Administración de usuarios

Jordi Serra Ruiz
Miquel Colobran Huguet
Josep Maria Arqués Soldevila
Eduard Marco Galindo

PID_00190207

UOC
Universitat Oberta de Catalunya

Índice

Introducción

En este módulo nos centraremos en el usuario y en todo lo que tenemos que saber en relación con los aspectos siguientes:

- Servidores.
- Estaciones de trabajo.
- Software.
- Datos.
- Incidencias.
- Formación.

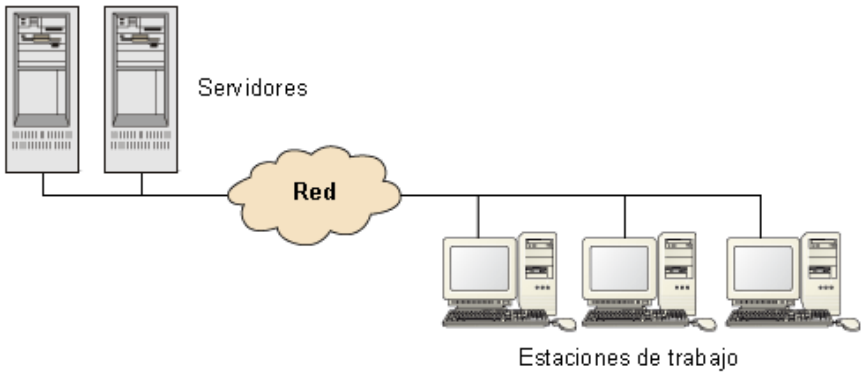
La función del sistema informático es dar apoyo y servicio a los usuarios, y ayudarlos a hacer su tarea dentro de la organización.

La filosofía del departamento

Hay autores que tienden a considerar el servicio informático como un negocio y a tener a los usuarios como clientes. En tales casos, ésta es la filosofía de organización, trabajo y actuación en todo momento del departamento informático.

A grandes rasgos, el esquema en que todas las redes se pueden ver lo podemos representar así:

Esquema de una red



Por lo tanto, el tratamiento de los usuarios, desde el punto de vista de la administración, lo podemos dividir en unos servicios o funciones que, necesariamente, se tienen que hacer en la parte "servidor", y unos servicios o funciones que se tienen que hacer en la parte "usuario" o cliente.

Primero veremos cómo se hace el diseño del entorno de los usuarios por la parte que afecta a los servidores. Un buen diseño simplifica la administración y ayuda a los usuarios a tener un entorno más coherente y robusto. Eso quiere decir que, a medio plazo, también se convierte para ellos en una herramienta más sencilla de utilizar.

Después seguiremos con la instalación, la configuración y el mantenimiento de las estaciones de trabajo. Una configuración bien pensada y un mecanismo de recuperación de configuraciones permiten dar un buen servicio de averías y, una vez más, simplifican la administración de las estaciones de trabajo. Con ello, se acaba la parte que atañe al entorno del usuario.

Los puntos siguientes inciden en lo anterior directamente, dado que tratan de la formación y la atención de incidencias del usuario. Son tan importantes como los anteriores, y a menudo se llevan poco a la práctica. La formación reduce costes a medio plazo, ya que ahorra tiempo del departamento de informática, en formar al personal de la organización y hacerlo autosuficiente en cosas nuevas, y una gestión de incidencias correcta ahorra costes a la organización y también, indirectamente, al departamento de informática.

Gestión de incidencias

Muchas veces, la gestión de incidencias se llama *centro de atención al usuario* (CAU) o *HelpDesk*.

Objetivos

Los materiales didácticos de este módulo contienen las herramientas necesarias para que el estudiante adquiera las competencias siguientes:

1. Saber diseñar un entorno para los usuarios adecuado a la organización.

2. Saber diferenciar las tareas que afectan a los servidores de las que afectan a las estaciones de trabajo.

3. Saber diseñar un entorno para las estaciones de trabajo útil para los usuarios y que sea lo más sencillo posible de administrar.

4. Saber hacer del departamento de informática un servicio ágil para responder a las incidencias de los usuarios.

5. Saber que las tareas se pueden sistematizar en procedimientos.

6. Conocer las responsabilidades del administrador de usuarios.

7. Conocer herramientas para configurar, mantener y recuperar estaciones de trabajo en situaciones problemáticas.

1. Diseño del entorno de usuarios

Desde el punto de vista del hardware, el sistema informático está compuesto de los servidores, la red, el *router* y las estaciones de trabajo. Desde el punto de vista del software, tiene los sistemas operativos y las aplicaciones. Y no basta con unirlos. Tenemos que diseñar la manera de hacerlo para obtener el resultado esperado.

A continuación, definiremos todo lo que el usuario encontrará cuando se conecte a los servidores de la organización. Tenemos que diseñar el entorno de los usuarios.

Diseñar el entorno de los usuarios quiere decir preparar todo aquello con que se encontrará el usuario cuando utilice la informática de la organización.

Los criterios y objetivos que hay que seguir en nuestro diseño serán los siguientes:

Observación

La lista de criterios y objetivos que hay que seguir en el diseño es aproximativa.

- Tiene que ser simple de utilizar e intuitivo para el usuario.
- Tiene que proporcionar un entorno homogéneo a todos los usuarios.
- Si cambia de ordenador o de puesto de trabajo, el entorno (software y hardware) no le tiene que resultar extraño.
- El sistema tiene que ser rápido, en tiempo de respuesta de los servidores y en respuesta de velocidad de la red.
- Tiene que dar un buen nivel de seguridad.
- Tiene que ser fácil de administrar.
- El software tiene que ser fácil de actualizar.
- Si el ordenador falla, tiene que ser fácil de reinstalar.
- Si el ordenador se desconfigura, tiene que ser fácil de reconfigurar.
- Si el ordenador falla no se tiene que perder información, o cuando menos se ha de perder la mínima posible y no tiene que ser crítica.

- Tiene que ser sencillo hacer copias de seguridad.

- Ha de ser fácil poder responder ante una situación de desastre de una estación de trabajo.

Las contradicciones

Los criterios y objetivos de diseño a menudo entran en contradicciones. La seguridad acostumbra a contradecirse con la comodidad y la velocidad. El resultado final siempre es una solución de compromiso entre estos elementos.

La utopía

Con la relación de objetivos y criterios de diseño que os hemos presentado, lo primero que parece evidente es intentar conseguir lo siguiente:

- Que todo el entorno del software tenga una interfaz homogénea.
- Que todo el entorno del hardware de estaciones de trabajo sea homogéneo.

Aunque son dos objetivos muy interesantes, difícilmente se pueden llevar a cabo en la práctica; por lo tanto, es más factible intentar que el entorno del usuario y del hardware sean lo más homogéneos posible.

Teniendo presentes estos objetivos, cuántos servidores corporativos hay, la red existente, las estaciones de trabajo instaladas, el conocimiento sobre los puestos de trabajo de la organización, la estructura de los departamentos y de la organización, etc., tenemos que diseñar el entorno en el cual trabajarán muchas horas diarias los usuarios. Por lo tanto, es importante una planificación esmerada.

El diseño del entorno de los usuarios afecta tanto a los servidores como a las estaciones de trabajo y, por lo tanto, se tiene que hacer teniendo en cuenta las dos partes (como una unidad), ya que de hecho trabajan conjuntamente, de manera que no es posible el diseño general de una parte sin tener en cuenta la otra. Una vez establecidas las líneas maestras de este diseño, se puede pasar a detallar cada una de las partes.

1.1. Necesidades generales del usuario

Todas las organizaciones son diferentes. A pesar de eso, las necesidades informáticas de los usuarios se pueden generalizar un poco. Podemos decir que todos los usuarios tienen las necesidades del sistema informático siguientes:

- Una estación de trabajo. Generalmente es un ordenador. Es posible que algunos usuarios particulares necesiten dispositivos especiales, como grabadoras de DVD, escáneres, impresoras locales, impresoras de etiquetas, lectores de tarjetas inteligentes, etc.

- Un lugar donde se pueda imprimir.

- Espacio para guardar la información.

- Software para trabajar.

Genéricamente, el software que necesita el usuario lo podemos dividir en diversas categorías:

- **Software de base**. Sistema operativo y aplicaciones básicas de comunicaciones en los servidores.

- **Software de ofimática**. Son los paquetes de ofimática, que normalmente incluyen una hoja de cálculo, un procesador de textos, una base de datos y una agenda.

- **Software de comunicaciones**. Generalmente podemos incorporar el correo electrónico y un navegador de Internet.

- **Aplicaciones específicas**. Es el grupo de aplicaciones que engloba programas dependientes de la organización e incluso del departamento. Programas de facturación, contabilidad, diseño gráfico, control de la producción, nóminas, etc.

Al poner en marcha la mayoría de aplicaciones específicas, normalmente piden un usuario y una contraseña (adicionales a los que se han puesto al entrar en la red) para acceder[1]. Esta identificación, que normalmente es para aplicaciones que tienen bases de datos en servidores, sirve para asignar privilegios dentro de la aplicación, de manera que la parte cliente es idéntica para todo el mundo y lo que se puede hacer sólo depende del usuario que ha entrado.

[(1)]En inglés, *single sign on*.

Single sign on

En el sistema *Single Sign On* se busca identificarse una sola vez y poder acceder a todos los sistemas. Hay diversos mecanismos como:

- E-SSO.
- Web-SSO.
- Kerberos.
- OpenID.

El acceso a estas aplicaciones (tanto si son estándares como específicas) tiene que estar controlado de alguna manera, ya que no todo el mundo tiene acceso a toda la información de la organización. Para manipular la información de la organización (es decir, crearla, modificarla o consultarla), en principio no hace falta que el usuario sepa dónde está esta información, sino sólo la manera de acceder a ella y cómo manejarla para trabajar.

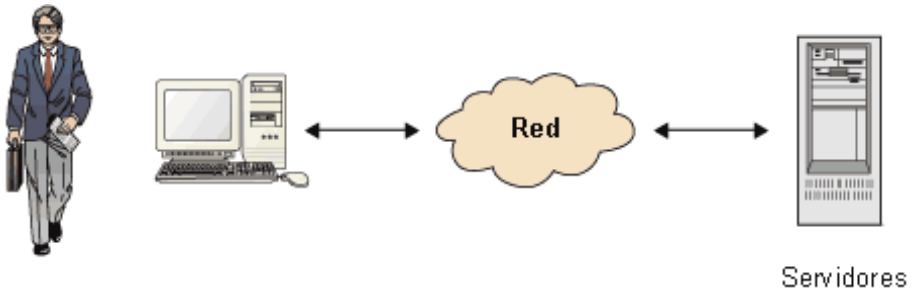
Para que funcionen correctamente todas estas necesidades se tienen que presentar en un entorno que sea agradable y fácil de utilizar. De lo contrario, el sistema, en lugar de ayudar a la tarea, lo que hace es dificultarla, y en vez de cumplir el objetivo global de mejorar el rendimiento se consigue lo contrario, disminuirlo y dificultar el flujo de información por toda la organización.

Todos los usuarios de una organización se pueden unir en grupos de necesidades muy similares. No habrá muchos grupos y tampoco serán muy diferentes.

1.2. El sistema informático y el usuario

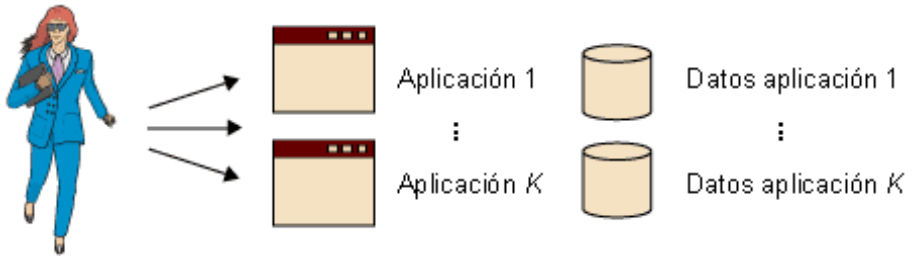
El esquema global que se puede llegar a imaginar un usuario del sistema informático es parecido al siguiente:

Esquema de un sistema informático



Y la que tiene de las aplicaciones es

Esquema de un sistema informático



Un usuario, sin embargo, no sabe dónde están las aplicaciones físicamente ni dónde "viven" realmente los datos.

Misterios informáticos

A menudo, es sorprendente ir a otro ordenador, conectarse y encontrar todos los datos y los programas. De la misma manera, si se ha guardado alguna cosa (en local), cuando se va a otro ordenador y no se encuentra, no se entiende, ya que "lo han guardado como siempre", enseñan muchos ficheros como demostración y, en cambio, lo que han guardado hace una hora "ha desaparecido". Nadie nace enseñado y es muy normal que pase. Poco a poco, se va educando al usuario en estas nuevas herramientas de trabajo.

A partir de la lista de objetivos que hemos hecho antes, y de la visión que sabemos que los usuarios tienen de la red informática, veremos diversos mecanismos de control de acceso que nos permiten diseñar el entorno del usuario.

1.3. El control de acceso

Una de las cuestiones fundamentales en el diseño del entorno del usuario es conseguir que éste acceda únicamente a aquello que necesite (principio de privilegio mínimo).

