

# **Ciclo Formativo de Grado Superior de Administración de Sistemas Informáticos en Red**



**Módulo Profesional: SAD  
Unidad de Trabajo 3.- Seguridad pasiva**

*Departamento de Informática y Comunicación  
IES San Juan Bosco (Lorca-Murcia)  
Profesor: Juan Antonio López Quesada*





# Índice de Contenidos

Principios de la Seguridad Pasiva

Alojamiento de la Información

Copias de Seguridad

Recuperación de Datos

Medidas de Actuación

Prácticas/Actividades



# Objetivos de la Unidad de Trabajo:

Profundizar en aspectos de seguridad pasiva, como son las copias de seguridad y medidas específicas de seguridad física y ambientas

Valorar las importancia de realizar periódicamente copias de seguridad de la información sensible de nuestros sistemas.

Analizar los distintos aspectos que influyen en la ubicación física de los sistemas.

Valorar la importancia de los centros de procesamiento de datos CPD y analizar qué medidas específicas requieren.

Analizar los distintos dispositivos hw que permiten mejorar la seguridad física, como SAI, sistemas de refrigeración, armarios de seguridad, circuitos de seguridad, circuitos cerrados de tv, etc

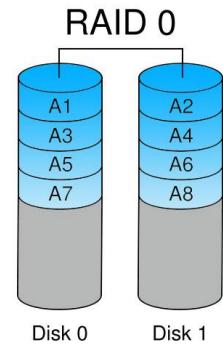
Investigar sobre nuevos métodos de seguridad física y de control de acceso a los sistemas mediante biometría

# Abstract/Resumen:

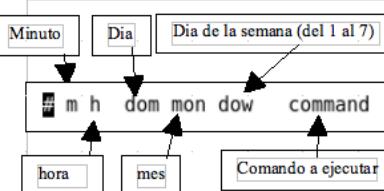
La actividad de seguridad en un sistema comprende un nivel lógico/físico y activo/pasivo. El nivel de seguridad activo de un sistema consiste en la protección ante posibles intentos de comprometer los componentes que lo integran. Un firewall es un ejemplo de seguridad activa, filtra el acceso a ciertos servicios en determinadas conexiones para bloquear el intento de ataque desde alguno de ellos.

El nivel de **seguridad pasiva** se refiere al conjunto de medidas implementadas en los sistemas para minimizar los efectos causados por un accidente. Son tales como el uso de un hardware adecuado, realización de copias de seguridad ..etc.

*En este tema se pretende describir los métodos, herramientas y técnicas de recuperación más ampliamente utilizadas, dando énfasis a un proceso de enseñanza-aprendizaje básicamente práctico.*



root@usuario-desktop:~# crontab -e



```
# m h dom mon dow      command
33 10 21 4 * tar -jcf /tmp/coptot.tar.bz /home/usuario/Escritorio
```

# Principios de la Seguridad Pasiva

La seguridad pasiva intenta minimizar el impacto y efectos causados por accidentes, es decir, se considera medidas o acciones posteriores a un ataque o incidente.

Las consecuencias o efectos producidos por las distintas amenazas (suministro eléctrico, robos o sabotaje, condiciones atmosféricas y naturales) son:

- Perdida y/o mal funcionamiento del Hw.*
- Falta de disponibilidad de servicios.*
- Pérdida de información.*

Como he mencionado en la unidad de trabajo anterior la pérdida de información o la no disponibilidad de la misma, es un aspecto fundamental en torno la que gira gran parte de la seguridad informática, en el que se circumscribe actuaciones centradas en **técnica de copias de seguridad, imágenes del sistema de información, alojamiento de los datos sensibles y los medios que minimicen las amenazas mencionadas.**

# Alojamiento de la Información

## Introducción.-

Uno de los factores clave de la seguridad de cualquier sistema **es cómo y donde** se almacena la información.

En este punto hablaremos de los tres aspectos más importantes que debemos tener en cuenta cuando tratemos la seguridad física de la información: el **rendimiento, la disponibilidad y la accesibilidad** a la misma.

Existen numerosas técnicas que proporcionan estas características, como son los **sistemas RAID, los Clusters de servidores, arquitecturas SAN y NAS ..etc**



Racks de computadoras de un CPD

*Pero, ¿qué entendemos por rendimiento, disponibilidad o accesibilidad a la información?*

# Alojamiento de la Información

## Introducción.-

- *Pues bien, siempre que hablamos de **rendimiento** nos estaremos refiriendo a la capacidad de cálculo de información de un ordenador.* El objetivo es obtener un rendimiento mayor, y esto se puede conseguir no solo con grandes y modernos ordenadores, sino también utilizando arquitecturas que aprovechen las potencialidades de las distintas tecnologías existentes en el Centro de Cálculo.
- *El concepto de **disponibilidad** hará referencia a la capacidad de los sistemas de estar siempre en funcionamiento.* Un sistema de alta disponibilidad está compuesto por sistemas redundantes o que trabajan en paralelo, de modo que cuando se produzca un fallo en el sistema principal, se arranquen los sistemas secundarios automáticamente y el equipo no deje de funcionar en ningún momento.
- *Otro factor importante es la **accesibilidad** a la información;* si nuestra información se encuentra duplicada y en lugar seguro, pero la accesibilidad a ella es mala, en caso de desastre el tiempo que se empleará en poner en marcha el plan de recuperación será mayor que con un sistema considerado como accesible.

# Alojamiento de la Información

## Almacenamiento redundante y distribuido.-

**RAID Redundant Array of Independent Disks**, «conjunto redundante de discos independientes» consiste en un conjunto de técnicas hardware o software que utilizando varios discos proporcionan principalmente *tolerancia a fallos, mayor capacidad y mayor fiabilidad en el almacenamiento*. Se trata de un sistema de almacenamiento que utilizando varios discos y distribuyendo o replicando la información entre ellos consigue algunas de las siguientes características:

**Mayor capacidad:** es una forma económica de conseguir capacidades grandes de almacenamiento. Combinando varios discos más o menos económicos podemos conseguir una unidad de almacenamiento de una capacidad mucho mayor que la de los discos por separado.

**Mayor tolerancia a fallos:** en caso de producirse un error, con RAID el sistema será capaz en algunos casos de recuperar la información perdida y podrá seguir funcionando correctamente.

**Mayor seguridad:** debido a que el sistema es más tolerante con los fallos y mantiene cierta información duplicada, aumentaremos la disponibilidad y tendremos más garantías de la integridad de los datos.

**Mayor velocidad:** al tener en algunos casos cierta información repetida y distribuida, se podrán realizar varias operaciones simultáneamente, lo que provocará mayor velocidad.

# Alojamiento de la Información

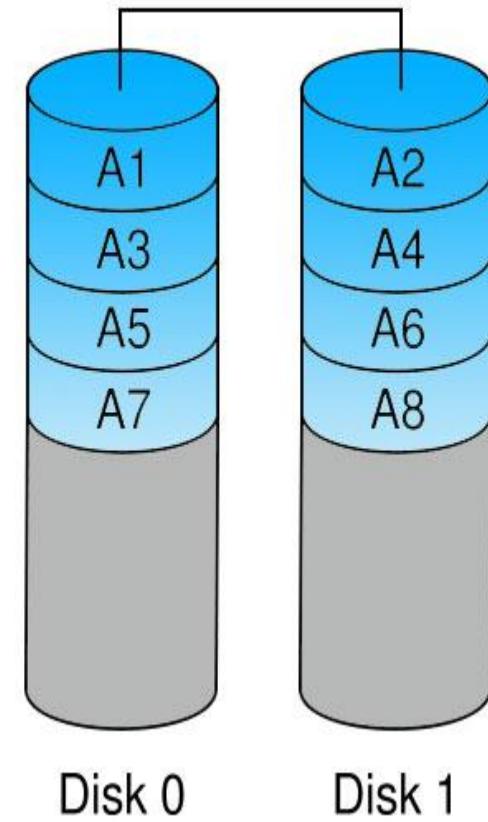
## Almacenamiento redundante y distribuido.-



Este conjunto de técnicas están organizadas en niveles. *Algunos de estos niveles son:*

**RAID nivel 0 (RAID 0):** en este nivel los datos se distribuyen equitativamente y de forma transparente para los usuarios entre dos o más discos. Como podemos ver en la siguiente figura, los bloques de la unidad A se almacenan de forma alternativa entre los discos 0 y 1 de forma que los bloques impares de la unidad se almacenan en el disco 0 y los bloques pares en el disco 1.

- ❑ Esta técnica favorece la velocidad debido a que cuando se lee o escribe un dato, si el dato está almacenado en dos discos diferentes, se podrá realizar la operación simultáneamente. Para ello ambos discos tienen que estar gestionados por controladoras independientes.
- ❑ Hay que tener en cuenta que RAID 0 no incluye ninguna información redundante, por lo que en caso de producirse un fallo en cualquiera de los discos que componen la unidad provocaría la pérdida de información en dicha unidad.

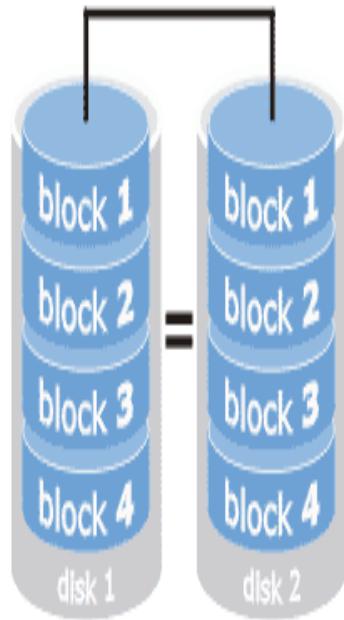


# Alojamiento de la Información

## Almacenamiento redundante y distribuido.-



**RAID 1**  
mirroring



**RAID nivel 1 (RAID 1):** a menudo se conoce también como espejo. Consiste en mantener una copia idéntica de la información de un disco en otro u otros discos, de forma que el usuario ve únicamente una unidad, pero físicamente esta unidad está siendo almacenada de forma idéntica en dos o más discos de forma simultánea.

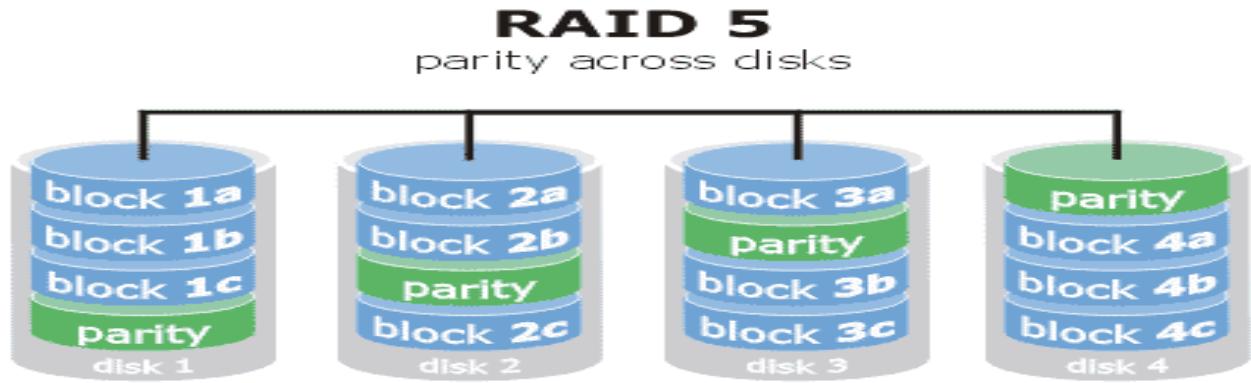
- Si se produjera un fallo en un disco la unidad podría seguir funcionando sobre un solo disco mientras sustituimos el disco dañado por otro y rehacemos el espejo.
- Adicionalmente, dado que todos los datos están en dos o más discos, con hardware habitualmente independiente, el rendimiento de lectura se incrementa aproximadamente como múltiplo lineal del número de copias; es decir, un RAID 1 puede estar leyendo simultáneamente dos datos diferentes en dos discos diferentes, por lo que su rendimiento se duplica. Para maximizar los beneficios sobre el rendimiento del RAID 1 se recomienda el uso de controladoras de disco independientes, una para cada disco (práctica que algunos denominan *splitting* o *duplexing*).

# Alojamiento de la Información

## Almacenamiento redundante y distribuido.-



**RAID nivel 5 (RAID 5):** Los bloques de datos se almacenan en la unidad, y la información redundante de dichos bloques se distribuye cíclicamente entre todos los discos que forman el volumen RAID 5.

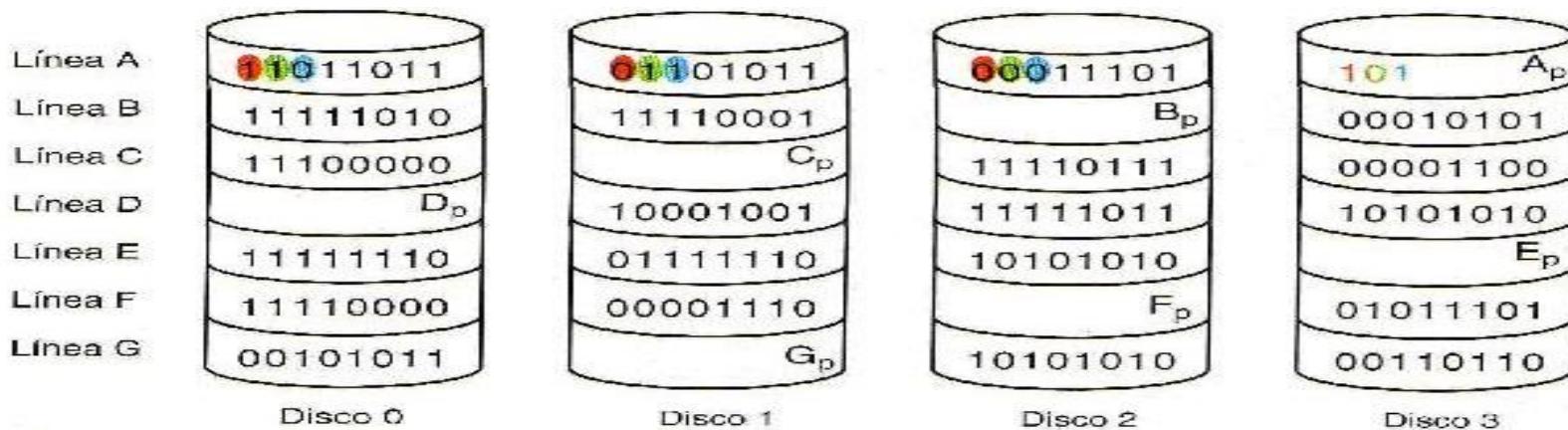


- Por ejemplo si aplicamos RAID 5 sobre un conjunto de 4 discos, como vemos en la siguiente figura, los bloques de datos se colocan en tres de los cuatro bloques, dejando un hueco libre en cada línea que irá rotando de forma cíclica (una línea está formada por un bloque con el mismo número de orden de cada disco y está representado en la figura con el mismo color). En este hueco se colocará un bloque de paridad. Con este sistema, el bloque de paridad se coloca cada vez en un disco.

# Alojamiento de la Información

## Almacenamiento redundante y distribuido.-

- El bloque de paridad se calcula a partir de los bloques de datos de la misma línea, de forma que el primero será un 1, si hay un número impar de unos en el primer bit de los bloques de datos de la misma línea, y 0 si hay un número par de unos.
- Por ejemplo, en la siguiente figura en el bloque de paridad Ap el primer bit (el más significativo) será un 1 porque hay un número impar de unos en el primer bit de cada bloque de datos de esa línea (es decir, los bit marcados en rojo). El espacio total disponible para un volumen RAID 5 que utiliza N discos es la suma del espacio de los N discos menos el espacio de uno.



# Alojamiento de la Información

## Clusters de servidores.-

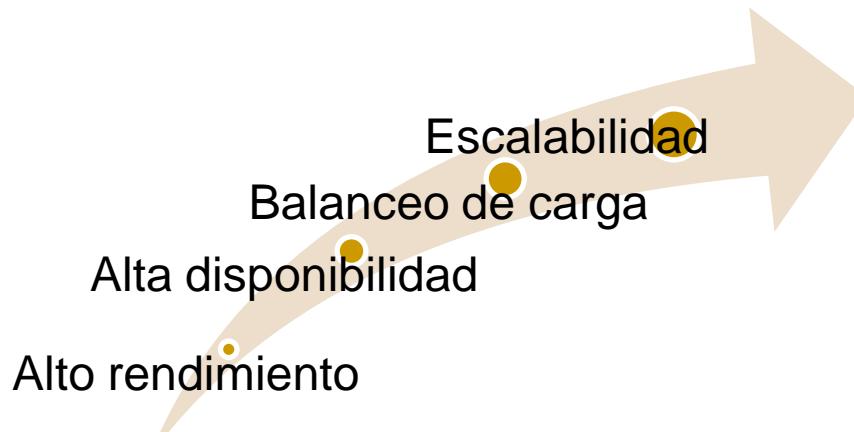
- *El término cluster (a veces españolizado como clúster) se aplica a los conjuntos o conglomerados de computadoras/equipos formados mediante la utilización de hardware comunes y que se comportan como si fuesen una única entidad.*
- Hoy en día desempeñan un papel importante en la solución de problemas de las ciencias, las ingenierías y del comercio moderno.
- La tecnología de clústeres ha evolucionado en apoyo de actividades que van desde aplicaciones de supercómputo y software de misiones críticas, servidores web y comercio electrónico, hasta bases de datos de alto rendimiento, entre otros usos.
- El cómputo con clústeres surge como resultado de la convergencia de varias tendencias actuales que incluyen la *disponibilidad de microprocesadores económicos de alto rendimiento y redes de alta velocidad, el desarrollo de herramientas de software para cómputo distribuido de alto rendimiento, así como la creciente necesidad de potencia computacional.*

# Alojamiento de la Información

## Clusters de servidores.-

*Simplemente, un clúster es un grupo de múltiples ordenadores unidos mediante una red de alta velocidad, de tal forma que el conjunto es visto como un único ordenador, más potente que los comunes de escritorio.*

- Los clústeres son usualmente empleados para mejorar el rendimiento y/o la disponibilidad por encima de la que es provista por un solo equipo, siendo más económico que dispositivos individuales de rapidez y disponibilidad comparables.
- De un clúster se espera los siguientes servicios:



# Alojamiento de la Información

## Clusters de servidores.- Clasificación

Como en tantas otras tecnologías, podemos realizar la clasificación de los clusters en función de varios conceptos, pero todos ellos relacionados con los servicios que se han mencionado.

Atendiendo a estas características hablamos de tres tipos de clusters:

**Clusters de alto rendimiento (HC o High Performance Clusters).** Este tipo de sistemas ejecutan tareas que requieren de una gran capacidad de cálculo o del uso de grandes cantidades de memoria

**Clusters de alta disponibilidad (HA o High Availability).** Con estos clusters se busca dotar de disponibilidad y confiabilidad a los servicios que ofrecen. Para ello se utiliza hardware duplicado.

**Clusters de alta eficiencia (HT o High Throughput).** En estos sistemas el objetivo central de diseño es que se puedan ejecutar el mayor número de tareas en el menor tiempo posible.

# Alojamiento de la Información

## Clusters de servidores.- Clasificación

Otro tipo de clasificación de los clusters de servidores viene dada por *su ámbito de uso*, donde hablaremos de dos tipos:

**Clusters de infraestructuras comerciales**, que conjugan la alta disponibilidad con la alta eficiencia.

**Clusters científicos**, que en general son sistemas de alto rendimiento.



# Alojamiento de la Información

## Clusters de servidores.- Componentes

Para que un cluster funcione necesita de una serie de componentes, que, como ya sabemos, pueden tener diversos orígenes; es decir, no tienen por qué ser de la misma marca, modelo o características físicas. Entre estos componentes están:

**Nodos:** es el nombre genérico que se dará a cualquier máquina que utilicemos para montar un cluster, como pueden ser ordenadores de sobremesa o servidores.



# Alojamiento de la Información

## Clusters de servidores.- Componentes

**Sistema operativo:** podemos utilizar cualquier sistema operativo que tenga dos características básicas: debe ser multiproceso y multiusuario.

**Conexión de Red:** es necesario que los distintos nodos de nuestra red estén conectados entre sí. Para ello podemos utilizar una conexión Ethernet u otros sistemas de alta velocidad .

**Middleware:** es el nombre que recibe el software que se encuentra entre el sistema operativo y las aplicaciones. Su objetivo es que el usuario del cluster tenga la sensación de estar frente a un único superordenador ya que provee de una interfaz única de acceso al sistema. Mediante este software se consigue *optimizar el uso del sistema y realizar operaciones de balanceo de carga, tolerancia de fallos, etc.* Se ocupa, además, de detectar nuevos nodos que vayamos añadiendo al clúster, dotándolo de una gran posibilidad de escalabilidad.

