Módulo de Proyecto Integrado

José Mariscal Prieto - 2º ASI

Proyecto: Copias de Seguridad

Curso 2006/2007

Índice de contenido

1.- Introducción

Nuestro proyecto plantea solventar el problema de las copias de seguridad de datos (ficheros), creando un sistema en el cual se puedan mantener copias de seguridad de los datos importantes permitiendo la recuperación de los datos a la fecha más actual posible en caso de fallo.

La realización de copias de seguridad evitará en su totalidad la pérdida de información en caso de algún inconveniente provocado por un virus, rotura de algún equipo, etc, permitiendo la recuperación de los datos a un estado consistente.

Nuestro sistema se centrará únicamente en el diseño e implementación del mismo.

El sistema deberá permitir:

- Preservar la información de la parte de administración
- Garantizar las copias periódicas de la información de dichos equipos
- Poder recuperar los datos en caso de pérdida

2.- Objetivos y requisitos del proyecto

El problema que se nos plante a es crear un sistema de copias de seguridad para el centro en la parte de administración que permita la creación de copias de seguridad regularmente contra un servidor. La solución buscada deberá basarse en software libre para evitar costos de licencias. El sistema costara de dos partes, una los clientes que realizarán una copia periódica, aproximadamente diaria al servidor y otro el servidor que realizará una copia semanal. Los clientes son equipos con windows por tanto el programa deberá funcionar bajo windows, deberá permitir una configuración lo mas sencilla posible y tener opciones para poder copiar los ficheros al servidor. El servidor también sera lo mas simple posible su funcionamiento y configuración.

Objetivos:

- El sistema se debe de adecuar a la legislación actual de protección de datos.

- Creacion de un sistema que permita la creación de copias de seguridad de la forma mas automatizada posible.

Requisitos Internos:

- Los respaldos se deben realizar en diferentes periodos de tiempo con tal de no saturar el servidor, por ejemplo una diferencia de 5 minutos entre cliente y cliente.
- Tendrán limitaciones de copia por extensión de fichero, por ejemplo no se copiarán ficheros avi, mpg, mov, mp3, wma, wmv
- En caso de que no se realice el respaldo de forma correcta el sistema deberá informar al administrador mediante el envió de correo electrónico o algún tipo de aviso.

- La solución debe basarse en software libre, para eliminar a ser posible los costes de licencias.

Requisitos Externos:

- Se debe tener una cuenta configurada de STMP con autenticación o sin ella para el envío de correo electrónico a la hora de enviar informes de copia.
- Los clientes que utilizaremos serán Windows 98, Windows 2000 o Windows XP.

- Estos clientes estarán conectados mediante una LAN al servidor.

3.- Estudio previo

3.1.- Estado actual

La situación actual de copias de seguridad es que se lleva de una forma particular. Cada usuario hace copias de seguridad según estima necesario. No hay una política clara en materia de copias de seguridad.

3.2.- Estudio de soluciones existentes

Búsqueda y descripción de soluciones a ese problema ya instaladas en otros sitios.

Para la copia de ficheros al servidor existen varias soluciones: rsync, unison, bacula, cobian backup.

rsync

Rsync, escrita inicialmente por Andrew Tridgell y Paul Mackerras, viene prácticamente con la totalidad de distribuciones Linux y sistemas Unix. En caso de no ser así se dispone del código fuente en rsync.samba.org. La principal utilidad de rsync es la de sincronizar estructuras de árboles de directorios a través de la red, aunque puede ser utilizado perfectamente también dentro de una máquina de forma local.

Es muy fácil de utilizar y configurar, y al contrario que la utilización de programas de script basados en FTP, ofrece una serie de funcionalidades que lo diferencian claramente. El algoritmo que utiliza envía únicamente la información que ha cambiado dentro de cada archivo, evitando enviar el archivo completo, y permite comprimirla para reducir la utilización de ancho de banda, o enviarlo a través de ssh si se requiere un nivel extra de seguridad en la transmisión.

El inconveniente de rsync es su tediosa configuración en Windows. Al ser en modo texto hay que buscar métodos para informar de que el volcado de datos se ha hecho de forma correcta. Difícil sino imposible es la opción de enviar un mensaje de correo electrónico.

Unison

Unison permite mantener actualizados árboles completos en el mismo ordenador (diferentes directorios) o en ordenadores remotos (usando ssh u otros métodos). Además propaga las modificaciones en ambos sentidos. Así es posible mantener sincronizados casi los ordenadores que queramos. Si no hay conflictos (i.e. el mismo fichero modificado en ordenadores distintos y que es imposible hacerles un "merge"), todos tendrán las mismas copias.

El inconveniente es su tediosa configuración en Windows. Aunque existe un modo gráfico para Windows, hace dificultosa su configuración, aunque es altamente recomendable para desarrolladores a la hora de distribuir código fuente. Funciona francamente bien para varios gigas de información. Ideal para sincronizar cuentas Linux,

Bacula

Bacula es un sistema de gestión de copias altamente modularizado con partes prácticamente independientes.

El sistema se divide en:

- Bacula director:

El demonio encargado de gestionar todas las operaciones de backup. El director sabe los trabajos que se van a realizar, cuando , donde y como. Y además se encarga de restaurar los ficheros que le pidamos y su verificación (una especie de suma de comprobación de integridad). Se puede instalar en cualquier máquina de la red.

- Bacula File

El cliente. Es necesario instalarlo en todas las máquinas de las que queramos hacer respaldo. Su función es leer y transmitir los ficheros que el director le pida, o restaurarlos.

- Bacula Storage

Este demonio se encarga de la lectura/escritura física en los volúmenes que estén definidos (cintas, ficheros)

Bácula es de fácil configuración pero su desarrollo en Windows deja mucho que desear aún.

Cobian Backup

Cobian Backup es una aplicación que nos permitirá hacer nuestras copias de seguridad de manera sencilla y efectiva. Gratuito y en castellano, le puedes indicar que copias deseas realizar y donde hacerlo. Me comentó su existencia una programadora de Cajasur que lo utilizan para hacer copias de seguridad remotas o bien en particiones diferentes.

Además, no consume recursos, permite la compresión de las copias así como te guarda sólo las novedades de tus directorios y archivos a la copia ya efectuada anteriormente.

Se puede instalar como servicio o aplicación dependiendo si es Windows 98 o Windows 2000, XP. Es altamente configurable y su interfaz es muy sencilla. La copia remota se realiza por FTP y puede ser completa, incremental, diferencial, puede incluso comprimirse y encriptarse si se desea. En el caso de que la cinta se quiera dejar descomprimida se pueden tener los ficheros comprimidos en zip. Por supuesto incluye la opción de enviar un mensaje por correo electrónico al administrador desde el mismo cliente, también se puede configurar con clave para evitar que se modifiquen las tareas de backup mediante clave.

Comparativa clientes

Clientes	Soporte SMTP	Requiere Cinta	Depende otros clientes	Fácil Configuración	Exclusión de Extensiones	Apagado	Bloqueo con contraseña	Servicio de Windows
rsync	No	No	No	No	No	No	No	No
Unison	No	No	No	No	Si	No	No	No
Bacula	Si	Si	Si	No	Si	No	No	Si
Cobian	Si	No	No	Si	Si	Si	Si	Si

Es un requisito imprescindible el soporte SMTP, Unison y Rsync no los soportan, aunque podrian utilizarse scripts en bat pero sería muy tedioso y depende de otros programas, ademas utilizamos Windows, Cobian lo soporta plenamente y con autenticación. El bacula no envía de forma directa los correos sino que utiliza el bacula director para el envío de correo. El único que tiene una fácil configuración es Cobian. Bácula es configurable pero no de forma intuitiva. La solución adoptada es Cobian, debido a su flexibilidad, facilidad de configuración y soporte SMTP nativo configurable.

Luego en el servidor para realizar las copias de seguridad tenemos programas como:

Bacula

Se ha comentado en el punto anterior aunque hemos de comentar que tiene su propio lenguaje para acceso a los datos en caso de recuperar datos hemos de aprender una nueva sintaxis para el almacenamiento y recuperación.

