Índice de contenido

1 Fundamentos de Computadores

1.1 Multiprogramación

Se denomina **multiprogramación** a la técnica que permite que dos o más procesos ocupen la misma unidad de memoria principal y que sean ejecutados al "mismo tiempo" (pseudo-paralelismo, en una única CPU sólo puede haber un proceso a la vez) en la unidad central de proceso o CPU.

1.2 Multiproceso

Multiproceso es tradicionalmente conocido como el uso de múltiples procesos concurrentes en un sistema en lugar de un único proceso en un instante determinado. Como la multitarea que permite a múltiples procesos compartir una única CPU, múltiples CPUs pueden ser utilizados para ejecutar múltiples hilos dentro de un único proceso.

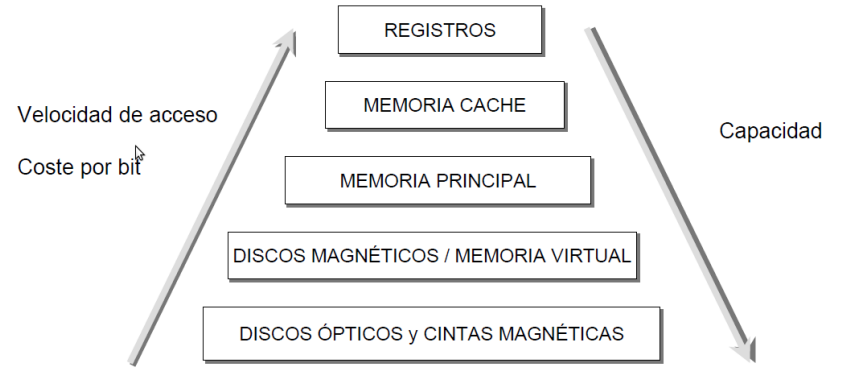
1.3 Multiproceso simétrico

SMP es la sigla de Symmetric Multi-Processing, multiproceso simétrico. Se trata de un tipo de arquitectura de ordenadores en que dos o más procesadores comparten una única memoria central.

que varios microprocesadores comparten el acceso a la memoria. Todos los microprocesadores compiten en igualdad de condiciones por dicho acceso, de ahí la denominación “simétrico”.

1.4 Organización jerárquica de la memoria

T6 Sistema de me



1.5 Caché

1.5.1 El término "Cache"

En informática, el término **cache** se aplica a un conjunto de datos duplicados de otros originales, con la propiedad de que los datos originales son costosos de acceder, normalmente en tiempo, con respecto a la copia en el cache. Cuando se accede por primera vez a un dato, se hace una copia en el cache; los accesos siguientes se realizan a dicha copia, haciendo que el tiempo de acceso medio al dato sea menor.

1.5.2 Memoria Cache o RAM Cache

Un cache es un sistema especial de almacenamiento de alta velocidad. Puede ser tanto un área reservada de la memoria principal como un dispositivo de almacenamiento de alta velocidad independiente. Hay dos tipos de cache frecuentemente usados en las computadoras personales: memoria cache y cache de disco. Una memoria cache, llamada también a veces almacenamiento cache o RAM cache, es una parte de memoria RAM estática de alta velocidad (SRAM) más que la lenta y barata RAM dinámica (DRAM) usada como memoria principal. La memoria cache es efectiva dado que los programas acceden una y otra vez a los mismos datos o instrucciones. Guardando esta información en SRAM, la computadora evita acceder a la lenta DRAM.

1.5.3 Política de ubicación

Decide dónde debe colocarse un bloque de memoria principal que entra en la memoria cache.

- *Directa*: Al bloque i-ésimo de memoria principal le corresponde la posición *i módulo n*, donde n es el número de bloques de la memoria cache.
- *Asociativa*: Cualquier bloque de memoria principal puede ir en cualquiera de los n bloques de la memoria cache.
- *Asociativa por conjuntos*: La memoria cache se divide en k conjuntos de bloques, así al bloque i-ésimo de memoria principal le corresponde el conjunto *i módulo k*. Dicho bloque de memoria podrá ubicarse en cualquier posición de ese conjunto.

1.5.4 Política de extracción

La política de extracción determina cuándo y qué bloque de memoria principal hay que traer a memoria cache. Existen dos políticas muy extendidas:

- *Por demanda*: Un bloque sólo se trae a memoria cache cuando ha sido referenciado y se produzca un fallo.
- *Con prebúsqueda*: Cuando se referencia el bloque i-ésimo de memoria principal, se trae además el bloque (i+1)-esimo. Esta política se basa en la propiedad de localidad espacial de los programas.

1.5.5 Política de reemplazo

- *Aleatoria*: El bloque es reemplazado de forma aleatoria.
- *FIFO*: Se usa un algoritmo *First In First Out* FIFO
- *Menos recientemente usado (LRU)*: Se sustituye el bloque que hace más tiempo que no se ha utilizado.
- *Menos frecuentemente usado (LFU)*: Se reemplaza el bloque que se ha usado con menos frecuencia.

Siendo la Aleatoria y la LRU las de mejor rendimiento.

1.5.6 Política de escritura

Determina cuándo se actualiza la información en memoria principal cuando se ha escrito en memoria cache. Existen dos políticas principales:

- *Escritura inmediata* o *escritura directa*: En inglés *Write Through*. Cuando se escribe en un bloque que se encuentra en memoria cache, la información se modifica también simultáneamente en

memoria principal, manteniendo así la coherencia en todo momento.

- *Escritura aplazada* o *post-escritura*: En inglés *Write Back*. Cuando se escribe en un bloque que se encuentra en memoria cache, queda marcado como *basura* usando un bit especial llamado normalmente *dirty bit* o *bit de basura*.

1.6 Memoria Asociativa

Se entiende por **memoria asociativa** el almacenamiento y recuperación de información por asociación con otras informaciones. Normalmente se buscan por contenido.

1.7 Memoria Virtual

La **Memoria virtual** es una técnica que permite al software usar más memoria principal que la que realmente posee el ordenador.

2 Raid

Raid, Array de Discos Independiente y Redundantes, se utiliza para proteger de fallos la información y para acelerar el acceso al disco.

Sus ventajas son:

- Tolerancia a fallos.
- Mejora del rendimiento.
- Mayor fiabilidad
- Alta disponibilidad

Los tenemos de dos tipos:

- **Software**, bajo coste inicial, pero alto coste de mantenimiento. No protege el S.O. No permite cambio instantáneo de disco. Disminuye la capacidad del computador
- **Hardware**, Independiente del sistema operativo, utiliza controladoras RAID. Mejora del rendimiento, permite cambio de disco.

2.1.1 Niveles RAID

1. **RAID 0**, no proporciona redundancia utiliza un array de dos o más discos entre los que distribuye la información, si se estropea uno no tiene reparación, mejora las transferencias.
2. **RAID 1**, dos discos uno tiene la copia del otro, hay redundancia y emjoran las transferencias.
3. **RAID 10**, mezcla de los dos anteriores.
4. **RAID 2**, Acceso paralelo con hamming.
5. **RAID 3**, Síncrono con un disco para paridad >=3 discos.
6. **RAID 4**, Independiente con disco para paridad >=3.
7. **RAID 5**, Independiente con paridad distribuida
8. **RAID 6**, Independiente con doble paridad distribuida

3 Estructuras de un Sistema operativo

Los sistemas operativos atienden a distintas clasificaciones, **Monousuario, Multiusuario, Monotarea, Multitarea, Procesamiento**

por lotes, Procesamiento distribuido.

Algunos conceptos

- Entrada/Salida
  - Interrupciones
  - Conmutación de contexto
- Procesos
  - Listo->Espera->Ejecución
  - Los cambios de estado se guardan en la BCP
- Planificación de Procesos
  - RR, SRR, quantum, FIFO
- Comunicación entre procesos
  - Monitores
  - Semáforos
  - Paso de mensaje
  - Interbloqueo
- Gestión de memoria
  - Asignación continua, se meten uno tras otro.
    - Partición estática, se pre-divide la memoria, queda fragmentación interna.
    - Partición dinámica, se va incrementado, fragmentación externa.
  - Asignación no continua
    - Paginación, páginas iguales entre si e iguales al marco.
    - Segmentación, reduce la fragmentación interna..

3.1 Capas típicas de un S.O jerárquico

1. Nivel 1, Manejo de hardware.
2. Nivel 2, Abstracción de la memoria secundaria, convertir el disco duro en un fichero.
3. Nivel 3, Memoria principal
4. Nivel 4, Manejo de archivos a alto nivel.
5. Interprete de comandos

3.2 Estructura jerárquica de un Sistema Operativo

1. Núcleo
2. Gestor de procesos
3. Gestor de memoria
4. Gestor de E/S
5. Gestor de memoria secundaria, ficheros, directorios
6. Interfaz de ususario

4 GNU

El **proyecto GNU** fue iniciado por Richard Stallman con el objetivo de

crear un sistema operativo completamente libre: el **sistema GNU**.[1] El 27 de septiembre de 1983 se anunció públicamente el proyecto por primera vez en el grupo de noticias net.unix-wizards.

GNU es un acrónimo recursivo que significa **GNU No es Unix** (*GNU is Not Unix*).