**Sistema de almacenamiento:** cuando trabajamos con clusters podemos hacer uso de un sistema de almacenamiento interno en los equipos, utilizando los discos duros de manera similar a como lo hacemos en un PC, o bien recurrir a **sistemas de almacenamiento más complejos**, que proporcionarán una mayor eficiencia y disponibilidad de los datos, como son los dispositivos **NAS** (*Network Attaches Storage*) o las redes **SAN** (*Storage Area Network*).

# Alojamiento de la Información

## Clusters de servidores.- *Ejemplo*



*Cluster Ubuntu 1*



*Cluster Ubuntu 2*



*Cluster Ubuntu 3*



*Cluster Ubuntu 4*



*Cluster Ubuntu 5*



# Alojamiento de la Información

## Almacenamiento Externo.-

En el apartado anterior hemos visto que con los clusters podemos procesar mucha más información que un ordenador independiente,

*pero ¿dónde guardamos esta información?*

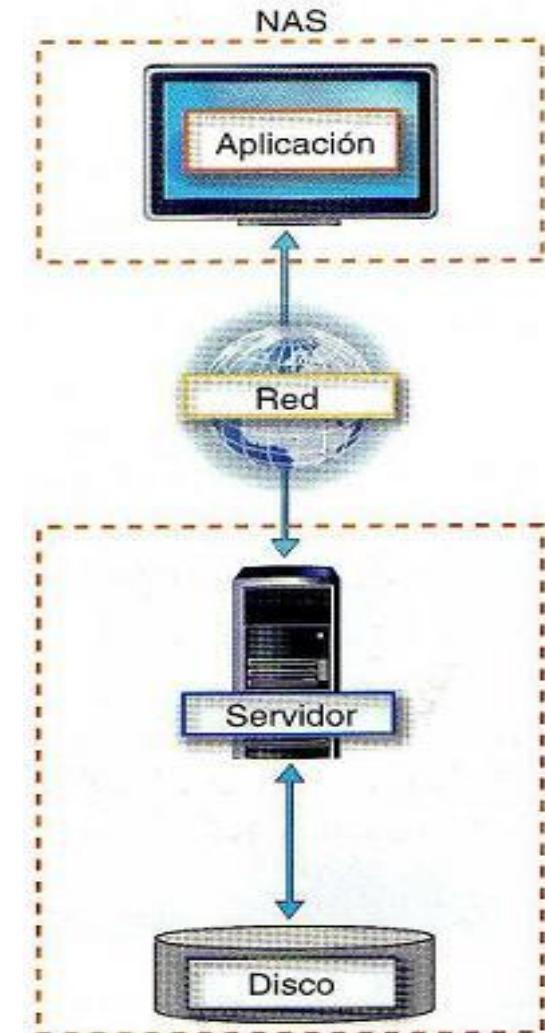
- Una posibilidad es utilizar los sistemas de almacenamiento de los nodos, sus discos duros, por ejemplo. Pero existen otras alternativas que nos permitirán un control y una gestión mucho mayores sobre los datos procesados, como las **tecnologías NAS y SAN**.
- El uso de cualquiera de estas tecnologías es independiente de la existencia de un cluster, aunque resulta idóneo como método de almacenamiento cuando se dispone de uno, especialmente si las complementamos con utilidades para la realización de **copias de seguridad**.

# Alojamiento de la Información

## Almacenamiento Externo.- NAS (almacenamiento conectado a red)

Los dispositivos **NAS** (*Network Attached Storage*) son dispositivos de almacenamiento específicos, a los cuales se accede utilizando **protocolos de red**, como NFS (*Sistema de archivos de red*), FTP (*Protocolo de Transferencia de Archivos*), CIFS (*Common Internet File System nombre que adoptó Microsoft en 1998 para el protocolo SMB*). o SMB (*Server Message Block*), como puedes ver en la siguiente figura.

- ❑ El uso de NAS permite, con bajo coste, realizar balanceo de carga y tolerancia a fallos, por lo que es cada vez más utilizado en servidores Web para proveer servicios de almacenamiento, especialmente contenidos multimedia.
- ❑ Hay otro factor que debemos tener en cuenta, y es que los sistemas NAS suelen estar compuestos por uno o más dispositivos que se disponen en RAID, como hemos visto anteriormente, lo que permite aumentar su capacidad, eficiencia y tolerancia ante fallos.

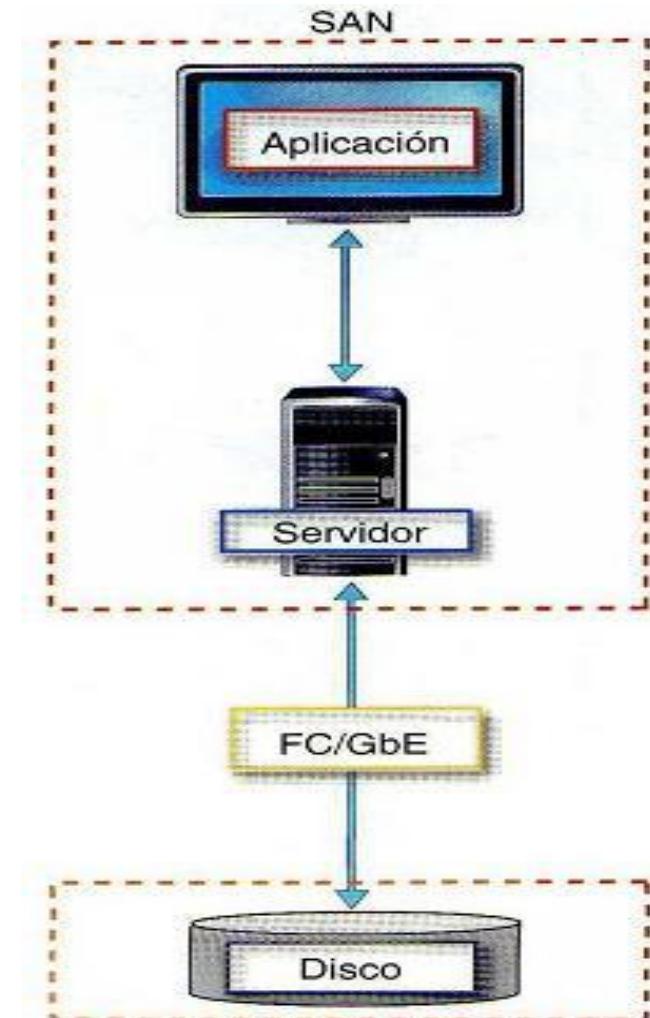


# Alojamiento de la Información

## Almacenamiento Externo.- SAN (red de área de almacenamiento)

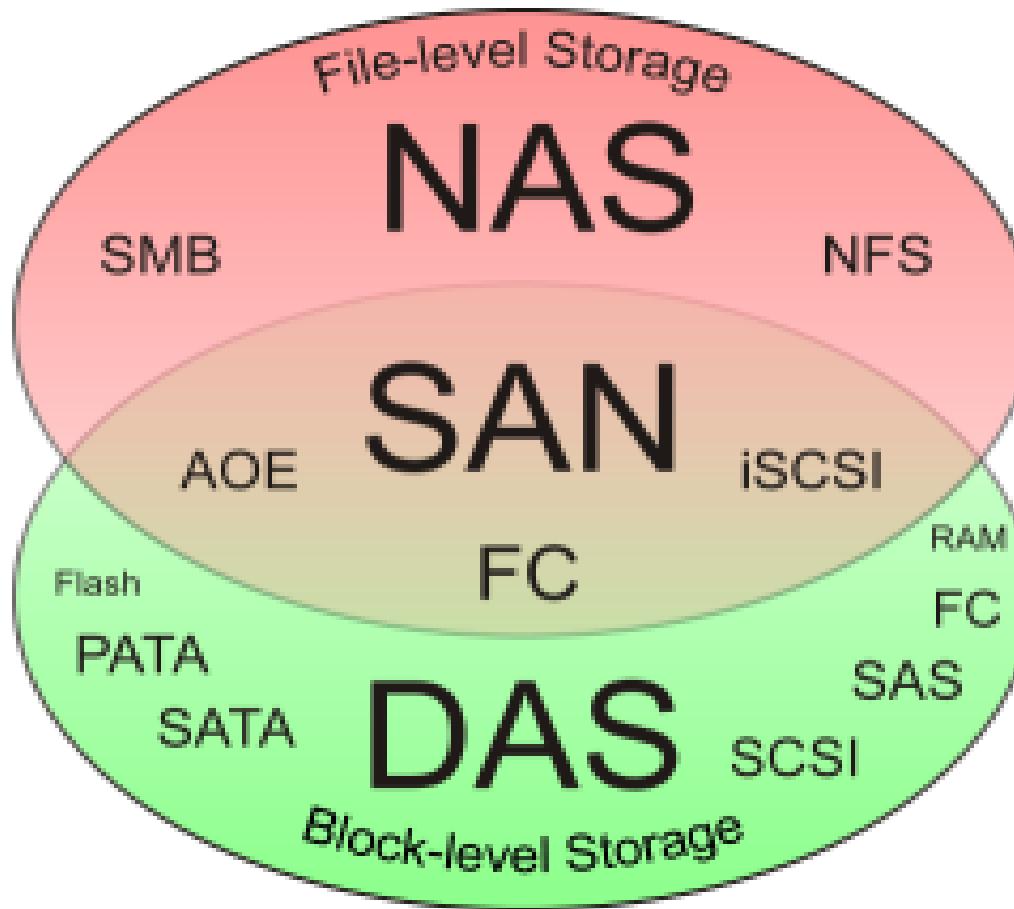
Una red **SAN** (*Storage Area Network*) o **red** con área de almacenamiento, está pensada para conectar servidores, discos de almacenamiento, etc., utilizando **tecnologías de fibra** (que alcanzan hasta 8 Gb/s) usando protocolos como **iSCSI** (*Abreviatura de Internet SCSI, es un estándar que permite el uso del protocolo SCSI sobre redes TCP/IP*)

- El uso de conexiones de alta velocidad permite que sea posible conectar de manera rápida y segura los distintos elementos de esta red, independientemente de su ubicación física.
- De modo general, un dispositivo de almacenamiento no es propiedad exclusiva de un servidor, lo que permite que varios servidores puedan acceder a los mismos recursos. El funcionamiento se basa en las peticiones de datos que realizan las aplicaciones al servidor, que se ocupa de obtener los datos del disco concreto donde estén almacenados.



# Alojamiento de la Información

## Almacenamiento Externo.-



**DAS (Direct Attached Storage):** Es el método tradicional de almacenamiento y el más sencillo. Consiste en conectar el dispositivo de almacenamiento directamente al servidor o estación de trabajo, es decir, físicamente conectado al dispositivo que hace uso de él. Es el caso convencional disponer un disco conectado directamente al sistema.

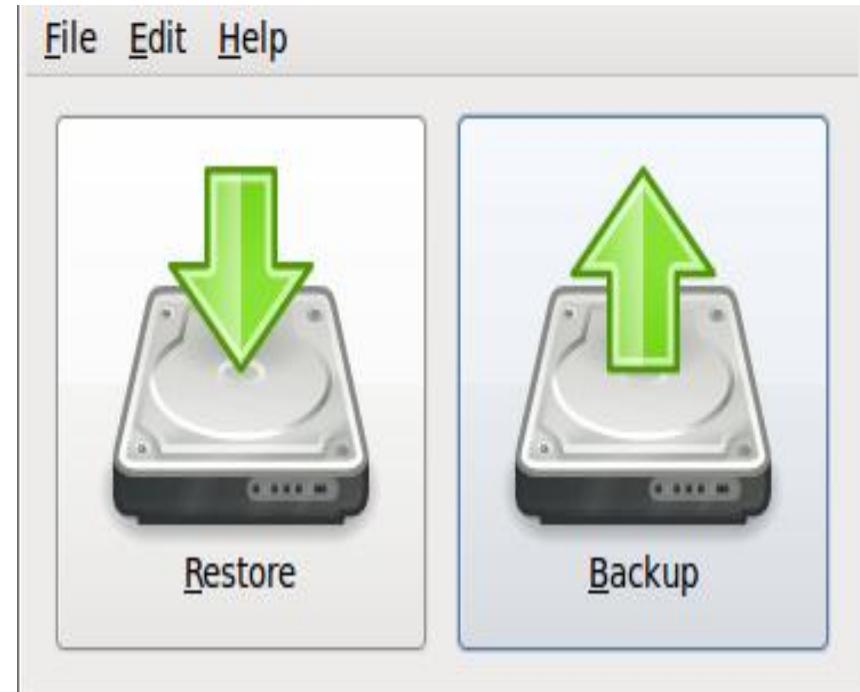
# Copias de Seguridad

## Introducción.-

Hoy en día, tanto las empresas como los particulares guardamos gran cantidad de información en los soportes de almacenamiento de nuestros equipos informáticos. En un gran número de entidades y hogares dicha información se encuentra **protegida contra amenazas lógicas**, una vez que tenemos instalados programas específicos para ello, como antivirus o firewall.

Sin embargo, son muchas menos las personas o entidades que realizan **copias de seguridad**, copias que permitirían restaurar la información en caso de perdidas por distintos motivos.

Como conclusión, las copias de seguridad garantizan dos de los objetivos estudiados en la primera unidad, la **integridad** y **disponibilidad de la información**.



# Copias de Seguridad

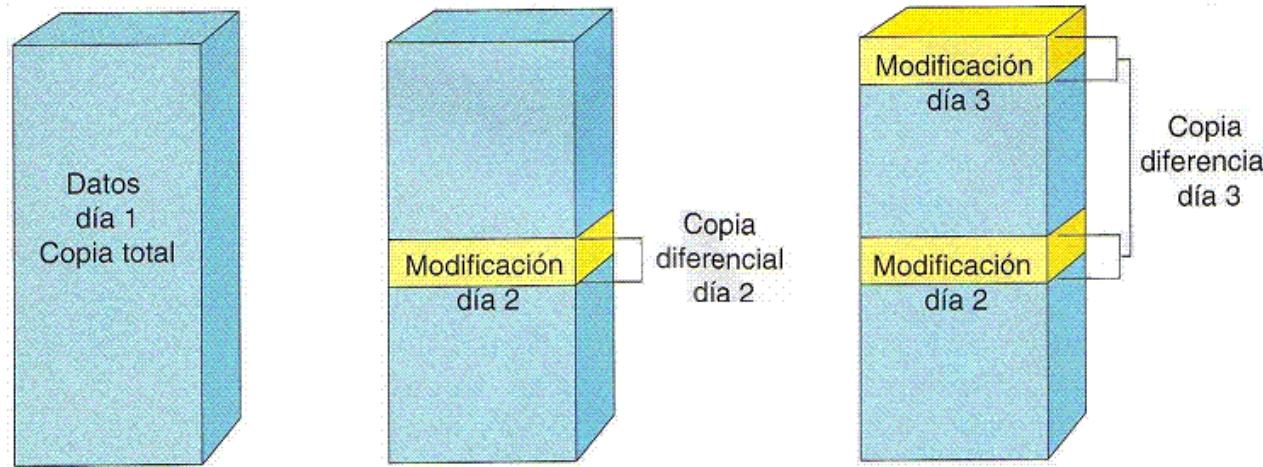
## Tipos de Copias de Seguridad.-

Dependiendo de la cantidad de ficheros que se almacenan en el momento de realizar la copia, podemos distinguir tres clases de copias de seguridad:

**Completa:** como su nombre indica, realiza una copia de todos los archivos y directorios seleccionados.

**Diferencial:** se copian todos los archivos que se han creado o actualizado desde la última copia de seguridad completa realizada.

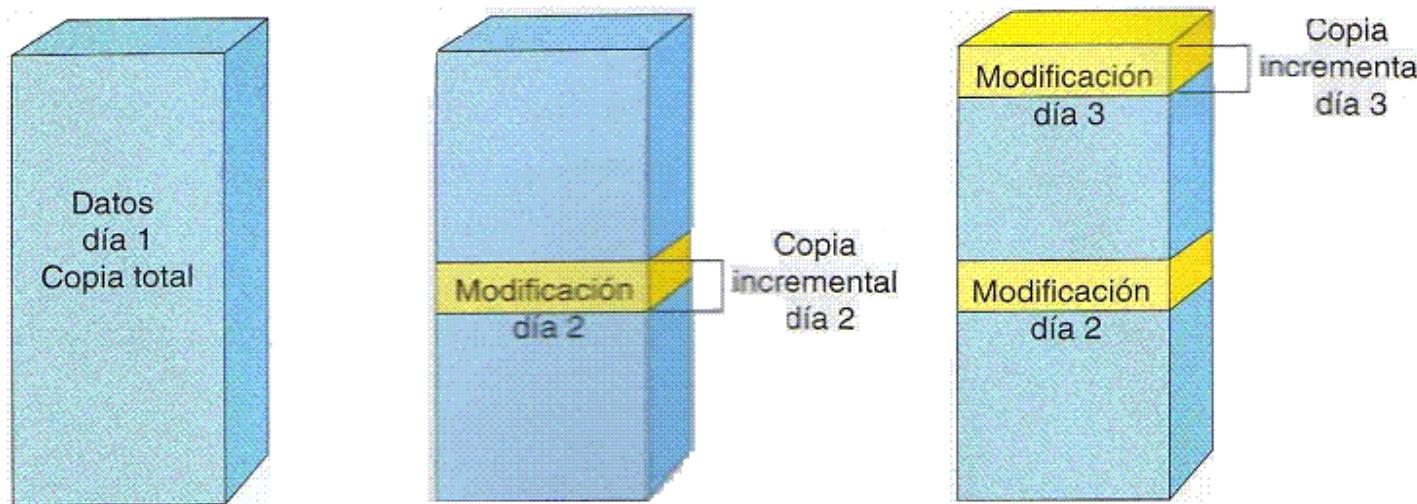
Una de las **ventajas** de este tipo de copia frente a la anterior es que se requiere menos espacio y tiempo para el proceso de la copia.



# Copias de Seguridad

## Tipos de Copias de Seguridad.-

**Incremental:** se copian los archivos que se han modificado desde la última copia de seguridad completa o diferencial realizada.



*Si el volumen de datos a realizar la copia de seguridad no es muy elevado (< 4GB), lo más práctico es realizar siempre copias totales ya que en caso de desastre, tan solo debemos recuperar la última copia. Si el volumen de datos es > 50 GB, pero el modificado  $\leq 4GB$ , lo más práctico es usar copias diferenciales. Si el volumen es > 50GB y el volumen de datos que se modifican también lo es, debería utilizarse copias incrementales*

# Copias de Seguridad

## Copias de Seguridad.- Sistemas Windows

Los sistemas Windows integra el Asistente para *copia de seguridad o restauración con el servicio de Programador de tareas*. Proporciona los puntos de *restauración de manera automática y manual, junto la protección automática del sistema*. La posibilidad de realizar copias de seguridad del *registro del sistema* de forma gráfica mediante el programa *regedit* o mediante el comando *reg*. Proceso de *reinicio del sistema en modo restauración, reparación o mediante línea de comandos*.

***En definitiva herramienta y utilidades integradas en el sistema operativo para superar un eventual desastre del sistema.***

# Copias de Seguridad

## Copias de Seguridad.- Sistemas Windows Server

El estado del sistema de controlador de dominio incluye los siguientes componentes:

- ◆ *El Directorio Activo.*
- ◆ *La carpeta compartida SYSVOL. Esta carpeta compartida contiene plantillas de políticas de grupo y secuencias de comando de inicio de sesión. La carpeta compartida SYSVOL está presente solamente en controladores de dominio.*
- ◆ *Registro. Esta base de datos contiene la información sobre la configuración del equipo.*
- ◆ *Ficheros de inicio del sistema. Windows Server 2008 requiere estos archivos durante su fase de inicio físico del equipo. Incluye el arranque y archivos de sistema.*
- ◆ *La base de datos de registros de clases COM+. Contiene información sobre servicios de aplicaciones.*
- ◆ *Base de datos del servicio de certificados. Esta base de datos contiene los certificados del servidor que Windows Server 2008 utiliza para autenticar usuarios. Esta base solamente está presente si el servidor está funcionando como "servidor de certificados".*

# Copias de Seguridad

## Copias de Seguridad.- Ejemplo de Sw para sistemas Windows

Hay muchas herramientas que permiten hacer copias de seguridad de los datos en sistemas Windows, entre ellas tenemos **Backup4all**, que nos permite proteger los datos de las posibles pérdidas parciales o totales, automatiza e proceso de realización de copias de seguridad y permite, entre otras funciones, comprimir y cifrar las copias de seguridad.

**Caso Práctico 1.- Crear copias de seguridad completa para poder recuperar los datos con facilidad en caso de desastre.**

La misma herramienta **Backup4allProfesional**, nos permite realizar copias de seguridad incrementales, como veremos en el siguiente caso práctico.

**Caso Práctico 2.- Crear copias de seguridad diferencial para salvaguardar los archivos que se han creado o actualizado desde la última copia de seguridad completa.**

Para comprobar el funcionamiento de la copia de seguridad diferencial es conveniente que modifiquéis la información almacenada en el directorio donde vamos a realizar la nueva copia diferencial.