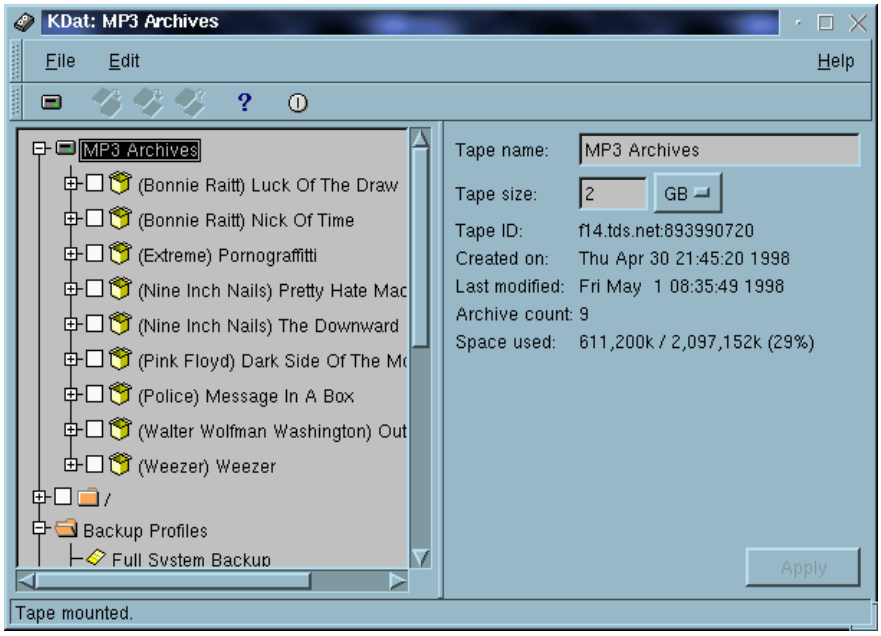
Amanda

AMANDA, el Archivador de disco automático avanzado de red de Maryland, es un sistema de backup que permite que el administrador instale un solo servidor de copias principal para sostener los anfitriones múltiples sobre red a las unidades de cinta, discos o medios ópticos. Es altamente configurable, se pueden definir el sistema de cinta. Inconvenientes, tiene tantas opciones de configuración que sobradamente podríamos utilizar, pero no disponemos de tanto tiempo para analizarlas. No lo hemos puesto en el punto anterior debido a que los clientes son Unix.

shellscripts

Permiten la creación de copias de seguridad en cinta de la forma que queramos, la recuperación de la información se puede realizar de la misma forma que si descomprimimos un fichero tar por ejemplo. Ademas del tar existe el dump para hacer copias funciona de forma similar pero la sintaxis del tar es mas simple y todo administrador en Unix la conoce. Pueden crearse tareas en el cron para que haga las copias cuando nosotros queramos. Para lo que necesitamos hacer esto es mas que suficiente.

kdat



Kdat es un programa muy sencillo y intuitivo en modo gráfico, esta pensado para hacer copias de seguridad en cinta de una serie de directorios, permite la recuperación de datos de la forma mas sencilla posible, por contra no es automatizado y se ha de estar delante del equipo para realizar las copias de seguridad.

Comparativa de Servidor

Clientes	Soporte Mail	Depende de clientes	Fácil Configu-ración	Automatiza-ble	Facilidad recupera-cion de datos
Bacula	Si	Si	No	Si	No
Amanda	Si	No	No	Si	No
Shell Scripts	Si	No	Si	Si	Si
Kdat	No	No	Si	No	Si

Bacula y Amanda utiliza propios lenguajes para el almacenamiento y la extracción quizás para un uso empresarial en una gran compañía sea recomendable, pero para lo que vamos a utilizar no necesitamos grandes herramientas sino algo simple para el día a día que nos permita en un momento dado recuperar la información de forma flexible y a la unidad que nosotros queramos por ejemplo un disco duro extraíble. El soporte SMTP lo lleva el propio servidor tiene que tener configurado un MTA para poder enviar correo al exterior, esto debe testearse en la parte final del montaje ya que la configuración de arriba y abajo es diferente.

4.- Plan de trabajo

Planificación temporal.

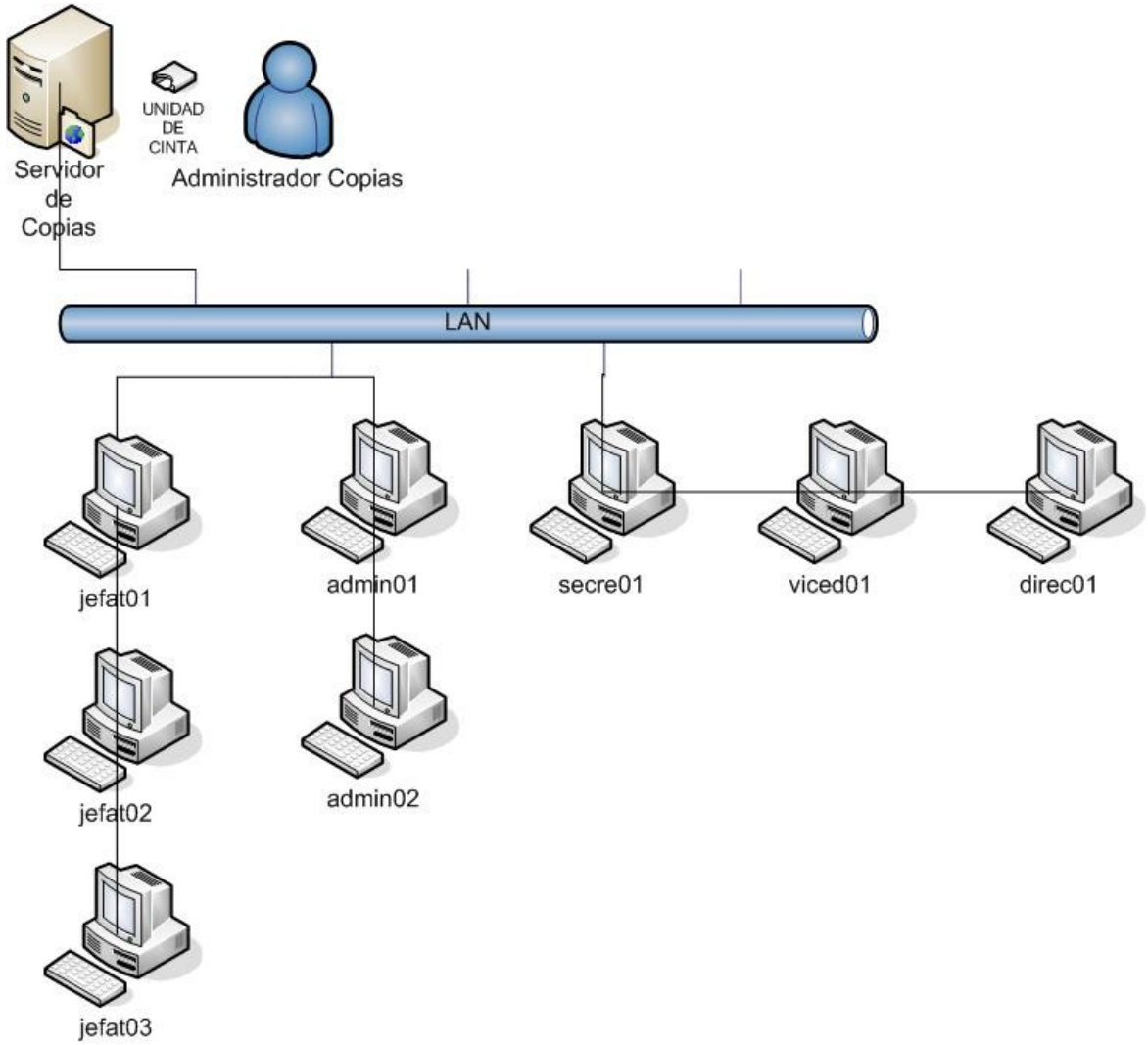
- 18 Abril - 21 Abril Definición del problema y Análisis soluciones posibles.
- 25 Abril Instalación del servidor. Independientemente del cliente que adoptemos el servidor puede instalarse y dejarlo en funcionamiento, ya simplemente habría que realizar cambios de configuración o instalar paquetes.
- 2 Mayo Testeo del funcionamiento de Cobian en caso de fallos, es posible que se requiera configurar una cuenta de correo para el proyecto (a elección antes de implementar). Puesta en funcionamiento del servidor FTP.
- 14-18 Mayo: Crear shell scrips para el volcado de la cinta, se utilizara crond para el volcado que ejecutara regularmente el volcado.
- 14 Mayo: Probar la unidad de cinta haciendo un primer volcado de información aunque sea rudimentario.
- 15 Mayo: Crear los shell scripts necesarios y especificar el funcionamiento del crond. (hecho)
- 16 Mayo: Puesta en común del proyecto, fork.
- 17 Mayo: Recogida de datos. Antes de realizar la instalación de los clientes es necesario saber cuantas máquinas hay, que se va a copiar de cada una y cuanto espacio aproximado es del que se quiere realizar una copia de seguridad.
- 17 Mayo: Creación del espacio necesario en el servidor, creación de los directorios $HOME para cada equipo al que se debe realizar una copia de seguridad.
- 18 Mayo: Mejorar shell scrips en el caso de que no exista unidad de cinta metida.
- 22-23 Mayo: Depuración de documentación.
- 10 Junio: Instalación del servidor abajo.
- 11 Junio se prueba la salida de smtp hacia afuera.

5.- Diseño

5.1.- Diseño general

La solución general es que los clientes hagan una copia regularmente contra el servidor. Al realizar la copia se informará al responsable de que la copia se ha realizado con éxito. Una vez tengamos las copias de los ficheros de los clientes se copiaran a cinta regularmente, probablemente usando un script en el cron y creando algún mecanismo para informar al responsable de que la cinta no esta metida.

El esquema básico del sistema a implementar sería el siguiente:



5.2.- Diseño detallado

El problema que se nos plantea es tener un servidor que es el tendrá las copias de seguridad y una serie de clientes que mandarán las copias de

seguridad al servidor.

Para poder realizar el proyecto vamos a desarrollar las siguientes partes del sistema.

5.2.1.- Legislación actual

Es imposible analizar todas las leyes y jurisprudencia existentes, por lo que nos centraremos en la principal ley que es La Ley Orgánica de Protección de Datos de Carácter Personal 15/1999, de 13 de Diciembre, (en adelante LOPD).

Existen varios tipos de datos según la LOPD, pero centrándonos en nuestro caso los datos que vamos a tratar son:

- Nombre
- Apellidos
- Direcciones de contacto (tanto físicas como electrónicas)
- Teléfono (tanto fijo como móvil)
- Otros

Estos datos son utilizados para crear informes o análisis con fines estadísticos. La principal información sobre los alumnos y notas se gestionan mediante red con el programa SÉNECA, siendo la Junta de Andalucía la que gestiona estos datos.