5 GPL

La **Licencia Pública General de GNU** o más conocida por su nombre en inglés ***GNU General Public License*** o simplemente su acrónimo del inglés **GNU GPL**, es una licencia creada por la Free Software Foundation a mediados de los 80, y está orientada principalmente a proteger la libre distribución, modificación y uso de software. Su propósito es declarar que el software cubierto por esta licencia es software libre y protegerlo de intentos de apropiación que restrinjan esas libertades a los usuarios.

Las libertades que proclama son

De acuerdo con tal definición, el software es "libre" si garantiza las siguientes libertades:[1]

- Libertad 0: la libertad de usar el programa, con cualquier propósito.
- Libertad 1: la libertad de estudiar cómo funciona el programa y modificarlo, adaptándolo a tus necesidades.
- Libertad 2: la libertad de distribuir copias del programa, con lo cual puedes ayudar a tu prójimo.
- Libertad 3: la libertad de mejorar el programa y hacer públicas esas mejoras a los demás, de modo que toda la comunidad se beneficie.

Las libertades 1 y 3 requieren acceso al código fuente porque estudiar y modificar software sin su código fuente es muy poco viable.

6 SVID System V

System V, abreviado comúnmente SysV y raramente System 5, fue una de las versiones del sistema operativo Unix. Fue desarrollado originalmente por AT&T y lanzado por primera vez en 1983.

7 Personalización e inicio del entrono en Unix

El intérprete de comandos más usado es el bash sin duda. En el caso de bash, dependiendo del tipo de intérprete se ejecutarán distintos archivos para ponerlo en marcha:

Ingreso	Ejecución de .bash_profile
Interactivo	Ejecución de .bashrc
No interactivo	Ejecución del script indicado

Hay más ficheros que nos van a interesar para el manejo de nuestro entorno de trabajo. De entre ellos vamos a listar algunos.

~/.bash_history	Historial de órdenes ejecutadas por el usuario.
/etc/X11/xinit	Script sesión gráfica arranca mediante xinit, 'startx'
/etc/X11/Xsession	Script gráfica con algún gestor como 'kdm' o 'gdm'
/etc/profile	Intérprete de comandos ingreso
/etc/csh.login	Intérprete de comandos ingreso
~/.login	Intérprete de comandos ingreso
~/.tcshrc	Intérprete de comandos interactivo
~/chrc	Es usado si .tcshrc no se encuentra

7.1 Alias

Alias es un comando de Linux que te permite ahorrar mucho texto asignándole un nombre a comandos largos. Hay dos formas de hacerlo.

- $ alias hola="echo Hola Mundo", Par borrar: unalias

Editando el archivo ~/.bashrc :

- alias busca='sudo aptitude search'
- alias instala='sudo aptitude install'

7.2 Variables de entorno

Las variables de entorno son un conjunto de valores dinámicos que normalmente afectan el comportamiento de los procesos en una computadora.

Por ejemplo, para mostrar la ruta de búsqueda de programas en un sistema Unix y Linux, se teclea : **echo $PATH**

Los comandos env, set, y printenv muestran todas las variables de entorno junto con sus respectivos valores. env y set se usan también para asignar valores a variables de entorno y normalmente son funciones incorporadas del intérprete de comandos. printenv permite también mostrar el valor de una variable de entorno particular si se le pasa su nombre como único parámetro.

La forma de asignar un valor a una variable es:

- variable=valor

Pueden usarse también los siguientes comandos, aunque dependen del intérprete.

- export VARIABLE=valor # en Bourne e intérpretes de comandos relacionados.
- setenv VARIABLE valor # en csh e intérpretes de comandos relacionados.

El manejo de variables de entorno es altamente versátil en entornos UNIX/ Linux**.**

7.2.1 Variables de entorno más comunes

- **$PATH**. Contiene una lista separada por dos puntos de directorios en los cuales el intérprete de comandos buscará los archivos ejecutables que no se invocan con una ruta. corriente.
- **$HOME**, Contiene la ubicación del directorio de usuario.
- **$DISPLAY**. Contiene el identificador del display que los programas de X11 deben usar por defecto.
- **$LANG, $LC_ALL. LAN** contiene el locale por defecto del sistema; LC_ALL permite ignorar su contenido. Por ejemplo, si contiene pt_BR, entonces el idioma será portugués de Brasil y el locale será Brasil.
- **$RANDOM**. Es una variable de entorno especial que, cuando se intenta obtener su contenido, devuelve un valor aleatorio.

7.2.2 La variable PS1

La forma de visualización del prompt viene dada por la variable del shell denominada PS, esto significa que configurando dicha variable modificamos el aspecto del prompt.

El contenido de PS1 está basado en una sintaxis que se denomina "secuencia de escape ANSI". Podemos ver esa secuencia a continuación:

- \a carácter de campana ASCII (07)
- \d la fecha en formato día mes día (p.ej., mar may 26)
- \e caracter de escape ASCII (033)
- \h el nombre del host hasta el primer
- \H el nombre del la máquina completo (FQDN)
- \n caracter de nueva línea
- \r retorno de carro
- \s el nombre del shell, el nombre base de $0 (el fragmento que sigue a la última barra)
- \t la hora actual en formato 24-horas HH:MM:SS
- \T la hora actual en formato 12-horas HH:MM:SS
- \@ la hora actual en formato 12-horas AM/PM
- \u el nombre de usuario del usuario actual
- \v la versión de bash (p.ej., 2.0)
- \V la versión del paquete del bash, versión + patch-level (p.ej., 2.00.0)
- \w el directorio actual de trabajo
- \W el nombre base del directorio actual de trabajo
- \! el número del comando actual en el histórico
- # el número de comando del comando actual
- \$ si el UID efectivo es 0, un #; en otro caso, $
- \nnn el caracter correspondiente al número en octal nnn
- \\ una contrabarra
- \[inicio de una secuencia de caracteres no imprimibles que pueden usarse para incrustar una secuencia de control del terminal en el prompt.
- \] fin de una secuencia de caracteres no imprimibles

Ejemplos de uso:

- PS1="\u@\h \W> "
- PS1="[\t][\u@\h:\w]\$ "

Las cadenas PS? son establecidas, según la persona o distribución en distintos lugares. Los más comunes son /etc/profile, /etc/bashrc, ~/.bash_profile, y ~/.bashrc.

7.2.3 etc/motd

El contenido de este fichero es mostrado tras hacer login de forma correcta en el sistema operativo.

8 Tipos de Shell

- **Bash,** llamada por sus siglas, Bourne Again SHell
- **Sh,** que viene de Bourne Shell
- **Ksh,** de las palabras Korn SHell

- **Csh,** de C Shell
- **Ash,** que viene siendo un clon al Bash

Para saber que tipo de Shell estamos usando abriremos una terminal o consola en linux, y escribiremos lo siguiente. **echo $SHELL**

Para cambiar el tipo de Shell que se esta usando es con el comando

chsh

9 Gestión Usuarios

9.1 Primer paso del administrador

Debe conocer los siguientes archivos importantes:

- el archivo **/etc/passwd**
- el archivo **/etc/group**

9.1.1 El archivo /etc/passwd

El archivo **/etc/passwd** contiene toda la información relacionada con el usuario (registro, contraseña, etc.). Sólo el superusuario (raíz) puede cambiarla. Por lo tanto, es necesario cambiar los derechos de este archivo para que sólo puedan leerlo los demás usuarios.

Este archivo posee un formato especial que permite marcar a cada usuario y cada una de sus líneas tiene el siguiente formato:

```
cuenta:contraseña:IDusuario:IDgrupo:comentario:directorio:programainicio
```

root:x:0:0:root:/root:/bin/bash

Las claves van encriptadas en /etc/shadow

Una cuenta privilegiada es aquella cuyo identificador (UID, ID del usuario) es cero.

9.2 El archivo /etc/group

El archivo **/etc/group** contiene una lista de los usuarios que pertenecen a los diferentes grupos.

Tiene diferentes campos separados por "**:**":

```
grupo:campo_especial:IDgrupo:miembro1,miembro2
```

Con frecuencia, el campo especial está vacío. El número de grupo corresponde al número del vínculo entre los archivos /etc/group y los archivos /etc/passwd.

A continuación encontrará un ejemplo de un archivo ***/etc/group***:

root:x:0:root	**bin:x:1:root,bin,daemon**
daemon:x:2:	**tty:x:5:**
lp:x:7:	**disk:x:6:**

- Cuando el comando *ls* se utiliza con la opción -1, el número de grupo se muestra junto con el del usuario al que pertenece el archivo (o directorio). Este número único corresponde al nombre de grupo único (a menudo tiene un máximo de 8 caracteres).
- Para añadir un grupo, el administrador puede cambiar el archivo */etc/group* con un editor de texto. También puede usar el comando **addgroup** o **groupadd** (no siempre presentes). En el primer caso, sólo tendrá que añadir las líneas relacionadas con los grupos. Por ejemplo, la línea:

- Para agregar un usuario a un grupo, sólo debe editar el archivo */etc/group* y agregar el nombre al final de la línea separando los nombres de los miembros con una coma.
- Para eliminar un grupo, sólo debe editar el archivo */etc/group* y eliminar la línea correspondiente. Tenga en cuenta: /etc/passwd, Si ese grupo tenía usuarios, no olvide cambiar los números (GID) del grupo eliminado.

