A envía a B, sólo tiene que adoptar un papel de puente entre A y el router.

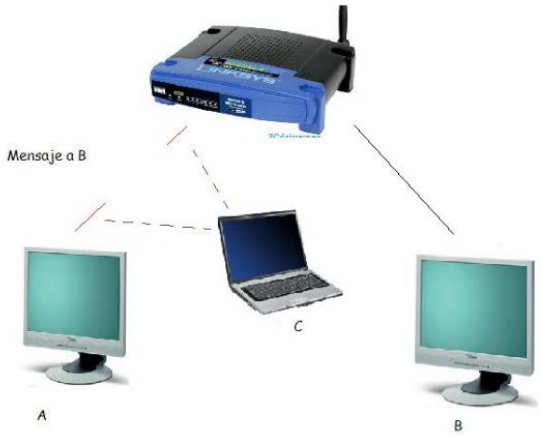



Figura 31. Implementación del ataque MIM.

Al ser un ataque pasivo, la víctima no detectaría nada raro, de ahí la dificultad de hacer frente a un ataque de este tipo.

En definitiva, este ataque permite monitorizar el tráfico que se desee de una red, tanto de un host hacia el router, como del router hacia un host.

### ***2.5.2. Técnicas de detección de sniffers.***

Es difícil detectar este tipo de aplicaciones (Wireshark o Cain), ya que son programas que trabajan de manera pasiva, y no dejan casi huellas, por no decir ninguna. Mucha de la información que circula por la red lo hace en texto plano, pudiendo acceder desde cualquier computadora de una misma red a esa información confidencial mediante un simple sniffer.

En la tabla número 9, se verán algunas de las técnicas para intentar detectar un ataque 'Man in the middle', no son excluyentes una con otra, así que se pueden combinar como más convenga.

| ***HERRAMIENTA*** | ***DESCRIPCION*** |
|---|---|
| Antisnif | Creada tanto para Windows como para sistemas Unix, lo que hace es probar los dispositivos de red para ver si alguno de ellos se está ejecutando en modo promiscuo, usa técnicas de test DNS, ping de latencia y test de ARP. Se introduce el rango de direcciones IP a analizar y la aplicación busca el posible sniffer en la red. |
| Sentinel | Hace uso de las librerías Libcap y Libnet.Es parecida a Antisnif, ya que también se encarga de detectar técnicas en modo promiscuo, y usa test de dns, test de ICMP, ping de latencia y test de ARP. |
| CPM | CPM es una aplicación creada por la universidad Carnegie Mellon, que se encarga también de ver si la interfaz de la máquina está en modo promiscuo. |
| SniffDet | Se basa en realizar pruebas de posibles protocolos que nos pueden llevar a la detección de un sniffer, prueba de ARP, test de ICMP, test de DNS, y test de ping de latencia. |
| NEPED | Se utiliza para detectar la intrusión de sniffers, realiza peticiones de ARP para cada dirección IP de la red, destinando los paquetes a una dirección inexistente, no a broadcast. Las interfaces que estén en modo promiscuo contestarán a estas peticiones. |
| Promiscan, Promisdetec, ProDETECT | Han sido creadas para sistemas Windows y tratan de detectar los hosts que se encuentran en modo promiscuo en redes LAN. |

Tabla 9. Detección de sniffers.

### ***2.5.3 Restricción de información.***

Muchas veces nos hemos visto en el caso de que al ingresar una memoria flash en una computadora pública al querer acceder a nuestra información esta ha desaparecido y sólo se tienen accesos directos, esto es obviamente a causa de un virus, para muchas personas este es el fin de la información pero en realidad lo que hace este tipo de virus es ocultar la información, así logrando restringirnos el acceso a esta, en algunas ocasiones esto no solo pasa en una memoria flash, sino que también llega a pasar en los discos duros , este método de restricción a la información es muy simple ya que sólo se han alterado los atributos de los documentos, para solucionarlo basta abrir una consola del sistema y posicionarnos en el directorio o en el disco donde se ha perdido la información y ejecutar lo siguiente:

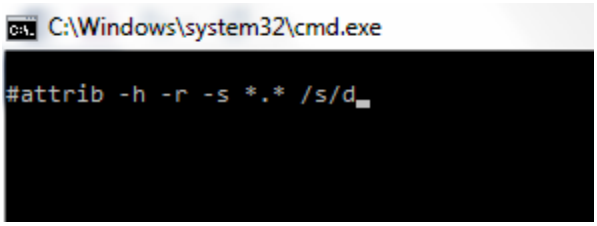



Figura 32. Comando attrib en cmd de Windows.

Lo que indicamos con este comando es que a todos los archivos con todas las extensiones que están en carpetas, en subcarpetas y que también a las propias carpetas les quite el atributo de solo lectura, de archivo de sistema y de oculto, y con esto nuestra información volverá al estado anterior.

Este tipo de problema depende mucho de cuánto daño o molestias quiera crear el atacante, ya que por ejemplo en el caso anterior bastaría ejecutar ese comando y se recuperaría la información, pero podría ser que el atacante una vez que ha ocultado nuestros archivos procediera a eliminarlos o a moverlos a otras carpetas todo depende de las intenciones de este.

Estos problemas dependen del ingenio y de las intenciones del atacante por ejemplo pueden eliminar la información o esconderla y tal vez lo más que ganan es hacer la maldad, pero también hay casos en los que las intenciones son más perversas.

La compañía de seguridad informática Kaspersky Labs anunció un virus extorsionador llamado virus GpCode que cifra los archivos del PC impidiendo su lectura, luego notifica al afectado que para obtener la clave usada para cifrar el material es necesario contactar a una dirección anónima de correo electrónico. La clave usada es de RSA de 1.024 bits y actualmente es imposible de romper.

El virus en cuestión cifra los archivos doc, txt, pdf, jpg y ccp. La raíz de los archivos intervenidos es modificada a .crypt y son subidas a un archivo de texto donde se indica que es necesario comprar una clave para recuperar el acceso a los archivos.

Los expertos de esta firma están abocados a detectar debilidades en el código del virus, con el fin de recuperar los archivos sin que sea necesario usar la clave.

Como este existen muchos casos en los que el usuario no puede hacer nada para recuperar su información ya que el cifrado que se usa para restringir el acceso a sus archivos es muy robusto y algunas veces llegan a ser hasta estándares de cifrado para algunos países.

### ***2.6 ROBO DE IDENTIDAD.***

*El robo de identidad* es cualquier clase de fraude que dé como resultado la pérdida de datos personales, como por ejemplo contraseñas, nombres de usuario, información bancaria o números de tarjetas de crédito.

El robo o usurpación de identidad es el hecho de apropiarse la identidad de una persona haciéndose pasar por ella, llegando a asumir su identidad ante otras personas, en un lugar público o privado, en general para acceder a ciertos recursos o la obtención de créditos y otros beneficios en nombre de esa persona.

El caso más común hoy en día se da cuando un atacante, por medios informáticos o personales, obtiene su información personal y la utiliza ilegalmente.

El robo de identidad es el delito de más rápido crecimiento en el mundo. Hasta no hace mucho tiempo, cuando un ladrón robaba la billetera o porta documentos, el dinero era lo único que pretendía. Eso está cambiando, ahora lo más valioso es el número de su documento, tarjeta de crédito, de débito, cheques y cualquier otro documento que contenga sus datos personales.

La tabla número 10, describe el procedimiento básico utilizado por un delincuente para robar la identidad de cualquier persona.

| | |
|---|---|
| Por lo general, este delito consta de tres etapas diferentes: | En la primera etapa, el delincuente obtiene información relativa a la identidad mediante, por ejemplo, programas informáticos dañinos o ataques destinados a la peska (Un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta) |
| | La segunda etapa se caracteriza por la interacción con la información obtenida antes de utilizarla en el marco de una actividad delictiva, como ocurre con la venta de ese tipo de información. |
| | La tercera etapa consiste en la utilización de la información relativa a la identidad en relación con una actividad delictiva. En la mayoría de los casos, con el acceso a esos datos los delincuentes pueden perpetrar nuevos delitos y, por ese motivo, dan menos prioridad al conjunto de datos propiamente dicho que a la capacidad para utilizarlos en actividades delictivas. Pueden citarse como ejemplo la falsificación de documentos de identidad o el fraude de las tarjetas de crédito. Los métodos aplicados para obtener datos, en el marco de la primera etapa, abarcan una gran variedad de acciones. |
| Hay varios tipos de datos que interesan a los delincuentes, | Número de la seguridad social (equivalente al número del documento nacional de identidad) utilizado en los Estados Unidos es un ejemplo clásico del tipo de dato de interés para los delincuentes. Los delincuentes pueden utilizarlo, de la misma forma que el número de pasaporte, para abrir cuentas financieras o apropiarse de las ya existentes, solicitar créditos o acumular deudas. |

| | |
|---|---|
| siendo los más importantes los siguientes: | Fecha de nacimiento, dirección y números de teléfono. Por lo general, estos datos sólo pueden utilizarse para el robo de identidad si van acompañados de otro tipo de información (por ejemplo, el NSS). El acceso a la información complementaria que representa la fecha de nacimiento y la dirección, puede servirle al delincuente para eludir procedimientos de verificación. |
| | Contraseña de cuentas no financieras. |
| | Contraseña de cuentas financieras. Como ocurre con los NSS, la información relativa a las cuentas financieras es un objetivo muy difundido en lo que atañe al robo de identidad, y se refiere a cuentas bancarias y de ahorro, tarjetas de crédito y de débito, así como a datos sobre planificación financiera. |

Tabla 10. Procedimiento y datos obtenidos en el robo de indentidad.

Se puede cometer este delito debido al escaso número de instrumentos necesarios para verificar la identidad de los usuarios por Internet. Resulta fácil identificar a las personas en el mundo real, pero la mayoría de los métodos de identificación en línea son más complejos. Las herramientas de identificación más modernas (por ejemplo, las que utilizan datos biométricos) son costosas y no están muy difundidas. Las actividades en línea tienen pocos límites y, por ello, el robo de identidad es fácil y rentable.

### ***2.6.1 Phishing.***

Phishing (pronunciado "fishing"), es decir, la suplantación de identidad, es un tipo de robo de identidad en línea. Usa el correo electrónico y sitios web fraudulentos diseñados para robar sus datos o información personal, como por ejemplo números de tarjetas de crédito, contraseñas, datos de cuentas u otra información.

Los estafadores podrían enviarle millones de mensajes de correo electrónico fraudulento con vínculos a sitios web fraudulentos que aparentemente provienen desde sitios web en los que la víctima confía, como su banco o compañía de tarjeta de crédito, solicitando que se proporcione información personal. Los delincuentes pueden usar esta información para cometer muchos tipos diferentes de fraude, tales como robar dinero desde una cuenta de banco, abrir nuevas cuentas a nombre de la víctima u obtener documentos oficiales mediante el uso de la identidad hurtada.

Hay varias maneras comunes que los spammers pueden obtener una dirección de correo electrónico:

- Navegando en la web, con el signo @. Los spammers y delincuentes cibernéticos utilizan herramientas sofisticadas para escanear la red y recopilar direcciones de correo electrónico.

- Utilizando herramientas para generar nombres de usuario comunes y un par de ellos con dominios comunes. Estas herramientas son similares a los que se utilizan para romper las contraseñas.
- El correo electrónico de la víctima, puede quedar almacenado en la bandeja de entrada de correo electrónico de alguna persona a la cual se le haya enviado un correo electrónico

alguna vez, o siempre. Los ciberdelincuentes utilizarán la ingeniería social para engañar a estas personas para que les den el acceso, o incluso robar esa información.

- Los spammers pueden comprar listas legal e ilegalmente.

### ***2.6.2 Métodos de defensa.***

Los criminales cibernéticos tienen muchas formas de robar información personal y dinero. Así como no se le daría a un ladrón la llave de casa, hay que asegurarse de tener protección contra el fraude y el robo de identidad en línea. Hay que descubrir los trucos comunes que los delincuentes emplean para saber protegerte del fraude en línea y del robo de identidad. Algunas de las medidas que hay que tener en cuenta son las siguientes:

- No responder si se detecta un mensaje de correo electrónico sospechoso, un mensaje instantáneo o una página web que solicita información personal o financiera
- Siempre tener cuidado con los mensajes o los sitios que piden información personal, o los mensajes que dirigen a una página web desconocida que pide cualquiera de los siguientes datos:

    - Nombres de usuario
    - Contraseñas
    - Números de Seguro Social
    - Números de cuentas bancarias
    - PIN (Números de identificación personal)
    - Números completos de tarjetas de crédito
    - Fecha de cumpleaños

- No llenar ningún formulario o pantalla de acceso que pueda provenir de esos mensajes.
- Si aparece un mensaje de alguien conocido, pero no parece de él, puede ser que su cuenta haya sido vulnerada por un criminal cibernético que está tratando de obtener dinero o información de la víctima, por lo que hay que tener cuidado con lo que se recibe.
- Nunca ingresar contraseñas cuando se llegue a un sitio mediante un vínculo en un correo electrónico o chat en el que no se tiene confianza
- No enviar contraseñas por correo electrónico y no compartirla con los demás
- Los sitios y servicios legítimos no piden que se envíen contraseñas por correo electrónico, por lo que no se debe responder a las peticiones de contraseñas para sitios en línea.
- Prestar mucha atención cuando se pide que acceda a su cuenta.
- Busca señales que indiquen la conexión con el sitio web: en primer lugar, mirar la barra de direcciones del navegador para ver si la URL parece real. También comprobar si la dirección web comienza con https://, lo que indica que la conexión al servidor es encriptada y más resistente a los espías y a la manipulación. Algunos navegadores también incluyen un ícono de candado en la barra de direcciones junto a https:// para indicar claramente que la conexión está encriptada y que se está conectado de forma más segura.

- Informar acerca de correos electrónicos sospechosos y trampas

La mayoría de los proveedores de correo electrónico, permiten hacer esto. Si se informa sobre un mensaje sospechoso al servidor de correo, se ayudará a bloquear a ese usuario para que no envíe más mensajes de correo electrónico y permitirá que la empresa proveedora del servicio de abuso detenga ataques similares.

### ***2.7 FRAUDE Y FRAUDE INFORMATICO.***

El fraude informático es uno de los delitos más populares cometidos por Internet, puesto que con la automatización y herramientas informáticas se pueden encubrir identidades delictivas.

Se puede definir como el delito informático realizado con la intención de engañar o perjudicar a una persona u organización y proporcionar un beneficio ilegitimo a quien lo realiza.

Gracias a la automatización, los delincuentes obtienen importantes beneficios a partir de un cierto número de pequeñas acciones. Aplican una estrategia que consiste en asegurar que la pérdida financiera de cada víctima esté por debajo de un cierto límite. Si tienen una "pequeña" pérdida, es menos probable que las víctimas inviertan tiempo y energía en dar a conocer e investigar esos delitos. Un ejemplo de este timo es la estafa nigeriana, que consiste en el pago de una suma por adelantado.

Aunque estos delitos se cometen utilizando tecnologías informáticas, la mayoría de los regímenes de derecho penal no los consideran delitos informáticos sino fraudes de carácter común. La distinción principal entre fraude informático y fraude tradicional consiste en el objetivo que se persigue. Si el estafador trata de manipular a una persona, se considera por lo general que el delito es un fraude; si su objetivo apunta a los sistemas informáticos o de procesamiento de datos, el delito suele catalogarse de fraude informático. Los regímenes de derecho penal que abarcan el fraude pero no contemplan aún la manipulación de sistemas informáticos con propósitos fraudulentos.

Los fraudes más habituales son, entre otros, los siguientes:

**1) Subasta en línea**

Son de los servicios más difundidos de cibercomercio. Los compradores tienen acceso a mercancías de los segmentos de mercado más especializados y variados del mundo entero.

Los ciberdelincuentes pueden explotar la ausencia del contacto cara a cara entre vendedores y compradores. Los dos timos más comunes son:

• ofrecer mercancías no disponibles para la venta y exigir su pago antes de la entrega; o

• adquirir mercancías y solicitar su envío, sin intención de pagar por ellas.

En respuesta los organizadores de subastas han creado sistemas de protección como, por ejemplo, el sistema de intercambio de información/comentarios. Después de cada transacción, compradores

y vendedores formulan comentarios que ponen a disposición de otros usuarios en calidad de información neutral sobre la fiabilidad de ambos.

Sin embargo, los delincuentes eluden esta protección recurriendo a cuentas de terceros o bien hablando positivamente de ellos mismos desde cuentas falsas.


Figura 33. Subasta en línea.

**2) Estafa nigeriana.**

En este tipo de fraude, los delincuentes envían mensajes electrónicos pidiendo ayuda a los destinatarios para transferir importantes cantidades de dinero a terceros con la promesa de darles un porcentaje si aceptan hacer esa operación a través de sus cuentas personales. Piden también que les transfieran a su nombre una pequeña cantidad de dinero para verificar los datos de la cuenta bancaria con la que se hará la transacción o que simplemente les envíen los datos de la cuenta bancaria. Hay pruebas que sugieren que esos mensajes electrónicos reciben miles de respuestas.

Según estudios en curso, y pese a diversas iniciativas y campañas de información, el número de víctimas y de pérdidas totales de dinero a causa de la estafa nigeriana sigue aumentando.

**3) Falsificación informática**

Por falsificación informática se entiende la manipulación de documentos digitales, por ejemplo:

- Crear un documento que parece provenir de una institución fiable;
- Manipular imágenes electrónicas
- Alterar documentos.

Estas conductas consisten en la manipulación ilícita, a través de la creación de datos falsos o la alteración de datos o procesos contenidos en sistemas informáticos, realizada con el objeto de obtener ganancias indebidas.

La tabla número 11, muestra distintos métodos para llevar a cabo la falsificación informática.

| | |
|---|---|
| Los distintos métodos para realizar estas conductas se deducen, fácilmente, de la forma de trabajo de un sistema informático: | En primer lugar, es posible alterar datos, omitir ingresar datos verdaderos o introducir datos falsos, en una computadora. Esta forma de realización se conoce como manipulación del input. |
| | En segundo lugar, es posible interferir en el correcto procesamiento de la información, alterando el programa o secuencia lógica con el que trabaja la computadora. Esta modalidad puede ser cometida tanto al modificar los programas originales, como al adicionar al sistema programas especiales que introduce el autor. |
| | Por último, es posible falsear el resultado, inicialmente correcto, obtenido por una computadora: a esta modalidad se la conoce como manipulación del output. |

Tabla 11. Métodos de falsificación informática.

Respecto a los objetos sobre los que recae la acción del fraude informático, estos son, generalmente, los datos informáticos relativos a activos o valores. En la mayoría de los casos estos datos representan valores intangibles (ej.: depósitos monetarios, créditos, etc.), en otros casos, los datos que son objeto del fraude, representan objetos corporales (mercadería, dinero en efectivo, etc.) que obtiene el autor mediante la manipulación del sistema. En las manipulaciones referidas a datos que representan objetos corporales, las pérdidas para la víctima son, generalmente, menores ya que están limitadas por la cantidad de objetos disponibles. En cambio, en la manipulación de datos referida a bienes intangibles, el monto del perjuicio no se limita a la cantidad existente sino que, por el contrario, puede ser «creado » por el autor.

En los fraudes informáticos se explotan las vulnerabilidades, es decir la información que deja un usuario a manera de huella y que es recabada por los hackers para establecer el perfil de las posibles víctimas y atacarlos. Tanto las empresas como los usuarios dejan información en la red sin protección, creyendo que no pueden convertirse en víctimas potenciales. Cada computadora tiene una dirección en el mundo, y existen herramientas que permiten indagar vulnerabilidades de las direcciones que son atractivas para el ataque, así es posible averiguar cuentas, uso de aplicaciones y rastrear a las víctimas.

Los atacantes ya no requieren una tecnología para cometer fraudes, sino que lo hacen mediante preguntas, técnicas de ingeniería social, espiando datos que dejen en el computador. Así como a través de redes sociales, correo electrónico o transacciones bancarias.

### ***2.7.1 Prevención y detección de fraudes.***

Las oportunidades para cometer fraudes existen, en diferentes grados, en casi todas las organizaciones que utilizan la informática y que presentan deficiencias en diferentes aspectos que influyen directa o indirectamente sobre la función informática.

Estos aspectos son:
- -Políticas de dirección
- -Controles administrativos
- -Control de personal
- -Control interno
- -Seguridad

La tabla número 12, describe los aspectos a tener en cuenta para la prevención de fraudes.

| | |
|---|---|
| **Políticas de dirección.** | Uno de los factores que se puede considerar a la hora de valorar las oportunidades para realizar un fraude es la ética o los estándares de conducta que sigue la organización. La política y la conducta fijada por la dirección establecen el ambiente en el que se trabaja. |
| **Controles administrativos.** | Aunque los controles administrativos deben establecerse en el marco de las políticas de dirección, inciden más específicamente en las reglas del día a día de los departamentos. Estas reglas tratan, preferentemente, de los procedimientos a seguir en la manipulación de datos. |
| **Control de personal.** | Al hablar de las fuentes del fraude, la mayoría son originados por personal interno de la organización. Por este motivo, debe ponerse especial énfasis en los controles de personal refiriéndonos tanto a las políticas de selección de nuevo personal como al seguimiento del ya existente. |
| **Control interno.** | El control interno comprende el plan de organización y el conjunto de métodos y procedimientos que aseguran el buen funcionamiento de la función informática. Se puede afirmar que los fraudes se realizan cuando los controles internos no existen, son débiles o son esquivados. Los controles pueden ser específicos de una aplicación, de un aspecto o generales de toda la función informática. |

Tabla 12. Prevención de fraudes informáticos.

Tener un sistema completamente seguro es casi imposible. Algunas razones por las que los sistemas en los que se ha establecido un plan de seguridad continúan siendo, en mayor o menor grado, vulnerables, son:

- La implantación de medidas de seguridad excesivas pueden llegar a dificultar la operación de la empresa.
- Pueden existir brechas en la seguridad que no se habían previsto.

- La empresa puede tener dificultades para afrontar los costos de las medidas de seguridad.
- El costo de las medidas puede ser superior a las pérdidas potenciales que evitarían
- La tecnología avanza más rápidamente que la evolución de la seguridad de una empresa

## *2.8 ATAQUES CONTRA LA INTEGRIDAD DEL SISTEMA*

Los ataques a los sistemas informáticos suscitan las mismas preocupaciones que los ataques a los datos informáticos. Cada vez hay más empresas que incorporan servicios Internet en sus procesos de producción, con lo que se benefician de una disponibilidad de 24 horas al día desde cualquier lugar del mundo. Al impedir que los sistemas informáticos funcionen correctamente, los infractores consiguen causar grandes pérdidas económicas a sus víctimas.

También es posible realizar ataques físicos a los sistemas informáticos. Si el delincuente tiene acceso físico al sistema informático, puede destruir los equipos. En la mayoría de las legislaciones penales, el daño físico no plantea mayores problemas, dado que son similares a los casos clásicos de daño o destrucción de propiedad. Ahora bien, en el caso de empresas de comercio electrónico muy rentables, las pérdidas económicas causadas a los sistemas informáticos son mucho mayores que el costo de los equipos informáticos.

Desde el punto de vista jurídico, resulta mucho más problemático el tema de los timos por la web.

Ejemplos de ataques a distancia contra sistemas informáticos son:

• Gusanos informáticos; o

• Ataques de denegación del servicio (DoS).

Los gusanos informáticos son programas informáticos que se reproducen de manera autónoma y que inician múltiples procesos de transferencia de datos con objeto de dañar la red. Su incidencia sobre los sistemas informáticos es la siguiente:

• En función de los efectos del gusano, la infección puede detener el buen funcionamiento del sistema informático y utilizar los recursos del sistema para reproducirse a sí mismo por Internet.

• La producción de tráfico de red adicional puede reducir la disponibilidad de ciertos servicios (por ejemplo, sitios web).

A diferencia de los gusanos informáticos que afectan generalmente a toda la red sin atacar directamente un sistema informático en particular, los ataques de DoS están dirigidos a sistemas informáticos concretos. Los ataques DoS hacen que los recursos informáticos queden indisponibles para los usuarios previstos. Al enviar a un sistema informático más solicitudes de las que puede gestionar, los infractores pueden impedir que los usuarios accedan a dicho sistema para consultar su correo, leer las noticias, reservar un vuelo o descargar archivos.

Estos ataques se pueden hacer con programas que se ejecutan en la PC del atacante o desde sitios web donde se introduce la IP del sitio a atacar y este sitio web envía las peticiones a la víctima haciendo un poco más difícil rastrear al atacante.


Figura 34. Ataque DoS.

### ***2.9 UTILIZACIÓN INDEBIDA DE DISPOSITIVOS***

Como se ha venido observando a lo largo de este capítulo para cometer un ciberdelito sólo hace falta un equipo sumamente básico y acceso a la red, por ejemplo en el caso del fraude en línea puede llevarse a cabo en un cibercafé. Pueden cometerse otros delitos más refinados utilizándose en ese caso herramientas informáticas especiales.

Todas las herramientas necesarias para cometer delitos más refinados pueden encontrarse en Internet generalmente en forma gratuita, muchas veces los atacantes crean sus propias herramientas, cuando tienen objetivos más complejos o quieren pasar desapercibidos más tiempo.

Las herramientas más modernas llegan a tener costo o incluso sólo son conocidas por unos cuantos, por ejemplo, en Internet se pueden buscar troyanos indetectables y en algunos sitios te ofrecen un programa que será indetectable por lo menos un mes, claro con un costo de varios cientos de dólares. Con ellas, los delincuentes pueden atacar otros sistemas informáticos pulsando tan sólo una tecla.

Los ataques más habituales son ahora menos eficaces ya que las empresas de programas informáticos de protección analizan las herramientas actualmente disponibles y se preparan para ese tipo de piratería. Los ataques de mayor resonancia suelen diseñarse exclusivamente para objetivos específicos. Pueden encontrarse herramientas informáticas para:

- Cometer ataques por denegación de servicio (DoS);
- Diseñar virus informáticos;
- Desencriptar información; y
- Acceder en forma ilegal a sistemas informáticos.

Con las actuales herramientas informáticas se ha logrado la automatización de muchos ciberdelitos, y los delincuentes pueden llevar a cabo numerosos ataques en muy poco tiempo. Además, las herramientas informáticas simplifican los ataques, de modo que hasta los usuarios menos experimentados pueden cometerlos. Con las herramientas disponibles para el correo basura, casi todos pueden enviar ese tipo de correo. Se cuenta también con herramientas para descargar archivos de los sistemas de intercambio de archivos o para colocarlos en ellos.

Cabe destacar que algunas de las aplicaciones que se ofrecen por Internet fueron creadas con el propósito de auditar una red o controlar tu propia computadora de forma remota, pero muchas de estas se usan con el propósito de hacer un ciberdelito.

# *3. DELITOS RELACIONADOS CON EL CONTENIDO.*

En el capítulo anterior se mostró a los equipos informáticos siendo herramientas y víctimas de ataques complejos los cuales pueden derivar en pérdidas económicas por ejemplo en un portal de pago expuesto a ataques SQL o XSS, o en pérdidas de información sensible, desde bases de datos empresariales hasta el correo electrónico personal de cualquier persona.

En este tercer capítulo se muestra al Internet y a los equipos de cómputo como herramientas para la elaboración de otros delitos desde pornografía hasta casinos en línea que, como se puede notar los delitos como tal son otros pero gracias a los sistemas informáticos tienen una mayor penetración en la sociedad.

## *3.1 MATERIAL ERÓTICO Y/O PORNOGRÁFICO.*

Pornografía en Internet abarca a toda la pornografía que se distribuye a través de las distintas tecnologías sobre las que Internet se apoya, principalmente vía sitios web, intercambio de archivos peer-to-peer o grupos de noticias Usenet. Si bien la pornografía ha formado parte de Internet desde los años 1980, fue la invención de la World Wide Web en 1991, así como la apertura de Internet al público general lo que condujo a una explosión de la pornografía online.

Al igual que las cintas de vídeo y los DVD, Internet se ha hecho popular en la distribución de pornografía porque permite que la gente vea pornografía de forma anónima en el confort y la privacidad de sus hogares. Por otro lado, también permite el acceso a la pornografía a gente cuyo acceso estaría restringido legalmente o por condiciones sociales.

El contenido sexual fue de los primeros en comercializarse por Internet, dado que presenta ventajas a los distribuidores minoristas de material erótico y pornográfico, en particular:

• Intercambiar medios (tales como imágenes, películas, cámaras en directo) ahorrándose los onerosos gastos de envío;

• Acceso mundial, que permite llegar hasta un número considerablemente mayor de clientes que en una tienda al por menor;

• Internet suele considerarse un medio anónimo (lo que a menudo es un error) -una característica que aprecian los consumidores de pornografía, en vista de las opiniones sociales preponderantes.

Según los estudios recientes, el número de sitios web dedicados a pornografía en Internet con acceso en cualquier instante asciende hasta 4,2 millones. Además de los sitios web, el material pornográfico puede distribuirse a través de:

• Sistemas de intercambio de archivos;

• En salas de charla cerradas.

En tan solo cinco minutos, habrá nacido, en Internet, un sitio de pornografía de los 300 que aparecen a diario en la Red de redes. También, más de 350 millones de personas estarán visitando uno de estos lugares entre portales comerciales, blogs, redes sociales, etc., que se dedican al erotismo de todo tipo.

Una medición independiente del portal Extremetech.com da cuenta de cuán grande y voluminosa es la pornografía en línea, que nació a la par de Internet, se materializó en los años 80 con el intercambio de arte erótico en redes privadas y se consolidó a comienzos de los 90, cuando, ya abierta al público, en la Web arrancaron los grupos de boletines y correos con fotos escaneadas de revistas porno.

En los años 80, Internet era una red cerrada aún, con muy poca capacidad de transmisión, en la que, por ende, la opción de transportar imágenes era muy reducida, aún más con videos.

Por ello, el 'arte ASCII' era la multimedia del momento, una forma de recrear imágenes a punta de caracteres y símbolos que, agrupados y 'artísticamente' acomodados, permitían 'pintar' cualquier cosa, entre esas: escenas eróticas.

En 1987 nació Rusty n Edie's BBS, un boletín en línea que alcanzó a tener 14.000 suscriptores (que pagaban 87 dólares al año) para recibir contenidos, principalmente eróticos sacados de la revista Playboy, emporio que les demandó y obligó a cerrar en menos de dos años.

En medio de listas de correos y boletines pequeños, dedicados al intercambio de erotismo, se registró en 1994 la dirección sex.com, el primer portal dedicado a la pornografía comercial, el cual fue el centro de una dura batalla legal (y hasta intriga policial) por su propiedad, por la cual pagaron alrededor de 15 millones de dólares.

Hoy, la pornografía en línea es amplia y variada. El mayor sitio de erotismo en la Red llega a surtir más de 1.000 GB de datos en video por segundo.

### *3.1.1. Estadísticas sobre la pornografía*

Para el año de 2013, se tenían las siguientes cifras en cuanto a pornografía, según el sitio web de MBA Online.

- 12% de los sitios de Internet son pornografía (24, 644,172)
    - 3% están hechas en Gran Bretaña.
    - 4% en Alemania.
    - 89% en Estados Unidos.
    - 4% en el resto de países del mundo.
- Cada segundo 3,075 dólares se gastan en pornografía
- Cada segundo hay 28258 usuarios viendo pornografía
- Cada segundo 372 personas escriben "adult" en las máquinas de búsqueda.
- 40 millones de estadounidenses visitan sitios pornográficos de manera regular
- 1 de cada 3 usuarios que ven pornografía son mujeres de estas 17% dicen ser muy adictas.

