Administración de redes y sistemas operativos

TEMA 1 INTRODUCCIÓN A LA ADMINISTRACIÓN DE SISTEMAS

Tema 1
Introducción a la administración de sistemas

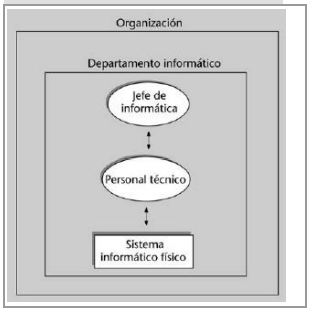
1. EL SISTEMA INFORMÁTICO Y LA ORGANIZACIÓN

La informática dentro de una organización puede estudiarse desde puntos de vista muy diferentes. Desde el punto de vista de la organización, desde el punto de vista de los informáticos, de los usuarios, de la dirección, etc, pero en cualquier caso el sistema informático debe ser eficaz (conseguir lo que pretende) y eficiente (hacerlo con un consumo de tiempo y recursos aceptable).

Destaca la figura del **jefe de departamento de informática** o jefe de las tecnologías de información cuyos objetivos son la planificación y gestión del departamento y ofrecer un buen servicio a los usuarios.

2. COMPONENTEL DEL SISTEMA INFORMÁTICO

Sistema informático



Destacan dentro del sistema informático las siguientes partes:

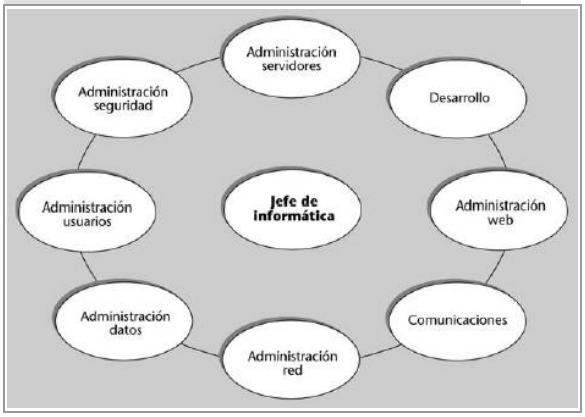
- **Servidores**: Es normal contar con diferentes servidores que se especializan en funciones distintas, lo que aumenta el control por parte de los administradores de sistemas y disminuye el riesgo de fallos.
- **Terminales de trabajo**: Se está llegando a alcanzar un Terminal de trabajo por cada trabajador de la empresa.
- **Red**: Es el cableado físico que conecta los terminales de trabajo y la electrónica de control de la red (hubs, routers, switches…).

Software: Podemos encontrar como mínimo dos sistemas operativos: el de los servidores y el de los terminales, lo que complica la administración de los sistemas.

3. PERSONAL RESPONSABLE DEL SISTEMA INFORMÁTICO

Existen diversas funciones que pueden ser cubiertas cada una de ellas por una persona o un grupo de ellas encabezadas por un jefe; o una persona puede llevar a cabo más de una función a la vez, todo ello estará en consonancia con la política y tradición de la empresa y también con la envergadura de la organización. Las distintas funciones y/o departamentos que podemos encontrar son:

Funciones



- **Administración de servidores**: Se encarga de instalar y mantener dando servicio a la organización en todo lo referente a los servidores, también se encarga de recuperarlos en caso de fallo.
- **Administración de usuarios**: Necesidades y atención a los usuarios y al mantenimiento de sus equipos de sobremesa, ya sean PCs o terminales.
- **Administración de la red**: Se debe asegurar que funcione correctamente la red y también controlar que se encuentre en buen estado, así como mejorarla y extenderla haciéndola llegar a todos los rincones de la organización.
- **Administración de los datos**: Esta función se ocupa de mantener la integridad de la información de la organización, tanto si se encuentra en un lugar físico como dispersa por los servidores (lo más habitual es una combinación de ambas).

- **Administración de la web**: Mantenimiento del servidor web y actualización del contenido de las páginas.
- **Administración de la seguridad**: Es compleja esta función pues incluye desde la seguridad de la información existente hasta la protección física de los equipos contra robos, prevención contra ataques por virus, etc.
- **Desarrollo**: Si se requiere nuevo software para cubrir necesidades que van apareciendo, el departamento de desarrollo es el encargado de llevarlo a cabo.
- **Jefe de informática**: Esta función junto con la de administración de servidores y de usuarios son las más importantes. El jefe de informática es el enlace entre las necesidades de la empresa y el trabajo que se realiza en el departamento. Qué software comprar o desarrollar, qué servidores son necesarios, que red instalar, etc, son decisiones a las que el jefe de informática debe enfrentarse

El **solapamiento de funciones** puede llegar a darse con mucha facilidad, es decir, si debemos dar de alta un usuario en un servidor, ¿Quién lo hace? El administrador de usuarios o el de servidores… este solapamiento de funciones se debe a que cada departamento tiene unas tareas muy definidas pero en absoluto independientes de otros departamentos.

De hecho, una misma persona puede asumir los tres cargos más importantes dentro del departamento informático, es decir: jefe de informática, administrador de usuarios y administrador de servidores, siempre y cuando la envergadura de la organización lo permita.

TEMA 2 ADMINISTRACIÓN DE SERVIDORES

1. EL SERVIDOR Y SUS FUNCIONES

Un **servidor** es una máquina que funciona las 24 horas los 7 días de la semana, lo que implica tener un hardware preparada para no detenerse nunca y soportar reparaciones y ampliaciones en caliente. Cuenta con sistemas para que los usuarios puedan acceder a la información de una manera selectiva, gestionan colas de impresión, muestran páginas web, registran la actividad de cuanto se realiza, tramitan el correo de la organización y ya no ocupan, como antaño, habitaciones enteras.

Las **funciones** de los servidores son varias:

- Servidores de ficheros
- Servidores de impresión
- Servidores de páginas web
- Servidores de Noticias
- Servidores de Correo
- Servidores de FTP…

Hemos de distinguir el servidor físico (o corporativo que es la cantidad de ordenadores que están instalados) de los servidores funcionales (que realizan una función de servidor al ofrecer información a otro ordenador cliente). El número y la función o funciones de cada servidor estará en función, como siempre, de la envergadura de la organización.

2. TIPOS DE SERVIDORES EXISTENTES

Existen dos grandes tipos de arquitecturas con sus diferencias:

- **Arquitecturas UNIX**: El ordenador suele ser el propietario del sistema operativo que se instala: Hewlett-Packard, SUN, Silicon Graphics, IBM, Dec Alpha…
- **Arquitecturas PC**: El hardware corresponde al de un PC, pero con componentes de elevadas prestaciones y con sistema operativo Linux, Unix, Microsoft para redes…

Como actualmente la tendencia es la informática distribuida, es decir, servidores con funciones específicas con un coste variable a las funciones que debe realizar, pero comunicados entre ellos para intercambiar información, contamos así con **servidores heterogéneos**: Las organizaciones suelen poseer más de un servidor físico que se conecta con otro servidor físico que probablemente tenga un sistema operativo diferente y un sistema de ficheros también distinto. Para solventar el problema de comunicación entre ambos primero debemos contar con una conexión física de cable entre ellos, y después o esperamos contar con una fórmula común para intercambiar información (TCP/IP para los servidores modernos) o con algún software de terceros que nos solucione la papeleta. En cualquiera de los dos casos debemos tener cuidado de no ralentizar en exceso la red global o empeorar el rendimiento del sistema al realizar un uso intensivo de este intercambio de información.

3. REQUERIMIENTOS DE LOS SISTEMAS OPERATIVOS DE RED

Las funciones que debe proporcionas el sistema operativo de red son:

- Servidor de ficheros: definir grupos de usuarios, compartir ficheros entre todos los usuarios, compartir ficheros entre grupos de usuarios y asignar un espacio personal para cada usuario.
- Servidor de aplicaciones: Compartir programas entre usuarios y grupos de usuarios.
- Servidor de impresión: Compartir impresoras.
- Servidor de correo: Enviar y recibir mensajes.

Todo esto por supuesto, con las restricciones de seguridad y permisos correspondientes.

4. REQUERIMIENTOS DE UN SERVIDOR

Un servidor es un ordenador con una configuración de hardware y software ajustada a la función que debe llevar a cabo. Las características más o menos especiales con que debe contar este ordenador especial son:

- **RAM**: Es fundamental una gran cantidad de RAM ya que se realizan multitud de peticiones de diferentes usuarios simultáneamente y si se trata del servidor de base de datos, la cuestión es entonces mucho más crítica.
- **CPU**: En contra de lo que pudiera parecer no se requiere una CPU especial, ni siquiera una CPU multiprocesador.
- **Caja con fuente de alimentación**: Es recomendable una caja grande, bien aireada con una fuente de alimentación si es posible sobredimensionada, para que o bien el exceso de temperatura no disminuya la frecuencia de trabajo en los servidores que lo soporten o, lo que es peor, no se quemen en los servidores que no soporten dicha disminución.
- **Placa base**: Debe ser de buena calidad para no disminuir el rendimiento general del servidor.
- **Placa de comunicaciones**: Determina la capacidad de transmitir información a la red del servidor, por lo cual es fundamental una placa 10/100 de par trenzado unida a un concentrador o conmutador de 100 Mb y si se cuenta con tecnología superior como la fibra óptica, mejor.
- **Discos**: Pueden ser IDE o SCSI como en los ordenadores de sobremesa. Los IDE presentan el inconveniente que solo se suelen soportar 4 discos (2 por cada bus IDE) y son muy lentos, como mucho 66 Mb/s. En cambio aunque los discos SCSI son más caros, se controlan hasta 8 discos por controladora, y su velocidad es de 320 Mb/s.