Por lo tanto los tipos de datos que vamos a tratar son de Nivel Básico. Según la LOPD se establecen una serie de medidas mínimas de seguridad que deben de cumplir estos tipos de datos.

Medidas de nivel básico

- Documento de seguridad (art. 8)
- Funciones y obligaciones del personal (art. 9)
- Registro de incidencias (art. 10)
- Identificación y autentificación (art.11)
- Control de acceso (art. 12)

- Gestión de soportes (art. 13)
- Copias de respaldo y recuperación (art. 14)

En nuestro caso específico el artículo 13 y 14 nos dice:

Artículo 13. Gestión de soportes.

1. Los soportes informáticos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y almacenarse en un lugar con acceso restringido al personal autorizado para ello en el documento de seguridad.

2. La salida de soportes informáticos que contengan datos de carácter personal, fuera de los locales en los que esté ubicado el fichero, únicamente podrá ser autorizada por el responsable del fichero.

Artículo 14. Copias de respaldo y recuperación.

1. El responsable de fichero se encargará de verificar la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

2. Los procedimientos establecidos para la realización de copias de respaldo y para la recuperación de los datos deberá garantizar su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

3. Deberán realizarse copias de respaldo, al menos semanalmente, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

Se deben de identificar las soportes informáticos, en nuestro caso las cintas deben estar inventariadas y solo el administrador de copias tendrá acceso a estas. Estas copias de seguridad nunca deberán salir del centro.

Al menos hemos de hacer una copia semanalmente para cumplir con la legalidad.

5.2.2.- Servidor

Disponemos de un IBM eServer xSeries 206

Para que servidor realice su función correctamente hemos de desarrollar los siguientes puntos:

- Crear varias particiones para tener los datos de forma independiente, de manera que si falla una partición no afecte a las demás.
- Instalar un servidor FTP para recibir los datos de los clientes.
- Crear cuentas de usuario para almacenar los datos.
- Crear scripts para el manejo de las cintas.

Datos del servidor:

Dirección IP:	172.26.0.70
Mascara:	255.255.255.0
Puerta de enlace:	172.26.0.1
Puertos ssh:	22 1010 4000
Puerto ftp:	21

5.2.3.- Clientes

Los clientes realizarán una copia de los datos importantes al servidor cada día, preferiblemente a horas en los que no estén los delante del pc, por ejemplo desayunos, recreo. Hay que tener en cuenta que la primera copia será la que mas tarde en realizarse, sobre todo en equipos que tienen 1 o 2 gigabytes de datos, aproximadamente unos 10 minutos en copiar los datos al servidor.

Antes de implementarlo es necesario hacer un listado de los equipos con los directorios y ficheros que quieren copiarse, para tener una estructura de directorios home preparada en el servidor. Para ello hay que tener un backup

completo de abajo para verificar además que espacio en disco se va a necesitar aproximadamente.

Cobian permite enviar mensajes por correo electrónico en caso de grabación exitosa o fallo, cabe la posibilidad o bien de utilizar el propio servidor como SMTP o utilizar uno externo para enviar el correo, esto ha de testearse antes de montar los equipos clientes.

5.2.4.- Unidad de cinta

La unidad de cinta que disponemos es una IBM DDS GEN5, DAT 72 que permite almacenar 36Gb sin compresión y 72 con compresión. La compresión que utiliza la cinta es por hardware y por defecto esta activada, por lo que no es necesario comprimir la cinta en las opciones de copia. La velocidad es de 3Mb por segundo sin compresión y 7 con compresión.

Las copias de seguridad se realizarán de forma completa. La unidad de cinta además soporta compresión mediante hardware, aunque si se quiere comprimir los datos se pueden usar las opciones z y j de tar. Disponemos de 5 cintas.

Política de rotación de cintas.

La política mas simple podría ser de 4 cintas rotando cada semana, sin embargo existen otros métodos mas complejos como por ejemplo el algoritmo de las Torres de Hanoi.

Con tres cintas

1 2 1 3 1 2 1

De esta forma tendríamos una cinta cada dos semanas, una cinta cada una y una cinta para cada 5 dias. La cinta 1 seria la que mas se estropearía mientras de la cinta 3 seria la que menos.

Cuatro cintas

1 2 1 3 1 2 1 4 1 2 1 3 1 2 1

5.2.5 Recuperación de datos

La forma de recuperación de datos será conectando un disco duro externo al cual volcaremos los datos. Acto seguido el responsable de copia se ubicará en el equipo en cuestión recuperando los ficheros necesarios. Si el equipo es Windows 98, el administrador de copias podrá o bien montar el software de almacenamiendo masivo para windows 98 o bien compartir en otro equipo el disco duro y recuperar los datos por red. Tambien es posible recuperar los datos si la copia es reciente por ejemplo de un día para otro mediante FTP conectándose al servidor de copias.

6.- Implantación

Pasos necesarios para instalar la solución.

1. Recopilación de información sobre el servidor
2. Instalación del servidor
3. Configuración del servidor FTP
4. Configuración unidad de Cinta
5. Recuperacíon de datos
6. Configuración equipos clientes

6.1.- Recopilación de información sobre el servidor

Lo más importante es que disponemos de dos discos duros exactamente iguales, lo que hace viable la creación de un sistema tolerante a fallos montando los dos discos duros en espejo.

Existen dos posibilidades, una montarla con Linux creando un sistema en espejo, esto se hace mediante software y otra si los medios técnicos lo permitían montar el espejo por hardware.

Tras buscar en Internet encontramos que la tarjeta SCSI Adaptec entre otras funcionalidades trae la opción de funcionar en modo RAID0 y RAID1.

Para activar el Raid primero hay que entrar en la BIOS y activar el modo RAID, una vez que esta activo, hay que entrar en la BIOS de la la controladora Adaptec y crear el raid con las dos unidades. Al crear un raid en modo 0 nos aparece una capacidad de aproximadamente el doble unos 150Gb aproximadamente, mientras que en el modo raid1 utiliza 74,5GB, pero en caso de fallo de alguno de los discos duros, solo tendríamos que reemplazar el que funcionase y ponerlo como primario.

La creación del array es lenta y permite la selección del disco duro que queremos clonar en el otro para tener una imagen idéntica, con lo cual debemos buscar o otro disco duro de iguales características o mayor, pero se ha de tener en cuenta que aunque sea de mayor capacidad el RAID solo utilizara la porción de disco que ocupe el de menor tamaño. Necesitamos un disco duro SATA de forma temporal para ver si puede crear un RAID aunque sea de diferente tamaño, en teoría es posible aunque conviene comprobarlo para referencias futuras.

Para instalar el sistema operativo, que utilizaremos Debian 4.0 Etch hemos de descargarlo en CDROM y su posterior instalación se realizara mediante el primer CD y luego tomaremos los demás datos de la red.

6.2.- Instalación del servidor y posterior configuración

Procedemos a la instalación de debian mediante CDROM ya que el equipo no dispone de DVD, utilizamos el primer CD y el resto instalaremos por red.

Como mencionamos anteriormente en el diseño hemos creado varias particiones:

- /boot de 50Mb (arraque, kernel) primaria
- / de 7.5Gb primaria
- /home 40Gb extendida
- /usr 10Gb extendida
- /var 10Gb extendida
- /tmp 5Gb extendida
- /mnt/backup 6Gb extendida

El home será el que almacene todos los datos de usuario /mnt/backup se ha dejado como partición de reserva para el futuro.

Todos los sistemas de ficheros son extendido 3 que pueden ser copiados fácilmente en caso de pérdida de información y además utiliza un sistema transaccional que en caso de mal apagado devuelven el sistema de ficheros en un estado consistente.

Hacer que en el arranque se autochequee el sistema de ficheros en caso de caída de luz. Modificamos en el /etc/default/rcS FSCKFIX=yes

De esta forma si hay algún error en el arranque y el sistema de ficheros esta dañado, automáticamente se repara, aunque no estaría de más en un futuro adquirir un SAI.

Mostrar un log de lo que esta ocurriendo en el sistema por pantalla, la salida de todos los mensajes esta redirigida a la terminal virtual 12. Para ello

hemos modificado el /etc/syslogd.conf añadiendo al final:

***.* /dev/tty12**

El servidor puede apagarse de forma sencilla presionando el botón de apagado, el sistema esta configurado de tal forma que se apague de forma segura.

6.3 Preparando el servidor

Instalamos el proftpd que será el servidor de ftp para sincronizar las copias de seguridad.

apt-get install proftpd

Para hacer las copias de seguridad en red utilizamos el servidor proftpd en el cual se guardan los logs de todas las transferencias de ficheros realizadas y si se han realizado cambios.

Modificaciones en el fichero */etc/proftpd/proftpd.conf*

UseIPv6 on ha sido cambiada a *off* para no utilizar el ipv6

AllowStoreRestart on Por si se corta la comunicación en la transferencia de un fichero, reanudar la comunicación por donde se quedo.

Para ello utiliza dos ficheros uno para controlar los accesos y otro para ver las transferencias así tenemos otro mecanismo en el servidor además de en los clientes.

Creamos las siguientes cuentas de usuario para el FTP con el comando *adduser*.

- jefat01
- jefat02
- jefat03
- admin01
- admin02
- secre01
- viced01

- direc01

La contraseña es el mismo login, aunque debe cambiarse.