- El 70% de hombres entre 18-24 años visitan páginas pornográficas de manera típica cada mes
- En los estados unidos la pornografía deja ganancias anuales de 2,000MDD y en el mundo es de 4900 MDD
- 2.5 millones de e-mails son pornografía (al día), 8% de los e-mails que se mandan al día en el mundo
- 25% de todas las búsquedas en Internet son relacionadas con la pornografía, al día son 68 millones
- 35% de las descargas de Internet son pornografía
- De las búsquedas de pornografía en Internet el 75 millones es SEX, 30millones adult dating, 23 millones porn
- La edad en la que se comienza a ver pornografía regularmente es a los 11 años
- El día más popular para consumir pornografía son los domingos
- Cada 39 minutos, un nuevo vídeo de pornográfico es producido en los EEUU.
  Cada día se crean 266 nuevo sitios pornográficos en Internet.
- El 70% de las visualizaciones de pornografía en Internet se produce de 9 AM a 5 PM (jornada laboral).
- Visitantes a sitios pornográficos a nivel mundial: 72 millones anuales.
- Los motores de búsqueda obtienen unas 116. 000 solicitudes relacionadas con pornografía infantil.
- El 47% de familias Estadounidenses afirman que la pornografía es un problema en sus hogares.
- Solicitaciones sexuales de la juventud realizadas en salas de chat: 89%.
  Jóvenes que reciben solicitaciones/invitaciones sexuales por Internet: 20%.
- La industria de pornográfica en Internet tiene mayores ganancias que Microsoft, Google, Amazon, eBay, Yahoo, Apple y Netflix juntos.
  Sólo en EEUU, la pornografía de Internet produce más ganancias que la NFL, la Ligas Mayores de Baseball y la NBA.
- La capital de pornografía mundial es "San Fernando Valley".
  La web pornográfica con más tráfico es adultfriendfinder.
  Los paises que prohíben la pornografía son: Arabia Saudí, Irán, Bahréin, Egipto, Emiratos Árabes, Kuwait, Malasia, Indonesia, Singapur, Kenia, India, Cuba y China.

### ***3.1.2 Formas de distribución de la pornografía por Internet.***

En la Web existen alternativas tanto gratuitas como de pago a la hora de acceder a la pornografía. El ancho de banda requerido por un sitio web pornográfico es relativamente alto, y el beneficio que se puede obtener gracias a la publicidad puede no llegar a ser suficiente para satisfacer esa demanda, razón entre otras por la cual muchas empresas dedicadas al hosting establecen condiciones especiales cuando se trata de contenidos para adultos.

La popularidad del material pornográfico en Internet se ve en los números, cada segundo 28,258 personas buscan este tipo de material en línea.

Las cuatro formas de distribución más comunes que se pueden encontrar, se describen a continuación en la tabla número 13.

| ***Forma de distribución*** | ***Descripción*** |
|---|---|
| **TGP**<br>Los Thumbnail gallery post (galerías de miniaturas) | Son páginas que ofrecen una lista a menudo categorizada de pequeñas imágenes o thumbnails que enlazan con galerías cortas de entre diez y veinte imágenes. Una variante de este tipo de páginas son las MGP (Movie gallery post), que en lugar de ofrecer imágenes, ofrecen vídeos de corta duración (entre uno y tres minutos aproximadamente). Una práctica habitual es el intercambio de tráfico entre diferentes sitios TGP, de tal forma que no todas las imágenes mostradas enlazan a galerías reales, sino a otros sitios TGP. |
| **Listas de enlaces** | Al contrario que las galerías TGP/MGP, este tipo de sitios web no muestran imágenes sino enlaces con textos provocativos o estimulantes para el visitante. Al igual que en las galerías de imágenes, esta recopilación de enlaces aparece categorizada según la temática, y puede conducir a galerías gratuitas, a sitios de pago o a otras listas de enlaces. |
| **Usenet** | Otra fuente gratuita de pornografía en Internet son los grupos de noticias Usenet, pioneros en albergar dicho material. Sin embargo, entre sus desventajas se encuentran que tienden a presentar una organizada deficiente y a menudo los mensajes no están relacionados con el tema o son spam. |
| **Peer to peer** | Las redes de intercambio de archivos P2P constituyen otra forma de acceso gratuito a la pornografía. Aunque muchas de estas redes se han asociado ampliamente al intercambio ilegal de música y películas con copyright, la compartición de pornografía también constituye un uso muy popular de las mismas. Algunos sitios comerciales han reconocido esta tendencia y distribuyen contenidos propios de ejemplo en redes peer-to-peer. |

Tabla 13. Distribución de la pornografía en Internet.

En ocasiones, es posible que algunos sitios web contengan código malicioso, como virus o spyware, o que ofrezcan la descarga de pequeños programas para, en principio, facilitar la conexión a un sitio web determinado o el visionado de vídeos. Esto lleva a la descarga de *dialers* o troyanos que pueden suponer un costo elevado al visitante o poner en peligro datos del usuario. Es por tanto aconsejable visitar este tipo de sitios web con los complementos y lenguajes de scripting del navegador desactivados, como pudieran ser Java, JavaScript o ActiveX, y prestar especial cuidado en la ejecución de todo contenido descargado.

### ***3.1.3. Presentaciones típicas de contenido pornográfico.***

- **Imágenes**

Probablemente el formato de distribución más común sean las imágenes, generalmente en formato JPEG. Estas imágenes encuentran sus principales fuentes en revistas pornográficas escaneadas, fotografías tomadas con cámaras digitales o en vídeos que se dividen en frames.

- **Videos**

Al contrario que en la distribución tradicional basada en películas completas con varias escenas, en la web es más común encontrar cortos de vídeo con escenas individuales. Los formatos de vídeo más populares son MPEG, WMV y Quick Time. Menos común es la distribución web de imágenes completas de VCD o DVD, si bien por p2p es algo más común.

Otra opción que ofrecen algunos sitios web comerciales es la posibilidad de acceder a los vídeos vía streaming a través del navegador web.

- **Webcams**

Otro formato de contenido para adultos que ha emergido con la llegada de Internet ha sido el de las cámaras web. En comparación con las fotografías y los vídeos, es único en el sentido de que no existe un equivalente offline, y por tanto es posterior a la popularización de la red. En general, se pueden distinguir dos categorías del servicio: shows ofrecidos a miembros de un sitio de pago, y sesiones privadas 1-a-1, generalmente ofrecidas en régimen de pay per view. El formato de vídeo más popular para el streaming de cámaras en directo es Flash Video.

- **Otros formatos**

Otros formatos incluyen el texto y el audio. En el primero de los casos, consiste en la distribución de relatos eróticos vía web, foros, grupos de noticias o email, en ocasiones intercalando imágenes para ambientar la experiencia. Respecto al audio, se puede distinguir entre sonidos de personas practicando sexo o bien personas leyendo relatos eróticos.

## ***3.2 PORNOGRAFÍA INFANTIL.***

Se denomina pornografía infantil a toda representación de menores de edad de cualquier género en conductas sexualmente explícitas. Puede tratarse de representaciones visuales, descriptivas (por ejemplo en ficción) o incluso sonoras.

Tradicionalmente, se consideran como pornografía infantil a aquellas representaciones fotográficas o fílmicas en formatos digital o analógico de menores de edad de cualquier sexo en conductas sexualmente explícitas ya sea solos o interactuando con otros menores de edad o con adultos.

Sin embargo cuando se trata de pornografía infantil, ésta se encuentra expresamente definida en el protocolo facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la

prostitución infantil y la utilización de niños en la pornografía de Organización de las Naciones Unidas, en los siguientes términos:

*Artículo 2 A los efectos del presente Protocolo: c) Por pornografía infantil se entiende toda representación, por cualquier medio, de un niño dedicado a actividades sexuales explícitas, reales o simuladas, o toda representación de las partes genitales de un niño con fines primordialmente sexuales.*

El Consejo de Europa define la pornografía infantil como "*cualquier material audiovisual que utiliza niños en un contexto sexual*" (Recomendación R (91) 11 e Informe del Comité Europeo de Problemas Delictivos (1993).

La literatura erótica infantil debe quedar deslindada de la pornografía infantil, por cuanto constituye un concepto diverso que alude a materiales relacionados con niños en los que están presentes alegorías o propósitos sexuales, lo que no es objeto de prohibición legal en los ordenamientos estatales.

### ***3.2.1 Producción y difusión de la pornografía infantil motivada por Internet.***

En la década de los años setenta puede situarse el momento de máximo apogeo de la producción comercial de pornografía infantil en el mundo occidental. En aquellos años Dinamarca, Holanda y Suecia constituían los principales centros de producción. A finales de dicha década y comienzos de los años ochenta se verifica una mayor intervención gubernamental y el impulso de medidas legislativas, centradas en la prohibición de la producción, la venta y distribución, de la pornografía infantil. Desde los años noventa se ha acrecentado la adopción de medidas legislativas prohibitivas y el impulso de la represión penal sobre las actividades de producción, difusión, exhibición y distribución de material pornográfico infantil al compás de la evolución tecnológica, y no faltan además muestras de una "nueva cruzada legislativa" en la que incluso se opta por la incriminación de la mera tenencia o posesión de material pornográfico infantil.

En la actualidad se constata una tendencia según la cual el tráfico de pornografía infantil no viene presidido por el ánimo de lucro ni por motivos comerciales. Se ha acrecentado así el intercambio de material entre pedófilos, pauta de comportamiento que se ha ampliado en Internet, donde los usuarios pueden introducir material y convertirse en difusores de dicho material. Por consiguiente, puede trazarse una línea evolutiva que desplaza la elaboración y producción de la pornografía infantil de parámetros comerciales organizados a ámbitos descentralizados amateurs y domésticos. A esta evolución ha contribuido también el denominado "turismo sexual", pues se ha constatado en los últimos tiempos que una buena parte de la elaboración de material pornográfico infantil tiene su origen en filmaciones amateurs llevadas a cabo por turistas que entablan relaciones con menores, principalmente en países del continente asiático.

### ***3.2.2 Técnicas de difusión de la pornografía infantil.***

Las técnicas de producción e introducción de tal material en la Red se han multiplicado (escaneado de fotos, introducción en la Red de videoclips, correos electrónicos provistos de imágenes o vídeos).

Y estas nuevas formas de difusión y tráfico de pornografía infantil pueden ser llevados a cabo desde el anonimato que proporciona Internet.

Entre las formas más comunes, se encuentran las siguientes:

- Anonymous remailers
- Computer Bulletin Boards
- Comunicaciones en línea (chats en vivo)
- Alteración de imágenes por computadora

Al alcance del usuario mínimamente avanzado se halla la utilización de ***los anonymous remailers***, que permiten el envío de correos electrónicos sin remitente; los remailers suponen el uso de servidores de correo electrónico intermedios entre el remitente y el destinatario final, de modo que el remitente envía un mensaje a un servidor que, a la vez, lo reenvía al destinatario final sin que aparezcan los datos del remitente.

El empleo de los denominados ***computer bulletin boards*** ("tablones de anuncios de computadora") también puede constituir otro mecanismo de intercambio de información entre pedófilos por el hecho de que permiten mantener conversaciones; debe subrayarse además que, en la mayoría de los países, no se requiere licencia ni registro para introducir dichos tablones de anuncios.

Las posibilidades que ofrece Internet se proyectan también en la posibilidad de mantener ***comunicaciones en línea***, con incorporación de imágenes, a través de las denominadas sesiones interactivas de chat, mediante las cuales los menores pueden quedar involucrados en un contexto sexual con adultos.

Frente a tales peligros las normas de autorregulación de usuarios y operadores de la Red aconsejan acrecentar medidas de autoprotección para los usuarios menores, por medio de técnicas de bloqueo al acceso infantil a materiales que incorporan contenidos nocivos. Sin embargo, las medidas de bloqueo que pueden incorporarse a los programas de software pueden quedar vulneradas por los menores con conocimientos informáticos.

Por último, la evolución de la informática permite la ***alteración de imágenes por computadora***, de modo que se puede enmascarar la imagen de adultos que participan en actos pornográficos o de contenido sexual para que parezcan menores de edad; se trata de la denominada pornografía técnica. Este tipo de pornografía presenta una menor lesividad en la medida que no utiliza menores reales en la elaboración del material.

### ***3.2.3 Pseudopornografia de menores***

La pseudopornografía de menores, consiste en la alteración de imágenes por medio de la colocación de la cara de un menor sobre la imagen de un adulto o bien en el añadido de objetos a una imagen; en tales casos, siempre que se incorporen, aunque sea parcialmente, imágenes de menores reales, la lesividad de la conducta es mayor y probablemente debe ser objeto de sanción penal.

La venta de material de pornografía infantil es muy lucrativa, dado que los coleccionistas están dispuestos a pagar grandes cantidades por películas e imágenes que muestren niños en un contexto

sexual. Los motores de búsqueda permiten encontrar este tipo de material con rapidez. La mayor parte de este material se intercambia en foros cerrados protegidos con contraseña, a los que difícilmente pueden acceder los usuarios ordinarios de Internet y las fuerzas de seguridad. Así pues, las operaciones secretas son esenciales para luchar contra la pornografía infantil.

Hay dos factores básicos de la utilización de las TIC que plantean dificultades en la investigación de delitos relacionados con el intercambio de pornografía infantil, a saber:

- ***La utilización de divisas virtuales y pagos anónimos:***

El pago en dinero en efectivo por ciertas mercancías permite al comprador ocultar su identidad, razón por la cual es el modo de pago predominante muchas actividades delictivas. La demanda de pagos anónimos ha dado lugar a la aparición de sistemas de pago virtual y divisas virtuales. Al pagar con divisas virtuales no se exige la identificación y la validación, lo que impide a las fuerzas de seguridad rastrear el intercambio de divisas para encontrar a los delincuentes. Las recientes investigaciones sobre pornografía infantil han conseguido dar con los infractores siguiendo la pista de los pagos efectuados por éstos. Sin embargo, cuando los infractores efectúan pagos anónimos resulta difícil rastrearlos.

- ***La utilización de tecnología de cifrado:***

Los autores de estos delitos recurren cada vez más al cifrado de sus mensajes. Las fuerzas de seguridad se han percatado de que los infractores utilizan técnicas de cifrado para proteger la información almacenada en sus discos duros, lo que dificulta sobremanera las investigaciones penales.

Además de una penalización general de los actos relacionados con la pornografía infantil, se está estudiando la posibilidad de recurrir a otros métodos, tales como imponer a los proveedores de servicios Internet la obligación de registrar a los usuarios o de bloquear o filtrar el acceso a sitios web que contengan contenido de pornografía infantil.

Un informe sociológico presentado por la Fundación Alia2 en 2011 reveló que Estados Unidos, España y México eran los principales países con mayor número de producción y distribución de pornografía infantil a través de la web, material que incluye fotografías, negativos, diapositivas, revistas, libros, dibujos, películas, videos y archivos o discos de computadora.

### ***3.3. RACISMO, LENGUAJE OFENSIVO.***

El racismo se entiende como la exacerbación o defensa del sentido racial de un grupo étnico, especialmente cuando convive con otro u otros, así como designa la doctrina antropológica o la ideología política basada en este sentimiento.

La discriminación racial es un concepto que suele identificarse con el de racismo y que lo abarca, aunque se trata de conceptos que no coinciden exactamente. Mientras que el racismo es una ideología basada en la superioridad de unas razas o etnias sobre otras, la discriminación racial es un acto que, aunque suele estar fundado en una ideología racista, no siempre lo está. En este sentido hay que tener en cuenta que la discriminación racial positiva (cuando se establecen discriminaciones con el fin de garantizar la igualdad de las personas afectadas), constituye una forma de discriminación destinada a combatir el racismo.

El racismo suele estar estrechamente relacionado y ser confundido con la xenofobia, es decir el "odio, repugnancia u hostilidad hacia los extranjeros". Sin embargo existen algunas diferencias entre ambos conceptos, ya que el racismo es una ideología de superioridad, mientras que la xenofobia es un sentimiento de rechazo; por otra parte la xenofobia está dirigida sólo contra los extranjeros, a diferencia del racismo. El racismo también está relacionado con otros conceptos con los que a veces suele ser confundido, como el etnocentrismo, los sistemas de castas, el clasismo, el colonialismo, el machismo e incluso la homofobia.

Las actitudes, valores y sistemas racistas establecen, abierta o veladamente, un orden jerárquico entre los grupos étnicos o raciales, utilizado para justificar los privilegios o ventajas de las que goza el grupo dominante

### ***3.3.1 Definición de la UNESCO.***

El racismo es el resultado de diferentes teorías pseudocientíficas, que afirman la existencia de diversas razas en la especie humana y las clasifican con arreglo a un orden jerárquico. Según el preámbulo de la Convención Internacional sobre la Eliminación de todas las Formas de Discriminación Racial, adoptada en 1965, "*toda doctrina de superioridad basada en la diferenciación racial es científicamente falsa, moralmente condenable y socialmente injusta y peligrosa, y [...] nada en la teoría o en la práctica permite justificar, en ninguna parte, la discriminación racial*".

Asimismo, en el Artículo 2 de la Declaración de la UNESCO sobre la Raza y los Prejuicios Raciales de 1978, se dice que "*el racismo engloba las ideologías racistas, las actitudes fundadas en los prejuicios raciales, los comportamientos discriminatorios, las disposiciones estructurales y las prácticas institucionalizadas que provocan la desigualdad racial, [y] se manifiesta por medio de disposiciones legislativas o reglamentarias y prácticas discriminatorias, así como por medio de creencias y actos antisociales*".

### ***3.3.2 Racismo en Internet.***

Los grupos radicales utilizan los medios de comunicación de masas, como Internet, para divulgar propaganda. El número de sitios web con contenido racista y lenguaje ofensivo ha aumentado recientemente, según un estudio realizado en 2005 el número de páginas web con apología del racismo, la violencia y la xenofobia aumentó en un 25 por ciento entre 2004 y 2005. En 2006 existían en Internet más de 6 000 sitios web de este tipo.

La distribución por Internet ofrece varias ventajas a los delincuentes, tales como los menores costos de distribución, la utilización de equipos no especializados y una audiencia mundial. Aparte de la propaganda, Internet se utiliza para vender ciertas mercancías, por ejemplo artículos relacionados con la ideología nazi, como banderas con símbolos, uniformes y libros, que se ponen a disposición en plataformas de subastas y cibertiendas especializadas.

También se utiliza Internet para enviar mensajes de correo electrónico y boletines informativos y para distribuir vídeos y programas de televisión por lugares populares tales como YouTube. Estos actos no están penalizados en todos los países.

En algunos países, este tipo de contenido está protegido por el principio de libertad de expresión.

Las opiniones son divergentes respecto hasta qué punto el principio de libertad de expresión es aplicable a ciertos temas, lo que a menudo dificulta las investigaciones de ámbito internacional. Un ejemplo de conflicto de legislaciones fue el caso en que estuvo implicado el proveedor de servicios Yahoo! en 2001, cuando un tribunal francés dictó a Yahoo! (con sede en Estados Unidos) que bloqueara el acceso de usuarios franceses a material nazi. En virtud de la primera enmienda a la Constitución de Estados Unidos, la venta de este tipo de material es legal en este país. En aplicación de la primera enmienda, un tribunal de Estados Unidos decidió que la orden dictada por el tribunal francés no podía aplicarse contra Yahoo! en Estados Unidos.

La discrepancia de opiniones entre los países sobre estos asuntos quedó patente durante la redacción del Convenio sobre la Ciberdelincuencia del Consejo de Europa. La finalidad de este Convenio es armonizar la legislación en materia de ciberdelincuencia para garantizar que las investigaciones de alcance internacional no se vean obstaculizadas por la divergencia en las legislaciones. Las Partes que entablaron negociaciones no pudieron llegar a un consenso acerca de la penalización del material xenófobo, de modo que este tema quedó excluido del Convenio y se aborda por separado en un Primer Protocolo. De lo contrario, algunos países (con inclusión de Estados Unidos) no lo hubieran firmado.

El día 27 de marzo de 1995, se lanzó la primera página WEB racista, llamada “Orgullo Blanco Mundial” a cargo de un expresidiario, partidario del Ku Klux Klan, de nombre Black Stormfront.

La siguiente gráfica, tomada del sitio http://dimencionesdescubiertas.blogspot.mx, muestra el crecimiento que ha tenido el contenido racista en Internet, desde el año de 1995 y hasta 2009; se observa un aumento exponencial en el aumento de este contenido, principalmente causado por el aumento de páginas de Internet, el aumento en el número de usuarios, y la no persecución a este tipo de contenido.


Figura 35. Crecimiento de los sitios web que hacen apología del racismo.

Utilizando el mismo tiempo, la posibilidad del anonimato y llegar a millones de usuarios de Internet, el racismo se ha extendido de forma intensiva en el mundo digital durante los últimos diez años. A través de discursos de índole racista, revisionistas o neonazistas, millares de sitios, blogs,

comunidades virtuales de Orkut y MySpace han diseminado el odio racial a la intolerancia. En varios países, la divulgación del racismo, incluso por medio Internet, es un crimen, ya que se caracteriza por la legislación propia de distintos sistemas legales. Algunos sitios tratan de defender el derecho a la libertad de expresión y dicen que no se consideran racistas, simplemente expresan opiniones divergentes.

Quienes defienden este tipo de pensamiento sugieren diversas maneras de cómo mantener el material fuera del alcance de las autoridades. Por esta característica, muchos sitios, principalmente los alojados en sistemas gratuitos con una clara política acerca de estos contenidos, permiten remover fácilmente todo el contenido generado pero, sin embargo, pueden llegar a volver a reaparecer en nuevos servidores o dominios con alojamiento en el extranjero.

La nueva ola de discriminación racista por Internet es una réplica de cómo la sociedad es capaz de exhibir sus ideales y sus pensamientos antisociales en una esfera donde se escudan con la posibilidad de no ser conocidos.

## *3.4 EXALTACIÓN DE LA VIOLENCIA. CIBERACOSO.*

### *3.4.1 Ciber-bullying*

Es el Bullying que se lleva a cabo utilizando medios socio-digitales, como computadoras, celulares, asistentes personales (PDAs), iPods, iPads, consolas de videojuegos, etcétera, a través de servicios como el correo electrónico, la mensajería instantánea, sitios de redes sociales, mensajes cortos (SMS) de celular, publicaciones digitales de texto (Blogs) o videos, etcétera.

Se llaman medio socio-digital porque en el formato digital, nos ponen en contacto con todo lo que nos rodea, amigos, familia, servicios, contenido, etcétera. Siendo estrictos, además de lo anterior, el Ciber –bullying también debe reunir las características del bullying:

- Violencia
- Reiteración
- Desbalance de fuerza o poder.

Es importante aclarar que la definición de Bullying podría no ser apropiada para definir simples ofensas interpersonales, ni llamarlo Ciber-bullying cuando estas suceden en Internet.

Por ejemplo, si en un partido de futbol se desata una pelea entre jóvenes de la misma edad y condiciones físicas, es claro que no reúne las características de Bullying, y tampoco lo es cuando dos muchachos se pelean a la salida de la escuela porque les gusta la misma niña, o porque juegan de forma brusca.

En el caso de Internet, no se considera Ciber-bullying si una persona escribe de pronto un comentario negativo sobre nosotros, o publica una foto que de alguna forma nos moleste, pero puede llegar a considerarse si dichos comentarios o publicaciones se vuelven repetitivos y tienen la intención de causarnos un daño.

En todo caso, el término correcto para definir molestias eventuales, o agresiones interpersonales en línea, sería "Hostigamiento en línea", y podríamos categorizarlo como Ciber-bullying, sólo en el caso que se vuelvan reiterativas, y que incluyan violencia física o psicológica.

El concepto de "Desbalance de fuerza o poder" requiere de mayor aclaración. En el caso del Bullying, este concepto se refiere a la mayor fuerza física que un estudiante tiene, y que aprovecha abusivamente para lograr intimidar a los demás, que no están en posibilidad de defenderse, pero en el caso del Ciber-bullying, es verdad que un estudiante corto de estatura, y físicamente débil, puede lanzar fuertes agresiones y provocar un profundo dolor por publicaciones en línea, sin requerir de ninguna fuerza física, afectando si quiere, al más grande y fuerte de su escuela.

El "Desbalance de fuerza o poder" en este caso se refiere a las habilidades técnicas del agresor, no presentes en la víctima –o no disponibles-, y que igualmente le impiden defenderse.

### ***3.4.2 Características del ciberacoso.***

- Requiere destreza y conocimientos sobre Internet. Esta información la obtiene principalmente de foros informáticos.
- Falsa acusación: La mayoría de los acosadores intentan dañar la reputación de la víctima manipulando a gente contra él.
- Publicación de información falsa sobre las víctimas en sitios web. Pueden crear sus propias webs, páginas de redes sociales (páginas de Facebook), blogs o fotologs para este propósito. Mientras el foro donde se aloja no sea eliminado, puede perpetuar el acoso durante meses o años. Y aunque se elimine la web, todo lo que se publica en Internet se queda en la red.
- Recopilación de información sobre la víctima: Los ciberacosadores pueden espiar a los amigos de la víctima, su familia y compañeros de trabajo para obtener información personal. De esta forma saben el resultado de los correos difamatorios, y averiguan cuales son los rumores más creíbles de los que no crean ningún resultado.
- A menudo monitorizarán las actividades de la víctima e intentarán rastrear su dirección de IP en un intento de obtener más información sobre ésta.
- Envían de forma periódica correos difamatorios al entorno de la víctima para manipularlos.
- Manipulan a otros para que acosen a la víctima. La mayoría tratan de implicar a terceros en el hostigamiento. Si consigue este propósito, y consigue que otros hagan el trabajo sucio hostigándole, haciéndole fotos o vídeos comprometidos, es posible que use la identidad de éstos en las siguientes difamaciones, incrementando así la credibilidad de las falsas acusaciones, y manipulando al entorno para que crean que se lo merece. A menudo la víctima desconoce la existencia de estos hechos, debido al silencio de los testigos. Incluso el acosador puede decir que la víctima ya conoce estas fotos/vídeos, para intentar evitar que algún testigo le informe; incrementando así las sospechas y creando una falsa paranoia en la víctima.
- El acosador puede trasladar a Internet sus insultos y amenazas haciendo pública la identidad de la víctima en un foro determinado (blogs, websites), incluso facilitando en algunos casos sus teléfonos, de manera que gente extraña se puede adherir a la agresión.

- Quizá acuse a la víctima de haberle ofendido a él o a su familia de algún modo, o quizá publique su nombre y teléfono para animar a otros a su persecución.
- Falsa victimización. El ciberacosador puede alegar que la víctima le está acosando a él.
- Ataques sobre datos y equipos informáticos. Ellos pueden tratar de dañar la computadora de la víctima enviando virus.
- No necesita la proximidad física con la víctima. El 'ciberacoso' es un tipo de acoso psicológico que se puede perpetrar en cualquier lugar y momento sin necesidad de que el acosador y la víctima coincidan ni en el espacio ni en el tiempo. Por ejemplo, quien abusa puede mandar una amenaza desde cientos de kilómetros a medianoche y quien lo recibe lo hará a la mañana siguiente cuando abra su correo electrónico.

## ***3.5 DELITOS CONTRA LA RELIGIÓN.***

Son cada vez más, los sitios web con material que algunos países consideran que atenta contra la religión, por ejemplo declaraciones antirreligiosas por escrito. Si bien cierto tipo de material corresponde a los hechos objetivos y a la tendencia, esta información se considera ilícita en algunas jurisdicciones. Otros ejemplos son la difamación de religiones o la publicación de caricaturas.

Internet ofrece ventajas a las personas interesadas en criticar o debatir acerca de un determinado asunto, ya que se pueden formular comentarios, publicar material o artículos sin que los autores estén obligados a revelar su identidad. Muchos grupos de debate se basan en el principio de libertad de expresión. La libertad de expresión es uno de los factores esenciales que explican el éxito de Internet y, de hecho, existen portales creados específicamente para el contenido generado por los usuarios. Si bien es fundamental proteger este principio, incluso en los países más liberales existen condiciones y leyes que rigen la aplicación del principio de libertad de expresión.

La divergencia de normas jurídicas sobre contenido ilícito denota los problemas que entraña la reglamentación del contenido. Incluso en los países donde la publicación de contenido está contemplada en las disposiciones relativas a la libertad de expresión, es posible acceder al material publicado desde otros países con reglamentación más estricta. La publicación de doce caricaturas en el periódico danés Jyllands-Posten generó protestas generalizadas en el mundo Islámico.

Al igual que en el caso del contenido ilícito, la disponibilidad de cierta información o material es un delito penal en algunos países. La protección de las diferentes religiones y símbolos religiosos varía de un país a otro. Algunos países penalizan la formulación de observaciones peyorativas sobre el Sagrado Profeta o la profanación de copias del Corán, mientras que otros adoptan una posición más liberal y no penalizan tales actos.

Algunos ejemplos de sitios web que llevan a cabo esta práctica son:

**Sinfest** es un webcómic escrito y dibujado por el artista de tiras cómicas Tatsuya Ishida. La primera tira apareció el 17 de enero de 2000 en la página web de Sinfest, aunque fue impresa el 16 de octubre de 1991 en el periódico de la Universidad de California, donde Ishida se encontraba.

Con 4580 tiras en la actualidad, Sinfest tiene una temática de comedia basada en la naturaleza humana y sus características, tales como amor, sexo, roles de género, adicciones y sobre

todo religiones, teniendo numerosas referencias y bromas teológicas y una constante sátira de la religión.

El cómic se compone principalmente de sátira religiosa, a menudo criticando los argumentos de la religión, los textos religiosos y decretos y las acciones de los creyentes. Como los rasgos cómicos sólo figuras cristianas y musulmanas, éstas se dirigen generalmente en las dos religiones, aunque algunos se aplican a muchas formas de teísmo.

El Proyecto "***LOLCat traducción de la Biblia***" es un sitio web basado en wiki creada en julio de 2007 por Martin Grondin, donde los editores apuntan a la parodia de toda la Biblia en "broma", popularizado por el fenómeno de Internet LOLcat "Laughing out loud" o sea gatos riendo a carcajadas.

### ***3.6 APUESTAS ILEGALES EN LÍNEA.***

Las apuestas por Internet son uno de los campos que experimenta un mayor crecimiento en este medio. Según Linden Labs, el creador del juego en línea "Segunda Vida", se han abierto unos diez millones de cuentas.

Los Informes muestran que algunos de estos juegos se han utilizado para cometer delitos, en particular:

- Intercambio y presentación de pornografía infantil
- Fraude
- Casinos en línea
- Difamación (por ejemplo, escribir mensajes difamatorios o calumnias).

Según las estimaciones, los ingresos en concepto de juegos en línea por Internet pasará de 3 100 millones USD en 2001 a 24 000 millones USD en 2010 (si bien es cierto que comparadas con las cifras que mueve el juego tradicional, éstas son relativamente pequeñas).

La reglamentación del juego dentro y fuera de Internet varía de un país a otro -una laguna legislativa que aprovechan tanto los infractores como los negocios legales y casinos. El efecto de la diversidad legislativa resulta evidente en Macao. Tras haber sido devuelta por Portugal a China en 1999, Macao se ha convertido en una de los destinos para el juego más importantes del mundo. Los ingresos anuales en 2006 se estimaron en 6 800 millones USD, llegando a superar a Las Vegas (6 600 millones USD). El éxito en Macao se debe al hecho de que el juego es ilegal en China por lo que miles de ludópatas de la China continental se desplazan a Macao para jugar.

