



## 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](http://www.cef.es)

[info@cef.es](mailto:info@cef.es)

### Índice Tema 3

---

1. Administración de redes locales.
2. Gestión de usuarios.
  - 2.1. Gestión de usuarios.
  - 2.2. Gestión de datos.
3. Gestión de dispositivos.
  - 3.1. Impresión.
  - 3.2. Conceptos de backup y recuperación.
4. Monitorización y control de tráfico.





## 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 3

**Administración de redes locales. Gestión de usuarios. Gestión de dispositivos. Monitorización y control de tráfico.**

#### 1. ADMINISTRACIÓN DE REDES LOCALES.

La administración de redes se está convirtiendo en un elemento esencial para asegurar la disponibilidad tanto física como lógica de las redes locales. La complejidad de las actuales redes impone la necesidad de utilizar sistemas de gestión capaces de controlar, administrar y monitorizar redes locales y extensas, a la vez que dispositivos de interconexión, los servidores y sus clientes.

En la actualidad existen diferentes niveles en la concepción de las herramientas de ayuda a la gestión; cada uno de estos niveles permite acometer una problemática particular del entorno de redes y en general no están integrados en un único sistema capaz de proporcionar una visión completa de los subsistemas que conforman las redes.

Un elevado porcentaje del mantenimiento de redes de área local, motivada por la evolución de los sistemas operativos de red, se realiza hoy en día por acceso remoto. De esta forma propietarios de redes pequeñas pueden recibir asistencia contratada de forma instantánea.

En la misma línea los servicios de interconexión ofrecidos por operadores de telecomunicaciones pueden delegar la gestión de los elementos de red al contratista o bien ofrecer informes periódicos para el seguimiento del servicio.

La tendencia en la evolución de la tecnología de gestión de redes se encamina hacia el desarrollo de productos integrados capaces de gestionar conjuntamente subsistemas de voz, datos e imagen en sus diferentes niveles: medio físico de transmisión, redes, aplicaciones, etc.

¿Qué es la gestión de redes?

La ISO (International Organization for Standardization) define la gestión de red como:

«El conjunto de elementos de control y supervisión de los recursos que permiten que la comunicación tenga lugar sobre la red».

La gestión de redes comprende las herramientas necesarias para realizar las siguientes funciones:

Supervisión de la red:

Se suele realizar de dos formas: mediante una estación de gestión ordenador personal o estación de trabajo que reciba mensajes de los dispositivos de la red (puentes o bridges, encaminadores o routers, servidores de terminales, etc.) o mediante una estación que pregunte regularmente el estado de los dispositivos.

Control de los dispositivos de la red:

Se realiza enviando comandos por la red desde la estación de gestión hasta los dispositivos de la red para cambiar su configuración.

Los sistemas de gestión de redes permiten satisfacer requisitos de tipo técnico y funcionales:

Requisitos técnicos:

- Administración de entornos heterogéneos desde una misma plataforma.
- Administración de elementos de interconexión.
- Interfaces con grandes sistemas.
- Interfaz gráfico amigable.
- Evolución según las necesidades del cliente.

Requisitos funcionales

- Gestión del nivel de servicio para garantizar la disponibilidad, la atención a los usuarios, el tiempo de respuesta, etc.
- Gestión de problemas para facilitar la segmentación de los mismos resolviéndolos en etapas o niveles.
- Gestión de cambios para minimizar el impacto asociado habitualmente con los procesos de modificación de las configuraciones existentes.
- Apoyo a la toma de decisiones y facilitar que la gestión de red actúe de puente, o interfaz entre el personal técnico y la dirección, gracias a la facilidad de generar informes.
- Apoyo en la resolución de incidencias para preservar la experiencia del grupo de gestión, reduciendo el tiempo de resolución de situaciones que deberían ser familiares.
- Apoyo en la formación para reducir el esfuerzo de aprendizaje y optimizar el grado de uso requiriendo perfiles de personal poco exigentes.

Los sistemas de gestión deben poder crecer a medida que crecen las necesidades de los usuarios, de forma que se puedan proteger las inversiones realizadas. Un entorno integrado de gestión es una combinación de recursos humanos, organizativos y tecnológicos. La gestión de redes es una estrategia a largo plazo que puede afectar a todo el personal de una organización:

- A los usuarios de la red que necesitan acceder a la información de estado de la misma.
- A los directivos que han de preocuparse de cómo afectarán las prestaciones de la red al desarrollo de sus áreas dentro de la organización.
- A los administradores de red que se encargan de la operativa diaria.

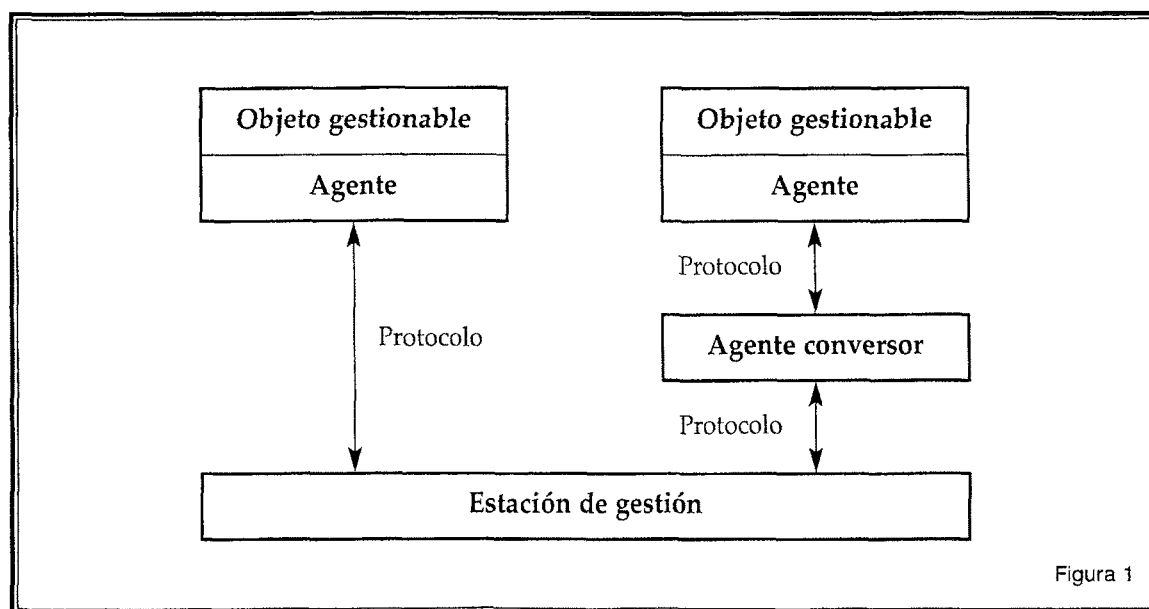
Administración de la red.

Ademas de la gestión operativa (atender usuarios, resolver fallos en el menor tiempo posible, monitorizar, etc.) existen otros aspectos involucrados que permiten definir el análisis y la optimización de la red:

- Descripción funcional de tareas que serán objeto de la gestión.
- Adecuación organizativa en las entidades, organismos, centros o empresas.
- Especificación de procedimientos que faciliten la tramitación de sucesos de interés.
- Adquisición de medios técnicos.
- Adaptación de los medios humanos disponibles.

Componentes de un sistema de gestión.

Los componentes de un sistema de gestión de red y las relaciones entre ellos se representa en el siguiente diagrama:



Cada uno de los elementos tiene el siguiente significado:

- Objeto gestionable: representa cualquier dispositivo físico o lógico de la red y el equipamiento lógico relacionado con él que permita su gestión.
- Agente: es el equipamiento lógico de gestión que reside en el objeto gestionable.
- Protocolo: utilizado por el agente para pasar información entre el objeto gestionable y la estación de gestión.
- Objeto ajeno: se define como un objeto gestionable que utiliza un protocolo ajeno, es decir un protocolo distinto al de la estación de gestión.
- Agente conversor: actúa de conversor entre el protocolo ajeno y el protocolo utilizado por la estación de gestión.
- Estación de gestión: está formada por varios módulos o programas corriendo en una estación de trabajo u ordenador personal. En el siguiente gráfico se muestran los componentes de la estación de gestión.

A continuación se hace una descripción de los componentes de la estación de gestión:

- Interfaz de usuario: es la interfaz entre el usuario y el sistema y puede ser en modo carácter o gráfico.
- Base de datos: mantiene cualquier información de la red (descripciones de diferentes parámetros, configuración de contadores...), almacenando el histórico de eventos y permitiendo la realización de seguimientos.
- Programa monitor: supervisa las condiciones actuales y permite la inspección futura. Visualiza las alarmas activadas por los agentes, y realiza actualizaciones mediante sondeos regulares.
- Arranque y configuración: comprueba que cada estación pueda ser atendida enviándole los parámetros actuales de configuración y el equipamiento lógico de arranque.
- Protocolo de gestión: controla las operaciones de gestión entre el gestor y el agente.

