



CENTRO DE ESTUDIOS FINANCIEROS

VIRIATO, 52	28010 MADRID	914 44 49 20
PONZANO, 15	28010 MADRID	914 44 49 20
G. DE GRÀCIA, 171	08012 BARCELONA	934 15 09 88
ALBORAYA, 23	46010 VALENCIA	963 61 41 99

www.cef.es

info@cef.es

Índice Tema 1

1. ¿Qué es la administración de sistemas?
2. Tareas de la administración de sistemas.
 - 2.1. El soporte de usuarios.
 - 2.1.1. Creación de cuentas de usuario.
 - 2.1.2. Proporcionar soporte.
 - 2.2. El soporte de sistemas.
 - 2.2.1. Añadir nodos.
 - 2.2.2. Copias de seguridad (backups).
 - 2.2.3. Carga de los sistemas y su rendimiento.
 - 2.3. Recursos para la administración.
 - 2.3.1. Los archivos de ayuda.
 - 2.3.2. Los recursos de información de Internet.
 - 2.4. Las herramientas del oficio.
 - 2.4.1. Archivos de comandos.
 - 2.4.2. Herramientas de automatización.
 - 2.4.3. Herramientas de Intranet.
3. Principios de instalación.
 - 3.1. Requerimientos de espacio.
 - 3.1.1. ¿Quién hará uso del sistema?
 - 3.1.2. ¿Con qué propósito?
 - 3.1.3. Determinación de los servidores adecuados.
 - 3.2. Planificar la instalación.

- 3.3. Empleo de múltiples particiones de disco.
- 3.4. Llevar a cabo la instalación.
- 4. Arranque y parada.
 - 4.1. Arranque.
 - 4.2. Parada.
- 5. Salvaguarda y recuperación.
 - 5.1. Dispositivos de almacenamiento.
 - 5.2. Planificación de las salvaguardas.
 - 5.3. Verificación y custodia de las salvaguardas.
- 6. Control de cambios y gestión de incidencias.
 - 6.1. Tendencias en la organización.
 - 6.2. El acuerdo de nivel de servicio.
 - 6.3. Organización.
 - 6.4. Control de cambios.
 - 6.4.1. Inventario de recursos.
 - 6.4.2. Distribución de software e instalación del hardware.
 - 6.4.3. Control de licencias software.
 - 6.5. Herramientas de gestión de incidencias y cambios.
- 7. Contabilidad y monitorización del sistema.
 - 7.1. El sistema de contabilidad.
 - 7.2. Monitorización del rendimiento.



CENTRO DE ESTUDIOS FINANCIEROS

VIRIATO, 52	28010 MADRID	914 44 49 20
PONZANO, 15	28010 MADRID	914 44 49 20
G. DE GRÀCIA, 171	08012 BARCELONA	934 15 09 88
ALBORAYA, 23	46010 VALENCIA	963 61 41 99

www.cef.es

info@cef.es

TEMA 1

Administración del sistema operativo y software de base. Funciones y responsabilidades. Control de cambios.

1. ¿QUÉ ES LA ADMINISTRACIÓN DE SISTEMAS?

La Administración de sistemas consiste en planificar, instalar y mantener sistemas informáticos. Si esta frase parece una respuesta muy general es porque la administración de sistemas realmente lo es.

Si leyéramos cualquier anuncio típico de trabajo en el que se solicite un Administrador de Sistemas, encontraríamos que un Administrador instala y configura el sistema operativo, añade nuevos usuarios, realiza salvadas de los sistemas, los mantiene seguros y se asegura que permanezcan en marcha. También configurar el acceso a las redes y a internet y mantenerlo conectado y funcionando es parte de ese trabajo.

Sin embargo, lo visto no es más que la mitad del cometido a desempeñar. Ser un experto en instalar, hacer funcionar y mantener la mayoría de las posibles variantes de sistemas informáticos no es suficiente para ser un buen Administrador de Sistemas. Existe un componente no-técnico muy significativo a desarrollar, en términos de planificación, organización y habilidad personal.

Conforme los ordenadores se han ido introduciendo más y más en los negocios, la administración de sistemas ha adquirido una posición crítica en un mayor número de organizaciones. El Administrador tiene que comprender el sistema del que es responsable, a las personas que lo usan y la naturaleza de los negocios en los que se emplea. Una técnica clave de la administración es la planificación, pues a la velocidad con que los sistemas se crean, se revisan y expanden, intentar la improvisación y el diseño de la red «sobre la marcha», sencillamente no funciona.

Las compañías están moviendo sus procesos no solo a los ordenadores, sino a sus sistemas punto de venta (como el comercio Web) y sofisticados sistemas de tienda como catálogos electrónicos y cajas registradoras que se encuentran conectados directamente a los sistemas de inventario y contabilidad.

Las compañías que han pasado a los ordenadores su control de inventario desde hace cinco años, persiguen ahora informatizar la entrada de pedidos e incorporarla a la Web. Mientras tanto, las empresas que todavía no han automatizado estos sistemas persiguen hacerlo, intentando mantener su competitividad.

El correo electrónico se considera ahora tan importante como los faxes y el teléfono, tal y como cualquier parte de un servicio de atención al cliente que se pueda manejar por ordenador o un sistema automático de recuperación y distribución de faxes ya lo es.

Las compañías dependen casi completamente de sus ordenadores y sus administradores de sistemas necesitan conocer bastante más que la forma de dividir un disco, añadir memoria a un sistema o instalar Office.

2. TAREAS DE LA ADMINISTRACIÓN DE SISTEMAS.

La administración de sistemas se puede dividir en dos amplias categorías: Soporte de Usuarios y Soporte de Sistemas.

2.1. EL SOPORTE DE USUARIOS.

Para un Administrador de Sistemas, los usuarios son sus clientes. Los administradores dan soporte a los usuarios creando sus cuentas de acceso y suministrándoles la información que necesitan para hacer un uso adecuado de sus ordenadores, sin obligarles a convertirse en expertos informáticos o en adictos a la informática.

2.1.1. Creación de cuentas de usuario.

La parte más importante que un administrador puede hacer por un usuario es crearle una cuenta de acceso. Si bien esta suele ser una tarea sencilla, la corrección en su realización aconseja contar con alguna herramienta de automatización que evite errores comunes y ahorre tiempo.

Usualmente la creación de cuentas supone:

- Establecer un identificativo único para cada usuario, que lo diferencie de cualquier otro usuario
- Asignar permisos generales de acceso a los recursos compartidos.
- Copiar en la cuenta creada, los archivos pertinentes que configuren el entorno de trabajo del usuario: variables de entorno, aplicaciones a emplear, etc.
- Registrar la cuenta en los sistemas en Red para facilitar el acceso desde los diferentes servidores.

2.1.2. Proporcionar soporte.

Proporcionar a los usuarios el soporte y la documentación que precisan es otra de las tareas claves de la administración, y un quebradero de cabeza potencial. El mejor Administrador de Sistemas es, a la vez, invisible y nunca se le echa en falta. También es consciente de que, pretender que los usuarios se sientan tan emocionados aprendiendo el manejo de un ordenador, como se siente él, es pedir demasiado.

Un famoso proverbio habla sobre las ventajas de enseñar a pescar, en lugar de proporcionar los peces. La idea que subyace se puede aplicar a los usuarios con unos resultados asombrosos, sin embargo serían muy pocos los usuarios que dejaran de lado otras ocupaciones, para aprender a manejar sus sistemas. ¿Cómo puede un administrador enseñar a sus usuarios el modo de hacer las cosas ellos mismos, sin enfrentarse a una lucha interminable?

Cada grupo de personas es diferente y no existe una solución universal para adiestrar a los usuarios, aunque hay un par de ideas que pueden ayudar:

- Intentar establecer, forzando suavemente su cumplimiento, un método formal de solicitud de cambios en los sistemas y de petición de ayuda. Si los usuarios se acostumbran a las respuestas inmediatas a sus problemas, se enfadarán en cuanto el administrador no suelte aquello que tenga entre manos, para ayudarles. Intentar establecer un sistema de ayuda basado en correo electrónico o Web, puede parecer algo excesivamente burocrático y ser rechazado en un principio, sin embargo servirá para evitar que, el trabajo diario de administración, se convierta en un trabajo «manejado por interrupciones», a la vez que proporcionará un registro de peticiones de gran utilidad para evaluar la carga y variedad de los problemas y la rapidez y calidad en las respuestas. Sobre esta base, será posible generar una base de conocimiento con la que ayudar de una manera mucho más efectiva a los usuarios.
- Proporcionar tanta información como se pueda, mediante el empleo de interfaces de manejo sencillo (como exploradores Web). El tiempo empleado desarrollando esta información, en un formato amigable al usuario, se recuperará posteriormente en llamadas de teléfono y conversaciones que nunca tendrán lugar, a la vez que pueden ayudar al propio administrador a conocer sus sistemas mejor que hasta ese momento. Si los usuarios disponen de acceso a internet, seguramente dedicarán hora a navegar con el explorador. Se puede tomar ventaja de ello, mucha de la información que reclaman los usuarios se encuentra ya disponible en internet. Es posible enlazar a los usuarios con la información que demandan sin generarla uno mismo.

2.2. EL SOPORTE DE SISTEMAS.

La otra mitad del trabajo de Administración es el soporte de los sistemas. Los sistemas se tienen que instalar, actualizar, ajustar y salvarse.

2.2.1. Añadir Nodos.

Una tarea frecuente de la administración de sistemas es añadir nuevos nodos a la red. Es también una de las partes del trabajo que pueden obtener un claro beneficio de una correcta planificación y visión de futuro.

No todos los sistemas se crean igual, ni todos ellos se emplean para las mismas cosas. Dedicar tiempo a comprender para qué se emplea de verdad la red y aplicar este conocimiento a los sistemas, es clave en la planificación de la red. Las estaciones de trabajo deberían contar con funciones bien definidas y ser configuradas de acuerdo a esas funciones.

Cuando se diseñan y evalúan los sistemas, algunas de las cuestiones que puede preguntar el administrador son:

- ¿Deberán acceder los usuarios a todos o solamente a parte de los sistemas?, ¿necesitan acceder los usuarios a más de un sistema?, ¿existirán sistemas a los que los usuarios no deberían acceder nunca?
- ¿A qué tipo de sistemas de archivos necesita acceder cada estación de trabajo?, ¿son tantos que el uso de herramientas para el automontaje sean de utilidad?
- ¿Qué tipo de servicios de red, como telnet, impresoras compartidas, archivos compartidos, correo electrónico, etc. deben proveer las estaciones de trabajo?, ¿se puede justificar la necesidad de cada servicio?
- ¿A qué redes necesitan acceder las estaciones de trabajo?, ¿existen redes que deban ser inaccesibles desde otras?

Estas preguntas deben permitirnos establecer un perfil para cada estación de trabajo. El seguir un determinado perfil facilita la instalación y configuración de las estaciones de trabajo, su mantenimiento y la resolución de problemas, sin olvidar el aumento de la fiabilidad, dado que tienden a ser menos complejas.