9.3 Sistema de fichero

9.3.1 Definición y tipos de sistemas de ficheros

- *ext2, ext3* Es el sistema de ficheros nativo de Linux.
- *vfat 12, 16 y 32* Es el sistema de ficheros usados por la gama baja de las plataformas win32. No admite características multiusuario como propiedad de ficheros.
- *Iso9660* Es el sistema de ficheros propio de los CDROM.
- *msdos* Análogo a los sistemas FAT, aunque sólo admite ficheros con nombre 8+3.

9.3.2 Particiones

Una partición es una división del disco que se gestiona de forma lógica independiente al resto de las particiones del disco. Cada partición puede contener su propio sistema de ficheros. Esta división se describe en la tabla de particiones que se encuentra en el sector cero del disco (MBR). Tenemos que tener en cuenta que *Linux* necesita al menos una partición para su sistema de ficheros raíz. Además también es necesario usar particiones de intercambio (swap) en la mayoría de los casos. En equipos compatibles con Intel, la BIOS que arranca el sistema puede a menudo acceder solamente a los primeros 1024 cilindros del disco. Por esta razón la gente con discos grandes a menudo crean una tercera partición, de sólo unos cuantos MB de grande, montada típicamente en `/boot`, para almacenar allí la imagen del núcleo y unos pocos ficheros auxiliares que se necesitan en el momento del arranque, de forma que uno se asegure de que estas cosas están accesibles para la *BIOS*.

9.3.3 Dispositivos

En particular los dipositivos de almacenamiento que nos interesan son los discos. La partición es un nombre de dispositivo seguido por un número de partición. Por ejemplo, `/dev/hda1` es la primera partición del primer disco duro IDE en el sistema.

9.3.4 Creación de la partición

Para modificar las particiones de una unidad de disco disponemos de la orden **fdisk**. Con la orden **fdisk** podemos ver la lista de particiones de una determinada unidad si le añadimos la opción -l. Por ejemplo:

- **fdisk -l /dev/hda**

Si lo que queremos es modificar la lista de particiones entonces usamos la orden fdisk indicando sólo el dispositivo correspondiente a la unidad que queremos editar. Por ejemplo:

- **fdisk /dev/hda**

9.3.5 Creación de un sistema de ficheros: mkfs

Una vez que tenemos creada un partición podemos dedicarla a dos usos; para contener ficheros o bien como partición de intercambio; este último caso lo veremos más adelante.

- **mkfs -t ext2 /dev/hdc2**

9.3.6 Verificar un sistema de ficheros: fsck

En ciertas ocasiones es necesario verificar la integridad del sistema de ficheros y corregir los posibles errores que hubiese. Esta acción la realiza la orden *fsck*.

10 Estructura de Directorios

- **Estaticos:**

  /bin, /sbin, /opt, /boot, /usr/bin

- **Dinamicos:**

  /var/mail, /var/spool, /var/run, /var/lock, /home

- **Compartibles:**

  /usr/bin, /opt

- **No compartibles:**

  /etc, /boot, /var/run, /var/lock

A continuación una lista con los directorios mas importantes del sistema:

- **/bin/** Comandos/programas binarios esenciales *(cp, mv, ls, rm, etc)*
- **/boot/** Ficheros utilizados durante el arranque del sistema *(núcleo y discos RAM)*
- **/dev/** Dispositivos esenciales, discos duros, terminales, sonido, video, lectores dvd/cd, etc
- **/etc/** Ficheros de configuración utilizados en todo el sistema y que son específicos del ordenador
- **/etc/opt/** Ficheros de configuración utilizados por programas alojados dentro de /opt/

- **/etc/X11/** Ficheros de configuración para el sistema X Window
- **/home/** Directorios de inicios de los usuarios
- **/lib/** Bibliotecas compartidas esenciales para los binarios de /bin/, /sbin/ y el núcleo del sistema.
- **/mnt/** Sistemas de ficheros montados temporalmente.
- **/media/** Puntos de montaje para dispositivos de medios como unidades lectoras de discos compactos.
- **/opt/** Paquetes de aplicaciones estáticas.
- **/proc/** Sistema de ficheros virtual que documenta sucesos y estados del núcleo. Contiene principalmente ficheros de texto.
- **/root/** Directorio de inicio del usuario root
- **/sbin/** Comandos/programas binarios de administración de sistema.
- **/tmp/** Ficheros temporales
- **/usr/** Jerarquía secundaria para datos compartidos de solo lectura (Unix system resources). Este directorio puede ser compartido por múltiples ordenadores y no debe contener datos específicos del ordenador que los comparte.
- **/usr/bin/** Comandos/programas binarios.
- **/usr/include/** Ficheros de inclusión estándar *(cabeceras de cabecera utilizados para desarrollo)*.
- **/usr/lib/** Bibliotecas compartidas.
- **/usr/share/** Datos compartidos independientes de la arquitectura del sistema. Imágenes, ficheros de texto, etc.
- **/var/** Ficheros variables, como son logs, bases de datos, directorio raíz de servidores HTTP y FTP, colas de correo, ficheros temporales, etc.
- **/var/cache/** Cache de datos de aplicaciones.
- **/var/lib/** Información de estado variable. Algunos servidores como MySQL y PostgreSQL almacenan sus bases de datos en directorios subordinados de éste.
- **/var/lock/** Ficheros de bloqueo.
- **/var/log/** Ficheros y directorios de registro del sistemas *(logs)*.
- **/var/mail/** Buzones de correo de usuarios *(Opcional)*
- **/var/opt/** Datos variables de /opt/.
- **/var/spool/** Colas de datos de aplicaciones.
- **/var/tmp/** Ficheros temporales preservados entre reinicios.

11 Tuberías y redirecciones y otros comandos

11.1 Manipulación de archivos con cat

`Cat`, diminutivo de *concatenate*, que significa combinar o concatenar archivos.

El comando `cat` visualizará también los contenidos de un archivo entero en la pantalla (por ejemplo, teclee `cat filename.txt`). Si un archivo es bastante largo, se deplazará rápidamente y por completo por la pantalla. Para evitar esto, use el comando `cat filename.txt | less`.

11.2 Uso de redireccionamiento

El redireccionamiento significa hacer que la shell cambie lo que está considerado como entrada estándar o el lugar donde va a parar la salida estándar.

Para redireccionar la salida estándar, usaremos el símbolo >. Al colocar > tras el comando `cat` (o tras cualquier utilidad o aplicación que escriba la salida estándar) reorientará su salida al nombre de archivo que siga al símbolo.

- `cat > sneakers.txt`
- `cat sneakers.txt home.txt > saturday.txt`
- `cat home.txt >> sneakers.txt`
- `cat < sneakers.txt`

11.3 Tuberias

En el mundo Linux, las tuberías (también conocidas como pipes) relacionan la salida estándar de un comando con la entrada estándar de otro comando.

Considere el comando `ls` discutido anteriormente. Existen varias opciones disponibles con el comando `ls`, pero ¿qué pasa si la visualización del contenido de un directorio es demasiado rápida como para verla?

Vamos a ver el contenido del directorio `/etc/` con el comando:

- `ls -al /etc`
- `ls -al /etc | less`

11.4 El comando more

La diferencia principal entre `more` y `less` es que `less` le permite ir hacia adelante y hacia atrás en un archivo usando las flechas direccionales, mientras que `more` realiza la navegación usando la [Barra espaciadora] y la tecla [B].

Para buscar ciertas palabras dentro de un archivo de texto usando `more`, presione [/] y luego escriba la palabra que desea encontrar en el archivo.

11.5 El comando head

Puede utilizar el comando `head` en caso de que desee ir al inicio de un archivo.

11.6 El comando tail

El contrario de `head` es `tail`. Usando `tail`, puede volver a ver las diez últimas líneas de un archivo

11.7 El comando grep

- `grep coffee sneakers.txt`

`-núm  Las líneas concordantes se mostrarán acompañadas de núm línea anteriores y posteriores. Sin embargo, grep nunca mostrará cualquier línea dada más de una vez.`

> -A núm , --after-context=NÚM
> Muestra núm líneas de contexto después de las que concuerden con el patrón.