**Caso Práctico 3.- Programar la realización de una copia de seguridad incremental todos los días a las 22:00 horas.**

Como es lógico, la herramienta nos permite, en caso de pérdida de datos, recuperar la información a partir de las copias de respaldo realizadas. Veamos un ejemplo en el siguiente caso práctico.

**Caso Práctico 4.- Restaurar copia de seguridad para recuperar los datos perdidos.**

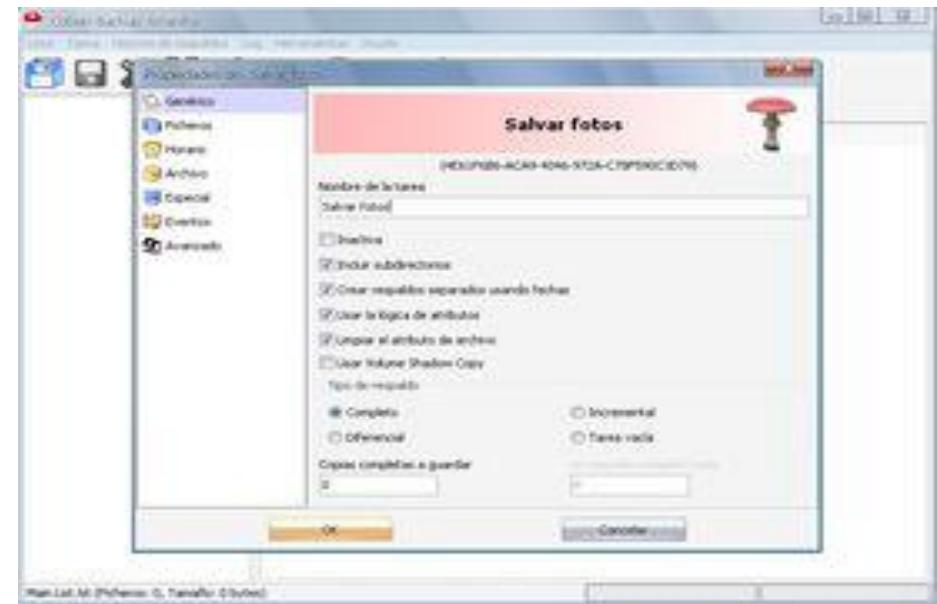
# Copias de Seguridad

## Copias de Seguridad.- Ejemplo de Sw para sistemas Windows

Otra herramienta que podemos utilizar para la realización de copias de seguridad es Cobian Backup.

Cobian Backup es un programa gratuito, multitarea, capaz de realizar copias de seguridad en un equipo, unidad extraíble, red local o incluso en/desde un servidor FTP. Soporta conexiones seguras mediante SSL. Se ejecuta sobre windows y uno de sus grandes fuertes es que consume muy pocos recursos y puede estar funcionando en segundo plano.

Soporta compresión, cifrado de sus ficheros usando 4 métodos: RSA-Rijndael (1024-256 bits), Blowfish (128 bits), Rijndael (64 bits) o DES (64 bits). Permite definir eventos antes o después de realizar la copia, como por ejemplo, provocar el cierre de un determinado programa que utilice el fichero ..etc



# Copias de Seguridad

## Copias de Seguridad.- Sistemas Operativos Linux

Para realizar copias de seguridad, puede utilizarse herramientas básicas que proporciona el sistema operativo (p.e. dump, restore, tar, cpio) o herramientas más avanzadas que permiten centralizar las copias de seguridad de los equipos de una red en un servidor. En la siguiente tabla, puede verse algunas herramientas que permiten realizar copias de seguridad:

Nombre	Licencia	URL
Amanda	Open Source	<a href="http://www.amanda.es">www.amanda.es</a>
Afbackup	Open Source	<a href="http://sourceforge.net/projects/afbackup/">http://sourceforge.net/projects/afbackup/</a>
Burt	Open Source	<a href="http://pages.cs.wisc.edu/~jmelski/burt/">http://pages.cs.wisc.edu/~jmelski/burt/</a>
BRU	Comercial	<a href="http://www.estinc.com">www.estinc.com</a>
Arkeia	Comercial	<a href="http://www.arkia.com">www.arkia.com</a>
Mondo	Open Source	<a href="http://www.mondorescue.org">www.mondorescue.org</a>

# Copias de Seguridad

## Copias de Seguridad.- Sistemas Operativos Linux

Comandos dump y restore:

La herramienta clásica para realizar copias de seguridad en entornos UNIX/linux es **dump**, que copia sistemas de ficheros completos. **restore**, se utiliza para recuperar ficheros de esas copias.

Indicar que la mayor parte de las versiones de **dump** permiten realizar copias de seguridad sobre máquinas remotas directamente desde línea de comandos (en el caso de que la variante de nuestro sistema no lo permita, podemos utilizar **rdump/rrestore**) sin más que indicar el nombre de la máquina precedido del dispositivo donde se ha de realizar la copia.

Ejemplo: *dump 0uf /dev/sdb1 /dev/sda1*

# Copias de Seguridad

## Copias de Seguridad.- Sistemas Operativos Linux

Comandos dump y restore:

Para realizar copias remotas tenemos que anteponer el nombre del sistema donde deseemos realizar la copia al nombre del dispositivo donde se va a almacenar, separado este por el carácter ‘:’. Opcionalmente, se puede indicar el nombre de usuario en el sistema remoto, separándolo del nombre de máquina por ‘@’:

*Ejemplo:*

*ufsdump 0uf nombre\_usuario@nombre\_equipo:/dev/sdb1 /dev/sda1*

Si utiliza **rdump**, tiene que definir la máquina denominada dumphost en el fichero /etc/hosts, que será el sistema donde se almacena la copia remota. De cualquier forma (usemos **dump**, **ufsdump** o **rdump**), el host remoto ha de considerarse como máquina de confianza (a través de /etc/host.equiv o .rhosts), con las consideraciones de seguridad que esto implica.

# Copias de Seguridad

## Copias de Seguridad.- Sistemas Operativos Linux

Comandos dump y restore:

Para restaurar las copias de seguridad, se utiliza el comando restore. **restore** permite extraer los ficheros de una copia de seguridad directamente mediante comandos o de forma interactiva utilizando la opción –i.

La sintaxis de esta orden es:

*restore opciones argumentos ficheros*

Donde opciones y argumentos tienen una forma similar a dump, y *ficheros*, evidentemente, representa una lista de directorios y ficheros para restaurar. En la siguiente tabla se muestra las opciones más utilizadas.

Opción	Acción
r	Restaurar el dispositivo
f	Indica el dispositivo o fichero está el backup
i	Modo interactivo
x	Extraer los ficheros y directorios desde el directorio actual
t	Imprimir el nombre de los ficheros

# Copias de Seguridad

## Copias de Seguridad.- Sistemas Operativos Linux

### Comandos dump y restore:

Si desea restaurar de forma interactiva la copia realizada, debe ejecutarse el comando restore – i (-f /dev/sdb1) para iniciar la consola de recuperación. Dentro de la consola de administración debe especificarse los archivos que desea recuperar con el comando add, para extraer los ficheros ejecute extract, y para finalizar exit. Si desea información sobre los diferentes comandos. Ejecutar help:

```
luisa:~# restore -i -f backup
restore > help
Available commands are:
  ls [arg] - list directory cd
  arg - change directory
  pwd - print current directory
  add [arg] - add `arg' to list of files to be extracted
  delete [arg] - delete `arg' from list of files to be extracted
  extract - extract requested files
  setmodes - set modes of requested directories
  quit - immediately exit program
  what - list dump header information
  verbose - toggle verbose flag (useful with ``ls'')
  help or `?' - print this list If no `arg' is supplied, the current directory is used
restore > ls
```

# Copias de Seguridad

## Copias de Seguridad.- Sistemas Operativos Linux

Comando tar:

- La utilidad tar (*Tape Archiver*) es una herramienta de fácil manejo disponible en todas las versiones de Unix que permite volcar ficheros individuales o directorios completos en un único fichero; inicialmente fué diseñada para crear archivos de cinta (esto es, para transferir archivos de un disco a una cinta magnética y viceversa), aunque en la actualidad casi todas sus versiones pueden utilizarse para copiar a cualquier dispositivo o fichero, denominado `contenedor'.
  
- Su principal desventaja es que, bajo ciertas condiciones, si falla una porción del medio (por ejemplo, una cinta) se puede perder toda la copia de seguridad; además, tar no es capaz de realizar por sí mismo más que copias de seguridad completas, por lo que hace falta un poco de programación *shellscrips* para realizar copias progresivas o diferenciales.

# Copias de Seguridad

## Copias de Seguridad.- Sistemas Operativos Linux

Comando tar:

- En la tabla muestra las opciones de tar más habituales; algunas de ellas no están disponibles en todas las versiones de tar, por lo que es recomendable consultar la página del manual de esta orden antes de utilizarla. Si la implementación de tar que existe en nuestro sistema no se ajusta a nuestras necesidades, siempre podemos utilizar la versión de GNU (<http://www.gnu.org/>), quizás la más completa hoy en día.

Opción	Acción realizada
c	Crea un contenedor
x	Extrae archivos de un contenedor
t	Testea los archivos almacenados en un contenedor
r	Añade archivos al final de un contenedor
v	Modo verbose
f	Especifica el nombre del contenedor
Z	Comprime o descomprime mediante compress/uncompress
z	Comprime o descomprime mediante gzip
p	Conserva los permisos de los ficheros

# Copias de Seguridad

## Copias de Seguridad.- Sistemas Operativos Linux

Comando tar:

- En primer lugar debemos saber cómo crear contenedores con los archivos deseados; por ejemplo, imaginemos que deseamos volcar todo el directorio /export/home/ a la unidad de cinta /dev/rmt/0.
- Esto lo conseguimos con la siguiente orden:

```
anita:~# tar cvf /dev/rmt/0 /export/home/
```

*Como podemos ver, estamos especificando juntas las diferentes opciones necesarias para hacer la copia de seguridad de los directorios de usuario; la opción 'v' no sería necesaria, pero es útil para ver un listado de lo que estamos almacenando en la cinta. En muchas situaciones también resulta útil comprimir la información guardada (tar no comprime, sólo empaqueta); esto lo conseguiríamos con las opciones `cvzf`.*

# Copias de Seguridad

## Copias de Seguridad.- Sistemas Operativos Linux

Comando tar:

- Si en lugar de (o aparte de) un único directorio con todos sus ficheros y subdirectorios quisiéramos especificar múltiples archivos (o directorios), podemos indicárselos uno a uno a tar en la línea de comandos; así mismo, podemos indicar un nombre de archivo contenedor en lugar de un dispositivo.

Por ejemplo, la siguiente orden creará el fichero /tmp/backup.tar, que contendrá /etc/passwd y /etc/hosts\*:

```
anita:~# tar cvf /tmp/backup.tar /etc/passwd /etc/hosts*
tar: Removing leading `/' from absolute path names in the archive
/etc/passwd
/etc/hosts
/etc/hosts.allow
/etc/hosts.deny
/etc/hosts.equiv
anita:~#
```

# Copias de Seguridad

## Copias de Seguridad.- Sistemas Operativos Linux

Comando tar:

- Una vez creado el contenedor podemos testear su contenido con la opción `t' para comprobar la integridad del archivo, y también para ver qué ficheros se encuentran en su interior:

```
anita:~# tar tvf /tmp/backup.tar
-rw-r--r-- root/other 965 2000-03-11 03:41 etc/passwd
-rw-r--r-- root/other 704 2000-03-14 00:56 etc/hosts
-rw-r--r-- root/other 449 2000-02-17 01:48 etc/hosts.allow
-rw-r--r-- root/other 305 1998-04-18 07:05 etc/hosts.deny
-rw-r--r-- root/other 313 1994-03-16 03:30 etc/hosts.equiv
-rw-r--r-- root/other 345 1999-10-13 03:31 etc/hosts.lpd
anita:~#
```

# Copias de Seguridad

## Copias de Seguridad.- Sistemas Operativos Linux

Comando tar:

- Si lo que queremos es recuperar ficheros guardados en un contenedor utilizaremos las opciones `xvf` (o `xvzf` si hemos utilizado compresión con gzip a la hora de crearlo). Podemos indicar el archivo o archivos que queremos extraer; si no lo hacemos, se extraerán todos:

```
anita:~# tar xvf /tmp/backup.tar etc/passwd  
etc/passwd  
anita:~#tar xvf /tmp/backup.tar  
etc/passwd  
etc/hosts  
etc/hosts.allow  
etc/hosts.deny  
etc/hosts.equiv  
etc/hosts.lpd  
anita:~#
```

*La restauración se habrá realizado desde el directorio de trabajo, creando en él un subdirectorio etc con los ficheros correspondientes en su interior. Si queremos que los ficheros del contenedor sobrescriban a los que ya existen en el sistema hemos de desempaquetarlo en el directorio adecuado, en este caso el raíz.*

# Copias de Seguridad

## Copias de Seguridad.- Sistemas Operativos Linux

### Comando cpio:

- ❑ cpio (*Copy In/Out*) es una utilidad que permite copiar archivos a o desde un contenedor *cpio*, que no es más que un fichero que almacena otros archivos e información sobre ellos (permisos, nombres, propietario...). Este contenedor puede ser un disco, otro archivo, una cinta o incluso una tubería, mientras que los ficheros a copiar pueden ser archivos normales, pero también dispositivos o sistemas de ficheros completos.
- ❑ En la tabla se muestran las opciones de cpio más utilizadas; la sintaxis de esta orden es bastante más confusa que la de tar debido a la interpretación de lo que cpio entiende por '*dentro*' y '*fueras*': copiar '*fueras*' es generar un contenedor en salida estándar (que con toda probabilidad desearemos redireccionar), mientras que copiar '*dentro*' es lo contrario, es decir, extraer archivos de la entrada estándar (también es seguro que deberemos redireccionarla).

Opción	Acción realizada
o	Copiar 'fuera' (out)
i	Copiar 'dentro' (in)
m	Conserva fecha y hora de los ficheros
t	Crea tabla de contenidos
A	Añade ficheros a un contenedor existente
v	Modo verbose

# Copias de Seguridad

## Copias de Seguridad.- Sistemas Operativos Linux

Comando cpio:

- Por ejemplo, si deseamos copiar los archivos de /export/home/ en el fichero contenedor /tmp/backup.cpio podemos utilizar la siguiente sintaxis:

```
anita:~# find /export/home/ | cpio -o > /tmp/backup.cpio
```

Como podemos ver, cpio lee la entrada estándar esperando los nombres de ficheros a guardar, por lo que es conveniente utilizarlo tras una tubería pasándole esos nombres de archivo. Además, hemos de redirigir su salida al nombre que queramos asignarle al contenedor, ya que de lo contrario se mostraría el resultado en salida estándar (lo que evidentemente no es muy utilizado para realizar *backups*). Podemos fijarnos también en que estamos usando la orden 'find' en lugar de un simple 'ls': esto es debido a que 'ls' mostraría sólo el nombre de cada fichero (por ejemplo, 'passwd') en lugar de su ruta completa ('/etc/passwd'), por lo que cpio buscaría dichos ficheros a partir del directorio actual.

# Copias de Seguridad

## Copias de Seguridad.- Sistemas Operativos Linux

Comando cpio:

- Una vez creado el fichero contenedor quizás resulte interesante chequear su contenido, con la opción `t'. Por ejemplo, la siguiente orden mostrará en pantalla el contenido de /tmp/backup.cpio:

```
anita:~# cpio -t < /tmp/backup.cpio
```

Igual que para almacenar ficheros en un contenedor hemos de pasarle a cpio la ruta de los mismos, para extraerlos hemos de hacer lo mismo; si no indicamos lo contrario, cpio -i extraerá todos los archivos de un contenedor, pero si sólo nos interesan algunos de ellos podemos especificar su nombre de la siguiente forma:

```
anita:~# echo "/export/home/toni/hola.tex" |cpio -i </tmp/backup.cpio
```

Para conocer más profundamente el funcionamiento de cpio, así como opciones propias de cada implementación, es indispensable consultar la página del manual de esta orden en cada clon de Unix donde vayamos a utilizarla.

# Copias de Seguridad

## Copias de Seguridad.- Sistemas Operativos Linux

Comando dd:

- El comando dd permite realizar copias exactas (bit a bit) de discos duros, particiones o ficheros. La sintaxis de dd es la siguiente:

dd if=fichero-origen of=fichero destino

- Si quisiéramos clonar el disco duro /dev/sda en el disco duro /dev/sdb, ejecutaría:

dd if= /dev/sda of=/dev/sdb

1.- Haciendo imágenes ISO de un CD: dd if=/dev/cdrom of=micd.iso

2.- Copia una partición en otra: dd if=/dev/hdx of=/dev/hdy (a,b  
*partición;x,y disco rígido)*

3.- Copia un disco en otro: dd if=/dev/hdx of=/dev/hdy (*x,y disco rígido*)

4.- Haciendo imágenes ISO de una partición: dd if=/dev/hda of=micd.iso

5.- Haciendo imágenes ISO de un disco rígido: dd if=/dev/hda of=micd.iso

# Copias de Seguridad

## Copias de Seguridad.- Sistemas Operativos Linux

Comando dd - ddrescue :

- Para recuperar una imagen realizada con dd tenemos la herramienta rrescue.

```
admin$> ddrescue -n /dev/old_disk /dev/new_disk
```

[http://www.gnu.org/s/ddrescue/manual/ddrescue\\_manual.html](http://www.gnu.org/s/ddrescue/manual/ddrescue_manual.html)

**Ddrescue - Herramienta de  
recuperación de datos**



# Copias de Seguridad

## Copias de Seguridad.- Sistemas Operativos Linux

### Herramienta rsync:

- ❑ **rsync** es una aplicación libre para sistemas de tipo Unix y Microsoft Windows que ofrece transmisión eficiente de datos incrementales, que opera también con datos comprimidos y cifrados. Mediante una técnica de delta encoding, permite sincronizar archivos y directorios entre dos máquinas de una red o entre dos ubicaciones en una misma máquina, minimizando el volumen de datos transferidos.
- ❑ Actuando como un dominio de servidor, rsync escucha por defecto el puerto TCP 873, sirviendo archivos en el protocolo nativo rsync o vía un terminal remoto como RSH o SSH. En el último caso, el ejecutable del cliente rsync debe ser instalado en el host local y remoto.

*rsync se distribuye bajo la licencia GNU General Public License.*

# Copias de Seguridad

## Copias de Seguridad.- Sistemas Operativos Linux

Herramienta *duplicity*:

*duplicity* nos permite realizar backups de nuestros directorios produciendo un fichero encriptado en formato tar y subiendo este a un servidor de ficheros local o remoto.