2.2.2. Copias de seguridad (Backups).

Los archivos se corrompen, se pierden, se sobrescriben de forma accidental o se eliminan. Nuestra única protección ante estas situaciones son las copias de seguridad (conocidas usualmente por su palabra inglesa Backups).

Todos los sistemas proveen, de una u otra manera, un conjunto de herramientas para realizar las copias de seguridad. Qué tipo de herramienta y método es el adecuado puede resultar una tarea difícil.

Establecer una planificación de las salvallas es clave para asegurar la protección de los datos, fijar el qué salvar, cuándo y con qué frecuencia, vendrá determinado por los requerimientos de protección y salvaguarda que establezca la dirección, asumiendo ésta el grado máximo de pérdida aceptable de información.

Normalmente, la planificación de las Copias de Seguridad vendrá derivada de un estudio previo de análisis y gestión de riesgos, en el que se estudiarán y analizarán los riesgos, las amenazas, el impacto de estas amenazas sobre los sistemas y su repercusión en la actividad empresarial, estableciéndose los límites permisibles de pérdidas y las medidas a adoptar para no superar dichos límites (MAGERIT es la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas que puede emplearse para esto).

Si bien la tarea de realizar las copias de seguridad no son competencia directa del Administrador, sino del perfil laboral de operador, si es su responsabilidad asegurar que se siguen los procedimientos en su realización y resolver cualquier incidencia que se pueda producir.

La determinación de las herramientas adecuadas para la realización de las copias de seguridad, el estudio de posibles herramientas de terceros y su viabilidad en el entorno de la organización, son funciones que deben ser realizadas por el Administrador, como responsable de la seguridad de los sistemas y los datos en ellos almacenados.

2.2.3. Carga de los sistemas y su rendimiento.

La tarea de monitorizar la carga de los sistemas y su rendimiento, recae sobre el Administrador, es ésta otra área donde, la planificación y la anticipación son mucho mejores que esperar a que ocurra algo y reaccionar ante ello.

La monitorización diaria de las estadísticas de uso es una buena idea, especialmente en sistemas de misión crítica y sistemas con los que, los usuarios, interactúan regularmente, como servidores Web o pantallas X. Estas estadísticas se pueden obtener mediante herramientas de automatización (archivos de scripts automatizados, programas de terceros, etc.).

2.3. RECURSOS PARA LA ADMINISTRACIÓN.

El Administrador de Sistemas, necesita cada pedazo de información y ayuda que pueda conseguir y, como muchos suministradores de sistemas tienen que admitir, la información que acompaña a los equipos tiene a veces grandes carencias. Por fortuna, existe un gran mundo ahí fuera.

2.3.1. Los archivos de ayuda.

Los archivos de ayuda, instalados y suministrados con el sistema, contienen documentación e instrucciones sobre prácticamente la totalidad de los comandos, funciones y archivos de un sistema.

Estos archivos, suelen apoyarse en un entorno de ayuda común en los sistemas (HTML Help de Microsoft, las Man Pages de UNIX, etc.), que proporcionan las herramientas de visualización y búsqueda de información. Normalmente, el acceso a la información se encuentra organizado por temas o palabras clave y, entre las utilidades del entorno, está el poder acceder a él desde otra aplicación, proporcionando una ayuda «sensible al contexto» de una gran utilidad.

2.3.2. Los recursos de información de Internet.

Internet también proporciona a los administradores un gran cantidad de recursos:

- Foros de noticias: aunque no son tan útiles como en el pasado, debido a la superpoblación y al descenso de la relación señal-ruido (o sea, demasiadas personas accediendo y demasiados mensajes inútiles, dañinos, o faltos de rigor, que se entremezclan y dificultan el acceso a la verdadera información de utilidad), siguen siendo una gran fuente de información y de comunicación entre personas que desarrollan un cometido similar y por tanto, se enfrentan a una problemática también similar. Los Foros son el lugar adecuado para compartir experiencias, ayudando a otros a resolver problemas que en algún momento alguien ha sufrido y resuelto, y buscando respuestas a los problemas aún sin resolver en nuestra instalación.

Dado el elevado tráfico de los foros algunos sitios no los soportan. Si no se puede conseguir el acceso, se puede intentar con un servicio de búsqueda como <http://www.dejanews.com> para encontrar lo que se busca. A veces es preferible buscar artículos de interés que navegar directamente. Dejanews ofrece tanto búsqueda como navegación.

- Listas FAQ: las comúnmente conocidas listas FAQ (Acrónimo inglés de Frequently Asked Question -Preguntas que se hacen frecuentemente-) contienen una gran cantidad de informa-

ción. La mayoría de los grupos de noticias relacionados con ordenadores, disponen de su propia lista FAQ. La gran mayoría de proveedores y fabricantes, con servicio Web, también disponen, como parte estándar de su soporte técnico en línea, de una página FAQ sobre sus productos y servicios.

- La Web: una enorme cantidad de información se encuentra disponible a través de la navegación usando el servicio Web. La información proviene tanto de los vendedores de sistemas como de la gente y grupos implicados en su desarrollo y evolución. Muchos usuarios y desarrolladores también aportan gran cantidad de información con el solo ánimo de ser útiles. La mejor forma de acceder es empleando los servicios de búsqueda disponibles por internet, como <http://www.google.es>, <http://es.altavista.com> u otros similares.

Existe una gran cantidad de documentación y ayudas libremente accesibles en Internet, y se aprende mucho más mientras se busca una respuesta que pagando a un consultor por ella o encargándole a alguien que haga lo que deberíamos hacer nosotros.

2.4. LAS HERRAMIENTAS DEL OFICIO.

Un buen administrador aprovecha todas las ventajas que le ofrecen las herramientas que acompañan a los sistemas.

2.4.1. Archivos de comandos.

Todo sistema operativo dispone de alguna forma de agrupar comandos independientes, de forma que se facilite la realización de tareas repetitivas, sobre todo conforme aumenta el tamaño de las redes y en consecuencia, el mantenimiento requiere más tiempo. La salva de archivos, la creación de nuevos usuarios y nodos de la red, la recolección de estadísticas de uso y una gran variedad de tareas administrativas sobre los equipos son perfectos candidatos para la creación de este tipo de archivos (conocidos usualmente como scripts), que se ejecutan sin la intervención directa del administrador, mediante herramientas de temporización (El programador de tareas de Microsoft, el cron de UNIX, etc.). Usualmente estos archivos admiten construcciones complejas como bucles, operadores de comparación y bifurcación, constituyendo a veces un completo lenguaje de programación.

2.4.2. Herramientas de automatización.

Existen, tanto en el mercado como en el mundo de código libre, herramientas de ayuda a la Administración que realizan una determinada tarea o presentan un entorno donde desarrollar, de una manera mucho más sencilla, intuitiva y eficaz que con las propias herramientas del sistema operativo (potentes pero a veces muy crípticas y de difícil manejo e interpretación) las tareas de administración. Por ejemplo, se pueden emplear para tareas como:

- Analizar los archivos de registro, aplicando patrones que detecten posibles anomalías y avisen al Administrador mediante el correo electrónico o mensajes a móviles.
- Convertir de manera automática estadísticas del sistema en páginas Web, que puedan ser accedidas desde un punto remoto de una forma sencilla.
- Automatizar los procesos de creación de usuario, añadir y distribuir perfiles de usuarios, realizar salvas de sistemas o crear contenidos html.

2.4.3. Herramientas de Intranet.

Como se mencionó anteriormente, se debe considerar el empleo de las herramientas de Intranet, como los servidores Web y de correo electrónico, para comunicarse con los usuarios.

Existen una gran cantidad de aplicaciones para crear «libros de visitas» sobre páginas Web, que se pueden modificar fácilmente, para permitir que los usuarios realicen sus solicitudes de petición de soporte.

Una página web interna puede emplearse para comunicar acontecimientos, como paradas programadas o actualizaciones de sistemas. La Web también permitiría enlazar directamente a los usuarios con la documentación y el soporte ofrecido por los suministradores.

3. PRINCIPIOS DE INSTALACIÓN.

La instalación de los sistemas requiere de un tiempo previo de reflexión y planificación, necesarios para asegurar la correcta integración de los equipos en el sistema informático de la Organización, y la adecuación al cometido a que se destinen.

Será preciso decidir si el sistema a instalar actuará independientemente o dependerá de un servidor de la red; si tendrá como misión ser un equipo cliente, para un usuario final, o será un servidor corporativo o departamental. Será necesario prestar atención a los recursos de sistema con que se cuente (espacio en disco, velocidad del procesador, memoria, etc.).

Un punto importante a destacar es la elección del sistema operativo que se instalará. La decisión puede venir obligada por la máquina a instalar, pues podría ser un hardware propietario, con un S.O. específico; puede ser una elección corporativa impuesta desde la dirección (p. ej. el uso de sistemas de código abierto); podría venir forzado por necesidades concretas de integración e interoperabilidad con otros sistemas, en el seno de la Organización o fuera de ella; por homogeneidad de las instalaciones; por una funcionalidad específica que se precise, etc.

Cada sistema operativo requiere de unas consideraciones previas a su instalación. Preguntas cuya respuesta hay que conocer para garantizar una instalación adecuada a las necesidades a cubrir. Con independencia de las particularidades propias de cada sistema, en mayor o menor medida podemos hablar de una serie de consideraciones a tener en cuenta en toda instalación.

Lo primero que se debe decidir es qué se va a instalar en el sistema. Esta decisión no depende solamente del sistema concreto a instalar, sino que se ve afectada por el resto de sistemas que se encuentran en la red donde se integre. La decisión se basará en el uso a que se destine; qué sistemas serán servidores para él y a cuáles proporcionará sus servicios.

3.1. REQUERIMIENTOS DE ESPACIO.

Ciertos sistemas operativos no están bien preparados para compartir grandes partes de su instalación, otros esperan que exista esa compartición en alguna medida. El grado de espacio de almacenamiento compartido por los sistemas conduce a la definición de máquinas independientes «stand-alone», servidores, sin disco «diskless», sin datos «Dataless»:

Un sistema independiente puede funcionar por sí mismo, sin requerir la ayuda o participación de ningún otro sistema de la red.

Un sistema servidor se encuentra conectado en una LAN y ejecuta servicios que aportan ciertas funcionalidades a clientes remotos como correo, noticias, acceso a Bases de Datos, etc. Técnicamente un servidor puede ser un sistema independiente, aunque dada su funcionalidad nunca lo es.

Si un sistema cliente no tiene ningún tipo de disco, se le considera un sistema sin disco o Diskless. Depende de su servidor para arrancar, para todo el sistema operativo y para el área de swap (almacenamiento secundario en la gestión de memoria). Mucha gente emplea estos sistemas como terminales tontos, o sistemas que solamente proporcionan un interfaz para conectarse a sistemas remotos.