El principio de privilegio mínimo

El principio de privilegio mínimo consiste en otorgar el conjunto de privilegios más restrictivo necesario (la autorización más baja) para llevar a cabo su tarea.

Cuando un usuario necesita acceder a un recurso del sistema informático se tiene que **identificar** (**autenticar**). Una vez se ha identificado, el sistema controla **(autoriza**) el acceso a los recursos del sistema informático y registra (**audita**) qué uso se hace de cada recurso. Este modelo se conoce como modelo de seguridad **AAA**[2].

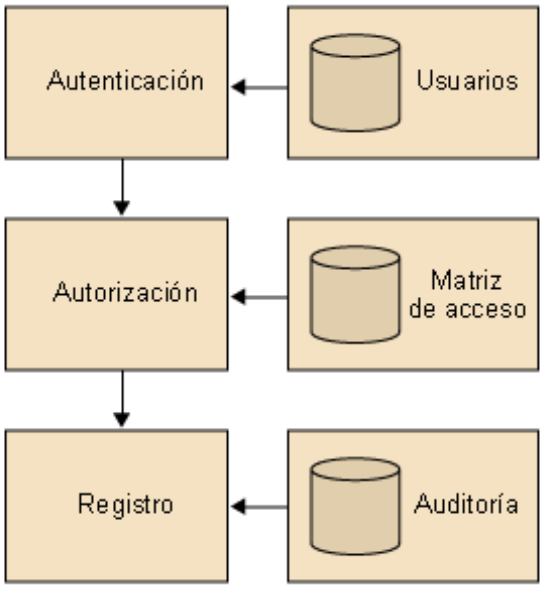
[(2)]AAA es la sigla de la expresión inglesa *authentication, authorization & accounting*.

Se podrán definir diferentes unidades de red, es decir, discos virtuales en la red, de forma que solo los usuarios del mismo departamento tengan acceso, de este modo protegeremos los datos de accesos no permitidos. El departamento de producción no tiene que tener acceso a los datos del departamento de recursos humanos, o a la dirección.

El control de acceso

El control de acceso es un tema muy extenso de la seguridad y sobrepasa los objetivos de estos materiales. Nosotros sólo veremos aquella parte que nos resulta útil para el diseño global del sistema informático.

Esquema del modelo de seguridad AAA



Lectura recomendada

Sobre el principio de privilegio mínimo, podéis ver *DOD-5200.28-STD. Libro Naranja* (Documento Criterios de Evaluación de Sistemas Informáticos de Confianza del Departamento de Defensa).

La **autenticación** es el proceso de verificación de la identidad de una persona o de un proceso que quiere acceder a los recursos de un sistema informático. Habitualmente, se hace a través del nombre del usuario y contraseña o *token* del proceso.

La **autorización** es el proceso a través del cual el sistema autoriza al usuario identificado el acceso a los recursos de un sistema informático.

Ved también

Ved más ampliamente la autenticación en el módulo "Administración de la seguridad".

La autorización determina qué acceso se permite para cada usuario a qué entidad. La autenticación es el proceso de verificar la identidad de una persona, mientras la autorización es el proceso de verificación, que una persona conocida tiene la autoridad para realizar una cierta operación. La autenticación, por lo tanto, tiene que preceder a la autorización.

El **control de acceso** determina qué privilegios tiene un usuario dentro del sistema informático y a qué recursos tendrá acceso. Este control de acceso se tiene que pensar muy bien y cuidadosamente, puesto que podríamos tener problemas de acceso a información privada otras personas o grupos de la empresa.

El **registro** del uso de los recursos es la información de *log* guardada de la actividad del usuario en el sistema informático.

1.3.1. Matriz de control de acceso

La matriz de control de acceso o matriz de acceso es un modelo formal de seguridad computacional usado en sistemas informáticos que caracteriza los derechos de cada sujeto con respecto a todos los objetos del sistema. Los objetos son entidades que contienen información, pueden ser físicos o abstractos. Los sujetos acceden a los objetos, y pueden ser usuarios, procesos, programas u otras entidades.

Los derechos de accesos más comunes son: acceso de lectura (**L**), acceso de escritura (**E**) y acceso de ejecución (**X**).

Las filas de la matriz representan dominios (o sujetos) y las columnas representan objetos. Las entradas de la matriz consisten en una serie de derechos de acceso. Por ejemplo, la entrada $access_{(i,j)}$ define el conjunto de operaciones que un proceso, ejecutándose en el dominio D_i, puede invocar sobre un objeto O_j.

		Objeto	
		Fichero	Directorio
Dominio	D1	Lectura	Lectura Escritura Ejecución
	D2		Lectura Escritura
	D3	Ejecución	Lectura

1.3.2. Lista de control de acceso

No se acostumbra a guardar la matriz, ya que es muy grande. Gran parte de los dominios no tienen ningún acceso a la mayoría de los objetos, por lo que el almacenamiento de una matriz enorme casi vacía es un despilfarro de espacio de disco. Lo que se hace es asociar a cada objeto una lista (ordenada) con todos los dominios que pueden tener acceso a él y la forma de hacerlo. Esta lista se llama lista de control de acceso (ACL).

Ved también

Sobre la lista de control de acceso, ved también el módulo "Administración de la seguridad".

1.4. Diseño del sistema informático

Veamos cómo podemos aplicar la matriz de acceso en diversos diseños. Estudiaremos también sus ventajas e inconvenientes.

1.4.1. Mínima seguridad

Hacemos un diseño, que simplifica bastante la administración, basándonos en los criterios siguientes:

- Todos los usuarios ven todos los programas y todas las aplicaciones.
- Todos los usuarios tienen permisos mínimos (por lo tanto de lectura y ejecución) para todo.
- Las aplicaciones específicas (como, por ejemplo, bases de datos), que ya tienen permisos de acceso propios, quedan controladas por la misma aplicación. No hacen falta permisos especiales.
- A las carpetas personales de usuario sólo puede entrar el mismo usuario con permisos de lectura, escritura y ejecución.

Las ventajas de este diseño son las siguientes:

- Simplifica la administración, ya que todos los usuarios son iguales y, por lo tanto, crear un usuario no representa tener nada en cuenta.
- Facilita la preparación de la estación de trabajo modelo. Es decir, todos los puntos de trabajo serán idénticos.
- Una vez clonado un equipo, casi no hay ajuste final.
- Cualquier usuario tiene permiso para ejecutar cualquier aplicación, por lo cual la modificación de los esquemas de trabajo de la organización no representa ningún problema ni ninguna modificación en las estructuras informáticas creadas.

- El cambio de rol de trabajo de una persona no implica modificar nada de su perfil, ya que tiene todas las aplicaciones disponibles, sólo tiene que escoger otras para trabajar.

- El cambio de punto de trabajo no tiene el coste añadido de instalar las aplicaciones específicas para aquel usuario, puesto que están todas disponibles en todas las estaciones de trabajo.

- El entorno de trabajo es completamente homogéneo en toda la organización, dado que todo el mundo ve exactamente lo mismo.

- Facilita la tarea de hacer búsquedas de información dentro del sistema informático, porque toda la información es "plana" (no está jerarquizada ni protegida) dentro del sistema.

- El usuario dispone de todo el potencial informático de la organización.

- Cualquier cambio que comporte utilizar un nuevo software no implica modificaciones en el sistema informático.

Los inconvenientes de este diseño son los siguientes:

- La idea de grupo de trabajo, grupo de personas, departamento, etc., en definitiva, la agrupación no queda incluida en la estructura informática, y eso puede complicar la administración en momentos en que haya que incorporarla para manipular información.

Ved también

Sobre la estación modelo, ved el subapartado 3.3 de este módulo.

- La compartimentación de información entre grupos de usuarios no es fácil, ya que no existe el concepto de grupo de personas. Por ejemplo, compartir información todo un departamento, sin que el resto de personas de la organización no tengan acceso a ella.

- El usuario se puede perder un poco ante demasiado software, dado que puede no saber cuál es el "suyo" (cuál tiene que utilizar para trabajar) y cuál no.

- Permitir que el directorio de un usuario, si el usuario quiere, sea accesible a la gente de su grupo de trabajo no es posible. Si lo hace, quedará automáticamente abierto a toda la organización.

- Puede ser negativo que cualquier persona de la organización pueda ejecutar cualquier aplicación. Puede haber información sensible que no tiene que estar al alcance de otros grupos de la organización.

- Muchas peticiones de grupos de usuarios con respecto a la manipulación de información, especialmente si es sensible, son muy complejas o incluso imposibles de hacer.

- Hay peligro de manipulaciones incorrectas con resultados no deseados.

1.4.2. Usuarios en grupos

Intentaremos una segunda solución modificando algunos de los criterios. Ahora nos basamos en los siguientes:

- Los usuarios se unen en grupos de una manera natural dentro de la organización. Intentamos reflejar esta situación dentro del sistema informático.

- Un usuario sólo puede pertenecer a un grupo.

- Una aplicación puede funcionar para todo el mundo o sólo para un grupo.

- Todos los usuarios tienen permisos mínimos (por lo tanto de lectura y ejecución) para los elementos del grupo.

- Todos los usuarios tienen permisos de lectura y ejecución para los elementos generales (de todo el mundo).

- Las aplicaciones específicas (como, por ejemplo, bases de datos), que ya llevan permisos de acceso propios, quedan controladas por la misma aplicación. No hace falta permisos especiales. Ahora sólo ven estas aplicaciones los grupos de usuarios que las necesitan.

- En las carpetas personales de usuario sólo puede entrar el usuario con permisos de lectura, escritura y ejecución.

- Tenemos que tener en cuenta las categorías de software que podríamos encontrar dentro de una organización.

Las ventajas de este diseño son las siguientes:

- Todos los usuarios son iguales por grupos; por lo tanto, crear un usuario representa tener en cuenta a qué grupo tiene que pertenecer.

- Cualquier usuario sólo tiene permiso para ejecutar cualquier aplicación del grupo y todas las aplicaciones comunes a todo el mundo.

- El usuario sólo puede acceder a información del grupo y a la información común. Por lo tanto, la información de la organización está mucho mejor protegida.

- No puede haber manipulaciones incorrectas de software, ya que ahora sólo lo pueden ejecutar los usuarios del grupo.

- El entorno de trabajo es bastante homogéneo en toda la organización, pero varía en la medida en que varían las aplicaciones que ve el usuario para trabajar. Afortunadamente, el paquete de aplicaciones comunes a todo el mundo es el mismo, y eso da una sensación de homogeneidad muy importante para el usuario.

- El usuario, básicamente, dispone de los recursos de software que necesita. Le facilita las cosas saber que el software que tiene al alcance es el que tiene que utilizar, y no como antes, que veía alguno que no tenía que utilizar.

- Ahora la idea de grupo de trabajo sí que se incluye, y es muy útil para compartir información en el grupo y para trabajar en aplicaciones específicas de una manera coordinada. Muchas veces la estructura de grupos, como consecuencia de las peticiones que recibe el departamento de informática, simplifica la administración, porque son para cuestiones características de un grupo de trabajo.

- Ahora se puede permitir que el directorio de un usuario, si el usuario quiere, sea accesible a la gente de su grupo de trabajo. Si lo hace, queda automáticamente abierto sólo a su grupo de trabajo.

Ved también

Ved el apartado 1.1 de este módulo.

Los inconvenientes de este diseño son los siguientes:

- Una modificación en los esquemas de trabajo puede representar modificar todos los permisos de las aplicaciones y de las carpetas de trabajo de los grupos, es decir, modificar las estructuras informáticas que se han creado.

- El cambio de rol de trabajo de una persona, en caso de que cambie de grupo, implica modificar el perfil, porque pasará a tener disponibles otras aplicaciones y parte de las que tenía (las específicas de su grupo) las dejará de tener.

- La busca de información dentro del sistema es más compleja, dado que ahora está organizada por grupos de trabajo dentro de la organización.

- Instalar un software nuevo puede ser un problema grave si lo tienen que utilizar diversos grupos de trabajo.

- Compartir información entre grupos es complejo.

1.4.3. Usuarios en múltiples grupos

La tercera solución surge del hecho de que algunos usuarios pertenecen a más de un grupo. El grupo funciona muy bien para la mayoría, pero para algunos no es suficiente. Si la organización, por ejemplo, utiliza grupos de trabajo dentro del departamento, o si se crean subgrupos dentro del grupo de trabajo, o incluso en el caso de los directivos, se da la situación de que una persona pertenece a más de un grupo a la vez. Por lo tanto, analizaremos esta situación valorando en primer lugar los criterios que hay que seguir:

- Los usuarios se unen en grupos de una manera natural.
- Un usuario puede pertenecer a un grupo o más.
- Una aplicación puede funcionar para todo el mundo o para uno o más grupos.
- Todos los usuarios tienen permisos mínimos (por lo tanto de lectura y ejecución) para los elementos del grupo.
- Todos los usuarios tienen permisos de lectura y ejecución para los elementos generales (de todo el mundo).
- Las aplicaciones específicas (como, por ejemplo, bases de datos), que ya llevan permisos de acceso propios, quedan controladas por la misma aplicación. No hacen falta permisos especiales. Ahora sólo ven estas aplicaciones los grupos de usuarios que las necesitan.
- En las carpetas personales de usuario sólo puede entrar el usuario con permisos de lectura, escritura y ejecución.