Para instalarlo: *\$ apt-get install duplicity*

*duplicity* es bastante similar a rsync pero presenta una ventaja sobre este: **No es necesario escribir ningún fichero de configuracion.**

Para usarlo, simplemente ejecuta algo como: *duplicity data scp://jose@server/saves*

*Realiza un backup del directorio “data” en un servidor remoto scp (server) al que te conectas como el usuario “jose” y dejando el backup en el folder /saves*

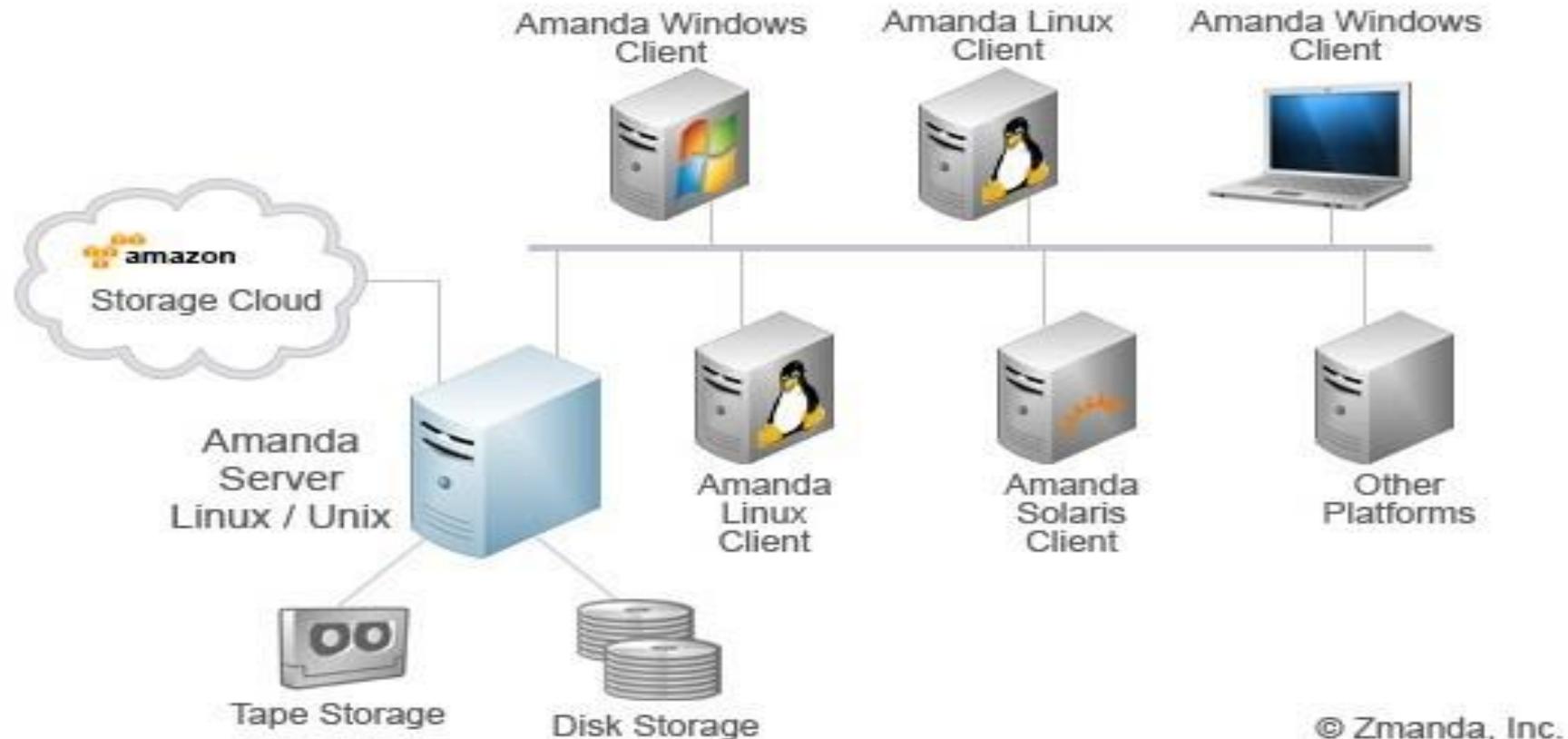
O si lo deseas para hacer un backup local: *duplicity data file:///var/backup/data*

Comando básico de restauración: restaura el directorio /home/me del backup al directorio restored\_dir: *duplicity scp://uid@other.host//usr/backup restored\_dir*

# Copias de Seguridad

## Copias de Seguridad.- Sistemas Operativos Linux

Herramienta Amanda:



# Copias de Seguridad

## Copias de Seguridad.- Sistemas Operativos Linux

Herramienta Amanda:

- *Herramienta orientada a crear copias de seguridad en múltiples terminales bajo la dirección del administrador de la red. El proceso se lleva a cabo gracias a un servidor que engloba a los terminales seleccionados y realiza un backup rápido y cómodo, ya que evita andar clonando disco por disco.*
- *Para poner en marcha amanda es necesario configurar cliente/servidor –instalación y configuración cliente y servidor-*



<http://www.amanda.org/>

# Copias de Seguridad

## Copias de Seguridad.- Sistemas Operativos Linux

Herramienta Amanda:

### Programar una copia de seguridad –Amanda

Las copias de seguridad las puede realizar el usuario *amanda* directamente a través del comando *amdump*, o si lo prefiere programarlas para que se realicen automáticamente, utilizando para ello crontab (como veremos en el siguiente punto)

### Restaurar copia de Seguridad

Para restaurar los datos de una copia de seguridad puede utilizar herramientas estándar (p.e. *dd*) o través de las herramientas que proporciona amanda (*amrecover o amrestore*). Si desea restaurar los datos con las herramientas de amanda con el comando *amadmin* puede verse las unidades en las que se encuentran los datos a restaurar. ***amadmin DailySet1 info cliente '/home\$'*** obtiene las unidades en las que se encuentran los datos de /home del equipo cliente. Ejecutamos el comando *amrecover* en el equipo cliente como root, indicar que debemos tener en */var/lib/amanda/.amandahost* del equipo cliente que el usuario root tienen acceso al servidor.

# Copias de Seguridad

## Copias de Seguridad.- Sistemas Operativos Linux - Planificación

Servicio crond-Programación de tareas:

### ¿Qué es cron?



Cron es el nombre del programa que permite a usuarios Linux/Unix ejecutar automáticamente comandos o scripts (grupos de comandos) a una hora o fecha específica. Es usado normalmente para comandos de tareas administrativas, como respaldos, pero puede ser usado para ejecutar cualquier cosa. Como se define en las páginas del manual de cron (#> man cron) es un demonio que ejecuta programas *!agendados*.

En prácticamente todas las distribuciones de Linux se usa la versión Vixie Cron, por la persona que la desarrolló, que es Paul Vixie, uno de los grandes gurús de Unix, también creador, entre otros sistemas, de BIND que es uno de los servidores DNS más populares del mundo.

# Copias de Seguridad

## Copias de Seguridad.- Sistemas Operativos Linux - Planificación

Servicio crond-Programación de tareas:

### Iniciar cron

Cron es un demonio (servicio), lo que significa que solo requiere ser iniciado una vez, generalmente con el mismo arranque del sistema. El servicio de cron se llama crond. En la mayoría de las distribuciones el servicio se instala automáticamente y queda iniciado desde el arranque del sistema, se puede comprobar de varias maneras:

#> /etc/rc.d/init.d/crond status

#> /etc/init.d/crond status Usa cualquiera de los dos dependiendo de tu distri. crond (pid 507) is running... o si tienes el comando service instalado:

#> service crond status crond (pid 507) is running...

se puede también revisar a través del comando ps:

# ps -ef | grep crond si por alguna razón, cron no esta funcionando:

#> /etc/rc.d/init.d/crond start Starting crond: [ OK ]

Si el servicio no estuviera configurado para arrancar desde un principio, bastaría con agregarlo con el comando chkconfig:

#> **chkconfig --level 35 crond on** *Con esto lo estarías agregando al nivel de ejecución 3 y 5, para que inicie al momento del arranque del sistema.*

# Copias de Seguridad

## Copias de Seguridad.- Sistemas Operativos Linux - Planificación

Servicio crond-Programación de tareas:

### Usando cron

Hay al menos dos maneras distintas de usar cron:

La primera es en el directorio etc, donde podremos encontrar los siguientes directorios:

*cron.hourly*

*cron.daily*

*cron.weekly*

*cron.monthly*

*Si se coloca un archivo tipo script en cualquiera de estos directorios, entonces el script se ejecutará cada hora, cada día, cada semana o cada mes, dependiendo del directorio.*

# Copias de Seguridad

## Copias de Seguridad.- Sistemas Operativos Linux - Planificación

Servicio crond-Programación de tareas:

### □ Usando cron

Para que el archivo pueda ser ejecutado tiene que ser algo similar a lo siguiente:

```
#!/bin/sh #script que genera un respaldo  
cd /usr/documentos  
tar czf respaldo *  
cp respaldo /otra_directorio/.
```

Nótese que la primera línea empieza con #!, que indica que se trata de un script shell de bash, las demás líneas son los comandos que deseamos execute el script. Este script podría nombrarse por ejemplo respaldo.sh y también debemos cambiarle los permisos correspondientes para que pueda ser ejecutado, por ejemplo:

```
#> chmod 700 respaldo.sh  
#> ls -l respaldo.sh -rwx----- 1 root root 0 Jul 20 09:30 respaldo.sh
```

La "x" en el grupo de permisos del propietario (rwx) indica que puede ser ejecutado.

*Si este script lo dejamos en cron.hourly, entonces se ejecutará cada hora con un minuto de todos los días.*

# Copias de Seguridad

## Copias de Seguridad.- Sistemas Operativos Linux - Planificación

Servicio crond-Programación de tareas:

### □ Usando cron

Como segundo modo de ejecutar o usar cron es a través de manipular directamente el archivo /etc/crontab. En la instalación por defecto de varias distribuciones Linux, este archivo contendrá algo como lo siguiente:

```
#> cat /etc/crontab
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root
HOME=/
# run-parts
01 * * * * root run-parts /etc/cron.hourly
02 4 * * * root run-parts /etc/cron.daily
22 4 * * 0 root run-parts /etc/cron.weekly
42 4 1 * * root run-parts /etc/cron.monthly
```

# Copias de Seguridad

## Copias de Seguridad.- Sistemas Operativos Linux - Planificación

Servicio crond-Programación de tareas:

### □ Usando cron

Las primeras cuatro líneas son variables que indican lo siguiente:

- **SHELL** es el 'shell' bajo el cual se ejecuta el cron. Si no se especifica, se tomará por defecto el indicado en la línea /etc/passwd correspondiente al usuario que este ejecutando cron.
- **PATH** contiene o indica la ruta a los directorios en los cuales cron buscará el comando a ejecutar. Este path es distinto al path global del sistema o del usuario.
- **MAIL TO** es a quien se le envía la salida del comando (si es que este tiene alguna salida). Cron enviará un correo a quien se especifique en este variable, es decir, debe ser un usuario válido del sistema o de algún otro sistema. Si no se especifica, entonces cron enviará el correo al usuario propietario del comando que se ejecuta.
- **HOME** es el directorio raíz o principal del comando cron, si no se indica entonces, la raíz será la que se indique en el archivo /etc/passwd correspondiente al usuario que ejecuta cron.

Los comentarios se indican con # al inicio de la línea.

# Copias de Seguridad

## Copias de Seguridad.- Sistemas Operativos Linux - Planificación

Servicio crond-Programación de tareas:

### Usando cron

# EXECUTE BACKUP.SH SCRIPT EVERY SUNDAY AT 2:36 AM					
36 2 * * 7 root /usr/local/sbin/backup.sh					
36	2	*	*	7	root /usr/local/sbin/backup.sh
VALUE RANGE	VALUE RANGE	VALUE RANGE	VALUE RANGE	VALUE RANGE	- COMMAND TO EXECUTE
0-59	0-23	1-31	1-12	0-7	- EXECUTE COMMAND AS A USER ROOT
<b>- DAY OF WEEK:</b> Sunday =0, Monday =1, Tuesday=2, Wednesday=3 Thursday=4, Friday=5, Saturday=6, Sunday=7					
<b>- MONTH:</b> January =1, February=2, March=3, April=4, May=5, June=6 July=7, August=8, September=9, October=10, November=11, December=12					
<b>- DAY OF MONTH</b>					
<b>- HOUR</b>					
<b>- MINUTE</b>					

# Copias de Seguridad

## Copias de Seguridad.- Sistemas Operativos Linux - Planificación

Servicio crond-Programación de tareas:

### □ Usando cron

Un asterisco \* como valor en los primeros cinco campos, indicará inicio-fin del campo, es decir todo. Un \* en el campo de minuto indicará todos los minutos

Ejemplo	Descripción
01 * * * *	Se ejecuta al minuto 1 de cada hora de todos los días
15 8 * * *	A las 8:15 a.m. de cada día
15 20 * * *	A las 8:15 p.m. de cada día
00 5 * * 0	A las 5 a.m. todos los domingos
* 5 * * Sun	Cada minuto de 5:00a.m. a 5:59a.m. todos los domingos
45 19 1 * *	A las 7:45 p.m. del primero de cada mes
01 * 20 7 *	Al minuto 1 de cada hora del 20 de julio
10 1 * 12 1	A la 1:10 a.m. todos los lunes de diciembre
00 12 16 * Wen	Al mediodía de los días 16 de cada mes y que sea Miércoles
30 9 20 7 4	A las 9:30 a.m. del dia 20 de julio y que sea jueves
30 9 20 7 *	A las 9:30 a.m. del dia 20 de julio sin importar el día de la semana
20 * * * 6	Al minuto 20 de cada hora de los sábados
20 * * 1 6	Al minuto 20 de cada hora de los sábados de enero

# Copias de Seguridad

## Copias de Seguridad.- Sistemas Operativos Linux - Planificación

Servicio crond-Programación de tareas:

### □ Usando cron

También es posible especificar listas en los campos. Las listas pueden estar en la forma de 1,2,3,4 o en la forma de 1-4 que sería lo mismo. Cron, de igual manera soporta incrementos en las listas, que se indican de la siguiente manera: Valor o lista/incremento

Ejemplo	Descripción
59 11 * 1-3 1,2,3,4,5	A las 11:59 a.m. de lunes a viernes, de enero a marzo
45 * 10-25 * 6-7	Al minuto 45 de todas las horas de los días 10 al 25 de todos los meses y que el día sea sábado o domingo
10,30,50 * * * 1,3,5	En el minuto 10, 30 y 50 de todas las horas de los días lunes, miércoles y viernes
*/15 10-14 * * *	Cada quince minutos de las 10:00a.m. a las 2:00p.m.
* 12 1-10/2 2,8 *	Todos los minutos de las 12 del día, en los días 1,3,5,7 y 9 de febrero y agosto. (El incremento en el tercer campo es de 2 y comienza a partir del 1)
0 */5 1-10,15,20-23 * 3	Cada 5 horas de los días 1 al 10, el día 15 y del día 20 al 23 de cada mes y que el día sea miércoles
3/3 2/4 2 2 2	Cada 3 minutos empezando por el minuto 3 (3,6,9, etc.) de las horas 2,6,10, etc (cada 4 horas empezando en la hora 2) del día 2 de febrero y que sea martes

# Copias de Seguridad

## Copias de Seguridad.- Sistemas Operativos Linux - Planificación

Servicio crond-Programación de tareas:

### □ Usando cron

Incluyendo el campo del usuario y el comando, los renglones de crontab podrían quedar entonces de la siguiente manera:

```
0 22 * * * root /usr/respaldodiario.sh
0 23 * * 5 root /usr/respaldosemanal.sh
0 8,20 * * * sergio mail -s "sistema funcionando" sgd@ejemplo.com
```

*Las dos primeras líneas las ejecuta el usuario root y la primera ejecuta a las 10 de la noche de todos los días el script que genera un respaldo diario.*

*La segunda ejecuta a las 11 de la noche de todos los viernes un script que genera un respaldo semana.*

*La tercera línea la ejecuta el usuario sergio y se ejecutaría a las 8 de la mañana y 8 de la noche de todos los días y el comando envia un correo a la cuenta sgd@ejemplo.com con el asunto "sistema funcionando".*

# Copias de Seguridad

## Copias de Seguridad.- Sistemas Operativos Linux - Planificación

Servicio crond-Programación de tareas:

### □ Usando cron con múltiples usuarios

- ❖ Linux es un sistema multiusuario y cron es de las aplicaciones que soporta el trabajo con varios usuarios a la vez. Cada usuario puede tener su propio archivo crontab, de hecho el /etc/crontab se asume que es el archivo crontab del usuario root, aunque no hay problema que se incluyan otros usuarios, y de ahí el sexto campo que indica precisamente quien es el usuario que ejecuta la tarea.
- ❖ Pero cuando los usuarios normales (e incluso root) desean generar su propio archivo de crontab, *entonces utilizaremos el comando crontab -e*. En el directorio /var/spool/cron (puede variar según la distribución), se genera un archivo cron para cada usuario, este archivo aunque es de texto, *no debe editarse directamente*.

# Copias de Seguridad

## Copias de Seguridad.- Sistemas Operativos Linux - Planificación

Servicio crond-Programación de tareas:

### □ Usando cron con multiples usuarios

Se tiene entonces, dos situaciones, generar directamente el archivo crontab con el comando:

```
$> crontab -e
```

Con lo cual se abrirá el editor por default con el archivo llamado crontab vacío y donde el usuario ingresará su tabla de tareas y que se guardará automáticamente como /var/spool/cron/usuario.

El otro caso es que el usuario edite un archivo de texto normal con las entradas de las tareas y como ejemplo lo nombre 'mi\_cron', después el comando :

```
$> crontab mi_cron
```

 se encargará de establecerlo como el archivo cron del usuario en /var/spool/cron/usuario:

# Copias de Seguridad

## Copias de Seguridad.- Sistemas Operativos Linux - Planificación

Servicio crond-Programación de tareas:

### □ Usando cron con multiples usuarios

```
$> vi mi_cron
# borra archivos de carpeta compartida
0 20 * * * rm -f /home/sergio/compartidos/*
# ejecuta un script que realiza un respaldo de la carpeta documentos el primer
día de cada mes
0 22 1 * * /home/sergio/respaldomensual.sh
# cada 5 horas de lun a vie, se asegura que los permisos sean los correctos en mi
home
1 *5 * * * 1-5 chmod -R 640 /home/sergio/*
:wq (se guarda el archivo)
$> ls mi_cron
$> crontab mi_cron (se establece en /var/spool/cron/usuario)
```

# Copias de Seguridad

## Copias de Seguridad.- Sistemas Operativos Linux - Planificación

Servicio crond-Programación de tareas:

### □ Usando cron con multiples usuarios

Resumiendo lo anterior y considerando otras opciones de crontab:

\$> crontab archivo.cron (*establecerá el archivo.cron como el crontab del usuario*)

\$> crontab -e (*abrirá el editor preestablecido donde se podrá crear o editar el archivo crontab*)

\$> crontab -l (*lista el crontab actual del usuario, sus tareas de cron*)

\$> crontab -r (*elimina el crontab actual del usuario*)

En algunas distribuciones cuando se editan crontabs de usuarios normales es necesario reiniciar el servicio para que se puedan releer los archivos de crontab en /var/spool/cron.

#> service crond restart

# Copias de Seguridad

## Copias de Seguridad.- Sistemas Operativos Linux - Planificación

Servicio crond-Programación de tareas:

### □ Controlando el acceso a cron

cron permite controlar que usuarios pueden o no pueden usar los servicios de cron. Esto se logra de una manera muy sencilla a través de los siguientes archivos:

`/etc/cron.allow`  
`/etc/cron.deny`

Para impedir que un usuario utilice cron o mejor dicho el comando crontab, basta con agregar su nombre de usuario al archivo `/etc/cron.deny`, para permitirle su uso entonces sería agregar su nombre de usuario en `/etc/cron.allow`, si por alguna razón se desea negar el uso de cron a todos los usuarios, entonces se puede escribir la palabra ALL al inicio de `cron.deny` y con eso bastaría.

```
#> echo ALL >>/etc/cron.deny o para agregar un usuario mas a cron.allow  
#> echo juan >>/etc/cron.allow
```

Si no existe el archivo `cron.allow` ni el archivo `cron.deny`, en teoría el uso de cron esta entonces sin restricciones de usuario.

# Copias de Seguridad

## Copias de Seguridad.- Sistemas Operativos Linux - Planificación

Ejemplo de shellscript en la planificación de copias de seguridad :

```
#!/bin/bash
```

```
# script de copia completa e incremental
# modificar directorios a respaldar y destino del Backup
DIRECTORIOS="/bin /boot /etc /initrd /home /lib /opt /root /sbin /srv /u sr /var"
# Directorio donde se guarda el backup
BACKUPDIR=/home/Backups # Directorio que guarda la fecha del último backup
completo
FECHADIR=/home/Backups
DSEM='date +%a' # Dia de la semana (por ej. mié)
DMES='date +%d' # Dia del mes (por ej.,06)
DYM='date +%d%b' # Día y mes (por ej. 06jun)
# "NUEVO" coge la fecha del backup completo de cada domingo
# Backup mensual completo - sobrescribe el del mes anterior
if [ $DMES = "01" ]; then
tar -cf $BACKUPDIR/CTM-$DYM.tar $DIRECTORIOS
fi
```

A modo de ejemplo se mostrará un script para realizar backup completo o total del sistema cada 1º de mes, otro backup completo semanal cada domingo y backup diarios incrementales -solo de los cambios realizados desde el último backup completo-.