Los sistemas sin datos o Dataless sí tienen algún almacenamiento, pero en él solamente están los archivos mínimos necesarios para su arranque.

Tanto los sistemas sin datos como los sistemas sin disco, no se emplean demasiado debido a la elevada carga que imponen en la red, si bien presentan grandes ventajas de instalación, configuración y mantenimiento, permitiendo, en grandes corporaciones, facilitar la administración y agilizar la respuesta a los cambios que se deban realizar (solamente se debe actualizar el sistema una vez, en el servidor, para que repercuta y funcione en todos los sistemas cliente sin disco, mientras que los sistemas sin datos son fácilmente sustituibles pues carecen de personalización alguna con el puesto de trabajo, o datos privados en ellos, siendo también muy sencilla su sustitución o actualización).

Además de compartir el sistema operativo, los sistemas pueden compartir otros discos con contenidos como Bases de Datos, archivos de usuarios, etc. Dependiendo de la instalación se requerirán diferentes necesidades de almacenamiento: un sistema para desarrollo requiere normalmente más espacio en disco, mientras que, un sistema sin datos solamente requiere espacio para el núcleo del sistema operativo. Según las necesidades se optará por una configuración u otra del disco.

3.1.1. ¿Quién hará uso del sistema?

Los usuarios que usan normalmente la máquina para tratamiento de textos y otras aplicaciones generales de oficina no requieren una cantidad enormemente grande de espacio en disco, o recursos del sistema. Sin embargo, un usuario avanzado o un desarrollador de aplicaciones requiere instalar muchas más cosas, posiblemente se incluyan compiladores y librerías de desarrollo. Será preciso pues tener en cuenta qué usuarios harán uso del sistema:

- Usuarios de aplicaciones: estos usuarios ejecutan aplicaciones comerciales o desarrolladas en la Organización; raramente interactúan con el sistema directamente y no escriben sus propias aplicaciones. Estos usuarios podrían estar ejecutando una aplicación de bases de datos, un procesador de texto, una hoja de datos, etc. Dedicar la mayor parte del tiempo decidiendo qué hacer con la información, que la aplicación les está mostrando, o introduciendo información en el sistema. Su necesidad de acceder a grandes cantidades de disco local es mínima, y ni cambian sus aplicaciones frecuentemente ni ejecutan muchas aplicaciones de forma simultánea (aunque podrían tenerlas abiertas, normalmente interactúan con un par de ellas a un tiempo, mientras el resto espera la entrada de datos).

Aunque las aplicaciones de usuarios pueden cargar mucho sus servidores de Bases de Datos, no suelen cargar los discos de sus propios sistemas.

- **Usuarios avanzados:** estos usuarios ejecutan aplicaciones, igual que los usuarios de aplicaciones, pero además interactúan con el sistema, a través de los interfaces disponibles. Es más fácil que puedan ejecutar múltiples aplicaciones a la vez, procesándose en paralelo. Estos usuarios mantienen varias aplicaciones ocupadas a un tiempo, acceden al disco más frecuentemente y emplean más recursos de CPU que los usuarios de aplicaciones usuales.
- **Desarrolladores:** los desarrolladores no ejecutan solamente aplicaciones, también ejecutan compiladores, acceden a aplicaciones diferentes, precisan de acceso a las librerías de desarrollo y generalmente, emplean más componentes del S.O. que el resto de los usuarios. Lo que es más, suelen emplear herramientas de depuración que requieren de mayor espacio de almacenamiento auxiliar (swap) y acceder a mayores recursos de disco y procesador.

3.1.2. ¿Con qué propósito?

Si un sistema se va a emplear como un servidor para compartir archivos, necesitará una gran cantidad de almacenamiento extra. Si se emplea para proporcionar servicios de procesamiento o servidores de Bases de Datos, requerirá mayores potencias de procesador y de almacenamiento auxiliar (área de swap).

3.1.3. Determinación de los servidores adecuados.

Normalmente es más sencillo determinar la idoneidad de un servidor que la de un cliente. En general un buen servidor debería contar con:

- **Gran cantidad de memoria RAM:** los servidores debe disponer de una gran cantidad de memoria. Un servidor debe ser capaz de manejar muchos clientes, cada uno ejecutando diferentes procesos al mismo tiempo. Para conseguir un funcionamiento eficiente, hay que tratar de evitar una paginación excesiva.
- **Discos rápidos:** un cliente ve el retraso en leer un bloque de disco, como la suma de los tiempos empleados en solicitar la lectura al servidor, lo que éste tarda en leerlo, y el tiempo necesario para transmitir, a través de la red, esta información al cliente. Si el servidor dispone de discos rápidos, este tiempo puede no ser mayor, y a veces puede ser incluso menor, que el tiempo en acceder a los propios discos locales.

Dado que un servidor maneja múltiples clientes, es probable que el bloque de disco solicitado se encuentre en la memoria caché del servidor. Esto es más probable para archivos de programa o utilidades del sistema operativo, dado que se utilizan muy a menudo. El acceso es muy rápido, desapareciendo el tiempo de acceso al disco, ayudando a que los servidores respondan tan rápidamente como si se tratara de un acceso a disco local.

- **Espacio en disco suficiente:** los servidores almacenarán sus propios archivos, una copia del sistema operativo e incluso el espacio auxiliar y temporal necesario para los clientes sin disco (cuando se empleen). Almacenarán los archivos de usuario y las Bases de datos en aquellos servidores instalados con ese propósito y cualquier otra información que se opte por compartir en el seno de la Organización. Un servidor adecuado, deberá disponer de espacio en disco de sobra para poder dar servicio a los usuarios actuales y para permitir el crecimiento de nuevos servicios y usuarios.
- **Recursos de sobra de CPU:** un servidor necesita disponer de suficiente potencia de procesador para servir a sus usuarios locales y proporcionar acceso a los discos y a la red a sus clientes. Sin embargo, esto no significa contar con el sistema más rápido posible, de hecho a menudo hay que optar por lo contrario.

No se precisan muchos recursos de procesador para ser un servidor. El acceso a archivos, así como el tráfico de red, se suele manejar de forma muy eficiente. Un sistema que se encuentra muy cargado, retrasa las peticiones de lectura de bloques de disco a sus clientes. Para mantener un buen tiempo de respuesta a los clientes, es mejor colocar a los usuarios avanzados sobre los sistemas más rápidos, dejando los sistemas con suficientes recursos y poca carga de usuarios como servidores, aunque éstos tengan CPU más lentas.

- Gestionar el tráfico de la red: antes de decidir cómo instala el nuevo sistema, se necesita comprobar el tráfico en la red. Este tráfico proviene de:
 - Tráfico de los sistemas en el Departamento «A» hacia su servidor local para:
 - Sistemas de archivo remotos, incluyendo unidades de disco compartidas y archivos de usuarios.
 - Acceso a aplicaciones Cliente/Servidor alojadas en el servidor del Departamento «A».
 - Clientes sin disco que acceden a los recursos de almacenamiento auxiliar, temporal y de spool.
 - Tráfico entre los sistemas del Departamento «A», incluido lo siguiente:
 - Tráfico de aplicaciones Cliente/Servidor.
 - Actualizaciones de visualización remota (una ventana, en un sistema, mostrando la información de salida de un proceso en un sistema diferente).
 - Compartición de archivos locales que no están en el servidor.
 - Tráfico entre los sistemas del Departamento «A» y el servidor corporativo:
 - Acceso remoto a archivos de acceso global (a nivel de la organización).
 - Acceso a aplicaciones Cliente/Servidor que funcionan sobre los servidores corporativos, como Bases de Datos corporativas.
 - Tráfico entre los sistemas del Departamento «A» y otros del Departamento «B»:
 - Acceso a archivos locales del Departamento «B».
 - Acceso a aplicaciones Cliente/Servidor ejecutándose en sistemas del Departamento «B».
 - Acceso remoto a archivos en discos locales de los sistemas del Departamento «B».

El tráfico adicional, que generará el nuevo sistema, debe compararse con el tráfico existente en la red, estudiando las posibles implicaciones derivadas de su instalación y puesta en marcha.

En resumen, antes de comenzar la planificación de la instalación de un nuevo sistema, se necesita determinar quién hará uso del sistema, cuánto acceso de disco se realizará y cuánto contribuirá al tráfico total en la red; si el sistema será un cliente o un servidor y si la red podrá soportar este nuevo sistema o habrán de tomarse medidas (como la división en nuevos segmentos) para su instalación.

3.2. PLANIFICAR LA INSTALACIÓN.

Ahora es el momento de determinar en qué segmento de la red se instalará el nuevo sistema, decidir para qué tipo de usuario es y dónde colocarlo. ¿Qué más hace falta por planificar, además de dónde conectar la alimentación y el cable de red?

Un pequeño cuestionario de preinstalación ayudará a realizar el proceso de instalación de la mejor manera posible, conociendo la respuesta a preguntas como estas:

- ¿Desde dónde se va a instalar?: tradicionalmente, los sistemas se instalaban colocando un medio extraíble (disco, cinta...) en un dispositivo y arrancando el sistema desde ese dispositivo. Con la llegada de las redes, el sistema se complica un poco más, pero resulta mucho más conveniente.

Se puede optar por dos formas de realizar la instalación: local o remota. La instalación local es el caso tradicional, donde se instala el medio extraíble en el dispositivo y se procede desde él.

La instalación remota se puede realizar de dos maneras: empleando un dispositivo remoto para acceder al medio extraíble de la instalación (porque el sistema a instalar no dispone de uno) o accediendo a un servidor de instalación, donde se encuentran ya todos los archivos necesarios para realizar la instalación. Esta segunda opción permite un acceso a los archivos mucho más rápida que desde el propio medio extraíble, sin embargo precisa de la instalación previa de los archivos sobre el servidor de instalación. Este sistema solo es recomendable cuando se tengan que realizar un gran número de instalaciones, caso donde la ventaja es manifiesta.

- ¿Será un servidor independiente o un sistema sin disco?: ahora es el momento de determinar si un sistema será un cliente sin disco de algún servidor, un sistema sin datos o un servidor o sistema independiente. Esta decisión se debe tomar para asegurar que el sistema se coloca en el mismo dominio que su servidor.

En general, es el precio el que suele determinar si un sistema es totalmente sin disco. Si se puede pagar, es preferible comprar sistemas con disco y hacerlos sin datos. Es mejor reservar los clientes sin disco a lugares donde es impracticable colocar un disco local, por cuestiones del entorno donde irá ubicado, de suministro de energía o donde el acceso al sistema para actualizar el disco local será difícil o imposible.