#### ***3.6.1. Casinos en línea.***

Internet permite a las personas burlar las prohibiciones de juego. Los casinos en línea han proliferado, la mayoría de los cuales se encuentran en países con legislación liberal o sin normativa

sobre el juego por Internet. Los usuarios pueden abrir cuentas en línea, transferir dinero y participar en juegos de azar.

### ***3.6.2. Lavado de dinero.***

Los casinos en línea también pueden utilizarse para lavar dinero y financiar el terrorismo. Al efectuar apuestas en casinos en línea que no mantienen registros o que están ubicados en países sin legislación contra el lavado de activos, resulta difícil para las fuerzas de seguridad determinar el origen de los fondos.

Resulta difícil a los países con restricciones de juego controlar la utilización o las actividades de los casinos en línea. Internet está socavando las restricciones jurídicas de los países sobre el acceso por los ciudadanos a los juegos en línea. Ha habido varios intentos de impedir la participación en los juegos en línea, en particular la Ley de 2006 de prohibición del juego por Internet en Estados Unidos cuya finalidad es limitar el juego en línea ilícito mediante la incriminación de proveedores de servicios financieros que se encargan de la liquidación de transacciones relacionadas con el juego ilícito.

### ***3.6.3 Apuestas inseguras.***

Uno de los puntos que suele preocupar a los jugadores es la privacidad de sus datos. Y es que se enfrentan al problema de que no saben dónde están almacenados los datos, ni qué medidas se están tomando para protegerlos.

El “problema” viene cuando los datos están fuera del país de donde se lleva a cabo esta actividad, ya que no se ajustan a los mismos controles. Por otro lado, para asegurar que los datos de los jugadores viajan de forma segura por Internet, la mayoría de portales de juego implementan una solución basada en el estándar de comunicaciones seguras SSL (Secure Sockets Layer; direcciones que empiezan por “https”).

Ese problema reside en que no todas las implementaciones de SSL son igual de seguras, ya que el protocolo ha ido evolucionando, mejorando y solucionando errores que podrían permitir a un atacante espiar las acciones realizadas por los jugadores. Por último, en relación a los procesos de registro, ninguno de los casinos comprobados, permitía la autenticación mediante algún DNI (Documento Nacional de Identidad) electrónico, que sería la forma más segura de proceder. Los resultados de este segundo estudio destacan la importancia de concienciar a los usuarios de juegos online de que existen peligros en los videojuegos y casinos en la red y que, contrariamente a lo que se pensaba hasta hace poco tiempo, el malware está atacando a los videojuegos en todas las plataformas. Las previsiones no son mucho mejores para los próximos años y se espera que los ataques a juegos online sean mucho más frecuentes y masivos.

## ***3.7 DIFAMACIÓN E INFORMACIÓN FALSA***

Internet puede utilizarse para divulgar información errónea con la misma facilidad que la información fidedigna. Los sitios web pueden contener información falsa o difamatoria, especialmente en los foros y salas de charla donde los usuarios pueden publicar sus mensajes sin la verificación de los moderadores. Los menores utilizan cada vez más los foros web y los sitios de

relaciones sociales donde también puede publicarse este tipo de información. El comportamiento delictivo puede consistir, por ejemplo, en la publicación de fotografías de carácter íntimo o información falsa sobre hábitos sexuales. En muchos casos, los infractores se aprovechan de que los proveedores que ofrecen la publicación económica o gratuita no exigen la identificación de los autores o no la verifican, lo que complica la identificación de los mismos. Además, los moderadores de foros controlan muy poco o nada el contenido publicado. No obstante, ello no es óbice para que se hayan desarrollado proyectos interesantes tales como Wikipedia, una enciclopedia en línea creada por los usuarios, que cuenta con procedimientos estrictos de control de contenido.

Ahora bien, los delincuentes pueden utilizar esta misma tecnología para:

- Publicar información falsa (por ejemplo, sobre los rivales);
- Difamar (por ejemplo, escribir mensajes difamatorios o calumnias);
- Revelar información confidencial (por ejemplo, publicar secretos de Estado o información comercial confidencial).

### ***3.7.1 Peligros de la difusión de información falsa.***

La difamación puede dañar la reputación y la dignidad de las víctimas en un grado considerable, dado que las declaraciones en línea son accesibles por la audiencia mundial. Desde el momento en que se publica la información en Internet el autor o autores pierden el control de la información. Aunque la información se corrija o se suprima poco después de su publicación, puede haber sido duplicada ("en servidores espejo") y esté en manos de personas que no desean retirarla o suprimirla. En tal caso, la información permanecerá en Internet aunque la fuente original de la misma se haya suprimido o corregido. Como ejemplo puede citarse el caso de mensajes de correo electrónico "fuera de control", que reciben millones de personas con contenido obsceno, erróneo o falso acerca de personas u organizaciones, que quizá nunca puedan reponerse del daño causado a su reputación, con independencia de la veracidad o falsedad del mensaje original. Por consiguiente, es preciso llegar a un equilibrio entre la libertad de expresión y la protección de las posibles víctimas de calumnias.

Actualmente existe un sinfín de sitios web donde se pueden publicar comentarios o quejas de cualquier cosa y no es necesario que se revelen tus datos verdaderos, algunas muy famosas son:

http://www.apestan.com

http://www.quejasydenuncias.com/

http://www.quejasonline.com/


Figura 36. Sitio web Apestan.com, el principal sitio web para difamación.

## ***3.8 CORREO BASURA Y AMENAZAS CONEXAS***

Se llama ***spam, correo basura o sms basura*** a los mensajes no solicitados, no deseados o de remitente desconocido.

Todos aquellos que tengan una dirección de correo electrónico reciben a diario varios mensajes publicitarios que no son solicitados sobre cosas que no interesan. Actualmente, se calcula que entre el 60 y el 80% de los mails (varios miles de millones de mails por día) que se envían son no solicitados, es decir, spam.

Por lo general, las direcciones son robadas, compradas, recolectadas en la web o tomadas de cadenas de mail. Aunque hay algunos spammers que envían solamente un mensaje, también hay muchos que bombardean todas las semanas con el mismo mensaje que nadie lee.

La mayoría de las veces si se contesta el mail pidiendo ser removido de la lista, lo único que hace es confirmar que su dirección existe. Por lo tanto, es conveniente no responder nunca a un mensaje no solicitado.

Si utiliza un programa (clientes de correo) para recibir sus correos como Outlook, The Bat, Mozilla Thunderbird, etc, se recomienda utilizar un programa antispam que le ayudara a filtrar estos correos molestosos.

Aunque se puede hacer spam por distintas vías, la más utilizada entre el público en general es la basada en el correo electrónico. Otras tecnologías de Internet que han sido objeto de correo basura incluyen grupos de noticias, usenet, motores de búsqueda, redes sociales, páginas web wiki, foros, web logs (blogs), a través de ventanas emergentes y todo tipo de imágenes y textos en la web.

El correo basura también puede tener como objetivo los teléfonos móviles (a través de mensajes de texto) y los sistemas de mensajería instantánea como por ejemplo Outlook, Lotus Notes, Windows live , etc.

También se llama correo no deseado a los virus sueltos en la red y páginas filtradas (casino, sorteos, premios, viajes, drogas, software y pornografía), se activa mediante el ingreso a páginas de comunidades o grupos o acceder a enlaces en diversas páginas o inclusive sin antes acceder a ningún tipo de páginas de publicidad.

De todas formas, el spam ha tomado una resemantización dentro del contexto de foros, siendo considerado spam cuando un usuario publica algo que desvirtúa o no tiene nada que ver con el tema de conversación. También, en algunos casos, un mensaje que no contribuye de ninguna forma al tema es considerado spam. Una tercera forma de Spamming en foros es cuando una persona publica repetidamente mensajes acerca de un tema en particular en una forma indeseable (y probablemente molesta) para la mayor parte del foro. Finalmente, también existe el caso en que una persona publique mensajes únicamente con el fin de incrementar su rango, nivel o número de mensajes en el foro.

### ***3.8.1 Técnicas de spam.***

- **Obtención de direcciones de correo**

- Los spammers (individuos o empresas que envían correo no deseado) utilizan diversas técnicas para conseguir las largas listas de direcciones de correo que necesitan para su actividad, generalmente a través de robots o programas automáticos que recorren Internet en busca de direcciones. Algunas de las principales fuentes de direcciones para luego enviar el correo basura son:
- Los propios sitios web, que con frecuencia contienen la dirección de su creador, o de sus visitantes (en foros, blogs, etc.).
- Los grupos de noticias de usenet, cuyos mensajes suelen incluir la dirección del remitente.
- Listas de correo: les basta con apuntarse e ir anotando las direcciones de sus usuarios.
- Correos electrónicos con chistes, cadenas, etc. que los usuarios de Internet suelen reenviar sin ocultar las direcciones, y que pueden llegar a acumular docenas de direcciones en el cuerpo del mensaje, pudiendo ser capturadas por un troyano o, más raramente, por un usuario malicioso.
- Páginas en las que se solicita tu dirección de correo (o la de "tus amigos" para enviarles la página en un correo) para acceder a un determinado servicio o descarga.

- **Entrada ilegal en servidores.**

Por ensayo y error: se generan aleatoriamente direcciones, y se comprueba luego si han llegado los mensajes. Un método habitual es hacer una lista de dominios, y agregarles "prefijos" habituales, como lo son online, net, best, etc.

- **Envío de los mensajes.**

Una vez que tienen una gran cantidad de direcciones de correo válidas (en el sentido de que existen), los spammer sutilizan programas que recorren la lista enviando el mismo mensaje a todas las direcciones. Esto supone un costo mínimo para ellos, pero perjudica al receptor (pérdidas económicas y de tiempo) y en general a Internet, por consumirse gran parte del ancho de banda en mensajes basura.

- **Verificación de la recepción**

Además, es frecuente que el remitente de correo basura controle qué direcciones funcionan y cuáles no por medio de web bugs o pequeñas imágenes o similares contenidas en el código HTML del mensaje. De esta forma, cada vez que alguien lee el mensaje, su computadora solicita la imagen al servidor de susodicho remitente, que registra automáticamente el hecho. Son una forma más de spyware. Otro sistema es el de prometer en los mensajes que enviando un mensaje a una dirección se dejará de recibirlos: cuando alguien contesta, significa no sólo que lo ha abierto, sino que lo ha leído.

- **Troyanos y computadoras zombis**

Recientemente, han empezado a utilizar una técnica mucho más perniciosa: la creación de virus troyanos que se expanden masivamente por computadoras no protegidas (sin cortafuegos). Así, las computadoras infectadas son utilizados por el remitente de correo masivo como "computadoras zombis", que envían correo basura a sus órdenes, pudiendo incluso rastrear los discos duros o correos nuevos (sobre todo cadenas) en busca de más direcciones. Esto puede causar perjuicios al usuario que ignora haber sido infectado (que no tiene por qué notar nada extraño), al ser identificado como spammer por los servidores a los que envía spam sin saberlo, lo que puede conducir a que no se le deje acceder a determinadas páginas o servicios. Así, con la potencia de cálculo de todos las computadoras es infectados, pueden mandar el spam fácilmente sin que se enteren los propios usuarios, y pueden incluso mandar un virus a la computadora de una empresa importante.

Actualmente, el 40% de los mensajes no deseados se envían de esta forma.

- **Servidores de correo mal configurados**

Los servidores de correo mal configurados son aprovechados también por los remitentes de correo no deseado. En concreto los que están configurados como Open Relay. Estos no necesitan un usuario y contraseña para que sean utilizados para el envío de correos electrónicos. Existen diferentes bases de datos públicas que almacenan las computadoras es que conectadas directamente a Internet permiten su utilización por susodichos remitentes. El más conocido es la Open Relay DataBase.

El éxito en la detección de correo basura depende de los cambios en la forma de distribución. En lugar de enviar mensajes desde un solo servidor de correo (que para los proveedores del servicio de correo electrónico sería muchos más fácil de identificar, al tratarse de un número reducido de fuentes), la mayoría de los infractores utilizan redes zombi (botnets) para distribuir correo electrónico no solicitado. Al recurrir a redes zombi (o robot) constituidas por miles de sistemas informáticos, cada computador envía sólo unos cientos de mensajes.

Por ese motivo, resulta más difícil a los proveedores de este servicio analizar la información sobre los remitentes y a las fuerzas de seguridad seguir la pista de los delincuentes. El correo basura es una actividad muy lucrativa ya que el costo de enviar miles de millones de correo es bajo, y aún menor cuando se utilizan redes zombi. Algunos expertos opinan que la única solución real en la lucha contra el correo indeseado es aumentar el costo de envío para los remitentes.

### ***3.8.2 Consejos para prevenir el Spam***

La dirección de correo electrónico es el medio más utilizado para registrar la identidad de una persona en Internet y suele servir de base para la acumulación de información en torno a la misma. En muchas ocasiones contiene información acerca de la persona como el apellido, la empresa donde trabaja o el país de residencia. Esta dirección puede utilizarse en múltiples lugares de la red y puede ser conseguida fácilmente sin nuestro conocimiento, por lo que es necesario seguir una serie de normas para salvaguardar nuestra privacidad.

**- Ser cuidadoso al facilitar la dirección de correo**

Facilitar únicamente la dirección de correo a aquellas personas y organizaciones en las que confía y aquellas con las que quiera comunicar.

**- Utilizar dos o más direcciones de correo electrónico**

Es aconsejable crear una dirección de correo electrónica, que será la que se debe proporcionar en aquellos casos en los que no se confíe o conozca lo suficiente al destinatario. De este modo, su dirección personal será conocida únicamente por sus amigos o por sus contactos profesionales, con el ahorro de tiempo que implica no tener que separar correos importantes de aquellos no deseados. Lo mismo se recomienda a la hora de utilizar servicios de mensajería instantánea.

**- Elegir una dirección de correo poco identificable.**

Los spammers obtienen las direcciones de correo electrónico de formas muy diferentes. Así navegando por la red, en salas de chat e IRC, o incluso en directorios de contactos o usando la ingeniería social. A veces compran incluso listas de correo electrónico en sitios web que venden los datos de sus clientes. Y, cuando todo esto falla, simplemente conjeturan. Las direcciones de correo electrónico que se refieren a una persona como tal, suelen contener algún elemento que les identifique y son fáciles de recordar.

***¿Qué hacer si ya recibe Spam?***

Una vez que se empieza a recibir Spam, es casi imposible detenerlo completamente sin recurrir a un cambio de dirección de correo electrónico. De todas formas, se recogen una serie de recomendaciones que pueden ser aplicados para reducir la proliferación del "correo basura".

**- No dar click sobre los anuncios de los correos basura.**

Entrando en las páginas web de los spammers podemos demostrar que nuestra cuenta de correo está activa, con lo que puede convertirse en un objetivo para nuevos envíos. Por otra parte, los gráficos e imágenes (también llamados web bugs –incluidos en los correos basura pueden proporcionar al spammer no sólo la información de que el mensaje ha sido recibido, sino también datos de carácter personal como la dirección IP.

**- Programas de filtrado de correo electrónico.**

Los programas de gestión de correo electrónico, así como muchas páginas web de correo, ofrecen la posibilidad de activar filtros que separan el correo deseado del Spam. Las principales desventajas son que puede confundir correos legítimos con mensajes basura. Cada vez se fabrican programas más avanzados en este campo, que en muchos casos pueden ser descargados libremente de Internet. Estos filtros reciben instrucciones para definir qué tipo de correos se quiere recibir y cuales son considerados como Spam.

**- Filtros basados en ISP**

Muchos proveedores de Internet ofrecen soluciones que pueden llegar a ser muy efectivas a la hora de bloquear el Spam. Utilizan combinaciones de listas negras y escaneado de contenidos para limitar la cantidad de Spam que llega a las direcciones. El principal inconveniente es que, en ocasiones, bloquean correos legítimos, y además suelen ser servicios de pago.

## ***3.9 OTRAS FORMAS DE CONTENIDO ILÍCITO***

Internet no sólo se utiliza para ataques directos, sino también como foro para:

- Solicitar, ofrecer e incitar el crimen;
- La venta ilegal de productos; y
- Dar información e instrucciones para actos ilícitos (por ejemplo, sobre cómo construir explosivos).

Muchos países han reglamentado el comercio de ciertos productos. Cada país aplica distintas reglamentaciones nacionales y restricciones al comercio de los diversos productos, por ejemplo, el material militar. La situación es similar en el caso de los medicamentos - algunos medicamentos pueden comprarse sin restricciones en unos países mientras que en otros se precisa receta médica. El contrabando dificulta el control de ciertos productos restringidos en un territorio. Dada la popularidad de Internet, este problema va en aumento. Las tiendas por las web situadas en países sin restricción alguna pueden vender productos a clientes de otros países, menoscabando así esas limitaciones.

Antes de que apareciera Internet, era difícil conseguir instrucciones sobre construcción de armas. La información estaba disponible (por ejemplo, en libros sobre los aspectos químicos de los explosivos), pero conseguirla llevaba mucho tiempo. Hoy en día, la información sobre cómo construir explosivos está disponible en Internet.

### *3.9.1 Ejemplos de aplicación.*

En la página www.metacafe.com/watch/.../how_to_make_a_homemade_bomb/ existen varios videos donde muestran cómo hacer bombas caseras, y aunque no son peligrosas son un buen comienzo para aquellos que necesiten ideas para actos vandálicos.

Otro ejemplo es la página http://ellasenlacalle.blogspot.mx/ donde se hacen publicidad e incluso muestran sus tarifas y el lugar donde se encuentran.

De igual modo esta la página www.quebarato.com.mx/ en la cual puedes encontrar desde comida, autos, cosas, hasta prostitutas, donde se muestran con fotos para mayores de edad y dan sus datos para que las contactes.

También la web está repleta de páginas web para hacer explosivos caseros algunos ejemplos son las siguientes: www.taringa.net/posts/info/5197983/Como-hacer-explosivos-caseros.html

## *3.10 DELITOS EN MATERIA DE DERECHOS DE AUTOR.*

### *3.10.1 Piratería.*

#### 3.10.1.1 Definición de la UNESCO:

*El término "piratería" abarca la reproducción y distribución de copias de obras protegidas por el derecho de autor, así como su transmisión al público o su puesta a disposición en redes de comunicación en línea, sin la autorización de los propietarios legítimos, cuando dicha autorización resulte necesaria legalmente. La piratería afecta a obras de distintos tipos, como la música, la literatura, el cine, los programas informáticos, los videojuegos, los programas y las señales audiovisuales.*

Tradicionalmente, la piratería consistía en la reproducción y distribución no autorizadas, a escala comercial o con propósitos comerciales, de ejemplares físicos de obras protegidas. No obstante, el rápido desarrollo de Internet y la utilización masiva en línea, no autorizada, de contenidos protegidos, en la que con frecuencia no existe el elemento "comercial", han suscitado un intenso debate. La cuestión acerca de si dicho uso es un acto de "piratería" y si se debe abordar de la misma manera que la piratería tradicional, constituye el eje del debate actual sobre el derecho de autor. Están surgiendo distintos puntos de vista, a menudo divergentes, y las respuestas a la cuestión difieren de un país a otro.

### 3.10.1.2 Definición de la Procuraduría General de la República.

La Procuraduría General de la República, en el Acuerdo Nacional contra la Piratería suscrito el 15 de junio de 2006, señala que por piratería debe entenderse toda aquella producción, reproducción, importación, comercialización, venta, almacenamiento, transportación, arrendamiento, distribución y puesta a disposición de bienes o productos en contravención a lo establecido en la Ley Federal del Derecho de Autor y en la Ley de la Propiedad Industrial.

*Piratería es cometer acciones delictivas contra la propiedad, como hacer ediciones sin permiso del autor o propietario.*

La Piratería tiene efectos nocivos en la sociedad, ya que no solo por este fenómeno se pierden miles de fuentes de trabajo, sino que además llegan a afectar a la salud (medicamentos piratas) o pueden ocasionar daños que hacen perder nuestro patrimonio (los discos piratas dañan los stereos o las luces de navidad pirata llegan a ocasionar incendios), la actitud de adquirir productos piratas puede traernos múltiples problemas.

### *3.10.2 Piratería informática.*

La piratería informática es la copia y distribución ilegal de fuentes o software. Las causas por las que se piratea pueden ser simplemente para uso personal y evitar los costos de los productos originales y con licencia, o el caso más grave todavía es el que hace de la piratería un negocio. Sea cual sea la intención o si se hace de modo deliberado o no, la piratería es un delito y está castigado por la ley.

La descarga o distribución ilícita en Internet de copias no autorizadas de obras, tales como películas, composiciones musicales, videojuegos y programas informáticos se conoce, por lo general, como piratería cibernética o en línea. Las descargas ilícitas se llevan a cabo mediante redes de intercambio de archivos, servidores ilícitos, sitios Web y computadoras pirateadas. Los que se dedican a la piratería de copias en soporte físico también utilizan Internet para vender ilegalmente copias de DVD en subastas o sitios Web.

A pesar de que el tráfico de obras protegidas por el derecho de autor utilizando medios electrónicos cada vez más complejos, tales como las redes de intercambio de archivos P2P, los espacios para charla en Internet y los grupos de debate, tiene repercusiones cada vez más negativas en las industrias culturales, también se aduce el argumento de que frenar dicho fenómeno limitaría el derecho de acceso a la información, el conocimiento y la cultura.

Hay diferentes formas de piratería informática:

-***Duplicados de usuarios con licencia para usuarios sin licencia:*** cuando se copia el software sin haber adquirido la cantidad necesaria de licencias, entonces se están infringiendo las leyes de copyright (hacer una copia de un programa de un amigo).

-***Distribución ilegal a través de Internet.*** Los sitios Web que ofertan descargas gratuitas suelen distribuir ese software de manera ilegal.

-***Distribución de fuentes o software falsos.*** Al comprar software a través de Internet muchos distribuidores que venden en Internet venden productos ilegales a sabiendas, si el precio es demasiado bajo es probable que sea falso y puede acompañarse de defectos de calidad.

### ***3.10.3 Algunos datos relevantes sobre piratería informática:***

- Se estima que 23.76 de todo el tráfico de Internet involucra material que infringe los derechos de autor.
- El BitTorrent constituye el 17.9 de todo el tráfico de Internet. El estimado es que más del 60% es contenido compartido ilegalmente.
- Los sitios como Rapidshare, Megaupload y Hotfile, llamados cyberlockers, representan el 7% del todo el tráfico de Internet. El estimado es que más del 70% es contenido compartido ilegalmente.
- El tráfico de video streaming alcanza el 25% de todo el tráfico de Internet. Aquí solo el 5.3% involucra contenido ilegal.

Esta es la gráfica completa, según nos muestra el sitio web http://angelbc.files.wordpress.com/, actualizada a diciembre de 2011.

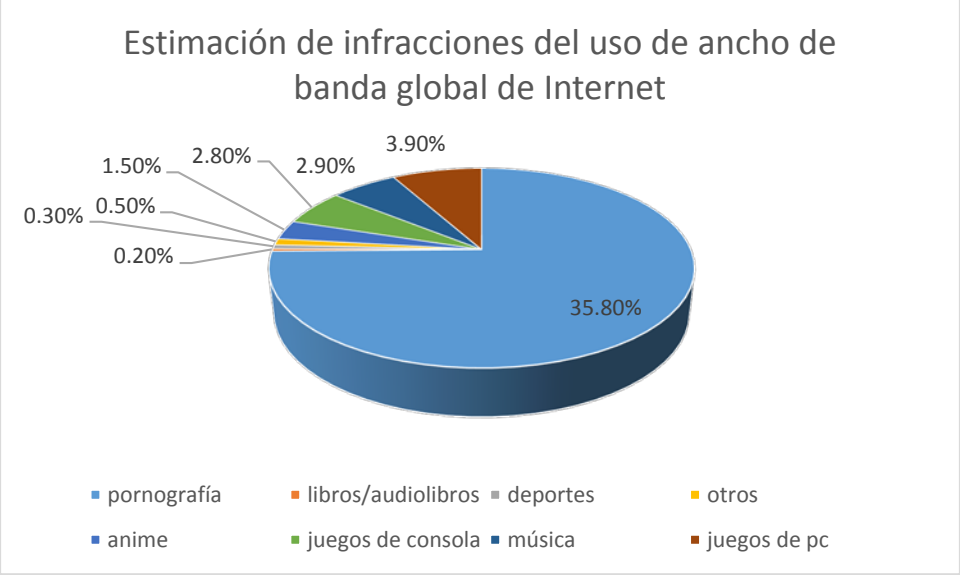



Figura 37. Porcentaje de productos pirata obtenidos vía Internet.

Se puede observar que en estas cifras ilegales no se incluye la pornografía, misma que queda incluida dentro del uso legal del ancho de banda de Internet. Según el estudio las dificultades para saber qué tanto es ilegal y qué no los hicieron tomar esta decisión. Así que asuman que ese 23.76% es potencialmente mayor.

Como verán BitTorrent es el método favorito para poder descargar material. Sin embargo queda la pregunta de ¿qué exactamente es lo que se está descargando? Para responder esto se analizaron los 10,000 archivos más populares en BitTorrent y se llegó a esta gráfica.

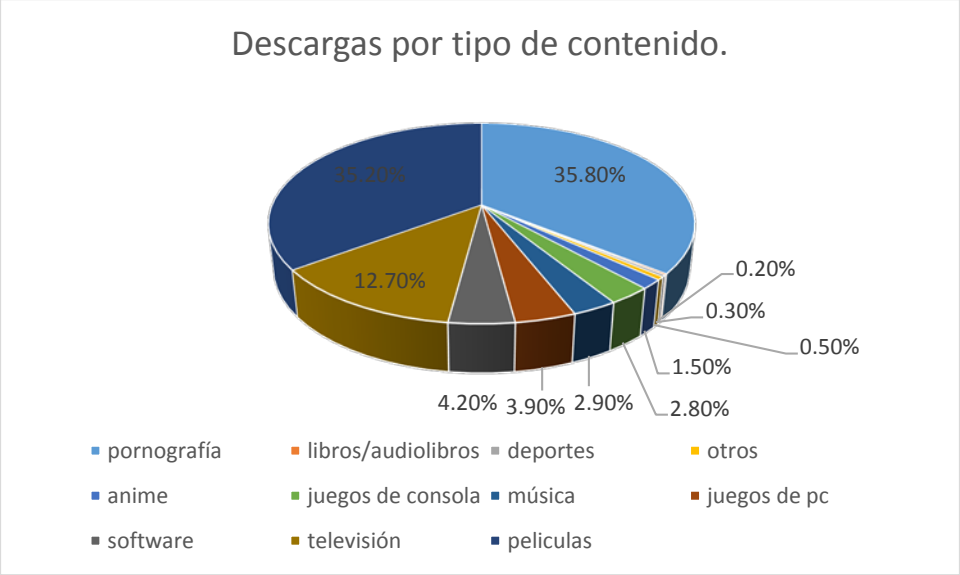



Figura 38. Descargas ilegales por contenido, diciembre de 2011.

- La música es de las cosas menos descargadas, con solo 2.9% de los archivos.
- La pornografía está en primer lugar, con 35.8% de los archivos.
- Las películas le siguen de cerca con 35.2%.
- En un lejano tercer lugar con 12.7% están programas de televisión.

Hoy día, la música en Internet es algo fácilmente disponible, pero sobre todo legal. Con tiendas virtuales como iTunes, y servicios como Pandora, Spotify, Grooveshark y muchos otros no es necesario ya estar descargando nada. Con una inversión pequeña es posible disfrutar de toda la música que se desee sin mayores dificultades.

### ***3.10.4 Productos mayormente pirateados.***

En Internet, pueden encontrarse muchos productos que son objeto de la piratería; sin embargo, hay algunos que son fácilmente distribuibles dentro de la red, como lo son los que a continuación se describen en la tabla número 14.

| ***PRODUCTO*** | ***DESCRIPCION*** |
|---|---|
| Libros | El sector editorial es el que por más tiempo se ha enfrentado a la piratería. Cualquier utilización no autorizada de una obra protegida por el derecho de autor, como un libro, un manual escolar, un artículo de periódico o una partitura, constituye una violación del derecho de autor o un caso de piratería, a menos que dicha utilización sea objeto de una excepción a ese derecho. La piratería de las obras impresas afecta tanto a las copias en papel como a las de formato digital. |
| Música | El hecho de cargar ilegalmente y poner a disposición del público archivos musicales o de descargarlos utilizando Internet, se conoce como piratería del ciberespacio o en línea. Dicho tipo de piratería también puede comprender ciertos usos de tecnologías relacionadas con el "streaming", que es la distribución de multimedia a través de una red de computadoras de manera que el usuario consume el producto, generalmente archivo de video o audio, en paralelo mientras se descarga. |
| Software | La piratería de programas informáticos denota los actos relacionados con la copia ilícita de dichos programas. Reproducción sin previa autorización del autor de software que se encuentre en línea, debe considerarse como piratería de software. |
| Películas | Como en el caso de la música, la piratería cinematográfica puede ser tradicional o perpetrarse mediante Internet. Esta práctica abarca, de manera no exclusiva, la piratería de vídeos y DVD, las filmaciones con videocámaras en salas de cine, el hurto de copias de películas destinadas a los cines, el robo de señales y la piratería de radiodifusión, así como la piratería en línea. |

Tabla 14. Productos mayormente pirateados.

### *3.11 DELITOS EN MATERIA DE DERECHOS DE AUTOR.*

La comúnmente denominada "piratería" es una actividad ilícita que afecta los derechos de autor, entendidos estos como la facultad exclusiva de los creadores intelectuales para explotar por sí o por terceros las obras de su autoría.

Bajo el concepto de propiedad intelectual se tutela a las obras literarias, artísticas, musicales, cinematográficas, fotográficas, arquitectónicas, programas de cómputo, entre otras (propiedad intelectual), así como lo relativo a las patentes, certificados de invención, marcas para productos o servicios, dibujos o modelos industriales y la competencia desleal (propiedad industrial).

El atentado más común contra la propiedad intelectual e industrial es el que afecta el derecho de reproducción y su distribución a escala comercial. Esta reproducción ocasiona no solamente daños al derecho moral de los autores, que consiste en la creación, divulgación, publicación, corrección o modificación, destrucción, etc., sino también el derecho patrimonial de los autores, que consiste en la reproducción, disposición, plusvalía, etc.

Una **infracción de derechos de autor**, **infracción de copyright** o **violación de copyright** es un uso no autorizado o prohibido de obras cubiertas por las leyes de derechos de autor, como el derecho de copia, de reproducción o el de hacer obras derivadas.

Algunos de las infracciones más comunes a los derechos de autor mediante herramientas informáticas se describen en la tabla número 15.

| ***TIPO DE PIRATERIA*** | ***DESCRIPCION*** |
|---|---|
| **Piratería del usuario final** | La forma más común de la piratería, el usuario final o la organización copian el software en más equipos de los que el acuerdo de la licencia permite (por defecto cada máquina que utiliza el software debe tener su propia licencia). |
| **Piratería de carga de disco duro** | Los distribuidores de equipos informáticos sin escrúpulos cargan previamente software sin licencia en los equipos, y no suministran a sus clientes las licencias necesarias. |
| **Piratería de falsificación y de CD-ROM** | Los vendedores ilegales, que con frecuencia se organizan en redes delictivas, transmiten software falso como si fuera auténtico, intentando emular el embalaje del producto con el nombre de la empresa y las marcas comerciales. |
| **Piratería por Internet** | Se trata de cualquier tipo de piratería que implique la distribución electrónica no autorizada o la descarga desde Internet de programas de software con copyright. |

Tabla 15. Infracciones más comunes en materia de derechos de autor.