# Copias de Seguridad

## Copias de Seguridad.- Sistemas Operativos Linux - Planificación

Ejemplo de shellscript en la planificación de copias de seguridad :

```
# Backup semanal completo
# Actualiza fecha del backup completo

if [ $DSEM = "dom" ] ; then
AHORA='date +%d-%b'
echo $AHORA > $FECHADIR/fecha-backup-completo
tar -cf $BACKUPDIR/CTS-$DSEM.tar $DIRECTORIOS
    # Backup incremental diario -sobrescribe semana anterior
    # Obtiene fecha del último backup completo, opcion newer.
else
NUEVO="--newer= ' cat $FECHADIR/ fecha-backup-completo ' "
tar $NUEVO -cf $BACKUPDIR/ID-$DSEM.tar $DIRECTORIOS
fi
```

# Copias de Seguridad

## Copias de Seguridad.- Sistemas Operativos Linux - Planificación

Ejemplo II de shellscript en la planificación de copias de seguridad :

#Al cambiar de mes, la primera copia es total

#Obtenemos los datos referidos a la fecha del sistema

```
dia=`date | cut -d" " -f3`
```

```
mes=`date | cut -d" " -f2`
```

```
anyo=`date | cut -d" " -f6`
```

```
nombre=`echo $mes$anyo `
```

#ruta indica el lugar donde se guarda la copia de seguridad, debería ser un disco duro secundario,

# montado en X, se debe montar automáticamente con el fichero /etc/fstab

```
ruta=/var/copiaSeguridad/
```

# Copias de Seguridad

## Copias de Seguridad.- Sistemas Operativos Linux - Planificación

Ejemplo II de shellscript en la planificación de copias de seguridad :

```
#Si ya existe el directorio no es la primera copia del mes en curso
if [ -d $ruta/$nombre ]; then
#preparo la copia primero guardo los ficheros antiguos
    rm -f $ruta/$nombre/*.bak
    for fichero in `ls $ruta$nombre/
    do
        mv $fichero $fichero.bak
    done
#orden de copia incremental
#nombre del fichero es $nombre.tar ya que si estuviera comprimido no puedo hacer actualizaciones del mismo
#orden de copia total
    tar -czf $ruta$nombre/$nombre.tar.gz /var/ficheros_moodle/ 2> /dev/null
    tar -czf $ruta$nombre/$nombre/www.tar.gz /var/www 2> /dev/null
else
#se trata de una copia total
    mkdir $ruta$nombre
#orden de copia total
    tar -czf $ruta$nombre/$nombre.tar.gz /var/ficheros_moodle/ 2> /dev/null tar -czf
    $ruta$nombre/$nombre/www.tar.gz /var/www 2> /dev/null
fi
```

# Copias de Seguridad

## Copias de Seguridad.- Sistemas Operativos Linux - Planificación

Ejemplo II de shellscript en la planificación de copias de seguridad :

```
#Inicio del volcado por la red
```

```
smbmount //192.168.3.30/share/copia/ /var/copiaSeguridad/destino -o password=clave
```

```
#Copio los ficheros
```

```
cp $ruta$nombre/* /var/copiaSeguridad/destino
```

```
# cierro la conexión
```

```
smbmount /var/copiaSeguridad/destino
```

```
#Fin de la copia de seguridad. #ANEXO: Línea para el fichero del demonio
```

```
crontab. #1 5 * * * /esteScript
```

# Copias de Seguridad

## Copias de Seguridad.- Sistemas Operativos Linux - Planificación

Ejemplo de shellscript en la planificación de copias de seguridad :

Cuando tengamos el *script* retocado a nuestro gusto le damos permisos de ejecución y lo copiamos a la carpeta */usr/bin*, por ejemplo:

```
chmod u+x backup-script
cp backup-script /usr/bin/
```

Después bastará con hacer que el *script* se ejecute cada día mediante cron, por ejemplo a las 3 de la mañana, para que no nos moleste mientras trabajamos con el PC.

**crontab -e**

escribiremos en la tabla:

```
03* * * /usr/bin/backup-script
```

# Copias de Seguridad

## Políticas de Copias de Seguridad.-

- + Las políticas de copias de seguridad deben definir el *tipo de copias y la periodicidad de las mismas, así como los soportes en las que se deben realizar y las ubicaciones de los centros de respaldo.*
- + Los **centros de respaldo** son las ubicaciones donde se guardar las copias de seguridad.

*Estos en la mayoría de las empresas pequeñas se encuentran muy cerca del centro de cálculo (CPD) o en la misma estancia, tanto por comodidad de los técnicos, que siempre tienen a mano el material, como por espacio, pero las empresas grandes que manejan grandes volúmenes de datos suelen ubicarlas lo suficientemente lejos como para que no se vean afectados por la misma catástrofe que provoque el percance en las instalaciones del centro de procesamiento.*

# Copias de Seguridad

## Políticas de Copias de Seguridad.-

- + Las ubicaciones de los centros de respaldo deben estar protegidas de la misma manera que los centros de procesamiento de datos, es decir, estarán protegidos los accesos para que solo pueda entrar el personal autorizado. Deberán estar protegidos tanto frente a los distintos accidentes o catástrofes naturales (incendios, inundaciones, etc.) como ante los posibles ataques software que estudiaremos más adelante.
  
- + Es frecuente encontrar las copias de seguridad almacenadas en **armarios ignífugos**. Gracias a este tipo de armarios podríamos proteger la información en caso de que se produzca un incendio.

# Copias de Seguridad

## Políticas de Copias de Seguridad.-

*Uno de los clásicos errores que se producen en las empresas es el mal etiquetado de las mismas. Una etiqueta correcta debería incluir la siguiente información:*

**Identificador de copia**, mediante esta cadena alfanumérica identificamos de manera unívoca cada una de las copias de seguridad realizadas. Facilita la búsqueda de las mismas.

**Tipo de copia**, debemos definir si la copia es incremental, diferencial o completa.

**Fecha** en la que se realizó la copia.

**Contenido**, siempre se incluirá el contenido -en clave- que almacena la copia de seguridad. En caso de querer recuperar un determinado archivo lo buscaremos sin necesidad de estar cargando cada una de las copias en el equipo. Hay que recordar que tanto el nombre de la copia como los datos almacenados en ella deben ir en clave para que en caso de encontrarse al alcance de intrusos, estos no sean capaces de descifrar la información almacenada en los mismos. Por tanto, tanto la información escrita en la etiqueta como la información almacenada en los soportes informáticos debería ir cifrada.

**Responsable**, debe figurar el técnico que realizó la copia de seguridad para poder pedirle que facilite las consultas o las peticiones de actualización y restauración de la misma.

# Copias de Seguridad

## Políticas de Copias de Seguridad.-

A continuación hemos diseñado una posible etiqueta para los soportes de los copias de seguridad:

COPIA DE SEGURIDAD					
Identificador de la copia					
Tipo de Copia	Completa	Incremental	Diferencial	Datos	Sistema
Fecha	(Año, Mes, Día)				
Datos	<ul style="list-style-type: none"><li>→ Se deberá utilizar la nomenclatura específica de la empresa, de forma que facilite la localización de archivos concretos y, en caso de que sea confidencial, un posible intruso no sea capaz de conocer la información grabada.</li></ul>				
Técnico	<ul style="list-style-type: none"><li>→ Nombre de la persona que realizó la copia de respaldo.</li></ul>				
Firma	<ul style="list-style-type: none"><li>→ Firma del responsable que realizó la copia.</li></ul>				

# Copias de Seguridad

## Políticas de Copias de Seguridad.-

Toda política de copias de seguridad debe contemplar los siguientes puntos:

- Determinar la persona o personas responsables encargadas de realizar y mantener las copias de seguridad.
- Debemos analizar los datos susceptibles de ser salvaguardados en copias de seguridad. Al realizar el análisis, debemos tener en cuenta la frecuencia con la que se modifica o actualiza la información.
- Debemos determinar el tipo de copia a realizar (completa, diferencial e incremental) en función de los datos a salvaguardar y de la periodicidad con la que se modifican.
- Debemos determinar la frecuencia con la que se realizarán las copias de seguridad
- Debemos determinar la ventana de backup (franja horaria en la que se deben realizar las copias de seguridad).
- Debemos determinar el tipo de soporte en el que se realizarán las copias de seguridad..
- Debemos determinar la ubicación de las copias de seguridad.

# Recuperación de Datos

En la recuperación de datos nos encontramos, por una parte, herramientas que permiten recuperar información de datos dañados, perdidos, borrados ..etc

*Windows: Recuva, ..etc*

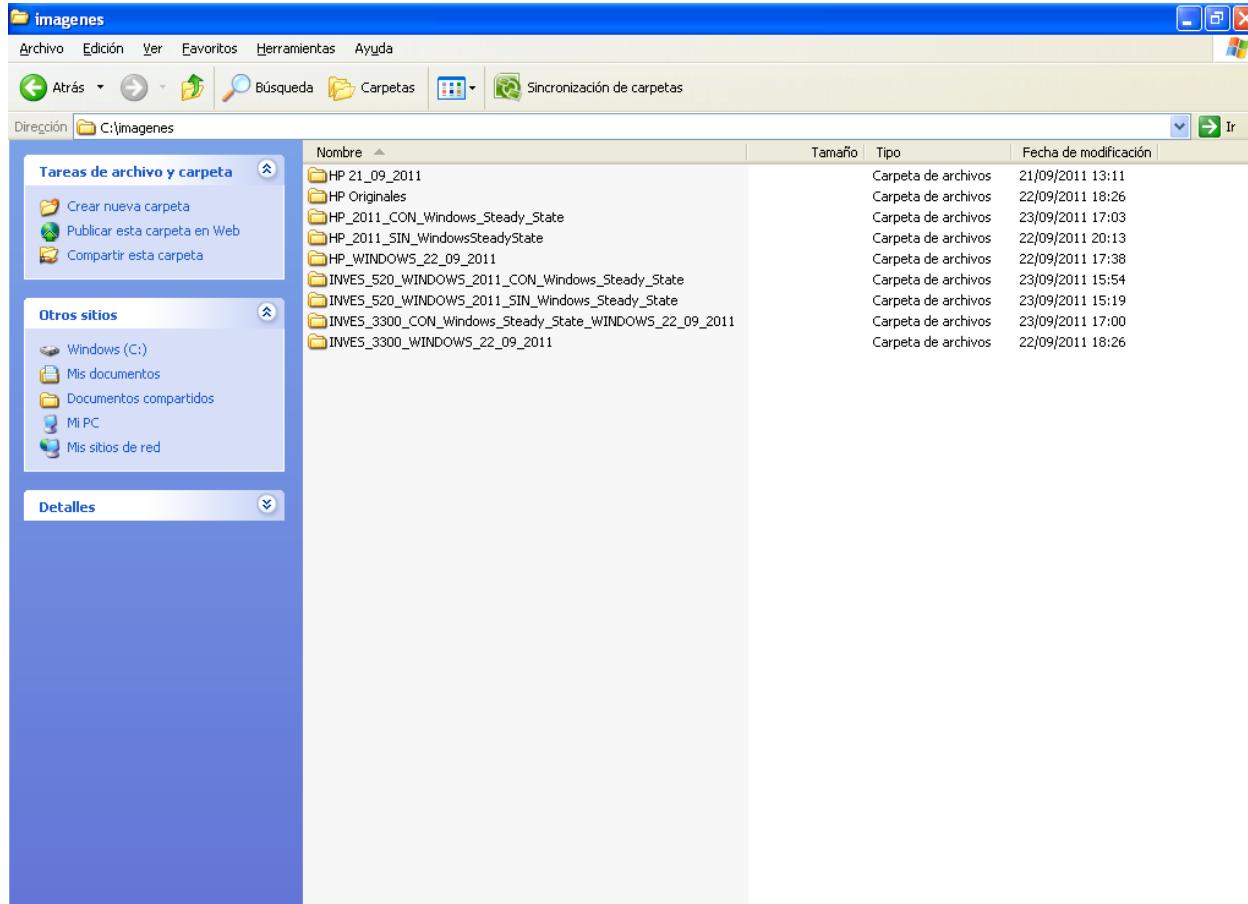
*GNU/Linux: TestDisk , Foresmost , PhotoRec , Scalpel .. etc*

Por otra parte nos encontramos herramientas con el propósito tanto de hacer copias de seguridad (imagen), como de recuperación de datos del sistema como: **Symantec Ghost**, **Acronis True Image**, ..etc.

*En el siguiente caso práctico muestro el proceso de crear una copia de seguridad o **imagen** y posterior recuperación de la misma utilizando para ello la herramienta **Symantec Ghost**.*

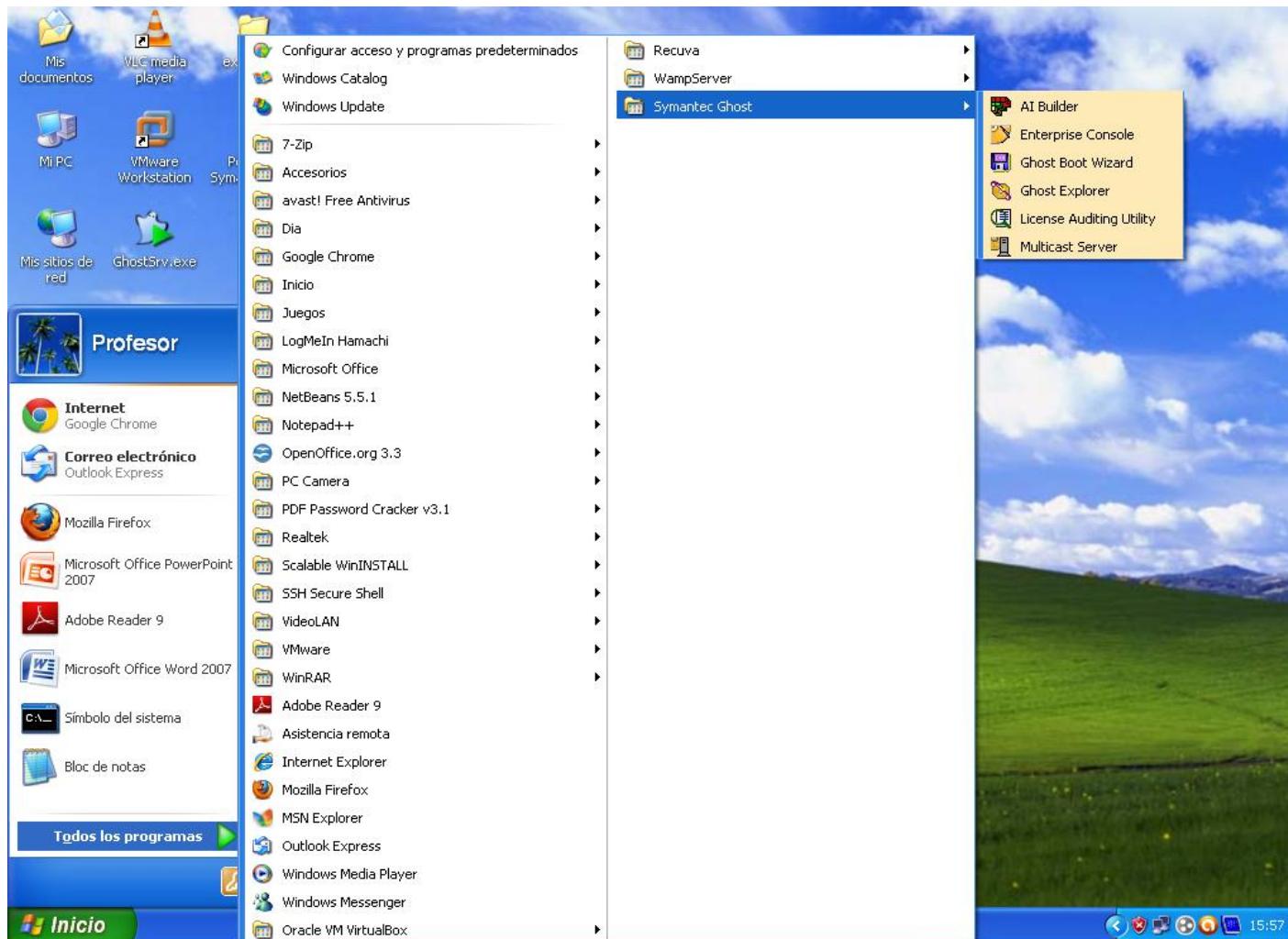
# Recuperación de Datos

Creación de una imagen del sistema con Symantec Ghost.-



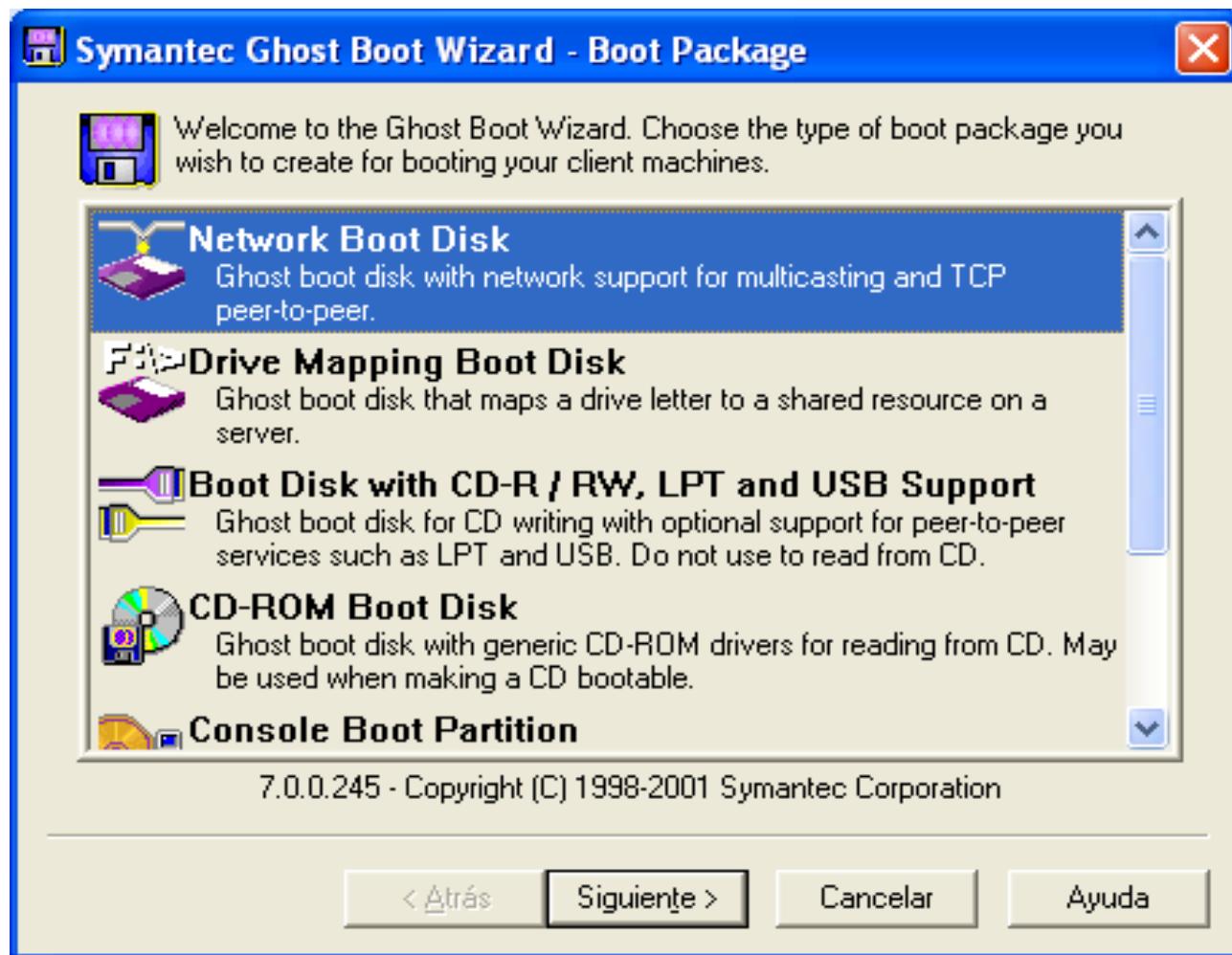
*Carpetas compartidas*

# Recuperación de Datos



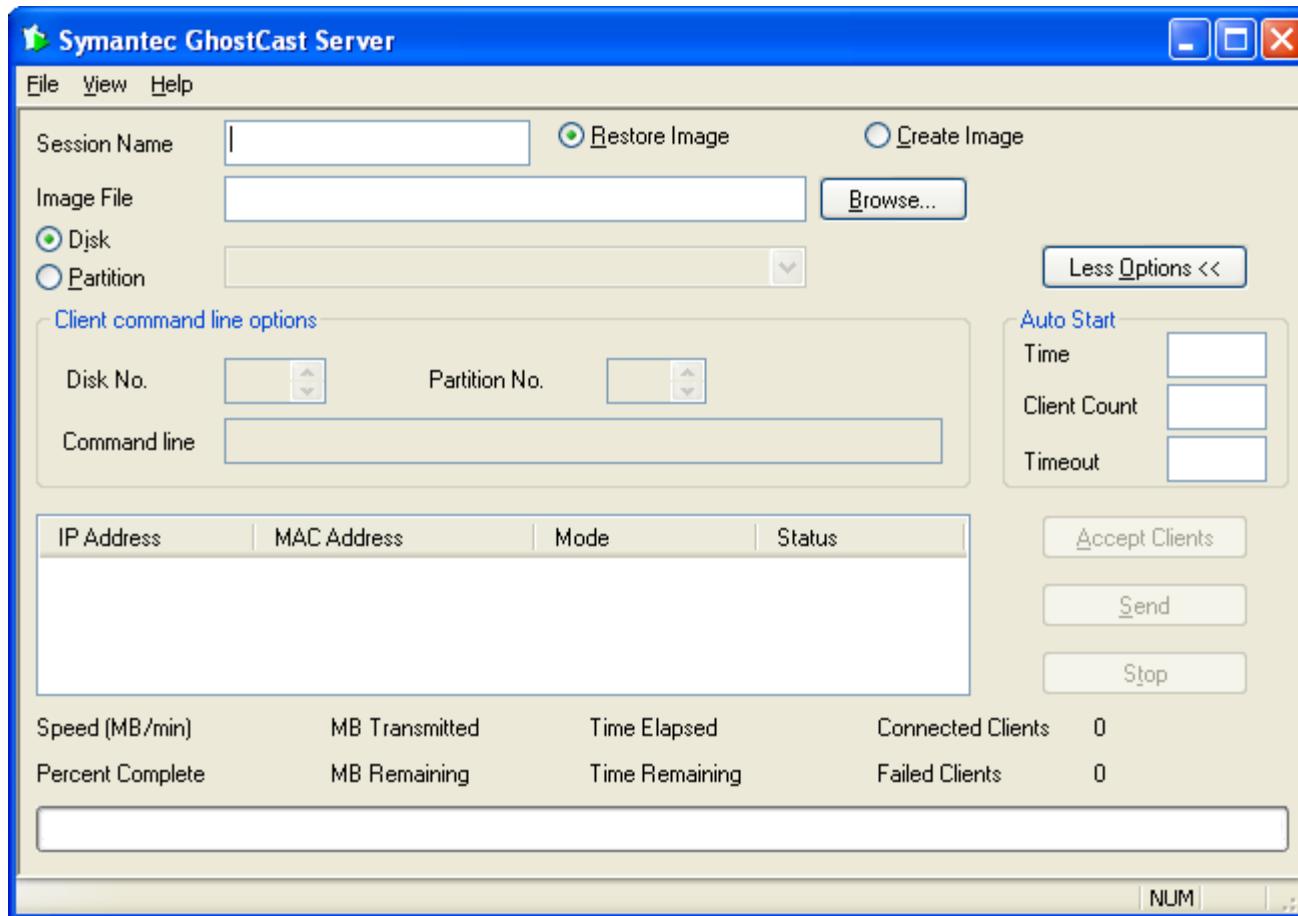
*Crear una ISO de arranque para el cliente*