5. DISCOS DUROS

Es fundamental realizar una buena gestión de particiones en los discos duros. Debemos particionar porque esto hace que un mismo disco físico tenga x particiones lógicas que son independientes y aunque una partición falle, el resto sigue siendo completamente accesible. Las particiones habituales son:

- **Sistema**: Es necesaria para poner en marcha al servidor y cuenta con el sistema operativo.
- **Usuarios**: Carpetas de usuarios y carpetas de grupos de usuarios.
- **Datos**: Hay directorios con datos de programas que deben ser instalados localmente en los terminales de trabajo.
- **Aplicaciones básicas**: Que todos suelen utilizar, el software base de los usuarios.

- **Aplicaciones**: No son las básicas es decir, no todos los usuarios las utilizan y por ello determinados usuarios tienen acceso a ellas y, probablemente, no a todas.
- **Gestión Informática**: Aquí se suelen instalar los programas y archivos de instalación al que solo tienen acceso los informáticos para instalar programas en cualquier Terminal sin tener que cargar siquiera con un disquete.

Las **extensiones de los discos en el servidor** se llevan a cabo para mejorar su capacidad y rendimiento:

- **Multivolumen**: Podemos unir dos discos de inferior capacidad para crear lógicamente un único disco con la suma de las dos capacidades, la principal ventaja es obtener una partición de la medida que se desee a partir de discos de menor capacidad, pero por desgracia, si un disco físico falla, no se puede acceder a ninguna de las particiones físicas que conforman un mismo volumen. Debido al actual precio de los discos duros (muy baratos) no se suele utilizar este sistema.
- **Espejo**: Si la información es primordial se coloca un disco extra por cada disco duro del servidor, de manera que cualquier cosa que se escriba en el disco 1, se escribe y actualiza también en el disco 2. Tenemos dos discos "fotocopiados", de forma que si uno falla, el otro sigue dando servicio hasta que en caliente, cambiamos el estropeado. El espejo puede ser mediante software (más lento) o hardware.
- **RAID**: El espejo es una opción costosa que solo se puede aplicar a un disco, si necesitamos un espejo para cada disco, el coste se dispara, la técnica RAID distribuye la información entre distintas unidades y ofrece un sistema de redundancia para aumentar la seguridad. Así podemos disponer de 5 discos funcionando y solo uno de ellos ofrecer la redundancia para poder recuperar datos. Hay varios niveles de RAID:
    - RAID 0: La información se distribuye entre distintos discos pero no hay redundancia, así que si algo falla no podemos recuperar la información.
    - RAID 1: Cada unidad está duplicada con otra de soporte, es similar al espejo pero la información se distribuye entre los discos.
    - RAID 2: No se emplea.
    - RAID 3: Datos distribuidos con relación al bit en todas las unidades menos en una que ofrece la paridad.
    - RAID 4: Igual que RAID 3 pero a nivel de sector, lo que mejora los tiempos de acceso.
    - RAID 5: Se escribe en todos los sectores de cada unidad y se añaden códigos correctores en cada sector, con tiempos de acceso en la lectura muy buenos.

El **sistema de ficheros** es otro aspecto muy importante a tener en cuenta. Hay varios sistemas, que de más antiguos a más modernos son:

- **FAT**: Es muy antiguo y solo soporta medidas de 2 GB. sin ofrecer además ninguna seguridad.
- **FAT32**: Igual al anterior pero soportando mayores dimensiones aunque también sin ofrecer ninguna medida de seguridad.
- **NTFS**: Introducido por Windows NT ofrece un tamaño del sector y clústeres muy pequeños por lo que se aprovecha mejor el disco, cuenta con seguridad para el sistema de ficheros.
- **UFS y EXT2**: Se utilizan en Unix y Linux con mucha seguridad.
- **HSFS**: High Sierra File SYstem utilizado en el formato de los CD-Rom y comúnmente aceptado.

6. DISPOSITIVOS DE COPIA DE SEGURIDAD

- **Cintas**: Hay varios tipos: las cintas **DAT** suelen ser dispositivos SCSI con capacidades de 20 Gb, por cinta; las cintas **DLT** suelen llegar hasta 100 Gb. y las **AIT** también. Otro tipo son las **LTO**.
- **Librerías de copia**: Con estos tamaños por cinta, en una gran organización con 20 Gb. de copia de seguridad no hacemos nada. Para evitar este problema existen "robots" motorizados y controlados por software que pueden controlar entre 20 y 2000 de estas cintas, con lo que tenemos asegurada una buena cantidad de información, unos 400 Terabytes.
- **Grabadoras Cd-Rom y DVD**: Los Cd con capacidades de hasta 700 Mb, grabables y/o regrabables al igual que los DVD con capacidades de hasta 8,5 Gb. son adecuados para copias de seguridad de poca cantidad, dado que el precio tanto del dispositivo como de los fungibles, es mínimo.
- **Unidades ZIP/Jazz**: Actualmente en desuso, son unidades de "disquete" con un tamaño igual a éstos pero con capacidades de hasta 250 Mb. que lo hacen insuficiente para una mínima copia de seguridad.
- **Disco duro**: Dado el precio actual de estos dispositivos no es descartable hacer una copia de seguridad sobre ellos mismos, dado que además necesitan muy poco tiempo para efectuarla y así no colapsan el sistema.

Librerías de Copia

7. COPIAS DE SEGURIDAD

Las copias de seguridad son imprescindibles para proteger la información de los usuarios frente a ellos mismos (borrados accidentales), frente a desastres naturales, frente a ataques de terceros, frente al propio sistema que puede dejar en un momento dado por malfuncionamiento la información inconsistente y además porque posibilita el traspaso de información cuando se actualiza o reinstala el sistema.

Tipos de copia de seguridad

La **copia de seguridad completa** es aquella en la que se hace una imagen del disco duro completo o una copia completa del sistema de ficheros. En el primer tipo de copia al restaurar ésta no puede ser selectiva, restaura toda la imagen del disco duro, en el segundo tipo sí podemos seleccionar los archivos y directorios a restaurar.

La **copia de seguridad incremental** guarda sólo los ficheros que se han modificado desde la última actualización. Esto hace que el copiado sea mucho más rápido, consuma menos recursos y tiempos del sistema.

La **copia de seguridad selectiva** solo copia ficheros y/o directorios determinados, generalmente los de más uso y cuya información cambia con más frecuencia.

Políticas de copia de seguridad

Es necesario analizar el tipo y cantidad de información y la organización en que nos movemos para llevar a cabo una adecuada política de copias de seguridad. Si optamos por un tipo de copia de seguridad completa diariamente nos aseguraremos que tenemos siempre toda la información disponible. Cada día en discos distintos se efectúa dicha copia de seguridad y guardamos la última copia del mes, el resto de cintas volvemos a utilizarlas en el mes siguiente; pero es un gran gasto en recursos y tiempo del sistema.

Si hacemos una copia de seguridad completa los Lunes y de Martes a Jueves una incremental consumimos menos recursos y es más rápido pero con la

desventaja de que si una copia de un día no funciona (por ejemplo la del Miércoles), el resto de cintas hasta la siguiente copia completa queda inservible aunque funciona correctamente (por ejemplo las del Jueves y Viernes).

Otro problema importante es saber **dónde guardar las copias de seguridad**, en muchas ocasiones se almacenan cerca del servidor o en la misma habitación; esto tiene su lógica dado que así se puede restaurar o solventar un problema con rapidez, pero si existe un desastre natural o un incendio perderemos toda la información. Tampoco el hecho de que estén bajo llave o en una caja fuerte nos solventa el problema, en un incendio las altas temperaturas destruyen los datos aunque estén en una caja fuerte; y el pensar que como todos los datos están en papel se pueden volver a introducir es un error, dado que actualmente muchos formularios y datos no se pasan a papel.

Por tanto hay que guardar una copia de seguridad alejada del servidor y actualizada frecuentemente para evitar males mayores, incluso se dice que debe estar a varios cientos de kilómetros (en otra placa tectónica diferente) para evitar el riesgo de destrucción por terremotos.

8. IMPRESORAS

Existen dos tipos de impresoras habitualmente: las **impresoras láser** que son caras, con una alta duración del cartucho, rápidas y versátiles; y las **impresoras de chorro de tinta** habitualmente de uso personal por ser de coste bajo, con baja duración de los cartuchos, en color habitualmente y de muy baja velocidad.

Aunque informáticamente lo que más nos interesa es la posibilidad de compartir impresora. En algunos casos las impresoras se comparten mediante una cola de impresión por software y un dispositivo que la conecta a la red de la empresa; en otros casos, la impresora ya tiene un puerto de red, que le asigna una IP dentro de la red interna de la empresa y hace que se comparta con total facilidad y transparencia.

9. LA CORRIENTE ELÉCTRICA

Si todos nuestros equipos dependen de la corriente eléctrica para funcionar, ¿porqué le damos tan poca importancia?, es decir, una vez que hemos conectado un aparato a la red eléctrica, ya pensamos que va a recibir corriente de manera constante, normalizada y fluida durante toda su vida útil, y esto no es cierto, ya que pueden haber picos de tensión (ruidos) e incluso cortes del fluido eléctrico. Las consecuencias de esto pueden ser pérdida o corrupción de los datos, daños directos en el equipo o un acortamiento de la vida útil de los mismos.