### *3.11.1 Infracciones a los derechos de autor utilizando métodos cibernéticos.*

Como se mencionó anteriormente, las facilidades y bondades que ofrece Internet para la distribución de material son muchos y muy diversos; la música, los libros, las películas, sea cual sea su contenido o clasificación, así como software no libre, son las principales víctimas de este tipo de distribuciones.

A continuación, en la tabla número 16, se muestran las formas más comunes de "subir" este material a la red, describiendo las formas de distribución utilizadas por los piratas cibernéticos para distribuir todo este material.

| ***MEDIO DE DISTRIBUCION*** | DESCRIPCION | RIESGOS | EJEMPLOS |
|---|---|---|---|
| ***Programas P2P.*** | Este tipo de programas, utiliza una red común (por lo general diferente para cada producto), para comunicar entre si las computadoras de sus | Uno de los peligros, es el intercambio de archivos que no son lo que dicen ser, o que directamente se tratan de virus, gusanos o troyanos camuflados. Existen decenas de ejemplos, y es una de las más importantes fuentes de propagación e infección. | **KaZaA**<br>**Ares**<br>**LimeWire** |

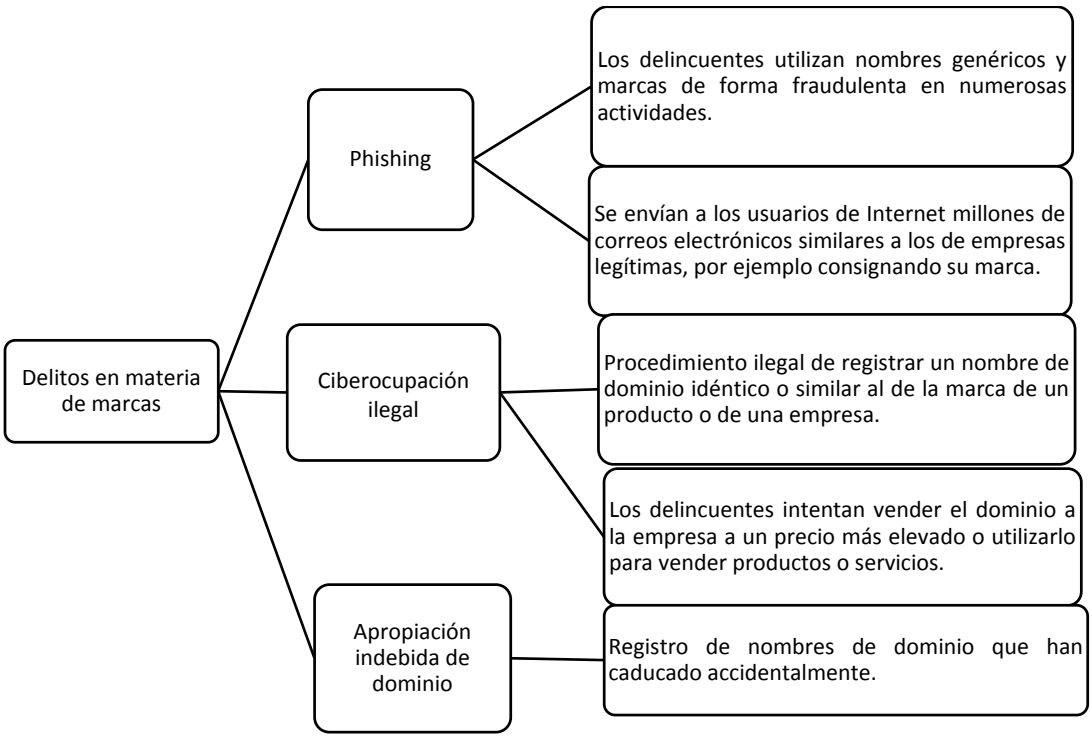
| | | | |
|---|---|---|---|
| | usuarios, los que comparten ciertos directorios, donde se encuentran los archivos a intercambiar. | Pero tal vez más grave, sea la instalación de otros programas no deseados (Spywares o Adwares), que estas aplicaciones esconden. | |
| ***Servidores de compartición de archivos.*** | Los servidores de compartición de archivos, son computadores que reciben toda clase de información relacionada con cualquier cosa: puede ser música, programas, videos, películas, libros, etc., las cuales son "subidas" a ese servidor por los usuarios que previamente se han registrado en la página, y descargada por gente que puede ser usuaria o no del sitio donde se alojen estos archivos. | Este tipo de sitios, es de los que más fomentan la piratería, puesto que no hay una forma precisa de regular este tipo de acciones, y es prácticamente imposible que los administradores de estos servidores se den cuenta de qué tipo de archivos (ya sea tengan copyright o no) son los que su servidor está alojando. Y en algunos casos, los mismos administradores de esos servidores son los que están fomentando la piratería. | Megaupload<br><br>Rapidshare<br><br>Mediafire |
| ***Modificación del software instalado en equipos móviles (Jailbreak)*** | Es un proceso que permite a los usuarios de los usuarios de algún sistema operativo en particular (puede ser iOS o Windows Phone) desbloquear su dispositivo para correr aplicaciones distintas a las de las tiendas autorizadas, así como instalar extensiones de aplicaciones que aumentan las funcionalidades del sistema no proporcionadas de manera oficial por las compañías armadoras. | Vulnerabilidad contra virus informáticos y hackers malintencionados que pueden acceder con mayor facilidad a los datos contenidos en el teléfono.<br><br>Pérdida de garantía: al modificar el software en el teléfono, cualquier garantía obtenida en la compra del teléfono se pierde, lo cual ocasiona graves problemas en el caso de descompostura de fabriación del teléfono.<br><br>Errores: los teléfonos quedan a merced de los programadores de jailbreak; así que si una de esas características no llegase a estar bien elaborada, se pueden ocasionar errores en el funcionamiento del teléfono, derivando, en el peor de los casos, en un bloqueo definitivo de la memoria del teléfono. | **Cydia.**<br><br>**Installous** |
| | | | |

| | | | |
|---|---|---|---|
| ***Elaboración de copias no autorizadas de software*** | La violación de derechos de autor de un disco, se puede llevar a cabo desde casa de una manera muy sencilla, si se cuenta con una PC, un lector/quemador de discos y a veces un software especializado La violación de derechos de autor de un disco, se puede llevar a cabo desde casa de una manera muy sencilla, si se cuenta con una PC, un lector/quemador de discos y a veces un software especializado | Una de las desventajas más grandes de clonar algún material que venga en DVD, es la mala calidad que esto puede generar; esta mala calidad, se origina debido a que no siempre se rompen todos los candados de seguridad que existen en los DVD originales, por lo que la copia se realizará, pero no con todas las características, algo muy normal en los discos con software; en el caso de los DVD con audio y vídeo, el problema radica en la calidad; para comenzar, la calidad de un disco virgen "pirata" y el disco original es muy grande, consecuencia de la diferencia de grosor de la capa de policarbonato del disco original y del disco virgen. | Nero<br><br>Alcohol120%<br><br>CloneDVD<br><br>DVDFab |

Tabla 16. Formas de distribución ilegal de productos en línea.

### ***3.11.2 DELITOS EN MATERIA DE MARCAS.***

En el cuadro 1, se describen brevemente los delitos más comunes utilizados contra las marcas comerciales, utilizando las tecnologías de la información.




Cuadro 1. Delitos en materia de marcas.

## ***3.12 CIBERTERRORISMO.***

El ciberterrorismo o terrorismo electrónico es el uso de medios de tecnologías de información, comunicación, informática, electrónica o similar con el propósito de generar terror o miedo generalizado en una población, clase dirigente o gobierno, causando con ello una violencia a la libre voluntad de las personas. Los fines pueden ser económicos, políticos o religiosos principalmente.

El término ha sido muy criticado, siendo considerado como un método de satanización para aquellas personas descontentas del orden establecido y que actúan en contra de éste es Internet, gracias a la libertad de ésta.

Ya durante el decenio de 1990 el debate sobre la utilización de la red por organizaciones terroristas giraba en torno a los ataques cometidos en la red contra infraestructuras esenciales como el transporte o el suministro de energía ("ciberterrorismo") y al uso de la tecnología de la información en conflictos armados ("guerra informática"). El éxito alcanzado por ataques con virus y redes robot son una prueba clara de las deficiencias de la seguridad en la red. Se pueden cometer, y con buenos resultados, ataques terroristas por Internet, pero resulta difícil evaluar la importancia de las amenazas; en ese momento, la interconexión no había alcanzado la difusión actual, siendo ése probablemente -aparte del interés de los Estados de mantener en secreto el gran suceso de esos ataques- uno de los principales motivos de que poquísimos incidentes de este tipo se hayan hecho públicos. Por consiguiente, al menos en el pasado, la caída de un árbol planteaba más riesgos para el suministro de energía que un ataque pirata afortunado.

La situación cambió después de los atentados del 11 de septiembre de 2001. Se entabló a partir de entonces un intenso debate sobre la utilización de las TIC por los terroristas, propiciado por informes que revelaban el uso de Internet en la preparación del ataque. Aunque no fueron ciberataques, puesto que el grupo que perpetró los atentados no cometió ataques por Internet, ésta se utilizó en la preparación de los mismos. En el marco de este contexto, se descubrió que las organizaciones terroristas utilizan Internet de distintas formas. Hoy ya se sabe que los terroristas recurren a las TIC y a Internet para los siguientes fines:

- Propaganda;
- Recopilación de información;
- Preparación de ataques al mundo real;
- Publicación de material de capacitación;
- Comunicación;
- Financiación de actividades terroristas;
- Ataques contra infraestructuras esenciales.

Debido a la vulnerabilidad de las tecnologías de la información y a la creciente subordinación a ellas, los ataques por Internet contra infraestructuras esenciales deben incluirse en estrategias concebidas para evitar el ciberterrorismo y combatirlo.

No se ha logrado llegar a un consenso con respecto a la definición de "terrorismo". En un Informe del CRS al Congreso de los Estados Unidos, por ejemplo, se afirma que el hecho de que un terrorista adquiera por Internet un billete de avión a los Estados Unidos es una prueba de que los terroristas recurren a Internet para preparar sus ataques. Parece un argumento un poco vago puesto que la compra de un billete de avión no se convierte en actividad terrorista sólo porque la lleve a cabo un terrorista.

En 1998, sólo 12 de las 30 organizaciones terroristas internacionales consignadas en el Departamento de Estado de los Estados Unidos disponían de páginas web para dar a conocer públicamente sus actividades. En 2004, según el Instituto de los Estados Unidos para la Paz, prácticamente todas las organizaciones terroristas tenían páginas web, entre ellas Hamas, Hezbollah, PKK y Al Qaeda. Los terroristas también han comenzado a participar en comunidades vídeo (como YouTube) para distribuir mensajes y propaganda. La utilización de páginas web y otros foros es una señal de la importancia que atribuyen los grupos subversivos a relaciones públicas más profesionales. La finalidad de recurrir a páginas web y otros medios reside en distribuir propaganda, dar una justificación de sus actividades y reclutar nuevos miembros y donantes así como establecer contacto con los ya existentes. En algunas páginas web se han difundido recientemente vídeos de ejecuciones.

### ***3.12.1 Recopilación de información***

En Internet puede hallarse información considerable sobre posibles objetivos. Por ejemplo, los arquitectos publican en sus páginas web planos de edificios públicos en cuya construcción participan.

A través de diversos servicios Internet y de forma gratuita pueden obtenerse actualmente imágenes de satélite de alta resolución que años atrás sólo estaban a disposición de un puñado de instituciones militares de todo el mundo. Asimismo, en un programa de ciberaprendizaje, se han hallado instrucciones para la construcción de bombas y hasta campos de entrenamiento virtuales que dan instrucciones para la utilización de armas. Por otra parte, se ha encontrado información delicada o confidencial, no protegida adecuadamente contra robots de búsqueda, a la que se puede tener acceso a través de motores de búsqueda. En 2003, el Departamento de Defensa de los Estados Unidos tuvo conocimiento de la existencia de un manual de capacitación vinculado a Al Qaeda con información que fuentes públicas podrían utilizar para obtener detalles sobre posibles objetivos.

En 2006, el New York Times informó que se había publicado información básica relativa a la fabricación de armas nucleares en una página web del Gobierno que presentaba pruebas sobre la capacidad de Iraq para fabricar dichas armas. Un incidente similar tuvo lugar en Australia, cuando en páginas web del Gobierno apareció información detallada sobre posibles objetivos de atentados terroristas. En 2005, según la prensa alemana, un grupo de investigadores descubrió que dos sospechosos de ataques al transporte público con bombas de fabricación casera, habían teledescargado de Internet en sus computadores manuales con instrucciones para la fabricación de explosivos.

### ***3.12.2 Publicación de material de capacitación***

A través de Internet se propaga material de capacitación, por ejemplo, instrucciones para utilizar armas y seleccionar objetivos. Ese tipo de material puede obtenerse a gran escala de diferentes fuentes en línea. En 2008, los servicios secretos occidentales descubrieron un servidor de Internet que facilitaba el intercambio de material de capacitación y la comunicación. Según se informó, las organizaciones terroristas se sirven de diferentes páginas web para coordinar sus actividades.

### ***3.12.3 Comunicación***

Las organizaciones terroristas no se limitan a utilizar las tecnologías de la información para crear páginas web o buscar información en las bases de datos. En el marco de las investigaciones realizadas después de los atentados del 11 de septiembre de 2001, se afirmó que los terroristas se comunicaban por correo electrónico para coordinar sus ataques. Los diarios informaron acerca del intercambio de instrucciones detalladas sobre los objetivos y el número de atacantes a través del correo electrónico. Si los terroristas utilizan tecnologías de encriptación y medios de comunicaciones anónimas, resulta más difícil identificarlos y controlar su comunicación.

### ***3.12.4 Financiación de actividades terroristas***

La mayoría de las organizaciones terroristas dependen de los recursos financieros que reciben de terceros. Con miras a la financiación terrorista, los servicios de Internet pueden utilizarse de varias formas.

Las organizaciones terroristas pueden recurrir a sistemas de pago electrónico para favorecer las donaciones en línea. También pueden utilizar páginas web para explicar la forma de hacer una donación, por ejemplo qué cuenta bancaria utilizar en las transacciones. La organización "Hizb al-Tahrir" publicó los datos de una cuenta bancaria destinada a posibles donantes. También se pueden efectuar donaciones en línea mediante tarjetas de crédito. Para evitar que las descubran, las organizaciones terroristas tratan de ocultar sus actividades implicando a quienes no despiertan sospechas, como las organizaciones caritativas.

Otro método (relacionado con Internet) es utilizar tiendas web falsas. Una de las principales ventajas de la red es la posibilidad de efectuar actividades comerciales en todo el mundo. Es muy difícil demostrar que las transacciones financieras realizadas en esos sitios no se deben a compras habituales sino a donaciones. Habría que investigar cada transacción, operación nada fácil si la tienda virtual está en funcionamiento en una jurisdicción diferente o si se utilizaron sistemas de pagos anónimos.

### ***3.12.5 Ataques contra infraestructuras esenciales***

Además de los ciberdelitos habituales, como el fraude y el robo de identidad, los ataques contra infraestructuras esenciales de la información también podrían convertirse en un objetivo terrorista.

Dada la dependencia incesante en las tecnologías de la información, la infraestructura esencial es más vulnerable a los ataques. Es lo que ocurre especialmente con los ataques contra sistemas interconectados a través de computadoras y redes de comunicación, puesto que los trastornos ocasionados por un ataque a la red no se limitan a los fallos de un solo sistema. Hasta breves interrupciones en los servicios podrían causar enormes daños financieros a las actividades del

cibercomercio, y no sólo en relación con la administración pública sino también con los servicios e infraestructuras militares. Investigar o incluso impedir esos ataques supone desafíos singulares.

A diferencia de los ataques físicos, los delincuentes no necesitan estar presentes en el lugar afectado. Y mientras llevan a cabo el ataque, pueden utilizar medios de comunicaciones anónimas y tecnologías de encriptación para ocultar su identidad. Como ya se indicó anteriormente, la investigación de este tipo de ataques exige instrumentos de procedimiento especiales, una tecnología aplicada a la investigación y personal capacitado.

Un claro ejemplo de una infraestructura esencial para un país, es un aeropuerto, el cual es uno de los blancos favoritos para los ciberterroristas.

• Los servicios de facturación de la mayoría de los aeropuertos del mundo ya disponen de sistemas informáticos interconectados. En 2004, el virus informático Sasser infectó millones de computadoras en todo el mundo, incluidos los sistemas informáticos de las principales compañías aéreas, con la consiguiente cancelación de vuelos.

• Actualmente, se compran en línea un número importante de billetes de avión. Las compañías aéreas utilizan las tecnologías de la información para diversas operaciones, y las principales compañías ofrecen a sus clientes la posibilidad de adquirir billetes en línea. Como sucede con otras actividades de cibercomercio, estos servicios en línea pueden convertirse en un objetivo para los delincuentes, que recurren habitualmente a una técnica conocida como ataques por denegación de servicio (DoS)

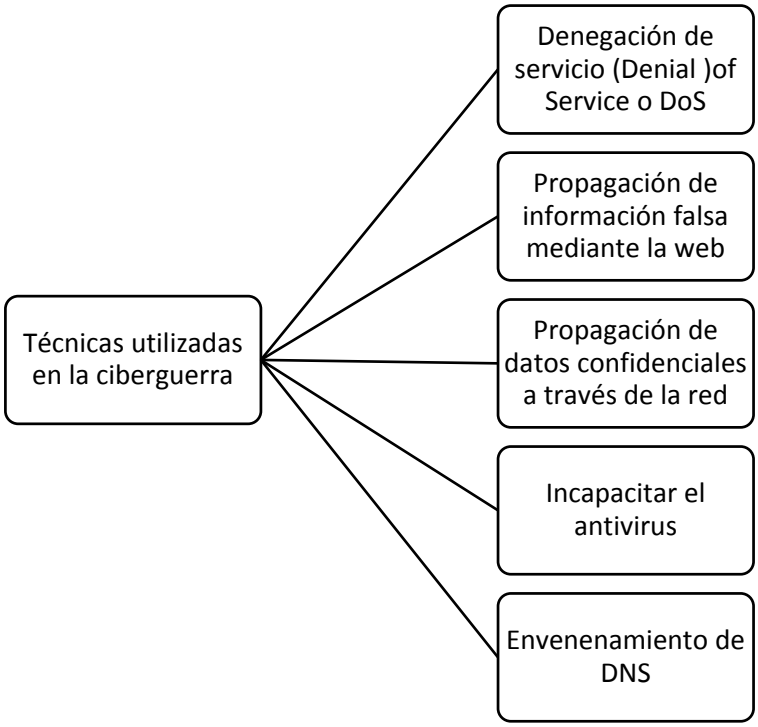
• Otro posible objetivo de los ataques contra la infraestructura esencial del transporte aéreo consumados por Internet es el sistema de control de los aeropuertos. La vulnerabilidad de los sistemas informáticos de control aéreo se puso de manifiesto en el ataque pirata cometido contra el aeropuerto de Worcester de los Estados Unidos en 1997, durante el cual dejaron de funcionar los servicios telefónicos de la torre de control y el sistema de control de luces de la pista de aterrizaje.

Muchos reconocen que la infraestructura esencial para una nación es un posible objetivo de atentado terrorista puesto que, por definición, resulta vital para la estabilidad y perdurabilidad del Estado. Una infraestructura se considera esencial si su incapacidad o destrucción puede afectar negativamente la defensa o seguridad económica de un Estado. Se trata, en particular, de sistemas de energía eléctrica y de suministro de agua, sistemas de telecomunicaciones, sistemas de almacenamiento y transporte de gas y petróleo, servicios bancarios y financieros, sistemas de transporte y servicios de emergencia.

### ***3.13 CIBERGUERRA.***

La guerra se define habitualmente como el uso de la fuerza, o la violencia, por parte de un país-nación para obligar a otro a cumplir su voluntad. El estratega prusiano Carl von Clausewitz la definía esencialmente de esta maneta en su tratado De la guerra, el cual era un clásico del pensamiento militar estratégico de principios del siglo XIX. Concretamente, definía a la guerra como la "continuación de la política por otros medios".

Protegerse contra los ciberataques no es fácil. Hasta ahora, se conocen muy pocos Informes que se refieran a la sustitución de conflictos armados por ataques a través de Internet. En este momento, los debates dan prioridad a los ataques contra infraestructuras esenciales y al control de la información durante un conflicto. Teniendo en cuenta tanto las comunicaciones civiles como militares, la infraestructura de la información constituye un objetivo fundamental en los conflictos armados. Sin embargo, no es seguro que esos ataques se cometan por Internet. Los ataques perpetrados a sistemas informáticos en Estonia y los Estados Unidos han sido asociados a la guerra informática. Dada la imposibilidad de determinar a ciencia cierta si un ataque procede de un organismo público oficial, resulta difícil catalogarlo de guerra informática. Ocurre lo mismo con respecto a los ataques físicos -por ejemplo, mediante armas y explosivos - contra infraestructuras.




Cuadro 2. Técnicas utilizadas en la ciberguerra

La técnica más peligrosa consiste en tumbar los servidores de páginas web. Se trata de colapsar la capacidad de recibir peticiones y responder a ellas. Un ejemplo es intentar meter a 2.000 personas en una oficina de atención al cliente: no podrá dar servicio y acabará por cerrar. Precisamente lo que consiguen los ciberterroristas con este tipo de asalto se llama denegación de servicio -***Denial of Service o DoS***-, y se consigue lanzando muchas solicitudes consecutivas para ver una misma página, de forma que se supere la capacidad de respuesta del servidor y deje de funcionar.

Para llevarlo a cabo existen dos tácticas distintas: o desde una sola máquina se lanzan muchas peticiones seguidas para ver páginas, o se usan miles de computadoras y se envían unas pocas peticiones desde cada una. La primera es más fácil de detener: averiguamos la dirección IP de esa máquina, el número que la identifica en la Red, y le cortamos el acceso; la segunda es mucho más complicada porque se realiza desde muchos puntos de toda la red global. A esta segunda estrategia se le llama denegación de servicio distribuida (DDoS) y es la que se aplicó contra Estonia

en 2007, como se menciona más adelante. Para lanzar un ataque de este tipo es fundamental dominar muchas computadoras es de todo el mundo, y esto se logra convirtiéndolas en PCs zombis que actúan a la vez.

Un zombi es una computadora en la que se ha insertado un programa troyano, que permite controlarla sin que lo sepa el usuario. Cuando un hacker se hace con varios zombis, ha conseguido una red de robots o botnet, que es un auténtico regimiento; se calcula que cada botnet se compone de unos 20.000 zombis. En todo el mundo hay unos 6 millones de zombis controlados para usos criminales sin que sus dueños tengan una idea.

Otro tipo de ataque, muy semejante al anterior, es el "***envenenamiento de DNS***", que penetra el servidor de los nombres de dominio para llevar al usuario hacia un servidor planeado por el hacker. Por ejemplo, está el caso de un grupo de hackers que desviaron un satélite militar británico, pidiendo por su restauración una gran suma de dinero.

Otra forma de realizar estos ataques es incapacitar el antivirus, dejando desprotegido el sistema; luego se envían gusanos mediante el correo electrónico o a través de archivos compartidos en la red.

Pero, en nuestra época, lo más peligroso consiste en la propagación de datos confidenciales a través de la red, ya que dicha información puede comprometer a la nación a que pertenece, y en muchas ocasiones ésta se ve comprometida frente a dichos ataques, o también corre peligro de ser eliminada información vital. En este rango caben los ciberarsenales o virus que borran información y se propagan a través del correo electrónico.

También podemos encontrar el caso de la propagación de información falsa mediante la web, acerca de cualquier tema específico. Esto podría traducirse en falsas especulaciones acerca de las posibles causas de algún accidente, o la denuncia soportada sobre falsas fallas a cualquier producto inmerso en la competencia, con el fin de desvirtuarlo y dañar las ventas de dicho producto.

### *3.13.1 Primer ciberguerra.*

El 27 de abril de 2007 el gobierno de Estonia retiró una estatua erigida en los tiempos de la dominación soviética en homenaje a los soldados que lucharon contra la invasión alemana en la Segunda Guerra Mundial. La escultura era un recuerdo del imperialismo de Moscú, que controló la república báltica de 1940 a 1991. Pero en un país con un 25% de la población de origen ruso la decisión resultó muy polémica, y ese día hubo protestas y graves desórdenes públicos. Cuando al caer la tarde la calma parecía haber vuelto, se inició el ataque más duro. Las páginas web de los principales periódicos, radios y televisiones sufrieron espectaculares incrementos de tráfico que colapsaron la capacidad de respuesta de los servidores y el ancho de banda disponible.

Este asalto fue seguido por otro mucho más sofisticado contra los enrutadores por los que circula el tráfico de Internet. Varias webs del gobierno cayeron y las páginas de dos grandes bancos sufrieron una fuerte embestida; incluso los cajeros automáticos se resintieron. Los webmasters advirtieron que las conexiones responsables del colapso provenían de lugares tan exóticos como Egipto, Perú o Vietnam, y la solución rápida fue cortar el acceso al tráfico internacional. Estonia se

desconectó del mundo. La crisis se recrudeció con nuevos raids (***Redundant Array of Independent Disks***, «conjunto redundante de discos independientes) hostiles la víspera del 9 de mayo, día en que Rusia celebra su victoria en la Segunda Guerra Mundial. Esa jornada, el entonces presidente Vladímir Putin criticó a las autoridades estonias por la retirada del monumento; más tarde se sugirió que los servicios secretos rusos pudieron haber amparado el ataque.

Para atajar la ofensiva fue necesaria la colaboración de equipos internacionales de respuesta a emergencias en Internet, así como de servicios de seguridad de otros gobiernos expertos en ciberdelincuencia y ciberterrorismo. Aun así, el asedio no cesó totalmente hasta el 18 de mayo. El ministro de defensa estonio, Jaak Aaviksoo, enjuició con gravedad lo ocurrido. En un país en el que el 90% de las transacciones bancarias y declaraciones de impuestos se realizan a través de Internet, los ciudadanos tuvieron la incómoda sensación de que su modo de vida había sido amenazado. Y aunque el gobierno no acusó formalmente a nadie, el político subrayó un dato: las oleadas de ataques tuvieron lugar de acuerdo con la hora de Moscú.

La crisis estonia sonó como un mazazo en los despachos gubernamentales de todo el mundo, desde el Pentágono a Bruselas. Como explica el español Francisco García Morán, director general de informática de la Comisión Europea, el ataque fue un despertador para todos los países porque mostró que el mundo es dependiente de Internet y que, si no se toman las medidas de protección adecuadas, es posible interrumpir servicios importantes para la sociedad.

Uno de los grandes temores de las autoridades internacionales es que las dianas de la ciberguerra no se limiten a instituciones o países, sino que el objetivo sea el propio funcionamiento global de Internet. El miedo está justificado porque esto ya ha ocurrido al menos dos veces, una en 2002 y otra en 2007. Ambas agresiones apuntaban al corazón de la Red: el Sistema de Nombres de Dominio (DNS). Las direcciones que tecleamos como www.x.com, se corresponden con complicados conjuntos de 10 cifras que son el código de ese dominio. Al conectarnos se produce una traducción de letras a cifras de forma invisible para nosotros. Sólo trece servidores en todo el mundo mantienen el listado oficial de dominios vivos. Son la clave de la interconexión mundial y si cayesen, Internet se fundiría de inmediato. El 6 de febrero de 2007 alguien intentó provocar ese tremendo apagón digital.

El ataque se originó en la región de Asia-Pacífico y tuvo dos fases: la primera duró dos horas y media, luego se produjo una pausa de tres horas y media y se reanudó la ofensiva durante cinco horas consecutivas. La tipología fue la misma que en Estonia: una denegación de servicio distribuida mediante computadoras zombis. La ofensiva se lanzó sobre seis de los trece servidores de nombres y dos de ellos quedaron gravemente afectados. Los agresores sabían lo que se hacían, aunque no consiguieron su propósito. Mayor trascendencia tuvo el episodio del 21 de octubre de 2002, el día que Internet estuvo más cerca del colapso, ya que los hackers dejaron KO nueve de los trece servidores.

### ***3.13.2 Virus utilizados en la ciberguerra.***

En tiempos recientes, los ataques de algunos países u organizaciones a varios objetivos específicos de sus rivales, como pueden ser plantas nucleares, se han llevado a cabo mediante la utilización de

programas informáticos. A continuación, se mencionan los dos virus más relevantes para estos fines, los cuales pueden ser catalogados entre los más potentes de la historia, por su nivel de peligrosidad.

#### ***3.13.2.1 Stuxnet.***

Stuxnet es un gusano informático que afecta a equipos con Windows, descubierto en junio de 2010 por VirusBlokAda, una empresa de seguridad radicada en Bielorrusia. Es el primer gusano conocido que espía y reprograma sistemas industriales, en concreto sistemas SCADA (**S**upervisory **C**ontrol **A**nd **D**ata **A**cquisition <<Supervisión, Control y Adquisición de Datos>>, el cual es un software para computadoras que permite controlar y supervisar procesos industriales a distancia), de control y monitorización de procesos, pudiendo afectar a infraestructuras críticas como centrales nucleares.

Stuxnet es capaz de reprogramar controladores lógicos programables y ocultar los cambios realizados. También es el primer gusano conocido que incluye un rootkit para sistemas reprogramables PLC.

La compañía europea de seguridad digital Kaspersky Labs describía a Stuxnet en una nota de prensa como "un prototipo funcional y aterrador de un arma cibernética que conducirá a la creación de una nueva carrera armamentística mundial". Kevin Hogan, un ejecutivo de Symantec, advirtió que el 60% de las computadoras contaminadas por el gusano se encuentran en Irán, sugiriendo que sus instalaciones industriales podrían ser su objetivo. Kaspersky concluye que los ataques sólo pudieron producirse "con el apoyo de una nación soberana", convirtiendo a Irán en el primer objetivo de una guerra cibernética real

En junio de 2010, una compañía bielorrusa de detección de malware recibió una solicitud de un cliente para determinar por qué sus máquinas fueron reiniciadas una y otra vez. El malware se encontraba con una firma de certificado digital para que pareciera que había venido de una compañía confiable. Esta hazaña llamó la atención de la comunidad antivirus, cuyos procesos automatizados de detección de programas no pudieron manejar este tipo de amenaza. Este fue el primer avistamiento de Stuxnet en la naturaleza.

El peligro que representan las firmas falsificadas fue tan aterrador que especialistas en seguridad informática comenzaron silenciosamente a compartir sus hallazgos a través de e-mail y en foros por líneas privadas. Mikko Hypponen H., jefe de investigación de F-Secure, una empresa de seguridad en Helsinki, Finlandia, mencionaba: “No puedo pensar en ningún otro sector de las TI, donde hay tal una amplia cooperación entre competidores." Sin embargo, las empresas pueden competir, por ejemplo, para ser el primero en identificar una característica clave de un cyberweapon.

Antes de que supiera para qué objetivos fue diseñado Stuxnet, los investigadores de Kaspersky y otras firmas de seguridad comenzaron con la ingeniería inversa del código, recogiendo pistas en el camino: el número de infecciones, la fracción de las infecciones en Irán, y las referencias de Siemens Industrial Programs, que son utilizados en las centrales eléctricas.