La estación de gestión puede acceder a los objetos gestionables de cuatro maneras diferentes:

- En banda (In-band): la gestión del objeto se realiza utilizando la red.
- Fuera de banda (Out-of-band): el sistema de gestión accede a los objetos gestionables a través de otros canales. Esto se puede realizar mediante un terminal conectado directamente a un puerto del objeto gestionable o que el objeto gestionable tenga algún tipo de visualizador o panel de control.
- Remotamente: la gestión se realiza desde otra estación que no es la estación principal de gestión. Existen varias posibilidades:
  - Mediante una estación adicional operadora que permite a varios operadores gestionar todo el sistema o partes de él.

- Utilizando una estación remota conectada a otro segmento de la red que da servicio a estaciones locales.
- Empleando un terminal remoto conectado mediante un modem.
- Un dispositivo de gestión dedicado que puede llamar al operador a través de un servicio de «buscapersonas» o correo electrónico.
- El sistema de gestión puede ser un elemento dentro de un gran sistema supervisado por un gestor de sistemas.

## 2. GESTIÓN DE USUARIOS.

### 2.1. GESTIÓN DE USUARIOS.

En cualquier red local existen diferentes tipos o categorías de usuarios en función de los privilegios que tengan para operar en ella. Las categorías anteriores se pueden resumir en dos: administrador y usuario. Sin embargo, esta simplificación no es del todo correcta porque ambas categorías se pueden subdividir en otras en función de distintos criterios de valoración.

No obstante, antes de profundizar en los tipos de usuarios a considerar vamos a ver los tipos de derechos existentes, añadiendo a los clásicos derechos sobre directorios y archivos los novedosos derechos sobre objetos y propiedades.

Los primeros son los que se conceden a los usuarios para que accedan a los directorios y archivos, de modo que puedan utilizar los programas y datos que almacenan. Los segundos, teniendo en cuenta que todos los usuarios y recursos de la red se representan por objetos, permiten gestionar estos objetos (crearlos, modificarlos, etc.) a aquellos usuarios con derechos sobre los mismos, mientras aquellos usuarios que solo posean derechos de propiedad sobre un objeto únicamente podrán ver y modificar ciertas propiedades del mismo, como puede ser su apellido o teléfono.

Una vez hecha la breve exposición anterior vamos a retomar el objeto de este apartado haciendo referencia a las cuatro categorías que se indican a continuación, aunque volvemos a insistir en que debemos pensar que esta diferenciación es del todo subjetiva y que lo mismo podemos hablar de más niveles como de uno sólo, al fin y al cabo todos son usuarios con más o menos privilegios.

Las categorías que vamos a considerar son:

- Admin.
- Group Manager.
- Usuario común.
- Operador.

El usuario Admin es el máximo responsable de la administración de todos los aspectos que engloba una red local, aspectos tales como la definición, estructura, organización, configuración y mantenimiento de los recursos.

Por tanto, es función suya el decidir quién, cómo y cuándo puede utilizar esos recursos. Lógicamente, para realizar esa función debe tener los máximos derechos que le permite el sistema.

El Group Manager, responsable del grupo, es un semi-Admin de un grupo de usuarios, pudiendo realizar casi todas las funciones del Administrador de la red para con ese grupo, es decir: puede crear nuevos elementos en ese grupo, borrar elementos, cambiar palabras de paso y restricciones de acceso, etc... Sin embargo, no puede modificar los derechos individuales sobre directorios y ficheros, solamente puede hacerlo de manera indirecta ya sea incluyendo o borrando un usuario del grupo y, por tanto, incluirlo o borrarlo de los usuarios que tienen derechos asignados por el Administrador al grupo en cuestión.

El Usuario es el individuo que trabaja con los recursos de la red. En función de sus necesidades y de los recursos existentes se crearan distintos tipos de usuarios, normalmente integrados en Grupos de trabajo, con los derechos y limitaciones necesarias para prestarles un servicio y asegurar el correcto funcionamiento de los servicios prestados por la red.

Por último, al Operador se le puede considerar como a un usuario especial, ya que tiene asignadas responsabilidades desde la manipulación (operación) de determinados recursos. Así, podemos considerar los operadores del sistema de impresión de la red ( impresoras, colas...), operadores de consola del Servidor de Ficheros, etc.

Sin embargo, estas funciones suelen estar asumidas por el propio administrador de la red (Admin) o bien por aquellos usuarios en los que el administrador delega muchas de sus funciones y por tanto de sus derechos y que tienen equivalencia al Admin.

Tras definir los diferentes tipos de usuarios vamos a exponer la gestión de los mismos, gestión que pasa, en primer lugar, por la creación tanto de usuarios como de grupos de trabajo. Sin embargo, antes vamos a dar unas breves notas sobre objetos, base de la nueva programación.

Un objeto es una unidad de información sobre un recurso de la red, comparable a un registro en una base de datos. Los objetos son usados para organizar, encontrar, acceder y manejar recursos de la red, tales como impresoras, sistemas de ficheros, servidores o usuarios.

Un objeto esta compuesto de propiedades y valores. Las propiedades son las categorías de información que se pueden almacenar para un objeto determinado. Un valor es el dato para una propiedad. Así, por ejemplo, un objeto coche tendría diferentes propiedades: color de la carrocería, velocidad máxima, etc., y sus valores serían: rojo, 140, etc. En el caso de la red local un usuario sería un objeto con propiedades tales como el «login name», la «password», apellidos, teléfono, dirección, y otras. Algunas propiedades contienen información que es vital para la red, tales como el nombre del usuario y su palabra de paso, o el nombre de la impresora. Otras propiedades no tienen esa importancia, tales como el cargo del usuario o su dirección de correo.

Los pasos para crear un objeto usuario serían:

- Situar en el contexto (es como la rama de un árbol, o como un directorio) donde se desea colocar el objeto.
- Activar Crear o Añadir y seleccionar el objeto Usuario.



- Indicar un nombre de usuario (login name) y un apellido (last name).
- Crear un directorio local (user home directory). Éste es opcional.

Existe la posibilidad, para facilitar la incorporación de nuevos usuarios, de utilizar plantillas en las que se especifican la asignación por omisión de derechos para cualquier usuario. Los pasos para crear un objeto grupo serían muy similares, añadiendo los usuarios que serían miembros de ese grupo y por tanto con los derechos y limitaciones derivados de su pertenencia al mismo, no entrando en detalles por no alargar excesivamente la exposición. Creados los objetos anteriores, la configuración de los mismos supone la materialización de las propiedades de estos objetos y la asignación de los derechos sobre otros objetos, directorios y ficheros que van a poder manejar.

Cuando mencionamos la palabra configuración estamos hablando implícitamente de gestión de usuarios ya que entre otras posibilidades se encuentran las siguientes:

- Restricciones de conexión: posibilidad de determinar cuándo caduca la cuenta de usuario (p. ej.: empleados temporales en una empresa) y el número de conexiones simultáneas que puede tener (para evitar que los usuarios se conecten desde más de un número determinado de estaciones de trabajo a la vez).
- Restricciones de contraseña: posibilidad de obligar a la utilización de la misma, incluyendo un número mínimo de caracteres, la necesidad de cambiarla cada cierto tiempo, o el número de conexiones permitidas (limit grace logins) una vez caducada la misma.
- Restricción del tiempo de conexión: posibilidad de especificar el momento exacto en que los usuarios pueden conectarse al sistema. Estas restricciones pueden aplicarse tanto a nivel individual como a grupos de usuarios plasmándose en unas gráficas día/hora, donde cada cuadro representaría (dependiendo del sistema) períodos de tiempo determinado, normalmente media hora.
- Restricción de direcciones de red: supone la limitación de las direcciones de las estaciones de trabajo de la red desde las que se puede conectar un usuario. Así un usuario podría estar obligado a conectarse desde su puesto de trabajo y no podría hacerlo desde ningún otro de la red.
- Equivalencia de seguridad: mecanismo que permite especificar equivalencias entre usuarios facilitando la asignación de derechos. La gestión en NT se realizaría con el Administrador de usuarios para dominios (User Manager for Domains), al cual se accedería vía Inicio-Programas-Herramientas Administrativas. Mediante esta herramienta de administración se pueden crear, modificar y administrar usuarios y grupos. Se pueden configurar opciones como miembro de grupo, perfiles, asignación de directorios home, punteros a los scripts de entrada, organización de los accesos, privilegios de las estaciones de trabajo y restricciones RAS (Servicio de acceso remoto) para cada usuario, o crear plantillas para las categorías de usuarios del sistema.

Con la herramienta citada también es posible controlar la directiva del sistema de cuentas, los derechos de los usuarios y la directiva de auditoría. La directiva de cuentas configura los parámetros como las contraseñas de los usuarios y el bloqueo de cuentas después de varios intentos fallidos de entrada. La directiva de sistema de derechos de usuarios configura los derechos para cada grupo o usuario, como acceso a los ordenadores de la red, cambiar la hora del sistema y agregar nuevos controladores de dispositivos, añadir nuevo software e incluso apagar el sistema. La directiva de sistema de auditoría controla los sucesos que se auditarán.

La operativa para crear un usuario pasaría por hacer clic sobre nuevo usuario, en el menú de usuario del Administrador de usuarios para dominios, configurando a continuación las siguientes opciones:

- Nombre de usuario (Username): nombre único. Es obligatorio.
- Nombre completo (Full name): nombre completo para ayudar a determinar a que persona pertenece la cuenta. Es opcional.
- Descripción: permite facilitar el puesto de trabajo, departamento, etc. Opcional. Contraseña (Password): contraseña de acceso a la cuenta. No es obligatoria pero debería serlo.