Sería conveniente tener en cuenta dos aspectos: la toma de tierra y los SAI. La **toma de tierra** debe realizarse con un supresor de picos situado justo antes del panel eléctrico de la oficina y unos estabilizadores situados justo antes de la conexión a la red de los servidores y/o los terminales individuales. Por otro lado, contar con **SAI** (Sistema de Alimentación Ininterrumpida) también nos protege frente a cortes de corriente y problemas con la tensión, permitiendo que los equipos se apaguen correctamente cuando hay un corte de fluido. Actualmente estos SAIs disponen de un puerto USB que informan al equipo del tiempo que les queda con la batería una vez que se ha ido la corriente eléctrica.

10. SEGURIDAD DE LOS SERVIDORES

La seguridad hay que contemplarla a dos niveles: seguridad física y seguridad de software. La **seguridad física** requiere de algunas precauciones:

- Cerrar el recinto donde está el servidor y no trabaja nadie, y bloquear el sistema mediante salvapantallas con contraseña.

- Fijar físicamente el equipo con cadenas para evitar robos.
- Evitar que el ordenador arranque desde disquete o, incluso, retirar este dispositivo si realmente no lo usamos.
- Colocar contraseñas de encendido en la BIOS del sistema.

En la **seguridad por software**:

- Contar con una buena política de cambio periódico de contraseñas, especialmente en aquellos usuarios que tengan privilegios especiales.
- Asimismo, estas cuentas especiales no deben tener nombres esperados, como administrador o admin.
- No instalar ni ejecutar software en el servidor por el peligro de virus que entraña.
- Contar con una buena política de usuarios y grupos con privilegios bien definidos.

11. EJEMPLO: SISTEMAS OPERATIVOS ACTUALES

Dos son los principales sistemas operativos que se utilizan: Windows y Unis/Linux. Ambos pueden realizar las mismas funciones, como veremos a continuación, a partir de sí mismos o de software de terceros:

- Ficheros: Ambos sistemas sirven ficheros sin ninguna dificultad, y además comparten recursos también sin problemas
- Web: Windows tiene el IIS (Internet Information Server) que es un servicio que se puede arrancar o no, mientras U/L necesita instalar un software como Apache, que es potente y gratuito.
- FTP y Correo: El FTP en un servicio en Windows que debe ser arrancado y configurado, y en el correo requiere el Microsoft Exchange Server; en U/L en cambio ya está preparado para trabajar.
- Ofimática: Windows parece más universal con su paquete Office; U/L cuenta con OpenOffice que es muy compatible.
- Seguridad: No hay acuerdo sobre qué sistema operativo es más seguro.
- Conexión entre ordenadores: generalmente para aprovechar CPU, Windows no puede, U/L es intrínseco al sistema operativo por lo que puede.
- Entornos gráficos: Windows cuenta con uno, U/L con cientos.

12. ASPECTOS LEGALES y TAREAS/RESPONSABILIDADES

El administrador de sistema operativo y redes puede llegar a hacer cosas, sin saber, que están fuera de la legalidad, como abrir simplemente un archivo o directorio de la carpeta personal de un trabajador. Actualmente existen colegios profesionales para dar apoyo legal e información a los informáticos en estos aspectos.

Son tareas del administrador:

- Velar por el buen funcionamiento de los servidores: es decir cuidar la protección física de los mismos, velar por unos tiempos de respuesta y recursos correctos, mantener el sistema operativo actualizado así como el software que le es asignado.
- Garantizar la información que contienen los servidores: hacer copias de seguridad siguiendo la política que se haya adoptado.
- Configurar adecuadamente todo el hardware del sistema.

TEMA 3 ADMINISTRACIÓN DE USUARIOS

1. DISEÑO DEL ENTORNO DE USUARIOS

Diseñar el entorno de los usuarios significa preparar todo aquello con lo que se encontrará el usuario cuando utilice el sistema informático de la organización. La idea es que debe resultar fácil e intuitivo para el usuario, proporcionar un entorno homogéneo (si el usuario cambiar de Terminal, no le debe resultar extraño), el sistema debe ser rápido de respuesta de los servidores y en la red, debe aportar un buen nivel de seguridad y además debe ser fácil de administrar (fácil de actualizar, de reinstalar, de reconfigurar, fácil en las copias de seguridad…). Todo esto supone una contradicción informática, dado que la seguridad acostumbra a estar reñida con la comodidad y la velocidad.

Las **necesidades de los usuarios** generalmente son:

- Un Terminal de trabajo.
- Un lugar donde se pueda imprimir.
- Espacio para guardar la información.
- Software para trabajar: que dividiremos en Software de base (sistema operativo y aplicaciones básicas de comunicaciones en los servidores), software de ofimática, software de comunicaciones y aplicaciones específicas como control de producción, nóminas, etc.

A partir de todas estas necesidades, podemos elaborar tres **diseños informáticos** distintos, con sus pros y sus contras:

- **Primer diseño**: Todos los usuarios ven todos los programas y todas las aplicaciones, con permisos de lectura y ejecución para todo. Las aplicaciones específicas que ya contaban con permisos de acceso propios, quedan controladas por las propias aplicaciones, y en las carpetas de usuario solo puede entrar el propio usuario. Las ventajas de este sistema es que es muy fácil de administrar, es fácil preparar un Terminal modelo, una vez clonado un equipo casi no existe ajuste final, el cambio de puesto de trabajo de un usuario no implica modificar en nada su perfil. Lo negativo, en cambio, es que la idea de grupo de trabajo no existe, por lo que compartir información con un grupo de personas no es posible; de hecho si un usuario quiere compartir la información de su carpeta personal, estará disponible para toda la organización. Además el usuario puede perderse ante tanto software disponible no sabiendo el que tiene que utilizar para trabajar y el que no.

- **Segundo diseño**: Los usuario se agrupan de manera natural en grupos de trabajo, de manera que un usuario pertenece a un grupo y sólo a uno; una aplicación o programa puede funcionar para todo el mundo o sólo para un grupo; al igual que antes las aplicaciones específicas siguen controlando sus permisos de acceso; a las carpetas de usuario sólo puede entrar el usuario con permisos de lectura, escritura y ejecución. Las ventajas de este diseño es que crear un usuario implica tener en cuenta a qué grupo deberá pertenecer. El usuario puede acceder a la información personal y a la del grupo por lo que la protección de la información está más asegurada; no se pueden producir manipulaciones incorrectas del software (ni se lía el propio usuario) ya que solo aparece el software que se debe utilizar por cada grupo. Se puede compartir información con el grupo de trabajo no siendo accesible para el resto de usuarios. Lo malo de este diseño es que modificar el esquema de trabajo puede llevar a una reorganización completa de permisos de grupos; el cambio de puesto de una persona implica modificar el perfil (en caso de que cambie de grupo); compartir información entre grupos sigue siendo complejo.

- **Tercer diseño**: Los usuarios, como antes, se agrupan pero un usuario puede pertenecer a un grupo o a más; una aplicación puede funcionar para todos los usuarios, o para uno o más grupos; las aplicaciones específicas, como siempre, siguen controlando el acceso propio. Las ventajas de poder pertenecer a más de un grupo son varias: Ahora sí que existe una verdadera idea de grupo de trabajo, se simplifica la administración, se puede compartir información sensible entre grupos de trabajo distintos, etc. Lo negativo, como en el segundo diseño, al crear un usuario debemos saber a qué grupo o grupos pertenece; el cambio en el puesto de trabajo de un usuario implica modificar el perfil…

Para poder decidirse por cualquiera de estos diseños hay que elaborar la **tabla de aplicaciones**. Es una tabla donde en la primera columna aparecen las aplicaciones existentes, en segundo lugar si se ejecutan en local (el propio Terminal) o en remoto (el servidor, lo cual aumenta la carga de trabajo para éste y el flujo de la red), si la información se almacena en local o en el servidor y los permisos que se les da a los distintos grupos de trabajo.

Tabla del Terminal
Tabla del Servidor

	Aplicación		Información		Grupo	Grupo	Grupo
	Local	Remoto	Local	Remoto			
Aplicación							
Aplicación					Permiso		

	Aplicación		Información		Médicos	Administración
	Local	Remoto	Local	Remoto		
Contabilidad	•			•		L/E
Facturación	•			•		L/E
Visitas		•		•	L/E	L/E
Recetas	•		•		L/E	L/E

En la figura lateral podemos observar esta primera tabla. La tabla inferior muestra los mismos datos, pero aplicándolos no ya a un Terminal, sino al servidor; lógicamente el diseño de los terminales va indisolublemente unido al diseño del servidor.

Por último, es fundamental el **sistema operativo del Terminal de trabajo**, el cual en los últimos tiempos es un sistema operativo de red con interfaz gráfica que facilite el uso del mismo. Su sencillez y flexibilidad de uso hace que sea inversamente fácil de administrar, es decir es difícil de instalar, configurar, y muy fácil de desconfigurar por manos inexpertas.

2. DISEÑO EN LOS SERVIDORES

Como indicábamos anteriormente, el diseño de los terminales de trabajo lleva emparejado el diseño del servidor o servidores. Para hacerlo adecuadamente y que no tengamos que llevar a cabo cambios de última hora que afecten tanto a los servidores como a todos y cada uno de los terminales, debemos elaborar escrupulosamente la tabla del servidor, para conocer qué aplicaciones se instalarán en él, saber donde se ubicará la información de los distintos programas y con todo ello prever las necesidades de disco y las particiones que debemos realizar.