Como mencionamos en la parte de Diseño necesitamos un MTA para el envío de correo. Para esto instalamos el postfix:

apt-get install postfix

No lo configuramos del todo porque la parte de arriba es diferente a la de abajo, habría que configurar el nombre de dominio con el de arriba y abajo. Además desde arriba tenemos bloqueado el puerto saliente TCP 25 con lo cual nos es imposible realizar pruebas de envió de forma correcta.

Realizamos las pruebas abajo de forma correcta para permitir en envío de información al exterior. Añadimos a mynetworks 172.26.0.0/16 para permitir la salida de correo desde los clientes utilizando el servidor, si no se pudiese enviar sería necesario configurarlos directamente con smtp saliente.

6.4 Preparando la copia

Para probar que funciona la cinta correctamente probamos los comandos básicos de la cinta.

Comandos Básicos de la unidad de cinta:

Muestra el estado

mt -f /dev/st0 status

Rebobinar la cinta

mt -f /dev/st0 rewind

Sacar la cinta

mt -f /dev/st0 offline

Crear un volumen con tar

tar cvf /dev/st0 Pathficheros

Extraer ficheros de un volumen tar (recuperación de datos)

tar xvf /dev/st0 Pathficheros

Por ultimo creamos un shellscript para la copia de la cinta y añadimos una entrada al crontab de root para crear los respaldos automáticamente.

/usr/local/bin/backup.sh

```
#!/bin/bash
#ejemplo de shellscript de copia

fecha=`date`

# si la salida es menos de 2 lineas no hay cinta metida
salida=`mt -f /dev/st0 status | wc -l `

if [ $salida -gt 2 ]; then
echo Realizando copia: $fecha >> /dev/tty10
#rebobinamos la cinta
mt -f /dev/st0 rewind

# empezamos a copiar el contenido del home
# y la salida la hacemos por la terminal 11
tar cvf /dev/st0 /home/* >> /dev/tty11

# rebobinamos la cinta
mt -f /dev/st0 rewind

# expulsamos la cinta
mt -f /dev/st0 offline
echo Copia realizada con exito $fecha | mail
informatica@iesgrancapitan.org

else
echo Error cinta no metida $fecha >> /dev/tty10
echo Error cinta no metida $fecha | mail informatica@iesgrancapitan.org
fi
```

En caso de que la copia no se realizase por caída de luz, es fácilmente comprobable si cuando vamos a recoger la cinta esta metida. Simplemente accedemos al servidor por SSH y ejecutamos este script que está localizado en

/usr/local/bin/backup.sh

Para que nos automatice las copias podemos crear una entrada en el cron del root con crontab

Ejemplo de Crontab:

crontab -e

```
MAILTO="informatica@iesgrancapitan.org"

# ejecuta a las 18:30 los viernes un backup completo

30 18 * * 5 /path/scriptbackup
```

Así nos enviaría un correo a la dirección que especifiquemos con el resultado de la ejecución del cron.

6.5.- Recuperación de los datos

Para recueprar los datos del servidor existen varias formas.

6.5.1 Mediante FTP

Si los datos son recientes pueden recuperarse mediante FTP, simplemente nos conectamos con el mismo navegador de la siguiente forma:

ftp://usuario:clave@172.26.0.70

y restauramos los datos que necesitemos, es posible que necesitemos recuperar directorios por lo que es recomendable utilizar un programa como filezilla.

6.5.2 Mediante un disco duro extraible

Lo que hacemos es conectar un disco duro extraíble de la siguiente forma:

mount /dev/sda1 /mnt/disco

Para descomprimir la cinta efectuamos lo siguiente:

cd /mnt/disco

tar -xf /dev/st0

umount /mnt/disco

Y simplemente nos vamos al equipo con el disco duro externo y restauramos los datos.

Es posible que el cliente sea Windows 98 y no detecte el disco duro o no tenga instalado el software de almacenamiento masivo para Windows 98, con lo cual puede recuperarse mediante FTP o compartiendo una carpeta con el disco duro en otro equipo de forma temporal.

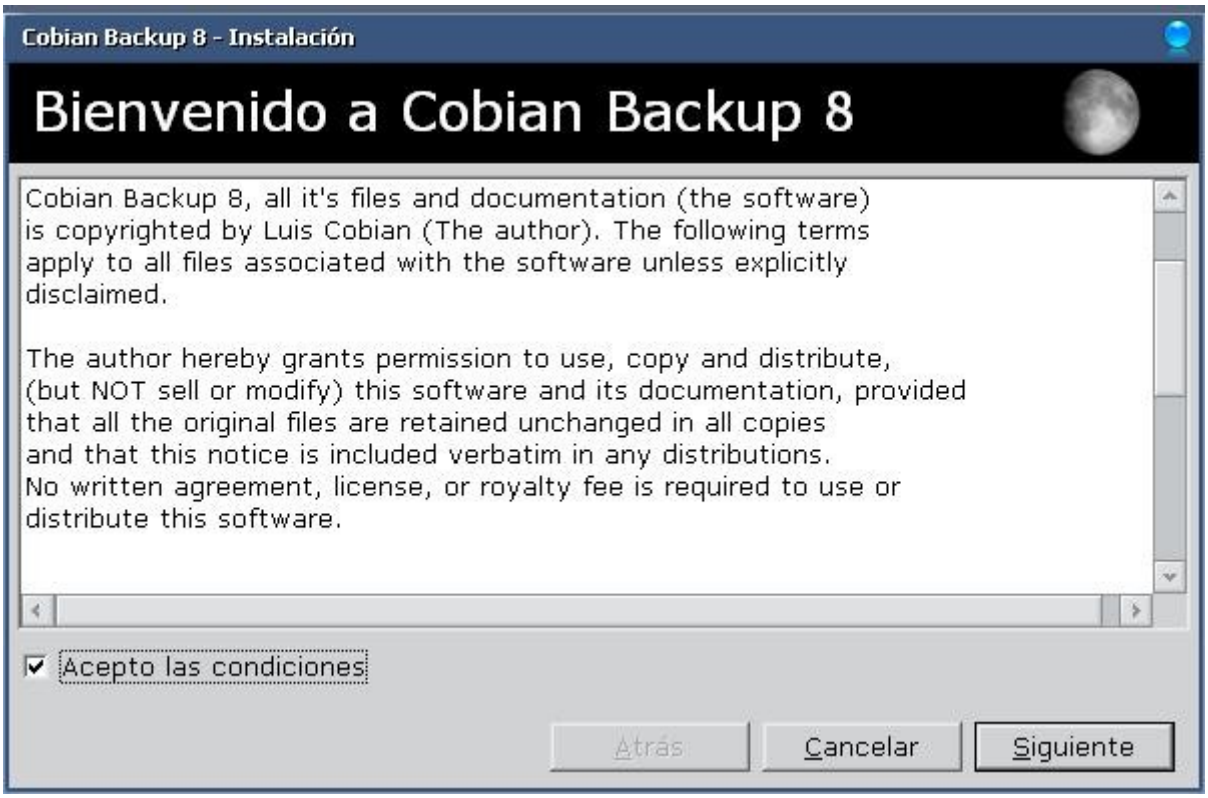
6.6.- Configuración de los clientes

Para configurar los clientes disponemos de dos versiones de Cobian, la versión 7 que utilizaremos en los clientes Windows 9X como se especifica en la pagina web y la versión 8 que utilizaremos en Windows 2000 / XP. Para facilitar la tarea de instalación hemos puesto en el ftp las dos versiones de cobian. Dado que la mayoría de los clientes son Windows XP exponemos a continuación el procedimiento de instalación de la version 8.