-B núm , --before-context=NÚM
Muestra núm líneas de contexto antes de las que concuerden con el patrón.
-C, --context
Equivalente a -2.
-V, --version
Muestra el número de versión de grep en la salida estándar de errores. Este número de versión debería incluirse en todos los informes de fallos (vea más abajo).
-b, --byte-offset
Muestra el desplazamiento en bytes desde el principio del fichero de entrada antes de cada línea de salida.
-c, --count
Suprime la salida normal; en su lugar muestra el número de líneas que concuerdan con el patrón para cada fichero de entrada. Con la opción -v, --revert-match (vea más abajo), muestra el número de líneas que no concuerden.
-e patrón,--regexp=PATRÓN
Emplea patrón como el patrón; útil para proteger patrones que comiencen con -.
-f fichero,--file=FICHERO
Obtiene el patrón de fichero.
-h, --no-filename
Suprime la impresión de los nombres de ficheros antes de las líneas concordantes en la salida, cuando se busca en varios ficheros.
-i, --ignore-case
No hace caso de si las letras son mayúsculas o minúsculas ni en el patrón ni en los ficheros de entrada.
-L, --files-without-match
Suprime la salida normal; en su lugar muestra el nombre de cada fichero de entrada donde no se encuentre ninguna concordancia y por lo tanto de cada fichero que no produciría ninguna salida. La búsqueda se detendrá al llegar a la primera concordancia.
-l, --files-with-matches
Suprime la salida normal; en su lugar muestra el nombre de cada fichero de entrada que produciría alguna salida. La búsqueda se detendrá en la primera concordancia.
-n, --line-number
Prefija cada línea de salida con el número de línea de su fichero de entrada correspondiente.
-q, --quiet
Silencioso; suprime la salida normal. La búsqueda finaliza en la primera concordancia.
-s, --silent
Suprime los mensajes de error sobre ficheros que no existen o no se pueden leer.
-v, --revert-match
Invierte el sentido de la concordancia, para seleccionar las líneas donde no las hay.
-w, --word-regexp
Selecciona solamente aquellas líneas que contienen concordancias que forman palabras completas. La comprobación consiste en que la cadena de caracteres concordante debe estar al principio de la línea o precedida por un carácter que no forme parte de una palabra. De forma similar, debe estar o al final de la línea o ser seguida por un carácter no constituyente de palabra. Los caracteres que se consideran como parte de palabras son letras, dígitos y el subrayado.
-x, --line-regexp
Selecciona solamente aquellas concordancias que constan de toda la línea.
-y Sinónimo obsoleto de -i.
-U, --binary
Trata el(los) fichero(s) como binario(s). De forma predeterminada, bajo MS-DOS y MS-Windows, grep intenta adivinar el tipo del fichero mirando los contenidos de los primeros 32 kB leídos de él. Si grep decide que el fichero es de texto, quita los caracteres CR (retorno de carro) de los contenidos originales del fichero (para que las expresiones regulares con ^ y $ funcionen correctamente). Al especificar -U deshabilitamos este intento de adivinación del tipo del fichero, haciendo que todos se lean y pasen al mecanismo de concordancia tal cuales; si el fichero lo es de texto y tiene al final de cada línea el par de caracteres CR/LF, esto hará que algunas expresiones regulares fallen. Esta opción sólo tiene sentido en MS-DOS y MS-Windows.
-u, --unix-byte-offsets
Informa de desplazamientos de bytes al estilo de Unix. Esta opción hace que grep muestre los desplazamientos de bytes como si el fichero fuera de texto al estilo de Unix; o sea, sin los caracteres CR al final de cada línea. Esto producirá resultados idénticos a ejecutar grep en un sistema Unix. Esta opción no tiene efecto a menos que se dé también la opción -b; sólo tiene sentido en MS-DOS y MS-Windows.

Para mostrar todas las líneas que contienen la cadena «tal» en una lista de archivos (donde «*» representa todos los archivos en el directorio actual):

- grep tal *

Para mostrar todas las líneas que no contengan la cadena «tal», se usa «-v»:

- grep -v tal *

Para mostrar sólo el nombre de tales archivos, se usa «-l»:

- grep -l tal *

Para mostrar sólo el nombre de los archivos que no contienen la cadena, se usa «-L»:

- grep -L tal *

Para buscar recursivamente, no sólo en los archivos del directorio actual sino también en los de sus subdirectorios (donde "." representa el directorio actual), se usa «-r»:

- grep -r tal .

La opción -r puede no estar disponible en todas las plataformas Unix.
Para buscar todas las líneas que comienzan por «Ahora» y terminan con «siempre» seguido de una cantidad arbitraria de espacio en blanco (nótese que el carácter ^ representa el inicio de la línea, así como $ representa el final):

- grep '^Ahora.*siempre *$'

Para hacer que grep lea de la entrada estándar, no se especifica archivo alguno. Por ejemplo, como ps -ef lista todos los procesos actualmente en ejecución, el siguiente comando imprime todos los procesos que está ejecutando el usuario actual:

- ps -ef | grep $USER

ó:

- ps -efa | grep $USER

11.8 Comodines

- * — Hace coincidir todos los caracteres
- ? — Hace coincidir un carácter en una cadena
- * — Hace coincidir el carácter *
- \? — Hace coincidir el carácter ?
- \) — Hace coincidir el carácter)

11.9 Encadenar comandos múltiples

Linux le permite introducir múltiples comandos al mismo tiempo. El único requisito es que separe los comandos con un punto y coma.

- `mkdir rpms/; mv foobar-1.3-2.i386.rpm rpms/`

11.10 Permisos

- `chmod o+w sneakers.txt`
- `chmod go-rw sneakers.txt`
- `chmod a-rwx sneakers.txt`
  - r = 4
  - w = 2
  - x = 1
  - - = 0

11.11 Crear y borrar archivos

Puede crear archivos nuevos con aplicaciones (tales como editores de texto) o usando el comando `touch`, el cual creará un archivo vacío que podrá usar para agregar texto o datos. Para crear un archivo con `touch`, escriba el comando siguiente en el intérprete de comandos del shell.

Para borrar carpetas vacias: `rm -r tigger`

12 Automatización

12.1 CRON

Se trata de unos de los servicios básicos de los sistemas GNU/Linux. De hecho, el demonio *cron* siempre está arrancado; además, dicho servicio asume, asimismo, que el sistema siempre está en funcionamiento.

La función básica de *cron* es la de ejecutar tareas programadas para un determinado momento, y por un usuario con los privilegios necesarios para poder programarlas.

Los ficheros más importantes implicados en el funcionamiento de servicio "cron" son:

- el propio demonio de funcionamiento: crond
- el fichero de configuración (disponible para *root*): /etc/crontab
- el fichero de inicio y parada del demonio: /etc/init.d/cron
- la orden para la programación de tareas (disponible para los usuarios con suficientes privilegios): crontab
- el sistema de informes (*logs*) típico de los sistemas GNU/Linux: /var/log/cron

Como se observa, la configuración del funcionamiento de *cron*, como ya es típico, se encuentra dentro del directorio /etc. Pero, poder arrancar o parar el demonio cron se deberían ejecutar las órdenes correspondientes:

- Parada del demonio cron: # /etc/init.d/cron stop
- Arranque del demonio cron: # /etc/init.d/cron start

Una vez vista su sintaxis, si se deseara ejecutar a las 10 y a las 17 horas, todos los días laborables, la orden `echo "Viva GNU y Linux!"`, se escribiría en el fichero de configuración la línea:

```
0 10,17 * * 1-5 echo "Viva GNU y Linux!" | wall
```

Como aclaración, se puede observar que el día de la semana se puede indicar en dos campos distintos. En caso que los dos forzasen un valor (es decir, que alguno de ellos o los dos no fuesen *), el sistema ejecutará el comando en cualquier de los dos casos (intentará que se cumplan los dos campos). Por ejemplo, en el siguiente ejemplo:

```
0,45 * 13 * 2 echo " Hola martes o 13!" | wall
```

Esta orden se ejecutará cada 45 minutos, todos los martes, y además todos los 13 de cada mes.

Además, en los cinco primeros campos se puede optar por los siguientes cadenas:

@reboot: Se ejecuta al iniciarse la máquina.

@yearly: Se ejecuta una vez al año.

@monthly: Se ejecuta una vez al mes.

@weekly: Se ejecuta una vez por semana.

@daily: Se ejecuta una vez al día.

@hourly: Se ejecuta una vez por hora.

12.1.1 Crontab

La orden crontab es la responsable de la planificación del servicio, y lo que hace es gestionar los ficheros crontabs asignados a cada usuario (en /var/spool/cron/crontabs/).

13 Búsqueda secuencial

La búsqueda secuencial es la técnica más simple para buscar un elemento en un arreglo. Consiste en recorrer el arreglo elemento a elemento e ir comparando con el valor buscado (clave). Se empieza con la primera casilla del arreglo y se observa una casilla tras otra hasta que se encuentra el elemento buscado o se han visto todas las casillas.

14 Búsqueda digital

La búsqueda binaria es el método más eficiente para encontrar elementos en un arreglo ordenado. El proceso comienza comparando el elemento central del arreglo con el valor buscado. Si ambos coinciden finaliza la búsqueda. Si no ocurre así, el elemento buscado será mayor o menor en sentido estricto que el central del arreglo. Si el elemento buscado es mayor se procede a hacer búsqueda binaria en el subarray superior, si el elemento buscado es menor que el contenido de la casilla central, se debe cambiar el segmento a considerar al segmento que está a la izquierda de tal sitio central.

15 Hashing

Una función de Hash es una caja negra que tiene como entrada una llave y como salida una dirección

h(K)=address
Ejemplo: h(LOWELL)=4

- El Hash permite que 2 llaves puedan producir la misma salida --> direcciones iguales, a esto se le conoce como "colisión".Existen distintos grados de colisiones.

15.1 Colisiones

Para reducir el número de colisiones se tienen algunas soluciones:

- **Propagar los registros**
- **Usar memoria extra**
- **Colocar más de un registro en una dirección** recuperar la cubeta

16 Cifrado y criptografía

Cuando se habla de esta área de conocimiento como ciencia se debería hablar de criptología, que a su vez engloba tanto las técnicas de cifrado, es decir la criptografía propiamente dicha, como sus técnicas complementarias, entre las cuales se incluye el criptoanálisis, que estudia métodos empleados para romper textos cifrados con objeto de recuperar la información original en ausencia de las claves.