# Recuperación de Datos



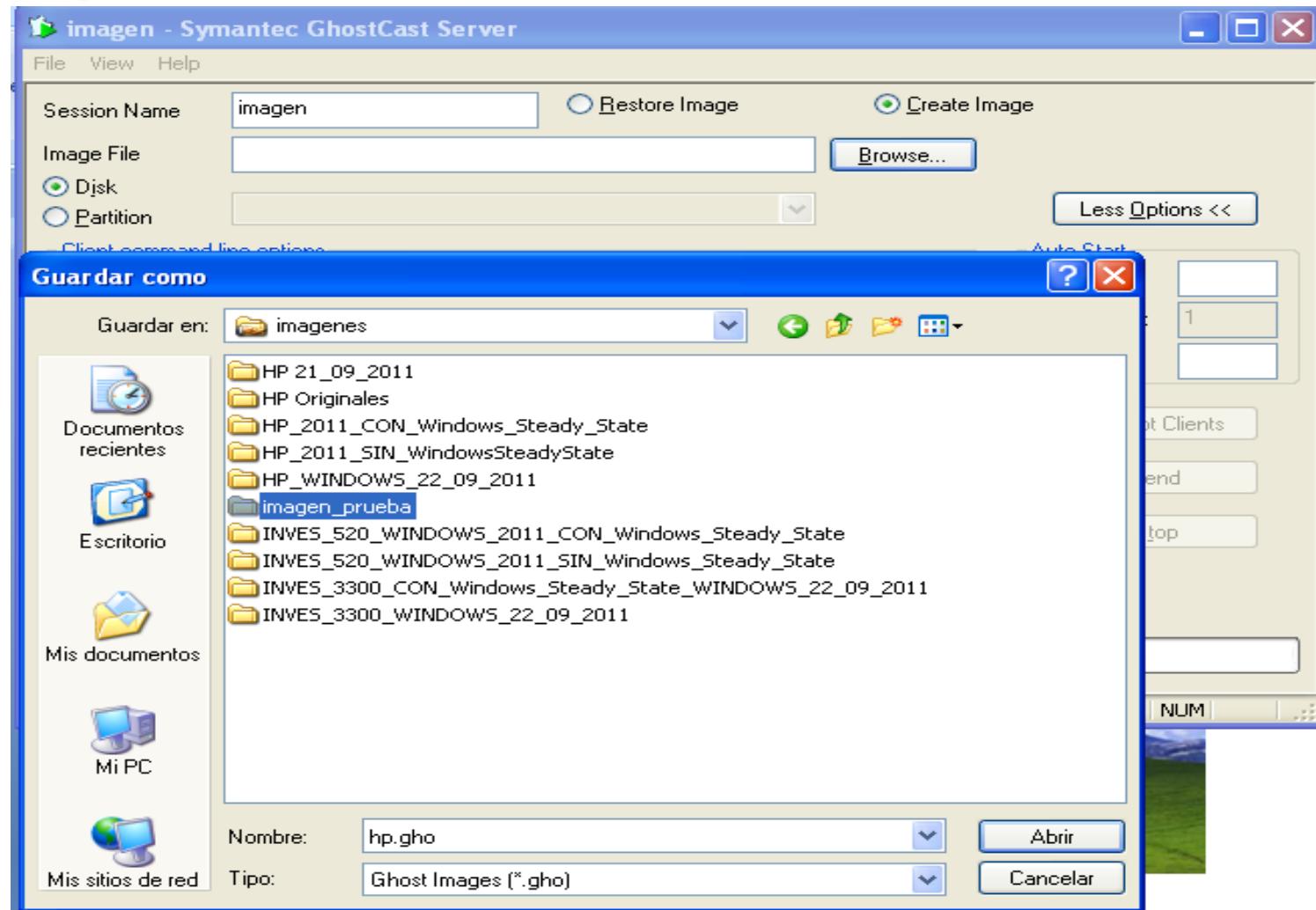
*Crear una ISO de arranque para el cliente*

# Recuperación de Datos



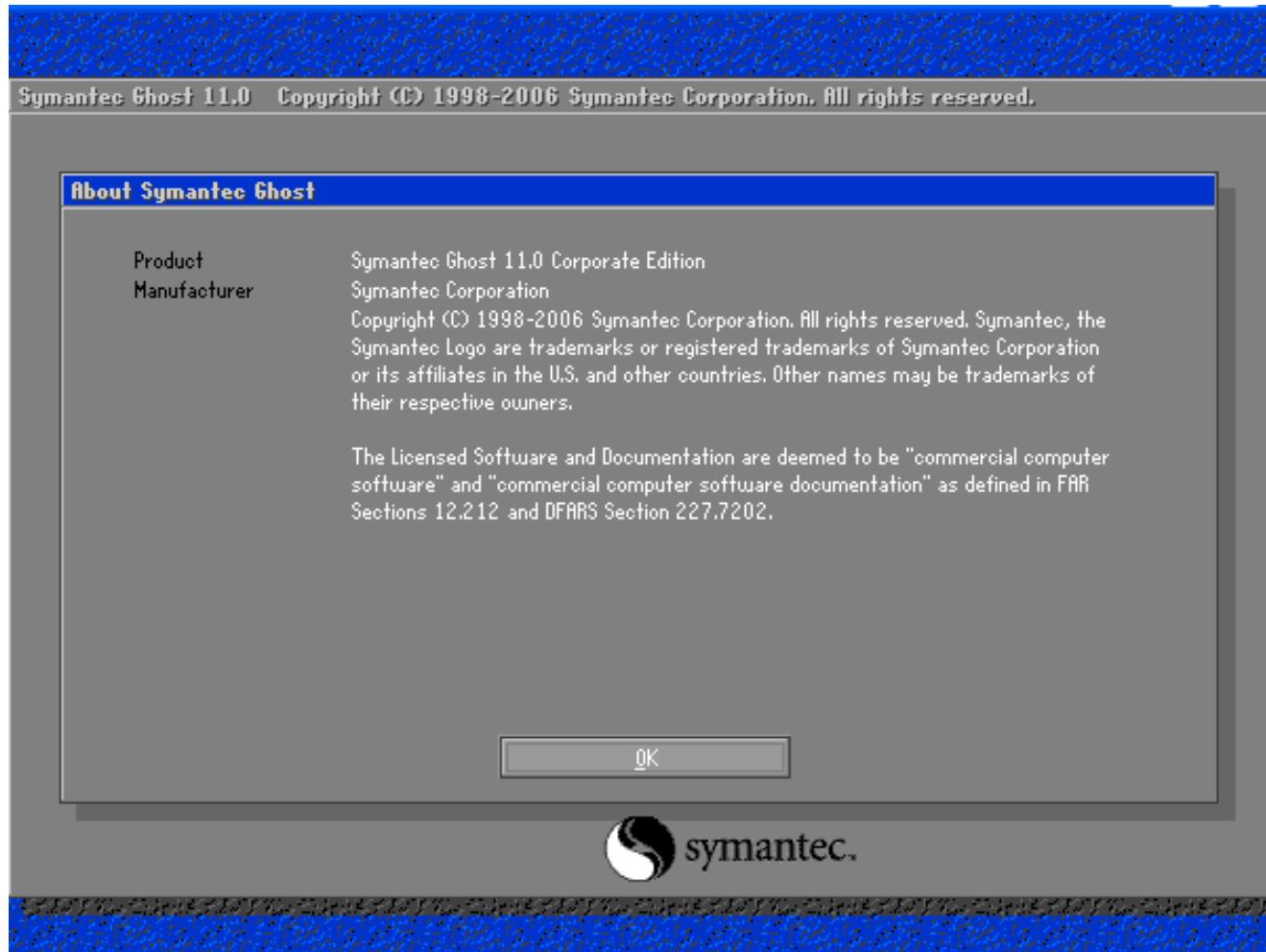
*Crear la imagen.- Ejecutar servidor Ghots*

# Recuperación de Datos



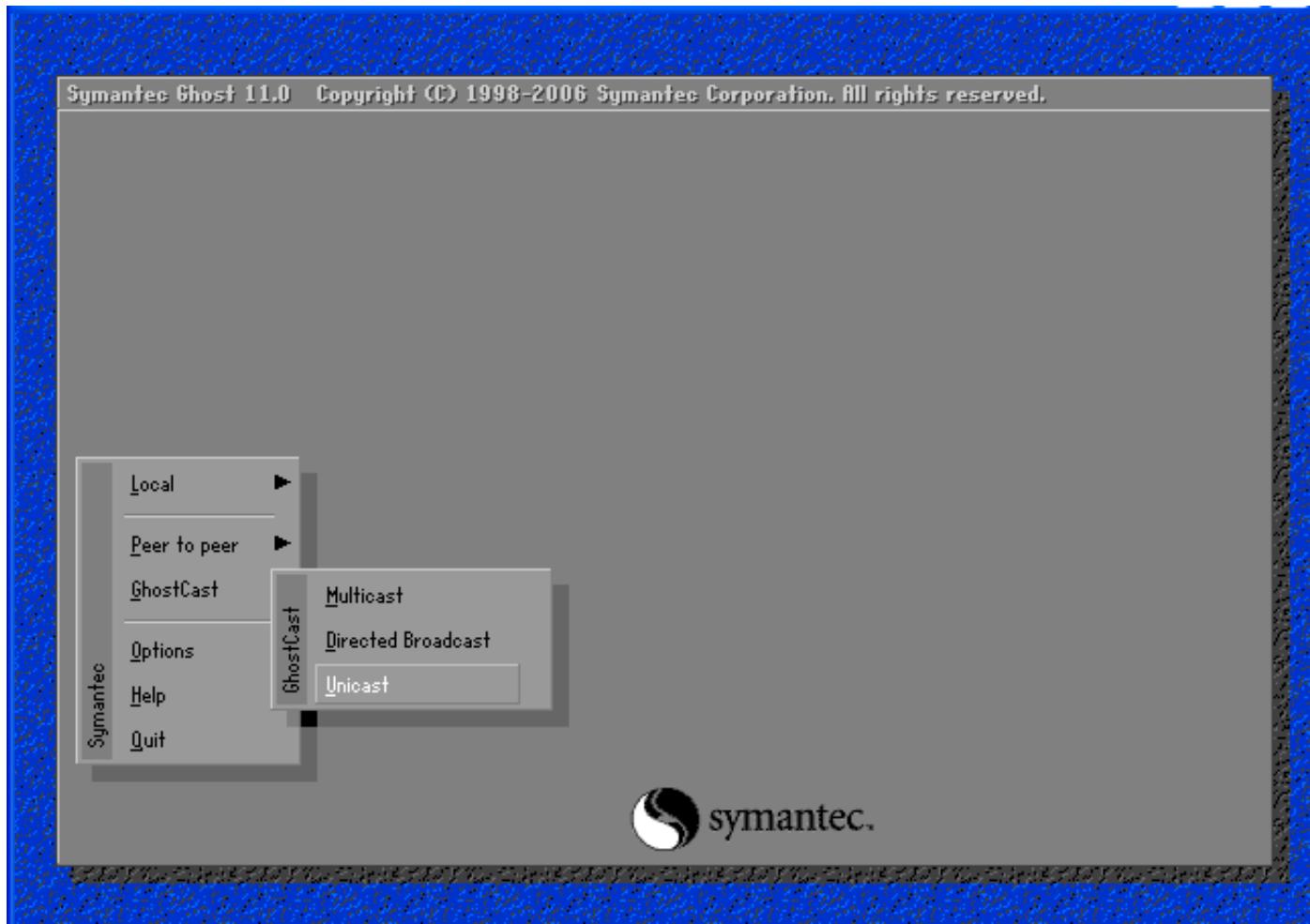
*Crear la imagen.- Ejecutar servidor Ghots*

# Recuperación de Datos

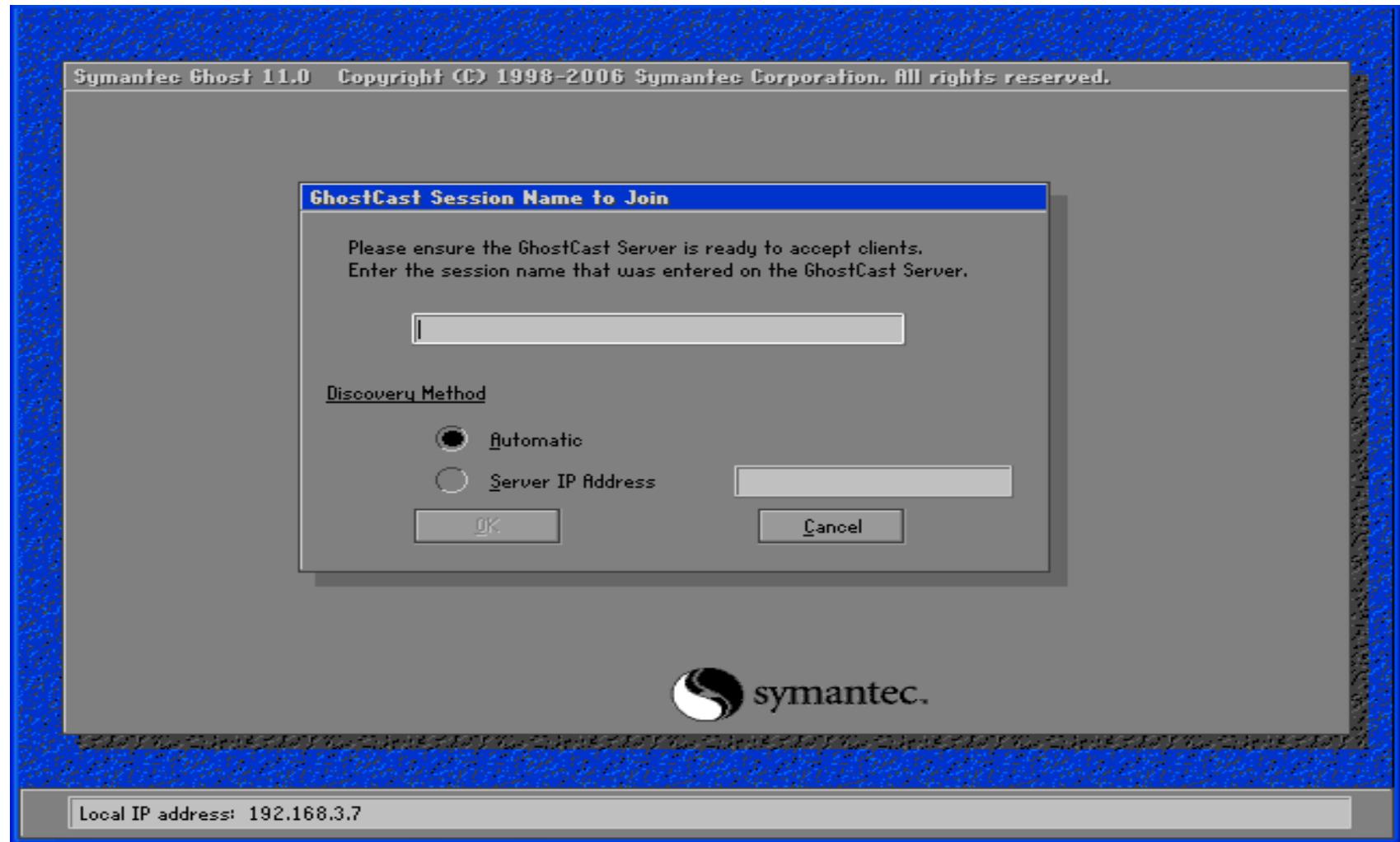


*CD de arranque en el equipo a realizar la imagen*

# Recuperación de Datos



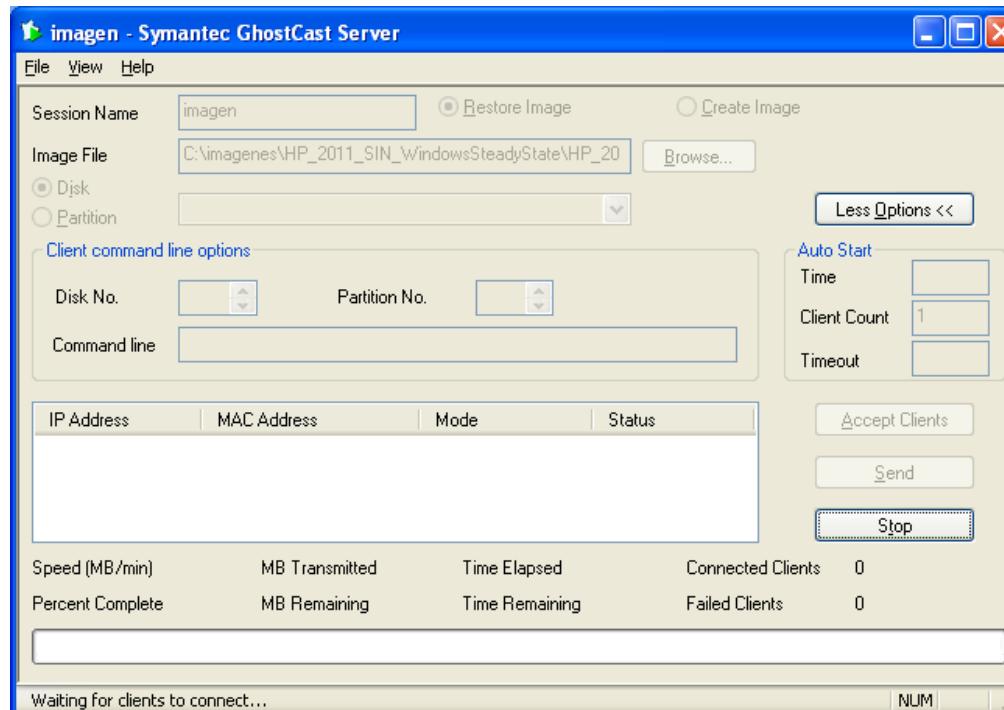
# Recuperación de Datos



# Recuperación de Datos

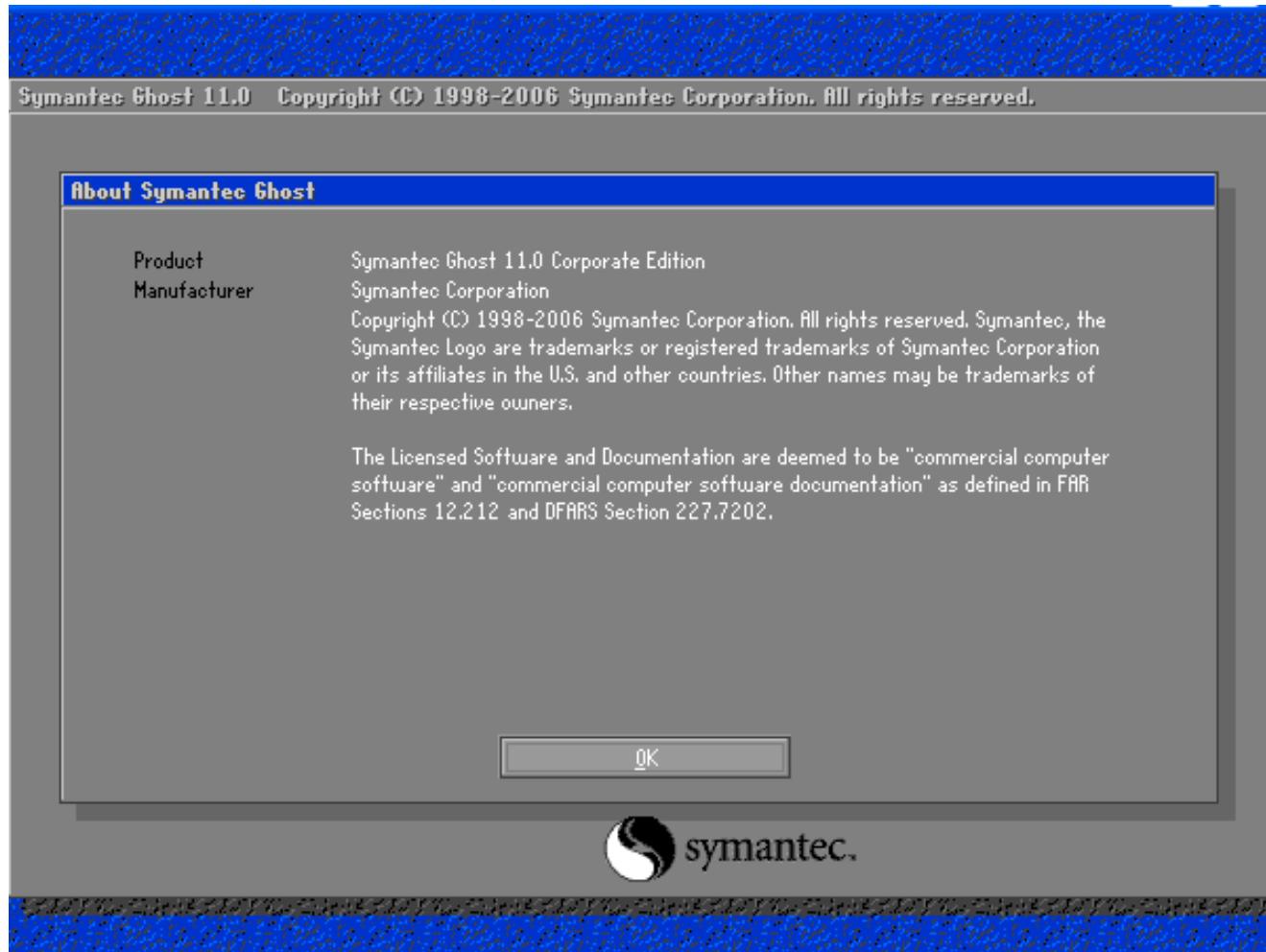
- Se introducirá el nombre de la sesión y a continuación aceptado las distintas ventanas se realizará la imagen, copiándose el resultado en la carpeta compartida del equipo donde se encuentra el Ghost portable.