Respecto a las **particiones** sabemos que son 4: de sistema, de usuarios, de aplicaciones y de datos; aunque también hay que decir que a poco que la organización sea medianamente grande, en lugar de particiones deberemos hablar de discos duros para cada una de estas 4 actividades

La **saturación de la red** es otro aspecto importante a tener en cuenta. Si las peticiones de los usuarios son tantas que el sistema se vuelve lento e inestable, habrá que repartir la carga de trabajo mediante diversos sistemas: usar tecnología SCSI (la más rápida), implementar servidores redundantes o servidores RAID, etc.

3. CONFIGURACIÓN DE TERMINALES DE TRABAJO

Finalmente configuramos los terminales de trabajo. Por una lado podemos decir que cuanto menos software se encuentre en el disco del usuario, menos peligro existe de pérdida de información y de tiempo para recuperar el equipo; pero claro, si todo se encuentra en el servidor, probablemente lo colapsaremos, también

colapsaremos la red, el sistema funcionará muy lentamente y tendremos muchas quejas de los usuarios acerca del rendimiento general del sistema. Obviamente, los inconvenientes superan a las ventajas, por lo que colocaremos todo el software de base, los paquetes de ofimática y el software que utiliza toda la organización en cada uno de los terminales de trabajo.

Bueno, esto tampoco es realmente así, crearemos lo que se llama un **Terminal modelo** con todo el software y la configuración que debe tener, es decir, instalamos el sistema operativo, las aplicaciones, los clientes de las aplicaciones remotas, configuramos todas las opciones del sistema operativo para ajustarlo a las necesidades de la organización y lo probamos durante algún tiempo. Cuando estamos seguros que todo funciona a la perfección y que no debemos aplicar ningún cambio más, creamos una imagen de disco de este Terminal modelo, lo situamos en la partición de administración en el disco duro del servidor, y lo utilizamos para clonarlo tantas veces como terminales debamos configurar.

4. MANTENIMIENTO DE LOS TERMINALES DE TRABAJO

Por mantenimiento de los terminales de trabajo entendemos todas las acciones necesarias para que el equipamiento esté en óptimas condiciones de funcionamiento para el usuario final y distinguimos dos partes: el mantenimiento del equipamiento y las tareas periódicas de mantenimiento.

El **mantenimiento del equipamiento** puede abarcar la sustitución y/o actualización del hardware o software del Terminal de trabajo por varias causas: avería grave de hardware a sustituir, añadir un nuevo elemento de hardware por política de empresa, sustitución completa de un ordenador, reinstalación de software de un equipo por cambio de ubicación y/o funciones del usuario, etc. También puede acontecer la desconfiguración completa del equipo debido a un virus, al propio usuario o a fallos de corriente eléctrica.

Para proceder correctamente con este mantenimiento, es fundamental tener bien preparado y configurado un Terminal modelo y además tener piezas de hardware (sobre todo las más comunes) para reparar sencillas averías.

Cuando se hace necesario extraer datos de un equipo, aunque siempre intentamos que los datos sensibles se encuentren en el servidor, muchas veces hay que recuperar también datos en terminales de trabajo dañados, tenemos dos opciones:

- Mover el disco duro e instalándolo como disco secundario en otro ordenador, y tras extraer los datos, y con el CD de clonación, recuperarlo a su estado habitual, copiando de nuevo los datos en él.
- Utilizar unidades Zip/Jazz para este proceso.

Las **tareas periódicas de mantenimiento** son la segunda parte del mantenimiento de los terminales de trabajo. Son tareas que se deben realizar forzosamente cada cierto tiempo y que son transparentes para el usuario final. Estar tareas pueden ser, entre otras:

- Control para que no se llenen los buzones de correo de los usuarios, esto se hace en el servidor.
- Control para que no se llenen los directorios de los usuarios en el disco compartido, también se hace en el servidor.
- Actualizar el fichero de firmas del software antivirus, para que se actualicen así todos los terminales de trabajo y mantener este problema a raya. Si un usuario cree, a pesar de todo, tener o haber tenido un virus, debe contactar con el administrador de usuarios para explicarle el problema y evitar así una propagación o, lo que es peor, que pueda salir al exterior.
- Control remoto: Es un software que permite desde una estación de trabajo, controlar otra tal como si se encontrase delante de ella y así poder diagnosticar y tratar los posibles problemas del Terminal.

- Documentación y procedimientos: Un procedimiento es una descripción del conjunto de acciones necesarias para realizar una tarea determinada; todos estos procedimientos deben encontrarse documentados en un manual, dado que a menudo intervienen distintos administradores y es conveniente saber qué procesos cambian según qué software en momentos determinados.

5. FORMACIÓN DEL USUARIO

Un aspecto a menudo olvidado por las grandes organizaciones es la formación de los usuarios. Las ventajas son muchas:

- Mejora del uso del software
- Mejora en la eficiencia y satisfacción del personal
- Disminución de incidencias en el dpto. de informática y, por lo tanto, de los costes derivados de ellos.

Además, las desventajas de no llevar a cabo un plan de formación, también son muchas:

- Pérdida de tiempo de los usuarios y errores frecuentes
- Probabilidad de que estos errores provoquen mal funcionamiento del sistema
- Gran parte del volumen de trabajo del dpto. de informática se deberá, sin duda, a consultas de los usuarios que se podrían haber evitado con un buen plan inicial.
- Desconcierto, quejas, sensación de mala instalación o software incorrecto en el usuario.

Generalmente la formación del usuario tendrá 3 planes de formación distintos:

- **Planes de actualización**: Cuando se actualiza software se puede informar en una charla, seminario o cursillo del porqué, como y qué ventajas aportarán estos cambios.
- **Implantación de software nuevo**: Es mucho más compleja que la anterior pues debemos incluir a los usuarios en esta nueva implantación, preguntándoles sus dudas, cómo creen que debe funcionar el programa, pidiendo opiniones, propuestas o quejas. Bien es cierto que daremos una imagen de interés por el usuario pero también es importante hacerles ver que no siempre es posible hacer todo lo que se pide y, por tanto, no se podrán satisfacer todas las peticiones.
- **Usuarios nuevos**: Cursillo con un fuerte componente estándar y una parte más pequeña dedicada a su específico puesto de trabajo.

6. CENTRO DE ATENCIÓN AL USUARIO

Para el usuario el ordenador debe ser una herramienta para aumentar su grado de organización y/o eficiencia y, por ello, no deben conocer necesariamente todos los detalles técnicos del equipamiento que utiliza. Cuando un usuario tiene un problema informático, debe dirigirse a un único lugar para resolverlo, que es el centro de atención al usuario (CAU); este CAU es una sección del departamento de informática que se dedica a gestionar las incidencias de los usuarios, resolverlas y documentarlas para que las soluciones puedan servir para el mismo o parecidos problemas futuros de otros usuarios.

Cuando el usuario contacto con el CAU lo hará con el **personal de atención** (Primer nivel) que no tiene que ser necesariamente un técnico; éste buscará en la base de datos el diagnóstico de los síntomas que el usuario refiera; si lo encuentra y le da la solución, perfecto; en otro caso abrirá una incidencia con toda la información que se encauzará a un **técnico** (segundo nivel) y éste solucionará el problema, documentándolo en la base de datos de primer nivel para futuras consultas.

Además de esto, alguien debe encargarse del control de **incidencias pendientes**, y realizar un seguimiento en los casos de mayor duración, avisando al usuario de los cambios que se van generando para que comprenda que el departamento de informática se preocupa de su problema

También el CAU ejerce de **filtro de peticiones**, pues en algunos casos el usuario exige procedimientos que no se pueden realizar, como puede ser por ejemplo la instalación de un software que se encuentra fuera de la organización.

7. RESPONSABILIDADES DEL ADMINISTRADOR DE USUARIOS

- Configurar los equipos terminales de trabajo.
- Abrir cuentas de usuario, espacio privado y cuentas de correo y mantenerlas para todos los usuarios.
- Facilitar mediante nombre de usuario y contraseña el acceso a aplicaciones corporativas o espacios de trabajo en grupo.
- Realizar copias de seguridad de los datos de los usuarios.
- Mantener y gestionar el hardware de los terminales de trabajo.,
- Gestionar y actualizar el CAU.

8. ASPECTOS LEGALES

Existe actualmente un vacío legal sobre el tratamiento y gestión de la información personal del usuario en los sistemas informáticos. Debemos ser conscientes del momento en que pueda surgir un problema y es entonces cuando necesitaremos un adecuado asesoramiento legal para resolverlo.

TEMA 4 ADMINISTRACIÓN DE LA RED

1. ELEMENTOS Y DISEÑO FÍSICO DE UNA RED

Tema 4
Administración de la red

1. Elementos y diseño físico de una red
2. Protocolos de comunicación
3. Configuración de la red en los ordenadores (cliente/servidor)
4. Seguridad de la red
5. Responsabilidades del administrador

Las redes, por su dispersión se pueden clasificar en:

- LAN: Local area network o redes de área local, de 10 metros a 1 km.
- MAN: Metropolitan area network o redes de area metropolitana: de 1 a 10 kms.
- WAN: Wide are network, más de 10 kms.