16.1 Criptografía simétrica

La criptografía simétrica es el método criptográfico que usa una misma clave para cifrar y descifrar mensajes. Las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar. Una vez

ambas tienen acceso a esta clave, el remitente cifra un mensaje usándola, lo envía al destinatario, y éste lo descifra con la misma.

16.2 Criptografía asimétrica

La **criptografía asimétrica** es el método criptográfico que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona a la que se ha enviado el mensaje. Una clave es *pública* y se puede entregar a cualquier persona, la otra clave es *privada* y el propietario debe guardarla de modo que nadie tenga acceso a ella. Además, los métodos criptográficos garantizan que esa pareja de claves sólo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas hayan obtenido casualmente la misma pareja de claves.

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

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

16.3 Firma digital

La **firma digital** hace referencia, en la transmisión de mensajes telemáticos y en la gestión de documentos electrónicos, a un método criptográfico que asocia la *identidad* de una persona o de un equipo informático al mensaje o documento. En función del tipo de firma, puede, además, asegurar la *integridad* del documento o mensaje.

La firma electrónica, como la firma ológrafa (autógrafa, manuscrita), puede vincularse a un documento para identificar al autor, para señalar conformidad (o disconformidad) con el contenido, para indicar que se ha leído o, según el tipo de firma, garantizar que no se pueda modificar su contenido.

17 SqlServer Registro de transacciones

Microsoft SQL Server es un sistema de gestión de bases de datos relacionales (SGBD) basado en el lenguaje Transact-SQL, y específicamente en Sybase IQ, capaz de poner a disposición de muchos usuarios grandes cantidades de datos de manera simultánea[*cita requerida*], así como de tener unas ventajas que más abajo se describen.

Microsoft SQL Server constituye la alternativa de Microsoft a otros potentes sistemas gestores de bases de datos como son ***Oracle***, ***Sybase ASE***, ***PostgreSQL***, ***Interbase***, ***Firebird*** o ***MySQL***.

Soporte de transacciones.

- Escalabilidad, estabilidad y seguridad.
- Soporta procedimientos almacenados.
- Incluye también un potente entorno gráfico de administración, que permite el uso de comandos DDL y DML gráficamente.
- Permite trabajar en modo cliente-servidor, donde la información y datos se alojan en el servidor y las terminales o clientes de la red sólo acceden a la información.
- Además permite administrar información de otros servidores de datos.

Todas las bases de datos de SQL Server 2005 tienen un registro de transacciones que registra todas las transacciones y las modificaciones que cada transacción realiza en la base de datos.

Operaciones compatibles con el registro de transacciones

- Recuperación de transacciones individuales.
- Recuperación de todas las transacciones incompletas cuando se inicia SQL Server.
- Puesta al día de una base de datos, un archivo, un grupo de archivos o una páginrestaurados hasta el momento exacto del error.
- Permitir replicaciones de transacciones.Permitir soluciones de servidor en espera.

18 SQL

El **Lenguaje de consulta estructurado** (SQL [/eseku'ele/ en español, /ɛskjuː'ɛl / o /'siːkwəl/, en inglés] **S**tructured **Q**uery **L**anguage) es un lenguaje declarativo de acceso a bases de datos relacionales que permite especificar diversos tipos de operaciones en éstas. Una de sus características es el manejo del álgebra y el cálculo relacional permitiendo efectuar consultas con el fin de recuperar -de una forma sencilla- información de interés de una base de datos, así como también hacer cambios sobre ella. Es un lenguaje de cuarta generación (4GL).

18.1 Lenguaje de definición de datos (LDD)

El lenguaje de definición de datos (en inglés *Data Definition Language*, o *DDL*), es el que se encarga de la modificación de la estructura de los objetos de la base de datos. Existen cuatro operaciones básicas: CREATE, ALTER, DROP y TRUNCATE.

CREATE

Este comando crea un objeto dentro de la base de datos. Puede ser una tabla, vista, índice, trigger, función, procedimiento o cualquier otro objeto que el motor de la base de datos soporte.

ALTER

Este comando permite modificar la estructura de un objeto. Se pueden agregar/quitar campos a una tabla, modificar el tipo de un campo, agregar/ quitar índices a una tabla, modificar un trigger, etc.

DROP

Este comando elimina un objeto de la base de datos. Puede ser una tabla, vista, índice, trigger, función, procedimiento o cualquier otro objeto que el motor de la base de datos soporte. Se puede combinar con la sentencia ALTER.

TRUNCATE

Este comando trunca todo el contenido de una tabla. La ventaja sobre el comando DELETE, es que si se quiere borrar todo el contenido de la tabla, es mucho más rápido, especialmente si la tabla es muy grande, la desventaja es que TRUNCATE solo sirve cuando se quiere eliminar absolutamente todos los registros, ya que no se permite la cláusula WHERE. Si bien, en un principio, esta sentencia parecería ser DML (Lenguaje de Manipulación de Datos), es en realidad una DDL, ya que internamente, el comando truncate borra la tabla y la vuelve a crear y no

ejecuta ninguna transacción.

18.2 Lenguaje de manipulación de datos (LMD)

Definición

Un lenguaje de manipulación de datos (*Data Manipulation Language*, o *DML* en inglés) es un lenguaje proporcionado por el sistema de gestión de base de datos que permite a los usuarios llevar a cabo las tareas de consulta o manipulación de los datos, organizados por el modelo de datos adecuado.

El lenguaje de manipulación de datos más popular hoy día es SQL, usado para recuperar y manipular datos en una base de datos relacional. Otros ejemplos de DML son los usados por bases de datos IMS/DL1, CODASYL u otras.

INSERT

- `INSERT INTO ''tabla'' (''columna1'', [''columna2,...''']) VALUES (''valor1'', [''valor2,...''])`
- `INSERT INTO agenda_telefonica (nombre, numero) VALUES ('Roberto Jeldrez', '4886850');`
- `INSERT INTO ''tabla'' VALUES (''valor1'', [''valor2,...''])`
- `INSERT INTO agenda_telefonica VALUES ('Roberto Jeldrez', '4886850');`
- `INSERT INTO ''tabla'' (''columna1'', [''columna2,...''']) VALUES (''valor1a'', [''valor1b,...'']), (''value2a'', [''value2b,...'']),...`

UPDATE

Una sentencia *UPDATE* de **SQL** es utilizada para modificar los valores de un conjunto de registros existentes en una tabla.

DELETE

- `DELETE FROM ''tabla'' WHERE ''columna1'' = ''valor1''`

19 Transac SQL

(T-SQL). Transact-SQL es una extensión del lenguaje SQL, propiedad de Microsoft y Sybase. La implementación de Microsoft funciona en los productos Microsoft SQL Server. En tanto, Sybase utiliza el lenguaje en su Adaptative Server Enterprise, el sucesor de Sybase SQL Server.

Para hacer a SQL más poderoso, le fueron agregados algunas características como:

-Mejora en las declaraciones DELETE y UPDATE.
-Variables locales.
-Soporte de varias funciones para el procesamiento de cadenas, datos, matemática, etc.
-Un lenguaje de control de flujos.

Para el lenguaje de control de flujos utiliza palabras claves como BEGIN y END, BREAK, CONTINUE, GOTO, IF y ELSE, RETURN, WAITFOR y WHILE.

Para las variables locales utiliza DECLARE para declararlas y SET para proveerles un valor.

En tanto las mejoras en las declaraciones DELETE Y UPDATE se debe a que ambas permiten una cláusula FROM.

20 MySql

MySQL es un sistema de gestión de base de datos relacional, multihilo y multiusuario con más de seis millones de instalaciones.[1] MySQL AB —desde enero de 2008 una subsidiaria de Sun Microsystems y ésta a su vez de Oracle Corporation desde abril de 2009— desarrolla MySQL como software libre en un esquema de licenciamiento dual.

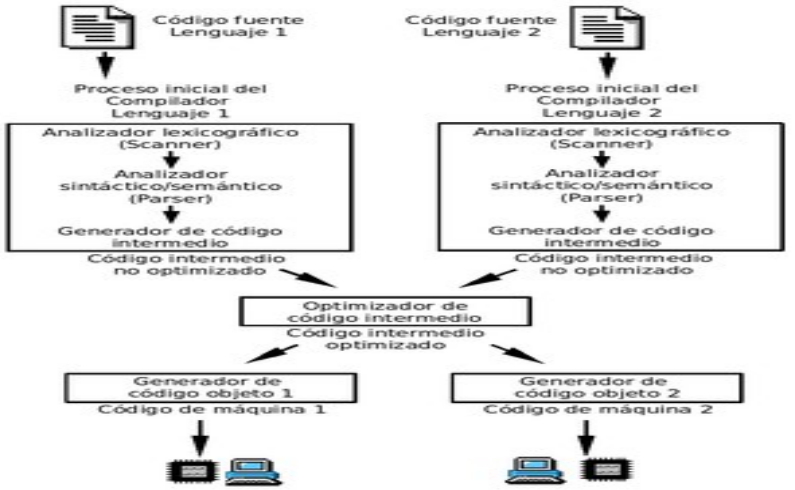
Por un lado se ofrece bajo la GNU GPL para cualquier uso compatible con esta licencia, pero para aquellas empresas que quieran incorporarlo en productos privativos deben comprar a la empresa una licencia específica que les permita este uso. Está desarrollado en su mayor parte en ANSI C.