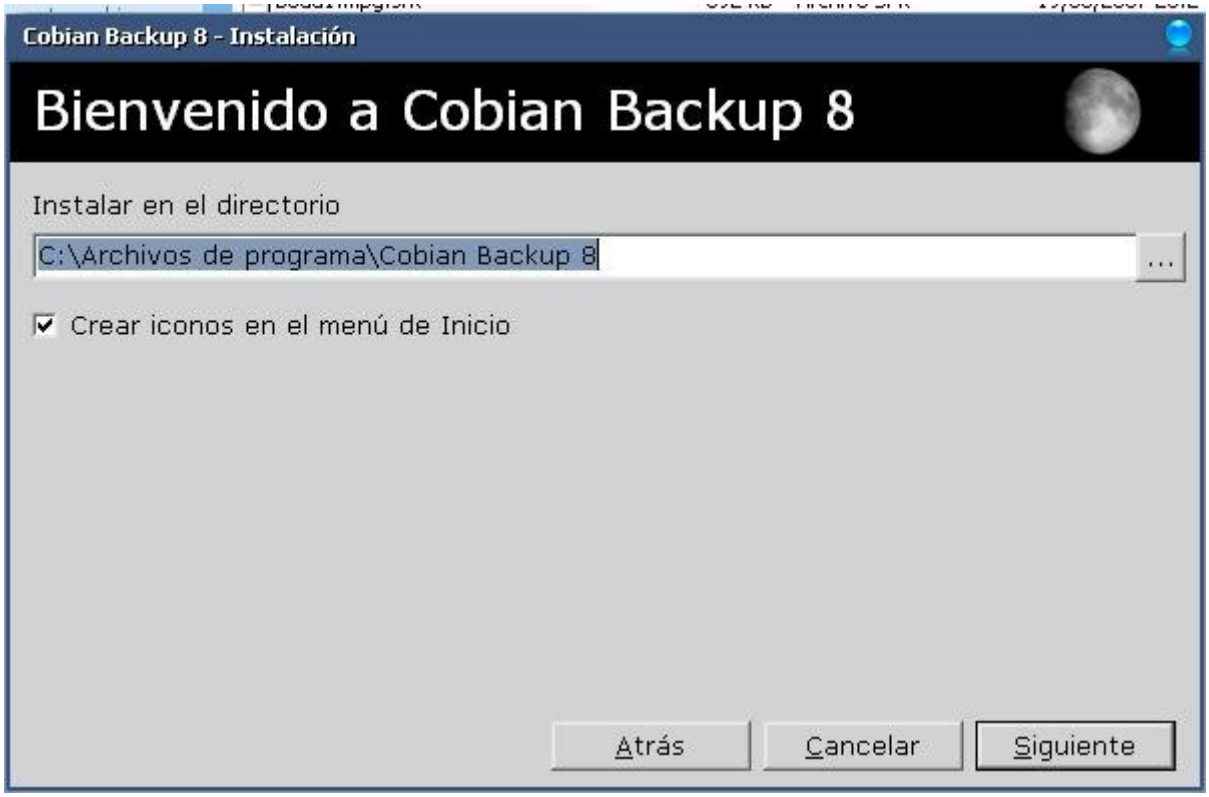
6.6.1.- Instalación del Cliente

Lo primero que nos aparece a la hora de instalar cobian backup es la selección de idioma. Seleccionamos el español.

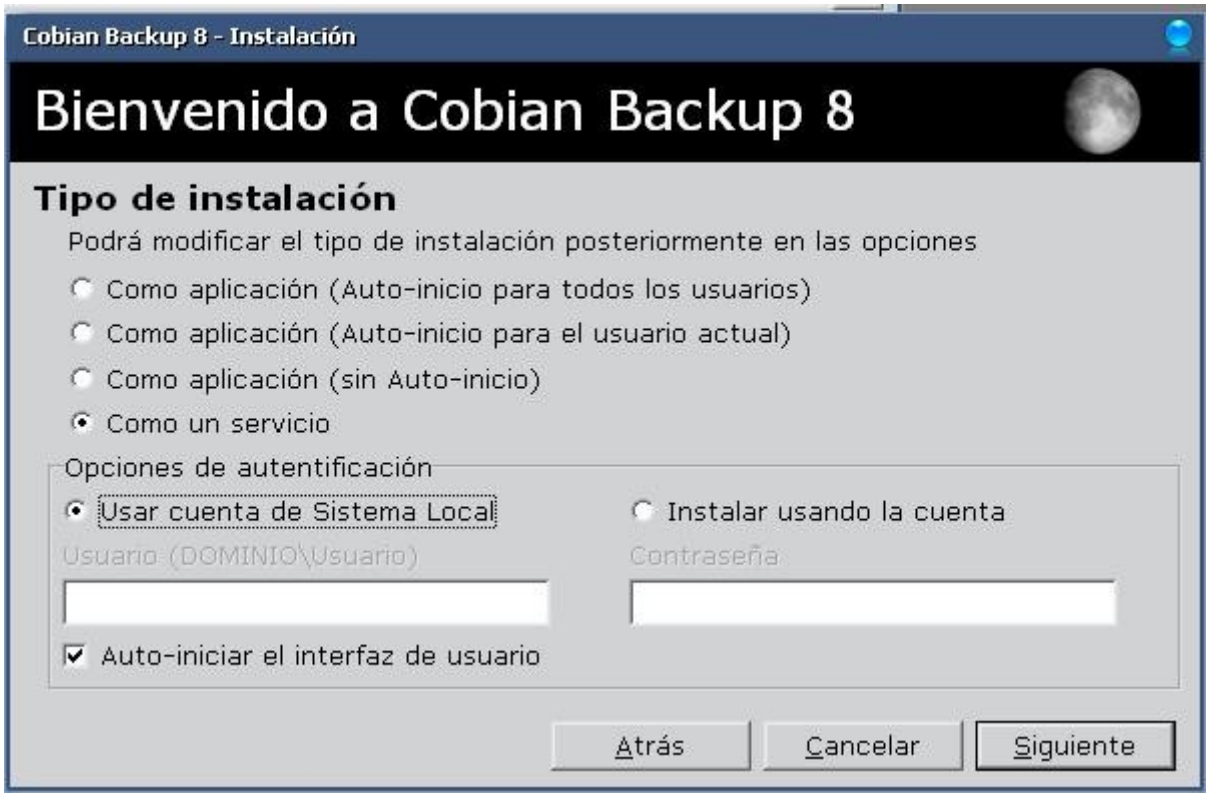
Para continuar con la instalación hemos de aceptar las condiciones legales. El software es de fuente abierta y se distribuye bajo la licencia Mozilla 1.1 que es más restrictiva que la GNU.



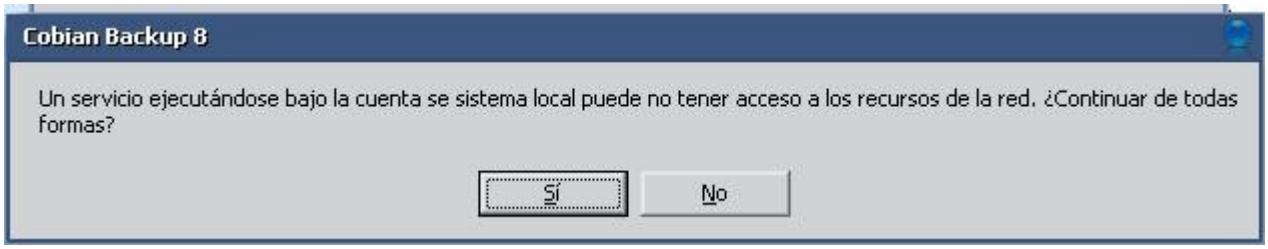
Selección de directorio de destino. Por defecto lo dejamos tal y como esta.



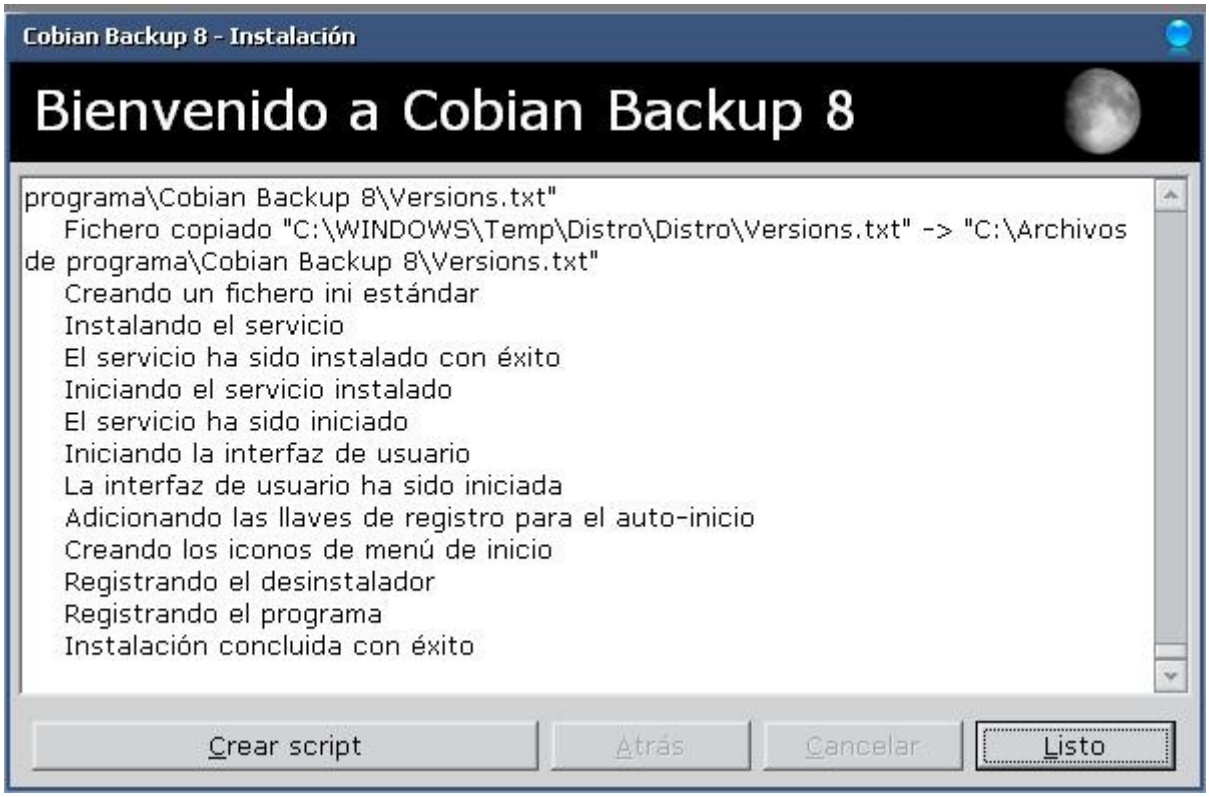
Tipo de instalación lo instalamos como Servicio si tenemos Windwos XP o 2000. Y usar cuenta del sistema local. Si tenemos un dominio o queremos grabar los datos en una maquina Windows mediante carpetas compartidas necesitaremos un usario y clave del dominio, como usaremos un FTP no lo necesitamos en este caso.