- ¿Cuál será el nombre de la máquina?: cada sistema se conoce por un nombre o un conjunto de nombres (su nombre de máquina, su nombre de red, a veces diferentes protocolos emplean diferentes nombres, etc.), que deben ser únicos en toda la Organización. La nomenclatura a emplear debe ser conocida, fácil de recordar o relacionar, y debería intentar ser independiente de características externas, como el usuario a quien va dirigido o la configuración de hardware de que dispone, dado que esta nomenclatura puede dar lugar a confusión, pues es muy común que varíen las características dando lugar a sistemas que se denominan de una manera que no se ajusta a la nomenclatura establecida.
- ¿Cuál será su dirección de red?: cada sistema que forma parte de una red debe tener asignado un identificativo único, establecido en la arquitectura de la red correspondiente. En este momento, se deberá asignar el correspondiente al sistema a instalar. Usualmente será el Administrador de la red quien aporte este dato, junto con otros relevantes para la configuración adecuada de la red, al Administrador de sistemas responsable de la instalación.

- ¿Qué paquetes u opciones se instalarán?: normalmente un Sistema Operativo no se suministra como un software monolítico, que se instala en su totalidad. En su lugar, el sistema suele venir dividido en varios módulos o paquetes, bien suministrados como parte del sistema e incluidos en el precio de la licencia, bien adquiridos por separado. Estos paquetes están compuestos por el software y las rutinas de instalación necesarias para incorporar alguna funcionalidad determinada al sistema. Del análisis previo realizado, donde se ha determinado la utilidad que se pretende dar al sistema, se obtendrán los paquetes necesarios de instalar, así como la necesidad de adquirir alguna funcionalidad, requerida pero no suministrada con la distribución del S.O.

Una vez conocidos los paquetes a instalar, su tamaño y los requerimientos de espacio, se está en condiciones de realizar la división de los discos.

- ¿Cómo se dividirán los discos?: cada Sistema Operativo realiza una gestión del almacenamiento en disco, determinada por el tipo de Sistema de Archivos que tenga implementado. Cómo ve el usuario cada unidad de disco físico, varía entre los diferentes sistemas, si bien todos tienen la posibilidad de tratar con almacenamientos más grandes que el tamaño de una unidad física o bien presentar dicha unidad física, como un conjunto de espacios de almacenamiento independientes (particiones, minidiscos, etc.). Por razones de seguridad y eficiencia, es usual dividir el almacenamiento disponible en partes independientes.

3.3. EMPLEO DE MÚLTIPLES PARTICIONES DE DISCO.

Entre las razones para emplear múltiples particiones de disco, presentándose al usuario como diferentes sistemas de archivo o incluso sistemas de archivo separados del de otros usuarios, podemos citar:

- Control de Daños: si un sistema falla, debido a un error de software, hardware o de alimentación eléctrica, algunos de los bloques de disco podrían estar en la memoria caché del sistema, pendientes de escribir en el disco. Este hecho provocaría daños en la estructura del sistema de archivos. Aunque los métodos empleados para tratar de reducir este daño pueden reparar en gran medida estos sucesos, la división de la información entre varios sistemas de archivo, puede reducir enormemente el alcance del daño, especialmente para archivos críticos, necesarios para el arranque del sistema.
- Control de Acceso: la división permite establecer políticas de seguridad y acceso sobre las diferentes porciones del almacenamiento, de manera independiente.
- Gestión del espacio: los archivos crecen, tomando el espacio que precisan del total de espacio libre existente en la partición a donde pertenece. Si todo el sistema estuviera montado sobre una sola partición, un usuario que reservara una gran cantidad de espacio, podría acaparar todo el espacio disponible, dejando al sistema sin espacio libre y provocando su colapso.

El empleo de sistemas de archivo separados, especialmente para los archivos de usuario, permite limitar el daño a un usuario o grupo de usuarios, que se verían afectados por un llenado del sistema de archivos, aunque el sistema seguiría funcionando, permitiendo al Administrador tratar de resolver el problema.

- Rendimiento: cuanto mayor es el sistema de archivos, mayor es el tamaño de las tablas que hacen referencia al almacenamiento, y que debe gestionar el Sistema Operativo. Conforme las tablas son más grandes, el sistema requiere más tiempo y recursos para su gestión, lo que repercute en el rendimiento total.

- Copias de Seguridad: muchas de las utilidades de salvaguarda y recuperación funcionan sobre sistemas de archivo completos, o mejoran su rendimiento cuando se aplican sobre éstos. Si la partición es muy grande, puede ser que se precise más tiempo del que se dispone para realizar la seguridad. Múltiples seguridades más pequeñas son más fáciles de manejar, tanto para realizar la salva como para recuperar desde ellas.

Es útil realizar un mapa del espacio disponible, y de la distribución de las particiones que se deseen, sobre ese mapa. Esta información se empleará en el momento de realizar la instalación y como ayuda para conocer la ubicación física de los datos, así como el alcance de los daños cuando ocurra el fallo de una unidad de disco física.

3.4. LLEVAR A CABO LA INSTALACIÓN.

Una vez seguidos los diferentes pasos hasta aquí, en este punto se debe contar con una lista de comprobación, con al menos los siguientes datos:

- El nombre del sistema donde está el dispositivo desde donde se realizará la instalación.
- El tipo de sistema a instalar: sin disco; sin datos; independiente o servidor.
- El nombre del servidor para el nuevo cliente (caso de sistemas sin disco o sin datos).
- El nombre del sistema y su identificación dentro de la Organización.
- El direccionamiento de red asignado y el resto de los parámetros de configuración de la red.
- Los paquetes o módulos a instalar.
- La partición o división del almacenamiento disponible.

Con esta información pasaremos a realizar el proceso de instalación, respondiendo a las preguntas que éste plantee en los diferentes pasos del mismo.

4. ARRANQUE Y PARADA.

El arranque y la parada de los sistemas se diferencian de otras tareas de administración en que, una vez tomada la decisión de hacerlo, el administrador es más un observador pasivo que un participante activo. La vigilancia y el conocimiento informado se precisan más que la anticipación a los problemas y necesidades.

Mostrándose en la consola del sistema, el arranque genera una gran cantidad de información sobre lo que está ocurriendo. Más importante aún, muestra los dispositivos que reconoce o están interrumpidos y muestra qué tareas se ejecutan. Además, la mayoría de los problemas de arranque generan algún tipo de mensaje sobre la consola del sistema.

4.1. ARRANQUE.

Desde un punto de vista general, el arranque de un sistema es un método de llevar a cabo un conjunto predefinido de tareas, de forma ordenada. Entre esas tareas normalmente se incluirán:

- Ejecución de un conjunto limitado de auto comprobaciones de los elementos hardware del sistema.
- La localización del dispositivo de arranque.
- Lectura del núcleo del sistema operativo desde el dispositivo de arranque.
- Búsqueda e inicialización de periféricos por parte del núcleo del S.O.
- El arranque de las tareas básicas del sistema.
- La ejecución de archivos de comandos o listas de trabajos que proporcionan los servicios.
- Arranque de otras aplicaciones.

4.2. PARADA.

Parafraseando aquello de «todo lo que sube tiene que bajar» (en informática, los sistemas en marcha están «up»: «subidos», «levantados» y los sistemas apagados están «down»: «bajados», «caídos»), alguna vez se hace preciso apagar los sistemas.

Una parada normal es un intento de terminar los procesos de una manera ordenada, para que, cuando se vuelva a arrancar el sistema, éste lo haga con ninguno o los menores errores posibles.

Un apagado ordenado irá acabando tareas con los menores problemas posibles. Posteriormente sincronizará los discos con cualquier salida en los buffer de memoria pendiente de actualizar y procederá a su desmontado o desconexión.

Cuando se deba hacer, es primordial asegurarse de la necesidad de apagar los sistemas. Esta decisión dependerá enormemente de la cultura de la Organización, del número de usuarios a los que afectará y de la gravedad o urgencia del asunto que requiera del apagado.

Cada sistema suele disponer de una variada gama de procedimientos de apagado, incluido el corte del suministro eléctrico. Cada sistema y máquina tiene sus propios procedimientos de apagado, que habrán de conocerse adecuadamente para evitar apagados incorrectos, que deriven en corrupción o pérdida completa de datos, e incluso de equipos.

Es importante conocer que, apagar un sistema eliminando la alimentación eléctrica, o cuando no se ha completado la sincronización (entre los discos y los buffers de memoria), casi seguro producirá la corrupción de algunos archivos del sistema, que precisarán corregirse durante el siguiente arranque. Todos los sistemas cuentan con alguna herramienta, invocada automáticamente por el sistema o de forma manual por el Administrador, para realizar la corrección de estos archivos con problemas, sin embargo, no garantizan la recuperación adecuada de la información contenida en ellos. El riesgo derivado de un apagado incorrecto deberá ser comprendido, evaluado y asumido por el Administrador cuando, ante la dificultad, urgencia o imposibilidad del apagado ordenado, se opte por esta opción.

5. SALVAGUARDA Y RECUPERACIÓN.

En un mundo perfecto, nadie perdería información, los discos no fallarían, los controladores no se estropearían y todos los sistemas insistirían en preguntar si realmente se desea eliminar toda la información de su sistemas.

De acuerdo a las leyes de Murphy, no existe el mundo perfecto. La información se pierde, los discos fallan, las controladoras enloquecen en algún momento. La pregunta no es si lo malo ocurrirá, sino cuándo sucederá.

Por fortuna, los sistemas cuentan con alguna manera de proteger la información, empleando herramientas para el archivado y salvaguardia en dispositivos de almacenamiento extraíbles (cintas magnéticas, CD-ROM o DVD grabables, etc.) o en otros sistemas, a través de la red.

Usualmente, las herramientas suministradas con el sistema tienen una funcionalidad muy limitada y poco amigable. Están orientadas a la salvaguardia del propio sistema y no disponen de utilidades de gestión de bibliotecas, como el seguimiento de las copias, control de cintas, aviso de incidencias, etc.

Una organización normal cuenta con decenas, cientos o miles de ordenadores personales o estaciones de trabajo, en los diferentes puestos de trabajo, conectados en red, actuando como clientes de decenas o cientos de servidores, departamentales y corporativos. Todos ellos almacenan algún tipo de información que es preciso salvar y poder recuperar en caso necesario.

Las herramientas usuales, suministradas con el sistema operativo, son insuficientes para dar una respuesta adecuada a las necesidades de salvaguardia que un entorno así requiere.

En el mercado existe una enorme variedad de productos comerciales, que responden a esta problemática aportando soluciones integradas y centralizadas que permiten, empleando la red, organizar la realización de copias de seguridad, mediante el empleo de programas agente en los equipos implicados, que pueden actuar como gestores de las copias locales (las salvases se realizan en los dispositivos locales de cada sistema, pero su realización o no y el registro de errores se gestiona remotamente a través de la red), o como suministradores de la información a salvar, la cual se almacena en repositorios o unidades de medios extraíbles (cabinas de discos, unidades de cinta, robots automatizados de cintas, etc.) de forma centralizada.