Existen otras opciones, marcando o desmarcando, de configuración como son: el usuario debe cambiar la contraseña en el próximo acceso, el usuario no puede cambiar la contraseña, la contraseña nunca expira, o la cuenta está deshabilitada. Una vez realizado lo anterior bastará pulsar el botón de Añadir para finalizar la creación del usuario.

Además de las opciones anteriores existen otros botones para definir mejor el perfil del usuario, pudiendo, entre otras posibilidades, limitar el horario de acceso al pulsar el botón de Horas apareciendo un cuadro día/hora en períodos de una hora (anteriormente vimos en NetWare períodos de media hora).

En los equipos Windows 2000, los perfiles de usuario crean y mantienen automáticamente la configuración de escritorio del entorno de trabajo de cada usuario en el equipo local. El perfil de usuario se crea cuando el usuario inicia por primera vez una sesión en el equipo.

Los perfiles de usuario ofrecen varias ventajas a los usuarios:

- Varios usuarios pueden utilizar el mismo equipo y cada uno dispone de su configuración de escritorio cuando inicia la sesión.
- Cuando los usuarios inician una sesión en sus estaciones de trabajo, reciben la configuración de escritorio que tenían al terminar la última sesión.
- La personalización del entorno de escritorio efectuada por un usuario no afecta a la configuración del resto de los usuarios.
- Los perfiles de usuario se pueden almacenar en un servidor para que los usuarios puedan utilizarlos en cualquier equipo de la red que ejecute Windows NT 4.0 o Windows 2000. Se denominan perfiles de usuario móviles.

Como herramienta administrativa, los perfiles de usuario ofrecen estas opciones:

- Puede crear un perfil de usuario predeterminado que sea adecuado a las tareas del usuario.
- Puede configurar un perfil de usuario obligatorio que no guarde las modificaciones del escritorio que haya efectuado el usuario. Los usuarios pueden modificar la configuración del escritorio en el equipo durante la sesión, pero no se guarda ningún cambio cuando la terminan. La configuración del perfil obligatorio se descarga en el equipo local siempre que el usuario inicia la sesión.

- Puede especificar la configuración de usuario predeterminada y que quede incluida en todos los perfiles de usuario individuales.

Los perfiles de usuario definen entornos de escritorio personalizados, en los que se incluye la configuración individual de la pantalla, las conexiones de red y de impresoras, y otras configuraciones especificadas. El usuario o el administrador del sistema pueden definir el entorno de escritorio.

Los tipos de perfiles de usuario incluyen:

- Perfil de usuario local. El perfil de usuario local se crea la primera vez que un usuario inicia una sesión en un equipo y está almacenado en el disco duro local del equipo. Todas las modificaciones efectuadas en un perfil de usuario local son específicas del equipo concreto en el que se hayan realizado.
- Perfil de usuario móvil. Los perfiles de usuario móviles los crea el administrador del sistema y se almacenan en un servidor. Este perfil está disponible siempre que el usuario inicie una sesión en cualquier equipo de la red. Los cambios efectuados en un perfil de usuario móvil se guardan en el servidor.
- Perfil de usuario obligatorio. Los perfiles de usuario obligatorios son perfiles móviles que se utilizan para especificar configuraciones particulares de usuarios o grupos de usuarios. Sólo los administradores del sistema pueden realizar cambios en los perfiles de usuario obligatorios.

## 2.2. GESTIÓN DE DATOS.

En este apartado nos referiremos exclusivamente a la administración del sistema de archivos, esto es, al manejo de directorios y ficheros identificando los mecanismos para encauzar la correcta utilización de los mismos. No será objeto de este punto la gestión del almacenamiento en disco, entendiendo como tal los procedimientos de administración de los discos, particiones, volúmenes, etc., incluyendo todos los mecanismos tendentes a asegurar la integridad de los datos.

El volumen es el nivel más alto de almacenamiento en el sistema de archivos, tanto de Novell NetWare como de Microsoft Windows NT, pudiendo disponer de uno o más volúmenes en función de nuestras necesidades y de las capacidades del Sistema. Así, NetWare tiene su límite en 64 volúmenes. El volumen es una parte del espacio de almacenamiento en disco de un tamaño fijo, aunque se puede aumentar añadiendo nuevo espacio. Es posible, inclusive, contar con un volumen suma de diferentes espacios correspondientes a diferentes discos físicos. Lo que no es posible es reducir el tamaño de un volumen sin perder los datos incluidos en el mismo. Un volumen está organizado, al igual que sucedía en los discos DOS, en un directorio raíz y subdirectorios que se ramifican de éste, siendo obligatorio que el primer volumen se denomine SYS.

Vamos a repasar los derechos sobre directorios y ficheros por ser, con ligeras diferencias, comunes a diferentes tipos de redes, no discriminando si hablamos de un grupo o de un usuario por no alterar su significado. Así podemos hablar de:

- R (R)ead, derecho de apertura para lectura sobre los ficheros de un directorio y/o fichero.
- W (W)rite, derecho de apertura para escritura sobre los ficheros de un directorio y/o fichero.
- C (C)reate, derecho de creación de directorio y/o fichero.

- E (E)rase, derecho de borrado de directorio y/o fichero.
- F (F)ile scan, búsqueda de archivos: permite ver el directorio y sus archivos utilizando las órdenes DIR o NDIR.
- M (M)odify, permite modificar los atributos y nombres del directorio, sus subdirectorios y sus ficheros, pero no cambiar su contenido.
- A (A)ccess, Control, garantiza el poder modificar cualquier derecho, exceptuando el de Supervisor, a cualquier usuario.
- S (S)upervisor, garantiza todos los derechos sobre el directorio, sus archivos y sus subdirectorios. Los usuarios con este derecho pueden conceder a otros usuarios derechos sobre el directorio, sus archivos y sus subdirectorios.

Enumerados los derechos, deberíamos tener en cuenta la existencia de los Atributos, los cuales confieren unas características especiales a los directorios y ficheros, ya que los solapes entre derechos y atributos se resuelven a favor de éstos últimos, de modo que si se posee el derecho de borrado sobre un fichero pero el atributo es «Di» o «Delete inhibit» no se podrá borrar ese fichero. Para el manejo de los volúmenes, directorios y ficheros utilizaríamos las herramientas de administración de NetWare (Nwadmin) o Windows NT (Explorer), así como algunas utilidades específicas como Filer en Novell NetWare.

Concretamente, en Windows NT, el acceso centralizado a los ficheros de la red se efectúa en base a la comparación de carpetas (Shared folders), siendo requisito indispensable que esa carpeta, o directorio, sea compartida antes de que un usuario, o grupo de usuarios, pueda conectarse a dicho recurso.

La herramienta que facilita la compartición de esas carpetas es el Windows NT Explorer. Con esta utilidad basta posicionarse sobre una carpeta y al pulsar el botón derecho del ratón y hacer clic en compartir (Sharing) aparece una ventana de propiedades (Properties). En esta ventana se nos presentan una serie de posibilidades a configurar: nombre asignado al recurso a compartir, comentario, máximo número de usuarios que pueden compartir el recurso y set de permisos sobre el mismo. Por defecto existe un grupo, denominado Everyone, al que se le asigna el derecho de Full Control sobre los nuevos recursos compartidos. Para asignar permisos a usuarios y grupos sobre estos recursos bastará presionar el botón de permisos en la ventana mencionada anteriormente y, tras hacer clic en Añadir de la nueva ventana aparecida a continuación, seleccionar el/los usuarios o grupos a los que queremos asignar los permisos. En la ventana de Tipo de Acceso seleccionaríamos el permiso apropiado para el usuario o grupo. Los permisos son de cuatro tipos:

- Full Control: todos los derechos.
- Cambio (Change): permite crear carpetas, añadir ficheros, cambiar y añadir datos en los ficheros, cambiar atributos de los ficheros, borrar carpetas y ficheros y efectuar todas las tareas permitidas por el permiso de lectura.
- Lectura (Read): muestra los nombres de las carpetas y ficheros, los datos y atributos de los ficheros y permite ejecutar los programas. También se autoriza a moverse entre carpetas de la carpeta compartida, es decir, moverse entre subdirectorios.
- Acceso Denegado (No Access): se establece exclusivamente la conexión pero el acceso es denegado y el contenido no aparece.

Si los discos del servidor han sido formateados NTFS (Windows NT File System) aparecería una pestaña adicional en la ventana de Propiedades mencionada anteriormente: Seguridad (Security). Mediante esta opción se aumenta la seguridad de los datos ya que puede aplicarse a carpetas y a ficheros individuales. Se suele hablar de permisos locales ya que se refieren a la máquina concreta en que se den, mientras que los permisos de carpetas compartidas eran a nivel de toda la red. Con los permisos NTFS podríamos tener unas opciones prácticamente similares a las que veíamos anteriormente en NetWare. Concretamente podemos asignar derechos de:

- (R)ead, lectura.
- (W)rite, escritura
- (X) ejecutable.
- (D)elete, borrado.
- (C)hange, cambio.
- (O)wner, tomar propiedad.