Como hemos mencionado el sistema ahora nos indicará que no hemos introducido un nombre de usuario y clave del dominio con los que no podremos acceder a los recursos de red de Windows.



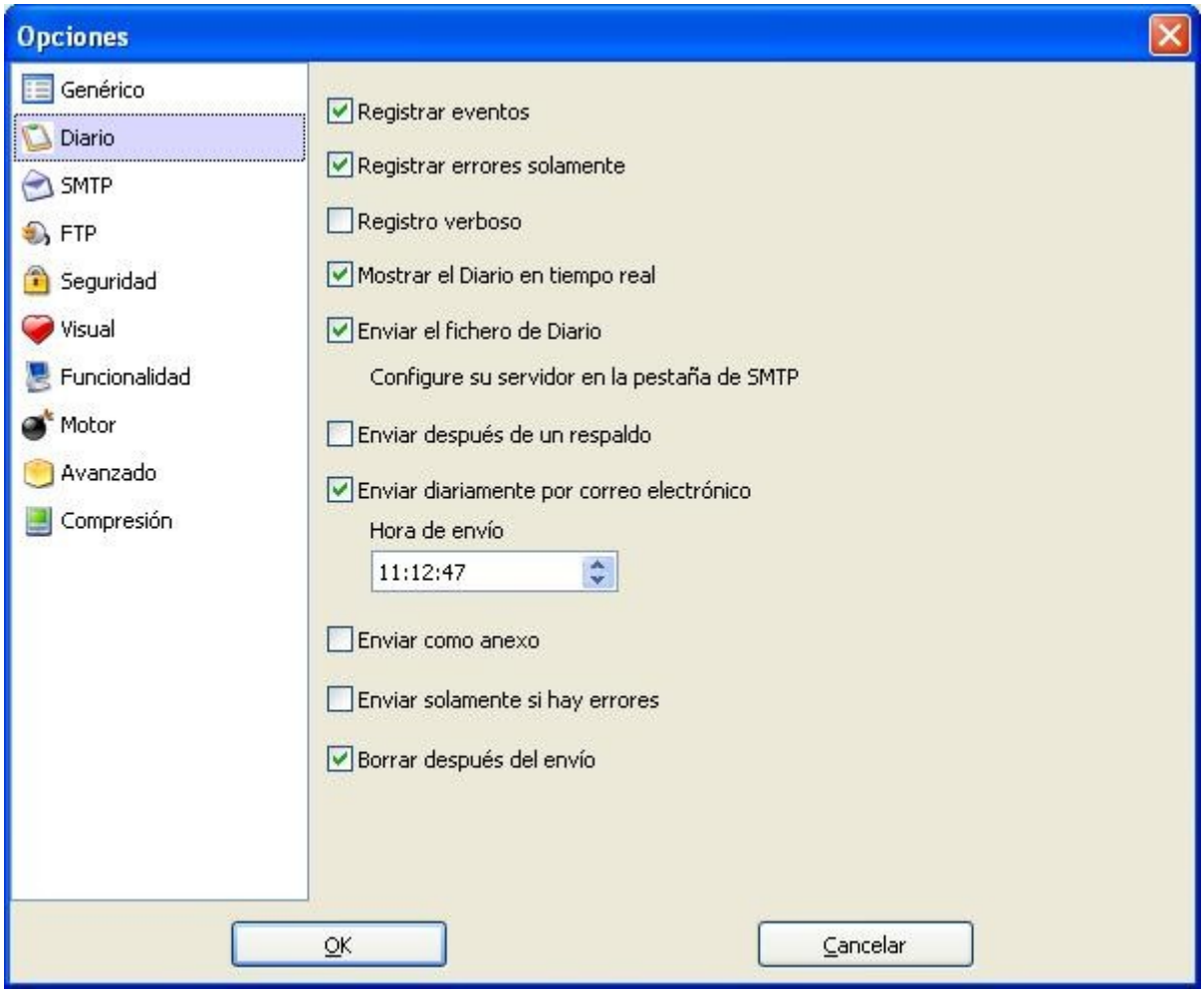
Ahora si todo marcha bien instalará Cobian y nos saldrá un log de la instalación indicando que se ha realizado de forma satisfactoria.



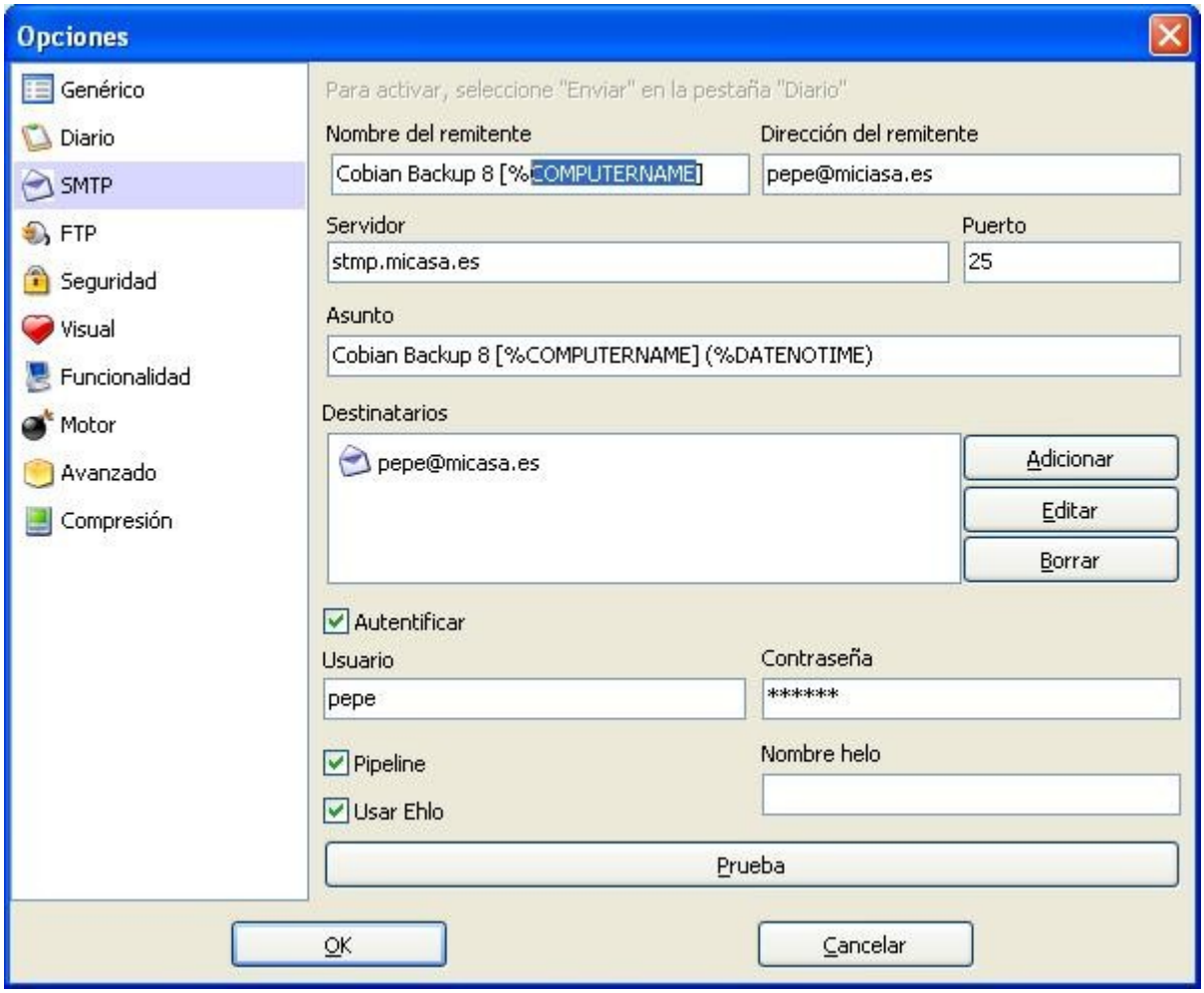
Solo tendremos que pulsar Listo y ya tenemos nuestro cliente funcionando lo siguiente es configurar las tareas de backup.