Un sistema integrado de copias de seguridad permite aislar la complejidad que conlleva la salvaguardia de diferentes sistemas, cada uno con una organización diferente de la información. Sin embargo, es un producto caro y de una gran repercusión en toda la organización, dado que todos los equipos de los que se quiera realizar copia de seguridad deben contar con el módulo agente correspondiente, lo que puede repercutir en un número elevado de licencias, y deben estar sometidos a un estricto control de supervisión y mantenimiento, comprobando las posibles actualizaciones y parches de seguridad que los fabricantes publiquen, para asegurar la calidad e integridad de las salvaguardas. También se debe tener en cuenta la posibilidad de recuperación de la información a través de versiones sucesivas del producto forward compatibility (un caso típico es el software de Backup suministrado por Microsoft con sus sistemas operativos, que resulta incompatible entre versiones diferentes del S.O. perdiéndose toda posibilidad de recuperación de la información al actualizar a una nueva versión del S.O.).

Es preciso realizar un estudio exhaustivo de los diferentes productos, pues no existe uno que responda a todas las expectativas, por lo que habrá que definir nuestras necesidades concretas, junto a nuestras expectativas previsibles de futuro, y elegir aquel que mejor responda a ellas.

5.1. DISPOSITIVOS DE ALMACENAMIENTO.

Existen multitud de dispositivos diferentes donde almacenar nuestras copias de seguridad, desde un simple disco flexible hasta unidades de cinta de última generación. Evidentemente, cada uno tiene

sus ventajas y sus inconvenientes, pero utilicemos el medio que utilicemos, éste ha de cumplir una norma básica: ha de ser estándar. Con toda probabilidad muchos administradores pueden presumir de poseer los streamers más modernos, con unidades de cinta del tamaño de una cajetilla de tabaco que son capaces de almacenar gigas y más gigas de información; no obstante, utilizar dispositivos de última generación para guardar los backups de nuestros sistemas puede convertirse en un problema: ¿qué sucede si necesitamos recuperar datos y no disponemos de esa unidad lectora tan avanzada? Imaginemos simplemente que se produce un incendio y desaparece una máquina, y con ella el dispositivo que utilizamos para realizar copias de seguridad. En esta situación, o disponemos de otra unidad idéntica a la perdida, o recuperar nuestra información va a ser algo difícil. Si en lugar de un dispositivo moderno, rápido y seguramente muy fiable, pero incompatible con el resto, hubiéramos utilizado algo más habitual (una cinta DAT, un CD-ROM, o incluso un disco duro) no tendríamos problemas en leerlo desde cualquier sistema similar, sin importar el hardware sobre el que trabaja.

Vamos a comentar algunos de los dispositivos de copia de seguridad más utilizados hoy en día; de todos ellos (o de otros, no listados aquí) cada administrador ha de elegir el que más se adapte a sus necesidades.

Discos flexibles:

Aunque los clásicos diskettes cada día se utilicen menos, aún se pueden considerar un dispositivo donde almacenar copias de seguridad. Se trata de un medio muy barato y portable entre diferentes sistemas operativos (evidentemente, esta portabilidad existe si utilizamos el disco como un dispositivo secuencial, sin crear sistemas de ficheros). Por contra, su fiabilidad es muy baja: la información almacenada se puede borrar fácilmente si el disco se aproxima a aparatos que emiten cualquier tipo de radiación, como un teléfono móvil o un detector de metales. Además, la capacidad de almacenamiento de los floppies es muy baja, de poco más de 1,4 MB por unidad; esto hace que sea casi imposible utilizarlos como medio de backup de grandes cantidades de datos, restringiendo su uso a ficheros individuales.

Un diskette puede utilizarse creándole un sistema de ficheros, montándolo en el sistema de archivos de la máquina y copiando en él los archivos a guardar.

Si quisiéramos recuperar el archivo, no tendríamos más que montar de nuevo el diskette y copiar el fichero en su ubicación original. No obstante, este uso de los discos flexibles es minoritario; es más habitual utilizarlo como un dispositivo secuencial (como una cinta), sin crear en él sistemas de ficheros -que quizás son incompatibles entre diferentes sistemas- sino accediendo directamente al dispositivo.

Discos duros:

Es posible utilizar una unidad de disco duro completa (o una partición) para realizar copias de seguridad; como sucedía con los discos flexibles, podemos crear un sistema de ficheros sobre la unidad o la partición correspondiente, montarla, y copiar los ficheros que nos interese guardar en ella (o recuperarlos). De la misma forma, también podemos usar la unidad como un dispositivo secuencial y convertirlo en un contenedor. En este caso hemos de estar muy atentos a la hora de especificar la unidad, ya que es muy fácil equivocarse de dispositivo y machacar completamente la información de un disco completo (antes también podía suceder, pero ahora la probabilidad de error es más alta). Algo muy interesante en algunas situaciones es utilizar como dispositivo de copia un disco duro idéntico al que está instalado en nuestro sistema, y del que deseamos hacer el backup; en este caso es muy sencillo hacer una copia de seguridad completa.

Cintas magnéticas:

Las cintas magnéticas han sido durante años (y siguen siendo en la actualidad) el dispositivo de backup por excelencia. Las más antiguas, las cintas de nueve pistas, son las que mucha gente imagina al hablar de este medio: un elemento circular con la cinta enrollada en él; este tipo de dispositivos se utilizó durante mucho tiempo, pero en la actualidad está en desuso, ya que a pesar de su alta fiabilidad y su relativa velocidad de trabajo, la capacidad de este medio es muy limitada (de hecho, las más avanzadas son capaces de almacenar menos de 300 MB, algo que no es suficiente en la mayor parte de sistemas actuales). Después de las cintas de 9 pistas aparecieron las cintas de un cuarto de pulgada (denominadas QIC), mucho más pequeñas en tamaño que las anteriores y con una capacidad máxima de varios Gigabytes (aunque la mayor parte de ellas almacenan menos de un Giga); se trata de cintas más baratas que las de 9 pistas, pero también más lentas. El medio ya no va descubierto, sino que va cubierto de una envoltura de plástico. A finales de los ochenta aparece un nuevo modelo de cinta que relegó a las cintas QIC a un segundo plano y que se ha convertido en el medio más utilizado en la actualidad: se trata de las cintas de 8mm, diseñadas en su origen para almacenar video. Estas cintas, del tamaño de una cassette de audio, tienen una capacidad de varios Gigabytes, lo que las hace perfectas para la mayoría de sistemas: como toda la información a salvaguardar cabe en un mismo dispositivo, el operador puede introducir la cinta en la unidad del sistema, ejecutar un sencillo comando, y dejar que el backup se realice durante toda la noche; al día siguiente no tiene más que verificar que no ha habido errores, retirar la cinta de la unidad, y etiquetarla correctamente antes de guardarla. De esta forma se consigue que el proceso de copia de seguridad sea sencillo y efectivo. No obstante, este tipo de cintas tiene un grave inconveniente: como hemos dicho, originalmente estaban diseñadas para almacenar video, y se basan en la misma tecnología para registrar la información. Pero con una importante diferencia: mientras que perder unos bits de la cinta donde hemos grabado los mejores momentos de nuestra última fiesta no tiene mucha importancia, si esos mismos bits los perdemos de una cinta de backup el resto de su contenido puede resultar inservible. Es más, es probable que después de unos cuantos usos (incluidas las lecturas) la cinta se dañe irreversiblemente.

Para intentar solucionar estos problemas aparecieron las cintas DAT, de 4mm, diseñadas ya en origen para almacenar datos; estos dispositivos, algo más pequeños que las cintas de 8mm pero con una capacidad similar, son el mejor sustituto de las cintas antiguas: son mucho más resistentes que éstas, y además relativamente baratas (aunque algo más caras que las de 8mm). En las cintas de 4mm se pueden almacenar hasta 36 GB de información, si bien se pueden emplear sistemas de compresión por hardware, anunciando los fabricantes capacidades de almacenamiento de hasta 72GB (con ratios de compresión 2:1) sin dejar claro si la tecnología usada es estándar o no. Evidentemente, esto puede llevarnos a problemas de los que antes hemos comentado: ¿qué sucede si necesitamos recuperar datos y no disponemos de la unidad lectora original? Es fundamental que nos aseguremos la capacidad de una fácil recuperación en caso de pérdida de nuestros datos (este es el objetivo de los backups al fin y al cabo), por lo que quizás no es conveniente utilizar esta compresión hardware a no ser que sea estrictamente necesaria y no hayamos podido aplicar otra solución.

CD-ROMs:

En la actualidad sólo se utilizan cintas magnéticas en equipos antiguos o a la hora de almacenar grandes cantidades de datos del orden de Gigabytes. Hoy en día, muchos sistemas poseen unidades grabadoras de CD-ROM, un hardware barato y, lo que es más importante, que utiliza dispositivos de muy bajo coste y con una capacidad de almacenamiento suficiente para muchos casos: con una unidad grabadora, podemos almacenar más de 650 Megabytes en un CD-ROM que cuesta menos de 1 euro. Por estos motivos, muchos administradores se decantan por realizar sus copias de seguridad en uno o varios CD-ROMs; esto es especialmente habitual en estaciones de trabajo o en PCs de sobremesa, donde la cantidad de datos a salvaguardar no es muy elevada y se ajusta a un par de unidades de CD, cuando no a una

sola. Podemos utilizar dispositivos CD-RW, similares a los anteriores pero que permiten borrar la información almacenada y volver a utilizar el dispositivo (algo muy útil en situaciones donde reutilizamos uno o varios juegos de copias), o utilizar medios con una mayor capacidad de almacenamiento (CD-ROMs de 80 minutos, capaces de almacenar hasta 700 MB); también es muy útil lo que se conoce como la grabación multisesión, algo que nos va a permitir ir actualizando nuestras copias de seguridad con nuevos archivos sin perder la información que habíamos guardado previamente.

DVDs:

La evolución de los CD-ROMs condujo la aparición de los DVD, originalmente desarrollados para almacenar video, hoy en día constituyen la alternativa a los CD-ROM. Los dispositivos grabadores han descendido a unos precios muy económicos (en torno a los 90 euros) y su capacidad de almacenamiento de unos 4,4 GB (7,5 GB en discos de doble capa) es más que aceptable para realizar copias de seguridad de sistemas clientes y servidores medios y pequeños. También están disponibles los equipos y discos regrabables DVD-RW que permiten borrar la información contenida en ellos para reutilizar el soporte.

5.2. PLANIFICACIÓN DE LAS SALVAGUARDIAS.

Podemos definir diversos tipos de copias de seguridad:

- Aquellas que necesitan de un almacenamiento permanente, pero cuya utilización en un breve plazo no es previsible: proyectos cerrados, cuentas de usuarios que ya no pertenecen a la empresa, copias de seguridad correspondientes a cierres de ejercicio. El método más indicado en estos casos es la grabación en CD-ROM o DVD.
- Aquellas que corresponden al trabajo diario, de frecuente renovación y que deben estar disponibles de forma sencilla. Si bien es posible una política de backups que consista en generar un CD-ROM al finalizar la jornada, no es ésta una actuación sensata (salvo para los vendedores de CD-RW). Por ello se crean las denominadas políticas de backup.