Al contrario de proyectos como Apache, donde el software es desarrollado por una comunidad pública y el copyright del código está en poder del autor individual, MySQL es propietario y está patrocinado por una empresa privada, que posee el copyright de la mayor parte del código.

21 PostgreSQL

PostgreSQL es un sistema de gestión de base de datos relacional orientada a objetos de software libre, publicado bajo la licencia BSD.

22 Del código al ejecutable



23 Clases de lenguaje de programación

23.1 Lenguajes de bajo nivel

- El lenguaje maquina: este lenguaje ordena a la máquina las operaciones fundamentales para su funcionamiento.
- El lenguaje ensamblador es un derivado del lenguaje maquina y esta formado por abreviaturas de letras y números llamadas mnemotécnicos.

24 Lenguajes de alto nivel

Los que se asemejan a la forma de hablar humana.

- Primera generación: lenguaje maquina.
- Segunda generación: se crearon los primeros lenguajes ensambladores.

- Tercera generación: se crean los primeros lenguajes de alto nivel. Ej. C, Pascal, Cobol…
- Cuarta generación. Son los lenguajes capaces de generar código por si solos, son los llamados RAD, con lo cuales se pueden realizar aplicaciones sin ser un experto en el lenguaje. Aquí también se encuentran los lenguajes orientados a objetos, haciendo posible la reutilización d partes del código para otros programas. Ej. Visual, Natural Adabes…
- Quinta generación: aquí se encuentran los lenguajes orientados a la inteligencia artificial. Estos lenguajes todavía están poco desarrollados. Ej. LISP

25 Poo

La programación orientada a objetos es una nueva forma de programar que trata de encontrar una solución a estos problemas. Introduce nuevos conceptos, que superan y amplían conceptos antiguos ya conocidos. Entre ellos destacan los siguientes:

- **Clase**:
- **Herencia**
- **Objeto**
- **Método**
- **Evento**
- **Mensaje**
- **Propiedad o atributo**
- **Estado interno**
- **Componentes de un objeto**
- **Representación de un objeto**

En comparación con un lenguaje imperativo, una "variable", no es más que un contenedor interno del atributo del objeto o de un estado interno, así como la "función" es un procedimiento interno del método del objeto.

25.1 Características de la POO

Hay un cierto desacuerdo sobre exactamente qué características de un método de programación o lenguaje le definen como "orientado a objetos", pero hay un consenso general en que las características siguientes son las más importantes (para más información, seguir los enlaces respectivos):

- **Abstracción**:
- **Encapsulamiento**
- **Principio de ocultación**
- **Polimorfismo**
- **Herencia**
- **Recolección de basura**

26 Entorno Gambas

Gambas es un lenguaje de programación libre derivado de BASIC. Es similar al producto de Microsoft Visual Basic y se distribuye con licencia GNU GPL. Cabe destacar que presenta ciertas similitudes con Java ya que en la ejecución de cualquier aplicación, se requiere un conjunto de librerías interprete previamente instaladas (Gambas Runtime) que entiendan el bytecode de las aplicaciones desarrolladas y lo conviertan en codigo ejecutable por el computador. Por otro lado, a diferencia de Java, no se experimentan ralentizaciones y es posible desarrollar grandes aplicaciones en poco tiempo.

Permite crear formularios con botones de comandos, cuadros de texto y muchos otros controles y enlazarlos a bases de datos como MySQL, PostgreSQL o SQLite además de facilitar la creación de aplicaciones muy diversas como videojuegos (utilizando OpenGL), aplicaciones para dispositivos moviles (en desarrollo pero muy avanzado), aplicaciones de red (con manejo avanzado de protocolos HTTP, FTP, SMTP, DNS), entre otras .

27 XHTML

28 1. Introducción

Con la introducción de la familia de módulos y documentos del tipo XHTML, el W3C ha contribuido a trasladar a la comunidad de desarrolladores de contenido de Internet desde los días del marcado mal formado, no-estándar hasta el mundo bien formado y válido de XML [XML]. En XHTML 1.0, este movimiento fue moderado por la meta de proporcionar una migración fácil desde el contenido existente, basado en HTML 4 (o anterior) a XHTML y XML. Con el advenimiento de los módulos XHTML definidos en Modularización de XHTML, el W3C ha eliminado el soporte para elementos y atributos en desuso de la familia XHTML. Estos elementos y atributos tenían una funcionalidad ampliamente orientada a la presentación que se maneja mejor vía hojas de estilo o comportamientos por defecto específicos de los clientes..

28.1 Normas

Norma número 1: Hay que hacer una declaración del tipo de documento (doctype)

En HTML también se puede hacer pero no es obligatorio. En XHTML es obligatorio.

Al comienzo del documento por encima de la etiqueta <html> hay que escribir la siguiente declaración:

```
<!DOCTYPE html PUBLIC "-//W3C//DTD
XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/
xhtml1-transitional.dtd">
```

A propósito, hacemos una simplificación. Nos quedamos con el tipo Transitional. Hay otros dos tipos, el estricto y el frameset. Para estos dos tipos y profundizar en este lenguaje, acudir a la red. Aquí, por ejemplo.

Es importante escribir el texto de la declaración tal cual está respetando mayúsculas y minúsculas.

Norma número 2: La etiqueta <html> debe llevar el namespace declarado en el atributo xmlns. El siguiente texto:

```
<html xmlns="http://www.w3.org/1999/xhtml">
```

Norma número 3: Todas las etiquetas (exceptuando la declaración, norma 1) y sus atributos, tienen que escribirse con letras minúsculas.

En HTML se pueden escribir con mayúsculas o minúsculas. En XHTML todas deben ser minúsculas.

Así:
 pasa a ser

La inclusión de una imagen, por ejemplo: <img src="imagenes/logo.png" widt="50" height="30"> tiene que escribirse ahora así Observa el espacio de separación antes de la barra de cierre.

Lo anterior es válido para todas las etiquetas similares. Incluído las etiquetas <meta> de la <head>.

Norma número 4: La etiqueta <head> (y por supuesto la <body>) son absolutamente obligatorias.

En HTML si no poníamos la <head> no pasaba nada...

Norma número 5: La anidación de las etiquetas y sus cierres debe hacerse respetando las simetrías correspondientes: Lo que primero se abre, se cierra lo último.

Por ejemplo:

```
<p> Marcar con <b> negrita <u> subrayado y <i> cursiva</i></u></b></p>
```

Norma número 6: Todas las etiquetas (todas) se deben cerrar.

En HTML, por ejemplo, la etiqueta <p> era opcional que se cerrase. Aquí es obligatorio.

Había etiquetas que no se cerraban nunca como
. En XHTML las etiquetas que no se cerraban en HTML tienen que escribirse con un espacio y la barra de cerrado dentro de la etiqueta.

Norma número 7: Todos los valores de los atributos deben entrecomillarse.

En HTML era opcional.

Por ejemplo <table border=2> que se permitía en HTML, pasaría a escribirse obligatoriamente <table border="2">

Módulo de Estructura*

```
body, head, html, title
```

Módulo de Texto*

```
abbr, acronym, address, blockquote, br, cite,
code, dfn, div, em, h1, h2, h3, h4, h5, h6,
kbd, p, pre, q, samp, span, strong, var
```

Módulo de Hipertexto*

```
a
```

Módulo de Lista*
`dl, dt, dd, ol, ul, li`
Módulo de Objetos
`object, param`
Módulo de Presentación
`b, big, hr, i, small, sub, sup, tt`
Módulo de Edición
`del, ins`
Módulo de Texto Bidireccional
`bdo`
Módulo de Formularios
`button, fieldset, form, input, label, legend, select, optgroup, option, textarea`
Módulo de Tablas
`caption, col, colgroup, table, tbody, td, tfoot, th, thead, tr`
Módulo de Imagen
`img`
Módulo de Mapa de Imagen del lado Cliente
`area, map`
Módulo de Mapa de Imagen del lado Servidor
Attribute `ismap` on `img`
Módulo de Eventos Intrínsecos
Events attributes
Módulo de Metainformación
`meta`
Módulo de Scripting
`noscript, script`
Módulo de Hoja de Estilo
`style` element
Módulo del Atributo Style *En desuso*
`style` attribute
Módulo de Link
`link`
Módulo de Base
`base`

29 PHP

Se escribe dentro de Html asi:

```
<? ?>
<%%>
<?php ?>
<script language="php"> </script>
```

29.1 Variables

A diferencia de otros lenguajes, PHP posee una gran flexibilidad a la hora de operar con variables. En efecto, cuando definimos una variable asignándole un valor, el ordenador le atribuye un tipo. Si por ejemplo definimos una variable entre comillas, la variable será considerada de tipo cadena:

```
<?
$cadena="5"; //esto es una cadena
$entero=3; //esto es un entero
echo $cadena+$entero
?>
```

29.2 Control de flujo de programa

Todo lenguaje de programación dispone de órdenes de control de flujo, que permite al programa *tomar decisiones lógicas* segun reciba unos parámetros o otros: *si llueve coge el paraguas; pero si hace sol vete a la playa*.