Las ventajas de este diseño son las siguientes:

- Todos los usuarios son iguales por grupos; por lo tanto, dar de alta a un usuario representa tener en cuenta a qué grupos tiene que pertenecer.
- Cualquier usuario sólo tiene permiso para ejecutar cualquier aplicación de los grupos a los cuales pertenece y todas las aplicaciones comunes a todo el mundo. También tiene permiso para acceder a la información común del grupo. Una modificación en los esquemas de trabajo puede representar modificar todos los permisos de las aplicaciones y de las carpetas de trabajo de los grupos, es decir, modificar las estructuras informáticas que se han creado.
- El cambio de rol de trabajo de una persona, en caso de que cambie de grupo, implica modificar el perfil, porque pasará a tener disponibles otras aplicaciones y parte de las que tenía (las específicas de su grupo) dejará

de tenerlas. Puede comportar modificar los grupos a que pertenece y la información a la cual tiene acceso.

- El entorno de trabajo es bastante homogéneo en toda la organización, pero varía en la medida en que varían las aplicaciones que el usuario ve para trabajar. Afortunadamente, el paquete de aplicaciones comunes a todo el mundo es el mismo, y eso da una sensación de homogeneidad muy importante para el usuario.

Los inconvenientes de este diseño son los siguientes:

- Ahora sí que se incluye la idea de grupo de trabajo, y es muy útil para compartir información del grupo y para trabajar en aplicaciones específicas de una manera coordinada. Muchas veces, la estructura de grupos, como consecuencia de las peticiones que recibe el departamento de informática, simplifica la administración, porque son para cuestiones características de un grupo de trabajo. El usuario es consciente de que pertenece a diversos grupos disjuntos (si es el caso) de trabajo y, por lo tanto, ve aplicaciones e información que su compañero de trabajo no tiene que ver necesariamente.

- Ahora se puede permitir que el directorio de un usuario, si el usuario quiere, sea accesible a la gente de su grupo de trabajo. Si lo hace, dependerá de los grupos y privilegios que tenga, ya que es posible que quede abierto a todos los grupos de trabajo a los cuales pertenece.

El diseño tiene que reflejar la estructura de la organización. Por contra, el diseño condiciona el funcionamiento del sistema informático en la medida en que lo define.

Así pues, el diseño que se adoptará se tiene que pensar esmeradamente y hace falta tener en cuenta qué grupos habrá en la organización, qué permisos tienen que tener para las aplicaciones, y qué personas tienen que pertenecer a cada grupo. Se puede hacer mediante una tabla de permisos, en los que se tiene que reflejar:

Grupo	**Persona**	**Persona**
Aplicación	Permiso	Permiso
Aplicación	Permiso	Permiso

Después de estas tablas, hay que hacer la tabla de aplicaciones/grupos, en la cual hay todas las aplicaciones y todos los grupos. Esta tabla, al incluir todas las aplicaciones de la organización, da una visión global de todo el software que se utiliza. Eso es especialmente importante para el software que utiliza información compartida o información que accede a bases de datos.

Software	Grupo	Grupo
Aplicación	Permiso	Permiso
Aplicación	Permiso	Permiso

Ejemplo para un hospital

Supongamos que hacemos un estudio para una organización pública, un hospital:

Médicos	Juan	Carmen
Visitas	L/E	L/E
Recetas	L/E	L/E

Administración	María	Pedro
Contabilidad	L/E	L/E
Facturación	L/E	L/E
Visitas	L	L
Recetas	-	-

Software	Médicos	Administración
Contabilidad	L/E	L/E
Facturación	L/E	L/E
Visitas	L/E	L/E
Recetas	L/E	L/E
Ofimática	L/E	L/E

1.5. Distribución de aplicaciones

Con las tablas que acabamos de hacer tenemos la lista de aplicaciones que nuestros usuarios necesitan. La próxima decisión que hay que tomar es ver dónde tienen que estar estas aplicaciones. Sólo pueden estar en dos sitios:

- **Local**. En la estación de trabajo. En este caso, la aplicación estará instalada en cada estación de trabajo y, por lo tanto, la estación de trabajo no tendrá

que ir a buscar el programa al servidor. Ocupa más espacio de disco en la estación de trabajo, pero carga menos la red y es más rápido de ejecutar.

- **Remoto**. Aquí la aplicación está instalada en algún servidor. La estación de trabajo hace peticiones a un servidor en relación con la aplicación. Hay muchas variantes posibles. Por ejemplo, que esté el programa en remoto (en el servidor), pero que se ejecute en local, que sólo haya un pequeño cliente (un navegador, por ejemplo) y, por lo tanto, que sólo se hagan peticiones a los servidores de lo que se necesita y todo el control lo lleve el servidor, que se utilice una herramienta de emulación de terminal y se conecte a un huésped, etc.

Dependiendo de la aplicación de que se trate, la decisión ya está tomada. Puede pasar que venga dada por el fabricante del software, o que sea muy clara la necesidad de una base de datos que tiene que funcionar sobre un servidor de bases de datos y, por lo tanto, las cosas tendrán que funcionar básicamente en remoto.

Pero, en general, tendremos dos elementos: la aplicación y la información que maneja esta aplicación, y los dos pueden estar en local o remoto. Las posibilidades son las siguientes:

		Información	
		Local	**Remoto**
Aplicación	**Local**		
	Remoto		
Aplicación	**Local**		
	Remoto		

Cada fila "Aplicación" tiene cuatro posibilidades, de las cuales sólo una es la mejor para cada aplicación que se instala en la organización.

Esta tabla se rellena con todas las aplicaciones de la organización. Las aplicaciones se ponen en la primera columna. Nos hace falta saber cuáles tendremos que instalar en cada estación de trabajo y, por eso, tenemos que decidir qué aplicaciones irán en local y cuáles en remoto.

La decisión sobre si la información la pondremos en local o en remoto depende básicamente de cuántas personas accederán a ella, de si la información es crítica y de la posibilidad y la frecuencia de hacer copias de seguridad.

La lista de aplicaciones que se utilizan, y el hecho de saber si están en local o en remoto, es fundamental para el diseño.

1.6. La tabla de aplicaciones

Dando todos los pasos de diseño que hemos explicado hasta ahora, tenemos diversas tablas pequeñas y dispersas. En la práctica, se construye una tabla que resume más de una y que sirve para extraer la información necesaria.

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

El permiso puede ser L, E o X (o una combinación de ellos), que indican lectura, escritura o ejecución.

De esta tabla podemos extraer la información siguiente:

- La lista de software completo que se utiliza en la organización. Está en la primera columna de la tabla.

- Dónde está la información de cada aplicación. Básicamente, si está en local o en remoto, es decir, si se encuentra en servidores o dispersa en estaciones de trabajo. Sirve para programas de copias de seguridad, para establecer permisos. Quizás es necesario hacer una copia de seguridad de datos de aplicaciones instaladas a las estaciones de trabajo.

- La relación de grupos de usuarios que se tienen que crear en los servidores.

- También podemos obtener la lista del software que se utiliza por grupos (y si los grupos representan departamentos, etc., también se puede saber por áreas de la organización) con los permisos que se necesitan.

- La relación de aplicaciones candidatas para crear la estación de trabajo modelo, y también las aplicaciones que hay que instalar en los servidores a fin de que las utilicen los usuarios. Eso lo extraeremos a partir de las aplicaciones que se instalan en remoto o en local.

Todo este conjunto de información también nos da el punto de partida para diseñar la parte servidor.

Estudio para un hospital

Veamos cómo quedaría la tabla con los datos del ejemplo anterior:

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

Con la relación de aplicaciones que se tienen que instalar en local, es decir, en la máquina del usuario, sabiendo dónde residirá la información que utilizará, los grupos de trabajo de los cuales formará parte y con qué permisos, sólo nos queda preparar una cosa: el sistema operativo del ordenador del usuario.

Con la tabla de aplicaciones extraemos mucha de la información para configurar el entorno de los usuarios en el servidor y en los clientes.

1.7. El sistema operativo de la estación de trabajo

Actualmente, los sistemas operativos de estaciones de trabajo están diseñados para trabajar en red (en entornos corporativos) y aportan al usuario una interfaz gráfica para facilitarle el uso del ordenador tanto como sea posible. Las contrapartidas que tienen es que son complejos de instalar y configurar, muy flexibles y, desgraciadamente, fácilmente desconfigurables en manos de usuarios inexpertos. Esto último suele complicar la tarea del administrador de sistemas. Su gran flexibilidad también hace que muchas veces los usuarios novatos se sientan perdidos ante el equipamiento informático. En cualquier caso, los sistemas operativos de red tienen unos puntos en común que vale la pena tener en cuenta:

Ved también

Ved el apartado 5 para intentar evitar estos problemas al máximo.

- El usuario se tiene que identificar forzosamente. La identificación correcta le permitirá acceder a los recursos de la red, dependiendo del usuario, ya que hay privilegios para grupos de usuarios, y acceder a su información privada (directorio personal, correo electrónico, etc.).

- El entorno se tiene que configurar para que sea tan homogéneo y simple como sea posible. Esto facilitará la movilidad.

- Tiene que tener un acceso fácil y rápido a las aplicaciones que más utilice.

- En caso de pérdida de información, el departamento de informática probablemente lo podrá resolver.

- Si tiene un problema con la estación de trabajo sabe dónde tiene que llamar para que lo resuelvan cuanto antes mejor.

El sistema operativo se tiene que poder comunicar bien con los diferentes servidores (recordemos que pueden ser heterogéneos), pueden tener diferentes versiones e incluso diferentes fabricantes.

2. Diseño en los servidores

Ahora ya tenemos las líneas maestras de cómo queremos el diseño de las estaciones de trabajo. Es decir, dónde estarán las aplicaciones, con qué permisos, con qué grupos y un poco cómo se estructurarán los servidores.

Veamos cómo se traslada este diseño a nuestros servidores. Este diseño puede afectar a los servidores en los puntos siguientes:

- Número y capacidad de los discos.
- Contenido y número de particiones de los discos.
- Disposición de la información en los servidores.
- Número de servidores.

Cambios por necesidades

No es la primera vez que en una organización, al analizar las necesidades de los usuarios, se descubre que es necesaria, por ejemplo, una base de datos compleja, lo cual hace que haga falta un servidor de base de datos; esto motiva la aparición de un ordenador servidor, de un servidor de bases de datos y de un software cliente de base de datos en todas las estaciones de trabajo. Si estas cosas se pueden prever antes de que aparezca la necesidad o que la necesidad haga que la base de datos actual se tenga que migrar, nos ahorraremos muchos quebraderos de cabeza, problemas, tiempo, quejas de los usuarios y la siempre latente sensación de que la informática es "aquello que no acaba de funcionar nunca bien".

Un posible procedimiento para detectar estos puntos podría ser:

Ved también

Recordad que en el apartado 1 de este módulo habéis hecho las tres primeras cosas.

1) Hacer una relación de todas las aplicaciones que será necesario instalar.

2) Ver dónde estará la información de todas estas aplicaciones.

3) Ver con qué permisos tendrán que funcionar todas estas aplicaciones.

4) Averiguar, según el número de usuarios actuales y previstos, las necesidades del disco. Básicamente, la partición de usuarios y la partición donde está almacenado el correo electrónico (los buzones de los usuarios).

5) Averiguar, teniendo en cuenta la información que se manipula y la previsión de información que se prevé manipular, las necesidades de disco.

6) Averiguar, considerando todos los elementos anteriores, las necesidades del servidor y de la red.

Finalmente, hace falta adecuar toda la infraestructura según lo que se haya detectado y ver si se tienen que hacer cambios y ampliar o cambiar los servidores.

Hay que ver las necesidades reales de los usuarios para reflejarlas en la estructura informática de los servidores.

2.1. Distribución de los discos

En el apartado anterior hemos hecho el diseño general, por lo que ya sabemos qué tiene que tener nuestro ordenador para los usuarios: sabemos, más o menos, el software que tiene que integrar, las aplicaciones que tienen que funcionar, los permisos, dependiendo del usuario y del grupo al cual pertenece, y donde estarán los datos (en el servidor, en el cliente, en una base de datos, etc.). Con este diseño presente, podemos empezar a diseñar detalladamente cómo será la distribución de los servidores, así como la cantidad.

La distribución básica de particiones de cualquier servidor es la siguiente:

Ved también

Sobre la distribución de las particiones en el servidor, ved el módulo "Administración de servidores".

- Partición de sistema.
- Partición de usuarios.
- Partición de aplicaciones.
- Partición de datos.

Con la tabla de aplicaciones que hemos hecho, conocemos las aplicaciones que necesitan los usuarios. Podemos establecer si son suficientes o si necesitamos suplementarias. También podemos descubrir si alguna aplicación requiere un servidor propio.