Normalmente podemos hablar de tres, o más, niveles de backup:

- Un backup de primer nivel (diario), que normalmente es realizado sobre disco duro en un servidor de backups. Este backup es incremental, esto es: se guardan solo las modificaciones respecto de la última copia.
- Un backup incremental semanal, que guarda en cinta las diferencias respecto del último backup semanal realizado
- Un backup completo (de nivel 0) mensual, que guarda en cinta el contenido completo de los servidores.

La razón de utilizar un backup de primer nivel (diario) sobre disco duro, en lugar de hacerlo sobre cinta es sencilla: el 99 por 100 de las peticiones de recuperación de datos corresponden a frases del tipo «oye, es que no me he dado cuenta, y he borrado el fichero XXXX que estaba editando. ¿Puedes recuperarme la copia de ayer?». El tener los datos en disco, puede hacer que incluso antes de colgar el teléfono, el usuario vea su fichero restaurado, lo que dará lugar al agradecimiento más efusivo.

Debido a que las diferencias de un día para otro crecen exponencialmente, entre el backup diario y el mensual se realizan backups incrementales semanales, en dispositivos de gran capacidad, que si bien no permiten un acceso «en línea» a los datos, permiten descargar al servidor de backups del exceso de copias diarias.

La política de mantenimiento de las copias de seguridad, deberá ajustarse a las necesidades de la organización. Un sistema contable quizás se vea obligado a mantener la información de al menos cinco años, un sistema de archivo deberá mantener la información tanto tiempo como sea posible.

Una cosa que no se debe olvidar sobre el soporte magnético es que es perecedero: una cinta puede guardar los datos durante unos cinco años, pero debido a campos magnéticos residuales, y a los propios materiales de la cinta, la magnetización remanente va deteriorándose. Es preciso, si se quiere una información no perecedera, proceder al almacenamiento en otros formatos, o bien al «refresco de las cintas», de lo contrario podremos con los años encontrarnos con kilómetros de cinta magnética llena de ruido que en su día fue una colección de datos altamente valiosos.

5.3. VERIFICACIÓN Y CUSTODIA DE LAS SALVAGUARDAS.

Asociados a los backups suelen existir problemas de seguridad típicos en muchas organizaciones. Uno de estos problemas es la no verificación de las copias realizadas:

El administrador ha diseñado una política de copias de seguridad correcta, incluso exhaustiva en muchas ocasiones, pero nadie se encarga de verificar estas copias hasta que es necesario restaurar ficheros de ellas. Cuando llega ese momento, el responsable del sistema se encuentra ante un gran problema, problema que se podría haber evitado simplemente teniendo la precaución de verificar el correcto funcionamiento de los backups.

Restaurar una copia completa para comprobar que todo está correcto puede ser demasiado trabajo para los métodos habituales de operación, una alternativa posible pasa por tratar de recuperar varios ficheros aleatorios del backup, asumiendo que si esta recuperación funciona, toda la copia es correcta.

Otro problema clásico de las copias de seguridad es la política de etiquetado a seguir. Son pocos los administradores que no etiquetan los dispositivos de backup, algo que evidentemente no es muy útil: si llega el momento de recuperar ficheros, el operador ha de ir cinta por cinta (o disco por disco, o CD-ROM por CD-ROM...) tratando de averiguar dónde se encuentran las últimas versiones de tales archivos.

Muchos administradores, por el contrario, siguen una política de etiquetado exhaustiva, proporcionando todo tipo de detalles sobre el contenido exacto de cada medio; esto, que en principio puede parecer una posición correcta, no lo es tanto: si por cualquier motivo un atacante consigue sustraer una cinta, no tiene que investigar mucho para conocer su contenido exacto, lo que le proporciona acceso a información muy concreta (y muy valiosa) de nuestros sistemas sin ni siquiera penetrar en ellos.

La política correcta para etiquetar los backups ha de ser tal que un administrador pueda conocer la situación exacta de cada fichero, pero que no suceda lo mismo con un atacante que sustraiga el medio de almacenamiento; esto se consigue, por ejemplo, con códigos impresos en cada etiqueta, códigos cuyo significado sea conocido por los operadores de copias de seguridad pero no por un potencial atacante.

La ubicación final de las copias de seguridad también suele ser errónea en muchos entornos; generalmente, los operadores tienden a almacenar los backups muy cerca de los sistemas, cuando no en la misma sala. Esto, que se realiza para una mayor comodidad de los técnicos y para recuperar ficheros fácilmente, es un grave error: no hay más que imaginar cualquier desastre del entorno, como un incendio o una inundación, para hacerse una idea de lo que les sucedería a los backups en esos casos. Evidentemente, se destruirían junto a los sistemas, por lo que la organización perdería toda su información. No obstante, existen voces que reivindican como correcto el almacenaje de las copias de seguridad junto a los propios equipos, ya que así se consigue centralizar un poco la seguridad (protegiendo una única estancia se salvaguarda tanto las máquinas como las copias).

Lo habitual en cualquier organización suele ser un término medio entre ambas aproximaciones: se puede disponer de un juego de copias de seguridad completas en un lugar diferente a la sala de operaciones, pero protegido y aislado como ésta, y un juego para uso diario en la propia sala, de forma que los operadores tengan fácil la tarea de recuperar ficheros. También se pueden emplear armarios ignífugos que requieran de ciertas combinaciones para su apertura (combinaciones que sólo determinado personal ha de conocer), si se opta por almacenar todos los backups en la misma estancia que los equipos.

6. CONTROL DE CAMBIOS Y GESTIÓN DE INCIDENCIAS.

El control de cambios es la aprobación formal y documentada de cualquier modificación en el sistema informatizado durante su vida operativa. El control de cambios será necesario cuando una modificación pueda afectar el estado de validación del sistema informatizado. Los procedimientos de control de cambios deberán estar aprobados antes de que el sistema sea operativo.

El control de cambios es una actividad procedimental que asegura la calidad y la consistencia a medida que se realizan cambios en los objetos de la configuración. El proceso de control de cambios comienza con una petición de cambio, lleva a una decisión de proseguir o no con el cambio y culmina con su actualización controlada.

El procedimiento deberá describir el método de evaluación para determinar las pruebas necesarias para mantener el estado de validación del sistema. El procedimiento de control de cambios deberá identificar a los responsables de valorar y aprobar los cambios necesarios.

Sea cual fuere el origen del cambio, proveedor o desarrollo interno, deberá disponerse de la información apropiada dentro del proceso de control de cambios. Los procedimientos de control de cambios deberán garantizar la integridad de los datos.

Por otro lado, contar con una correcta gestión de incidencias es un punto fundamental de toda gestión de sistemas. No solo permite un adecuado control y tratamiento de las anomalías que surgen durante la operación diaria de los sistemas, sino que constituye la parte más visible, de cara al usuario, del departamento de informática.

A través de los mecanismos de gestión de incidencias, los usuarios canalizan sus necesidades de comunicación con el departamento informático, los errores en la operación, las nuevas necesidades de información, etc. De la respuesta que obtengan, dependerá en gran medida la imagen que el departamento informático tendrá en el seno de la organización.

Este punto de contacto entre los usuarios y la informática de la organización se materializa a menudo en un CAU o Centro de Atención de Usuarios, que actúa como punto de entrada en el sistema de gestión de incidencias y primer paso en la atención al usuario, aportando asistencia inmediata a problemas de pequeña complejidad, o ya documentados en la base de conocimiento del SGI y de solución conocida.

A continuación estudiaremos las tendencias organizativas que empujan a la creación de las funciones de control de cambios y gestión de incidencias, para posteriormente estudiar su desarrollo.

6.1. TENDENCIAS EN LA ORGANIZACIÓN.

La situación actual en las organizaciones es que el personal dedicado a la función de las tecnologías de la información ha disminuido, por presiones competitivas, y tiende a estabilizarse. Por contra, movimientos tecnológicos como el downsizing han supuesto un incremento de los costes de posesión de los recursos informáticos, con un claro aumento del ratio coste trabajo/coste de capital por plataforma, que ha pasado, según el Gartner Group, de un 55%/45% en un entorno centralizado, a un 83%/17% en un entorno de PC aislados y a un 69%/31% en un entorno LAN.

Si a esto añadimos el hecho de haber pasado de proporcionar software y productos, a proporcionar middleware y herramientas, lo que conlleva que los usuarios finales están realizando aplicaciones (con los problemas que esto implica para su mantenimiento, la consistencia de las informaciones, etc.), nos encontramos con una organización distribuida geográficamente y funcionalmente, con unos usuarios a los que hay que dar un servicio integral y una función informática cada vez más reducida, sufriendo la presión competitiva del outsourcing.

En este panorama de búsqueda impuesta de la calidad, y evolución de la función informática desde su concepción como centro de costes, a su función como un centro de servicios, la importancia de una buena gestión de incidencias y cambios se hace patente, al ser éste el punto crítico para la percepción del servicio por parte de los usuarios, tanto si éste es prestado de forma interna, como si es realizado por una organización externa.

6.2. EL ACUERDO DE NIVEL DE SERVICIO.

Desde esta nueva óptica, se entiende por gestión de incidencias y cambios en una organización: aquella función o proceso, encargado de minimizar el impacto que las incidencias o cambios puedan tener sobre los objetivos de la organización.

Para ello es esencial el llegar a establecer un acuerdo de nivel de servicios (SLA, Service Level Agreement, en su versión inglesa), en el que deberán establecerse los objetivos a los que se compromete la función informática, siempre en función de los recursos que tenga asignados. Para su adecuado cumplimiento deberá comenzarse por dar lo básico, para poco a poco ir construyendo credibilidad en la organización sobre la función informática, y finalmente, poder integrar ésta dentro de la planificación estratégica de la organización, de forma que sea capaz de aportar valor añadido al negocio propiamente dicho.

En este acuerdo deberán recogerse claramente los objetivos comprometidos. Estos objetivos deberán ser concretos y medibles mediante indicadores que permitan realizar su adecuado seguimiento. Ejemplo de estos indicadores pueden ser el tanto por ciento de disponibilidad, el horario de actividad, etc.

Por último, reseñar la importancia de asignar claramente las responsabilidades en caso de incumplimiento, así como las concernientes a la realización del seguimiento y control del acuerdo.

6.3. ORGANIZACIÓN.

Para lograr desde la función informática el seguimiento y cumplimiento del acuerdo de nivel de servicios, es necesario la creación de un grupo especializado, cuyo tamaño variará en función de la organización, y entre cuyas funciones estarán:

- Obtener información sobre la calidad percibida por los usuarios.
- Abrir, seguir y resolver las incidencias y cambios que se produzcan desde su nacimiento hasta su resolución o abandono.
- Estandarización de los procedimientos de acceso a la función.
- Informar a los usuarios sobre los nuevos productos, sobre los cambios previstos, sus ventajas, inconvenientes, etc.
- Informar a la dirección de las excepciones.
- Centralizar el control.