Las posibilidades que ofrece php son:

- `if/else`
- `if/elseif/else`
- `switch`
- `do/while`
- `while`
- `for`

if else

Es la estructura de control mas corriente: La declaración **if** obliga a evaluar la expresión entre paréntesis; si se evalua como verdadera, se ejecuta un bloque de código; si se evalua como falsa, el bloque de código es ignorado. De esta forma nuestro script puede tomar *decisiones*:

```
<?php
$edad="";
if($edad>=18)
{
echo"puedes sacar el coche";
}
else
{
echo "ve en autobús";
}

?>
```

```
<?php
if ($user == "pepe")
{
//código especial para el usuario pepe
}

?>
```

29.3 Condiciones complejas

Mediante el uso de operadores podemos introducir condiciones complejas, agrupándolas con parentesis:

```
<?php
if(($edad>=18)&&($carnet_conducir==1))
{
}
?>
```

29.4 if elseif else

Exactamente igual que la anterior, solo que evaluando mas de una condición:

```
<?php
if ($user=="pepe")
{
//codigo para pepe
}
elseif ($user=="juan")
{
//codigo para juan
}

else
{
//codigo para quienes no son juan ni pepe
}

?>
```

29.5 switch

`switch` es una alternativa quizas mas legible cuando necesitamos evaluar una variable frente a multiples valores posibles:

```
<?php

$op="a";

switch($op){
case"a":
//código que se ejecuta si $op vale "a"
break;

case "b":
//código que se ejecuta si $op vale "b"
break;
case"c":
//código que se ejecuta si $op vale "c"
break;
default:
//código a ejecutar por defecto si no se cumple ninguna condición
}

?>
```

El uso de `break;` es necesario, ya que en la estructura `switch` una vez cumplida una condición se ejecutan el resto de declaraciones (incluso las comprendidas en los casos que siguen). La orden `break` evita esto saltando fuera del `switch` y continuando la ejecución del resto del script. Si en lugar de `break` usamos `exit`, el resto del script no se ejecutará.

29.6 While

```
<?php
$cuenta = 0;

echo "Voy a entrar al bucle while <br>";
```

```
while ( $cuenta <= 10) {
echo "Cuenta vale $cuenta <br>";
$cuenta++;
}

echo "He salido del bucle while";
?>
```

29.7 For

```
<?php
for ( $i = 1 ; $i <= 10 ; $i ++) {
print $i ;
}
?>
```

29.8 Funciones

```
function sumar($a,$b)
{return $a + $b;
};
```

30 Java

30.1 Tipos primitivos

Los tipos primitivos son los que permiten manmipular valores numéricos (con distintos grados de precisión), caracteres y valores booleanos (verdadero / falso). Los Tipos Primitivos son:

- **`boolean`** : Puede contener los valores **`true`** o **`false`**.
- **`byte`** : Enteros. Tamaño 8-bits. Valores entre -128 y 127.
- **`short`** : Enteros. Tamaño 16-bits. Entre -32768 y 32767.
- **`int`** : Enteros. Tamaño 32-bits. Entre -2147483648 y 2147483647.
- **`long`** : Enteros. Tamaño 64-bits. Entre -9223372036854775808 y 9223372036854775807.
- **`float`** : Números en coma flotante. Tamaño 32-bits.
- **`double`** : Números en coma flotante. Tamaño 64-bits.
- **`char`** : Caracteres. Tamaño 16-bits. Unicode. Desde `'\u0000'` a `'\uffff'` inclusive. Esto es desde 0 a 65535

30.2 Variables

Una variable es un área en memoria que tiene un nombre y un Tipo asociado. El Tipo es o bien un Tipo primitivo o una Referencia.

Es obligatorio declarar las variables antes de usarlas. Para declararlas se indica su nombre y su Tipo, de la siguiente forma:

tipo_variable nombre **;**

30.3 Clases

```
class Punto {
int x;
int y;
}
```

31 Ciclo de vida

1. Planificacion
2. Analisis
3. Diseño
4. Desarrollo
5. Implantacion/Pruebas/Validacion

32 Diagrama Entidad Relación

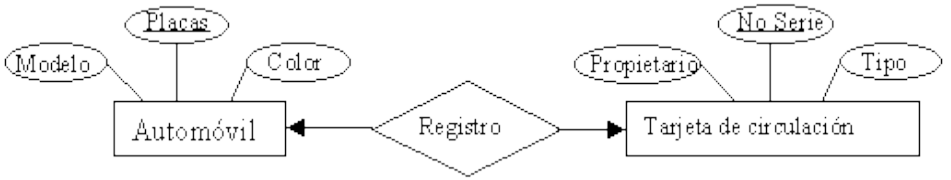
Denominado por sus siglas como: E-R; Este modelo representa a la realidad a través de un esquema gráfico empleando los terminología de entidades, que son objetos que existen y son los elementos principales que se identifican en el problema a resolver con el diagramado y se distinguen de otros por sus características particulares denominadas atributos, el enlace que que rige la unión de las entidades esta representada por la relación del modelo.

Recordemos que un rectángulo nos representa a las entidades; una elipse a los atributos de las entidades, y una etiqueta dentro de un rombo nos indica la relación que existe entre las entidades, destacando con líneas las uniones de estas y que la llave primaria de una entidad es aquel atributo que se encuentra subrayado.

A continuación mostraremos algunos ejemplos de modelos E-R, considerando las cardinalidades que existen entre ellos:

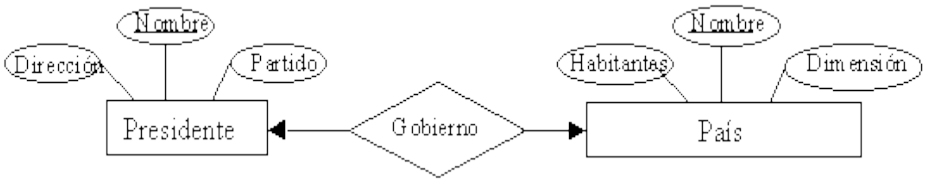
Relación Uno a Uno.

Diseñar el modelo E-R, para la relación Registro de automóvil que consiste en obtener la tarjeta de circulación de un automóvil con los siguientes datos:- Automóvil- Modelo, Placas, Color - Tarjeta de circulación -Propietario, No_serie, Tipo.



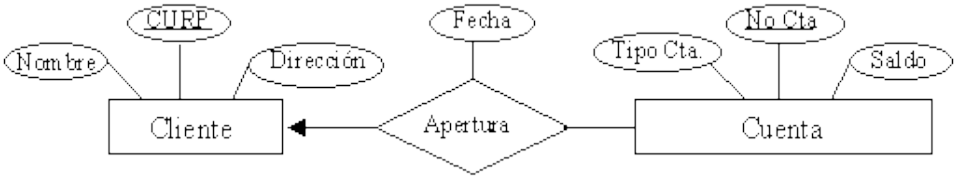
Indicamos con este ejemplo que existe una relación de pertenencia de uno a uno, ya que existe una tarjeta de circulación registrada por cada automóvil.

En este ejemplo, representamos que existe un solo presidente para cada país.



Relación muchos a muchos.

El siguiente ejemplo indica que un cliente puede tener muchas cuentas, pero que una cuenta puede llegar a pertenecer a un solo cliente (Decimos puede, ya que existen cuentas registradas a favor de más de una persona).



33 UML

En UML 2.0 hay 13 tipos diferentes de diagramas. Para comprenderlos de manera concreta, a veces es útil categorizarlos jerárquicamente, como se muestra en la figura de la derecha.

Los ***Diagramas de Estructura*** enfatizan en los elementos que deben existir en el sistema modelado:

- Diagrama de clases
- Diagrama de componentes
- Diagrama de objetos
- Diagrama de estructura compuesta (UML 2.0)
- Diagrama de despliegue
- Diagrama de paquetes

Los ***Diagramas de Comportamiento*** enfatizan en lo que debe suceder en el sistema modelado:

- Diagrama de actividades
- Diagrama de casos de uso
- Diagrama de estados

Los ***Diagramas de Interacción*** son un subtipo de diagramas de comportamiento, que enfatiza sobre el flujo de control y de datos entre los elementos del sistema modelado:

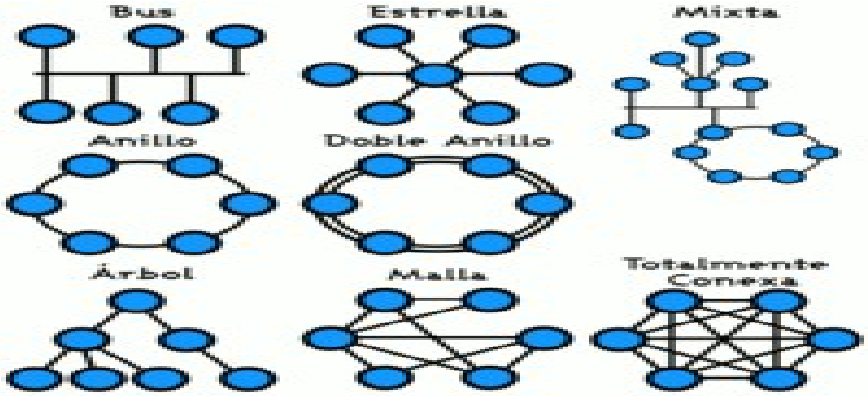
- Diagrama de secuencia
- Diagrama de comunicación, que es una versión simplificada del Diagrama de colaboración (UML 1.x)
- Diagrama de tiempos (UML 2.0)
- Diagrama global de interacciones o Diagrama de vista de interacción (UML 2.0)

34 Redes

34.1 Osi

Capa 1: Nivel físico
o Cable coaxial, Cable de fibra óptica, Cable de par trenzado, Microondas, Radio, Palomas, RS-232.
Capa 2: Nivel de enlace de datos
o Ethernet, Fast Ethernet, Gigabit Ethernet, Token Ring, FDDI, ATM, HDLC.
* Capa 3: Nivel de red
o ARP, RARP, IP (IPv4, IPv6), X.25, ICMP, IGMP, NetBEUI, IPX, Appletalk.
* Capa 4: Nivel de transporte
o TCP, UDP, SPX.
* Capa 5: Nivel de sesión
o NetBIOS, RPC, SSL.
* Capa 6: Nivel de presentación
o ASN.1.
* Capa 7: Nivel de aplicación
o SNMP, SMTP, NNTP, FTP, SSH, HTTP, SMB/CIFS, NFS, Telnet, IRC, ICQ, POP3, IMAP.