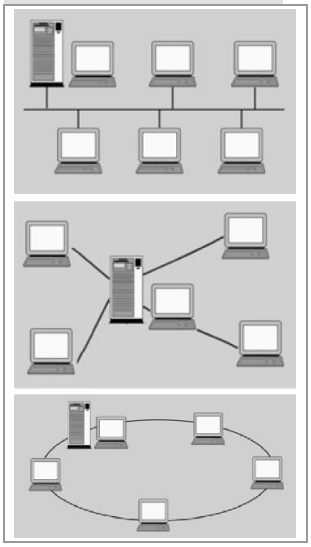
Los **elementos** que encontramos en una red son varios, por un lado tenemos el **cableado** del que existen varios tipos:

- **Par trenzado**: Son diferentes hilos conductores que pueden alcanzar los 100 metros de distancia sin experimentar amortiguamientos de la señal y una velocidad entre 10 y 100 Mbps. A su vez encontramos varios tipos: el STP (shielded twisted pair) son dos pares de hilos conductores recubiertos por una malla. El UTP (unshielded twisted pair) son cables sin apantallas formado por cuatro pares de hilos, que pueden ser de categoría 3 (velocidades de hasta 30 Mbps) o de categoría 5 (hasta 100 Mbps). Éste último es el típico cable que conecta el MODEM o router ADSL con el ordenador.
- **Cable coaxial**: Es un único conductor interno con varias capas de protección, permite velocidades de hasta 20 Mbps en distancias de hasta 2 kms, mientras que en distancia de hasta 100 metros llega los 100 Mpbs. Se reducen con este cable los problemas de amortiguamiento en distancias cortas, pero es muy sensible al ruido producido por aparatos eléctricos. Para conectar diferentes ordenadores a un mismo cable coaxial se utilizan los conectores en T.
- **Fibra óptica**: Permite una gran anchura de banda y puede conseguir velocidades del orden de centenares de Mbps e incluso Gbps. Experimenta una reducción mínima de la señal, es inmune a las interferencias electromagnéticas y resulta difícil de interceptar y espiar.

Los **elementos de interconexión de redes** son:

- **Repetidores**: Son dispositivos no inteligentes que amplifican la señal y evitan los problemas de amortiguamiento.
- **Puente**: llamado bridge, conecta entre sí dos segmentos de red.
- **Router**: Gestiona el tráfico de paquetes que proviene del exterior de la red y se dirige al interior, o al revés. Ofrecen servicios de encaminamiento de los datos que se transmiten.
- **Pasarela**: Actúa en los niveles superiores de la jerarquía de protocolos y permiten la interconexión de redes que utilizan protocolos incompatibles.

Topologías
Bus
En Estrella
En Anillo



Las **tipologías** más habituales en el diseño de redes son:

- **Topología de bus**: En una red en bus todos los nodos se conectan a un cable común, de forma que todos los mensajes llegan a todos los nodos, no hay que encaminar la información, la fiabilidad de la comunicación solo depende del bus (esto es un punto crítico), la configuración es muy flexible y modular siendo de bajo coste (por lo que todavía se utiliza bastante).
- **Topología en anillo**: El cable va de Terminal en Terminal si ningún punto final. Cada nodo amplifica y repite la información que recibe, no es necesario dirigir el encaminamiento de la información y la fiabilidad del anillo depende de cada uno de los nodos, de forma que si un solo Terminal cae, la red entera puede dejar de funcionar.
- **Topología en estrella**: Todos los terminales de trabajo y el servidor se conectan a un único concentrador o conmutador, lo cual se convierte en un punto crítico.

En los últimos años están proliferando las redes sin cable WLAN (Gíreles local area network) que solventa varios problemas como la dificultad de cablear en determinados lugares y facilita el crecimiento posterior de la red. Por el contrario la seguridad es su talón de Aquiles, dado que es muy fácil pasar a la red al no existir cortafuegos y el hardware actual no es demasiado seguro.

2. PROTOCOLOS DE COMUNICACIÓN

- **NetBIOS/NetBEUI**: Fue desarrollado por IBM y lo utilizan Windows 98 y NT.
- **IPX/SPX**: Desarrollado por Novell y utilizado por el sistema operativo de red NetWare.
- **TCP/IP**: Son un conjunto de protocolos que permiten compartir recursos de ordenadores de una red, desarrollado en 1972 por el departamento de defensa de los Estados Unidos, se caracteriza por enviar datagramas segmentados que son recibidos, recuperados y reorganizados (dado que no se tienen que recibir en orden cronológico) en el ordenador de destino. Existen interesantes comandos del protocolo TCP/IP que nos interesa conocer:
    - **ARP**: Addres resolution protocol, muestra las tablas de mapeo de las direcciones IP.
    - **IPCONFIG**: Configuración IP.
    - **NETSTAT**: Estadísticas de protocolo y conexiones actuales.
    - **PING**: Envía datagramas a una máquina de destino y mide el tiempo de respuesta, de este modo podemos saber si la máquina destino funciona o no.
    - **TRACERT**: Muestra el camino que conduce a un destino determinado.

3. CONFIGURACIÓN DE LA RED EN LOS ORDENADORES CLIENTE/SERVIDOR

Para **configurar los terminales de trabajo** en la red, los pasos que debemos seguir son los siguientes:

- Instalación y configuración de los controladores de la tarjeta de red, es decir, instalar los drivers de las tarjetas Ethernet.

- Selección y configuración del protocolo de comunicación: puede ser Novell, Apple talk o, lo más frecuente TCP/IP. En este último caso debemos configurar por este orden:

    - Dirección IP y máscara de subred: Reconoce la máquina de entre todas las que se hallan conectadas a la misma red. Suele tener las 3 primeras cifras iguales y la última permite tener hasta 254 direcciones o máquinas en la subred.
    - Configuración DNS: Permite que la traducción de nombres de direcciones IP (por ejemplo www.uoc.edu) sea traducida a su dirección real.
    - Puerta de enlace: Se introduce la dirección IP de los routers que permiten la salida al exterior, para poder tener Internet por ejemplo.

- Instalación y configuración de los clientes, para establecer un dominio de trabajo.

- Otros aspectos configurables: control de accesos, compartición de ficheros, carpetas e impresoras.

4. SEGURIDAD DE LA RED

Una red es un conglomerado de muchos elementos heterogéneos, y debemos cuidar especialmente los siguientes aspectos:

- **Sistema de ficheros**: Sólo deben acceder los usuarios autorizados.
- **Código malicioso**: Vigilar que especialmente virus y troyanos no infecten programas "autorizados".
- **Autenticación de usuarios**: Proceso de verificación de la identidad de una persona en el momento de acceder a un recurso.
- **Criptografía**: Permite la confidencialidad de la información que viaja por la red.
- **Herramientas de seguridad**: Existen herramientas para comprobar distintos aspectos de la red, y deben ser utilizadas.
- **Monitorización del sistema**: Una vez montada la red hay que vigilar que se mantienenlos parámetros de velocidad, comodidad y seguridad adecuados.

5. RESPONSABILIDADES DEL ADMINISTRADOR

Es evidente que las responsabilidades del administrador de la red son varias: velar por el funcionamiento correcto, garantizar un tiempo de respuesta que se encuentre entre los márgenes establecidos, controlar la seguridad, actualizar el sistema operativo de los servidores, gestionar y controlar las impresoras de la red y los servicios propios de la misma.

También es importante la adquisición de licencias para software de red, pues el uso de licencias monousuarios en red pueden conllevar sanciones posteriores.

TEMA 5 ADMINISTRACIÓN DE LOS DATOS

1. LOS DATOS Y LA ORGANIZACIÓN

La organización crea datos constantemente, pero un "gran depósito" de datos en bruto no es útil, porque si no existe coherencia no tiene ningún tipo de sentido. Los datos son los registros de los sucesos y lo que realmente nos interesa es la información: el procesamiento de estos datos para que tengan sentido; aunque en nuestra vida diaria usamos los dos conceptos como si fueran el mismo.

Generalmente, se guardan datos y se presenta al usuario información, es decir, el procesamiento de estos datos para que tenga sentido, en el dispositivo de salida. El gran problema es que el software puede guardar los datos en formatos diferentes, en sitios distintos y además siendo incompatible con otros programas.

El **sistema informático** pretende guardar la información de la organización para que sea fácil recuperarla posteriormente, manipularla y presentarla al usuario.

2. DÓNDE ESTÁ LA INFORMACIÓN

Ya apuntábamos anteriormente los principales problemas con los datos: están guardados en ficheros, con formatos determinados, no siempre en el sitio donde se necesitan y probablemente incompatibles entre sí.

Así, en la estructura de la red pueden existir datos dispersos en diferentes particiones y carpetas del servidor y de cualquiera de los terminales de trabajo, por no comentar los portátiles, que deben aparecer como dispositivos dentro y fuera de la organización, sacando datos al exterior y a veces conectándose y sincronizando los datos generados.

Varias soluciones podemos poner en marcha para intentar paliar todos estos problemas:

- A partir de la tabla de aplicaciones y del diseño de los usuarios podemos saber dónde se guarda la información.
- A partir de la misma tabla sabemos qué software genera información local que debe ser guardada en las copias de seguridad diarias.
- La información no controlable generada con software comercial debe guardarse por defecto en la unidad de red privada y no en el disco duro del Terminal individual.

3. LA CONSULTA DE LA INFORMACIÓN

Igual que los usuarios generan datos constantemente, también necesitan poder consultarlos (para, a su vez, generar más datos).

Ya que la seguridad de toda la información de la organización es responsabilidad del administrador, éste debe conocer la localización de los datos, disponer de un método de restauración en caso de problemas y tener una idea general del contenido.

Cuando conseguimos que todos los datos estén en los servidores podemos hacer que diferentes grupos/usuarios accedan a los mismos modificándolos o actualizándolos, de forma que no se dupliquen los mismos; además, sin duda alguna la seguridad es mucho más alta.