Este último punto, la centralización, es importante, especialmente en las grandes organizaciones. En estas últimas suelen categorizarse las incidencias y los cambios en función de su importancia o dificultad. Este escalonamiento en gradas de servicio, permite asignar el personal más valioso a aquellos problemas más importantes y difíciles de resolver, siguiendo el principio de Pareto del 80/20. Un ejemplo de clasificación típico es el escalonar los problemas en cinco gradas, aunque esto depende mucho de la organización propiamente dicha. Siguiendo este ejemplo tendríamos las siguientes categorías:

Categoría 0:

Categoría de emergencia. Se trata de un problema o cambio que paraliza todo el servicio proporcionado por la instalación.

Categoría 1:

Categoría de urgencia. Se trata de un problema o cambio muy complejo que, o bien no permite una vuelta a atrás, o bien paraliza una función, o afecta a prácticamente a todos los usuarios, o bien es el resultado de una escalada de la incidencia o cambio desde la grada inferior.

Categoría 2:

Se trata de problemas o cambios que presentan un riesgo grave predecible, o bien en caso de fallo llevarían aparejados un largo proceso de recuperación, o bien son susceptibles de parar toda una aplicación.

Categoría 3:

Se trata de problemas o cambios de solución sencilla, rápida y efectiva, y que en el peor caso afectarían a un grupo no muy grande, ni importante de usuarios.

Categoría 4

Son los problemas o cambios que se presentan prácticamente a diario, o bien de situaciones que en un futuro más o menos próximo podrían originar algún tipo de problema.

Finalmente, volver a incidir en lo importante del control de los indicadores de cumplimiento y la monitorización de este servicio con índices como el tiempo medio entre fallos (MTBF, Mean Time Between Failures); tiempos de respuesta; tanto por ciento de disponibilidad; número de incidencias abiertas, cerradas, pendientes, etc.

La medición y el control del acuerdo de nivel de servicio es imprescindible para poder evaluar el rendimiento del servicio prestado por la función informática, así como para medir la adecuación entre las necesidades de los usuarios y el servicio prestado por dicha función, verdadera piedra angular de la calidad de este servicio.

Para ello es muy interesante el complementar los índices de seguimiento con lo que se conoce como encuesta de satisfacción de usuarios (CSS, Customer Satisfaction Survey, en su acrónimo inglés más conocido). Esta encuesta, que deberá hacerse preferiblemente de forma automatizada y debidamente ajustada al nivel de cada usuario, nos permitirá, por una parte, conocer la calidad percibida por los usuarios del servicio prestado, pudiendo, de esta manera, orientar nuestro servicio mucho mejor hacia sus necesidades reales, consiguiendo así una mayor satisfacción de los usuarios y un mejor aprovechamiento de los recursos. Por otra parte, nos permite el publicar dichos resultados, fomentando de esta forma la comunicación con los usuarios, y contribuyendo a aumentar la credibilidad de la función informática. Una función que aún tiene mucho que hacer en esta área hasta alcanzar su madurez.

6.4. CONTROL DE CAMBIOS.

Tanto la gestión de incidencias, como el control de cambios, precisan contar con un conocimiento preciso de los sistemas sobre los que se actúa, para ello, es necesario disponer de un completo, exhaustivo y actualizado inventario de todos los recursos informáticos de la organización. El mantenimiento actualizado de ese inventario es fundamental para el resto de los procedimientos, ocupando un puesto muy importante el control de las licencias de software, por la enorme repercusión económica y legal, que puede derivarse de un inadecuado control.

6.4.1. Inventario de recursos.

El punto de arranque para una adecuada gestión de las diferentes plataformas que hay en toda organización, es la confección de un inventario actualizado de todos los recursos hardware y software con los que cuenta dicha organización.

Para ser útil, este inventario deberá estar automatizado y ser gestionado mediante algún tipo de base de datos.

El nivel de detalle con el que se mantenga el inventario puede variar, dependiendo de las necesidades específicas de la organización. Sin embargo, en general deberá incluir:

- Una lista de todos los sistemas hardware y la configuración de cada sistema.
- Una lista de todos los componentes software utilizados en cada sistema hardware (o clases de sistemas), y la versión o número de actualización de cada elemento software.
- Cómo están organizados los grupos de trabajo a través de las conexiones de red.

Existen programas que siguen automáticamente las aplicaciones en servidores y estaciones de trabajo, explorando sus unidades de disco. Estos programas de control de inventario recopilan información del hardware y software automáticamente, utilizando para ello listas de componentes estándar de hardware y aplicaciones conocidas. Desgraciadamente, estas listas no son ni mucho menos completas, y por otra parte, se desactualizan con una pasmosa facilidad, por lo que su utilidad es muy relativa, en especial en entornos suficientemente grandes y variados.

El contar con un inventario actualizado es la piedra angular de toda gestión integral de sistemas, y más aún cuando parte de esta se contrate externamente, como suele ocurrir con la gestión de incidencias. En este caso el inventario es la base de la negociación económica del contrato y constituye los elementos cubiertos por dicho contrato, por lo que conviene esmerarse en su confección al objeto de no incurrir en costes inútiles, ni caer en problemas de falta de cobertura. Además, la propia función de gestión de incidencias debe realimentar el inventario de forma sencilla, ya que cualquier incidencia puede servir para comprobar los datos que se poseen referentes al elemento que la ha causado, pudiendo de esta forma, detectarse cualquier variación, autorizada o no, que se haya podido producir desde la última actualización del inventario, lo que es especialmente útil, dada la extraordinaria velocidad con que se produce la obsolescencia tanto del hardware como del software.

6.4.2. Distribución del software e instalación del hardware.

Una vez hecho el esfuerzo de recopilar un inventario de recursos, para que éste sea de alguna utilidad debe mantenerse todo el entorno bajo control. Tanto la instalación de opciones hardware y nuevos sistemas, como la distribución e instalación de las actualizaciones software y/o nuevo software en los clientes y en los servidores, debe quedar perfectamente reflejada en el inventario.

Los cambios en el hardware requieren la intervención manual, de tal forma que el proceso no puede ser automatizado totalmente. Sin embargo, el inventario hardware puede ser actualizado simultáneamente para reflejar dichos cambios de forma fehaciente.

Los cambios software, por contra, pueden ser automatizados casi por completo. Ambos procesos, la instalación del software y la actualización del inventario, pueden ser llevados a cabo automáticamente y de forma concurrente, aunque siempre deba hacerse bajo el estricto control de los administradores de los sistemas.

Idealmente, una herramienta de distribución automática de software, debería funcionar con todos los sistemas operativos principales y de forma transparente para encaminadores (routers) y enlaces WAN (red de área extensa), dejando un adecuado registro de todos y cada uno de los sistemas actualizados, así como de las operaciones realizadas en cada uno de ellos.

6.4.3. Control de licencias software.

Un elemento clave en la gestión de cambios en el software, es el control de las políticas de licencias de los paquetes comerciales.

Para sistemas que no están interconectados, el control de las licencias software es relativamente simple. Esto es así, por que cada compra de software precintado se maneja de forma individual. Sin embargo, en un entorno distribuido y fuertemente interconectado se requiere un modelo de licencias más flexible, con el objeto de optimizar el uso efectivo de los acuerdos de licencias y al mismo tiempo, el coste de los productos software, de forma que éste sea un fiel reflejo de su uso real.

En una misma organización, pueden estar en vigor múltiples políticas de licencias. Así para un suministrador de software, la política de compras podría basarse en el número de licencias en uso en un momento determinado (licencias «flotantes» o de acceso concurrente), mientras que respecto a otro suministrador podría adoptarse la política de contar con una licencia por cada usuario específico de ese producto. En función del número de licencias y de su utilización se elegirá la menos onerosa para la organización.

Para asegurar que ambas políticas se ajustan a la legalidad vigente respecto al uso del software, así como para optimizar el coste del software en uso, la organización necesita de una herramienta que facilite dicho control y proporcione la información necesaria para su ejecución.

Los cada vez mayores costes de soporte del software, junto con las actualizaciones superfluas, hacen que los costes, ya de por sí importantes, de la adquisición de las licencias necesarias para su uso, sean pequeños en comparación con los costes de posesión de dichas licencias. Un estudio del Gartner Group pone de manifiesto que el soporte del software supone el 45 por 100 del coste total de propiedad de una aplicación, las tareas administrativas, como por ejemplo controlar que se cumplen las licencias de uso simultáneo, representan otro 13 por 100. Por contra, el coste de la adquisición de las licencias representa únicamente el 14 por 100 del coste total.

Los programas de control de inventario de software tienen una forma pasiva de hacer cumplir con las licencias que realmente se poseen, permitiendo que los responsables sepan qué es lo que se está ejecutando en la red. Estos programas, generan listas de aplicaciones que residen en la red y en los discos locales. Estas listas pueden contrastarse con las compras de software realizadas para, de esta forma, evitar incurrir en problemas legales sobre utilización de software.

Las herramientas específicas de medición o control de licencias, permiten además, el bloqueo en la ejecución para garantizar el cumplimiento de las condiciones de los contratos. Permiten determinar esquemas de utilización sobre los que basar las decisiones de compra y soporte, en función por ejemplo del tiempo de utilización e inactividad del software comercial, etc. Permiten también compartir licencias entre distintos servidores, reubicando dinámicamente las licencias no utilizadas dentro de la organización. Pueden permitir el situar a los usuarios en una cola cuando están ocupadas todas las licencias simultáneas, notificando, en su caso, al usuario en espera cuándo se ha liberado la licencia para su uso. Pueden contar con detectores de inactividad para liberación de licencias, priorización en la asignación de las licencias, etc. Todo esto nos puede permitir el realizar prácticas de ahorro que hagan que estas herramientas cuenten con un tiempo de amortización muy pequeño, entre ellas podríamos reseñar las siguientes:

- Reducir el número de licencias compradas, evitando la compra de nuevas copias de paquetes de aplicaciones que ya se poseen, y de los que se cuenta con licencias que apenas se están utilizando.

- Centralizar las compras para reducir el coste por licencia, aprovechando las ventajas de los descuentos por volumen y los menores costes que, en su caso, podrían tener las licencias por ubicación.
- Contratar licencias de uso simultáneo (de las que se necesitarán muchas menos) y utilizar las mediciones para garantizar el cumplimiento de los términos y condiciones del contrato.
- Reubicar dinámicamente o compartir las licencias para utilizar al máximo cada una de ellas.
- Reducir las llamadas repetidas al centro de soporte, contrastando los comportamientos de uso de software con la frecuencia de llamadas al centro de soporte.
- Imputar los costes de soporte a individuos y departamentos según su uso, no según el número de personas del departamento.
- Reducir el tiempo de inactividad en la red debida a la acción de los virus, al impedir que se ejecute cualquier software no autorizado.
- Evitar multas por uso de software sin licencia en los equipos de la organización.