6.6.2 Configuración del Cliente

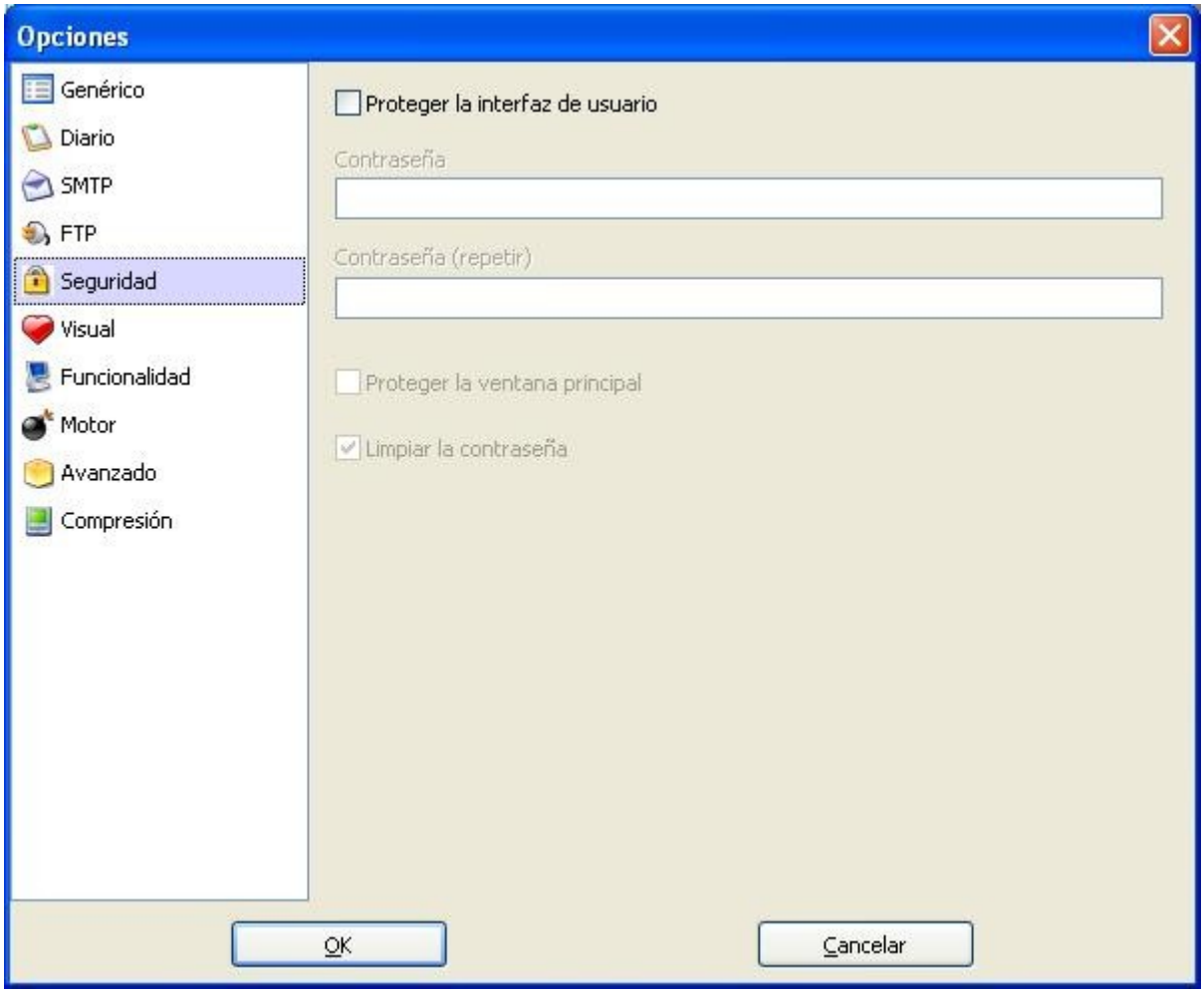
Hemos de modificar la configuración de los clientes para que pueda enviar correo mediante STMP. Para ello nos metemos en herramientas opciones. Una vez dentro nos metemos en la opción de Diario y activamos enviar al fichero de diario tal y como indica la imagen.



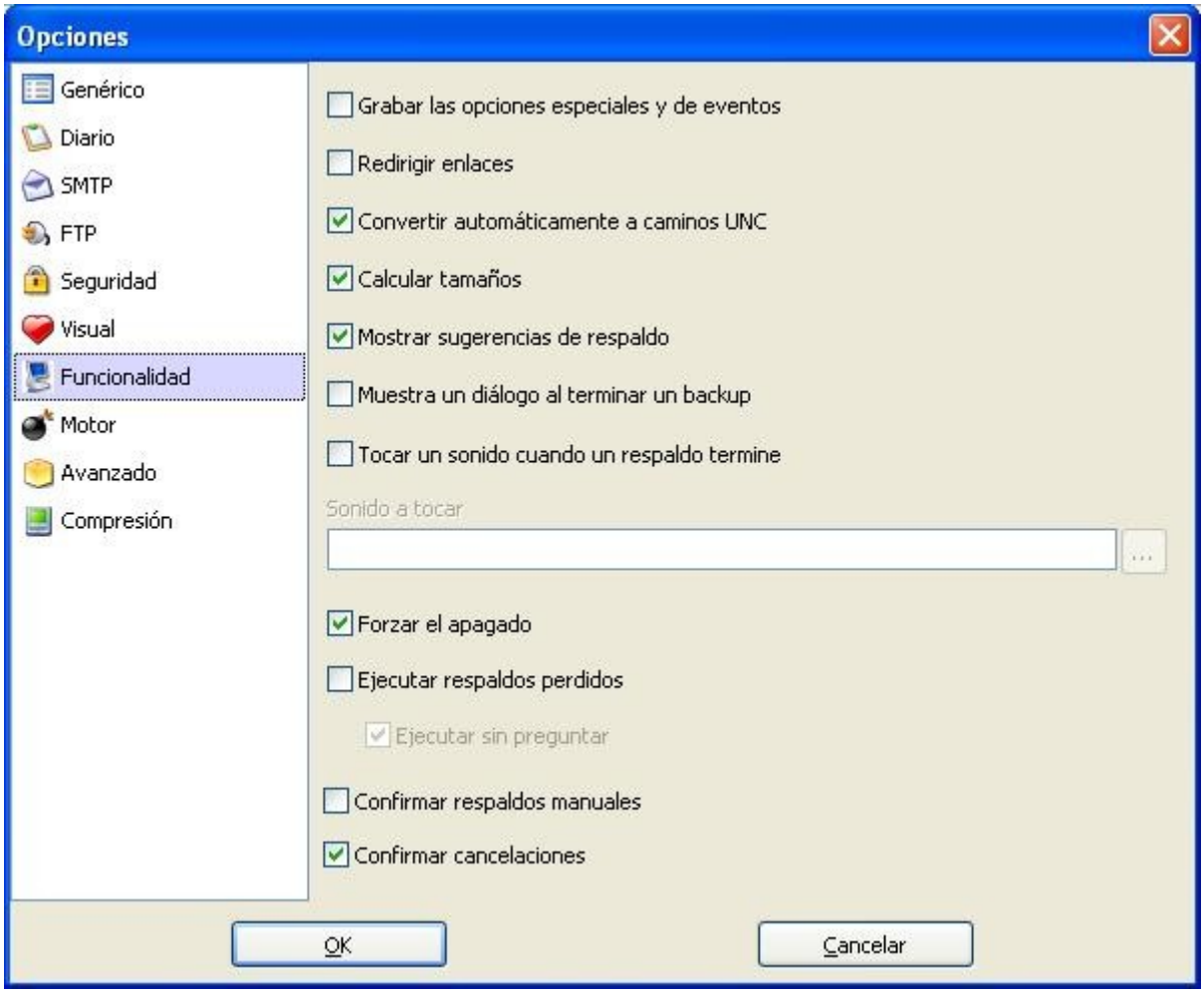
Ya tenemos que configurar el envió de correo en la opción de SMTP que ahora podremos modificarla con los datos del servidor SMTP y de los equipos.



Es interesante que el cliente este bloqueado por contraseña, así es difícil de desinstalar o incluso de cerrar el programa si este está en ejecución. Siempre que intentemos hacer alguna modificación en el cliente nos pedirá la contraseña que le hayamos puesto. En nuestra instalación no hemos puesto contraseña.