Si la organización necesita una web para sacar información de Internet, nos hace falta un servidor web (una aplicación) funcionando en un servidor, y los datos (toda la web) en algún servidor (normalmente el mismo). Seguramente todo en particiones diferentes (se tiene que decidir), y se ha de saber si esta web accederá a información (bases de datos) de la organización para decidir cuestiones de seguridad o incluso ver si se pone en un servidor corporativo independiente del servidor.

Por lo tanto, nos podemos encontrar que, en lugar de ser imprescindible distribuir la información en particiones, se tenga que distribuir en discos dentro del mismo servidor.

La relación de aplicaciones, la necesidad de información, el número potencial de usuarios y su nivel de concurrencia determinan la distribución de los discos duros que instalaremos en los servidores.

2.2. Acceso a la información

La información almacenada en los servidores se entrega a los usuarios mediante peticiones por la red.

Esquema de acceso a la información

La estructura física del disco hace que sólo pueda servir una información cada vez; por lo tanto, las diversas peticiones de lectura que se hacen al disco se ponen en cola. Este problema puede llegar a ser muy grave y moderar el rendimiento del servidor.

Ved también

Ved el módulo "Administración de servidores". Se habla de cómo se puede optimizar el problema del rendimiento del hardware del servidor.

Para evitar este problema, desde el punto de vista del diseño hay bastante con distribuir la carga de peticiones a discos o controladoras diferentes (dependiendo de la tecnología que se utilice), hacer peticiones paralelas y, a ser posible, no tener colas de peticiones paradas ni colapsadas. Si el problema es crítico, se puede llegar a tener que plantear soluciones de tipos servidores redundantes.

Detectar el problema del servidor

Los problemas del servidor son difíciles de detectar, porque normalmente se asocian a problemas de red, ya que la percepción del administrador de sistemas y la de los usuarios es que las peticiones de las estaciones de trabajo tardan más de lo normal en ser atendidas. El análisis del tiempo de respuesta del disco es correcto. Cuesta mucho detectar que en realidad se hacen demasiadas peticiones al disco.

Una vez más, con la lista de aplicaciones que tiene que haber en el servidor, tenemos que ver cuántos usuarios concurrentes tendrá cada uno para valorar la carga.

Hay que hacer lo mismo con la información de los servidores. Si hay aplicaciones o información con un gran volumen de accesos concurrentes, son candidatas a ir a otro disco o incluso a otra controladora de disco. Si la cantidad de peticiones puede llegar a ser tan crítica, entonces tienen que ir en otro servidor independiente.

Servidores web de intranets

Uno de estos casos son los servidores web de intranets que acceden a bases de datos de la organización. Se tiene que ir con cuidado con las cargas de disco. Una de las primeras soluciones es ponerlo todo sobre la tecnología más rápida –tecnología Small Computer System Interface (SCSI)– para evitar que el disco se convierta en el cuello de botella del sistema. Tampoco se descartan soluciones *Redundant Array of Inexpensive Disks* (RAID) ni de servidores redundantes.

El acceso a la información se puede convertir en un problema si no miramos a fondo cuántos usuarios simultáneos intentan acceder a un dispositivo.

El volumen de la empresa o entidad y el tipo de negocio o actividad, marcará un poco la cantidad de servidores y de discos necesarios.

2.2.1. Privilegios

El sistema de ficheros sobre el que se instale la información tiene que permitir seguir la estructura que se ha diseñado con los usuarios. Es decir, si hay grupos de usuarios y permisos sobre las aplicaciones, además de poder incluirse en el sistema operativo de los clientes y de los servidores, también se tienen que poder incluir en los sistemas de ficheros. Eso permite una seguridad adicional en el sistema, porque no forma parte de él solamente el sistema operativo, sino que el mismo sistema de ficheros la lleva "integrada".

3. Configuración de estaciones de trabajo

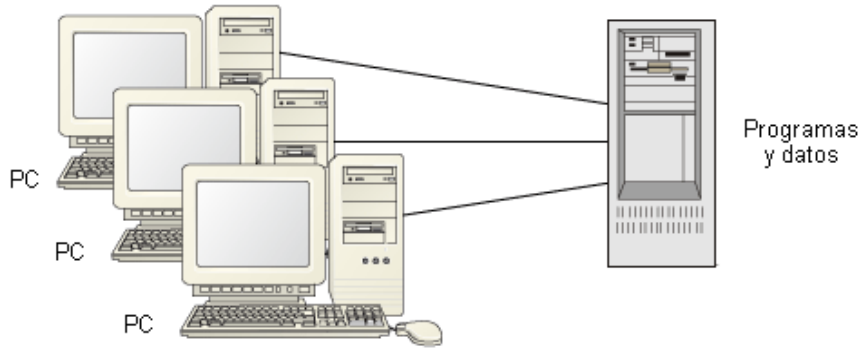
Ya tenemos una idea de las aplicaciones que necesitan los usuarios y sabemos bastante bien con qué permisos tienen que funcionar, y cuáles de estas aplicaciones lo harán en el servidor y cuáles en la estación de trabajo. El problema que hay que resolver ahora es decidir dónde estarán guardadas las aplicaciones que hemos decidido que funcionarán en la estación de trabajo. Pueden estar en el servidor (se verán como una unidad compartida, por ejemplo) o las podemos instalar en cada estación de trabajo.

El objetivo básico para tomar estas decisiones es conseguir que el mantenimiento de las estaciones de trabajo sea lo más sencillo posible.

3.1. Aplicaciones comunes en el servidor

Cuantas menos cosas haya en el disco del usuario, menos peligro hay de pérdida de información y de tiempo para recuperar el equipo.

El almacenaje en el servidor evita la pérdida de información



Por lo tanto, aparentemente "volvemos atrás" en una situación en que todo está en los servidores y las estaciones de trabajo se convierten en "terminales" o dispositivos "no inteligentes".

Esta tendencia pretende ponerlo todo en los servidores para evitar la pérdida de información (ya que ahora está toda en los servidores) y de tiempo para poner en marcha una estación de trabajo, dado que sólo tiene el sistema operativo, porque todas las aplicaciones están en los servidores.

Ved también

Ved, en el módulo "Administración de los datos", algunos criterios para decidir dónde guardar información.

Esta estructura presenta muchos problemas, algunos de los cuales son los siguientes:

- Se colapsan los servidores.

- Se colapsa la red.
- El sistema global va lento.
- Los usuarios tienen muchas quejas del rendimiento general del sistema.

A pesar de todo, tiene algunas ventajas:

- Como no hay nada en los discos de los usuarios, deja de ser peligroso que haya algún problema en las estaciones de trabajo.

- Todo el control de las cosas está en los servidores y, por lo tanto, no hay peligro de problemas y desastres que provengan de los clientes.

- Tampoco hay problemas de fallos en la seguridad si todo se encuentra en los servidores.

- Toda la información está en los servidores.

Con todo, no es una estructura que se utilice en la práctica, ya que los inconvenientes que presenta superan con creces a las ventajas. No obstante, la idea es válida para la instalación de algún software específico en que pueda ser necesario. Se instala todo en el servidor y es ejecutado remotamente por los clientes. Valorando la necesidad y las cargas que puede comportar en red, en servidor y en tiempo de ejecución, se utiliza como solución puntual, no como solución generalizada.

3.2. Aplicaciones comunes a los clientes

Intentamos aplicar los criterios siguientes:

- Todas las estaciones tienen lo mismo en sus discos duros (eso simplifica las instalaciones).

- Todas las estaciones tienen el software de base, que comprende el sistema operativo, los paquetes de ofimática y el software que utiliza toda la organización.

Diseñar con estos criterios tiene bastantes ventajas. He aquí algunas:

- Descarga mucho el tráfico de la red.

- Aumenta mucho la velocidad de ejecución del software de las estaciones de trabajo, ya que ahora la mayoría de aplicaciones se ejecutan en local.

- Mejora bastante el rendimiento general del equipo.

- El servidor sólo guarda los datos y los programas especiales (esto último si hace falta).

Por lo tanto, los usuarios no tendrán la sensación de una red pesada y lenta, porque muchas aplicaciones y utilidades funcionarán en la estación de trabajo sin pedir nada al servidor. Hay que decidir si los datos los guardará en local (en el disco duro) o en la red (en una unidad compartida o en un espacio privado del usuario dentro del servidor).

Espacio para el administrador del sistema

Tiene que haber una parte del disco del servidor, que no tiene que ser visible para los usuarios, exclusivamente reservada al administrador. Esta parte del disco se utilizará para rehacer las estaciones de trabajo en caso de desastre y cuando se tengan que hacer reinstalaciones. La recuperación de estaciones de trabajo es una parte de la administración de usuarios que tiene que estar prevista, ya que cuando el número de estaciones de trabajo es considerable, es una actividad prácticamente diaria.

En los discos de los clientes instalamos el software que tienen todos los ordenadores.

3.3. Creación de la estación modelo

Teniendo claro qué aplicaciones se instalan en local y cuáles en remoto, en este punto la tabla de aplicaciones tendría que estar completa.

Ahora, ya podemos proceder a crear el ordenador modelo de la estación de trabajo que se quiere poner en la organización. A grandes rasgos, el procedimiento es el siguiente:

1) Instalamos el sistema operativo.
2) Instalamos las aplicaciones.
3) Instalamos a los clientes de las aplicaciones que funcionan en remoto.
4) Configuramos todas las opciones del sistema operativo para ajustarlo a las necesidades de la organización.
5) Lo tenemos que probar durante un tiempo.

Cuando se han hecho las pruebas con todos los grupos de usuarios, privilegios, aplicaciones, etc. y la estación de trabajo nos ha funcionado correctamente, daremos por acabada la estación modelo.

El ordenador modelo es el diseño de software y configuración que queremos que tengan todos los ordenadores de la organización.

Su diseño tiene que ser muy esmerado y hace falta tener en cuenta muchos puntos, como por ejemplo:

- **Entorno de usuario**. Qué se encontrará cuando ponga en marcha el ordenador. Qué le preguntará, qué ventanas y qué colores tendrá. Qué podrá modificar del entorno.

- **Red**. Cómo se identifica la red. Qué podrá hacer dentro de la red, qué grupos de usuarios habrá y qué permisos tendrá.

- **Software**. Qué aplicaciones tendrá disponibles. Qué aplicaciones estarán en local y cuáles en remoto. Dónde estará el correo electrónico.

- **Facilidad de uso**. Todo tiene que estar pensado para facilitar la labor del usuario y hacer que se acostumbre rápidamente a esta herramienta de trabajo. Tiene que servir para mejorar el rendimiento.

- **Información**. Una vez que el administrador haya decidido dónde se guardan los datos y con qué formato, para el usuario eso tendría que ser tan automático y transparente como fuera posible, de manera que no se tenga que preocupar por el sitio real donde están los datos.

Todo ello conlleva que sea necesario diseñar un ordenador modelo y, posteriormente, clonarlo tantas veces como ordenadores haya en la organización, y si hace falta después ajustaremos el ordenador clonado al puesto de trabajo al cual se destina.

Los pasos, a grandes rasgos, son los siguientes:

1) Preparamos la estación de trabajo modelo. Es decir, configuramos un ordenador tal como queremos que sean todas las estaciones de la organización, con el software, las protecciones, las particiones de disco, la configuración de red, etc. La probamos a fondo para ver si todo funciona correctamente.

2) Con el software de clonación de discos duros por red clonamos el disco del ordenador modelo y guardamos la imagen en el servidor. Normalmente, esta imagen puede ocupar algunos GB, y la tendríamos que guardar en un servidor.

3) El software de clonación puede crear un cliente en un disquete para restaurar una imagen clonada desde el servidor en una estación de trabajo. Con esta operación podremos obtener una estación de trabajo con el software, las protecciones y la configuración de red que habíamos establecido en el ordenador modelo, ya que será una duplicación.

4) Finalmente, tenemos que ajustar la configuración de este ordenador para el usuario y/o el puesto de trabajo a que se destina.

Para la administración del sistema informático, la situación ideal es que todas las estaciones de trabajo sean homogéneas en software y hardware. Que lo sea el hardware facilita la compra, las reparaciones, el recambio y la sustitución

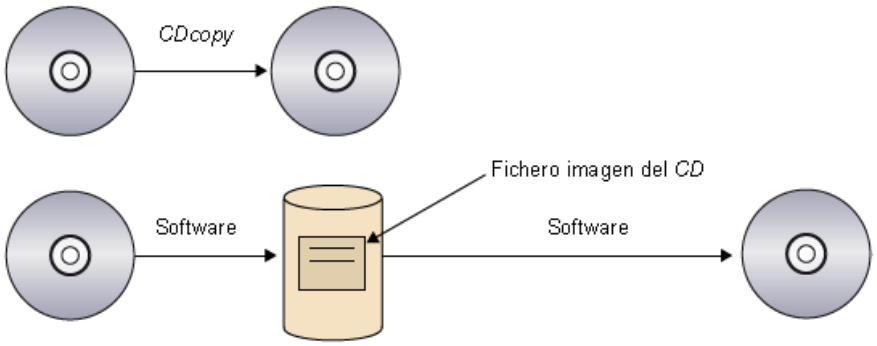
de material, ya que con el tiempo los ordenadores se estropean y necesitan reparaciones. Como en la práctica eso es imposible, al menos tiene que ser un objetivo (que no se alcanzará nunca).