Por último, habría que mencionar que además de las asignaciones de derechos y atributos sobre los directorios (carpetas) y ficheros, podríamos efectuar otras operaciones, como son la limitación de espacio disponible en un directorio, utilizando Filer en NetWare ó la limitación de espacio disponible para un usuario utilizando NwAdmin.

El sistema de archivos distribuido (Dfs, Distributed file system) permite a los administradores de sistemas facilitar a los usuarios el acceso y administrar archivos que se encuentran distribuidos a través de la red. Con Dfs, se puede hacer que parezca que los archivos distribuidos por múltiples servidores residen en un sitio de la red a ojos de los usuarios. Los usuarios ya no tendrán que saber y especificar la ubicación física real de los archivos para tener acceso a éstos.

Debe considerar la posibilidad de implementar Dfs si:

- Los usuarios que tienen acceso a las carpetas compartidas están distribuidos por uno o varios sitios.
- La mayor parte de los usuarios precisan el acceso a varias carpetas compartidas.
- El equilibrio de la carga del servidor puede mejorarse si se vuelven a distribuir las carpetas compartidas.
- Los usuarios precisan de un acceso ininterrumpido a las carpetas compartidas.
- La organización dispone de sitios Web para uso interno o externo.

Además del componente Dfs de servidor de Windows 2000, hay un componente Dfs de cliente. El cliente Dfs almacena en caché una referencia al servidor Dfs para un período específico, definido por el administrador.

Un equipo que ejecute el cliente Dfs debe ser miembro del dominio para la raíz Dfs.

La topología del sistema de archivos distribuido (Dfs) consta de una raíz Dfs, uno o varios vínculos Dfs y una o varias carpetas compartidas Dfs o duplicaciones, a las que señala cada vínculo Dfs.

El servidor de dominio en el que reside la raíz Dfs se conoce como servidor host. Puede duplicar una raíz Dfs mediante la creación de recursos compartidos raíz en otros servidores del dominio. De este modo, el archivo se encontrará disponible cuando el servidor host no lo esté.

Para los usuarios, una topología Dfs proporciona acceso unificado y transparente a los recursos de red que necesitan. Para los administradores del sistema, una topología Dfs es un único espacio de nombres DNS: con el Dfs de dominios, los nombres DNS para los recursos compartidos raíz Dfs resuelven los servidores host para la raíz Dfs.

Como el servidor host para un sistema de archivos distribuido de dominios es un servidor miembro dentro de un dominio, de manera predeterminada la topología Dfs se publica automáticamente en Active Directory, proporcionando de este modo la sincronización de las topologías Dfs por todos los servidores host. De esta forma, se proporciona la tolerancia a errores para la raíz Dfs y se permite la duplicación opcional de las carpetas compartidas Dfs.

Se puede agregar un vínculo Dfs a la raíz Dfs para expandir la topología Dfs. La única restricción en cuanto al número de niveles jerárquicos de una topología Dfs viene impuesta por el límite de Windows 2000 de 260 caracteres para cualquier ruta de acceso de archivo. Un nuevo vínculo Dfs puede referirse a una carpeta compartida que puede contener subcarpetas o a un volumen completo Windows 2000. Si dispone de los permisos adecuados, puede tener acceso además a cualquier subcarpeta local que exista o que se agregue a una carpeta compartida Dfs.

### 3. GESTIÓN DE DISPOSITIVOS.

#### 3.1. IMPRESIÓN.

Independientemente del software de red local que estemos considerando, es usual encontrarnos con tres conceptos fundamentales en el campo de la impresión en la red. Dichos conceptos son:

- Impresoras.
- Servidor de impresión.
- Colas de impresión.
- Las impresoras son los elementos físicos que se van a poner a disposición de todos aquellos usuarios de la red que lo necesiten, permitiendo su utilización conjunta y ordenada, lo cual redundará en una mejora en la utilización de los recursos disponibles. Estas impresoras se pueden conectar directamente a la red (llevan incorporada una tarjeta especial), a un servidor de impresión especial (por ejemplo, el Intel NetportExpress), al servidor de archivos o a cualquier estación de trabajo, DOS u OS/2, de la red. Cada impresora necesita un controlador para atender a las tareas de impresión de la red. Dicho controlador se cargará en el equipo al que se conectan, salvo cuando la conexión es directa, cargándose entonces en la propia impresora.

- El servidor de impresión es el que se encarga de controlar las impresoras y las colas de impresión. De forma similar a un guardia de tráfico, el servidor recoge las tareas de las colas de impresión y las envía a las impresoras que estén asignadas. Este sistema permite distribuir los trabajos entre las impresoras, ordenarlos (asignando prioridades), cancelarlos, repetirlos, etc... Un servidor de impresión es, en NetWare 4.x, un programa que se carga como módulo NLM en el servidor de la red. Actualmente permite el control de hasta 256 impresoras.
- Las colas de impresión son unos lugares de almacenamiento temporal para los trabajos que los usuarios mandan a las impresoras, siendo el servidor de impresión el que distribuye estos trabajos entre las impresoras correspondientes. Esto significa que cuando una estación envía un trabajo de impresión a una impresora de la red, el software de la red almacena provisionalmente esa tarea como un fichero, en un directorio de la red que se denomina cola de impresión, hasta que el servidor de impresión pueda enviarlo a una impresora. Si a una cola se le han asignado varias impresoras, la primera que quede libre tomará el trabajo. Asimismo, se le pueden asignar varias colas de impresión a una misma impresora. Cada una de éstas puede tomar una serie de usuarios o prioridades de impresión asignadas.

En los Servicios de Directorios (NetWare Directory Services) del sistema operativo NetWare 4.x existe el Objeto «cola de impresión» que contiene la siguiente información sobre la cola de impresión:

- Localización del directorio asignado.
- Servidor de impresión e impresoras que sirve la cola.
- Verificación de quién puede usar y operar la cola de impresión.
- Estado de la cola de impresión.

Con NetWare 4.x se pueden emplear utilidades gráficas o de texto para crear o modificar el entorno de impresión. Sin querer ser exhaustivo habría que hacer mención de la utilidad gráfica NwAdmin, que permite realizar todas las operaciones desde el entorno Windows y de la utilidad de texto Pconsole. Existen otras muchas utilidades que solo vamos a citar de pasada, pues no creemos que sea necesario profundizar en ellas: Printcon, Printdef, Nprinter, Netuser, etc.

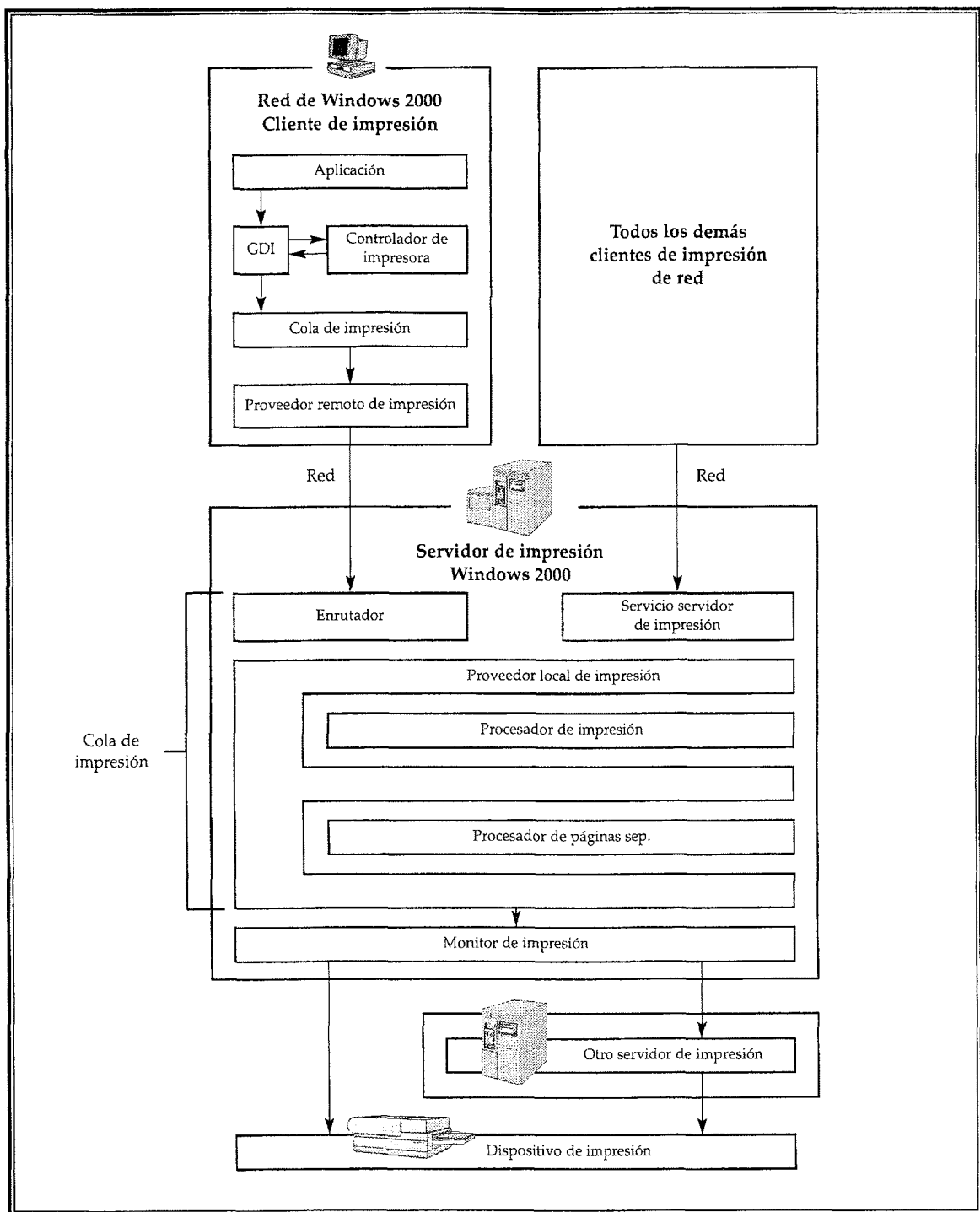
Por último, debemos hacer referencia a un comando de suma importancia para la utilización de los servicios de impresión desde cualquier aplicación no expresamente preparada para el trabajo en red, es decir, desde aquellas que no permiten especificar e imprimir directamente en las impresoras de la red. Al imprimir desde este tipo de aplicaciones es necesario desviar la impresión dirigida a las impresoras locales DOS. Esto se realiza con el comando CAPTURE que permite redirigir los trabajos enviados a los dispositivos LPT1 o LPT2 a una impresora de la red. El comando antes mencionado se puede utilizar con una serie de parámetros donde especificar tanto la impresora o la cola a donde se redirige el trabajo, como si el mismo va a ir precedido de una cabecera identificativa o «banner», a fijar el número de copias, el «Timeout» que permite regular el momento de la impresión, etc.