Restauración de una imagen del sistema con Symantec Ghost.-



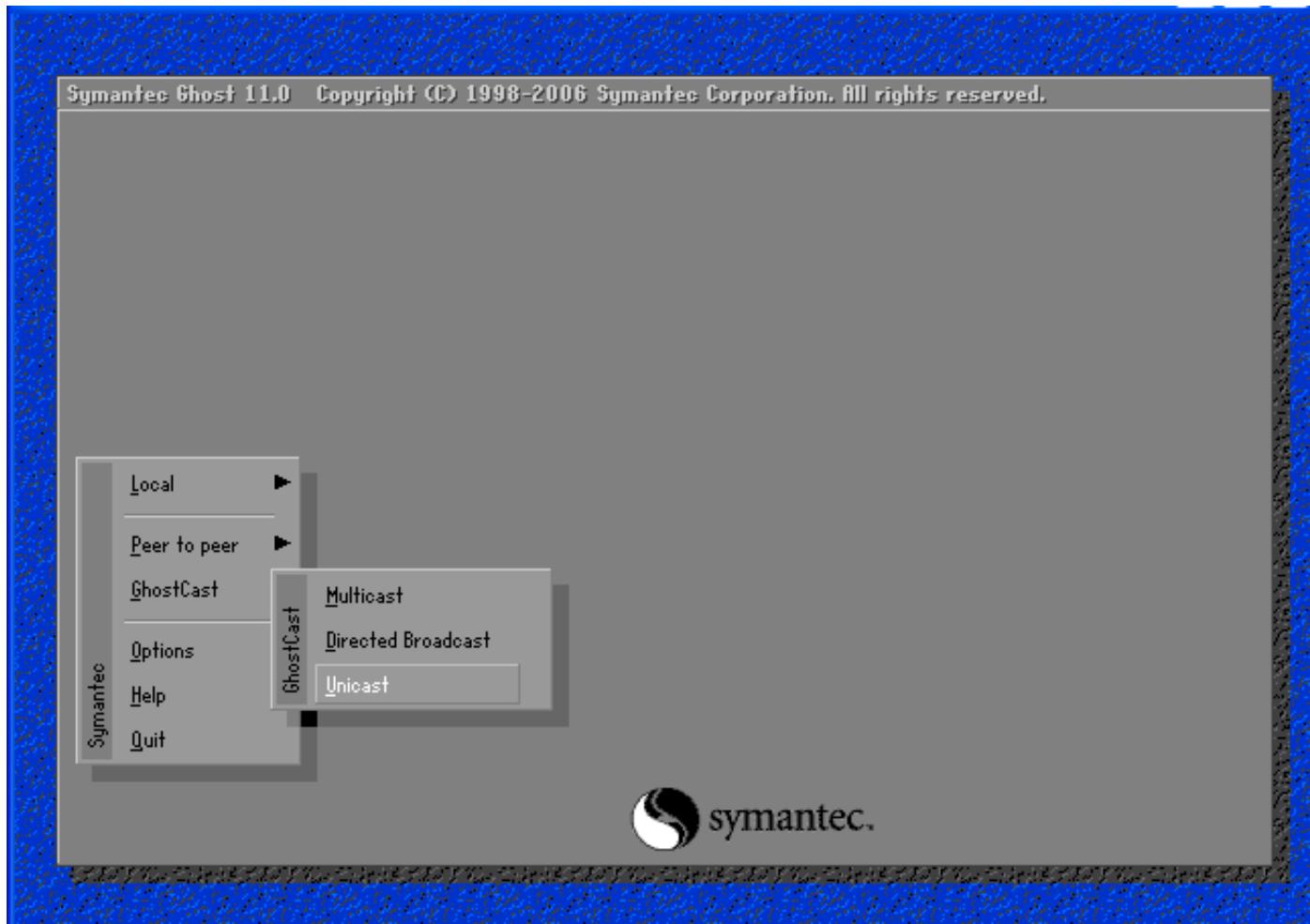
*Crear sesión para restaurar y esperamos un cliente – equipo a restaurar-*

# Recuperación de Datos

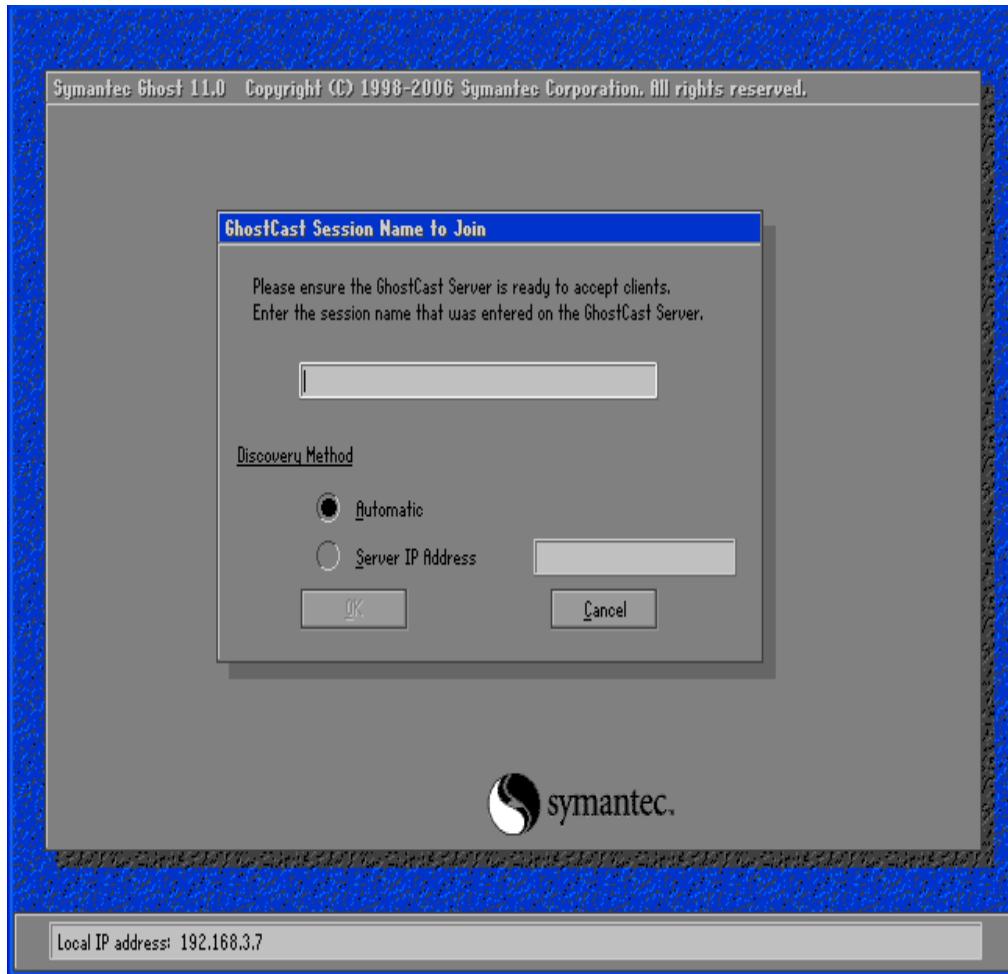


*CD de arranque en el equipo a restaurar*

# Recuperación de Datos



# Recuperación de Datos



- + Se introducirá el nombre de la sesión y a continuación aceptado las distintas ventanas , donde nos avisara de la perdida de los datos actuales, produciendose la restauración del sistema.

# Medidas de Actuación

## Ubicación y protección física.-

- El primer paso para establecer la seguridad de un servidor o un equipo es decidir adecuadamente dónde vamos a instalarlo. Esta decisión puede parecer superflua, pero nada más lejos de la realidad: **resulta vital para el mantenimiento y protección de nuestros sistemas.**
- Los planes de seguridad física se basan en proteger el hardware de los posibles desastres naturales, de incendios, inundaciones, sobrecargas eléctricas, robos y otra serie de amenazas.
- Se trata, por tanto, de aplicar barreras físicas y procedimientos de control, como medidas de prevención y contramedidas para proteger los recursos y la información, tanto para mantener la seguridad dentro y alrededor del Centro de Cálculo, como los mecanismos de acceso remoto a él o desde él.
- Veremos algunos de los mecanismos de seguridad física de los que hemos hablado en la Unidad 2, relativa a amenazas y mecanismos de defensa de seguridad.

# Medidas de Actuación

## Ubicación y protección física.-

Amenazas	Mecanismos de defensa
Incendios	<ul style="list-style-type: none"><li>◆ El mobiliario de los centros de cálculo debe ser ignífugo.</li><li>◆ Evitar la localización del centro de procesamiento de datos cerca de zonas donde se manejen o almacenen sustancias inflamables o explosivos.</li><li>◆ Deben existir sistemas antiincendios, detectores de humo, rociadores de gas, extintores... para sofocar el incendio en el menor tiempo posible y así evitar que se propague ocasionando numerosas pérdidas materiales.</li></ul>
Inundaciones	<ul style="list-style-type: none"><li>◆ Evitar la ubicación de los centros de cálculo en las plantas bajas de los edificios para protegerse de la entrada de aguas superficiales.</li><li>◆ Impermeabilizar las paredes y techos del Centro de Cálculo. Sellar las puertas para evitar la entrada de agua proveniente de las plantas superiores.</li></ul>
Robos	<ul style="list-style-type: none"><li>◆ Proteger los centros de cálculo mediante puertas con medidas biométricas, cámaras de seguridad, vigilantes jurados..., con todas estas medidas pretendemos evitar la entrada de personal no autorizado.</li></ul>
Señales Electromagnéticas	<ul style="list-style-type: none"><li>◆ Evitar la ubicación de los centros de cálculo próximos a lugares con gran radiación de señales electromagnéticas, pues pueden interferir en el correcto funcionamiento de los equipos informáticos del cableado de red.</li><li>◆ En caso de no poder evitar la ubicación en zonas con grandes emisiones de este tipo de señales deberemos proteger el centro frente de dichas emisiones mediante el uso de filtros o de cableado especial, o si es posible, utilizar fibra óptica, que no es sensible a este tipo de interferencias.</li></ul>
Apagones	<ul style="list-style-type: none"><li>◆ Para evitar los apagones colocaremos Sistemas de Alimentación Ininterrumpida (SAI), que proporcionan corriente eléctrica durante un periodo de tiempo suficiente.</li></ul>
Sobrecargas Eléctricas	<ul style="list-style-type: none"><li>◆ Además de proporcionar alimentación, los SAI profesionales incorporan filtros para evitar picos de tensión, es decir, estabilizan la señal eléctrica.</li></ul>
Desastres Naturales	<ul style="list-style-type: none"><li>◆ Estando en continuo contacto con el Instituto Geográfico Nacional y de Meteorología, organismos que informan sobre los movimientos sísmicos y meteorológicos en España.</li></ul>

# Medidas de Actuación

## Ubicación y protección física.-

- Cada sistema informático es único. Por ejemplo, en la siguiente figura se puede ver la vista parcial de un Centro de Procesamiento de Datos (CPD) de una organización grande, pero en pequeñas empresas u organizaciones, el CPD podría estar compuesto solo por uno de estos módulos o por un servidor. Cuando hablamos del plan de seguridad física no podemos pensar que existe un plan de seguridad general aplicable a cualquier tipo de instalación.



- En esta unidad nos centraremos en las pautas de aplicación general, teniendo en cuenta que estas deben personalizarse para cada empresa y cada edificio.

# Medidas de Actuación

## Ubicación y protección física.- *Factores para elegir la ubicación*

■ Cuando hay que instalar un Centro de Cálculo o Procesamiento de Datos es necesario fijarse en varios factores. En concreto, se elegirá la ubicación en función de la **disponibilidad física** y la facilidad para modificar aquellos aspectos que vayan a hacer que la instalación sea más segura. Existen una serie de factores que dependen de las instalaciones propiamente dichas, como son:

**El edificio.** Debemos evaluar aspectos como el espacio del que se dispone, cómo es el acceso de equipos y personal, y qué características tienen las instalaciones de suministro electrónico, acondicionamiento térmico, etc. Igualmente, hemos de atender a cuestiones de índole física de los espacios disponibles, la iluminación, etc.

**Tratamiento acústico.** En general, se ha de tener en cuenta que habrá equipos, como los de aire acondicionado, necesarios para refrigerar los servidores, que son bastante ruidosos. Deben instalarse en entornos donde el ruido y la vibración estén amortiguados.

# Medidas de Actuación

## Ubicación y protección física.- *Factores para elegir la ubicación*

**Seguridad física del edificio.** Se estudiará el sistema contra incendios, la protección contra inundaciones y otros peligros naturales que puedan afectar a la instalación.

**Suministro eléctrico propio del CPD.** La alimentación de los equipos de un centro de procesamiento de datos tiene que tener unas condiciones especiales, ya que no puede estar sujeta a las fluctuaciones o picos de la red eléctrica que pueda sufrir el resto del edificio. No suele ser posible disponer de toda una red de suministro eléctrico propio, pero siempre es conveniente utilizar un sistema independiente del resto de la instalación y elementos de protección y seguridad específicos, *como sistemas de alimentación ininterrumpida*: equipos electrógenos, baterías, etc.

# Medidas de Actuación

## Ubicación y protección física.- *¿Dónde se debe instalar el CPD ?*

Atendiendo solo a estos factores ya podemos obtener las primeras conclusiones para **instalar el CPD** en una ubicación de características idóneas. Así pues, siempre que podemos, tendremos en cuenta que:

- Deben evitarse áreas con fuentes de interferencia de radiofrecuencia, tales como transmisores de radio y estaciones de TV.
- El CPD no debe estar contiguo a maquinaria pesada o almacenes con gas inflamable o nocivo.
- El espacio deberá estar protegido ante entornos peligrosos. especialmente inundaciones.

**Se buscará descartar:**

- Zonas cercanas a paredes exteriores, planta baja o salas de espera, ya que son más propensas al vandalismo o los sabotajes.*
- Sótanos, que pueden dar problemas de inundaciones debido a cañerías principales, sumideros o depósitos de agua.*
- Última planta, evitando desastres aéreos, etc.*
- Encima de garajes de vehículos de motor, donde el fuego se puede originar y extender más fácilmente.*

*Según esto, la ubicación más conveniente se sitúa en las plantas intermedias de un edificio o en ubicaciones centrales en entornos empresariales.*

# Medidas de Actuación

## Ubicación y protección física.- *Control de Acceso*

■ De modo complementario a la correcta elección de la ubicación del CPD es necesario un férreo control de acceso al mismo. Dependiendo del tipo de instalación y de la inversión económica que se realice se dispondrá de distintos sistemas de seguridad, como los siguientes:

- **Servicio de vigilancia**, donde el acceso es controlado por personal de seguridad que comprueban la identificación de todo aquel que quiera acceder a una ubicación. En general, suele utilizarse en el control de acceso al edificio o al emplazamiento y se complementa con otros sistemas en el acceso directo al CPD.
- **Detectores de metales y escáneres de control de pertenencias**, que permiten “revisar” a las personas, evitando su acceso a las instalaciones con instrumentos potencialmente peligrosos o armas.
- **Utilización de sistemas biométricos**, basados en identificar características únicas de las personas cuyo acceso esté autorizado, como sus huellas digitalizadas o su iris.
- **Protección electrónica**, basada en el uso de sensores conectados a centrales de alarma que reaccionan ante la emisión de distintas señales. Cuando un sensor detecta un riesgo, informa a la central que procesa la información y responde según proceda, por ejemplo, emitiendo señales sonoras que alerten de la situación.

# Medidas de Actuación

## Ubicación y protección física.- *Sistemas de climatización y protección en el CPD*

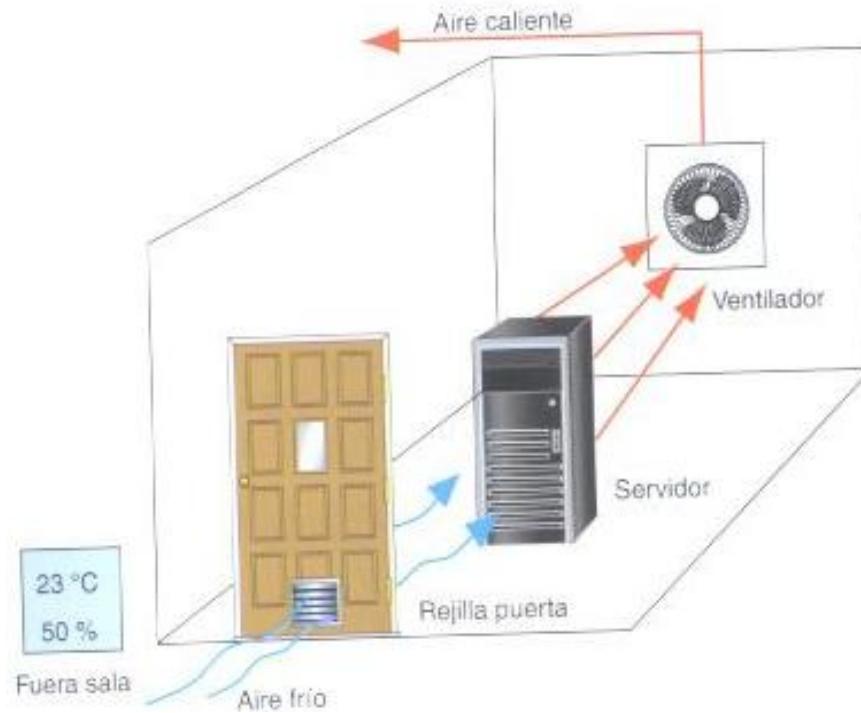
Además de instalar el CPD en la mejor localización posible y un control de acceso al mismo, es imprescindible que se instalen en su interior, junto con los equipos propios de procesamiento de datos, *sistemas de climatización, de protección contra incendios (PCI)* apropiados.

Los equipos de un centro de proceso de datos disipan mucha energía calorífica y hay que refrigerarlos adecuadamente para mantener las condiciones interiores de temperatura y humedad estables, ya que altas temperaturas podrían dañar estos equipos. La decisión sobre qué sistemas de climatización han de instalarse depende de las características de cada CPD, pero hay un hecho que siempre ha de tenerse en cuenta: no se trata de climatizar el cuarto sino de refrigerar el equipo. Por ello debemos situar el servidor o rack a la altura adecuada para que le alcance la circulación de aire, y de modo que el aire frío de la máquina se dirija a la parte del equipo que absorbe aire, no a la que la expulsa.