Lo mismo pasa con el software, que también tendría que ser homogéneo, pero eso tampoco es posible en la práctica, sino que es un objetivo que nunca se llega a alcanzar.

3.3.1. Imágenes de disco

Más o menos, todo el mundo conoce alguna utilidad para copiar disquetes o CD/DVD. La utilidad nos permite hacer una copia exacta del CD en otro CD. De esta manera, si desgraciadamente se estropea el disco original, tenemos la copia, que es un duplicado exacto del original. De alguna manera es la idea de la fotocopia en papel. Un duplicado del original. Ahora bien, ¿qué pasa si queremos hacer un duplicado de un CD pero no tenemos un segundo CD para hacerlo? Hay software que permite hacer una copia del CD, pero en lugar de archivar el resultado en un CD (el copiado), lo ponen en un fichero. Este fichero no lo podemos leer ni escribir, ni tan sólo ejecutarlo como un CD directamente. Se tendrá que crear el CD de copia o usar unos programas que simulan tener el CD puesto en un lector.

Proceso de duplicación de un CD mediante una imagen



Con este software podremos hacer tantos duplicados de nuestro CD como queramos, sin necesidad de tener el CD original, porque el fichero creado lo podemos tener guardado en el disco duro tanto tiempo como sea necesario. Al fichero guardado en el disco duro se le llama **imagen de CD**.

Una imagen de CD puede parecer una cosa poco útil, pero lo es mucho si pensamos que podemos hacer lo mismo con todo un disco duro. Podemos hacer una imagen de un disco duro[3], y es muy útil.

(3)Hacer una imagen o copia de un disco duro también se llama clonar un disco duro.

Con el procedimiento de hacer una imagen de un disco duro obtenemos un fichero muy grande (del orden de varios GB) que contiene la imagen del disco duro que hemos copiado. Si tenemos la desgracia de que se estropea el disco duro original (desde el punto de vista de software, es decir, se desconfigura o

se degrada el sistema hasta el punto de que hace falta reformatear el disco o reinstalar el sistema), se puede **restaurar la imagen del disco** en el disco duro, de manera que en pocos minutos el disco duro y, por lo tanto, el ordenador, vuelve a ser completamente funcional.

El único requisito necesario para hacer una imagen de disco es un software que cree el fichero imagen en algún lugar. Lógicamente, no podemos crear la imagen del disco en el mismo disco. Si queremos poner la imagen del disco dentro del mismo disco físico, se tiene que poner en una partición diferente. En caso de un fallo físico o mecánico del disco, no podremos recuperar la imagen, por lo cual no es la solución más recomendable. Otros sitios aconsejables son los siguientes:

- En el servidor, en alguna partición o trozo de disco administrativo, que no quede al alcance de los usuarios.

- Generar el fichero imagen y, posteriormente, traspasarlo a un DVD. Después, si se tiene que restaurar la imagen de disco, se puede hacer desde cualquier lector de DVD.

- En una cuenta destinada exclusivamente a tareas de administración de usuarios.

- En un dispositivo externo de cinta magnética del servidor: *Digital Audio Tape* (DAT), *Digital Lineal Tape* (DLT), *Advanced Intelligent Tape* (AIT), etc.

- En dispositivos de copia externa, como unidades USB o similares.

Hay que señalar que, igual que las copias de seguridad, al restaurar las imágenes de disco, el estado de este disco es el mismo que cuando se hicieron, por lo que los datos posteriores a la realización de la imagen se habrán perdido. En este caso, se tendría que recurrir a copias de seguridad para recuperar la información. Por ello, una de las grandes utilidades de las imágenes de discos es hacer **ordenadores modelo**.

4. Mantenimiento de las estaciones de trabajo

Por mantenimiento de estaciones de trabajo entendemos todas las acciones necesarias para que el equipamiento esté en óptimas condiciones de funcionamiento para el usuario final.

En la práctica, el mantenimiento de las estaciones de trabajo se divide claramente en dos partes muy bien diferenciadas. La primera es el mantenimiento del equipamiento del usuario (tanto el hardware como el software), y la segunda son las tareas necesarias para que el sistema funcione correctamente.

4.1. Mantenimiento del equipamiento

Una de las partes importantes de la administración de usuarios es el mantenimiento, la sustitución y/o la actualización del hardware y el software de las estaciones de trabajo. Normalmente, esta parte responde a diversos motivos:

- Darse cuenta, por avería de hardware grave, de que se requiere una sustitución importante del equipo. A veces, es necesaria una reinstalación del software del ordenador.
- Sustituir el ordenador por uno nuevo por actualización del hardware.
- Instalar un hardware por un plan de modernización/actualización.
- Cambiar al usuario de la estación de trabajo y, por precaución, destruir la información y volver a instalar el software de usuario.
- Reinstalar el equipo como consecuencia de haberlo trasladado por un cambio de función dentro de la organización.
- Reinstalar el equipo para un nuevo sistema de funciones dentro de la estructura de la organización.

En la mayoría de los casos, el responsable de informática está enterado y el plan estratégico de la organización es clave para llevar a cabo estas acciones dentro del plan global de la organización. Pero fuera de estos casos, también podemos encontrar situaciones como las siguientes:

- Desconfiguración completa del equipo por virus.
- Borrado del disco por virus.
- Borrado parcial del disco por mal uso involuntario de los usuarios.

- Fallo de la corriente eléctrica que ha provocado una desconfiguración del equipo.
- Fallo de la corriente eléctrica que ha provocado un problema de hardware que obliga a reinstalar el software.

Hay muchas situaciones que pueden provocar que un equipo funcione mal. Ahora bien, de la misma manera que tenemos que tener cuidado en el modo en que se tiene que preparar el equipo para el usuario, también se tiene que hacer bien la recuperación de un equipo ante un desastre que nos deja el ordenador inútil, a fin de que sea operativo cuanto antes mejor. Un buen diseño del equipo modelo nos permite recuperar correctamente los equipos con problemas. El método de disco de imagen/clonación es perfectamente aplicable al mantenimiento de equipamiento, ya que nos permite restablecer, en muy poco tiempo, la operatividad de un equipo que ha dejado de ser funcional para la organización, siempre que sólo se trate de problemas de software. En caso de que los problemas sean de hardware, tenemos que tener una pequeña cantidad de piezas de sustitución para las averías frecuentes y fáciles de reparar (si también queremos dar servicio de reparación de hardware).

Hay una gran cantidad de causas que pueden dejar una estación de trabajo inoperante. Tenemos que estar preparados para las más usuales.

4.2. Extraer datos de un equipo

Hay muchos escenarios de problemas posibles. Muchos tienen solución, incluso sin tener que estar físicamente delante del equipo. Pero hay uno especialmente conflictivo. Aunque hemos procurado que los datos estén en los servidores y que no haya información en las estaciones de trabajo, muchas veces no es así. Si un equipo tiene el sistema operativo corrupto (y, por lo tanto, necesitamos aplicar la técnica de la clonación para restaurar el ordenador y devolverlo al estado original), de manera que no es posible conectarse a la red para copiar la información, y tiene información dentro del disco duro que necesitamos extraer, tenemos que buscar alguna manera de copiarla. Quizás el equipo no es ni capaz de arrancar, pero nosotros, con cualquier método (un DVD, o un lápiz de memoria para arrancar el ordenador, por ejemplo), conseguimos poner en marcha el ordenador y acceder a la información. ¿Cómo la podremos extraer ahora que sabemos que está en buen estado? Hay dos maneras para hacerlo:

1) Mover el disco duro. La idea es sencilla. Extraemos el disco duro del ordenador y lo ponemos en otro ordenador que funcione. Lo instalamos como disco no principal y ponemos en marcha el ordenador. El sistema operativo instalado en el otro ordenador tendría que detectar otro disco duro, y se ten-

drían que ver todos los ficheros de este otro disco duro. Copiamos los ficheros que nos interesan en el disco duro principal, y después ya podremos hacer la operación de clonación sobre este disco duro (que destruirá el contenido).

2) Utilizar una unidad DVD, Blu-Ray o *Lineal Tape Open* (LTO). Si se ha hecho todo el diseño de servidores, los discos de los usuarios contienen poca información. Eso permite, con los dispositivos de memoria masiva de reducidas dimensiones y gran capacidad, hacer fácilmente una copia de seguridad de los datos. Por lo tanto, el procedimiento es el siguiente. Una de estas unidades (una grabadora Blu-Ray2 de 50 GB, por ejemplo) se conecta en el puerto USB. Se arranca el ordenador con un lápiz de memoria, y desde este mismo lápiz se hace reconocer el dispositivo Blu-Ray. Por lo tanto, se tiene configurada una unidad, como un disco duro más, de capacidad 50 GB. Ahora, como se puede acceder al disco duro, es posible copiar en cada Blu-Ray hasta 50 GB. Una vez se ha hecho la copia, se puede proceder a reparar el equipo. Mientras tanto, por ejemplo, se puede poner esta información en el espacio del usuario del servidor. De esta manera, tan pronto como esté solucionado el problema, encontrará la información que, lógicamente, se tendrá que volver a colocar en el sitio adecuado.

Esto implica tiempo y presupuesto para tener estas herramientas adicionales y poder realizar este mantenimiento y recuperación de datos en el menor tiempo posible y con la pérdida mínima de información.

Ante un ordenador que tiene información y no se pone en marcha, tenemos que buscar maneras de extraer esta información importante.

4.3. Tareas periódicas de mantenimiento

Las tareas periódicas de mantenimiento son muy importantes para el funcionamiento correcto del sistema global, pero no responden a ninguna situación extraordinaria. Se tienen que hacer forzosamente cada cierto tiempo y la mayoría son transparentes para el usuario, el cual sólo sabe que están cuando no funcionan correctamente.

4.3.1. Mantenimiento en el servidor

Tal como ya hemos dicho, hay una serie de tareas que se sitúan en una línea divisoria muy fina. ¿Son responsabilidad del administrador de usuarios o del administrador de servidores? Afectan al servidor, pero muy directamente al usuario. Estas tareas son:

- **Controlar que no se llenen los buzones de correo de los usuarios**. Generalmente, hay un guión[4] que permite controlar el espacio de los buzones de los usuarios, y en caso de que alguno esté lleno, y antes de que el

(4)En inglés, *script*.

servidor de correo se colapse por falta de espacio, se avisa al usuario (o usuarios) para que haga limpieza de los correos. Esta tarea se tiene que llevar a cabo periódicamente.

- **Controlar que no se llenen los directorios de los usuarios.** Con el mismo criterio de antes, hay que evitar quedarse sin espacio en la partición de usuarios. Se tiene que vigilar periódicamente la medida de esta partición. También hay que avisar a los usuarios de los directorios que sobrepasan un tamaño para que hagan limpieza.

4.3.2. Virus

Los virus son uno de los problemas con que se enfrentan todos los administradores de usuarios. Hoy hay antivirus que funcionan de una manera centralizada, es decir, se instala el antivirus servidor en un ordenador que hará el papel de "servidor", se definen ordenadores, usuarios, permisos, etc., y cuando el usuario entra dentro del sistema, automáticamente, se instala el software antivirus en el ordenador. El administrador actualiza diariamente el **fichero de firmas** del antivirus, que se actualiza automáticamente en todos los ordenadores de la organización cuando el usuario se identifica. También actualiza periódicamente el software, el cual, siguiendo el mismo procedimiento, se actualiza en toda la organización.

Ved también

Ved en el módulo "Administración de la seguridad" más información sobre los virus.

Cuando se pone en marcha, el programa antivirus se dedica a controlar toda la información que entra en la estación de trabajo (especialmente por Internet), por correo electrónico, y a buscar constantemente virus en el sistema de los discos locales de la estación de trabajo. ¿Qué pasa si los encuentra?

- Los puede eliminar.

- No los puede eliminar. En este caso, quizás propone borrar el fichero. Si el fichero es crítico para el sistema operativo (muchas veces el usuario no lo sabe), puede ser que borrarlo sea peligroso para su funcionamiento, por lo cual en estos casos lo mejor siempre es avisar al administrador de usuarios.

Sea como fuere, si detectamos o sospechamos que hay virus en nuestro ordenador es conveniente avisar telefónicamente al administrador de usuarios, porque tiene conocimiento de la peligrosidad y la capacidad de propagación del virus. Si el antivirus lo ha eliminado y no decimos nada, puede ser una medida insuficiente, porque el virus ya se puede haber propagado por la organización (o todavía peor, haber salido fuera).

Éste es el mensaje que hay que difundir a los usuarios, para evitar propagaciones. Como en muchos casos, se los tiene que educar en el uso de herramientas informáticas.

4.3.3. Control remoto

El control remoto es un software fundamentado en la tecnología cliente/servidor que permite acceder, mediante la red, a un ordenador físicamente distante, y acceder a sus datos, administrar su sistema y facilitar la ayuda a sus usuarios ante posibles problemas.

Ved también

Ved el apartado 6 dedicado al centro de atención al usuario.