Si estuviéramos en un sistema Windows NT empezaríamos por crear (añadir) y compartir una impresora vía Inicio-Configuración-Impresoras. Una vez creada, y de un modo similar a como compartíamos carpetas, iríamos a la ventana de Propiedades de la impresora, configurando las distintas opciones en las pestañas que en ella se muestran.

A continuación se incluye información general acerca de las operaciones que se realizan en un documento enviado a una impresora desde un cliente Windows en el que se utiliza Windows 2000 Server como servidor de impresión. Algunos procesos son ligeramente diferentes en los clientes de impresión que no son de Windows.

1. Un usuario en un equipo cliente Windows 2000 decide imprimir un documento.
2. Si el documento se envía desde una aplicación Windows, la aplicación llama a la interfaz de dispositivo gráfico (GDI) que, a su vez, llama al controlador de impresora asociado a la impresora de destino. Con la información de documento procedente de la aplicación, la GDI y el controlador intercambian datos para procesar el trabajo de impresión en el lenguaje de la impresora y, a continuación, lo transfieren a la cola de impresión del equipo de cliente. Si el cliente está utilizando un sistema operativo distinto a Windows o una aplicación que no esté basada en Windows, otro componente reemplazará a la GDI para realizar una tarea similar.
3. El equipo de cliente entrega el trabajo de impresión al servidor de impresión. En los clientes Windows NT 4.0 o Windows 2000, la cola de impresión del cliente realiza una llamada a procedimiento remoto (RPC) a la cola de impresión del servidor, que emplea el enrutador para sondear al proveedor de impresión remota del cliente. El proveedor inicia otra RPC a la cola de impresión del servidor, que recibe el trabajo de impresión a través de la red.
4. En el servidor de impresión, los trabajos de impresión procedentes de clientes Windows NT o Windows 2000 utilizan el tipo de datos de metarchivo mejorado (EMF). La mayor parte de las aplicaciones que no usan Windows utilizan el tipo de datos RAW (preparado para imprimir).
5. El enrutador del servidor transfiere el trabajo de impresión al proveedor de impresión local del servidor (componente de la cola de impresión), que pone en la cola el trabajo (lo escribe en el disco).
6. El proveedor de impresión local sondea al procesador de impresión. El procesador de impresión reconoce el tipo de datos del trabajo y recibe el trabajo de impresión. A continuación, el procesador de impresión convierte el trabajo de impresión según su tipo de datos.
7. Si la impresora de destino se define en el equipo del cliente, el servicio del servidor de impresión decide si la cola de impresión del servidor alterará el trabajo de impresión o le asignará un tipo de datos diferente. El trabajo de impresión se transfiere al proveedor de impresión local, que lo escribe en el disco.
8. El control del trabajo de impresión se pasa al procesador de páginas de separación, que agrega una página de separación, si se especifica, al principio del trabajo.
9. El trabajo sale de la cola de impresión hacia los monitores de impresión. Si se utiliza una impresora bidireccional, un monitor de lenguaje supervisa la comunicación de dos direcciones entre el remitente y la impresora, y, después, transfiere el trabajo de impresión a un monitor de puerto. En caso contrario, el trabajo va directamente al monitor de puerto que, a su vez, lo envía a la impresora de destino (o a otro servidor de impresión de red).
10. La impresora recibe el trabajo de impresión, convierte cada página al formato de mapa de bits y lo imprime.





### 3.2. CONCEPTOS DE BACKUP Y RECUPERACIÓN.

Vamos a estudiar estos conceptos en el entorno Windows 2000. Una copia de seguridad le ayuda a proteger los datos de pérdidas accidentales si su sistema tiene un problema de hardware o de medios de almacenamiento. Por ejemplo, puede utilizar una copia de seguridad para crear un duplicado de los datos del disco duro y, a continuación, archivarlos en otros dispositivos de almacenamiento, como pueden ser un disco duro o una cinta. Si los datos originales de su disco duro se borran o sobrescriben accidentalmente, o el acceso a ellos es imposible debido a un error de funcionamiento del disco duro, podrá restaurar los datos que estén en la copia archivada.

Puede hacer copias de seguridad de la tabla de asignación de archivos (FAT) o de volúmenes del sistema de archivos NTFS. No obstante, si hubiera realizado una copia de seguridad de un volumen NTFS utilizado en Windows 2000, es recomendable que restaure los datos en un volumen NTFS de Windows 2000. De lo contrario, podría perder datos y algunas características de archivos y carpetas, como permisos, configuración del sistema de cifrado de archivos (EFS), información de cuota de disco, información de unidad montada e información sobre el almacenamiento remoto.

Se pueden utilizar cinco métodos de copia de seguridad para los datos del equipo o de la red:

- **Copia de seguridad intermedia.** Una copia de seguridad intermedia incluye todos los archivos pero no los marca individualmente como copiados (es decir, no desactiva el atributo de modificado). Este método es útil cuando se desea hacer copias de seguridad de archivos entre copias de seguridad normales e incrementales, ya que no afecta a estas operaciones.
- **Copia de seguridad diaria.** Una copia de seguridad diaria incluye todos los archivos seleccionados que se hayan modificado el día en que se realizó la copia diaria. Los archivos incluidos en la copia de seguridad no se marcan como tales (en otras palabras, no se borra su atributo de archivo).
- **Copia de seguridad diferencial.** Una copia de seguridad diferencial copia los archivos creados o modificados desde la última copia de seguridad normal o incremental. No pone una marca de copiado a los archivos (es decir, no desactiva el atributo de modificado). Si realiza una combinación de copias de seguridad normales y diferenciales, para restaurar los archivos y carpetas debe disponer de la última copia de seguridad normal y la última copia de seguridad diferencial.
- **Copia de seguridad incremental.** Una copia de seguridad incremental sólo copia los archivos creados o modificados desde la última copia de seguridad normal o incremental. Marca los archivos como copiados (es decir el atributo de modificado está desactivado). Si usa una combinación de copias de seguridad normales e incrementales, la restauración de los datos debe realizarse con la última copia de seguridad normal y todas las copias de seguridad incrementales.
- **Copia de seguridad normal.** Una copia de seguridad normal incluye todos los archivos seleccionados y pone a cada archivo una marca que indica que se ha hecho una copia de seguridad del mismo (es decir, se desactiva el atributo de modificado). En las copias de seguridad normales, sólo necesita la copia más reciente del archivo o la cinta que contiene la copia de seguridad para restaurar todos los archivos. Las copias de seguridad normales se suelen realizar al crear por primera vez un conjunto de copia.

Debe contar con ciertos permisos o derechos de usuario para realizar copias de seguridad de archivos y carpetas. Si es administrador o un operador de copia de seguridad en un grupo local puede realizar la copia de seguridad de cualquier archivo o carpeta almacenada en el equipo local al que se aplique el grupo local. Del mismo modo, si es administrador o un operador de copia de seguridad en un controlador de dominio puede realizar la copia de seguridad de cualquier archivo o carpeta del dominio o en cualquier equipo del dominio con el que tenga una relación de confianza en ambos sentidos (salvo los datos del Estado del sistema). Sin embargo, si no es administrador ni operador de copia de seguridad y desea realizar una copia de seguridad de los archivos, debe ser el propietario de los archivos y carpetas cuya copia de seguridad desee llevar a cabo o tiene que contar con uno o varios de los permisos siguientes para esos archivos y carpetas: Lectura, Lectura y ejecución, Modificación o Control total.