34.2 Tipologías de redes



34.3 Direccionamiento

La direccion es el identificador que permite a otras maquinas enviar información , en el protocolo IP ifica un punto de union en la red llamado interfaz .Una ,aquina puede tener multiples interfaces, teniendo una direccion IP por cada una de ellas , las interfaces son por lo general conexiones fisicas distintas , pero tambien pueden ser conexiones logicas compartiendo una misma interfaz.

34.4 Estructura de una dirección IP

Las direcciones IP poseen 32 bits de longitud y están divididas en cuatro octetos (8 bits). Una dirección IP puede ser escrita en varias formas: binaria, decimal y hexadecimal. Una dirección IP consiste de dos niveles jerárquicos, los cuales son: el identificador de red, netid, y el identificador de máquina, hostid. En el protocolo IP el identificador de red representa un número de máquinas que pueden comunicarse entre ellas a través de la capa dos del modelo de referencia OSI. El identificador de máquina representa el número de la máquina dentro de la red. La dirección IP identifica la máquina de forma única en toda Internet.

34.5 Numeros de red y mascara

La división del número de red y de máquina es distinta para cada red. Esto facilita al software de enrutadores y máquinas identificar con facilidad dónde ocurre la división. Cada dirección tiene una máscara de red asociada, la cual es representada por un número de 32 bits, donde todos los bits de la porción de red están en 1 y todos los bits de la porción de máquina están en 0. Los primero 16 bits están asociados al número de red y los 16 restantes al número de la máquina dentro de la red. Una computadora puede extraer el número de red de una dirección IP realizando una operación lógica AND de la máscara con la dirección IP. Las máscaras de redes permiten tener 1 discontinuos, pero esta práctica ha sido eliminada pues tiende a confundir a las personas.

34.6 Clases de dirección IP.

Clase	Rango	N° de Redes	N° de Host	Máscara de Red	Broadcast
A	1.0.0.0 - 127.0.0.0	126	16.777.214	255.0.0.0	x.255.255.255
B	128.0.0.0 - 191.255.0.0	16.384	65.534	255.255.0.0	x.x.255.255
C	192.0.0.0 - 223.255.255.0	2.097.152	254	255.255.255.0	x.x.x.255
D	224.0.0.0 - 239.255.255.255				
E	240.0.0.0 - 255.255.255.255				

34.7 Enrutamiento Estatico

Enrutamiento Estático Una red con un número mínimo de enrutadores puede ser configurada con enrutamiento estático. Para una red con un solo gateway, la mejor opción es el enrutamiento estático. Una tabla de

enrutamiento estático es construida manualmente, por el administrador de la red, usando el comando route. Las tablas de enrutamiento estático no se ajustan a los cambios de la red, ellos trabajan mejor cuando las rutas no cambian. Para agregar una ruta se utiliza el comando route. El destino final debe ser conocido. El Linux utiliza el comando route para agregar o borrar entradas manualmente en la tabla de enrutamiento. Por ejemplo, para agregar la ruta 150.185.156.1 a la tabla de enrutamiento en linux se procede de la siguiente forma :

- `#route add –host 150.185.156.1 eth0`
- `Esta nueva ruta se agregará a la tabla de enrutamiento: # route –n`
- `#route add default gw 150.185.162.1`

34.8 Enrutamiento Dinamico

Enrutamiento Dinámico Una red con más de una posible ruta al mismo destino podría usar enrutamiento dinámico. Una ruta dinámica es construida por información intercambiada por los protocolos de enrutamiento. Los protocolos son diseñados para distribuir información que dinámicamente ajustan las rutas reflejadas en las condiciones de la red. Los protocolos de enrutamiento manejan complejas situaciones de enrutamiento más rápido de lo que un administrador del sistema podría hacerlo. Los protocolos de enrutamiento no sólo están diseñados para cambiar a una ruta de respaldo cuando la ruta primaria se vuelve inoperante sino que ellos también evalúan y deciden cual es la mejor ruta para un destino. Una red con múltiples caminos a un mismo destino puede utilizar enrutamiento dinámico.

`Este lo único que necesita hacer es iniciar el demonio ROUTED.`

34.9 Redes Virtuales

La **Red Privada Virtual** (**RPV**), en inglés *Virtual Private Network* (**VPN**), es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

Ejemplos comunes son, la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet, permitir a los miembros del equipo de soporte técnico la conexión desde su casa al centro de cómputo, o que un usuario pueda acceder a su equipo doméstico desde un sitio remoto, como por ejemplo un hotel. Todo ello utilizando la infraestructura de Internet.

34.10 VPN de acceso remoto

Es quizás el modelo más usado actualmente y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hoteles, aviones preparados, etcétera) utilizando Internet como vínculo de acceso. Una vez autentificados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa. Muchas empresas han reemplazado con esta tecnología su infraestructura dial-up (módems y líneas telefónicas).

34.11 VPN punto a punto

Este esquema se utiliza para conectar oficinas remotas con la sede central de la organización. El servidor VPN, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet,

típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos punto a punto tradicionales, sobre todo en las comunicaciones internacionales. Es más común el punto anterior, también llamada tecnología de túnel o *tunneling*.

34.12 TUNNELING

Básicamente, esta técnica consiste en abrir conexiones entre dos máquinas por medio de un protocolo seguro, como puede ser SSH (*Secure SHell*), a través de las cuales realizaremos las transferencias inseguras, que pasarán de este modo a ser seguras. De esta analogía viene el nombre de la técnica, siendo la conexión segura (en este caso de *ssh*) el túnel por el cual se envían los datos para que nadie más aparte de los interlocutores que se sitúan a cada extremo del túnel, pueda ver dichos datos. Este tipo de técnica requiere de forma imprescindible tener una cuenta de acceso seguro en la máquina con la que se quiere comunicar los datos.

34.13 VPN interna

Este esquema es el menos difundido pero uno de los más poderosos para utilizar dentro de la empresa. Es una variante del tipo "acceso remoto" pero, en vez de utilizar Internet como medio de conexión, emplea la misma red de área local (LAN) de la empresa. Sirve para aislar zonas y servicios de la red interna. Esta capacidad lo hace muy conveniente para mejorar las prestaciones de seguridad de las redes inalámbricas (WiFi).

Un ejemplo clásico es un servidor con información sensible, como las nóminas de sueldos, ubicado detrás de un equipo VPN, el cual provee autenticación adicional más el agregado del cifrado, haciendo posible que sólo el personal de recursos humanos habilitado pueda acceder a la información.

35 Ley de Protección de datos

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 las Fuerzas 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 integro 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 prohíbe 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 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 o 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 ya 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 contraprestación 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 sobre 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*.

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 tributarias 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 a la 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 del 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 promociona1 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 contraprestación 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 o 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 serle 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.*

1. 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.

2. Las resoluciones de la Agencia Española de Protección de Datos se harán públicas, una vez hayan sido notificadas a los interesados. La publicación se realizará preferentemente a través de medios informáticos o telemáticos.

Reglamentariamente podrán establecerse los términos en que se lleve a cabo la publicidad de las citadas resoluciones.

Lo establecido en los párrafos anteriores no será aplicable a las resoluciones referentes a la inscripción de un fichero o tratamiento en el Registro General de Protección de Datos ni a aquéllas por las que se resuelva la inscripción en el mismo de los Códigos tipo, regulados por el artículo 32 de esta ley orgánica.

[El apartado 2 de este artículo ha sido añadido por el art. 82.1 de la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social (BOE núm. 313, de 31-12-2003, pp. 46874-46992).]

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 reglamentariamente.

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 1), 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 ya 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 del 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 4 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.

5. 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.

3. Los procedimientos sancionadores tramitados por la Agencia Española de Protección de Datos, en ejercicio de las potestades que a la misma atribuyan esta u otras Leyes, salvo los referidos a infracciones de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, tendrán una duración máxima de seis meses.

[El apartado 3 de este artículo ha sido añadido por el art. 82.2 de la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social (BOE núm. 313, de 31-12-2003, pp. 46874-46992).]

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 del 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 del 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 Tributaria 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 tributaria 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 2.º 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. *Subsistencia de normas preexistentes.*

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.