Ahora bien, para manipular toda esa información que se encuentra en los servidores, se "inventaron" los **servidores de bases de datos**, que intentan integrar en un único punto toda la información, así es más rápido, seguro, fácil de usar, sencillo de ampliar, accesible para copias de seguridad, toda la información aunque pueda entrar en formatos heterogéneos se encuentra en un formato homogéneo, facilita las consultas de la dirección, etc. Entre estos sistemas comerciales encontramos Microsoft Access que se usa solo en sobremesa, SQL Server es su hermano mayor que acepta mayor cantidad de datos y consultas, Informix y Oracle que también son realmente potentes.

Actualmente todavía se ha llevado mucho más allá la idea de los servidores de bases de datos, mediante los **ERP**. Un ERP es un conjunto de módulos o paquetes perfectamente integrados que circulan sobre un servidor de bases de datos, de manera que todas las aplicaciones que el usuario requiera ya se encuentren instaladas y homogeneizadas. Un ejemplo de ello es **SAP/R3**, donde los sistemas de nóminas, facturas, ventas, etc, se encuentran en una plataforma homogénea; en un sistema además que intenta adaptarse a las características de la empresa, pero que claro, también hace que los usuarios tengan que amoldarse al nuevo sistema. Además adquirir un SAP implica adquirir un servicio, de manera que cambios de moneda, cambios en el IRPF, etc, se mantiene constantemente actualizado.

4. PROTECCIÓN DE LA INFORMACIÓN

La información es uno de los bienes más valiosos de la organización. Se debe invertir una parte importante de los esfuerzos en salvaguardarla. La seguridad ya la hemos tratado en el apartado anterior, pero por otro lado, las copias de seguridad se realizarán de forma más segura y completa si las aplicaciones guardan la información por defecto en los espacios personales de red o en el servidor, no en el Terminal de cada usuario; y se le explica a los usuarios el uso que deben hacer de su espacio personal de red para salvaguardar su información.

En cuanto a las **copias de seguridad** estudiaremos brevemente las que se pueden realizar con el backup recovery de Oracle. Pueden ser copias lógicas o físicas. Las copias lógicas son breves en el tiempo pero su restauración puede ser muy laboriosa, incluso de días. Este sistema funciona bien como complemento al sistema de copias físico, por si se estropea alguna tabla, ya que se puede importar ésta únicamente sin importar el resto. Por otro lado las copias físicas son el sistema por excelencia en oracle, dado que con un archiveLog activado se puede recuperar el sistema hasta un segundo antes de la caída, eso sí siempre que el log esté activado.

5. RESPONSABILIDADES DEL ADMINISTRADOR

- Velar para que los datos se almacenen en los servidores
- Mantener en buen funcionamiento las bases de datos
- Diseñar y llevar a cabo una adecuada política de copias de seguridad.
- Evitar en lo posible la duplicación de información.
- Saber donde se encuentran todos los datos sensibles de la organización.

TEMA 6 ADMINISTRACIÓN DE LA WEB

1. LOS SERVIDORES WEB Y LA ORGANIZACIÓN

Normalmente, cuando el servidor web se utiliza como parte de una aplicación, solamente ejerce de interfaz para la aplicación, de forma que es un elemento más. Es un medio, eso sí muy flexible, para hacer funcionar la aplicación.

El servidor web también puede funcionar como servidor de páginas, tanto para la intranet como para Internet; en este último caso hay que ser muy cuidadoso con los datos y la estética común pues muestra la imagen corporativa de la organización a la comunidad Internet, es decir, a todo el mundo.

2. EL ADMINISTRADOR Y EL SERVIDOR

El binomio administrador-servidor debe coordinarse perfectamente para obtener el mejor rendimiento posible. Un servidor web se compone de un núcleo que es el centro del servidor web y de módulos que aumentan la funcionalidad del mismo. Instalar un servidor web no plantea muchos problemas dado que es un proceso bastante automatizado y que proporciona herramientas de control que nos pueden servir para monitorizar y analizar el rendimiento. Hay que ser muy estricto en la organización y estructura de directorios y páginas para saber en todo momento donde se encuentran o pueden encontrar determinadas páginas y así poder obrar en consecuencia al realizar la copia de seguridad; pero eso sí, el administrador instala y cuida la web, pero no el contenido.

Para el administrador web existen dos tipos de usuarios: el consumidor del material de la web, y el creador el mismo; el administrador debe promover la utilización de los recursos de la web entre los creadores de páginas, les debe proporcionar los recursos y conocimientos necesarios para que puedan crear páginas web y colgarlas en el servidor.

3. RECURSOS PARA CREAR PÁGINAS WEB

- **HTML**: Es el lenguaje por excelencia y que interpretan todos los navegadores, basado en marcas actualmente está algo anticuado por la imposibilidad de construir páginas dinámicas, pero aun así es fundamental conocerlo para cualquier administrador web.
- **XML**: Intentado poseer un lenguaje de marcas único, es un estándar ajustado a las necesidades de Internet. Al ser incompatible con el HTML, se creó otro lenguaje intermedio y compatible el XHTML.
- **CSS**: Para que todas las páginas tuvieran un mismo estilo e imagen corporativa: color de texto, fuentes, etc. se crearon las Cascade Style Sheet u hojas de estilo en cascada; de esta forma se definen todos estos parámetros de estilo en un único punto y automáticamente se aplican a todas las páginas de un sitio web, sin necesidad de ir cambiando estos parámetros en todas ellas.
- **JavaScript**: Es un código de ejecución insertado dentro de la página HTML que se ejecuta en el cliente y que dota de cierto dinamismo la página web.
- **CGI**: Common Gateway Interface fue el primer intento de acceder a bases de datos a través de páginas web, el problema es que consume demasiados recursos en el servidor.
- **Perl**: Practical Extraction and Report Language, permite así mismo ejecutar código en el servidor.
- **Java**: Son programas que se copian del servidor al cliente y es en éste último donde se ejecutan con fuertes restricciones de seguridad. La independencia de plataforma y de sistema operativo es uno de los puntos clave de su éxito.

- **Servlets (JDBC)**: Son programas que se ejecutan en un servidor web y construyen una página web, con la ventaja sobre el CGI de que consumen menos recursos pues se ejecutan como hilos de ejecución y no como procesos.
- **ESL**: Embedded Scripting Language, es una programación como JavaScript pero se trata de un elenguaje completo que se ejecuta en el servidor.
- **PHP**: Hypertext preporcessor, el servidor interpreta las páginas PHP y las convierte en HTML antes de enviárselas al cliente. Es el lenguaje por excelencia de las páginas dinámicas.
- **ASP**: Active Server Page, Servidor de páginas activo, es una DLL de Microsoft que debe correr en servidor Windows y proporciona prácticamente, los mismos elementos que PHP pero con el inconveniente que no es código libre, sino propiedad de Microsoft.
- **JSP**: Servidor de páginas Java, nos permite mezclar HTML estático con dinámico.

4. EJEMPLOS DE SERVIDORES

- **Apache Server**: Es gratuito en la página www.apache.org. Corre sobre plataforma Linux aunque hay versiones Windows, es código libre y es un servidor francamente potente.
- **Internet Information Server (IIS)**: Es el servidor web de Microsoft.
- **Netscape SuiteSpot**: Fue gratuito hasta determinada versión.

En general todos estos servidores son sencillos de instalar y llevan herramientas para monitorizar y controlar la seguridad, además de soportar sin problemas un número elevado de accesos concurrentes.

5. SEGURIDAD

Hay que vigilar distintos aspectos:

- Seguridad de publicación: para evitar que se puedan publicar por error, datos internos de la organización.
- Seguridad del software: la cantidad de información a la que pueden acceder los servidores les hace especialmente interesantes para ser atacados.
- Protocolos de comunicación cifrados: Los famosos HTTPS son los protocolos más extendidos para comunicación cifrada por Internet, se basan en el estándar SSL y la escucha se realizar por el puerto 443 y no por el habitual 80.
- Registro de las conexiones: Con poco trabajo añadido los servidores web pueden registrar las direcciones DNS, fecha y hora, páginas y tiempo de conexión que ha tenido un determinado usuario.
- Copias de seguridad: El servidor web tiene pocos ficheros de configuración, pero por su importancia y la imagen que puede dar dentro y fuera de la organización es indispensable volver a restaurarlo rápidamente en caso de fallo.
- Virus: Dado que un servidor web está constantemente distribuyendo documentos a clientes y proporcionando ficheros puede ser una fuente importante de infección dentro y fuera de la organización.
- Bases de datos: para acceder a bases de datos, lo usual es situar un cortafuegos entre la web y el servidor de aplicaciones, además se sitúan en máquinas separadas para que si se cuelga el servidor de aplicaciones no afecte al servidor web.

6. ASPECTOS LEGALES

Aunque el administrador web no se encargue de los contenidos, sí debe vigilarlos, dado que la aparición de imágenes, música, etc que han podido subir los

administradores de contenidos pueden tener derechos de copyright. Cualquier creación o producto de la creatividad humana se intenta proteger mediante la propiedad intelectual, y el caso del ciberespacio no es ninguna excepción.

7. RESPONSABILIDADES DEL ADMINISTRADOR

- Hacer que la web se mantenga siempre activa, con un tiempo de respuesta dentro de los márgenes aceptados, controlando su seguridad y las estadísticas que genera.
- Hacer que la web resulte homogénea y prepara la formación de las personas que deben mantener los contenidos, aunque nos debemos responsabilizar sólo parcialmente de los mismos.