También debe asegurarse de que no existen restricciones de cuota de disco que puedan limitar su acceso a un disco duro, lo que imposibilitaría la realización de una copia de seguridad de los datos. Para comprobar si tiene alguna restricción de cuota del disco, puede hacer clic con el botón secundario del mouse (ratón) en el disco cuyos datos desee guardar, en propiedades y, después, en la ficha Quota.

También puede restringir el acceso a un archivo de copia de seguridad si activa Permitir sólo al propietario y al Administrador el acceso a los datos de copia de seguridad en el cuadro de diálogo Información sobre el trabajo de copia de seguridad. Si selecciona esta opción, sólo un administrador o la persona que creó el archivo de copia de seguridad podrán restaurar los archivos y las carpetas.

- Sólo puede realizar la copia de seguridad de los datos de Estado del sistema en un equipo local. No puede realizar dicha copia de seguridad en un equipo remoto, incluso aunque sea un administrador u operador de copia de seguridad en el equipo remoto.

Con una copia de seguridad puede realizar una copia de seguridad y restaurar los siguientes componentes del sistema:

- Registro.
- Base de datos COM+Class Registration.
- Archivos de inicio, incluidos los archivos del sistema.
- Base de datos de Servicios de Certificate Server.
- Servicio de Directorio de Active Directory.
- Directorio SYSVOL.
- Información del Servicio Cluster.

La copia de seguridad se refiere a estos componentes del sistema como los datos del Estado del sistema. Para los sistemas operativos de Windows 2000 Server, los datos del Estado del sistema incluyen el Registro, la base de datos COM+Class Registration, los archivos de inicio del sistema y la base de datos de Servicios de Certificate Server (si el servidor es un servidor de certificados). Si el servidor es un controlador de dominio, los datos del Estado del sistema incluyen también el directorio SYSVOL y Active Directory. Asimismo, si ejecuta el servicio de nombre de dominios (DNS) en un controlador de dominio, la porción de Active Directory de los datos de Estado del sistema también contiene toda la información de la zona DNS (DS integrado y no integrado).

Si el servidor ejecuta el servicio Cluster, los datos del Estado del sistema también incluirán cualquier punto de comprobación del Registro de recursos y el Registro de recuperación del recurso de quórum, que contiene la información más reciente de la base de datos de clúster.

En una copia de seguridad, los servicios distribuidos, como el servicio de directorios de Active Directory, están contenidos en un conjunto conocido como los datos del Estado del sistema. Cuando realice la copia de seguridad de los datos del Estado del sistema en un controlador de dominio, estará realizando una copia de seguridad de todos los datos de Active Directory que haya en ese servidor (junto con otros componentes del sistema como el Directorio y el Registro). Con el fin de restaurar estos servicios distribuidos en dicho servidor, debe restaurar los datos del Estado del sistema. Sin em-

bargo, si tiene más de un controlador de dominio en la organización y Active Directory está duplicado en alguno de dichos servidores, tendrá que ejecutar lo que se denomina una restauración autoritaria con el fin de asegurar que todos los datos restaurados se dupliquen en todos los servidores.

Durante una operación de restauración normal, la Copia de seguridad funciona en un modo de restauración no autoritario. Es decir, cualquier dato que restaure, incluidos los objetos de Active Directory, tendrán su propio número original de secuencia de actualización. El sistema de duplicación de Active Directory utiliza este número para detectar y propagar los cambios de Active Directory entre los distintos servidores de la organización. Debido a este hecho, cualquier dato que se restaure de forma no autoritaria aparecerá en el sistema de duplicación de Active Directory como si fuera anterior, lo que significa que los datos nunca se duplicarán en el resto de los servidores. Por el contrario, el sistema de duplicación de Active Directory actualizará realmente los datos restaurados con los datos más recientes de sus otros servidores. La restauración autoritaria resuelve este problema.

Windows 2000 tiene varias características que permiten reparar un sistema que no puede iniciar o cargar Windows 2000. Estas características son útiles cuando algunos de los archivos de sistema están dañados o son eliminados accidentalmente, o cuando se ha instalado software o los controladores de dispositivos hacen que el sistema no funcione correctamente.

El modo a prueba de errores le permitirá iniciar el sistema con un número mínimo de controladores de dispositivos y servicios. Por ejemplo, si un nuevo controlador de dispositivo o software recién instalados impiden que el equipo se inicie, podrá iniciar el equipo en modo a prueba de errores para después eliminar el software o controladores de dispositivos del equipo. El modo a prueba de errores no funcionará en todas las circunstancias, especialmente si los archivos de sistema están dañados o no están presentes o si el disco duro está dañado o tiene errores.

La Consola de recuperación proporciona una interfaz de línea de comandos que le permitirá reparar problemas del sistema utilizando un número limitado de comandos desde la línea de comandos. Por ejemplo, se puede utilizar la consola de recuperación para habilitar o deshabilitar servicios, reparar el sector de arranque principal, o copiar archivos de sistema desde un disco o CD-ROM. Esta característica concede un control máximo sobre el proceso de reparación, por lo tanto, deberá ser usada sólo por usuarios avanzados y administradores.

El disco de reparación de emergencia (ERD) le ayudará a reparar problemas relacionados con los archivos de sistema, el entorno de inicio (si tiene un sistema de inicio dual, o de inicio múltiple), y la partición del sector de arranque del volumen. Antes de poder usar la característica del disco de reparación de emergencia para reparar el sistema deberá crear un disco de reparación de emergencia. Esto se puede hacer usando la utilidad de la Copia de seguridad. Si no ha sido creado un disco de reparación de emergencia se puede intentar usar el proceso de disco de reparación de emergencia, sin embargo, cualquier cambio que haya hecho en el sistema, como por ejemplo una actualización del Service Pack, podría perderse, siendo necesaria su reinstalación.

#### **4. MONITORIZACIÓN Y CONTROL DE TRÁFICO.**

La monitorización o evaluación y administración del uso de los recursos de la red, es un punto fundamental para garantizar el óptimo funcionamiento de las redes locales, ya que, en la medida en que seamos capaces de detectar cualquier problema, a ser posible de manera proactiva, esto es, antes de que se produzca un fallo en el sistema, o configurar de manera adecuada los distintos parámetros a nuestro alcance, estaremos asegurando un servicio de calidad, es decir, bastante más que asegurar, simplemente, el funcionamiento de la red.

Existen tres aspectos fundamentales a tener en cuenta al hablar de la palabra monitorización, aspectos que englobaremos en los siguientes apartados:

- Sesiones de usuario.
- Recursos compartidos.
- Recursos en uso.

#### A) Entorno Windows 2000 Server.

En Windows 2000 Server el Monitor de red supervisa el flujo de datos en la red, que incluye toda la información transferida a través de la red en cualquier momento específico. Antes de la transmisión, el software de red divide esta información en elementos más pequeños, denominados tramas o paquetes.

Las tramas, ya sean de difusión o dirigidas, están compuestas por diferentes partes que se pueden analizar por separado. alguna de estas partes contiene datos que el Monitor de red puede utilizar para solucionar problemas de red. Por ejemplo, si se examina la dirección de destino, se puede determinar si la trama era una trama de difusión al indicar que todos los hosts debían recibirla y procesarla, o bien, una trama dirigida enviada a un host específico. Al analizar las tramas, puede determinar la causa exacta de la trama, lo cual ayuda a determinar si se puede optimizar el servicio que genera este tipo de tramas.

Se conoce como capturar al procedimiento por el que el Monitor de red copia tramas. Puede capturar todo el tráfico de red hacia y desde la tarjeta de red local, o bien, configurar un filtro de captura y capturar un subconjunto de tramas. También puede especificar un conjunto de condiciones que activen un suceso en un filtro de captura del Monitor de red. Con el uso de activadores, el Monitor de red puede responder a sucesos en la red. Por ejemplo, puede hacer que Windows inicie un archivo ejecutable cuando el Monitor de red detecte un conjunto de condiciones particulares en la red. Después de capturar datos, puede verlos. El Monitor de red realiza una parte del análisis de los datos pues convierte los datos capturados sin procesar a la estructura lógica de tramas.

El Monitor de red utiliza una característica de especificación de interfaz de controlador de red (NDIS) para copiar todas las tramas que detecta al búfer de captura.

El Monitor de red se compone de una herramienta administrativa llamada Monitor de red y un protocolo de red denominado Controlador del Monitor de red. Estos dos componentes deben estar instalados para que pueda capturar, mostrar y analizar los paquetes de la red (también denominados tramas).

El Monitor de red se utiliza para capturar y mostrar las tramas que un equipo con Windows 2000 Server recibe desde una red de área local (LAN). Los administradores de red pueden utilizar el Monitor de red para detectar y solucionar los problemas de red que puedan ocurrir en el equipo local. El Monitor de red se puede instalar en equipos que ejecutan Windows 2000 Server. Cuando se instala el Monitor de red, el Controlador del Monitor de red se instala automáticamente en el mismo equipo.