6.5. HERRAMIENTAS DE GESTIÓN DE INCIDENCIAS Y CAMBIOS.

Existen múltiples herramientas que automatizan, en lo posible, esta función, y que sobretodo, ayudan a realizar su tarea y seguimiento. Estas herramientas se pueden clasificar en:

Control de llamadas.

Se trata de herramientas que permiten abrir, tratar, seguir y cerrar consultas, incidencias y cambios. Permiten obtener listados, estadísticas y realizar consultas sobre los ya realizados. Suelen ser herramientas que corren sobre ordenadores personales o estaciones de trabajo.

Gestión de problemas y cambios.

Se trata de herramientas que cuentan con una base de datos de configuración, incidencias y cambios. Permiten la realización de inventarios y dan soporte a la escalada de problemas mediante sistemas de Workflow o Workgroup.

Herramientas integradas.

Se trata de herramientas que incluyen el control del acuerdo de nivel de servicios, permiten integrar la gestión de configuración e incluyen sistemas basados en el conocimiento, capaces de asesorar en el tratamiento de las incidencias y cambios, no sólo basados en la experiencia de la propia instalación, sino que también incorporan conocimiento de otras instalaciones.

En definitiva, se trata de un mercado con cientos de productos y en continua ebullición, conforme las organizaciones van tomando conciencia de la necesidad de contar con un adecuado sistema de gestión de incidencias y control de cambios, que le garantice la continuidad y calidad de sus servicios informáticos, de los que depende, cada vez más, su propia subsistencia.

7. CONTABILIDAD Y MONITORIZACIÓN DEL SISTEMA.

De entre las funciones que un sistema operativo debe tener, para permitir la gestión y correcta administración del mismo, se encuentran las funciones de Contabilidad. Es necesario que el sistema operativo lleve una contabilidad detallada de la utilización de todos sus recursos para, por un lado, poder evaluar la carga que soporta y permitir la configuración del sistema de acuerdo a las necesidades reales y, por otro lado, poder tarificar los servicios prestados (si ello fuese necesario o conveniente).

Hay que señalar que esta función de la administración de sistemas, se convierte en crítica cuando hablamos de su aplicación en sistemas grandes o muy grandes y en aquellos cuyo funcionamiento es crítico. Es muy distinto hablar de la posible ineficiencia en el funcionamiento de nuestro ordenador doméstico o incluso en el ordenador de escritorio de la oficina, donde garantizar que estamos realizando los trabajos de forma suficientemente concurrente y con una gestión óptima de los recursos disponibles no es primordial, a referirnos a los grandes ordenadores que generalmente llevan asociado un sistema de información crítico para una empresa, donde la detección prematura de problemas y el uso eficiente, o no, que se esté dando de él puede repercutir en unos costes verdaderamente importantes e incluso en la propia supervivencia de la empresa.

Cabe destacar la tendencia que han experimentado los sistemas medios, perdiéndose en muchos casos el aspecto crítico que tenían estas funciones en el pasado, debido fundamentalmente a la caída del precio del hardware (lo que repercute en los costes derivados de un posible fallo o mal funcionamiento), aún así tiene una gran importancia a la hora de la detección prematura de problemas.

La función de contabilidad, usualmente se encuentra minusvalorada en casi todas las organizaciones, cuando realmente es una fuente inagotable de información muy útil y susceptible de utilizarse para lograr drásticas reducciones de costes.

Mediante estas herramientas se pueden obtener todo tipo de información útil, como es: tiempos de conexión por usuario y sistema (o aplicación); grado de utilización del espacio de almacenamiento; tiempo de acceso a archivos; uso del procesador y de todos y cada uno de los diferentes recursos del sistema.

Toda esta información tiene un doble uso. Por un lado se debe utilizar para realizar el análisis del rendimiento de los sistemas, redes, bases de datos... y poder de esta forma realizar una adecuada planificación de la capacidad de los sistemas y recursos, con los consiguientes ahorros, al tomar las decisiones de ampliaciones y compras sobre datos reales y no sobre impresiones.

Por otro lado, y cada vez en mayor medida, la función de las tecnologías de la información debe pasar de ser considerada como un centro de costes a integrarse dentro de la planificación estratégica de la empresa. En este camino, se debe comenzar por pasar de ser un centro de costes a ser un centro de servicios y facturar internamente por los servicios que se prestan. Esta imputación de costes y su mero conocimiento por parte de los responsables del resto de las áreas funciones de la empresa, puede hacer que se cambien multitud de ideas preconcebidas sobre la informática, que el diálogo sea más fluido y haya una más adecuada relación entre las peticiones de las áreas de la empresa y sus necesidades reales.

7.1. EL SISTEMA DE CONTABILIDAD.

El sistema de contabilidad tiene por misión, recabar información sobre el uso de los recursos del sistema, empleados por usuarios o grupos de usuarios. Los informes de contabilidad generados por el sistema, proporcionan información que, el Administrador de Sistemas, puede emplear para evaluar la asignación actual de recursos, los límites de recursos y los topes establecidos, así como predecir futuros requerimientos.

En general, una vez que el sistema se ha inicializado, asumiendo que se ha activado la contabilidad del sistema (la tarea de contabilidad afecta el rendimiento de todo el sistema, por lo que debe ser activada con cuidado), comienza la recolección de estadísticas. Los datos recogidos corresponden a alguna de las siguientes categorías:

- Estadísticas de Sesiones establecidas: la unidad responsable de los sistemas de información de la Organización puede emplear las estadísticas de sesiones para facturar a cada usuario por el tiempo que ha estado empleando los recursos del sistema.
- Uso de Procesos: el sistema de contabilidad también recoge estadísticas de los procesos individuales, ejecutados en el sistema, con indicadores de los recursos asignados (memoria, tiempo de CPU, estadísticas de E/S) lo que permite una política de imputación de costes más adecuada que el mero tiempo de conexión. Estas estadísticas permiten al administrador detectar procesos sumidero de recursos, que puedan ocasionar problemas de rendimiento en el conjunto del sistema.
- Utilización del espacio en disco: la contabilidad proporciona la capacidad de monitorizar la utilización del espacio de almacenamiento. Si se establece para los usuarios un cierto límite de uso, es posible crear un sistema de topes o cuotas para evitar que, un solo usuario, acapare todo el espacio disponible.
- Uso de impresoras: la contabilidad de impresoras permite controlar el volumen de emisión de papel a través de los sistemas, guardando información como el número de páginas imprimidas por usuario.
- Uso de la red: la contabilidad de la red guarda estadísticas sobre el volumen de información transmitido o recibido a través de los dispositivos de la red, esto permite conocer la participación del sistema en el tráfico total de la red. Otros datos más útiles son las estadísticas sobre recepciones o transmisiones fallidas y otras anomalías que pueden ayudar a detectar una red con problemas.

Usualmente, el sistema de contabilidad almacena la información en archivos especiales. Sobre ellos, mediante procesos manuales o automatizados, se generan las diferentes estadísticas solicitadas, en un formato legible para el usuario.

En resumen, el sistema de contabilidad genera información útil para, entre otras cosas:

- Establecer un sistema de cobro por uso, equitativo.
- Monitorizar el uso de los recursos del sistema.
- Emplearlo como base para el establecimiento de cuotas de recursos.
- Proporcionar información para justificación de costes ante los gestores.
- Efectuar previsiones de necesidades futuras.

7.2. MONITORIZACIÓN DEL RENDIMIENTO.

Una gran parte de la utilidad del sistema de contabilidad reside en la información que aporta sobre la utilización del sistema y su rendimiento. Algunos de los informes obtenidos son de gran utilidad en la detección de problemas de rendimiento.

Parece obvio decir que cuando la productividad de los usuarios se ve afectada, también se ve afectado el tiempo y el dinero de la organización (a veces en grandes cantidades). Mediciones básicas sobre la pérdidas de tiempo, causadas por un bajo rendimiento, pueden ser suficiente para justificar nuevas inversiones o actualizaciones de viejos sistemas.

A menudo sucede que solamente se comienzan a estudiar las variables que están afectando el rendimiento de los sistemas, cuando existe la queja de los usuarios, lo que en sí mismo es ya parte del problema. El Administrador de sistemas debería tener un conocimiento exhaustivo de la actividad del sistema antes de que salte la crisis a los usuarios. El administrador debe conocer las características de cada grupo de usuarios del sistema, esto incluye el tipo de trabajo que realizan durante la jornada laboral, así como los trabajos que generan para procesar en modo desatendido el resto de las horas. Cuáles son los requerimientos de CPU, de E/S y de memoria de los trabajos más frecuentes o más importantes, qué impacto provocan esos trabajos sobre las redes conectadas al sistema, así como los condicionantes temporales de los trabajos (p. ej. una nómina debe terminarse en una determinada fecha).

El conocimiento de estos perfiles de actividad y requisitos de usuario, pueden ayudar al Administrador a adquirir una comprensión global de la actividad del sistema. Este conocimiento no solo será útil en el caso de que surja una crisis de rendimiento, sino en el caso de una degradación paulatina del sistema.

Mientras el sistema se encuentra en marcha, éste mantiene una serie de contadores para contabilizar el uso de los recursos críticos del sistema. Los recursos más relevantes son:

- Utilización de la CPU.
- Actividad de E/S de disco.
- Actividad en los terminales.
- Actividad de cambio de contexto (cuando se pasa de modo usuario a modo kernel).
- Actividad de las peticiones.
- Actividad de paginación.
- Asignación de memoria para el núcleo del sistema.
- Compartición remota de archivos.
- Uso de buffers.
- Actividad de E/S de dispositivos.
- Actividad de llamadas al sistema.
- Utilización del acceso a ficheros.
- Comunicaciones entre procesos.
- Memoria disponible y área de intercambio o memoria auxiliar.
- Tablas del sistema.

Mediante el estudio de los informes basados en estos contadores es posible determinar cómo están comportándose los tres subsistemas más importantes: CPU, Memoria y la Entrada/Salida.

La monitorización del rendimiento y el ajuste de los sistemas no es siempre una ciencia exacta. Diferentes grupos de usuarios tienen diferentes necesidades de recursos, y no siempre es posible un ajuste perfecto. Algunos grupos necesitan capacidad de proceso, otros necesitan capacidad de E/S y otros requieren de gran capacidad de comunicaciones. El ajuste del rendimiento es siempre una sucesión de aproximaciones y compromisos. El éxito reside en conseguir un compromiso óptimo que satisfaga las necesidades de recursos del sistema de la mayoría de los usuarios.

BIBLIOGRAFÍA

- Temario de las pruebas selectivas para ingreso en el Cuerpo Superior de Sistemas y Tecnologías de la Información de la Administración del Estado. ASTIC.
- Temario de las pruebas selectivas para el acceso, por promoción interna, al Cuerpo de Gestión de Sistemas e Informática de la Administración del Estado. Ministerio para las Administraciones Públicas.
- Seguridad en UNIX y Redes. Antonio Villalón Huerta.
- UNIX Unleashed, System Administrator's Edition. Robin Burk and David B. Horvath, CCP, *et al.* Macmillan Computer Publishing.