Siguiendo la tecnología cliente/servidor, este software tiene su parte servidora en la estación de trabajo del usuario dedicada a servir las órdenes dictadas desde la estación cliente situada en la estación de trabajo del administrador de usuarios.

Gracias a su gran utilidad, el software de control remoto ha incorporado nuevas capacidades como: busca de elementos dentro de la red, autoinstalación en estaciones servidoras, conexiones compartidas en estaciones de trabajo, facilidad de transferencia de datos y muchas otras.

Hay, pues, muchas ventajas que recomiendan la utilización del control remoto:

- **Económicas**. Gracias a la reducción de personal, de tiempo y de desplazamientos, la recuperación de la inversión está garantizada.

- **Trabajo a distancia**. Permite trabajar a distancia, flexibilizando tareas específicas, por ejemplo en fines de semana vía teletrabajo.

- **Asistencia rápida y eficaz**. Mejora mucho el apoyo al usuario, ya que permite a los técnicos acceder al sistema y comprobar personalmente los problemas existentes. A su vez, permite solucionarlos sin necesidad de desplazamientos.

- **Formación**. Permite formar remotamente mediante la conexión compartida a una estación de trabajo.

- **Mantenimiento**. Mejora sustancial en el mantenimiento de las estaciones de trabajo.

Hay, sin embargo, aspectos que pueden dificultar las tareas del administrador:

- **Seguridad**. La información entre estación cliente (servidor) y estación administradora (cliente) se realiza mediante la red. Si ésta no es segura, compromete el control.

- **Recursos de red**. Consumen un ancho de banda importante al viajar por la red las pantallas de las estaciones de trabajo. El software de control remoto

incorpora herramientas que permiten escoger la resolución y el color de la pantalla para evitar el consumo desmesurado.

- **Comunicación específica**. La comunicación se establece por puertos que, muchas veces, no son visibles desde redes remotas debido a la existencia de elementos de red que impiden la comunicación. Normalmente por seguridad.

- **Aspectos legales**. Muy importantes, se podría incurrir en incumplimientos de la normativa legal si el usuario no es avisado sobre la conexión en su estación de trabajo. Se podría violar su derecho a la intimidad.

Este software, que se utiliza mucho en organizaciones, pretende mejorar el servicio que se da al usuario.

4.3.4. Actualización diferida

Cuando hay instalaciones geográficamente alejadas o un número elevado de estaciones de trabajo, ¿cómo podemos actualizar un software que está en las estaciones?

Hay software capaz de hacerlo. Permiten seleccionar el software y las estaciones de destino, y proceder a la actualización masiva, sin tener que trasladarnos físicamente delante de ningún equipo o tener que hacer la operación y repetirla cada vez.

4.4. Documentación y procedimientos

Uno de los aspectos que a menudo se olvida es la documentación y los procedimientos. Los procedimientos son una cuestión de documentación técnica para los administradores de sistemas.

4.4.1. Procedimientos

Dado que hay muchos usuarios, muchas de las tareas acostumbran a ser repetitivas, mucho más que en la administración de servidores. Esto hace que a menudo sea conveniente describir los pasos para hacer una tarea, ya que a veces consta de muchos pasos y, aunque se hace muchas veces, se lleva a cabo en intervalos de tiempo lo suficientemente espaciados para que se olvide. A este conjunto de pasos para hacer una tarea lo llamamos procedimiento, y para que nos sea sencillo llevarlo a término, cuando se tenga que hacer, lo tendremos escrito, es decir, documentado.

La definición formal (algorítmica) de procedimiento es la siguiente: descripción no ambigua y precisa de acciones que hay que llevar a cabo para resolver un problema bien definido en un tiempo finito.

La **acción** es el acontecimiento finito en el tiempo y que tiene un efecto definido y previsto. El **proceso** es la ejecución de una o diversas acciones.

Adaptándola a nuestras necesidades de este momento, podemos dejarla de la manera siguiente:

> Un procedimiento es una descripción del conjunto de acciones para hacer una tarea determinada.
>
> Todos los procedimientos tendrían que estar reflejados en un documento.

Formato de un documento

Un documento puede estar en formato papel, HTML o cualquier otro.

Por lo tanto, cada uno de los procedimientos tendría que estar escrito en un documento. De esta manera, cada vez que tengamos que hacer cualquier tarea, sólo habrá que consultar este "manual de procedimientos" y hacer las acciones que hay especificadas para llevar a cabo la tarea encomendada.

Hay muchas maneras de tener recogida esta información. Una es en forma de preguntas más frecuentes (FAQ[5]), colgada en formato HTML en algún servidor web, de manera que el personal técnico la puede consultar en cualquier momento y desde cualquier sitio. Muchas veces, junto con los documentos, se adjuntan ficheros, porque el formato de web permite transferir ficheros al mismo tiempo.

(5)FAQ es la sigla de la expresión inglesa *frequently asked questions*.

Ejemplos de procedimientos

Los siguientes son ejemplos de procedimientos:

- Dar de alta a un usuario.
- Configurar una impresora.
- Configurar una estación de trabajo.
- Configurar el correo electrónico.
- Restaurar una imagen en una estación de trabajo.

Ninguna de estas tareas se puede hacer con una sola acción. Hay que tener presente que algunas veces un procedimiento puede implicar acciones sobre el servidor y sobre la estación de trabajo.

4.4.2. Software

De la misma manera, de todo el software que se utiliza, el administrador de usuarios tendría que procurar que los usuarios tuvieran acceso a algún tipo de documentación (en algún formato) sobre la utilización de este software. Esto facilita el hecho de poder conocer las herramientas con que trabajan. Es mejor que la documentación esté en diversos formatos a la vez. En cualquier caso, tiene que ser fácilmente accesible para los usuarios. También es muy interesante poder tener tutoriales de este software. Muchos programas los incorporan, pero otros se pueden encontrar gratuitamente incluso en Internet.

Es importante poder facilitar documentación a los usuarios sobre las herramientas que utilizan. Su percepción es que los administradores se preocupan por ellos. A pesar de todo, no se tiene que olvidar la formación, ya que esto no pretende sustituirla, sino complementarla.

5. Formación del usuario

Un aspecto a menudo olvidado en las organizaciones es el plan de formación de los usuarios, que tiene que ser dirigido por el responsable de informática con las directrices de la organización y el plan estratégico.

Las ventajas de un plan de formación se pueden resumir en las siguientes:

- Mejora del uso de las herramientas de software.
- Aumento de la efectividad y la eficiencia del personal.
- Disminución de las incidencias en el departamento de informática.
- Satisfacción del personal.
- Disminución de costes del departamento de informática.

Algunas de las consecuencias indirectas son las siguientes:

- Detección de nuevas necesidades informáticas en la organización.

- Aumento de la información en los sistemas informáticos. Esto permite nuevos métodos de busca de datos para tomar decisiones en los estamentos directivos.

Nadie nace enseñado

De la misma manera que para conducir un coche nos tienen que formar (y al final nos dan un título que reconoce los conocimientos que tenemos), para poner en marcha un teléfono móvil o una lavadora también nos tienen que explicar cómo funciona como usuarios, es decir, de una manera simple, didáctica y sin tecnicismos.

Muchas organizaciones tienen la sensación de que un plan de formación es malgastar el tiempo, pero no seguirlo ocasiona los problemas siguientes:

- Pérdidas de tiempo de los usuarios que se enfrentan a software o hardware nuevo sin conocimientos y, por lo tanto, la curva de aprendizaje es muy elevada.

- La probabilidad de error en esta fase de autoaprendizaje es muy importante, con consecuencias de tiempo y de coste para solucionarlo impredecibles.

- Las probabilidades de que los errores involuntarios produzcan problemas, fallos, malos funcionamientos, desconfiguraciones, etc. en los equipos y/o servidores es alta, con el tiempo y el coste para el personal del departamento informático que ello puede comportar.

- La posibilidad de que gran parte del volumen de trabajo (se puede llegar a una situación de colapso) del departamento de informática se deba a problemas indirectos de formación del personal se tiene que tener en cuenta.

- El desconcierto, las quejas, la sensación de mala instalación, de software o hardware incorrecto o defectuoso, que no se ajusta a las necesidades reales

de la organización, es muy posible que aparezcan, con el peligro de poder hacer fracasar planes de informatización o planes de actualización que se intenta llevar a cabo.

Todo eso tampoco quiere decir que el plan de formación tenga que ser siempre igual y general para todo el mundo. Un buen plan de formación está estudiado y se tiene muy en cuenta qué se explica y a qué colectivo se explica.

La misma aplicación genera cursos de formación diferentes para colectivos diferentes de la misma empresa u organización.

Formación diferente para colectivos diferentes

Una aplicación de nóminas integrada tendrá un cursillo de formación diferente para el departamento de recursos humanos, para el de contabilidad, para todos los trabajadores que tienen que fichar a la entrada y a la salida, y que pueden consultar por medio de una web de la intranet su registro de entradas y salidas, etc. Finalmente, como es lógico, el cursillo de formación para el departamento informático sobre esta aplicación también tiene que ser diferente.

Así, pues, hay diversos planes de formación: para actualizaciones, para implantación de software nuevo o para usuarios nuevos.

1) Planes de formación para actualizaciones

Los planes de formación para actualizaciones se limitan, simplemente, a poner al día a los usuarios sobre cambios que se han hecho en el software y/o hardware. Son cortos, y permiten tener la plantilla al día. Una gran ventaja es que evitan bastantes problemas en el departamento informático.

Implantar software

Implantar software puede ser desarrollar una aplicación nueva dentro de la misma organización, subcontratarla o instalar un software estándar (parametrizable).

Son muy cortos (por este motivo, muchas veces también se llaman *sesiones*, *seminarios*, *cursillos*, *charlas*, etc.). Tienen otra función secundaria muy importante, que es mantener la imagen del departamento de informática de preocupación por los usuarios.

2) Planes de formación para implantación de software nuevo

Son realmente los más complejos, ya que normalmente se tienen que hacer sesiones previas para escuchar las ideas, las sugerencias y las propuestas del colectivo implicado, y todo eso integrarlo en el software que se está implantando. Lo más complejo de estas sesiones es que implantar sistemas nuevos implica cambiar procesos y maneras de trabajar, y generalmente eso les cuesta aceptarlo a los colectivos de usuarios. Es mejor hablar de ello en esta fase porque:

- Los usuarios sienten que ellos participan en el proyecto, y eso les predispone más a aceptarlo.

- Es más fácil cambiar la oposición inicial si se argumentan las ventajas que obtendrán con el nuevo sistema (que todavía no tienen y, por lo tanto, continúan trabajando de la manera usual) y se dice que las propuestas que se hagan se tendrán en cuenta en el desarrollo del proyecto.

- Se pueden argumentar los inconvenientes del método de trabajo actual, porque como lo siguen cada día, y todavía lo harán durante un cierto tiempo, se darán cuenta de la diferencia.

- Como no es un sistema impuesto, sino que se hace participar en él para conseguir que sea ágil, útil y cómodo para los usuarios, se evita la sensación de que tendrá errores básicos.

- Se tienen que pedir opiniones, propuestas, ideas, quejas, etc. sobre cómo tendría que trabajar el sistema. Pero también se tiene que dejar claro que no siempre es posible hacer todo lo que se pide y que, por lo tanto, no se podrán llevar a cabo todas las peticiones.

Una vez desarrollado el software, se tendría que hacer una formación piloto en un grupo representativo. Esto serviría para ajustar el plan de formación y para detectar y corregir anomalías en los procedimientos de instalación y configuración.

Si todo va bien, después se puede formar a los usuarios y, seguidamente, instalar el software. De esta manera, tan pronto como lo encuentren instalado en las estaciones de trabajo, lo podrán empezar a utilizar sin que les sea extraño y sin causar incidencias motivadas por el desconocimiento del software.

3) Planes de formación para usuarios nuevos

El plan de formación para usuarios nuevos tiene que ser un cursillo con un fuerte componente estándar, porque implica básicamente enseñar a los usuarios toda la operativa común que se utiliza en la organización. Haciéndolo de esta manera, se evitan muchos errores y se gana mucho tiempo, ya que se familiariza al usuario con el entorno de trabajo con el que se encontrará. A ser posible, se tendría que hacer un pequeño apartado más específico para el puesto de trabajo que tendrá que ocupar, qué herramientas específicas utilizará y cómo, qué bases de datos utilizará, etc.

Es muy importante para los responsables del departamento de informática y para los propietarios y gerentes de las empresas reducir al máximo los problemas de usabilidad que se encuentran los usuarios con los cambios de programación. Es importante hacer cursos de formación continuada a los trabajadores.

6. Centro de atención al usuario

Hoy en día, la gran mayoría de las empresas disponen de servicios de tecnología de la información (TI) con las cuales sus empleados tienen que interactuar en mayor o menor grado. Estos empleados son simplemente usuarios de una tecnología cuyos fundamentos no tienen por qué conocer. Los servicios TI son para estos empleados una herramienta, indispensable en muchos casos, que tiene que estar disponible el mayor tiempo posible.

¿Qué sucede cuando uno de estos servicios o herramientas no trabaja correctamente, o simplemente no trabaja? El usuario detecta un problema o incidencia en una de sus herramientas, pero no tiene una noción clara (ni una explicación técnica) de lo que pasa.