El Controlador del Monitor de red permite al Monitor de red recibir tramas desde un adaptador de red y permite a los usuarios de la versión del Monitor de red, proporcionada con Microsoft Sys-

tems Management Server, capturar y mostrar las tramas desde un equipo remoto, incluso los que tienen una conexión de acceso telefónico. Cuando un usuario de un equipo que ejecuta el Monitor de red en Systems Management Server conecta de forma remota con un equipo en el que se ha instalado el Controlador del Monitor de red, y ese usuario inicia una captura, las estadísticas de la captura se transfieren a través de la red hasta el equipo administrador. El Controlador del Monitor de red se puede instalar sólo en equipos que ejecutan Microsoft Windows 2000 Professional o Windows 2000 Server.

Por razones de seguridad, el Monitor de red en Windows 2000 sólo captura las tramas enviadas al equipo local o desde el equipo local, incluyendo las tramas de difusión y de multidifusión. El Monitor de red también muestra estadísticas globales de los segmentos de la red sobre tramas de difusión, tramas de multidifusión, utilización de la red, número total de bytes recibidos por segundo y número total de tramas recibidas por segundo.

Además, para ayudar a proteger la red del uso no autorizado de instalaciones del Monitor de red, el Monitor de red proporciona la capacidad de detectar otras instalaciones del Monitor de red que se estén ejecutando en el segmento local de la red.

Para proteger la red de la supervisión no autorizada, el Monitor de red puede detectar otras instalaciones del Monitor de red en el segmento local de la red. El Monitor de red también detecta todas las instancias del controlador del Monitor de red que se están utilizando de forma remota por un Monitor de red de Systems Management Server o un Monitor del sistema para capturar datos en la red.

Cuando el Monitor de red detecta que se están ejecutando en la red otras instalaciones del Monitor de red, muestra la siguiente información acerca de las mismas:

- Nombre del equipo.
- Nombre del usuario que ha iniciado la sesión en ese equipo.
- Estado del Monitor de red en el equipo remoto (ejecutándose, capturando o transmitiendo).
- Dirección del adaptador del equipo remoto.
- Número de versión del Monitor de red en el equipo remoto.

En algunos casos, la arquitectura de la red puede impedir que una instalación del Monitor de red detecte otra. Por ejemplo, si un enrutador que no reenvía multidifusiones separa otra instalación de la suya, su instalación no podrá detectar la otra.

#### B) Arquitecturas de gestión de red.

En este apartado se describen las dos principales arquitecturas de gestión de red:

- Modelo OSI.
- Modelo Internet (SNMP).

#### a) Modelo OSI.

ISO ha definido una arquitectura de gestión OSI (Open Systems Interconnection) cuya función es permitir supervisar, controlar y mantener una red de datos. Está dividida en cinco categorías de servicios de gestión denominadas Áreas Funcionales Específicas de Gestión (Specific Management Functional Áreas, SMFA). Estas categorías son las siguientes:

##### Gestión de configuración.

La gestión de configuración comprende una serie de facilidades mediante las cuales se realizan las siguientes funciones:

- Iniciación y desactivación.
- Definición o cambio de parámetros de configuración.
- Recogida de información de estado.
- Denominación de los elementos de la red.

##### Gestión de fallos.

Detección, diagnóstico y corrección de los fallos de la red y de las condiciones de error. Incluye:

- Notificación de fallos.
- Sondeo periódico en busca de mensajes de error.
- Establecimiento de alarmas.

##### Gestión de prestaciones.

Se define como la evaluación del comportamiento de los elementos de la red. Para poder efectuar este análisis es preciso mantener un histórico con datos estadísticos y de configuración.

##### Gestión de contabilidad.

Determinación de los costes asociados a la utilización de los recursos y la asignación de sus correspondientes cargas.

##### Gestión de seguridad.

Comprende el conjunto de facilidades mediante las cuales el administrador de la red modifica la funcionalidad que proporciona seguridad frente a intentos de acceso no autorizados. Incluye aspectos como la gestión de claves, cortafuegos e históricos de seguridad.

La arquitectura de gestión OSI define un objeto gestionable como la interfaz conceptual que han de presentar los dispositivos que ofrecen funciones de gestión. El proceso de supervisión y control de un objeto gestionable se realiza mediante una serie de interacciones. Estas interacciones son de dos tipos:

- De operación: el gestor solicita algún dato al objeto gestionable o desea realizar alguna acción sobre él.
- De notificación: cuando el objeto gestionable intenta enviar algún dato al gestor como consecuencia de algún evento ocurrido en el dispositivo.

Un objeto gestionable se caracteriza además por un conjunto de atributos que son las propiedades o características del objeto, y un comportamiento en respuesta a las operaciones solicitadas.

La comunicación entre el gestor y el objeto gestionable no es directa, se realiza mediante un intermediario: el agente de gestión (esto se corresponde con un modelo centralizado gestor-agente). La función del agente es controlar el flujo de información de gestión entre el gestor y el objeto. Este control lo realiza comprobando una serie de reglas de gestión (por ejemplo, que el gestor tenga la capacidad para solicitar una determinada operación), que han de cumplirse para poder realizar la operación. Estas reglas se incluyen en los datos como parte de la solicitud de una operación.

El flujo normal de información de gestión y control entre el gestor y el agente se realiza mediante el protocolo CMIP, perteneciente al nivel de aplicación OSI.

El protocolo permite que un sistema se pueda configurar para que opere como gestor o como agente. La mayoría de las realizaciones prácticas de sistemas gestionados se configuran con unos pocos sistemas operando en modo gestor, controlando las actividades de un gran número de sistemas operando en modo agente.

Cuando dos procesos se asocian para realizar una gestión de sistemas, deben establecer en qué modo va a operar cada uno de ellos (en modo agente o en modo gestor). Los procesos indican, mediante las denominadas unidades funcionales, qué funcionalidades de gestión y estándares utilizarán durante la asociación.

Otros componentes de la arquitectura de gestión OSI son:

- Estructura de la Información de Gestión (Structure of Management Information, SMI). Define la estructura lógica de la información de gestión OS. Establece las reglas para nombrar a los objetos gestionables y a sus atributos. Define un conjunto de subclases y tipos de atributos que son, en principio, aplicables a todos los tipos de clases de objetos gestionables.
- Base de Información de Gestión (Management Information Base, MIB). Representa la información que se está utilizando, modificando o transfiriendo en la arquitectura de los protocolos de gestión OSI. La MIB conoce todos los objetos gestionables y sus atributos. No es necesario que este centralizada físicamente en un lugar concreto, puede estar distribuida a través del sistema y en cada uno de sus niveles.
- CMIS (Common Management Information Services) es un conjunto de reglas que identifican las funciones de una interfaz OSI entre aplicaciones, utilizado por cada aplicación para intercambiar información y parámetros. CMIS define la estructura de la información que es necesaria para describir el entorno. Prácticamente todas las actividades de la gestión de red OSI están basadas en diez primitivas de servicio CMIS que son utilizadas por las SMFA.



## b) Modelo Internet (SNMP).

En 1988, el IAB (Internet Activities Board, Comité de Actividades Inter-red) determinó la estrategia de gestión para TCP/IP (Transfer Control Protocol/Internet Protocol, Protocolo de Control de Transmisión/Protocolo de Inter-Red). Esto significó el nacimiento de dos esfuerzos paralelos: la solución a corto plazo, SNMP, y la solución eventual a largo plazo, CMOT (CMIP Over TCP/IP, CMIP sobre TCP/IP).

CMOT pretendía implantar los estándares del modelo de gestión OSI en el entorno Internet (TCP/IP). CMOT tuvo que afrontar los problemas derivados de la demora en la aparición de especificaciones y la ausencia de implementaciones prácticas. Como consecuencia de ello, la iniciativa CMOT fue paralizada en 1992.

SNMP es una extensión del protocolo de gestión de red para gateways SGMP (Simple Gateway Monitoring Protocol, Protocolo Sencillo de Supervisión de Pasarelas), que se convirtió en 1989 en el estándar recomendado por Internet. Está dirigido a proporcionar una gestión de red centralizada que permita la observación, el control y la gestión de las instalaciones. Utilizando SNMP, un administrador de red puede direccionar preguntas y comandos a los dispositivos de la red.

SNMP se ha convertido, debido al enorme éxito que ha tenido desde su publicación, en el estándar de facto de gestión de redes. Prácticamente todo el equipamiento de redes puede ser gestionado vía SNMP.

Algunas de las funciones que proporciona SNMP son:

- Supervisión del rendimiento de la red y su estado.
- Control de los parámetros de operación.
- Obtención de informes de fallos.
- Análisis de fallos.