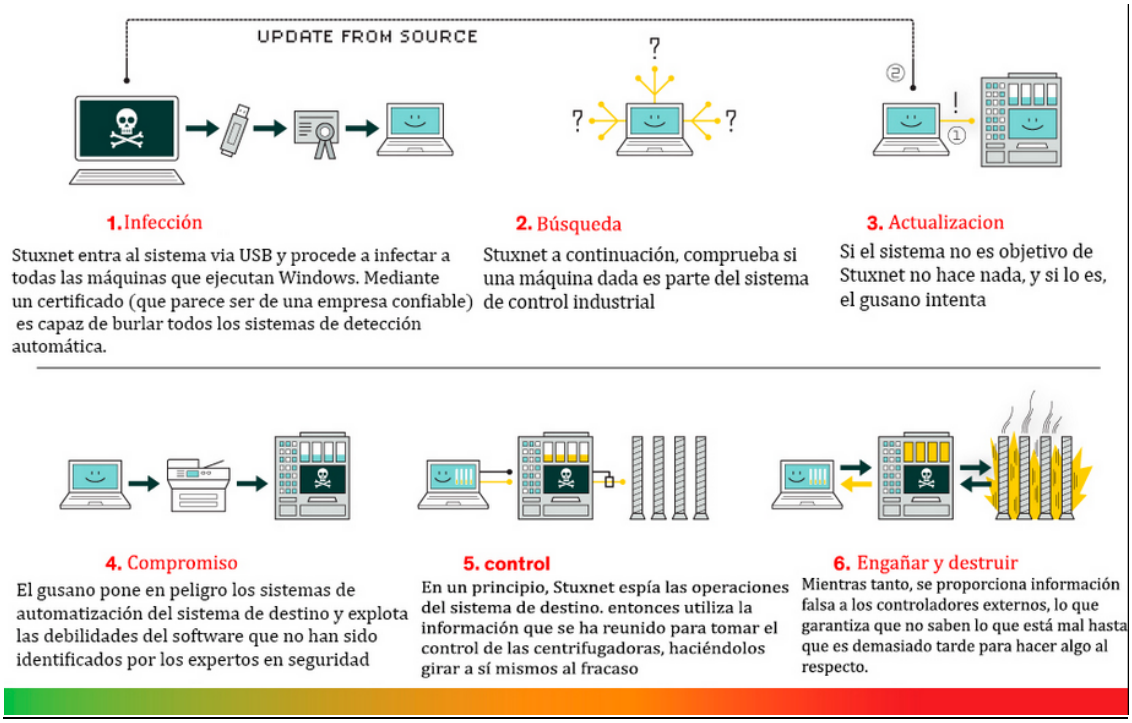



Figura 39. Funcionamiento del virus Stuxnet.

### ***3.13.2.2 Flame.***

Flame es un muy sofisticado programa malicioso que está siendo activamente utilizado como arma cibernética para dirigir a entidades de varios países. Descubierto por los expertos de Kaspersky Lab durante una investigación que fue impulsada por la Unión Internacional de Telecomunicaciones (UIT), Flame está diseñado para llevar a cabo espionaje cibernético. Se puede robar información valiosa - incluyendo pero no limitado a contenido de la pantalla de una computadora, información acerca de los sistemas de destino, los archivos almacenados, datos de contacto y conversaciones incluso audio. Su complejidad y funcionalidad superiores a las de todas las armas cibernéticas otros conocidos.

Flame es el arma más grande cyber descubierto hasta la fecha, y fue diseñado de una manera que hace que sea casi imposible de rastrear. Mientras que el malware convencional está diseñado para ser pequeño y escondido, magnitud Flame le permitió permanecer sin ser descubiertas. Flame infecta los equipos de cómputo mediante el uso de sofisticadas técnicas que fueron utilizadas anteriormente por una sola arma cibernéticca: Stuxnet. Aunque parece que la llama está en funcionamiento desde marzo de 2010, ningún software de seguridad lo había descubierto, excepto Kaspersky Lab.

El virus Flame, ha estado infectando computadoras en Irán, Israel, Líbano, Sudán, Siria, Arabia Saudita y Egipto. Ha sido el acaparamiento de las imágenes de las pantallas de computadora de los usuarios, registrando sus chats de mensajería instantánea, de forma remota de encender sus micrófonos para grabar sus conversaciones de audio y el control de sus pulsaciones y el tráfico de la red, de acuerdo con un informe de Kaspersky Labs, una empresa de seguridad con sede en Moscú.

Si los resultados del informe demuestran que es verdad, Flame sería la tercera arma de Internet más importantes que se han descubierto desde 2010. El primero, llamado Stuxnet, tenía la intención de atacar software en equipos industriales especializados, y fue utilizado para destruir las centrífugas en una instalación nuclear iraní en 2010. El segundo virus, llamado Duqu, como la llama, realizó reconocimiento. Los investigadores de seguridad creen que Duqu fue creado por el mismo grupo de programadores detrás de Stuxnet.c

El malware tiene un tamaño inusual grande de 20 MB, está escrito parcialmente en el lenguaje de programación interpretado Lua con código C++ compilado y permite que otros módulos atacantes sean cargados después de la infección inicial. El malware usa cinco métodos diferentes de cifrado y una base de datos SQLite para almacenar información. El método usado para inyectar el código en varios procesos es silencioso, de forma que los módulos malware no aparecen en la lista de los módulos cargados en un proceso y las páginas de memoria son protegidas con los permisos READ, WRITE y EXECUTE que la hacen inaccesible para las aplicaciones en modo usuario. El código interno tiene pocas similitudes con otros malware, pero aprovecha dos vulnerabilidades que también fueron usadas previamente por Stuxnet para infectar sistemas. El malware determina qué software antivirus está instalado en el sistema y modifica su comportamiento (por ejemplo, cambiando la extensión de archivo que utiliza) para reducir la probabilidad de ser detectado por ese software. Indicadores adicionales de que un sistema está infectado son la exclusión mutua (mutex) y la actividad del registro. También la instalación de un driver de audio falso que permite al software iniciarse al arrancar el sistema. A diferencia de Stuxnet, el cual fue diseñado para dañar procesos industriales, Flame parece haber sido escrito solo con propósitos de espionaje. No parece dirigirse a un sector determinado, sino que más bien es "un conjunto de herramientas diseñadas para el ciber-espionaje".

Flame no contiene una fecha predefinida en la cual se desactiva, pero permite a los operadores enviar un comando "kill" que elimina todos sus rastros de un sistema.

Según los expertos en criptografía más reconocidos del planeta, Marc Stevens y B.M.M. de Weger, han estudiado a Flame y seguido los pasos del software añadiendo que para realizar ciertos ataques sólo es posible realizarlos usando técnicas de criptografía de clase mundial, que requiere a las mentes matemáticas más brillantes que incluso han hecho nuevos descubrimientos matemáticos para aplicarlos en Flame.

Los expertos señalan que Flame usa ataques de colisión MD5 que eran conocidos sólo en la teoría y que es muy interesante desde el punto de vista científico. El ataque genera órdenes criptográficas idénticas en teoría hasta que en el 2008 un grupo de investigadores lo llevó a la práctica. esto fue posible mediante el uso de un banco de 200 consolas PlayStation 3 para encontrar colisiones en el algoritmo MD5 (*Message-Digest Algorithm 5*, Algoritmo de Resumen del Mensaje 5, un algoritmo de reducción criptográfico de 128 bits) y explotar las debilidades en forma de certificados seguros de SSL que se emitieron, luego construyeron una autoridad de certificación rebelde que fue de confianza para todos los principales navegadores y sistemas operativos.

Flame representa la primera vez que se usan los ataques de colisión MD5 con fines maliciosos en el mundo real y hasta ahora ningún criptógrafo había visto algo similar. Según mencionan los expertos en Flame hubo matemáticos haciendo nueva ciencia para crear el malware.

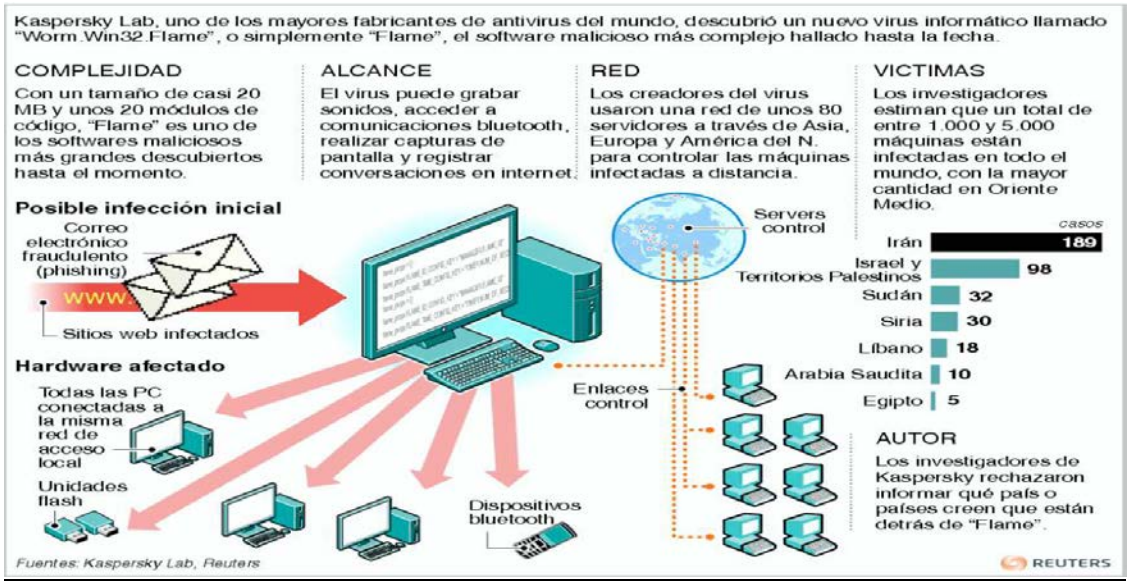



Figura 40. Funcionamiento del virus Flame.

### ***3.14 CIBERBLANQUEO DE DINERO.***

Internet está transformado los métodos de blanqueo de dinero. Pese a que, cuando se trata de cantidades importantes, las técnicas tradicionales proporcionan todavía un cierto número de ventajas, Internet facilita también varias ventajas. Los servicios financieros en línea ofrecen la opción de efectuar con gran rapidez numerosas transacciones financieras en todo el mundo. Internet ha contribuido a suprimir la dependencia de transacciones con dinero en efectivo. Las transferencias por cable sustituyeron el transporte de dinero en efectivo como primer paso para poner fin a esa dependencia, pero la implantación de normas más estrictas para detectar transferencias por cable dudosas ha obligado a los delincuentes a elaborar nuevas técnicas. La detección de transacciones sospechosas en la lucha contra el blanqueo de dinero se basa en obligaciones de las instituciones financieras que intervienen en las transferencias.

El ciberblanqueo de dinero se divide por lo general en tres etapas:

1) Depósito;

2) Estratificación;

3) Integración.

Con respecto al depósito de grandes cantidades de dinero en efectivo, Internet no podría quizás ofrecer esas numerosas ventajas tangibles, pero recurrir a ella resulta especialmente interesante para los delincuentes en la etapa de estratificación (u ocultamiento). En este contexto, la investigación es particularmente difícil cuando los blanqueadores de dinero utilizan casinos en línea.

Las normas que se aplican a las transferencias de dinero son por ahora limitadas e Internet ofrece a los delincuentes la posibilidad de realizar transferencias internacionales de dinero poco costosas y libres de impuestos. Las dificultades actuales en la investigación de técnicas de blanqueo de dinero por Internet emanan por lo general de la utilización de moneda virtual y de casinos en línea.

### *3.14.1 Utilización de moneda virtual*

Uno de los motores fundamentales de la difusión de moneda virtual fue el micropago en operaciones (por ejemplo, teledescarga de artículos en línea que costaban 10 centavos USD o menos) en las que no podían utilizarse tarjetas de crédito. Con la demanda creciente de micropagos, se implantó la moneda virtual, incluidos los "valores en oro virtuales", siendo éstos sistemas de pago por cuenta cuya cuantía está respaldada por los depósitos en oro. Los usuarios pueden abrir cuentas virtuales en oro, generalmente sin tener que registrarse.

Algunos proveedores autorizan incluso transferencias directas entre pares (persona a persona) o extracciones en efectivo. Los delincuentes pueden abrir este tipo de cuentas en diferentes países y combinarlas, lo cual complica la utilización de instrumentos financieros para el blanqueo de dinero y la financiación de actividades terroristas. Además, en el momento de registrarse, los titulares de esas cuentas podrían facilitar información inexacta con objeto de ocultar su identidad.

Un ejemplo de esto es la Bitcoin, que es una moneda digital, un protocolo, y un software que permite:

- Transacciones instantáneas persona  a persona
- Pagos en todo el mundo
- Bajas o cero gastos de tramitación

Las cuales se pueden usar tanto en negocios legítimos, como en muchos sitios que se dedican a actividades ilícitas en las darknets (del cual se hablará más adelante).

Estas se pueden dar como pago a una actividad ilícita y cambiarlas por dinero por ejemplo:


Figura 41. Moneda virtual Bitcoin.

Cuando la empresa interesada en cobrar un bitcoin lo recibe, ya es poseedora de ese bitcoin; la empresa entonces tiene dos opciones, guardar el bitcoin para usarlo ellos mismos, o también puede decidir venderlo a cambio de su moneda local si lo necesita (en MtGox o en cualquier otro sitio, normalmente hay intercambiadores locales). Entre los usuarios de bitcoins que tienen una empresa o simplemente quieres ser poseedoras de bitcoins han convencido a sus proveedores para aceptar bitcoins. Esto es lo ideal, así se cierra el círculo y se empieza a crear una economía que funciona solo en bitcoins.

### ***3.14.2 Utilización de casinos en línea.***

En contraposición al establecimiento de un verdadero casino, no se necesitan importantes inversiones para crear casinos en línea. Por otra parte, la reglamentación de los casinos en línea y fuera de línea suele ser diferente según los países. Sólo se pueden localizar las transferencias de dinero y demostrar que los fondos no son ganancias de lotería sino dinero blanqueado, si los casinos tienen constancia de ellas y lo ponen en conocimiento de las autoridades competentes.

La reglamentación jurídica actual de los servicios financieros por Internet no es tan estricta como la reglamentación tradicional. Dejando de lado ciertas lagunas en la legislación, los motivos de los problemas planteados en materia de reglamentación son los siguientes:

• Dificultades en la verificación del cliente: la precisión de una verificación puede correr peligro si el proveedor del servicio financiero y el cliente no se han conocido nunca;

• Falta de contacto personal: resulta difícil aplicar procedimientos tradicionales del tipo "conozca a su cliente";

• Participación frecuente, en las transferencias por Internet, de proveedores de diversos países;

• Falta de un código legal/penal para supervisar ciertos instrumentos: en particular, plantea dificultades cuando los proveedores autorizan a los clientes a efectuar transferencias de valores con arreglo al modelo "de par a par".

Por ejemplo en www.casino.com/mx/about.html nos podemos encontrar con un servicio de casino al cual se puede ingresar desde cualquier parte del mundo siendo prácticamente imposible el rastreo del capital manejado por los jugadores y el propio casino, lo cual hace de este tipo de sitios web un blanco perfecto para llevar a cabo esta actividad ilícita.

## ***3.15 REDES OSCURAS (DARKNET).***

El concepto de red oscura, también conocido por su nombre original en inglés darknet, ha ido evolucionando con el tiempo desde su definición original dada por unos investigadores de Microsoft. Actualmente el término Darknet no tiene una definición universalmente aceptada. Sin embargo, basándose en las versiones actuales más populares, se puede decir que la Darknet es una colección de redes y tecnologías usadas para compartir información y contenidos digitales (ej. textos, software, canciones, imágenes, películas) que está "distribuida" entre los distintos nodos y que trata de preservar el anonimato de las identidades de quienes intercambian dichas información,

es decir, persiguen el anonimato del origen y el destino cuando se produce la transferencia de información.

En la definición anterior, cuando se habla de redes, no se refiere a redes físicas separadas de las redes actuales sino a redes superpuestas que pueden usar protocolos y puertos "no estándar" sobre la red subyacente. Por eso se dice que estas redes operan aparte de las redes públicas sobre las que se montan y que sus contenidos se mantienen inalcanzables para el público general de la red subyacente (son privadas). Para acceder a la red y sus contenidos es necesaria cierta información adicional, la cual puede ser compartida por un grupo restringido de personas. Esa información suele incluir la necesidad de ejecución de un software específico y a veces es necesaria la conexión a algún tipo de servidor que no estará accesible vía los DNS tradicionales. Por esta dificultad de acceso los motores de búsqueda no suelen buscar en estas redes, permaneciendo sus contenidos invisibles. Por todos estos impedimentos para acceder a la información a estas tecnologías se les llama red oscura o Darknet.

A veces el término darknet se usa de una forma general para describir sitios no comerciales de Internet o para referirse a las comunicaciones web underground, principalmente asociadas con la actividad ilegal o disidente.

Entre las darknets hay dos tipos las peer-to-peer (por ejemplo las construidas con Freenet, i2p, GNUnet, Entropy, ANts P2P), conocidas como redes peer-to-peer anónimas, y las que no son peer-to-peer (ej. Tor). Dentro de las redes peer-to-peer anónimas son especialmente interesantes las que son friend-to-friend porque tienen una propiedad muy aprovechable para conseguir el anonimato: En ellas cada host se conecta directamente sólo a hosts cuyos operadores son conocidos y confiables a priori.

Un tipo especial de darknets que están teniendo un fuerte incremento son aquellas que utilizan como tecnología subyacente (son redes superpuestas) conexiones wireless para establecer redes. Observar que este tipo de redes tienen una serie de características que las hace especialmente interesantes en el mundo de las darknet, frente a las que usan cables:

- No es necesario pagar por el servicio de cable a ningún proveedor. Por tanto por ese lado no es necesario revelar la identidad.
- Los equipos pueden tener movilidad. Por lo que puede ser difícil su localización.
- Permiten establecer fácilmente topologías en malla y por tanto si un equipo es desconectado esto no afecta de forma grave a la interconexión entre los demás.
- Para acceder al servicio basta con una tarjeta de red wireless. Esta se puede adquirir fácilmente de forma que no que sea posible asociar una identidad a esa tarjeta dirección MAC.
- Las siguientes imágenes, son algunos ejemplos de lo que se puede encontrar en este tipo de redes.

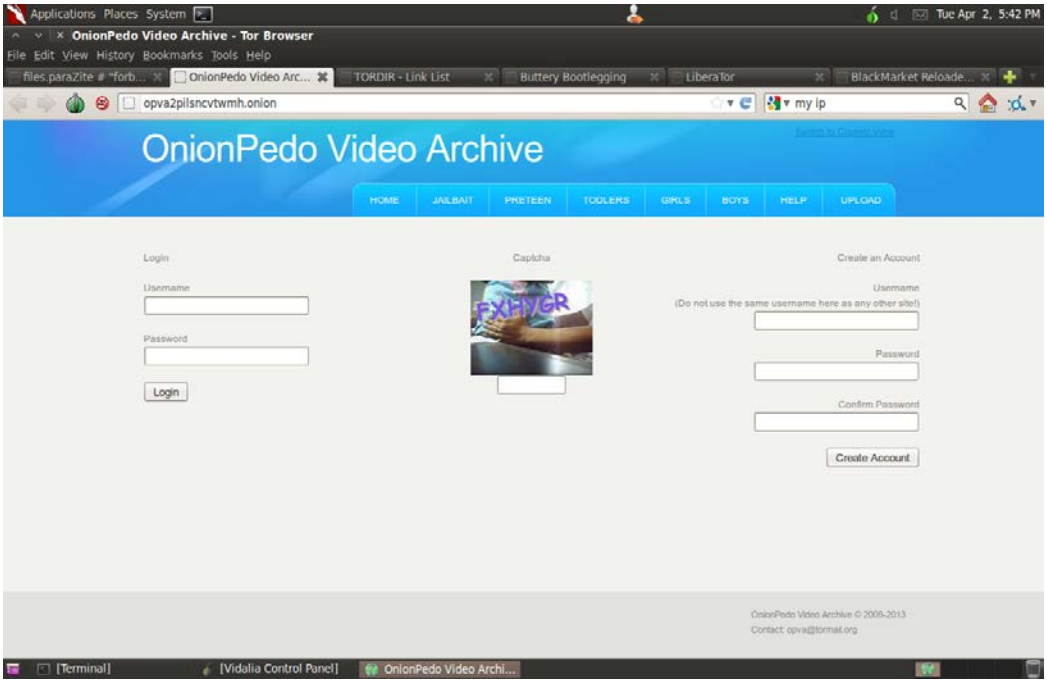



Figura 42. Red de pedofilia en la darket Onion.

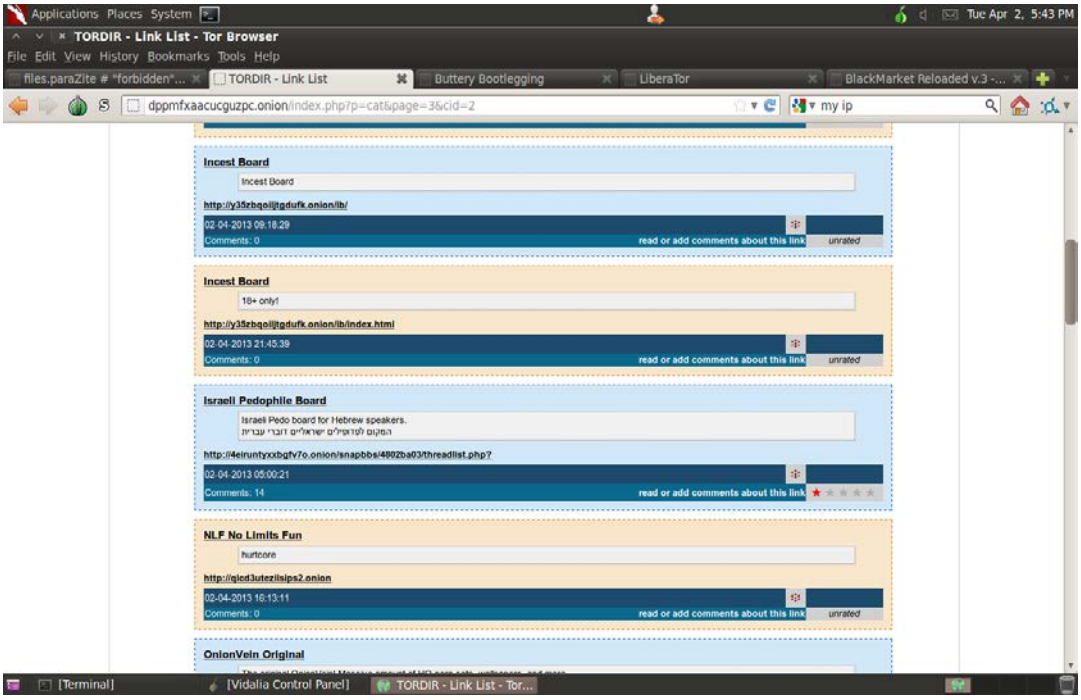



Figura 43. Resultados de una búsqueda en Onion.


Figura 44. Forma de pagar servicios en las darknets: mediante la Bitcoin.


Figura 45. Búsqueda en darknet Tor.

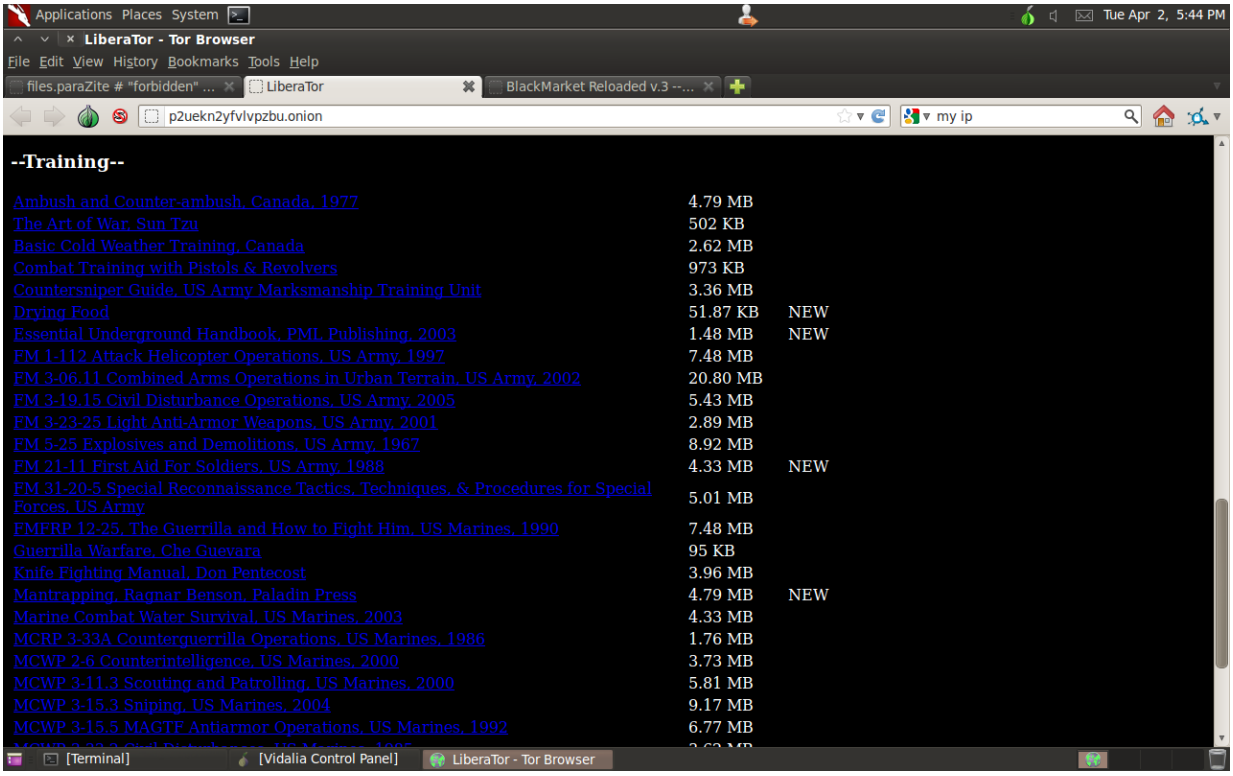



Figura 46. Otros resultados en la darknet Tor.

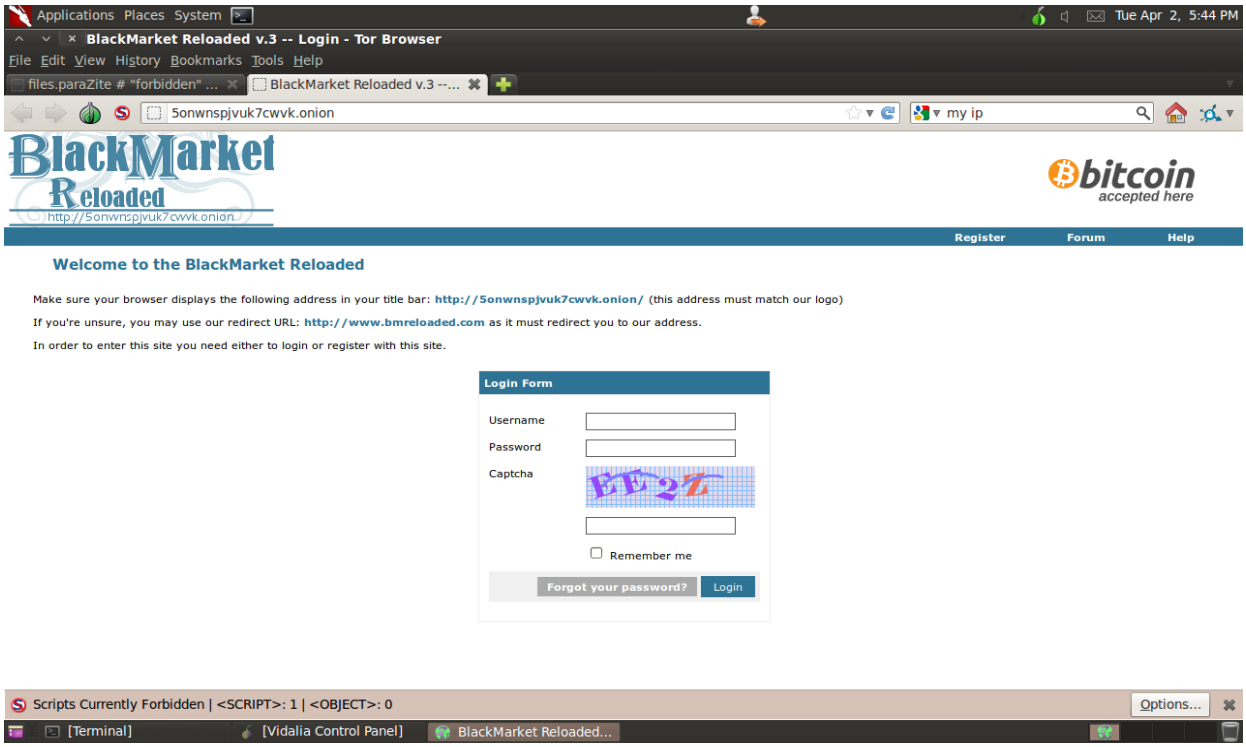



Figura 47. Mercado negro en Internet.

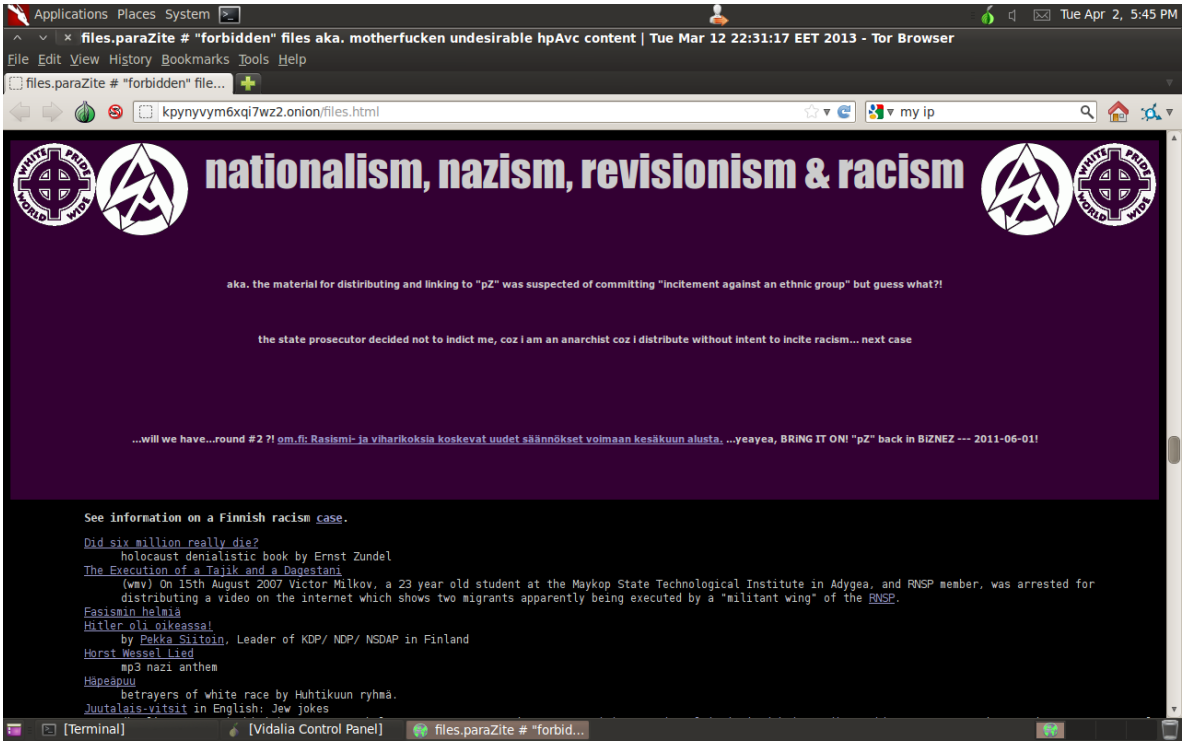



Figura 48. Páginas racistas, también en las darknet.