Para el usuario, el ordenador es una herramienta para aumentar su grado de organización y/o eficiencia y no tiene la necesidad de conocer los detalles técnicos del equipamiento que utiliza.

Objetivo de un buen sistema informático

De la misma manera que un usuario utiliza un fax, una fotocopiadora, el coche, un ascensor o el cajero automático sin conocer su funcionamiento interno, éste tendría que ser el objetivo de un buen sistema informático desde el punto de vista del usuario.

En este punto, aparece el concepto de centro de atención al usuario (CAU[6]) para resolver la siguiente pregunta que nos podemos formular. Si el usuario detecta un problema en una herramienta y no tiene los conocimientos necesarios para solucionarlo, ¿qué tiene que hacer?

[6]El centro de atención al usuario (CAU) a veces también recibe el nombre de HelpDesk.

Cuando un usuario tiene un problema informático, se tiene que dirigir a un único punto para resolverlo, el centro de atención al usuario.

Un CAU es un servicio integral que, mediante un punto de contacto, ofrece la solución de incidencias y atención de requisitos relacionados con las TI[7], como son: computadores, periféricos, recursos informáticos, software y plataformas sobre las que trabajan la mayoría de las organizaciones.

[7]TI es la sigla de *tecnologías de la información*.

El CAU tiene una función importante en la provisión de los servicios TI. Es un único punto de acceso para los empleados o usuarios que necesitan ayuda. Sin un CAU, una organización ciertamente podría afrontar pérdidas debidas a la ineficiencia.

Aunque hay diferentes tipos de CAU, como los Call Center, CAU expertos, y otros, en este apartado comentaremos el más común de todos, el **CAU de tres niveles**.

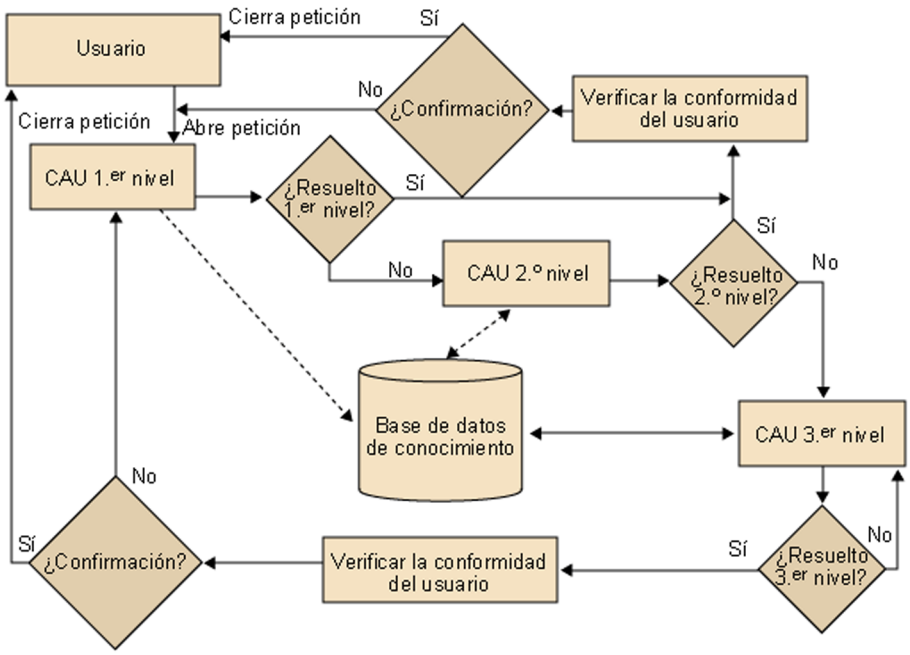
Cuando un usuario detecta un problema, se pone en contacto con el punto central de apoyo, ya sea por teléfono, por correo u otros métodos. En este punto, su petición será recibida por el **primer nivel** de apoyo, que registrará sus datos, el problema y abrirá una **petición**.

Una vez abierta la petición, el primer nivel intentará resolver la petición revisando la **base de datos de conocimiento**, donde se encontrará la información y métodos de resolución de incidencias ya tratadas o comunes. Si el primer nivel puede resolver la petición, la verificará con el usuario y la cerrará. Si no puede solucionar la petición, será asignada al segundo nivel.

El **segundo nivel**, formado por personal con un perfil técnico más avanzado y especializado (redes, servidores, software), intentará resolver la petición. Si el técnico asignado puede resolver la petición, la verificará con el usuario y la cerrará; además, actualizará la base de datos de conocimiento para futuras consultas. Si no puede solucionar la petición, la asignará al **tercer nivel**.

Este último nivel es el más especializado y, muchas veces, es personal externo a la organización. Éstos resolverán la petición, la comunicarán al usuario y actualizarán la base de datos de conocimiento para que esta información sirva en futuras consultas.

Esquema de funcionamiento de un CAU de tres niveles



Así pues, cada nivel de un CAU tiene asignadas funciones específicas. Las podemos resumir en:

1) Primer nivel. Según el esquema presentado y la funcionalidad del CAU, el primer nivel de asistencia tendrá que gestionar las siguientes actividades:

- Recibir las incidencias de los usuarios, ya sea vía telefónica, correo electrónico o software específico.

- Crear una petición o ticket en el sistema de control de peticiones. Esto es imprescindible para una buena gestión y seguimiento de las incidencias.

- Clasificar la petición o incidencia, especificando el grupo afectado: comunicaciones, servidores u otros.

- Priorizar la petición o incidencia según su criticidad, que puede venir dada por el número de usuarios afectados, por la afectación a los sistemas productivos y otros dependiendo de la organización.

- Escalar la petición al grupo adecuado de segundo nivel si es necesario.

- Buscar información de resolución en la base de datos de conocimiento para resolver la petición al primer nivel.

- Actualizar los datos del usuario y del grupo TI si procede.

- Verificar periódicamente el estado de las incidencias abiertas y la comunicación con el usuario.

- Preparar documentación de gestión de la incidencia.

2) Segundo nivel. Tal como se ha dicho en el primer nivel, vamos a comentar las acciones pertinentes a este segundo nivel (técnicos especializados):

- Reclasificar la petición o incidencia si ésta está definida de forma errónea.

- Escalar la incidencia al grupo correcto si ha sido asignada a un grupo erróneo.

- Investigar y resolver la incidencia. Hay que ponerse en contacto con el usuario si es necesario.

- Mantener la base de datos de conocimiento con respecto a la resolución de la incidencia, si se ha podido resolver. Hay que documentar correctamente los pasos a seguir para solucionar una petición como la que se acaba de resolver.

- Desarrollar mecanismos con el fin de evitar peticiones e incidencias como las que se han podido solucionar. Mejora del sistema TI.

- Cerrar la petición o ticket si se ha podido resolver.

- Escalar la incidencia al tercer nivel si no se ha podido resolver.

3) Tercer nivel. En este tercer nivel, encontraremos a los especialistas en cada ámbito que, muchas veces, será personal externo a la organización, y que dará servicio en momentos puntuales ante una petición o problema de un nivel de resolución muy alto.

- Reclasificar la petición o incidencia si ésta está definida de forma errónea.

- Investigar y resolver la incidencia. Hay que ponerse en contacto con el usuario si es necesario.

- Mantener la base de datos de conocimiento con respecto a la resolución de la incidencia, si se ha podido resolver. Hay que documentar los pasos a seguir para solucionar una petición como la que se acaba de resolver.

- Desarrollar mecanismos con el fin de evitar peticiones e incidencias como las que se han podido solucionar. Mejora del sistema TI.

- Cerrar la petición o ticket cuando se haya resuelto.

Finalmente, alguna persona se tiene que encargar de ver diariamente qué incidencias hay pendientes y hacer el seguimiento del estado en que las tienen los técnicos. Normalmente lo hace la persona del primer nivel del CAU, ya que de esta manera está en contacto con los técnicos para consultar el estado de las incidencias, actualizar la base de datos, si hace falta, e informar al usuario. Mantener al usuario informado sobre el estado de la incidencia (especialmente si es compleja y/o larga de resolver) es importante para tranquilizarlo y comunicarle el sentimiento de que el departamento de informática se preocupa por su problema.

Otra función muy importante del personal de atención del CAU es hacer de filtro de las peticiones que están más allá de las funciones o capacidades del departamento de informática o del sistema informático implantado en la organización (eso no quiere decir que no se puedan recoger sugerencias). Sin embargo, el CAU tiene que tener la capacidad de denegar la gestión de incidencias.

Funciones del personal de atención del CAU

Imaginemos que nos encontramos con la siguiente petición de un usuario en el CAU: "Necesito que se instale el programa ABC en mi ordenador". El CAU, sin muchos problemas, encuentra que es un software que no está en la organización. Por lo tanto, esta petición no puede prosperar a través del CAU, sino que como el software se tiene que comprar, ha de ir vehiculado por medio de los jefes de departamento, por ejemplo. Se tiene que explicar así al usuario y, por lo tanto, no se puede atender la petición.

7. Responsabilidades del administrador de usuarios

Una relación aproximada de las tareas/responsabilidades del administrador de usuarios es la siguiente:

a) Configurar los equipos destinados a ser utilizados por los usuarios (estaciones de trabajo).

b) Abrir cuentas.

c) Dar espacio a los usuarios.

d) Dar una cuenta de correo a los usuarios (es decir, dirección electrónica).

e) Dar acceso a las aplicaciones corporativas.

f) Dar acceso a los datos que necesita el usuario (con los permisos que haga falta).

g) Proteger los datos del usuario de accesos no deseados.

h) Asegurar la disponibilidad de su información.

i) Asegurar el acceso a su correo electrónico.

j) Asegurar el acceso a los recursos que necesite.

k) Hacer copias de seguridad de los datos de los usuarios.

l) Mantener y gestionar las instalaciones de hardware de las estaciones de trabajo.

m) Gestionar el CAU.

n) Atender consultas/incidencias/problemas del usuario durante el transcurso del uso del equipamiento.

o) Mantener y gestionar el software de los usuarios.

p) Asegurar el espacio para los datos y para el correo electrónico.

8. Aspectos legales del administrador de usuarios

Los aspectos legales del administrador de usuarios están muy relacionados con la información. Los usuarios tienen unos espacios con su información. Estos espacios son el directorio personal, el correo personal y la agenda, por ejemplo. Cuando hay problemas, el administrador de usuarios puede acceder a estos espacios (como la agenda personal, el correo del usuario, etc.), con el consentimiento de los usuarios.

Nos tenemos que volver a cuestionar dónde están los límites legales de todo ello, y otra vez nos encontramos con que actualmente la cuestión va cambiando y que la legislación se mueve bastante.

Ved también

Con respecto a los aspectos legales, ved el módulo "Administración de la seguridad".

Tenemos que ser muy conscientes de que, en el momento en que surja el problema de verdad, tendremos que buscar asesoramiento legal para resolverlo, pero pensamos que es muy importante saber reconocer el problema real en una situación.

Resumen

Hemos visto que el usuario es una de las partes que da sentido al sistema informático. Sin usuarios, la mayoría de sistemas informáticos no tendría sentido.

Un buen diseño del entorno facilita la administración posterior de los servidores y simplifica los procesos. Aquí la planificación previa es clave.

De la misma manera, una buena planificación de las configuraciones e instalaciones de las estaciones de trabajo permite una administración eficaz para resolver problemas de los usuarios, y simplifica todos los procesos y accesos posteriores. También tenemos un buen conjunto de herramientas que nos ayudan mucho a llevar a cabo esta tarea. Una vez más, la planificación previa es esencial.

El usuario tiene que tener un punto de referencia único en caso de problemas informáticos. Este punto de referencia permitirá resolver rápidamente los problemas inmediatos, responder las consultas sobre situaciones conocidas, emitir una respuesta en un tiempo razonable si el problema es singular y, sobre todo, la sensación de que alguien se preocupa por él. Este punto de referencia es el centro de atención al usuario (CAU).

La instalación de un nuevo software cambia la manera de trabajar, y se tiene que tratar con mucho cuidado con el fin de no crear mal ambiente laboral, y para que los usuarios utilicen correctamente el nuevo software, ya que, de lo contrario, pueden hacer fracasar esta instalación.

La formación de los usuarios es una cuestión a menudo olvidada, pero clave para una organización que utiliza el sistema informático de una manera eficiente. Hay diferentes tipos de formación dependiendo de la situación del usuario; hay que tenerlas en cuenta para aprovechar al máximo su utilidad.

Sea como fuere, el usuario siempre tiene que tener la sensación de que tiene el apoyo y la ayuda del departamento de informática para llevar a cabo su tarea. De esta manera, emitirá el juicio de que el departamento de informática funciona “correctamente”.

Actividades

1. Como responsables de la gestión de usuarios de vuestra organización, la primera tarea que queréis hacer es definir la matriz de control de accesos. Podríais confeccionar esta matriz para los grupos de usuarios y objetos más representativos de vuestra organización.

2. Buscad por la red uno de los múltiples aplicativos de control remoto de estaciones de trabajo que tienen una versión de pruebas e instaladla para hacer pruebas de su utilidad. ¿Qué ventajas creéis que aportaría a vuestra organización?