TEMA 7 ADMINISTRACIÓN DE LA SEGURIDAD

1. SEGURIDAD INFORMÁTICA

Dado que es completamente imposible garantizar la seguridad e inviolabilidad absoluta de un sistema informático, en lugar del inalcanzable concepto de seguridad, será preferible utilizar el término fiabilidad. Diremos que un sistema informático es fiable cuando cumpla las tres propiedades siguientes:

- **Confidencialidad**: Sólo pueden acceder a los recursos los elementos autorizados a hacerlo.
- **Integridad**: Los recursos del sistema sólo pueden ser modificados o alterados por los elementos autorizados a hacerlo.
- **Disponibilidad**: Los recursos del sistema permanecen accesibles a los elementos autorizados.

Los **tipos de ataque** que puede sufrir el hardware y el software pueden ser:

- **Interrupción**: Es un ataque contra la disponibilidad, de forma que se destruye o queda no disponible un recurso del sistema.
- **Intercepción**: Es un ataque contra la confidencialidad, donde un elemento no autorizado consigue el acceso a un recurso, como puede ser interceptar un correo electrónico dirigido a otra persona.
- **Modificación**: Es un ataque contra la integridad, pues además de conseguir el acceso no autorizado al recurso, se modifica, borra o altera de cualquier forma.
- **Fabricación**: Es un ataque contra la integridad, pues se inserta o crea un objeto falsificado en el sistema, por ejemplo un usuario nuevo con su contraseña de acceso.

La mayor parte de los ataques **provienen de personas** y pueden ser pasivos o activos. Los ataques pasivos son aquellos en los que el atacante no modifica ni destruye ningún recurso informático, simplemente lo observa. Los ataques activos pueden ser varios: suplantación de identidad, reactuación (por ejemplo intentar repetir varias veces un ingreso en una cuenta bancaria), degradación fraudulenta del servicio (por ejemplo interceptar y eliminar todos los mensajes de correo de un dominio o hacia una cuenta determinada) y modificación de mensajes (se intercepta y se reenvía modificado el mensaje).

Las personas que pueden provocar estos ataques pueden ser el mismo usuario (por descuido o ignorancia el propio trabajador puede provocar grandes males en el sistema de una empresa), antiguos trabajadores (por lo que hay que anular todos los privilegios de los trabajadores en cuanto abandonan la empresa), intrusos informáticos que pueden ser por hobbie, pueden ser remunerados por empresas contrarias o incluso por la propia empresa para tratar de descubrir sus puntos débiles.

2. SEGURIDAD DEL ENTORNO

Analizamos ahora las medidas de protección física que se pueden utilizar para evitar los accesos no autorizados a los sistemas informáticos. Como medidas de prevención podemos aplicar las siguientes:

- Mantener todos los servidores en una zona de acceso físico restringido y ubicar los dispositivos de almacenamiento en un lugar diferente del resto del hardware.
- Llevar a cabo inventarios o registros de todos los elementos del sistema informático.

- Utilizar cámaras de vigilancia y escoger una topología de red adecuada a nuestra organización.
- Utilizar contraseñas de entrada en la BIOS, en el sistema operativo, en los ahorros de pantalla, etc.

Y un apartado fundamental son establecer **mecanismos de autenticación**, denominamos autenticación al proceso de verificación de la identidad de una persona o de un proceso que quiere acceder a los recursos de un sistema informático. Dividiremos estos mecanismos de autenticación en dos tipos, de usuarios y de datos.

Los **mecanismos de autenticación de usuarios** pueden estar basados en elementos conocidos por el usuario, en elementos que posee el usuario o biométricos.

Como elementos conocidos por el usuario es el conocido sistema de nombre de usuario y contraseña; es un método muy extendido por la facilidad de uso y lo barato de su aplicación pero en absoluto es seguro, especialmente porque tendemos a poner contraseñas conocidas (teléfono, DNI), a usar las mismas contraseñas en varios procesos y a no cambiarlas nunca.

Como elementos que posee el usuario destacan las tarjetas inteligentes, que pueden funcionar por contacto o por proximidad.

Por último los sistemas biométricos son los más seguros y también los más caros; basados en la voz, escritura, huellas dactilares, patrones de retina o geometría de la mano, están basados en características físicas del usuario que no pueden copiarse fácilmente.

Los **mecanismos de protección de datos** se basa en dos sistemas principalmente: la criptografía y la esteganografía.

La **criptografía** es la ciencia y el estudio de la escritura secreta. Varios sistemas criptográficos de clave secreta, pública y compartida son la base de la firma digital. Destacan la función hash o resumen con algoritmos de 128, 256 e incluso 512 bits; también tenemos la PGP que es una herramienta criptográfica en origen gratuita y de dominio público hasta determinada versión.

La **esteganografía** es el conjunto de técnicas que permiten ocultar o esconder cualquier tipo de datos. No se pretende aquí cifrar datos para intentar ocultarlos sino simplemente esconderlos en los bits menos representativos de archivos que pasarían completamente desapercibidos, como por ejemplo una imagen JPG. El fichero original y el que oculta información son una casi misma imagen, con el mismo tamaño de archivo y esa es la principal característica de esta técnica, que al tratarse de un fichero normal y corriente no despierta sospechas. Es decir, un fichero criptografíado se puede pensar que esconde información importante, y aunque tardemos mucho tiempo en descifrarlo lo conseguiremos; en cambio un fichero esteganografiado no despierta sospechas y, por eso mismo, no intenta descifrarse su contenido que, por otro lado, sería fácil de hacer.

3. SEGURIDAD DEL SISTEMA

Ataques a contraseña

Las contraseñas en UNIX almacenadas en /etc/passwd son muy sensibles a los cambios. Cuando un usuario accede al sistema no se descifra su contraseña almacenada en este fichero, sino que se traduce la que ha introducido y se compara con la que está guardada en el fichero, si son iguales, de acuerdo, el usuario puede acceder al sistema. En ocasiones si la contraseña es demasiado fácil o guarda relación con datos del usuario o su entorno puede intentar descifrarse por ingeniería social; si es una palabra que existe en el idioma del país, se puede intentar encontrar con ataques de diccionario repetidos, mientras que si contiene pocos caracteres puede intentar descubrirse por ataques de fuerza bruta.

Código malicioso y amenazas lógicas

Se denomina código malicioso al que se inserta dentro de un programa autorizado y realiza una serie de acciones desconocidas por el usuario. Puede eliminar datos, reenviar información sensible por correo electrónico, etc. Este código malicioso se vale de:

- Software incorrecto: agujeros de seguridad que deben ser parcheados constantemente actualizándonos el sistema operativo y los distintos programas.
- Bombas lógicas: partes de código malicioso que se mantiene inerte hasta que se produce una cierta condición: una fecha, una secuencia de teclas, etc.
- Virus, como los gusanos (se autoejecuta para propagarse por la red y colapsar el ancho de banda), troyanos (código oculto que puede capturar contraseñas y otros datos pero que aparentemente no produce daños en el sistema), bacterias (se reproducen hasta agotar los recursos del sistema) y backdoors (puertas de acceso a sistema operativo y software general que permite saltarse todas las medidas de seguridad establecidas).

Detectores (sniffers)

Son programas que permiten la captura y el registro de la información que circula por una red y se basan en la activación del modo promiscuo de las interfaces de red de los terminales de trabajo. Su actividad es difícilmente detectable pues no dejan huellas, sin embargo existen distintas herramientas software para comprobar la presencia de interfaces en modo promiscuo.

Escáneres

Son herramientas de seguridad que sirven para detectar las vulnerabilidades de un sistema informático, tanto local (escáneres de sistema) como en la red (escáneres de red).

Ataques de denegación de servicio

Es toda acción iniciada por una persona o por otras causas, que inutiliza el hardware y/o software de manera que los recursos del sistema no sean accesibles desde la red. Pueden ser ataques contra el hardware de la red (envío de paquetes erróneos al sistema que el receptor no puede procesar), ataques contra el sistema operativo (por ello hay que actualizarse con los últimos parches disponibles) o ataques contra aplicaciones que utilizan el sistema operativo (aprovechando al igual que en el propio sistema operativo, errores de programación).

Auditoría y ficheros log

El logging es el proceso mediante el cual se registran en un fichero las actividades que se producen en un sistema operativo y log es el fichero propiamente dicho. Estos ficheros del sistema operativo son demasiado conocidos por los intrusos, por lo que conviene utilizar herramientas de logging diferentes y complementarias a ellas para llevar otros registros más personalizados y ocultos. La información contenida en los ficheros log es fundamental en la investigación de los delitos que se hayan podido cometer con el concurso de las nuevas tecnologías, y aunque no existe ninguna legislación por el momento que obligue a crear y mantener estos ficheros, la gran mayoría de proveedores de servicios disponen de ellos y los almacenan durante un período de tiempo razonable.

4. EL DELITO INFORMÁTICO

El delito informático no aparece en el actual Código Penal (1995) por lo que se debe hablar de delitos cometidos con el concurso de la informática o las nuevas tecnologías. Entre estos delitos destacan:

- **Delitos contra la intimidad**: Como la intercepción del correo electrónico está asimilada a la violación de la correspondencia, las conductas de apoderamiento de mensajes de correo electrónico, intercepción de las telecomunicaciones y

utilización de artificios de escucha, transmisión o grabación de señales de telecomunicación, están prohibidas. Ahora bien, también es cierto que un correo electrónico laboral no debe ser utilizado con fines personales y de ahí que las empresas reivindiquen sus derechos a poder "consultar" el correo electrónico de sus trabajadores.