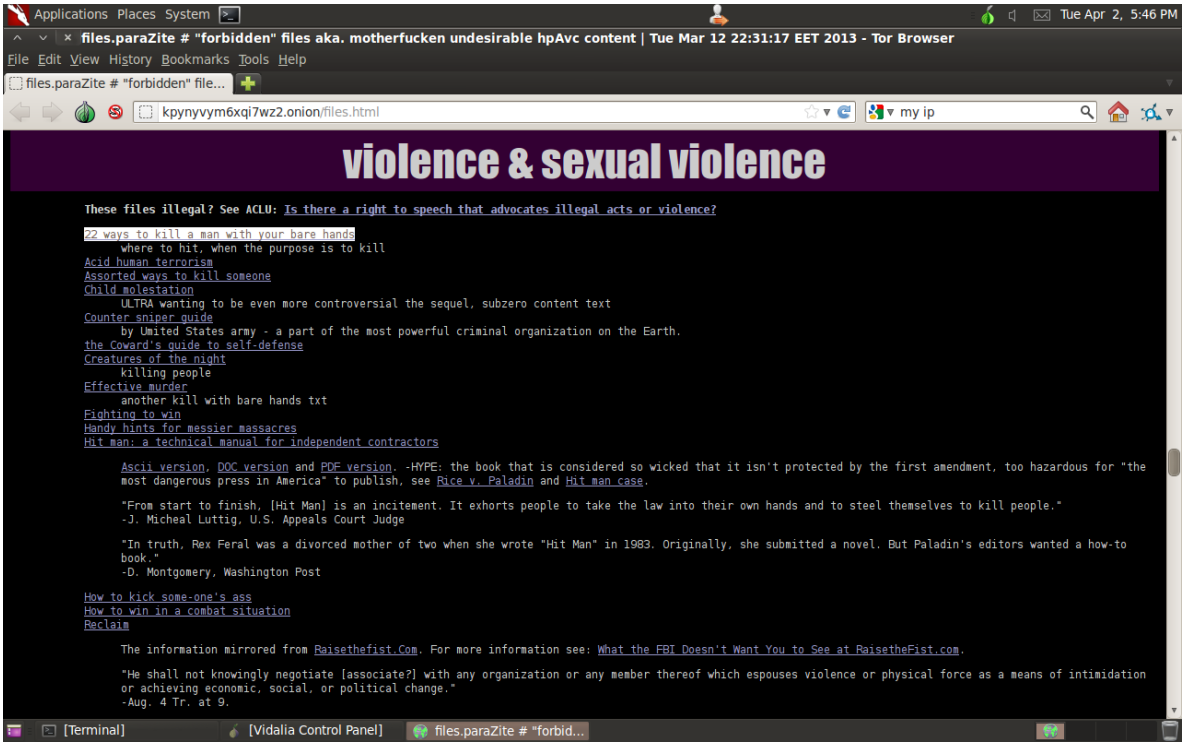



Figura 49. Resultados de búsqueda: violencia sexual.

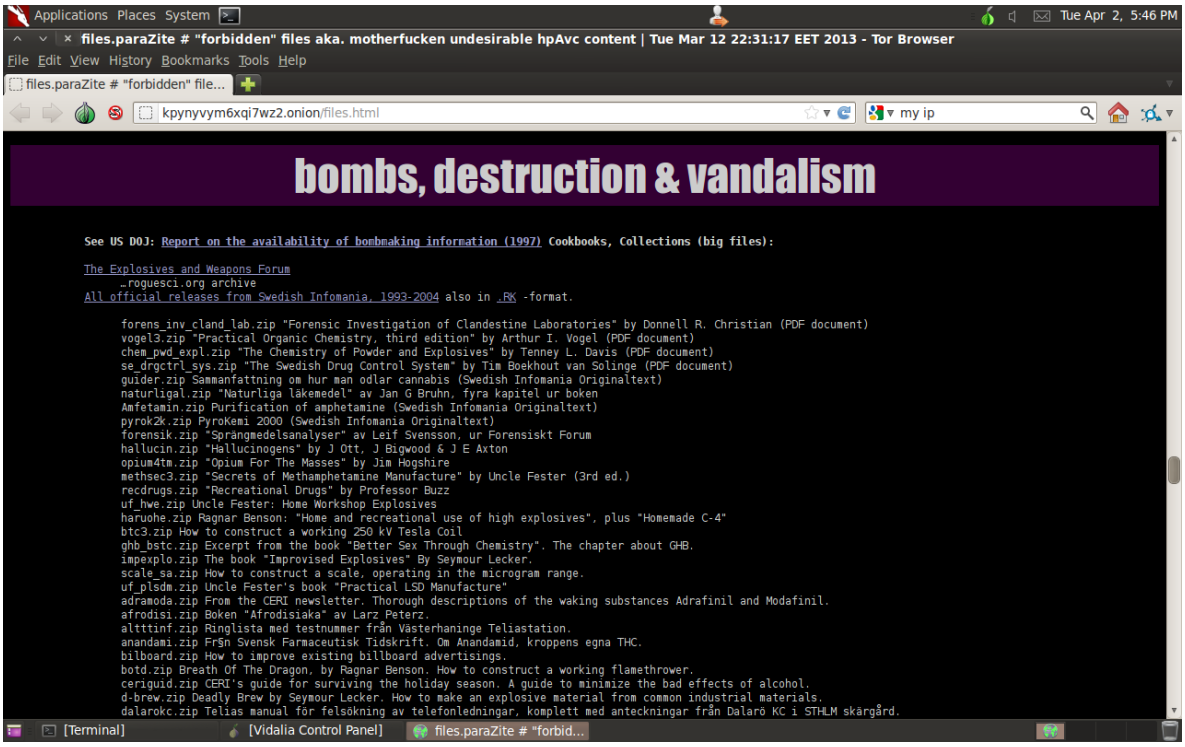



Figura 50. Resultados de la búsqueda: bombas y destrucción.

# *4. DERECHO INFORMÁTICO Y CIBERDELITOS.*

Ante toda la problemática que se mostró en los capítulos anteriores se deben llevar a cabo medidas de protección y regulación y así evitar el crecimiento de todos estos delitos que afectan de una o de otra forma a diversas áreas de la sociedad.

En este último capítulo se muestran las regulaciones y tratados que existen alrededor del mundo para poder combatir este tipo de actividades, también se mostrará la legislación y penalización sobre el tema en nuestro país.

Aunque la evolución de la informática, entendida como la ciencia de tratamiento automático de la información, es uno de los fenómenos que más ha influido en el vertiginoso cambio social que estamos viviendo, no implica en absoluto su conocimiento ni su aprovechamiento en beneficio de la humanidad.

Se debe, por tanto, adaptar a los nuevos métodos que nos proporcionan las técnicas asociadas a los equipos de cómputo y adecuar la actividad jurídica al desarrollo tecnológico. Por otro lado, la información da poder a quien la posee, pero no basta con poseer la información, es necesario también saber manejarla. Actualmente el desarrollo alcanzado en los sistemas de telecomunicaciones que han permitido que una misma información sea accesible a un gran número de personas está cambiando radicalmente la forma de vida. Si se une la informática con las posibilidades que ofrece de almacenamiento, tratamiento y recuperación de la información registrada en soportes magnéticos, permite controlar esa información y puede llegar a convertirse en un instrumento de presión y control de masas.

Se puede conceptualizar el derecho de la informática, como el conjunto de normas jurídicas que regulan la creación, desarrollo, uso, aplicación de la informática o los problemas que se deriven de la misma en las que existan algún bien que es o deba ser tutelado jurídicamente por las propias normas.

En realidad, es cuestionable todavía hoy en día si en verdad existe esta disciplina como tal, por lo que una gran mayoría de estudiosos de la materia han preferido analizar algunos campos en los que, aplicando la informática, se podrían relacionar los resultados con el campo del derecho, y así han preferido mejor estudiar los puntos siguientes:

- La protección jurídica de la información personal;
- La protección jurídica del software
- El flujo de datos transfronterizo
- Los convenios o contratos informáticos
- Los delitos informáticos
- El valor probatorio de los documentos electromagnéticos (documentos almacenados en dispositivos electrónicos, como lo son memorias USB, discos duros, CD´s, etc)

Una legislación adecuada es la base para la investigación y procesamiento del ciberdelito. Sin embargo, los legisladores deben responder constantemente a los desarrollos de Internet y

supervisar la eficacia de las disposiciones existentes, especialmente teniendo en cuenta la velocidad de desarrollo de las tecnologías de redes.

Históricamente la introducción de servicios informáticos o tecnologías de Internet ha dado lugar a nuevas formas de delito, poco después de que se introdujese la tecnología. Un ejemplo es la aparición de las redes informáticas; el primer acceso no autorizado a estas redes informáticas se produjo poco después. De forma similar, los primeros delitos de software aparecieron al poco tiempo de la introducción de las computadoras personales en los años 80, cuando estos sistemas se utilizaron para copiar productos de software.

Lleva algún tiempo actualizar las leyes penales para procesar nuevas formas de ciberdelito en línea y algunos países aún no han finalizado este proceso de ajuste. Los delitos que han sido criminalizados con arreglo a las leyes penales nacionales deben revisarse y actualizarse, por ejemplo, la información digital debe tener un carácter equivalente a las firmas y los listados impresos tradicionales. Sin la integración de los ciberdelitos no pueden procesarse estas infracciones.

El reto principal de los sistemas jurídicos penales nacionales es el retraso existente entre el reconocimiento de abusos potenciales de las nuevas tecnologías y las modificaciones necesarias que deben introducirse en las leyes penales nacionales. Este reto sigue siendo tan importante y fundamental como siempre, puesto que cada vez es mayor la velocidad en la innovación de las redes. Muchos países están trabajando intensamente para introducir los ajustes jurídicos pertinentes. Por regla general, el proceso de ajuste consta de tres etapas:

- Los ajustes a las leyes nacionales deben empezar con el reconocimiento de una utilización delictiva de la nueva tecnología. Es necesario que las autoridades nacionales competentes cuenten con departamentos específicos cualificados para investigar los posibles ciberdelitos. La creación de equipos de respuesta de emergencia informática (CERT), de equipos de respuesta a incidencias informáticas (CIRT), de equipos de respuesta a incidentes de seguridad informática (CSIRT) y de otros mecanismos de investigación ha mejorado la situación.
- La segunda etapa consiste en identificar las lagunas en el Código Penal. Para garantizar unas bases jurídicas eficaces, es necesario comparar la situación de las disposiciones jurídicas penales en las leyes nacionales con los requisitos que surgen debido a los nuevos tipos de delitos. En muchos casos, las leyes existentes pueden cubrir nuevas variedades de delitos existentes (por ejemplo, las leyes relativas a la falsificación pueden aplicarse fácilmente a documentos electrónicos). La necesidad de introducir modificaciones legislativas se limita a los delitos omitidos o insuficientemente contemplados por las leyes nacionales.
- La tercera etapa es la redacción de la nueva legislación. Basándose en la experiencia, puede ser difícil para las autoridades nacionales llevar a cabo el proceso de redacción relativo a los ciberdelitos sin la cooperación internacional, debido al rápido desarrollo de las nuevas tecnologías y a sus complejas estructuras. Una legislación sobre el ciberdelito por separado puede dar lugar a una duplicación significativa y a un derroche de recursos, y también es necesario verificar el desarrollo de la normativa y estrategias internacionales. Sin la armonización internacional de las disposiciones jurídicas penales nacionales, la lucha contra

el ciberdelito transnacional tropezará con serias dificultades debido a la incoherencia o a la incompatibilidad de las legislaciones nacionales. En consecuencia, cada vez adquieren más importancia los intentos internacionales para armonizar las diferentes leyes penales nacionales. Las leyes nacionales pueden beneficiarse enormemente de la experiencia de otros países y de la asesoría jurídica de expertos internacionales.

El número cada vez mayor de ciberdelitos reconocidos y las herramientas técnicas para automatizar estos tipos de delitos (incluidos los sistemas de compartición de archivos anónimos y los productos de software diseñados para crear virus informáticos) hace que la lucha contra el ciberdelito se haya convertido en un elemento esencial de las actividades relativas al cumplimiento de la ley en todo el mundo. El ciberdelito constituye un reto para las autoridades competentes tanto de los países desarrollados como en desarrollo. Como las TIC crecen de manera tan rápida, especialmente en los países en desarrollo, es esencial la creación e implementación de una estrategia anticiberdelito eficaz como parte de la estrategia de ciberseguridad nacional.

La ciberseguridad desempeña un papel importante en el desarrollo en curso de la tecnología de la información así como de los servicios de Internet. Hacer que Internet sea más seguro (y proteger a los usuarios de Internet) se ha convertido en parte integrante del desarrollo de nuevos servicios así como de la política gubernamental. Las estrategias de ciberseguridad, por ejemplo el desarrollo de sistemas de protección técnica o la educación de los usuarios para evitar que sean víctimas de ciberdelitos, pueden ayudar a disminuir el riesgo del ciberdelito.

***Implementación de las estrategias existentes***

Una posibilidad consiste en que las estrategias anticiberdelito establecidas en los países industrializados puedan introducirse en los países en desarrollo, lo que ofrece la ventaja de una disminución en los costos y en el tiempo para su desarrollo. La implementación de estrategias existentes podría permitir a los países en desarrollo beneficiarse de los actuales conocimientos y experiencia.

No obstante, la implementación de una estrategia anticiberdelito ya existente plantea un cierto número de dificultades. Aunque tanto los países en desarrollo como los países desarrollados se enfrentan a retos similares, las soluciones óptimas que pueden adoptarse dependen de los recursos y capacidades de cada país. Los países industrializados pueden promover la ciberseguridad de manera distinta y más flexible; por ejemplo, centrándose en temas de protección técnica más costosos.

Existen otros temas que deben tener en cuenta los países en desarrollo que adopten estrategias anticiberdelito existentes:

• Compatibilidad de los respectivos sistemas jurídicos;

• Situación de las iniciativas de apoyo (por ejemplo, educación de la sociedad);

• Ampliación de las medidas de autoprotección in situ; y

• Ampliación del soporte por parte del sector privado (por ejemplo, mediante asociaciones públicas/privadas), entre otros temas.

La Agenda sobre Ciberseguridad Global tiene siete objetivos estratégicos principales basados en cinco áreas de trabajo:

1) Medidas legales;

2) Medidas técnicas y de procedimiento;

3) Estructuras institucionales;

4) Creación de capacidades;

5) Cooperación internacional.

Las medidas legales son probablemente las más importantes con respecto a una estrategia anticiberdelito. Ello requiere en primer lugar la elaboración de las leyes penales sustantivas necesarias para criminalizar actos tales como fraude informático, acceso ilegal, interferencia en los datos, violaciones del derecho de propiedad intelectual y pornografía infantil. El hecho de que existan disposiciones en el Código Penal que son aplicables a actos similares cometidos fuera de la red no significa que puedan aplicarse también a los actos cometidos a través de Internet. Por consiguiente, es muy importante realizar un análisis profundo de la actual legislación nacional a fin de identificar posibles lagunas jurídicas.

Los delincuentes pueden actuar desde cualquier lugar del mundo y tomar las medidas necesarias para enmascarar su identidad. Las herramientas e instrumentos jurídicos necesarios para investigar el ciberdelito pueden ser muy distintos de los que se utilizan en la investigación de los delitos ordinarios. Debido a la dimensión internacional de los ciberdelitos es preciso, además, desarrollar un marco jurídico nacional capaz de cooperar con las autoridades competentes exteriores

Las investigaciones relativas al ciberdelito a menudo tienen una fuerte componente técnica. Además, el requisito de mantener la integridad de la evidencia durante una investigación exige la aplicación de procedimientos precisos. Por consiguiente, el desarrollo de las capacidades y procedimientos necesarios es un requisito esencial en la lucha contra el ciberdelito.

***Desarrollo de los sistemas de protección técnica.***

Los sistemas informáticos bien protegidos son más difíciles de atacar. Un primer paso de gran importancia es la mejora de la protección técnica estableciendo las adecuadas normas de seguridad. Por ejemplo, los cambios en el sistema bancario en línea han eliminado la mayoría de los peligros planteados por los actuales ataques de usurpación de identidad ("phishing"), demostrando la importancia fundamental que tiene el adoptar las soluciones técnicas.

La protección del usuario puede lograrse de manera indirecta, ofreciendo seguridad a los servicios que utiliza el consumidor; por ejemplo, servicios bancarios en línea. Este método indirecto para proteger a los usuarios de Internet puede reducir el número de personas e instituciones necesarias que deben incluirse en las etapas para promover la protección técnica.

Aunque limitar el número de personas necesarias que deben incluirse en el sistema de protección técnica puede parecer conveniente, los usuarios de servicios informáticos y de Internet a menudo constituyen el eslabón más débil y el objetivo principal de los delincuentes. Generalmente es más sencillo atacar computadoras privadas para obtener información sensible que sistemas de computadoras bien protegidas de una institución financiera. A pesar de estos problemas logísticos, la protección de la infraestructura del usuario final es fundamental para lograr la protección técnica de toda la red.

El ciberdelito es un fenómeno global. Para poder investigar eficazmente estos delitos es necesario establecer una armonización de las leyes y desarrollar los métodos adecuados para lograr la cooperación internacional. Con objeto de garantizar el desarrollo de las normas mundiales en los países desarrollados así como en los países en desarrollo es preciso la creación de capacidad.

Además de la creación de capacidad se requiere la educación del usuario. Algunos ciberdelitos, especialmente los relativos al fraude tales como usurpación de identidad ("phishing") y falsificación de direcciones de origen o piratería ("spoofing"), no se producen generalmente debido a la ausencia de protección técnica sino a causa de una falta de atención por parte de las víctimas.

Un requisito importante para lograr una estrategia educativa e informativa eficaz es la comunicación abierta de las últimas amenazas de los ciberdelitos. Algunos Estados y/o empresas privadas rehúsan hacer hincapié en el hecho de que los ciudadanos y clientes están afectados por amenazas de ciberdelito, para evitar la pérdida de confianza en los servicios de comunicación en línea.

Cuando el delincuente no se encuentra en el mismo país que la víctima, la investigación requiere la cooperación entre las autoridades competentes de todos los países que resulten afectados. Las investigaciones internacionales y transnacionales sin el consentimiento de las autoridades competentes en los países correspondientes son difíciles en lo que respecta al principio de soberanía nacional. Este principio, en general, no permite que un país lleve a cabo investigaciones dentro del territorio de otro país sin el expreso permiso de las autoridades locales. Por lo tanto, las investigaciones deben realizarse con el apoyo de las autoridades de todos los países implicados.

## ***4.1 LEGISLACIÓN SOBRE ACCESO ILÍCITO A SISTEMAS INFORMÁTICOS***

La legislación sobre protección de los sistemas informáticos ha de perseguir acercarse lo más posible a los distintos medios de protección ya existentes, creando una nueva regulación sólo en aquellos aspectos en los que, basándose en las peculiaridades del objeto de protección, sea imprescindible.

Si se tiene en cuenta que los sistemas informáticos, pueden entregar datos e informaciones sobre miles de personas, naturales y jurídicas, en aspectos tan fundamentales para el normal desarrollo y funcionamiento de diversas actividades como bancarias, financieras, tributarias, previsionales y de identificación de las personas. Y si a ello se agrega que existen Bancos de Datos, empresas o entidades dedicadas a proporcionar, si se desea, cualquier información, sea de carácter personal o sobre materias de las más diversas disciplinas a un Estado o particulares; se comprenderá que están

en juego o podrían ha llegar a estarlo de modo dramático, algunos valores colectivos y los consiguientes bienes jurídicos que el ordenamiento jurídico institucional debe proteger.

No es la amenaza potencial de la computadora sobre el individuo lo que provoca desvelo, sino la utilización real por el hombre de los sistemas de información con fines de espionaje.

No son los grandes sistemas de información los que afectan la vida privada sino la manipulación o el consentimiento de ello, por parte de individuos poco conscientes e irresponsables de los datos que dichos sistemas contienen.

La humanidad no está frente al peligro de la informática sino frente a la posibilidad real de que individuos o grupos sin escrúpulos, con aspiraciones de obtener el poder que la información puede conferirles, la utilicen para satisfacer sus propios intereses, a expensas de las libertades individuales y en detrimento de las personas. Asimismo, la amenaza futura será directamente proporcional a los adelantos de las tecnologías informáticas.

La protección de los sistemas informáticos puede abordarse tanto desde una perspectiva penal como de una perspectiva civil o comercial, e incluso de derecho administrativo. Estas distintas medidas de protección no tienen por qué ser excluyentes unas de otras, sino que, por el contrario, éstas deben estar estrechamente vinculadas. Por eso, dadas las características de esta problemática sólo a través de una protección global, desde los distintos sectores del ordenamiento jurídico, es posible alcanzar una cierta eficacia en la defensa de los ataques a los sistemas informáticos.

Un análisis de las legislaciones que se han promulgado en diversos países arroja 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.

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, aun 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 clientes.

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

El «Manual de la 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.

* Falta de 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. Las ventajas y las necesidades del flujo nacional e internacional de datos, que aumenta de modo creciente aún en países latinoamericanos, conlleva también a la posibilidad creciente de estos delitos; por eso puede señalarse que 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.

### ***4.1.1 Acceso ilícito y otros***

El acceso ilícito a los sistemas informáticos dificulta a los operadores una gestión, explotación y control de sus sistemas sin perturbación o impedimento. La finalidad de la protección es mantener la integridad de los sistemas informáticos. Es esencial hacer una distinción entre el acceso ilícito y las subsiguientes infracciones (tales como el espionaje de datos), dado que las disposiciones jurídicas abordan de diferente manera la protección. En la mayoría de los casos, el acceso ilícito (cuando la ley trata de proteger la integridad del propio sistema informático) no es el objetivo final, sino más bien un primer paso en la consecución de otros delitos, tales como la modificación u obtención de datos almacenados (cuando la ley trata de proteger la integridad y la confidencialidad de los datos).

La cuestión consiste en determinar si se debe penalizar o no el acto de acceso ilícito, además de los subsiguientes delitos. De un análisis de los diversos enfoques aplicados para la penalización del acceso informático ilícito a escala nacional se desprende que las disposiciones vigentes al respecto a veces confunden el acceso ilícito con los delitos subsiguientes, o tratan de limitar la penalización del acceso ilícito únicamente a los casos de graves violaciones. En algunos países se penaliza el mero acceso, mientras que en otros se limita la penalización únicamente a los casos en los cuales el sistema al que se ingresó está protegido con medidas de seguridad, o cuando el perpetrador tiene

intenciones perjudiciales, o cuando se obtuvieron, modificaron o dañaron datos. En otros países no se penaliza el acceso propiamente dicho, sino únicamente los delitos subsiguientes. Los detractores de la penalización del acceso ilícito aducen como argumento en contra situaciones en las cuales la mera intrusión no creó peligro alguno, o los casos en los cuales los actos de "acceso ilícito" condujeron a la detección de fallos o debilidades en los sistemas de seguridad de las computadoras.

### ***4.1.2 Convenio sobre la Ciberdelincuencia***

El Convenio sobre la Ciberdelincuencia, realizado por los integrantes del Consejo de Europa el 23 de noviembre de 2001, contiene una disposición sobre el acceso ilegal que protege la integridad de los sistemas informáticos mediante la penalización del acceso no autorizado a un sistema. Habida cuenta de la adopción de enfoques incoherentes a escala nacional, el Convenio ofrece la posibilidad de imponer limitaciones que por lo menos en la mayoría de los casos permiten a los países carentes de legislación mantener en vigor unas leyes más liberales en la esfera del acceso ilícito.

Disposición

Artículo 2 – Acceso ilícito

*"Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a todo o parte de un sistema informático. Las Partes podrán exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos u otra intención delictiva, o en relación con un sistema informático conectado a otro sistema informático."*

***Actos contemplados***

El término "acceso" no especifica un medio concreto de comunicación, sino que admite diversas connotaciones y está abierto a nuevos adelantos técnicos. Este término se refiere a todos los medios de ingresar en otro sistema informático, con inclusión de los ataques por Internet, así como el acceso ilícito a las redes inalámbricas. En la disposición se contempla incluso el acceso no autorizado a las computadoras que no están conectadas a ninguna red (por ejemplo, esquivando la protección de una contraseña). En aplicación de este amplio enfoque, el acceso ilícito no sólo abarca los futuros adelantos técnicos, sino también los datos secretos a los que tienen acceso las personas informadas y los empleados. La segunda frase del Artículo 2 ofrece la posibilidad de limitar la penalización del acceso ilícito al acceso a través de una red.

Así pues, los actos ilícitos y los sistemas protegidos se definen de tal modo que su concepto queda abierto a la evolución futura. En el Informe Explicativo se enumeran los equipos, componentes, datos almacenados, directorios, los datos relacionados con el contenido y el tráfico como ejemplos de las partes de un sistema informático a las que es posible obtener acceso.

***Predisposición***

Al igual que todos los otros delitos definidos en el Convenio sobre la Ciberdelincuencia, en el Artículo 12 se exige que para penalizar un delito el delincuente lo haya efectuado de manera intencional. El Convenio no contiene una definición del término "internacionalmente". Los redactores del Informe Explicativo subrayaron que la definición de "intencionalmente" debe considerarse a nivel nacional.

***Sin derecho***

Lo que dice el Artículo 2 del Convenio, es que el acceso a una computadora sólo puede penalizarse si éste tiene lugar "sin derecho". Se considera que el acceso a un sistema que permite al público su acceso libre y abierto o el acceso a un sistema con la autorización del propietario u otro titular de derechos no es un acceso "sin derecho".

Además del tema del acceso libre, también se aborda la legitimidad de los procedimientos de ensayo de seguridad. Los administradores de la red y las compañías encargadas de la seguridad que someten a prueba la protección de los sistemas informáticos con miras a detectar posibles deficiencias manifestaron su inquietud respecto de la posibilidad de penalización en el marco del acceso ilegal. Pese al hecho de que en general estos profesionales trabajan con el permiso del propietario y por consiguiente actúan legalmente, los redactores del Convenio hicieron hincapié en que "el ensayo o la protección del sistema de seguridad de una computadora con autorización del propietario o del operador [...] se consideran actos con derecho".

El hecho de que la víctima del delito le haya transmitido al infractor una contraseña o un código de acceso similar no implica forzosamente que el delincuente haya actuado con derecho al penetrar al sistema informático de la víctima. Si el delincuente persuadió a la víctima de que le revelase una contraseña o un código de acceso mediante una astuta manipulación social, es necesario verificar si la autorización concedida por la víctima incluye al acto efectuado por el delincuente. Por lo general éste no es el caso y por lo tanto el delincuente actúa sin derecho.

### ***4.1.3 El G8***

En la Conferencia del G8 (la cual está conformada por: Canadá, Francia, Alemania, Italia, Japón, Gran Bretaña EE.UU. y la Federación Rusia) organizada en París, Francia, en 2008, el G8 abordó el tema del ciberdelito e hizo un llamamiento para oponerse a la constitución de refugios digitales ilegales. Ya en esas fechas, el G8 se esforzó por ofrecer una relación entre los intentos de sus miembros por buscar soluciones internacionales en lo que concierne al Convenio sobre la Ciberdelincuencia del Consejo de Europa. El G8 debatió sobre una serie de instrumentos de procedimiento para luchar contra el ciberdelito en un taller celebrado en Tokio en 2001, en el cual la atención se centró en determinar si habría que implementar la obligación de retener datos o si la preservación de los mismos podría ser una solución opcional.

### ***4.1.4 Naciones Unidas***

En el contexto internacional, son pocos los países que cuentan con una legislación apropiada. Entre ellos, se destacan, Estados Unidos, Alemania, Austria, Gran Bretaña, Holanda, Francia, España, Argentina y Chile.

Dado lo anterior a continuación se mencionan algunos aspectos relacionados con la ley en los diferentes países, así como con los delitos informáticos que persigue.

### ***4.1.5 Estados Unidos.***

Este país adoptó en 1994 el Acta Federal de Abuso Computacional que modificó al Acta de Fraude y Abuso Computacional de 1986.

Con la finalidad de eliminar los argumentos técnicos acerca de qué es y que no es un virus, un gusano, un caballo de Troya y en que difieren de los virus, la nueva acta proscribe la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, a los sistemas informáticos, a las redes, información, datos o programas. La nueva ley es un adelanto porque está directamente en contra de los actos de transmisión de virus.

Asimismo, en materia de estafas electrónicas, defraudaciones y otros actos dolosos relacionados con los dispositivos de acceso a sistemas informáticos, la legislación estadounidense sanciona con pena de prisión y multa, a la persona que defraude a otro mediante la utilización de una computadora o red informática.

#### ***4.1.6 Alemania.***

Este país sancionó en 1986 la Ley contra la Criminalidad Económica, que contempla los siguientes delitos:

* Espionaje de datos.

* Estafa informática.

* Alteración de datos.

* Sabotaje informático.

#### ***4.1.7 Austria.***

La Ley de reforma del Código Penal, sancionada el 22 de Diciembre de 1987, 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 comenten este hecho utilizando su profesión de especialistas en sistemas.

#### ***4.1.8 Gran Bretaña.***

Debido a un caso de hacking en 1991, comenzó a regir en este país la ComputerMisuseAct (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 específica la modificación de datos sin autorización.

#### ***4.1.9 Holanda.***

El 1º de marzo de 1993 entró en vigencia la Ley de Delitos Informáticos, en la cual se penaliza los siguientes delitos:

* El hacking.

* El phreacking (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).

* La distribución de virus.

### ***4.1.10 Francia.***

En enero de 1988, este país dictó la Ley relativa al fraude informático, en la que se consideran aspectos como:

* Intromisión fraudulenta que suprima o modifique datos.

* Conducta intencional en la violación de derechos a terceros que haya impedido o alterado el funcionamiento de un sistema de procesamiento automatizado de datos.

* Conducta intencional en la violación de derechos a terceros, en forma directa o indirecta, en la introducción de datos en un sistema de procesamiento automatizado o la supresión o modificación de los datos que éste contiene, o sus modos de procesamiento o de transmisión.

* Supresión o modificación de datos contenidos en el sistema, o bien en la alteración del funcionamiento del sistema (sabotaje).

### ***4.1.11 España.***

En el Nuevo Código Penal de España, se establece que al que causare daños en propiedad ajena, se le aplicará pena de prisión o multa. En lo referente a:

* La realización por cualquier medio de destrucción, alteración, inutilización o cualquier otro daño en los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

* El nuevo Código Penal de España sanciona en forma detallada esta categoría delictual (Violación de secretos/Espionaje/Divulgación), aplicando pena de prisión y multa.

* En materia de estafas electrónicas, el nuevo Código Penal de España, solo tipifica las estafas con ánimo de lucro valiéndose de alguna manipulación informática, sin detallar las penas a aplicar en el caso de la comisión del delito.