3. Si tenéis la posibilidad de disponer de una estación de trabajo de pruebas, cread vuestra propia estación de trabajo siguiendo los pasos que se indican en este módulo. Si no existe tal posibilidad, intentad definir cuáles son estos pasos adaptados a vuestra propia organización.

4. Si disponéis de un CAU en vuestra organización, intentad definir el diagrama de niveles sobre el cual se basa su funcionamiento. Si no tenéis ningún CAU en vuestra organización, intentad definir cómo os gustaría que funcionara y dibujad el diagrama de niveles. Como tarea adicional, podéis buscar en la red software de demostración dedicado a gestionar CAU, con el fin de escoger uno adecuado.

Ejercicios de autoevaluación

1. Teniendo en cuenta los grupos de usuarios y las aplicaciones siguientes que forman parte de vuestra organización (instituto de secundaria), elaborad la tabla de aplicaciones y comentad la información que se desprende de ella.

- Grupos:
  - Alumnos.
  - Profesores.
  - Equipo directivo.
  - Gestión del centro.

- Aplicaciones:
  - Ofimática.
  - Herramientas de aprendizaje.
  - Aplicación de evaluación (gestor de notas de alumnos).
  - Contabilidad del centro.

- Control centro (gestor horarios, entradas y salidas de material, registro...).

2. La dirección ha pedido poner en marcha un sistema de control horario en la organización. Vuestro jefe de informática se reúne con vosotros, que sois técnicos de sistemas, para que le deis la información técnica para poner en marcha un paquete informático que controle la entrada y salida de los trabajadores. Así lo hacéis, pero le recordáis que se tendría que hacer un plan de información y formación de los usuarios. El jefe os dice que de acuerdo, pero os pide la opinión. ¿Qué le diríais?

3. En una organización, se crea un puesto de trabajo nuevo. Han colocado una mesa nueva, y a vosotros, administradores de sistemas, os lo comunican. Elaborad el procedimiento completo para que esta persona, cuando llegue la semana que viene, se pueda sentar ante la nueva mesa, poner en marcha el ordenador y empezar a trabajar.

4. Como responsables del CAU de tres niveles de vuestra organización, definid todos los pasos que se realizarán hasta el segundo nivel, desde el momento en que recibáis la incidencia de un usuario de una delegación que se encuentra, aproximadamente, a 200 km de la sede central.

Solucionario

Ejercicios de autoevaluación

1. Creamos la tabla de aplicaciones. Ésta es una de las posibilidades:

	Aplicación		Información		Alumnos	Profesores	Equipo directivo	Gestión centro
	Local	**Remoto**	**Local**	**Remoto**				
Ofimática	X			X	L/E/X	L/E/X	L/E/X	L/E/X
Herramientas aprendizaje	X		X		L/E/X	L/E/X	L/E/X	
Aplicación evaluación		X		X		L/E/X	L/E/X	
Contabilidad		X		X			L/E/X	L/E/X
Control centro		X		X				L/E/X

Extraemos información:

- Lista de software completo que se utiliza en la organización (que de hecho ya conocíamos). Es la primera columna de la tabla.
  - Software de ofimática.
  - Software herramientas de aprendizaje.
  - Software de evaluación.
  - Software de contabilidad.
  - Software de control del centro.

- Dónde está la información de cada aplicación. Vemos que hemos decidido que esté toda en remoto, excepto los datos de la herramienta de aprendizaje, ya que son aplicaciones que no actualizan sus datos una vez han interactuado con el usuario.
- Relación de grupos de usuarios. Con la relación de grupos que tenemos, vemos que habrá usuarios que podrán pertenecer a como mínimo un par de grupos: profesores y equipo directivo.
- Lista de software que se utiliza por grupos. La organización tendrá el software que parece que necesita todo el mundo, y cada grupo tendrá lo que es específico para cada departamento. Hay que ir con cuidado con la información, ya que la ofimática requiere un estudio detallado, porque si no, con permisos para todo el mundo, todos los usuarios verían toda la información.
- La relación de aplicaciones candidata para fabricar la **estación de trabajo modelo**.
  - Ofimática: sí.

2. Como técnico de sistemas (o administrador de los servidores y/o de los usuarios), se supone que le hemos informado de una aplicación que se ajusta a las necesidades de la organización, desde el punto de vista técnico y desde el punto de vista de la necesidad que se tiene que cubrir. Ahora bien, se trata de dar la opinión sobre cómo pensamos que se tiene que desarrollar el plan de formación; por lo tanto, le explicaríamos las líneas maestras con que lo haríamos.

Formación general:

- Que el personal de la organización conozca la herramienta de gestión horaria.
- Que entienda las ventajas que se desprenden de esta nueva herramienta.
- Que no la vea como un mecanismo de control.
- Enumerar las ventajas que comporta. Por ejemplo:
  - Consulta del tiempo de entrada y salida desde cualquier ordenador (controlado por contraseña) individualizado para cada persona.
  - Petición de días para asuntos personales desde cualquier ordenador en cualquier momento.

- Recuperación automática de horas por el sistema, en caso de que algún día se llegue tarde.
- Se pueden introducir incidencias (decir que se ha llegado tarde) directamente desde cualquier ordenador.
- Ahora –antes no era posible– el tiempo sobrante se podrá usar para asuntos personales, gracias a este nuevo sistema.
- Y otras cosas.

Formación de administración:

Este software necesita formación adicional para las personas que gestionan las incidencias y detectan las anomalías horarias. Como utilizan otra parte del software que no utiliza toda la organización, necesitan una formación complementaria.

Formación de nóminas:

Lógicamente, un software de estas dimensiones tiene que enlazar con nóminas, y como se hacen mensualmente y se ocupa otro departamento, se utiliza una parte del software que no utiliza nadie más. Necesitan una formación complementaria.

Formación de informática:

La aplicación maneja datos sensibles, tiene dispositivos para fichar en uno o diversos sitios de la organización, y parece que enlaza elementos diferentes (al menos nóminas y administración). Es, por lo tanto, una aplicación bastante compleja. Es necesaria la formación de alguna o algunas personas del departamento para asegurar que la instalación se hace correctamente, que un problema se puede resolver, y que las copias de seguridad se hacen de la manera adecuada.

Seguramente, un posible orden de la formación sería:

- Jornada inicial con el personal de la organización para evaluar su opinión.
- Formación de informática.
- Formación de nóminas.
- Formación de administración/formación de la organización.

Por lo tanto, se harían unas jornadas de dos horas para explicar al personal el funcionamiento del sistema, cómo se utiliza, las ventajas que tiene y los cambios y las mejoras que se introducirán en la organización gracias a la implantación de este software.

3. En líneas generales, las tareas pueden ser las siguientes:

- Comprar un ordenador completo (pantalla, teclado, caja, placa de comunicaciones, etc.).
- Preguntar al departamento adecuado el puesto de trabajo y las responsabilidades de esta persona, para determinar:
  - El sitio físico donde tiene que ir el ordenador.
  - El grupo o los grupos a los cuales pertenece la persona.
  - Por lo tanto, los permisos que tendrá dentro del sistema.
  - Por lo tanto, el software que necesita utilizar.

- Establecer la conexión de red física hasta el puesto de trabajo.
- Dar de alta al usuario en los servidores.
- Crearle una cuenta de correo.
- Habilitar su espacio privado.
- Darle, si hace falta, permisos especiales en los servidores de bases de datos.
- Habilitar encaminadores (*routers*) y conmutadores (*switches*), con la dirección en placa para que esta placa de comunicaciones pueda enviar y recibir información por la red de la organización.
- Clonar la imagen de las estaciones de trabajo en este ordenador nuevo.
- Ajustar la configuración, dado que tenemos el ordenador modelo: ajustar los parámetros de red, como el nombre del ordenador, la dirección IP, configurar las impresoras que utilizará, etc.
- Instalar, si hace falta, software específico.
- Probar el ordenador como si fuéramos esta persona.
- Si todo ha ido bien, llevar el ordenador al puesto de trabajo de la persona, para que cuando llegue lo encuentre.

No está de más enviarle un correo electrónico que explique cuál es la operativa básica (si no ha hecho ninguna formación en la organización) y a dónde se puede dirigir para solucionar los problemas. También es recomendable hacerlo en soporte papel, telefónico o presencial,

porque si no sabe utilizar la herramienta de correo electrónico, un mensaje de correo no sirve de gran cosa.

4. Teniendo en cuenta que tenemos un CAU de tres niveles:

Primero de todo, recibiremos la incidencia por un único punto de control que gestionará el primer nivel del CAU. Se abrirá el ticket identificativo de la incidencia en la base de datos del CAU y se informará de ella al usuario.

Desde el primer nivel, se accederá a la base de datos de conocimiento para intentar buscar soluciones ya certificadas para el problema. Si se soluciona el problema, se cerrará la incidencia de acuerdo con el usuario. En caso contrario, se escalará ésta al segundo nivel.

En el segundo nivel, un técnico especializado en el área (comunicaciones, bases de datos...) atenderá el problema y buscará una solución. Con el fin de realizar las acciones convenientes en la estación de trabajo afectada, o incluso con el fin de comprobar el error *in situ*, utilizaremos herramientas de conexión remota que nos permitirán un acceso rápido sin tener que desplazarnos.

Si la soluciona, actualizará la base de datos de conocimiento y cerrará la incidencia con la conformidad del usuario. En caso contrario, pasará al tercer nivel.

Glosario

antivirus *m* Software que busca virus en el disco duro de los ordenadores.

base de datos de conocimiento *f* Base de datos con la información necesaria para resolver incidencias resueltas anteriormente. También permite extraer patrones y conductos de resolución.

CAU *m* Ved **centro de atención al usuario**.

centro de atención al usuario *m* Parte del departamento de informática dedicado a atender las incidencias de los usuarios.
sigla: **CAU**.

clonación *f* Operación de duplicar el contenido de un disco duro en otro disco duro, con lo cual se obtiene una copia exacta imposible de distinguir del original.
sin. **clonar**.

control remoto *m* Control a distancia de una estación de trabajo o servidor mediante un software cliente/servidor para tal efecto.

entorno de usuario *m* Lo que encuentra el usuario cuando pone en marcha el ordenador para trabajar.

estación modelo *f* Ordenador patrón que se prepara y se utiliza como base para configurar todos los otros ordenadores de la organización. Se hace mediante software, ya que de esta manera la tarea es más sencilla.

FAQ *f pl* Ved **preguntas más frecuentes**.

fichero de firmas *m* Relación de marcas que identifican los virus. Lo utiliza el antivirus para comparar y encontrar virus.

imagen del disco *f* Copia exacta del contenido de un disco en un momento dado.

incidencia *f* Demanda de un usuario para la solución de un problema que le impide trabajar correctamente.

perfil *m* Información guardada sobre el usuario que, con la identificación, configura la estación de trabajo, de manera que ajusta los permisos, los accesos, la configuración del entorno gráfico, etc. (el entorno de trabajo en general).

petición *f* Demanda de un usuario para la actualización de un software, nueva instalación o configuración.

PMF *f pl* Ved **preguntas más frecuentes**.

preguntas más frecuentes *f pl* Conjunto de dudas sobre un tema concreto que los internautas se plantean repetidamente y que se guardan en una página web con las soluciones correspondientes.
en frequently asked questions.
sigla: **PMF**.
sigla en: **FAQ**.

software de base *m* Software que se considera que tienen que tener todos los ordenadores de la organización que utilizan los usuarios. Normalmente comprende como mínimo el sistema operativo, el software de ofimática, un navegador y un programa de correo electrónico, y también aplicaciones específicas de la organización comunes a todas las estaciones de trabajo.

software de ofimática *m* Software que comprende un programa de hoja de cálculo, un procesador de textos, una base de datos pequeña, un programa de presentaciones, una agenda y, actualmente, también un programa cliente de correo electrónico.

tabla de aplicaciones *f* Resumen que contiene la lista de aplicaciones con la información y los permisos que se asocian a cada grupo de la organización para cada aplicación.

TI *f pl* Tecnologías de la información.

TIC *f pl* Tecnologías de la información y la comunicación.

ticket *m* Número o identificador que identifica la petición o incidencia abierta por el usuario a fin de que se pueda llevar un control sobre la misma.

Bibliografía

Barceló García, M.; Pastor i Collado, J. (1999). *Gestió d'una organització informàtica*. Barcelona: Universitat Oberta de Catalunya.

CEP (2007). *Administración del servicio de atención al usuario*. Formación CEP.

Jumes, James G.; Coopper, Neil F.; Chamoun, Paula; Feinman, Todd M. (1999). *Microsoft Windows NT 4.0 Seguridad, auditoria y control*. Madrid: MacGraw Hill.

Microsoft Corporation (1997). *Sourcebook for the help desk 2/Ed*. USA: Microsoft Press.

Microsoft Corporation (1997). *Windows NT 4.0 Workstation Kit de Recursos*. Madrid: Mc-Graw Hill.

IT Governance Institute (2007). *COBIT Quickstart, 2nd Edition*. IT Governance Institute.

OGC (2007). ITIL: *Service Strategy*. OGC.