- **Usurpación y cesión de datos reservados de carácter personal**: El apoderamiento, utilización, modificación, revelación, difusión o cesión de datos reservados de carácter personal que se encuentren almacenados en ficheros, soportes informáticos, electrónicos o telemáticos son constitutivas de delito. La Ley Orgánica de Protección de Datos de Carácter Personal de 1999 establece 3 niveles de seguridad según el tipo de datos que se contengan:
    - Nivel básico: Requiere medidas de autenticación y control de acceso a estos ficheros personales.
    - Nivel medio: El administrador debe elaborar un catálogo sobre las medidas de seguridad genéricas y se deben implantar mecanismos seguros de autenticación remota.
    - Nivel alto: Es necesario usar métodos criptográficos para evitar que los datos sensibles sean inteligibles, y los datos relativos a ideología, creencias, origen racial, salud, vida sexual, etc, son susceptibles de ser protegidos en este nivel.
- **Revelación de secretos de empresa**.
- **Daños**: Destrucción, alteración, inutilización o cualquier otra modalidad que implique el daño de datos, software o documentos electrónicos almacenados en redes, soportes o sistemas informáticos. Cuando se denuncia una acción delictiva deben valorarse los daños, como por ejemplo restauración de una página web y compensación por el tiempo durante el que no se ha podido prestar un determinado servicio.
- **Delitos contra la propiedad intelectual**: Reproducción íntegra de software y venta al margen de los derechos de licencia, utilización de una única licencia de software para su uso en varios ordenadores, instalación de copias no autorizadas de software en u ordenador en el momento de su compra, publicación del código fuente de software al margen de los derechos de autor y ruptura de los mecanismos de protección que permiten el funcionamiento correcto aunque protegido del software.

TEMA 8 EL SISTEMA INFORMÁTICO DENTRO DE LA ORGANIZACIÓN

1. EL JEFE DE INFORMÁTICA

El jefe de informática gestiona los recursos del departamento de informática y actúa de enlace entre el departamento y la organización. Esto quiere decir que el jefe de informática posee información relativa a la situación de la organización que el personal técnico no es necesario que conozca; también se ocupa de velar por una serie de proyectos que desempeñan los administradores relativos a la informática de la organización.

Por todo ello, el jefe de informática tiene una visión más global de todo, y necesita la figura del administrador que es quien cuida de los servidores.

2. LOS PLANES

Una **planificación estratégica** es un conjunto de propuestas realistas para fijar los objetivos de la organización en un futuro. La planificación estratégica para minimizar riesgos y maximizar resultados, debe plantear estrategias y objetivos simples, claros, alcanzables y mensurables.

Para realizar correctamente esta planificación en los últimos años ha aparecido el análisis DAFO (debilidades, amenazas, fortalezas y oportunidades) que se ha convertido en un instrumento de diagnóstico para la dirección estratégica de la dirección. Se estudian las debilidades, amenazas, fortalezas y oportunidades y, de esa manera se establece un plan de contingencias, que aplicándolo exclusivamente al sector informático intenta un doble objetivo: reducir la posibilidad de que pueda ocurrir algún percance y prever las acciones y actuaciones que es preciso poner en práctica si esto llegara a ocurrir.

El **plan de seguridad y análisis de riesgos** debe velar por toda la seguridad del equipamiento informático, para ello se preguntan qué puede ir mal, estimar el coste que comportaría para la organización y calcular la probabilidad de que se dé cada uno de los posibles problemas. A la par se estudia paralelamente qué se intenta proteger y qué valor tiene dentro de la organización. Según la probabilidad de riesgos, lo que cueste reponerlo y el valor que tiene dentro de la organización se tomarán unas u otras medidas conducentes a la protección de ese equipamiento.

3. DETECCIÓN DE LAS NECESIDADES DE SOFTWARE EN LA ORGANIZACIÓN

Cuando la informática está implantada en una organización, siempre existen necesidades nuevas, dado que una organización es una entidad viva, con necesidades que varían a lo largo del tiempo, entre las que se encuentran, por supuesto, las informáticas.

El cubrir estas necesidades suele tener 3 etapas:

- **Detección**: A menudo una necesidad muy evidente es difícil de detectar, puede provenir de muchas fuentes: quejas en el CAU, peticiones en el CAU, desde el mismo departamento de informática para mejorar el servicio, el rendimiento o simplemente ampliarlo, desde cualquier punto de la organización, etc. por tanto la aparición de una necesidad que deba cubrir el departamento de informática puede llegar por muchas vías.
- **Concreción**: Ya se ha detectado una necesidad, pero a menudo son personas ajenas al mundo de la informática las que en su lenguaje habitual nos la demandan; es necesario por tanto concretar esa necesidad con sucesivas

reuniones. La comunicación con todas las personas y departamentos relacionados directa o indirectamente con la necesidad puede ser clave para concretar el problema y, especialmente, la solución.

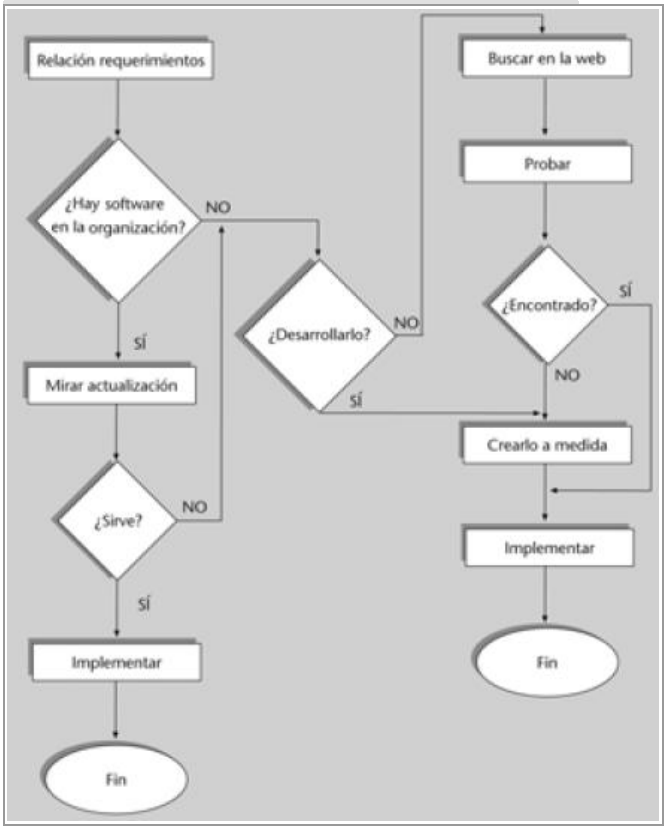
- **Análisis**: Se elabora un primer estudio sobre viabilidad del proyecto para determinar cómo puede encajar en el sistema informático actual o cual sería la mejor manera de solucionar el problema planteado. Se prepara un informe técnico preliminar con todos los recursos hardware, software, humanos y económicos con que contamos.

4. IMPLANTACIÓN/DISEÑO DE APLICACIONES

Si para cubrir una necesidad informática necesitamos software nuevo, se nos plantean varias posibilidades: modificar el software que tenemos (si podemos), comprar software estándar o crear software a medida.

En el primer caso debemos ver si con actualizar el software de que disponemos es suficiente; esta tarea puede ser tan sencilla como leer las especificaciones vía web o papel de las últimas versiones disponibles, o tan compleja como pedir un cd-rom de evaluación para comprobar in situ si se adapta a nuestra necesidades.

Decisión de software



Si nos decantamos por comprar software estándar debemos saber que nunca se adaptará del todo a nuestras necesidades y que se va a introducir un elemento nuevo que el personal de la organización deberá aceptar y aprender; debemos estar pendientes de todo el proceso de parametrización del software (adaptación a la empresa), implantación en servidores, en los terminales y diseñar un plan de formación para todos los usuarios. A pesar de estas desventajas es una opción más barata que la siguiente.

El desarrollar software a medida implica a mucha gente, mucho dinero y muchas reuniones. Si la organización es lo suficientemente grande como para contar con un equipo de desarrollo perfecto, de no ser así deberemos contratar una empresa externa y, en este caso, habrá que negociar en un contrato la propiedad de las fuentes y la programación y, por otro lado, escoger una empresa lo suficientemente fuerte como para que se mantenga en el mercado y nos permita actualizaciones posteriores.

En cualquier caso, escoger la mejor opción es muy difícil y de ello se encargará el jefe de informática. El diagrama lateral puede ser una ayuda para la elección de la mejor solución.

5. ASPECTOS LEGALES

Cuando sucede un problema de seguridad son varios los pasos a seguir:

1. Que el administrador de sistemas ponga en marcha el protocolo técnico de parada, copia, restauración; previamente recogiendo los ficheros de log y todas las pruebas para poder hallar al culpable. En caso de delitos como pornografía infantil se ha de poner primero en contacto con la policía con el fin de no destruir pruebas que podrían resultar fundamentales.

2. Hablar con la dirección de administración sobre el problema de seguridad que se ha producido.
3. Informar al cuerpo de policía adecuado para denunciar el hecho, elaborando un informe exhaustivo sobre lo ocurrido con toda la documentación y pruebas que se hayan podido reunir; se elabora paralelamente un informe de desperfectos y valoración de daños económicos y materiales.

Respecto al software a medida, es fundamental la redacción de un contrato adecuado para dilucidar la propiedad del código fuente (o alguna parte de éste) antes de empezar el proyecto.

6. RESPONSABILIDADES DEL JEFE DE INFORMÁTICA

- Elaboración del plan estratégico del departamento, subordinado al plan estratégico de la organización y velar por su cumplimiento.
- Elaboración de los planes de actualización informático y contingencias.
- Detección y concreción de necesidades
- Actuación y respuesta ante situaciones que comprometan la seguridad del sistema.