### ***4.1.12 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. Esta ley se refiere a los siguientes delitos:

* La destrucción o inutilización de los de los datos contenidos dentro de una computadora es castigada con penas de prisión. Asimismo, dentro de esas consideraciones se encuentran los virus.

* Conducta maliciosa tendiente a la destrucción o inutilización de un sistema de tratamiento de información o de sus partes componentes o que dicha conducta impida, obstaculice o modifique su funcionamiento.

* Conducta maliciosa que altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información.

### ***4.2 VISIÓN GENERAL DE LAS LEYES FEDERALES DE ESTADOS UNIDOS***

En general, un delito informático infringe las leyes Federales cuando cae dentro de una de estas categorías:

* Concierne el robo o pone en compromiso información sobre defensa nacional, relaciones exteriores, energía atómica u otra información reservada.

* Concierne una computadora propiedad de un departamento o agencia del gobierno de los EEUU.

* Concierne un banco o a la mayor parte de otros tipos de instituciones financieras.

* Concierne comunicaciones interestatales o con el extranjero.

* Concierne a gente u computadoras de otros estados o países.

De estos delitos, el FBI habitualmente tiene jurisdicción sobre los casos que afectan a la seguridad nacional, terrorismo, banca y crimen organizado. El Servicio Secreto tiene jurisdicción cuando la víctima es el Departamento del Tesoro o cuando se atacan computadoras es que no están bajo la jurisdicción del FBI o del Servicio Secreto de los EEUU (por ejemplo, en casos de robo de contraseñas o códigos de acceso). En ciertos casos federales, el Departamento de Aduanas, el Departamento de Comercio o una organización militar, como la Oficina de Investigación de las Fuerzas Aéreas, pueden tener la jurisdicción.

En los Estados Unidos hay un cierto número de leyes federales que protegen contra ataques a computadoras, uso indebido de contraseñas, invasiones electrónicas de la privacidad y otras transgresiones. La Ley sobre Fraude y Abuso Informático de 1986 es el principal conjunto de legislación por el que se gobierna la mayor parte de los delitos informáticos, aunque se puede recurrir a otras muchas leyes para perseguir diferentes tipos de esta clase de delitos. La ley enmendó el Título nº 18 del Código de los Estados Unidos s1030. También se complementó la Ley sobre Privacidad en las Comunicaciones Electrónicas de 1986, que prohibía la interceptación no autorizada de comunicaciones digitales, que no ha sido aprobada hasta hace realmente poco. La Ley de Enmienda sobre Abuso Informático de 1994 amplió la Ley de 1986 para tratar la transmisión de virus y otro código dañino.

Además de las leyes federales, la mayoría de los Estados han adoptado sus propias leyes sobre delitos informáticos. Cierto número de países fuera de los Estados Unidos han aprobado también legislaciones definiendo y prohibiendo el delito informático.

#### ***4.2.1 Las dos leyes sobre delitos federales más importantes en EEUU.***

Como se menciona más arriba, las dos leyes sobre delitos Federales de los EEUU más importantes son el Título nº 18 del Código de los EEUU: Capítulo 47, Secciones 1029 y 1030.

##### ***4.2.1.1 Sección 1029***

La sección 1029 prohíbe el fraude y demás actividades relacionadas que son posibles gracias a dispositivos de acceso falsificados como PINs (números privados de identificación), tarjetas de crédito, números de cuenta y diversos tipos de identificadores electrónicos. Las nueve áreas de

actividad delictiva cubiertas por la Sección 1029 están listadas en la tabla número 17. Todas "exigen" que el delito involucre comercio interestatal o internacional.

| ***DELITO*** | ***MULTA Y/O CASTIGO*** |
|---|---|
| Crear, usar o traficar con dispositivos de acceso falsificados. (El delito debe ser cometido con conocimiento e intención de defraudar). | Multa de 50.000 dólares o el doble del valor del delito y/o hasta 15 años de prisión, 100,000 dólares y/o hasta 20 años si hay reincidencia. |
| Usar u obtener dispositivos de acceso no autorizados para obtener algo de un valor de 1000 dólares o más durante un periodo de un año. (El delito debe ser cometido con conocimiento e intención de defraudar). | Multa de 10.000 dólares o el doble del valor del delito y/o hasta 10 años de prisión, 100,000 dólares y/o hasta 20 años si hay reincidencia. |
| Poseer 15 o más dispositivos de acceso falsificados o no autorizados. (El delito debe ser cometido con conocimiento e intención de defraudar). | Multa de 10.000 dólares o el doble del valor del delito y/o hasta 10 años de prisión, 100,000 dólares y/o hasta 20 años si hay reincidencia. |
| Crear, traficar con, o tener equipos de fabricación de dispositivos de acceso. (El delito debe ser cometido con conocimiento e intención de defraudar). | Multa de 50,000 dólares o el doble del valor del crimen y/o hasta 15 años de prisión, 1,000,000 de dólares y/o hasta 20 años si hay reincidencia. |
| Efectuar transacciones con dispositivos de acceso facilitados a otra persona con el objeto de recibir pagos o algo de un valor total de 1000 dólares o más durante el periodo de un año. (El delito debe ser cometido con conocimiento e intención de defraudar). | Multa de 10,000 dólares, o el doble del valor del crimen y/o hasta 10 años en prisión, 100.000 y/o hasta 20 años si hay reincidencia. |
| Contactar con una persona con el propósito de ofrecer un dispositivo de acceso o vender información que puede ser usada para obtener un dispositivo de acceso. (El delito debe ser cometido con conocimiento e intención de defraudar, y sin la autorización del emisor del dispositivo de acceso). | Multa de 50.000 dólares o el doble del valor del delito y/o hasta 15 años de prisión, 100,000 dólares y/o hasta 20 años si hay reincidencia. |
| Usar, crear, traficar con o poseer un instrumento de telecomunicación que ha sido modificado o alterado para obtener el uso no autorizado de servicios de telecomunicaciones. (El delito debe cometerse con conocimiento e intención de defraudar). | Multa de 50.000 dólares o el doble del valor del delito y/o hasta 15 años de prisión, 100,000 y/o hasta 20 años si hay reincidencia. |
| Usar, crear, traficar con o tener un escáner de radiofrecuencia o hardware o software usados para alterar o modificar instrumentos de telecomunicación para obtener acceso no autorizado a servicios de telecomunicación. | Multa de 50.000 dólares o el doble del valor del delito y/o hasta 15 años de prisión, 100,000 y/o hasta 20 años si hay reincidencia. |
| Dar pie a u organizar la presentación por parte de una persona a un miembro de un sistema de tarjetas de crédito o su agente de pago de registros de transacciones hechas mediante un dispositivo de acceso. (El delito debe ser cometido con conocimiento e intención de defraudar, y sin | Multa de 10.000 dólares o el doble del valor del delito y/o hasta 10 años de prisión, 100,000 y/o hasta 20 años si hay reincidencia. |

| | |
|---|---|
| la autorización del miembro del sistema de tarjetas de crédito o su agente). | |

Tabla 17. Sección 1029 de la Ley de E.U.A.

#### ***4.2.1.2 Sección 1030***

Título nº 18 del Código de los EEUU, Capítulo 47, Sección 1030, promulgada como parte de la Ley sobre Fraude y Abuso Informático de 1986, prohíbe el acceso no autorizado o fraudulento a las computadoras del gobierno y establece penas para tal tipo de acceso. Esta ley es uno de los escasos componentes de legislación federal que se refiere exclusivamente a computadoras. Bajo la Ley sobre Fraude y Abuso Informático, al Servicio Secreto de los EEUU y al FBI se les ha proporcionado explícitamente jurisdicción para investigar los delitos definidos bajo este ACTA.

Las seis áreas de actividad delictiva cubiertas por la Sección 1030 se muestran en la tabla 18:

| ***DELITO*** | ***EJEMPLO DE APLICACIÓN*** | ***PENA*** |
|---|---|---|
| Adquirir información reservada sobre defensa nacional, relaciones exteriores o energía atómica con la intención o dando motivos razonables para creer que la información pueda ser usada para dañar a los Estados Unidos o beneficiar a cualquier otro país. | Un hacker irrumpiendo en páginas y archivos confidenciales del gobierno o de sus fuerzas armadas, con el único fin de traicionar a su patria. | No definida |
| Obtención de información en un registro financiero de una institución financiera o de un emisor de tarjetas de crédito, o información sobre un consumidor en un archivo de una agencia de información sobre consumidores. | Penetrar las bases de datos de cualquier institución bancaria o de los burós de crédito. | Multa y/o hasta 1 año de prisión, de hasta 10 años si hay reincidencia. |
| Afectar una computadora de uso exclusivo de un departamento o agencia del gobierno de los EEUU o, si no es exclusiva, una usada por el gobierno donde el delito afecte adversamente a su utilización por parte del gobierno. | Esto podría aplicarse a los ataques de inundación con paquetes syn y a los “pings de la muerte”, así como a otros ataques de denegación de servicio, la irrupción en una computadora y el andar fastidiando. | Multa y/o hasta un año de cárcel, hasta 10 años si hay reincidencia. |
| Agravar un fraude al acceder a una computadora de interés federal y obtener cualquier cosa de valor, a menos que el fraude y el objeto obtenido consistan únicamente en el uso del equipo. | Incluso si se descargan copias de programas sólo para estudiarlos, esta ley significa que si el dueño del programa dice “Bueno, yo diría que vale un millón de dólares”, se estará en un grave problema. | Multa y/o hasta 5 años de cárcel, hasta 10 años si hay reincidencia. |
| Mediante el uso de una computadora utilizada en el comercio interestatal, provocar con conocimiento de causa la transmisión de un programa, información, código u orden a un sistema informático. Hay dos escenarios distintos: 1. La persona que genera la transmisión pretende dañar el equipo o impedir su uso; y 2. La transmisión ocurre sin la autorización de los | La forma más común de meterse en problemas con esta parte de la ley es cuando se está intentando borrar las huellas después de irrumpir en una computadora. Mientras se edita o, aún peor, se eliminan diferentes archivos, el intruso puede accidentalmente borrar algo | Multa y/o hasta 5 años de prisión, hasta 10 años si hay reincidencia. |

| | | |
|---|---|---|
| propietarios u operadores de la computadora, y causa 1000 dólares o más de pérdidas o daños, o modifica o dificulta, o potencialmente modifica o dificulta, un tratamiento o examen médico | importante o complicarse de verdad con alguna orden que dé. | |
| Fomentar un fraude al traficar con claves o información similar que permita que se acceda a una computadora sin autorización, si el tráfico afecta al comercio interestatal o internacional o si la computadora afectada se usa por o para el gobierno. | Un modo común de infringir esta parte de la ley viene del deseo de alardear. Cuando un hacker encuentra un modo de entrar en la computadora de otra persona, puede ser realmente tentador pasar la clave a algún otro. Rápidamente docenas de novatos sin idea están incordiando en el equipo de la víctima, y por supuesto ellos también alardearán. | Multa y/o hasta 1 año de cárcel, hasta 10 años si hay reincidencia. |

Tabla 18. Sección 1030 de la Ley Federal de E.U.A.

### ***4.3 LEGISLACIÓN SOBRE DELITOS INFORMATICOS ESPAÑA***

Los artículos más importantes en el **Código Penal de España** en materia de delitos informáticos, son el 197 y el 264, los cuales incluyen casi todos los delitos en los que cualquier persona ajena al gobierno del país o a instituciones de cualquier índole puede ser víctima. Los artículos mencionan lo siguiente:

***Artículo 197***

- El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación.
- Al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en archivos o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.
- El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo.
- Difusión, revelación o cesión a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.
- Si los hechos descritos en los primeros dos apartados de este artículo se realizan por las personas encargadas o responsables de los archivos, soportes informáticos, electrónicos o

telemáticos, archivos o registros, se impondrá la pena de prisión de tres a cinco años, y si se difunden, ceden o revelan los datos reservados, se impondrá la pena en su mitad superior.

- Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o un incapaz, se impondrán las penas previstas en su mitad superior.
- Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado anterior, la pena a imponer será la de prisión de cuatro a siete años.
- Si los hechos descritos en los apartados anteriores se cometiesen en el seno de una organización o grupo criminales, se aplicarán respectivamente las penas superiores en grado.

***Artículo 264***

- El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese, o hiciese inaccesibles datos, o programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a dos años.
- El que por cualquier medio, sin estar autorizado y de manera grave obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, cuando el resultado producido fuera grave, será castigado, con la pena de prisión de seis meses a tres años.
- Se impondrán las penas superiores en grado a las respectivamente señaladas en los dos apartados anteriores y, en todo caso, la pena de multa del tanto al décuplo del perjuicio ocasionado, cuando en las conductas descritas concurra alguna de las siguientes circunstancias:

  1º. Se hubiese cometido en el marco de una organización criminal.
  2º. Haya ocasionado daños de especial gravedad o afectado a los intereses generales.

Otros artículos que hablan acerca de delitos informáticos dentro del Código Penal de España son los mencionados en la tabla 19.

| ***ARTICULO*** | ***DESCRIPCIÓN*** |
|---|---|
| ***Artículo 198*** | La autoridad o funcionario público que, fuera de los casos permitidos por la Ley, sin mediar causa legal por delito, y prevaliéndose de su cargo, realizare cualquiera de las conductas descritas en el artículo anterior, será castigado con las penas respectivamente previstas en el mismo, en su mitad superior y, además, con la de inhabilitación absoluta por tiempo de seis a doce años |
| ***Artículo 199*** | 1.- El que revelare secretos ajenos, de los que tenga conocimiento por razón de su oficio o sus relaciones laborales, será castigado con la pena de prisión de uno a tres años y multa de seis a doce meses.<br>2.- El profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue los secretos de otra persona, será castigado con la pena de prisión de uno a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para dicha profesión por tiempo de dos a seis años. |
| ***Artículo 211*** | La calumnia y la injuria se reputarán hechas con publicidad cuando se propaguen por medio de la imprenta, la radiodifusión o por cualquier otro medio de eficacia semejante. |
| ***Artículo 248*** | 1. Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.<br>2. También se consideran reos de estafa:<br>a) Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.<br>b) Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo.<br>c) Los que utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero. |
| ***Artículo 255*** | Será castigado con la pena de multa de tres a 12 meses el que cometiere defraudación por valor superior a 400 euros, utilizando energía eléctrica, gas, agua, telecomunicaciones u otro elemento, energía o fluido ajenos |
| ***Artículo 256*** | El que hiciere uso de cualquier equipo terminal de telecomunicación, sin consentimiento de su titular, ocasionando a éste un perjuicio superior a 400 euros, será castigado con la pena de multa de tres a 12 meses. |
| ***Artículo 270*** | . Será castigado con la pena de prisión de seis meses a dos años y multa de 12 a 24 meses quien, con ánimo de lucro y en perjuicio de tercero, reproduzca, plagie, distribuya o comunique públicamente, en todo o en parte, una obra literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios.<br><br>Será castigado también con la misma pena quien fabrique, importe, ponga en circulación o tenga cualquier medio específicamente destinado a facilitar la |

| | |
|---|---|
| | supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de computadora o cualquiera de las otras obras, interpretaciones o ejecuciones en los términos previstos en el apartado 1 de este artículo. |
| ***Artículo 278*** | El que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo |
| ***Artículo 536*** | La autoridad, funcionario público o agente de éstos que, mediando causa por delito, interceptare las telecomunicaciones o utilizare artificios técnicos de escuchas, transmisión, grabación o reproducción del sonido, de la imagen o de cualquier otra señal de comunicación, con violación de las garantías constitucionales o legales, incurrirá en la pena de inhabilitación especial para empleo o cargo público de dos a seis años. |

Tabla 19. Leyes de España sobre delitos informáticos.

## *4.4 LEGISLACIONES CONTRA EL CIBERDELITO EN LOS ESTADOS UNIDOS MEXICANOS.*

Este tipo de delitos, se manejan de un modo distinto a los que son meramente informáticos, ya que los delitos que a continuación se describen, no son de naturaleza tecnológica, es decir, se pueden cometer sin la ayuda de las tecnologías de la información.

Las tecnologías de la información, solo son una herramienta más para cometer este tipo de delitos; como un ejemplo, puede quedar el incurrir en homicidio: el arma puede variar, ya sea que utilicen un arma de fuego, un arma blanca; utilizando las tecnologías de la información, lo que cambia es el medio por el que se está difundiendo la información, o en su defecto, el medio por el cual se está realizando directamente el delito: un fraude bancario, ahora utilizando Internet y no medios tradicionales como cheques falsos, por mencionar alguno.

Cuando estos delitos se apoyan en las tecnologías de la información, repercuten en mayor grado al afectado o a los afectados y por desgracia no se considera el nivel de esta repercusión, sino solamente la naturaleza del delito.

En la tabla número 20, se muestra una descripción breve de las leyes y los artículos que describen y penalizan los delitos que utilizan medios informáticos para su ejecución.

| ***DELITO*** | ***DOCUMENTO QUE LA DESCRIBE*** | ***DESCRIPCION*** |
|---|---|---|
| ***Espionaje*** | Artículo 16 de la Constitución Política de los | Las comunicaciones privadas son inviolables, la ley sancionará de forma penal todo aquel acto y/o persona que espíe o que atente contra la libertad y la privacidad de la información confidencial; Un juez debe valorar el alcance de estas intervenciones, con la |

| | | |
|---|---|---|
| | Estados Unidos Mexicanos. | condición de que siempre contengan información relacionada con un delito; de cualquier otra información, que viole la privacidad de las personas, no se admitirá su intervención |
| | Código Penal Federal, artículo 167.<br><br>Código Penal Federal, artículo 167. | Irrupción e intervención de las comunicaciones alámbricas o inalámbricas, que sean telegráficas, telefónicas o vía satélite, y que contengan señales de audio, video o datos.<br>También se castigará a todas las personas que decodifiquen señales de telecomunicaciones distintas a las de satélite portadoras de programas, y a quien transmita la propiedad, uso de aparatos, instrumentos o información que permitan descifrar señales de telecomunicaciones distintas a las de satélite portadoras de programas |
| | Código Penal Federal, artículo 177. | A quien intervenga comunicaciones privadas sin mandato de orden judicial. |
| ***Terrorismo*** | Código Penal Federal, artículo 139. | El Código Penal Federal no menciona nada acerca de realizar terrorismo por medios informáticos. Solo se reserva a mencionar **cualquier medio físico para realizar estos actos, como lo pueden ser bombas, fuego, ataques con armas**, y todas las técnicas utilizadas tradicionalmente por grupos del crimen organizado, grupos revolucionarios, grupos anarquistas, o simplemente uno que otro hecho aislado procedente de "bromas"; sin embargo, una de las formas por las cuales se puede causar terror y pánico de manera colectiva, es mediante el uso de los recursos informáticos: una computadora, una conexión a Internet, y una cuenta en alguna red social, o en algún blog, más la difusión de alguna noticia con tintes terroristas, son suficientes para causarle pánico colectivo a la gente, lo que normalmente se define como terror |
| ***Conspiración y sabotaje*** | Código Penal Federal, artículos 140 y 141. | Al que dañe, destruya o ilícitamente entorpezca vías de comunicación, servicios públicos, funciones de las dependencias del estado, organismos públicos descentralizados, empresas de participación estatal o sus instalaciones; plantas siderúrgicas, eléctricas o de las industrias básicas; centros de producción o distribución de artículos de consumo necesarios de armas, municiones o implementos bélicos, con el fin de trastornar la vida económica del país o afectar su capacidad de defensa.<br>Se impondrá pena de uno a nueve años de prisión y multa hasta de diez mil pesos a quienes resuelvan de concierto cometer uno o varios de los delitos del presente Título y acuerden los medios de llevar a cabo su determinación.<br>Se consideran delitos de carácter político los de rebelión, sedición, motín y el de conspiración para cometerlos |
| ***Discriminación*** | Código Penal Federal, artículo 149. | A todo aquel que por razones de género, raza, preferencia sexual, edad, sexo, estado civil, condición económica, embarazo, o de cualquier otra índole, atente contra la dignidad humana o anule o menosprecie los derechos y libertades de las personas mediante la realización de ciertas conductas. |

| | | |
|---|---|---|
| ***Violación de correspondencia*** | Código Penal Federal, artículo 173. | Castigos al que abra indebidamente una comunicación escrita que no esté dirigida a él, y al que indebidamente intercepte una comunicación de este tipo, aunque la conserve cerrada.<br>Al que intervenga comunicaciones privadas sin mandato de la autoridad competente. |
| ***Pederastia*** | Código Penal Federal, artículo 209 bis. | A quien se aproveche de la confianza de un menor de 18 años, derivada de su parentesco, tutela, custodia, relación docente, o que tenga una relación de cualquier índole con el afectado, a obligar, inducir o convencer a ejecutar cualquier acto sexual con o sin el consentimiento del menor de edad, aparte de que también se castigara a quien abuse de una condición en que el afectado no sepa lo que hace o lo que le proponen, y si es con violencia física, la pena aumenta en un 50%. |
| ***Enriquecimiento Ilícito*** | Código Penal Federal, artículo 224. | Se sancionará a quien con motivo de su empleo, cargo o comisión en el servicio público, haya incurrido en enriquecimiento ilícito. Existe enriquecimiento ilícito cuando el servidor público no pudiere acreditar el legítimo aumento de su patrimonio o la legítima procedencia de los bienes a su nombre o de aquellos respecto de los cuales se conduzca como dueño, en los términos de la Ley Federal de Responsabilidades de los Servidores Públicos. |
| ***Falsificación de documentos en general*** | Código Penal Federal, artículo 243. | El delito de falsificación de documentos se comete por alguno de los medios siguientes:<br>I.- Poniendo una firma o rúbrica falsa, aunque sea imaginaria, o alterando una verdadera;<br>II.- Aprovechando indebidamente una firma o rúbrica en blanco ajena, extendiendo una obligación, liberación o cualquier otro documento que pueda comprometer los bienes, la honra, la persona o la reputación de otro, o causar un perjuicio a la sociedad, al Estado o a un tercero;<br>III.- Alterando el contexto de un documento verdadero, después de concluido y firmado, si esto cambiare su sentido sobre alguna circunstancia o punto substancial, ya se haga añadiendo, enmendando o borrando, en todo o en parte, una o más palabras o cláusulas, o ya variando la puntuación;<br>IV.- Variando la fecha o cualquiera otra circunstancia relativa al tiempo de la ejecución del acto que se exprese en el documento;<br>VI.- Redactando un documento en términos que cambien la convención celebrada en otra diversa en que varíen la declaración o disposición del otorgante, las obligaciones que se propuso contraer, o los derechos que debió adquirir<br>X.- Elaborando placas, gafetes, distintivos, documentos o cualquier otra identificación oficial, sin contar con la autorización de la autoridad correspondiente."<br>"Para que el delito de falsificación de documentos sea sancionable como tal, se necesita que concurran los requisitos siguientes:<br>I.- Que el falsario se proponga sacar algún provecho para sí o para otro, o causar perjuicio a la sociedad, al Estado o a un tercero; |

| | | |
|---|---|---|
| | | II.- Que resulte o pueda resultar perjuicio a la sociedad, al Estado o a un particular, ya sea en los bienes de éste o ya en su persona, en su honra o en su reputación, y<br>III.- Que el falsario haga la falsificación sin consentimiento de la persona a quien resulte o pueda resultar perjuicio o sin el de aquella en cuyo nombre se hizo el documento. |
| ***Juegos prohibidos*** | Ley Federal de Juegos y Sorteos, artículo 1. | Se prohíben en todo el territorio nacional, los juegos de azar y los juegos con apuestas, a excepción del juego de ajedrez, el de damas y otros semejantes; el de dominó, de dados, de boliche, de bolos y de billar; el de pelota en todas sus formas y denominaciones; las carreras de personas, de vehículos y de animales, y en general toda clase de deportes; Y de igual modo los sorteos, los juegos que no se señalaron se considerarán como prohibidos para esta Ley.<br>También nos dice esta ley que los juegos con apuestas pueden existir cuando la Secretaría de Gobernación este encargada de la reglamentación, autorización, control y vigilancia de estos. |
| ***Amenazas*** | Código Penal Federal, artículo 282. | El Código Penal Federal sanciona a todo aquel que amenace a otros con causarle un mal a su persona, sus bienes, su honor o sus derechos, o bien, al que trate de impedir que otro ejecute lo que tiene derecho a hacer, también por medio de amenazas.<br>Se exigirá caución de no ofender:<br>I.- Si los daños con que se amenaza son leves o evitables;<br>II.- Si las amenazas son por medio de emblemas o señas, jeroglíficos o frases de doble sentido, y<br>III.- Si la amenaza tiene por condición que el amenazado no ejecute un hecho ilícito en sí. En este caso también se exigirá caución al amenazado, si el juez lo estima necesario. |
| ***Injurias y difamación*** | Código Civil del Distrito Federal, artículo 1916. | Por daño moral se entiende la afectación que una persona sufre en sus sentimientos, afectos, creencias, decoro, honor, reputación, vida privada, configuración y aspectos físicos, o bien en la consideración que de sí misma tienen los demás. Se presumirá que hubo daño moral cuando se vulnere o menoscabe ilegítimamente la libertad o la integridad física o psíquica de las personas. |
| ***Fraude*** | Código Penal Federal, artículo 386. | Es el acto por el cual una persona, a partir de un engaño o aprovechándose del error en que la víctima de este delito se pueda encontrar, se hace ilícitamente de alguna cosa o bien alcanza un lucro indebido.<br>En este Código, se mencionan muchas causas por las cuales una persona va a ser castigada de fraude, siendo las más relacionadas a los fraudes por medios cibernéticos las siguientes fracciones:<br>VIII.- Al que valiéndose de la ignorancia o de las malas condiciones económicas de una persona, obtenga de ésta ventajas usuarias por medio de contratos o convenios en los cuales se estipulen réditos o lucros superiores a los usuales en el mercado. |

| | | |
|---|---|---|
| | | X.- Al que simulare un contrato, un acto o escrito judicial, con perjuicio de otro o para obtener cualquier beneficio indebido.<br>XI.- Al que por sorteos, rifas, loterías, promesas de venta o por cualquiera otro medio, se quede en todo o en parte con las cantidades recibidas, sin entregar la mercancía u objeto ofrecido.<br>XVIII.- Al que habiendo recibido mercancías con subsidio o franquicia para darles un destino determinado, las distrajere de este destino o en cualquier forma desvirtúe los fines perseguidos con el subsidio o la franquicia. |
| | En el Código Penal del Distrito Federal, artículo 231 fracción XIV | se menciona explícitamente un fraude cibernético, el cual menciona lo siguiente:<br>XIV. Para obtener algún beneficio para sí o para un tercero, por cualquier medio accese, entre o se introduzca a los sistemas o programas de informática del sistema financiero e indebidamente realice operaciones, transferencias o movimientos de dinero o valores, independientemente de que los recursos no salgan de la Institución; |
| ***Delitos en Materia de Derechos de Autor*** | Ley Federal del Derecho de Autor, artículo 11 | Establece el reconocimiento del Estado al creador de obras literarias o artísticas, entre las que, están los programas de cómputo, los cuales, al igual que las bases de datos, quedan protegidos por las disposiciones de la Ley de la misma forma que las obras literarias, en el sentido de que los autores tienen los derechos patrimoniales y morales sobre sus obras (explotación, reproducción, publicación, exhibición, acceso, distribución, divulgación, reconocimiento de la calidad de autor, modificación y respeto a la obra) así como la facultad de transmitir esos derechos. |
| | Ley Federal del Derecho de Autor, artículos 101 al 114 | Llos programas de computación y las bases de datos, estableciendo que: “se entiende por programa de computación la expresión original en cualquier forma, lenguaje o código, de un conjunto de instrucciones que con una secuencia, estructura y organización determinada, tiene como propósito que una computadora o dispositivo realice una tarea o función específica.”<br>La Ley amplía la protección a los programas tanto operativos como aplicativos y deja fuera a los que tienen por objeto causar efectos nocivos. Autoriza al usuario legítimo a hacer las copias que le permita la licencia, o bien, una sola que sea indispensable para la utilización del programa o sea destinada exclusivamente como resguardo. El autor tiene el derecho de autorizar o prohibir además de la reproducción, la traducción, adaptación, arreglo o cualquier modificación al programa o reproducción del resultante, la distribución, la decompilación (proceso para revertir la ingeniería del programa) y el desembalaje. |
| | Código Penal Federal, artículos 424 al 429 | Use en forma dolosa y con fines de lucro las obras protegidas por la Ley Federal del Derecho de Autor, o bien, dos a 10 años de prisión y dos mil a 20 000 días de multa al que produzca o reproduzca (entre |

| | | |
|---|---|---|
| | | otros actos) sin autorización y con fin de lucro obras protegidas por la Ley Federal de Derecho de Autor, así como a aquel que fabrique con fines de lucro, dispositivos o sistemas diseñados para desactivar los dispositivos electrónicos de protección de un programa de cómputo.<br>Multa al que fabrique, importe, venda o arriende algún sistema o dispositivo destinado a descifrar señales cifradas de satélite que contengan programas o realice con fin de lucro cualquier acto destinado al mismo efecto, sin autorización del distribuidor de la señal. |
| ***Acceso no autorizado a sistemas o servicios y destrucción de programas o datos.*** | Código Penal Federal, artículos 211 bis 1 a 211 bis 7 | Modificar, destruir o provocar pérdida de información contenida en sistemas o equipos informáticos protegidos sin autorización se castigará con: 6 meses a dos años prisión y de 100 a 300 días multa; si se trata de sistemas o equipos del Estado la pena será de: 1 a 4 años y 200 a 600 días multa; si se trata de sistemas o equipos de las instituciones que integran el sistema financiero la pena será de 6 meses a 4 años prisión y 100 a 600 días multa.<br>Conocer o copiar información contenida en sistemas o equipos informáticos protegidos sin autorización se castigará con: 3 meses a 1 año prisión y 50 a 150 días multa; si se trata de sistemas o equipos del Estado la pena será de: 6 meses a 2 años prisión y 100 a 300 días multa; Si se trata de sistemas o equipos de las instituciones que integran el sistema financiero la pena será de 3 meses a 2 años prisión y 50 a 300 días multa.<br>Modificar, destruir o provocar pérdida de información contenida en sistemas o equipos informáticos cuando se tenga autorización para el acceso: Si se trata de sistemas o equipos del Estado la pena será de: 2 a 8 años prisión y 300 a 900 días multa; Si se trata de sistemas o equipos de las instituciones que integran el sistema financiero la pena será de: 6 meses a 4 años prisión y 100 a 600 días multa.<br>Conocer o copiar información contenida en sistemas o equipos informáticos cuando se tenga autorización para el acceso: si se trata de sistemas o equipos del Estado la pena será de: 1 a 4 años prisión y 150 a 450 días multa; si se trata de sistemas o equipos de las instituciones que integran el sistema financiero la pena será de: 3 meses a 2 años prisión y 50 a 300 días multa.<br>Las penas se incrementarán en una mitad cuando las conductas se realicen por empleados del sistema financiero y se incrementarán hasta en una mitad cuando la información obtenida se realice en provecho. |

Tabla 20. Delitos relacionados con la informática en México.

### ***4.4.1 Relación de los medios informáticos con los delitos antes mencionados.***

#### ***4.4.1.1 Discriminación.***

Este delito, es fácilmente desarrollable en cuestión de informática, ya que hoy en día se utilizan las redes sociales, blogs, páginas de Internet, entre otras herramientas, para discriminar gente; sin embargo, ninguno de los artículos del Código Penal, hace referencia a estos tipos de discriminación; se puede castigar por el delito, siempre y cuando se compruebe que hubo algún tipo de discriminación, utilizando como herramienta la informática.