# Medidas de Actuación

**Ubicación y protección física.-** *Sistemas de climatización y protección en el CPD*

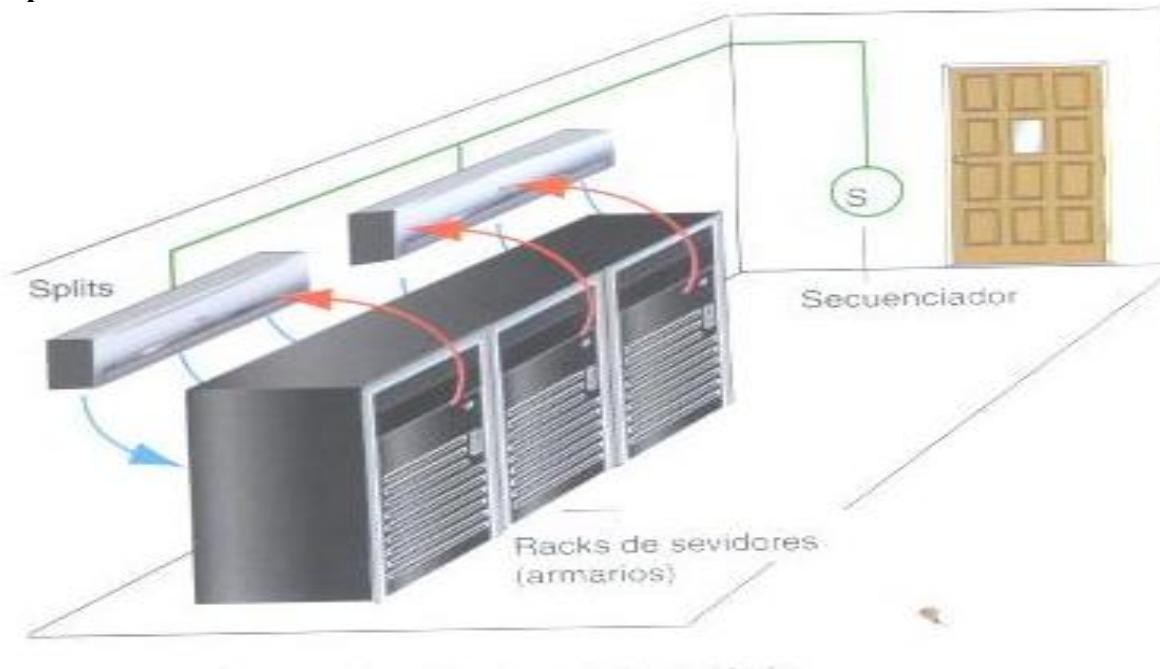
Podemos, por ejemplo, utilizar un ventilador que expulsa el aire caliente al exterior para refrigerar un servidor como el que ves en la siguiente figura.



# Medidas de Actuación

## Ubicación y protección física.- *Sistemas de climatización y protección en el CPD*

Para un CPD que tenga varios racks, podemos optar por el uso de equipos murales, o equipos de techo. En la siguiente figura puedes verse este tipo de instalación, donde también se ha instalado un servidor en una zona de temperatura característica. Este secuenciador proporciona un sistema de seguridad adicional, ya que alterna el uso de cada uno de los splits instalados, y, en caso de que suba la temperatura, ambos equipos se pondrán en funcionamiento para enfriar el CPD.



# Medidas de Actuación

## Ubicación y protección física.- *Sistemas de climatización y protección en el CPD*

- + Los sistemas contra incendios son otro de los factores clave en un CPD. No es tu misión instalarlos, pero sí debes conocer su funcionamiento básico ya que de ello puede depender incluso tu propia seguridad. *Es habitual utilizar dos tipos:*
  - ❑ **Sistema de detección**, como el sistema de detección precoz, que realiza análisis continuos del aire, de modo que puede observar un cambio de composición en el mismo, detectando un incendio incluso antes de que se produzca el fuego y activando el sistema de desplazamiento de oxígeno.
  - ❑ **Sistema de desplazamiento de oxígeno**. Este tipo de sistemas que reducen la concentración de oxígeno, extinguiendo así el fuego, de modo que no se utiliza agua, que puede dañar los equipos electrónicos. Dado que se produce un desplazamiento de oxígeno, es muy importante que el personal humano siga las normas de evacuación de la ubicación, ya que su activación podría perjudicar su integridad física.

# Medidas de Actuación

## Ubicación y protección física.- *Recuperación en caso de desastre.-*

- Nuestro objetivo debe ser siempre evitar daños en el CPD, pero hay que ser realista y tener preparado un plan de contingencia que debe ponerse en marcha en caso de desastre.
- Una opción que ha de tenerse en cuenta es tener un **centro de backup independiente**, de modo que aunque los equipos del CPD queden fuera de servicio por una avería muy grave, la organización podrá seguir realizando su actividad con cierta normalidad.
- Dentro de los planes de contingencia debemos tener en cuenta la realización de **sistemas redundantes, como los sistemas RAID y el uso de copias de seguridad.**
- En caso de que se produzca un desastre, el primer paso es que se reúna el comité de crisis para evaluar los daños. Si se decide poner en marcha el plan de contingencia, es importante que los trabajos comiencen por recuperar las bases de datos y ficheros esenciales, así como desviar las comunicaciones más críticas al centro alternativo, desde donde se comenzará a operar en las áreas que sean prioritarias, ya que de no hacerlo las consecuencias podrían ser desastrosas.

# Medidas de Actuación

## Sistemas de alimentación ininterrumpida.- *Definición de SAI*

Ningún equipo informático, por sofisticado que sea, está exento de sufrir un corte de luz y apagarse. Es por ello que es necesario, especialmente cuando se están procesando datos o dando servicios de alojamiento web u otros, utilizar **sistemas auxiliares de alimentación**.

*Un SAI o sistema de alimentación ininterrumpida es un dispositivo electrónico que permite proteger a los equipos frente a los picos o caídas de tensión. De esta manera se dispone de una mayor estabilidad frente a los cambios del suministro eléctrico y de una fuente de alimentación auxiliar cuando se produce un corte de luz.*

*Este tipo de sistemas nacieron originalmente con el objetivo de proteger el trabajo que se estaba realizando en el momento en que se producía un apagón. La idea consistía en proporcionar al usuario del equipo el tiempo suficiente para guardar la información y apagar correctamente los equipos cuando se producía un corte en el suministro eléctrico, aunque posteriormente se le ha agregado capacidad para poder continuar trabajando cierto tiempo, aunque no se disponga de suministro.*

# Medidas de Actuación

## Sistemas de alimentación ininterrumpida.- *Definición de SAI*

Las características de los SAI dependen de cada modelo en concreto, pero en la siguiente tabla se presenta un resumen de sus funcionalidades:

Características	Descripción
Alimentación de ordenadores	Se puede conectar de uno a varios equipos al mismo SAI.
Tiempo extra de trabajo	Permiten seguir trabajando con el ordenador de 15 a 270 minutos cuando se produce un corte en el suministro eléctrico.
Alimentación de otros equipos	No están diseñados para conectar dispositivos de alto consumo de energía (como grandes impresoras láser o plotters).
Regulador de voltaje	Integrado en algunos modelos para evitar que los picos de tensión que se producen en la línea afecten a la alimentación de los equipos.
Otros conectores	Algunos incorporan conectores para conectar el módem, router u otros dispositivos imprescindibles en la comunicación y protegerlos.

# Medidas de Actuación

## Sistemas de alimentación ininterrumpida.- *Tipos de SAI*

En general, podemos identificar dos tipos de SAI, en función de su forma de trabajar:

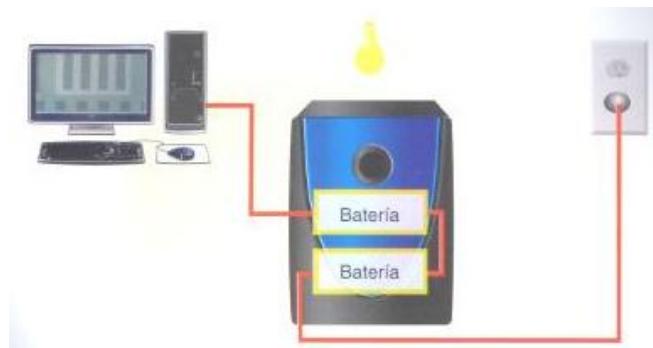
- **Sistemas de alimentación en estado de espera** o Stand-by Power Systems (SPS). Este tipo de SAI activa la alimentación automáticamente desde baterías, cuando detecta un fallo en el suministro eléctrico.
- **SAI en línea (on-line)**, que alimenta el ordenador de modo continuo, aunque no exista un problema en el suministro eléctrico, y al mismo tiempo recarga su batería. Este dispositivo tiene la ventaja de que ofrece una tensión de alimentación constante, ya que filtra los picos de la señal eléctrica que pudiesen dañar el ordenador, si bien el tiempo extra de trabajo que ofrece es menor que el de los SPS.



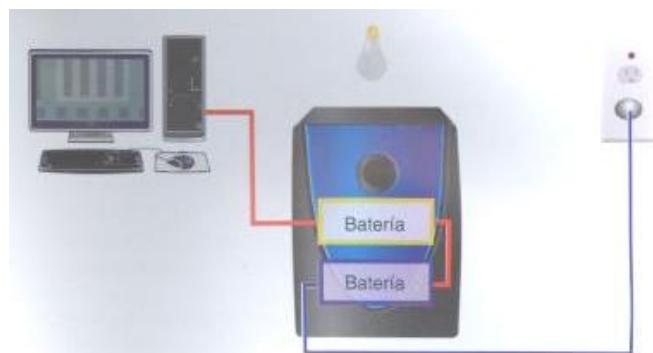
# Medidas de Actuación

## Sistemas de alimentación ininterrumpida.- *Modo de funcionamiento.-*

Como ya hemos dicho, un SAI es un dispositivo auxiliar que alimenta un ordenador, bien de modo continuo o bien quedando a la espera hasta que es necesario (cuando hay un corte de luz). Las siguientes figuras ilustran este funcionamiento.



En esta figura podemos ver una representación de un SAI en línea, en una situación normal donde hay suministro eléctrico. El SAI está conectado, por un lado, a un enchufe de la red, a través del cual recibe la corriente con la que va cargando sus baterías, y por otro se conecta al equipo o equipos a los que vaya a proteger.



En esta figura podemos ver cuál es la situación cuando se produce un corte de luz, y la alimentación del ordenador depende únicamente de las baterías internas del SAI. Disponemos de alimentación el tiempo que estas baterías tarden en descargarse.

# Medidas de Actuación

## Utilización de Sistemas Biométricos.-

Los **sistemas biométricos** consisten en la utilización de sistemas automáticos para la clasificación / reconocimiento de rasgos personales en identificación.

Los sistemas biométricos se clasifican en los siguientes tipos:

**Rasgos fisiológicos:** huellas dactilares, geometría de la mano/dedo, iris, ADN, etc.

**Rasgos del comportamiento:** voz, firma, modo de teclear, modo de andar, etc.



Imágenes de huellas y caras sintéticas generadas con los programas SFINGE y FACES

# **Medidas de Actuación**

## **Utilización de Sistemas Biométricos.-**

Las características que tienen los sistemas biométricos son las siguientes:

**Rendimiento:** precisión en el proceso de identificación.

**Aceptabilidad:** grado de aceptación / rechazo personal y social del sistema biométrico.

**Evitabilidad:** capacidad de eludir el sistema mediante procedimientos fraudulentos.

Las ventajas que ofrecen estos sistemas son las siguientes:

*No pueden ser sustraídos, perdidos, olvidados o descolocados.*

*Representan una manifestación tangible de lo que uno es.*

El principal riesgo que se deriva de los sistemas biométricos es la **suplantación** de identidad mediante la **imitación** (voz, cara) o la **reproducción** (huella, iris) del rasgo a reconocer.

# Prácticas/Actividades



6 Herramientas Sw



# Prácticas/Actividades

Formato de entrega:

*Documento en formato XHTML 1.0, por grupos, con enlaces a elementos multimedia, que resuelvan las cuestiones planteadas. El grupo deberá realizar la actividad 1,2. Dos actividades de entre la 3-11 y una actividad de entre la 12-16*

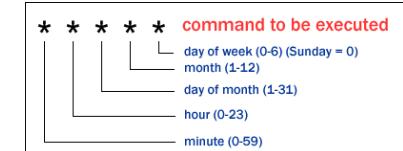
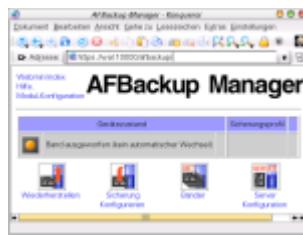


# Prácticas/Actividades

## Actividad 1.- Búsqueda de Información



*Búsqueda de información con el fin de elaborar un diccionario de herramientas mencionadas en este tema, y de aquellos que resulten de la búsqueda de información, en el que se describan los siguientes elementos: descripción, http de descarga y http de tutorial/manual de uso, http de ejemplo de aplicación/uso, otros aspectos.*



# Prácticas/Actividades

## Actividad 1.- Búsqueda de Información



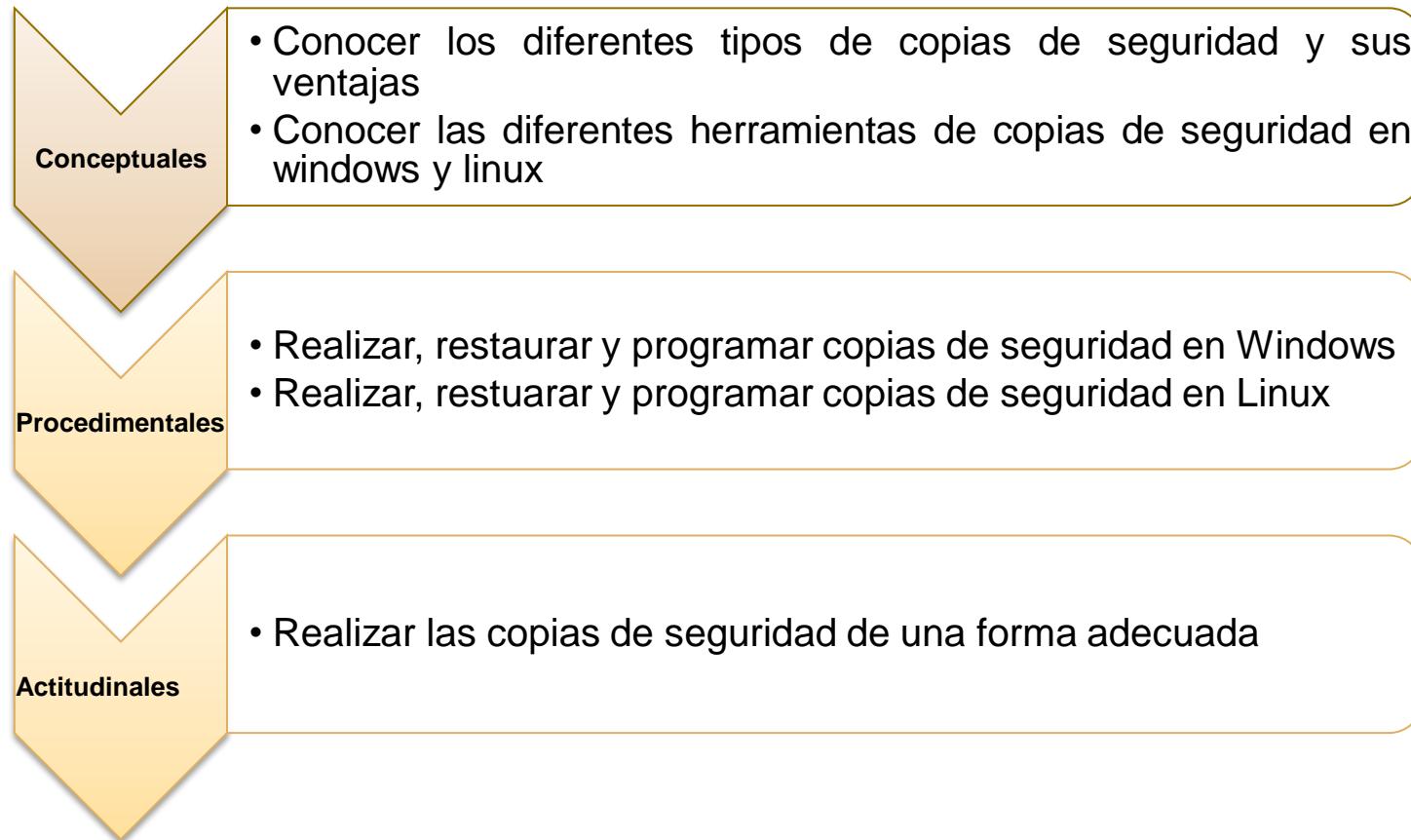
Herramientas  
Sw

*Analiza y describe los sistemas biométricos que actualmente se están utilizando, así como los estudios de implantación de nuevas tecnologías respecto a este campo.*



# Prácticas/Actividades

Al finalizar este bloque se pretende que el alumnado manifieste las siguientes competencias:



# Prácticas/Actividades



Copias de seguridad

## Actividad 2.-

Analiza el asistente/herramienta de copias de seguridad con el programador de tareas, restauración de las copias de seguridad, puntos de restauración, disco de reparación y reinicio del sistema en modo reparación/restauración en un entorno Windows 2003 o windows 2008 server. Realiza el ejemplo pertinente que muestre la utilización de dicha herramienta.

## Actividad 3.-

Analiza, configura y prueba la herramienta de copia de seguridad Cobian Backup.

## Actividad 4.-

Analiza, configura y prueba la herramienta de copia de seguridad Backup4all.

# Prácticas/Actividades



Copias de seguridad

## Actividad 5.-

Configura y automatiza la copia de seguridad en un entorno linux de una estructura de directorios. Utiliza para ello el comando tar y el servicio crond – consideramos que la copia se realiza en el mismo equipo-. *Considerar distintos programas de copia, cada uno de ellos con sus correspondientes momentos.*

## Actividad 6.-

Configura y automatiza la copia de seguridad en un entorno linux de una estructura de directorios, considerando que la copia se realiza en otro equipo linux/windows (host remote).

## Actividad 7.-

Analizar, implementa, configura en un entorno Windows la herramienta rsync.

## Actividad 8.-

Analizar, implementa, configura en un entorno linux la herramienta rsync.

## Actividad 9.-

Configura y automatiza la copia de seguridad en un entorno linux de una estructura de directorios. Utiliza para ello el comando dd y el servicio crond – consideramos que la copia se realiza en el mismo equipo-. *Considerar distintos programas de copia, cada uno de ellos con sus correspondientes momentos.*

# Prácticas/Actividades



Copias de seguridad

## Actividad 10.-

Implantación de la aplicación cliente/servidor AMANDA. Se definirá y probará una máquina servidora donde se centralizará todas las copias de seguridad y 1 cliente linux de que se realizará la copia de seguridad. *Considerar 2 clientes uno linux y otro windows*

## Actividad 11.-

Configura y automatiza la copia de seguridad en un entorno linux de una estructura de directorios. Utiliza para ello el comando dump y el servicio crond – consideramos que la copia se realiza en el mismo equipo-. *Considerar distintos programas de copia, cada uno de ellos con sus correspondientes momentos.*

# Prácticas/Actividades



## Actividad 12.-

Explica y ejercita las opciones más importantes de la herramienta de clonación **Clonezilla**. Considera que la clonación se realiza en el mismo equipo. Realiza la restauración con el fin de comprobar el proceso realizado.  
[http://www.youtube.com/watch?v=Cf9nrrnP4o\\_w](http://www.youtube.com/watch?v=Cf9nrrnP4o_w)

## Actividad 13.-

Explica y ejercita las opciones más importantes de la herramienta de clonación **Paragon Partition Manager**. Considera que la clonación se realiza en el mismo equipo o en otro equipo. Realiza la restauración con el fin de comprobar el proceso realizado.

## Actividad 14.-

Explica y ejercita las opciones más importantes de la herramienta de clonación **Symantec Ghost**. Considera que la clonación se realiza en otro equipo o en otro equipo. Realiza la restauración con el fin de comprobar el proceso realizado.

# Prácticas/Actividades



Restauración  
de Equipos

## Actividad 15.-

Explica y ejercita las opciones más importantes de la herramienta de clonación **Drive Imagen**. Considera que la clonación se realiza en el mismo equipo o en otro equipo. Realiza la restauración con el fin de comprobar el proceso realizado.

## Actividad 16.-

Explica y ejercita las opciones más importantes de la herramienta de clonación **Acronis True Image**. Considera que la clonación se realiza en el mismo equipo o en otro equipo. Realiza la restauración con el fin de comprobar el proceso realizado.

# Prácticas/Actividades

## Práctica Opcional:

*Instalación y puesta en marcha de un cluster de dos nodos utilizando Ubuntu*