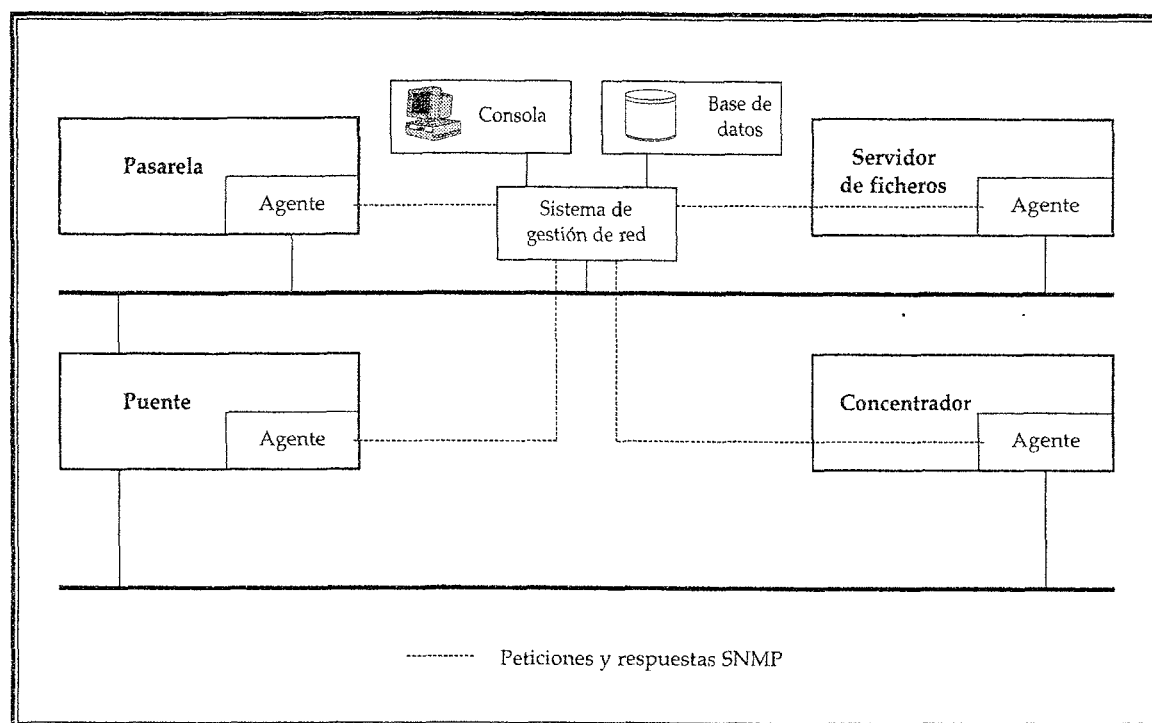
## SNMP.

El protocolo SNMP incorpora varios elementos presentes en otros estándares, como el modelo gestor-agente, la existencia de una base de datos de información de gestión (MIB) o el uso de primitivas de tipo PUT y GET para manipular dicha información. A continuación se describen dichos elementos:

- Agente: equipamiento lógico alojado en un dispositivo gestionable de la red. Almacena datos de gestión y responde a las peticiones sobre dichos datos.
- Gestor: equipamiento lógico alojado en la estación de gestión de red. Tiene la capacidad de preguntar a los agentes utilizando diferentes comandos SNMP.
- MIB (Management Information Base, Base de Información de Gestión): base de datos virtual de los objetos gestionables, accesible por un agente, que puede ser manipulada vía SNMP para realizar la gestión de red.

El protocolo SNMP realiza las funciones descritas anteriormente llevando información de gestión entre los gestores y los agentes.

En la figura siguiente se presenta un ejemplo de sistema de gestión SNMP.



El protocolo SNMP es sólo un aspecto dentro de toda la estructura de gestión, la cual está compuesta de los siguientes elementos:

- Estación de Gestión de Red (Network Management Station, NMS).

Es el elemento central que proporciona al administrador una visión del estado de la red y unas funciones de modificación de este estado (puede ser una estación de trabajo o un ordenador personal).

- Estructura de la Información de Gestión (SMI, Structure of Management Information).

Es un conjunto de reglas que define las características de los objetos de la red y cómo obtienen los protocolos de gestión información de ellos. Aunque ha sido diseñado después del SMI de OSI, no es compatible con éste.

- Base de Información de Gestión (MIB).

Es una colección de objetos, que representan de forma abstracta los dispositivos de la red y sus componentes internos. La MIB es conforme a la SMI para TCP/IP. Cada agente SNMP contiene instrumentación que, como mínimo, debe ser capaz de reunir objetos MIB estándar. Estos objetos incluyen direcciones de red, tipos de interfaz, contadores y datos similares.

El estándar MIB de Internet define 126 objetos relacionados con los protocolos TCP/IP. Los fabricantes que deseen pueden desarrollar extensiones del estándar MIB. Estas MIB privadas incorpo-

ran un amplio rango de objetos gestionables, y algunas veces contienen objetos que son funcionalmente similares a los MIB ya definidos. En otros casos el cambio de una variable en un objeto inicia una batería de funciones en el dispositivo gestionado (como por ejemplo un autodiagnóstico).

La carga de la gestión de todas las MIB y de las extensiones privadas recae en el sistema de gestión. Las MIB están escritas en una variante simple del lenguaje de definición OSI ASN.1.

En 1990 se introdujo una nueva versión de MIB, MIB II, donde la mayor aportación es la utilización de 185 nuevos objetos de extensiones privadas.

Aparte de la MIB, existe la Base de Datos de Estadísticas de Red (Network Statistics Database, NSD) que está en la estación de trabajo de gestión. En esta base de datos se recoge información de los agentes para realizar funciones de correlación y planificación.

Las limitaciones de SNMP se deben a no haber sido diseñado para realizar funciones de gestión de alto nivel. Sus capacidades lo restringen a la supervisión de redes y a la detección de errores. Como todos los elementos TCP/IP, ha sido creado pensando más en su funcionalidad y dejando a un lado la seguridad.

### SNMPv2 y v3.

En 1996 se publicó un nuevo estándar, el protocolo SNMPv2, resultado de una serie de propuestas para mejorar las características de SNMP. Los cambios se traducen fundamentalmente en una mejora de las prestaciones, un aumento de la seguridad y en la introducción de una jerarquía de gestión.

- Prestaciones.

SNMPv2 mejora el mecanismo de transferencia de información hacia los gestores, de forma que se necesitan realizar menos peticiones para obtener paquetes de información grandes.

- Seguridad.

A diferencia de SNMP, que no incorpora ningún mecanismo de seguridad, SNMPv2 define métodos para controlar las operaciones que están permitidas.

Desafortunadamente surgieron dos planteamientos diferentes en cuanto al modelo de seguridad, que han dado lugar a dos especificaciones conocidas como SNMPv2\* y SNMPv2u.

Se están realizando esfuerzos para unificar ambos enfoques en un único estándar: SNMPv3.

- Gestión jerárquica.

Cuando el número de agentes a gestionar es elevado, la gestión mediante el protocolo SNMP se vuelve ineficaz, debido a que el gestor debe sondear periódicamente todos los agentes que gestiona.

SNMPv2 soluciona este inconveniente introduciendo los gestores de nivel intermedio. Son estos últimos los que se encargan de sondear a los agentes bajo su control. Los gestores intermedios son configurados desde un gestor principal de forma que solo se realiza un sondeo de aquellas variables demandadas por este último, y sólo son notificados los eventos programados.

SNMPv2 también introduce un vocabulario más extenso, permite comandos de agente a agente y técnicas de recuperación de mensajes.

## RMON.

La especificación RMON (Remote MONitor, monitorización remota) es una base de información de gestión (MIB) desarrollada por el organismo IETF (Internet Engineering Task Force) para proporcionar capacidades de monitorización y análisis de protocolos en redes de área local (segmentos de red). Esta información proporciona a los gestores una mayor capacidad para poder planificar y ejecutar una política preventiva de mantenimiento de la red.

Las implementaciones de RMON consisten en soluciones cliente/servidor. El cliente es la aplicación que se ejecuta en la estación de trabajo de gestión, presentando la información de gestión al usuario. El servidor es el agente que se encarga de analizar el tráfico de red y generar la información estadística. La comunicación entre aplicación y agente se realiza mediante el protocolo SNMP.

RMON es una herramienta muy útil para el gestor de red pues le permite conocer el estado de un segmento de red sin necesidad de desplazarse físicamente hasta el mismo y realizar medidas con analizadores de redes y protocolos.

Las iniciativas se dirigen en estos momentos hacia la obtención de una mayor y más precisa información. En concreto, se trabaja en la línea de analizar los protocolos de nivel superior, monitorizando aplicaciones concretas y comunicaciones extremo a extremo (niveles de red y superiores). Estas facilidades se incorporarán en versiones sucesivas de la especificación (RMON II).

## Comparación SNMP/CMIP.

A continuación se hace una comparación entre los protocolos SNMP y CMIP:

- SNMP está basado en técnicas de sondeo, mientras que CMIP utiliza una técnica basada en eventos. Esto permite a CMIP ser más eficiente que SNMP en el control de grandes redes.
- CMIP es un protocolo orientado a conexión, mientras que SNMP es un protocolo sin conexión. Esto significa que la carga de proceso de SNMP es reducida, pero cuando se envía un mensaje nunca se puede asegurar que el mensaje llega a su destino. La seguridad de los datos no es prioritaria para SNMP.
- CMIP permite la implementación de comandos condicionales sofisticados, mientras que SNMP necesita el nombre de cada objeto.
- CMIP permite, mediante una única petición, la recogida de gran cantidad de datos de los objetos gestionables, enviando información de retorno en múltiples respuestas. Esto no está permitido en SNMP.
- CMIP está especialmente preparado para gestionar grandes redes distribuidas, mientras que SNMP está recomendado para la gestión inter-red.
- CMIP realiza una distinción clara entre los objetos y sus atributos. SNMP no permite esto, lo cual hace imposible la reutilización de atributos y definiciones.