#### ***4.4.1.2 Violación de correspondencia.***

En el último párrafo, es en el que puede hacer referencia a la intercepción de correos electrónicos dentro de la red; la ley, no menciona nada en específico sobre el delito de espionaje o intervención ilícita de correos electrónicos; sin embargo, para tales efectos, este párrafo es uno de los que se puede partir para promover un artículo acerca de la intervención a correo electrónico, que se ha vuelto muy común últimamente, y del cual cada vez más personas hacen uso; cada día, son menos los correos por correspondencia que llegan a las casas, todo se manda vía correo electrónico, y una intervención, o espionaje a este, supone los mismos efectos o aún más graves que si esa misma persona interviniera correspondencia escrita; la peligrosidad de eso radica en que los correos electrónicos pueden ser contestados en ese mismo momento, y una persona con una mente maliciosa, contestará el correo de una forma no muy grata al remitente original; también, pueden ser eliminados en segundos, lo que quiere decir que el correo electrónico se puede dar por recibido, pero jamás haberse enterado que existió, lo que sería catastrófico en caso de que fuese un correo de suma urgencia. No es lo mismo abrir una o dos cartas, que toda una bandeja de entrada de correo electrónico que contiene decenas o incluso miles de correos electrónicos que pueden contener cualquier tipo de información. Por todo esto, se vuelve más peligrosa la intervención a correos electrónicos, y la ley no dice nada al respecto.

#### ***4.4.1.3 Pederastia y pornografía infantil***

Haciendo referencia a los sistemas informáticos, y su utilización como herramientas para la difusión de pornografía infantil, no se encuentra ningún tipo de pena en la ley; sin embargo, ha habido numerosos casos en los que personas que abusan de su autoridad con algún menor de edad, para hacerlos participes en casos de pederastia utilizando medios informáticos, y han sido capturados gracias a este tipo de medios; anteriormente, estos casos se difundían mediante correspondencia, o clubes privados; hoy en día, estas imágenes y videos se difunden con ayuda de tecnologías de la información, y con ayuda de estas mismas se capturan a los líderes de las redes pederastas; los castigos que se imponen, no involucran ningún apartado de delito informático, pero utilizando la herramienta que sea, se castiga de la misma forma.

#### ***4.4.1.4 Enriquecimiento ilícito***

Utilizando los medios informáticos, es posible que el enriquecimiento ilícito por parte de los funcionarios públicos sea mucho más sencillo utilizando Internet. Estos funcionarios, suelen utilizar transferencias bancarias para robarse el dinero que está destinado a otra cosa, desviando de esta forma los recursos a cuentas particulares, sin dejar algún tipo de rastro.

La ley, no menciona nada de la utilización o no de medios informáticos; no solo eso, no menciona alguna forma en especial de llevar a cabo el ilícito, por lo que las tecnologías de la información no son la excepción para este caso, y solo serán consideradas como herramientas, como lo puede ser considerado de la misma forma un cheque con otro nombre o una transferencia tradicional de dinero por medio de ejecutivos bancarios.

#### ***4.4.1.5 Falsificación de documentos***

Este artículo es muy detallado en cuanto a lo que se le puede considerar como "falsificar un documento", pero es sumamente necesario que se extienda este articulo a documentos que viajan por la red, que se encuentran almacenados en una bandeja de correo electrónico, o los que están alojados en un disco duro, ya que al ser modificados podrían afectar un expediente médico, un contrato, o cualquier otro documento que podría tener grandes repercusiones en una persona o en una empresa.

#### ***4.4.1.6 Juegos prohibidos.***

Un aspecto que resaltamos es que esta ley debe actualizarse ya que al parecer no considera la existencia de juegos ilegales en línea ya que en el artículo 8 habla sobre clausurar por medio de la Secretaría de Gobernación de todo local abierto o cerrado en el que se efectúen juegos prohibidos o juegos con apuestas y sorteos, que no cuenten con autorización legal, el problema que radica aquí es que se podría tener un servidor ilegal en el país y no se consideraría propiamente como un local, o en un caso más extremo que dicho servidor estuviera en el extranjero pero que accedan personas desde nuestro país y ellos podrían decir que están jugando un juego ilegal pero en otro lado.

Las multas para estas faltas son de tres meses a tres años de prisión y multa de quinientos a diez mil pesos, y destitución de empleo en algunos casos como por ejemplo: a los empresarios, gerentes, administradores, encargados y agentes de loterías o sorteos que no cuenten con autorización legal.

#### ***4.4.1.7 Amenazas.***

Las amenazas por Internet se han vuelto muy comunes; basta con ver algunas páginas famosas en redes sociales, y nunca faltará el comentario que sea amenazador para el propietario de esa página o para los demás foristas; también, no necesariamente son amenazas para gente desconocida; personas que se odian entre sí, llegan a amenazarse por medio de las tecnologías de la información: redes sociales, Internet, telefonía celular, clientes de mensajería instantánea, etc., delitos que no están especificados en este código; sin embargo, el delito, al igual que muchos de los delitos pasados, se castigan por lo que se está realizando, en este caso la amenaza, y no por las herramientas que se están utilizando: computadoras, celulares, o mensajes escritos a mano en un papel.

#### ***4.4.1.8 Injurias.***

Se habla sobre daño moral y se entiende como la afectación que una persona sufre en sus sentimientos, afectos, creencias, decoro, honor, reputación, vida privada, configuración y aspecto físicos, por desgracia si este daño se ocasiona en redes sociales, en blogs o correos electrónicos difícilmente podría mostrarlo como evidencia y lo más probable es que este delito quedase impune.

El monto de la indemnización lo determinará el juez tomando en cuenta los derechos lesionados, el grado de responsabilidad, la situación económica del responsable, y la de la víctima, así como las demás circunstancias del caso.

#### ***4.4.1.9 Delitos contra la religión.***

Este tipo de delitos, no están tipificados en ninguno de los Códigos Penales, Civiles o dentro de alguna ley o reglamentos del país, tanto federales como locales; esto debido a que cualquier ataque contra algún individuo o grupo religioso, siempre involucran a otro tipo de delitos: difamación, discriminación, vandalismo, robo, terrorismo, fraude, etc.

Lo que se castiga en estos casos, no es el ataque contra la religión, sino que tipo de ataque fue perpetrado contra estos grupos religiosos; por ejemplo, un ataque directo a una iglesia; no castigan el que haya sido contra la institución religiosa, sino el daño a propiedad ajena.

En cuestión de la utilización de tecnologías de la información para cometer este tipo de ilícitos, aplica lo mismo que en algunos de los delitos anteriormente descritos: la informática solo es utilizada como un medio o una herramienta más para cometer esos delitos; inclusive para los jueces no se llega a considerar evidencia una foto en una red social o algún correo electrónico hostil. Por ejemplo, en caso de un ataque a la religión por medio de las redes sociales o alguna página de Internet, y que este conlleve una amenaza de muerte, y en caso de que la investigación por el delito proceda, no se va a castigar ni el medio por el que se difundió el delito, ni siquiera se va a tomar en cuenta que fue contra la religión, solo se va a tomar el delito más grave, que en este ejemplo es la amenaza de muerte.

## *5. CONCLUSIONES.*

Las tecnologías de la información son herramientas y métodos creados para hacer la vida más fácil a las personas con las que se puede recabar, retener, manipular o distribuir información; un ejemplo de esto, es el enviar un correo. Se tenía que redactar la carta, depositarla en un buzón para que otras personas se encargaran de llevarla a la central de correos y enviarla al destinatario, lo cual podía tardar hasta semanas en ocurrir, si el destino era muy lejano. Con las nuevas tecnologías, basta con redactar la carta, y enviarla a una dirección de correo electrónico para que ésta llegue en cuestión de segundos a cualquier parte del mundo.

Partiendo de esto, se puede concluir que las tecnologías de la información, y todas las herramientas que a partir de estas se han podido crear, son para la facilidad y comodidad del usuario; sin embargo como se ha constatado en este trabajo, este tipo de tecnologías han sido utilizadas como herramientas para infringir la ley, dañar a terceros, o para ocasionar desastres económicos y en algunos casos hasta sociales.

El desarrollo de las tecnologías de la información ha hecho muy fácil el acceso ilícito a muchos sistemas informáticos de los cuales se quiere extraer información, o simplemente dañar un sitio web, como una medida de rebelión, protesta, o simple maldad, sin que hasta el momento exista una herramienta que haga totalmente segura la información.

Se habla de firewalls, de antivirus, de contraseñas encriptadas con métodos numéricos muy avanzados, y de un sinfín de tecnologías creadas para garantizar la seguridad de los sistemas; sin embargo, así como avanza la tecnología, avanzan los métodos para poder irrumpir esos sistemas, haciendo que la efectividad de las herramientas defensivas nunca sea de 100%.

Es así que surge el término de ciberdelincuencia, en el cual se deben de incluir todos los delitos que son perpetrados utilizando a las tecnologías de la información, y específicamente, a los que involucren a sistemas informáticos.

Una de las consecuencias más graves que se ha visto en el uso de estas tecnologías es el que en este documento se menciona como ciberterrorismo, ya que ahora, esta práctica no se limita solo a causar terror físicamente, ya sea con bombas o guerras, sino que ahora se puede causar todo tipo de terror utilizando medios cibernéticos, como el caso de las herramientas Flame y Stuxnet, herramientas informáticas muy poderosas contra las cuales no se pudo hacer nada antes de que el desastre estuviera presente, y que paralizaron centrales nucleares en Irán.

Tampoco se puede dejar de lado al usuario común. Utilidades tan simples como lo son las redes sociales pueden causar un impacto profundamente negativo en cualquier persona, si es que éstas redes se utilizan con fines de difamación, burla, o como fuente de información para potenciales asaltos o secuestros; estos fines, se puede pensar que son propiciados por la falta de filtros de seguridad que tienen estas redes; sin embargo, en la sociedad en la que vivimos, no se puede estar subiendo a las redes sociales cosas que puedan ser consideradas “de lujo” por los delincuentes, ya que esto hace de las personas la presa fácil que estas personas están buscando para cometer sus actos ilícitos.

Un claro ejemplo donde el usuario común es víctima de la ciberdelincuencia, sin que sea su culpa en lo absoluto, es en casos de usurpación de identidad, fraudes bancarios, y el phishing. A final de cuentas, al usuario de un banco se le da la facilidad de realizar sus operaciones bancarias en línea, con tan solo introducir su número de tarjeta y una contraseña; los ciberdelincuentes aprovechan este método para clonar las páginas web de los bancos, los usuarios que desconozcan estas prácticas ingresan con toda la confianza del mundo, y entonces esos números de tarjeta y contraseñas caen en manos de los delincuentes, apoderándose de lo que quieran.

Y como estos ejemplos, se podrían nombrar muchos más en los que las personas son víctimas de ciberdelincuentes, o de desarrolladores que lo único que buscan es un beneficio propio ya sea para ellos o para las empresas en las que trabajan (el adware es un claro ejemplo de estas prácticas); sin conocimientos tan profundos en materia de informática, se es víctima de un hacker que su único fin es dañar o robar información, o en el peor de los casos, todo un equipo de cómputo; normalmente, la gente no tiene una forma de defensa efectiva para combatir estas acciones.

Es por estas acciones, que el tema de la informática tuvo que tomar un rumbo no solo en materia de programas o equipos de defensa, como lo son los antivirus y los firewalls, sino que también se ha tenido que tomar en cuenta el lado político y legal para poder hacer frente a estas acciones.

En muchos países se han creado leyes, existen acuerdos internacionales de cooperación para poder perseguir a los delincuentes cuando estos atacan de fuera del país en donde resida la víctima, y sin embargo, estas medidas siguen sin ser suficientes para poder mitigar esta clase de problemas.

Una de las razones por las que no se ha podido, es la falta de acuerdos y la falta de cooperación interna que hay en muchas naciones para poder crear leyes competentes que controlen estos delitos, y el claro ejemplo, es México.

Como pudimos constatar en este documento, las leyes que aquí existen no castigan explícitamente el hacer uso de las tecnologías de la información para realizar los delitos, sino se castiga el delito como tal y punto. Por este enorme hueco que hay en las leyes, es que los hackers pueden hacer lo que quieran con los equipos ajenos, y difícilmente se les va a castigar; no así a una persona que esté utilizando las tecnologías de la información para ser parte de redes de pedofilia; en estas redes, perseguirán a las personas involucradas en estas redes pero no por utilizar las redes para este fin, sino por ser pedófilos.

Otro de los grandes problemas que existen para la creación de leyes es meramente político, y de la lamentable fama que tienen los políticos en México. Se ha tratado de regular Internet, diciendo que solamente se va a perseguir a las personas que sean sospechosas de estar incurriendo en un delito. Partiendo de este punto, según sea lo que las personas vean en Internet, pueden ser sospechosas o no de estar incurriendo en algún delito; esto solo se sabría, investigando lo que cada uno de los sospechosos consulta en la red, lo que causa la ira de los ciberactivistas, argumentando que eso violenta las garantías individuales de las personas puesto que por este hecho están siendo espiadas, cayendo en el eterno problema de activistas contra políticos.

No solo ese es el problema; cuando se hace una ley en materia de tecnologías de la información, se involucra el término de sobrerregulación. Los activistas que están en contra de que se haga cualquier ley que regule la Internet, hacen referencia a que son muchas normas las que se incluyen en estos documentos, sin tener un argumento claro. Mencionan que se va a limitar el uso de Internet, que

no van a poder ingresar a el sitio que ellos quieren, que se están violentando las libertades, etcétera. De ninguna manera se está sobrerregulando Internet, puesto que ni siquiera está regulado en este país; todos hacen, visitan, consultan lo que quieren, el problema es que a causa de que no existe ninguna ley, o norma en materia de informática, se tienen todos los delitos informáticos que ya se mencionaron, y se cae en la impunidad de no poder castigar a los que hacen mal uso de Internet; ejemplos, la piratería: al descargar ilegalmente cualquier archivo protegido por derechos de autor; fraudes bancarios, al no poder perseguir a los hackers que roban la información de los usuarios de la banca.

Definitivamente la solución a este problema sigue siendo una regulación competente del Internet; leyes que castiguen a los verdaderos culpables de los delitos que en este documento se mencionaron, sin caer en violaciones a los derechos humanos; no violentar en ningún momento la libertad que goza una persona de navegar en Internet y hacer uso de muchísimas ventajas que esto involucra, pero tampoco dejando de lado, una persecución a los ciberdelincuentes que utilizan las ventajas que ofrece Internet para cometer ilícitos.

Lo anterior, se va a lograr cuando los políticos de este país logren ponerse de acuerdo, dejando de lado las ideologías partidistas que tengan, y mirando por el bien de las personas, que a final de cuentas son las principales víctimas de estos delitos. Cuando haya estos acuerdos, se puede proceder a hacer leyes que convengan a los habitantes de este país, y no solo a los intereses de unos cuantos políticos y unos cuantos empresarios, como lo es hoy en día.

Y precisamente, ese es el trabajo a futuro que tienen que hacer los ingenieros de hoy en día; ingenieros que eligieron el ramo de las telecomunicaciones, la informática, los sistemas computacionales, tienen la obligación de garantizar la seguridad en los servicios que se ofrecen, que en este caso utilicen las tecnologías de la información; y también se tiene la obligación, de hacer y de impulsar ideas para que se hagan leyes en esta materia, que si bien no es un ramo que le corresponda a un ingeniero, debe de colaborar totalmente con los expertos en materia jurídica y legislativa que se dedica a esto, donde probablemente exista una carencia de conocimientos técnicos en materia de las TI. Con esto, podrían ser posibles las iniciativas de ley necesarias para regular Internet, para perseguir delincuentes y minimizar en la medida de lo posible el impacto de la ciberdelincuencia en la vida diaria.

Para lograr el objetivo de garantizar la seguridad en los servicios informáticos que se ofrecen, y no ser víctima de la ciberdelincuencia, lo primero que se tiene que hacer es educar al usuario final. Campañas de educación informática, avisos de posibles falsificaciones de software o de clonación de páginas bancarias ayudarían en primera instancia para que los usuarios no caigan tan fácilmente en las trampas de los ciberdelincuentes. El usuario final que no esté educado, siempre será una víctima muy fácil en la ejecución de estos delitos, así sus equipos estén resguardados por los mejores antivirus o firewalls que existen en el mercado.

Después de crear una conciencia en el usuario final, lo que sigue es proteger de una manera efectiva los equipos con los que está trabajando. Se puede cambiar la encriptación que traen de fábrica los actuales módems, al pasar de una encriptación WEP a una WPA o WPA2, lo que haría que el hacker que quiera acceder, tarde mucho tiempo más, o incluso le resulte imposible acceder a las redes inalámbricas caseras que la mayoría de las personas tienen.

En materia de redes empresariales, el proceso debe ser más complejo, el cual siempre requiere de una inversión mayor que algunas ocasiones los encargados de las empresas no quieren realizar. Se debe cuidar los sitios donde se resguardan sus equipos, con personal de seguridad y cámaras de video vigilancia para poder evitar que un usuario malintencionado haga daños físicos; se debe también implementar un sistema de seguridad perimetral, basado en firewalls con configuraciones estratégicas para que funcionen como filtros de diversos ataques; y en caso de que un ataque llegue a ocurrir, estar listo para ese tipo de contingencias, con servidores de respaldo a los cuales solo personal de confianza tenga acceso.

Una vez hecho lo anterior, lo que sigue es la cooperación con los expertos en leyes. Se debe de obligar a los proveedores de servicios de Internet, a trabajar en conjunto con las dependencias encargadas de la impartición de justicia, como son las Procuradurías Generales de Justicia, tanto de los estados como de la República, para localizar la actividad de la red única y exclusivamente de las personas a las que se les tenga comprobado la realización de un hecho ilícito en que hayan utilizado las tecnologías de información como herramienta para delinquir. También, se deben crear leyes que hablen exclusivamente de derecho informático y de ciberdelitos, regulando de esta forma el uso que se le da a Internet para las actividades diarias; lo anterior no quiere decir que prohíban hacer cualquier actividad cotidiana, sino de poner especial atención en los sitios y en los medios utilizados para llevar a cabo cualquier clase de ciberdelito.

## *6. REFERENCIAS*


- El ciberdelito: Guía para los Países en Desarrollo
  Dr. Marco Gercke
  Ginebra Suiza
  Unión Internacional de Telecomunicaciones
  División de Aplicaciones TIC y Ciberseguridad
  Departamento de Políticas y Estrategias
  Sector de Desarrollo de las Telecomunicaciones de la UIT
  Abril de 2009, 239 páginas

***Capítulo 1: Breve historia del surgimiento de Internet.***

- http://bibliotecadigital.ilce.edu.mx/sites/ciencia/volumen3/ciencia3/149/htm/sec_6.htm
- http://es.kioskea.net/contents/histoire/internet.php3
- http://www.dipity.com/raxec/History-of-the-Internet-Copy/
- http://materias.fi.uba.ar/7533/m7543t/osi.PDF
- http://ingeniatic.euitt.upm.es/index.php/tecnologias/item/628-minitel
- http://www.tudiscovery.com/internet/nace-arpa-el-abuelo-de-internet.shtml
- http://viola.org/viola/violaScreenDumps2/violaWWWAbout_1.jpg
- http://img.windowsnoticias.com/wp-content/uploads/2010/03/1-422daf2d49f1a.jpg
- http://www.cad.com.mx/historia_de_amazon_com.htm
- http://www.cad.com.mx/historia_de_ebay.htm
- http://www.cad.com.mx/historia_de_hotmail.htm
- http://hotmail.correoiniciarsesion.com/historia-hotmail-com
- www.outlookiniciarcorreo.com/etiqueta/jack-smith
- http://www.jastebol.com/historia-de-los-blogs/
- http://www.google.com.mx/intl/es/about/company/history/
- http://www.ebanking.cl/columnas/los-inicios-del-internet-banking-007
- http://www.cad.com.mx/historia_de_napster.htm
- http://my.opera.com/apolobeta/blog/show.dml/360878
- http://www.genbeta.com/windows/windows-live-messenger-un-poco-de-historia
- http://es.wikipedia.org/wiki/Historia_de_Wikipedia
- http://www.cad.com.mx/historia_de_facebook.htm
- http://www.cad.com.mx/historia_de_twitter.htm
- http://www.cad.com.mx/historia_de_youtube.htm
- http://gigatecno.blogspot.mx/2012/01/ventajas-y-desventajas-de-internet.html
- http://recursostic.educacion.es/observatorio/web/ca/software/software-general/909-monografico-control-parental?start=1

- https://sites.google.com/site/lasticylaweb20/herramientas-we-2-0
- http://www.tudiscovery.com/internet/nace-arpa-el-abuelo-de-internet.shtml


***Capítulo 2. Delitos contra sistemas informáticos.***


- www.microsoft.com/security/portal/threat/encyclopedia/glossary.aspx#e
- http://www.eset-la.com/centro-amenazas/amenazas/Troyanos/2136
- http://ns2.elhacker.net/MITM.pdf
- http://www.microsoft.com/es-xl/security/resources/identitytheft-whatis.aspx
- http://www.google.com/intl/es-419/goodtoknow/online-safety/identity-theft/
- http://auditoriapublica.com/hemeroteca/199507_02_44.pdf
- https://wikileaks.org/About.html
- http://computacion.cs.cinvestav.mx/~mruiz/cursos/manuales/Administracion_linux.pdf
- Maiorano, Ariel Horacio
- Criptografía: Técnicas de desarrollo para profesionales. 1ª ed. Buenos Aires: Alfaomega Grupo Editor Argentino, 2009. 292 pp.; 17x23 cm


***Capítulo 3. Delitos relacionados con el contenido.***


- http://www.eltiempo.com/tecnologia/internet/ARTICULO-WEB-NEW_NOTA_INTERIOR-11623587.html
- http://www.muytranquilo.es/2012/05/datos-sobre-la-pornografia-en-el-mundo.html
- http://www.onlinemba.com/blog/the-stats-on-internet-porn/
- http://www.cristianosaldia.net/index.php/Mensajes-en-Video-y-Reflexiones/Estadisticas-alarmantes-sobre-la-pornografia-en-los-jovenes-y-el-matrimonio.-%C2%A1Misericordia-Senor.html
- http://www.canal-ayuda.org/a-seguridad/porninfantil.htm
- http://sipse.com/archivo/mexico-segundo-lugar-en-pornografia-infantil-por-internet-328.html
- http://noticias.terra.com/internacional/los-paises-lideres-en-pornografia-infantil,eca25dc8fad37310VgnVCM3000009acceb0aRCRD.html
- http://www.unesco.org/bpi/pdf/memobpi29_racism_es.pdf
- http://dimencionesdescubiertas.blogspot.mx/2009_05_10_archive.html
- http://www.escuelapedia.com/racismo-en-internet/
- http://www.asi-mexico.org/sitio/archivos/Guia2012_SOLO-ASI_Ciber-Bullying_WP_FINAL.pdf

- http://www.sinfest.net:
- http://www.jesusandmo.net/
- www.lolcatbible.com/
- http://www.scoop.it/t/informatica-forense/p/3995489106/ii-informe-seguridad-juegos-online-apuestas-online-inseguras
- http://www.apestan.com
- http://www.quejasydenuncias.com/
- http://www.quejasonline.com/
- http://www.agpd.es/portalwebAGPD/canaldocumentacion/lucha_contra_spam/common/pdfs/INFORMACI-OO-N-SPAM--ap-V.-30-mayo-cp-.pdf
- www.metacafe.com/watch/.../how_to_make_a_homemade_bomb/
- http://ellasenlacalle.blogspot.mx/
- www.quebarato.com.mx/
- www.taringa.net/posts/info/5197983/Como-hacer-explosivos-caseros.html
- http://portal.unesco.org/culture/es/ev.php-URL_ID=39397&URL_DO=DO_TOPIC&URL_SECTION=201.html
- http://pirateria.pgr.gob.mx/
- http://www.slideshare.net/vralmiron/la-pirateria-en-internet
- http://www.pgr.gob.mx/Combate%20a%20la%20Delincuencia/Delitos%20Federales/Delitos%20en%20materia%20de%20derechos%20de%20autor/Delitos%20en%20materia%20de%20derechos%20de%20autor.asp
- http://pav230889.blogspot.mx/2009/05/la-pirateria-definicion.html
- http://www.muyinteresante.es/tecnologia/articulo/iesto-es-la-ciberguerra
- http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet
- http://www.kaspersky.com/flame
- http://bits.blogs.nytimes.com/2012/05/28/new-computer-virus-looks-like-a-cyberweapon/

***Capítulo 4. Derecho informático y ciberdelitos.***

- https://www.uclm.es/profesorado/raulmmartin/Legislacion/apuntes.pdf
- http://www.itu.int/en/ITU-D/Cybersecurity/Documents/CybcrimeS.pdf
- http://www.monografias.com/trabajos/legisdelinf/legisdelinf.shtml
- http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_project_Phase3_2571/2571_CostaRica_WS/2571_CR_regWS_legworkingdoc_Spanish.pdf
- http://iriartelaw.com/sites/default/files/PreDictamen-Comision-Justicia_Delitos_Informaticos.pdf
- http://www.mailxmail.com/curso-delitos-informaticos/legislacion-contexto-internacional
- http://www.law.cornell.edu/uscode/text/18/1029
- http://www.law.cornell.edu/uscode/text/18/1030
- Código Penal Español: https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444

- Código Penal Federal de los Estados Unidos Mexicanos:
- http://www.diputados.gob.mx/LeyesBiblio/pdf/9_030614.pdf
- Ley Federal de Derechos de Autor: http://www.diputados.gob.mx/LeyesBiblio/pdf/122.pdf
- Constitución Política de los Estados Unidos Mexicanos: http://www.diputados.gob.mx/LeyesBiblio/htm/1.htm
- Ley Federal de Juegos y Sorteos: http://www.diputados.gob.mx/LeyesBiblio/pdf/109.pdf
- Código Civil del Distrito Federal: http://www.infodf.org.mx/nueva_ley/14/1/doctos/CCDF.pdf

## *7. Referencias imágenes*


- Figura 1. Primeros desarrollos de redes centralizadas.
  http://jencinar.typepad.com/.a/6a00d8341c04d953ef01287790b697970c-pi
- Figura 2: Sputnik 1.
  http://veneastro3000.blogspot.mx/2012/04/sputnik-primer-artificial.html
- Figura 3. Redes centralizadas, descentralizadas y redes distribuidas.
  http://jencinar.typepad.com/.a/6a00d8341c04d953ef01287790b697970c-pi
- Figura 4. Primeros 4 nodos de ARPANET, diciembre de 1969.
  http://timerime.com/es/evento/452280/Internet+Began/
- Figura 5. Tim Berners, creador de la WWW.
  http://frontroll.com/halkategori-55-5.html
- Figura 6. Proyecto Minitel.
  http://www.jnthistoria.fi/fi/sadas-vuosi/
  http://users.skynet.be/jaguar/minitel/
- Figura 7. Vinton Cerf, creador de la ISOC.
  http://mercadotecnianieveszacatecas.blogspot.mx/
- Figura 8. Viola, el primer navegador web gráfico.
  http://www.viola.org/
- Figura 9. Mosaic, el primer navegador popular entre el público.
  http://doble69.wordpress.com/2014/03/13/la-world-wide-web-cumple-25-anos/
- Figura 10. Netscape.
  http://www.comunicacionvisual.com/blog/tag/netscape/
- Figura 11. Yahoo!
  http://todosobrelosnavegadores.blogspot.mx/
- Figura 12. Amazon.
  https://xiomaramendoza.wordpress.com/tag/amazon/
- Figura 13. eBay.
  http://en.wikipedia.org/wiki/EBay
- Figura 14. Hotmail.
  http://www.abrircorreohotmail.com/hotmail-para-todos/
- Figura 15. Blogger, una de las web de blogs más grandes.
  http://bluedreamer27.blogspot.mx/2011/02/top-five-websites-that-changed-our.html
- Figura 16. Google, el buscador más importante en la actualidad.
  https://www.google.com.mx/
- Figura 17. Banca en línea.
  https://www.banorte.com/portal/personas/acceso.web?grupo=31&elemento=110&fullSite=true
- Figura 18. Napster.
  http://www.timetoast.com/timelines/54100
- Figura 19. ICQ.
  http://www.hurhaber.com/efsane-icq-geri-donuyor/haber-651690

- Figura 20. Wikipedia, la enciclopedia on-line más grande en la actualidad. http://todosobrelosnavegadores.blogspot.mx/
- Figura 21. Interacción de las redes sociales con otras redes. http://codicedigitalqr.com/2014/03/31/5-mejores-aplicaciones-para-administrar-redes-sociales/
- Figura 25. Ataque XSS. Descripción gráfica. http://stuxnethack.blogspot.mx/2013/10/que-es-y-como-opera-un-ataque-de-xss.html
- Figura 26. Funcionamiento básico de un Sniffer. http://ingenieriadelaseguridad.blogspot.mx/p/amenazas-malware-y-sistemas-de-defensa.html
- Figura 30. Funcionamiento básico de la técnica Man-in-the-Middle. http://carlosezequiels.wordpress.com/2011/09/26/man-in-the-middle-hackear-cuentas/
- Figura 31. Implementación del ataque MIM. http://es.scribd.com/doc/132385358/mitm
- Figura 33. Subasta en línea. https://bidwiz.es/
- Figura 34. Ataque DoS. http://sinformaticaweb.wordpress.com/
- Figura 35. Crecimiento de los sitios web que hacen apología del racismo. http://dimencionesdescubiertas.blogspot.mx/2009_05_10_archive.html
- Figura 36. Sitio web Apestan.com, el principal sitio web para difamación. http://www.apestan.com/
- Figura 37. Porcentaje de productos pirata obtenidos vía internet. http://angelbc.files.wordpress.com/2011/02/piechart-piraterc3ada.png
- Figura 38. Descargas ilegales por contenido. http://angelbc.files.wordpress.com/2011/02/bittorrent_pirateria.png
- Figura 39. Funcionamiento del virus Stuxnet. http://www.spectrogamma.com/2013/07/como-funciona-stuxnet.html
- Figura 40.Funcionamiento del virus Flame. http://www.taringa.net/posts/noticias/14928622/Virus-Flame-presagia-una-nueva-era-en-la-ciberguerra.html
- Figura 41. Moneda virtual Bitcoin. http://www.bitcoin.com.es/
- Figura 42. Red de pedofilia en la darket Onion. Opva2pilsncvtwmh.onion
- Figura 43. Resultados de una búsqueda en Onion. Dppmfxaacucguzpc.onion
- Figura 44. Forma de pagar servicios en las darknets: mediante la Bitcoin. 627kx22vati6uqkw.onion

- Figura 45. Búsqueda en darknet Tor.
  P2uekn2yfvlvpzbu.onion
- Figura 46. Otros resultados en la darknet Tor.
  P2uekn2yfvlvpzbu.onion
- Figura 47. Mercado negro en internet.
  5onwnspjvuk7cwvk.onion
- Figura 48. Páginas racistas, también en las darknet.
  Kpynyvym6xqi7wz2.onion
- Figura 49. Resultados de búsqueda: violencia sexual.
  Kpynyvym6xqi7wz2.onion
- Figura 50. Resultados de la búsqueda: bombas y destrucción.
  Kpynyvym6xqi7wz2.onion