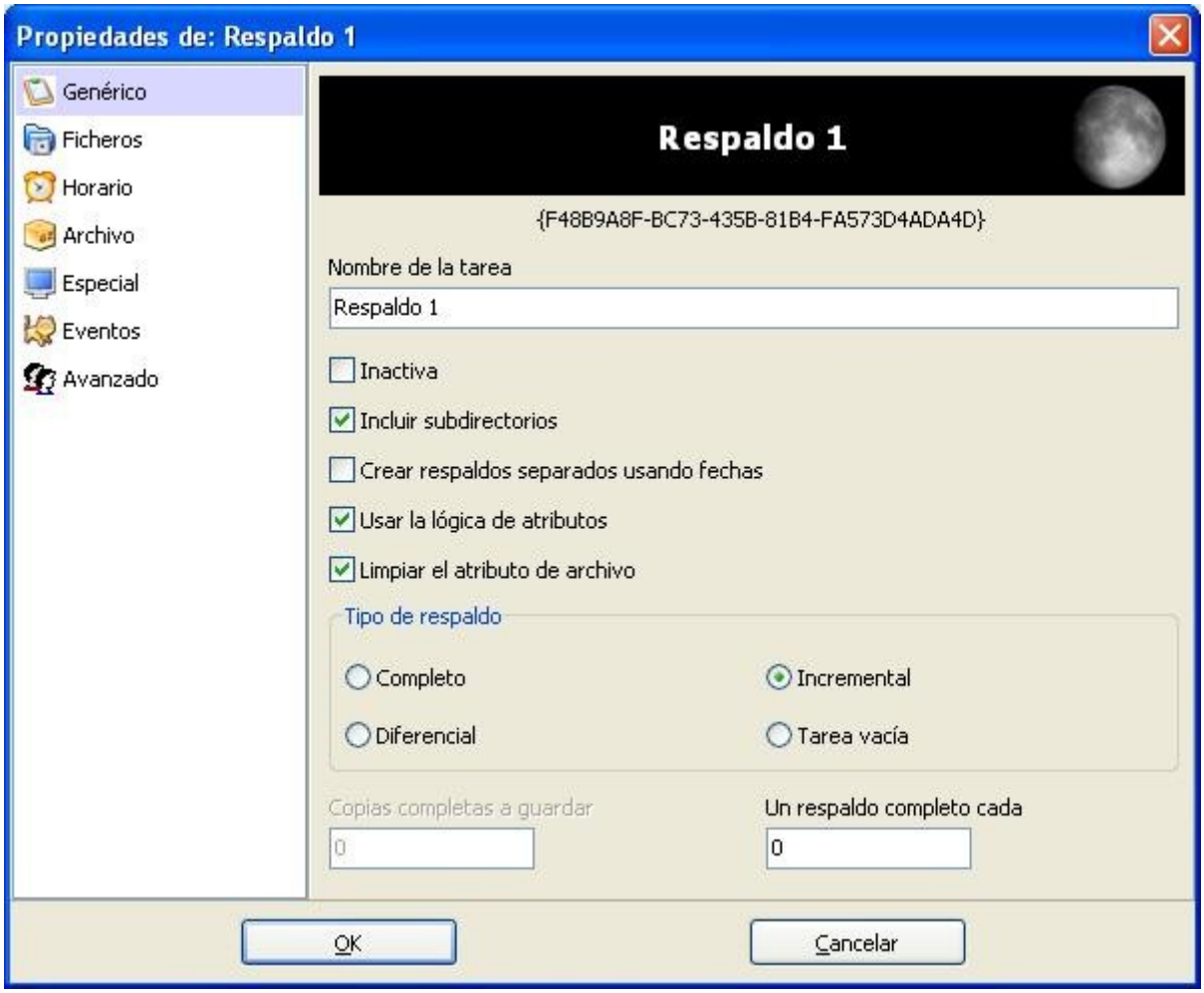


Hemos marcado la opción de forzar apagado en el caso de que la tarea termine y no pueda apagar el equipo porque haya otro programa en ejecución el cliente cerrará el equipo de forma forzada. No lo hemos activado en los clientes porque en algunas ocasiones puede ser que se trabaje con el equipo.



6.6.3 Configuración de la Tarea

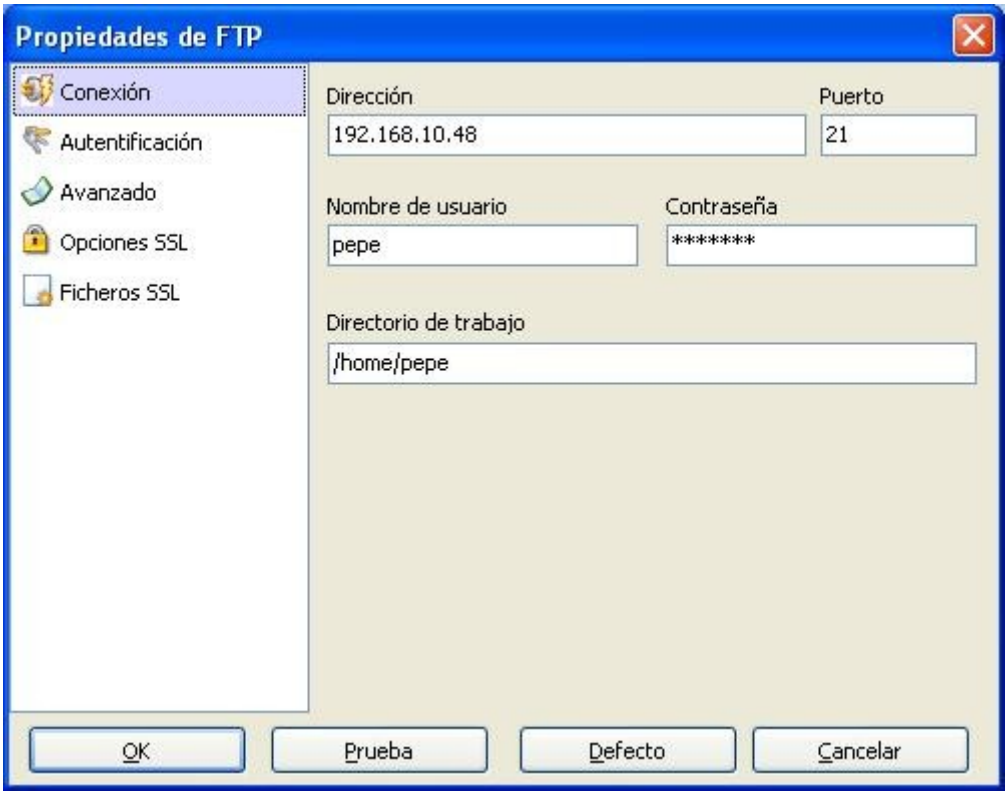
Lo que hacemos es crear una nueva tarea, es muy importante desmarcar la opción de Crear respaldos separados usando fechas. De esta forma se copiará en el mismo directorio y copiará los ficheros más nuevos no teniendo duplicados innecesarios.



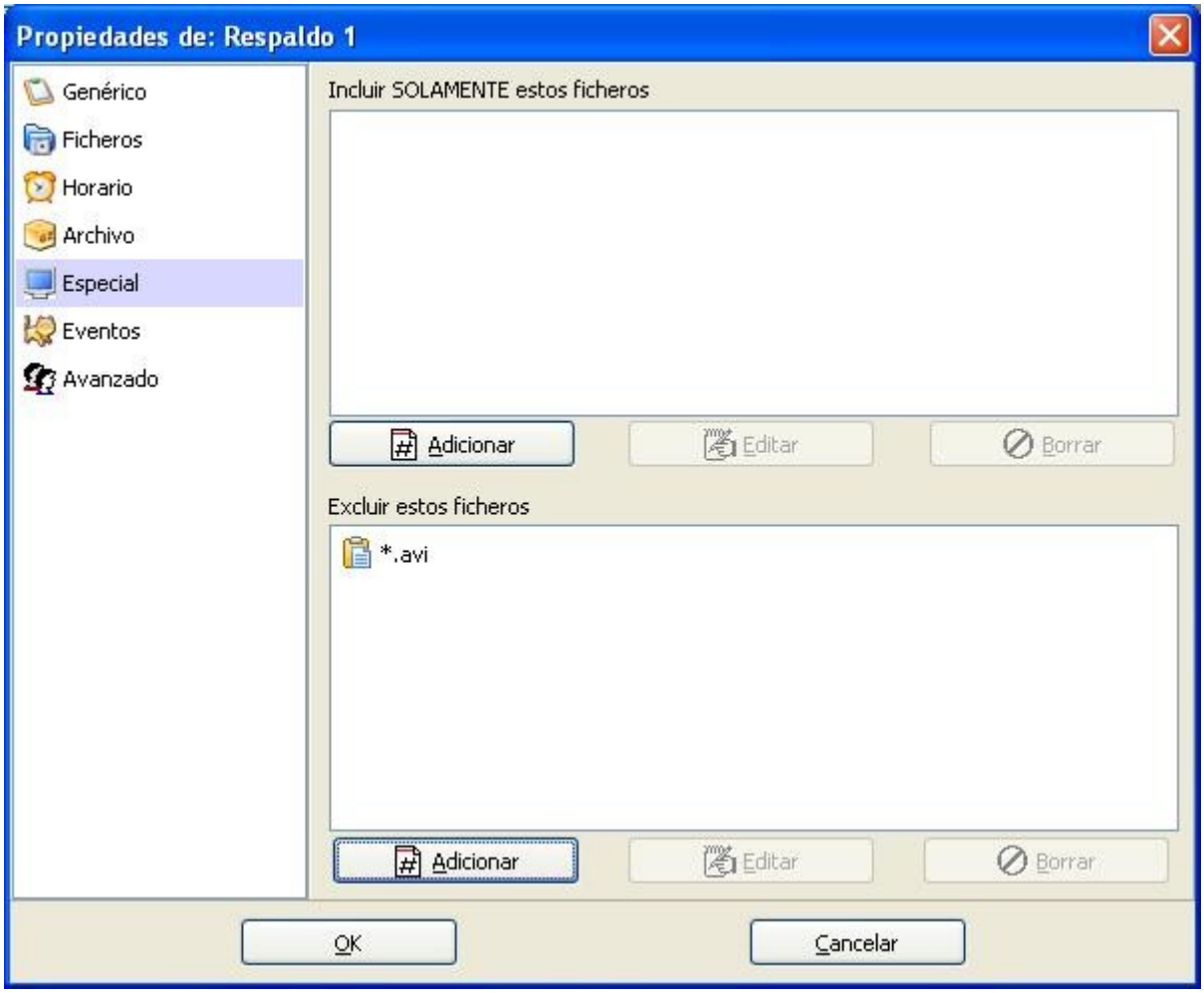
Seleccionemos incremental para que copie los ficheros mas nuevos. Es importante desmarcar la pestaña de Crear respaldos usando fechas ya que luego puede haber incidencias en la copia de cinta. Así creamos backups completos y no nos tendremos que parar a buscar donde esta localizado el fichero en las múltiples carpetas con fechas. También evitaremos duplicados innecesarios como los clientes de correo que algunos tienen 2Gb

En Ficheros en la fuente añadimos el origen que son los datos de lo que queremos hacer copia. Y el Destino que seleccionaremos FTP con los datos del servidor y el usuario de la cuenta de FTP.

En nuestro caso seria 172.26.0.70 el nombre del servidor y el usuario el correspondiente en cada caso con el creado en el ftp



En la opción Especial en Excluir estos ficheros añadimos la serie de extensiones que no se van a copiar. Para ello en la opcion de abajo en Adicionar añadimos la máscara correspondiente o los ficheros que no queramos copiar.

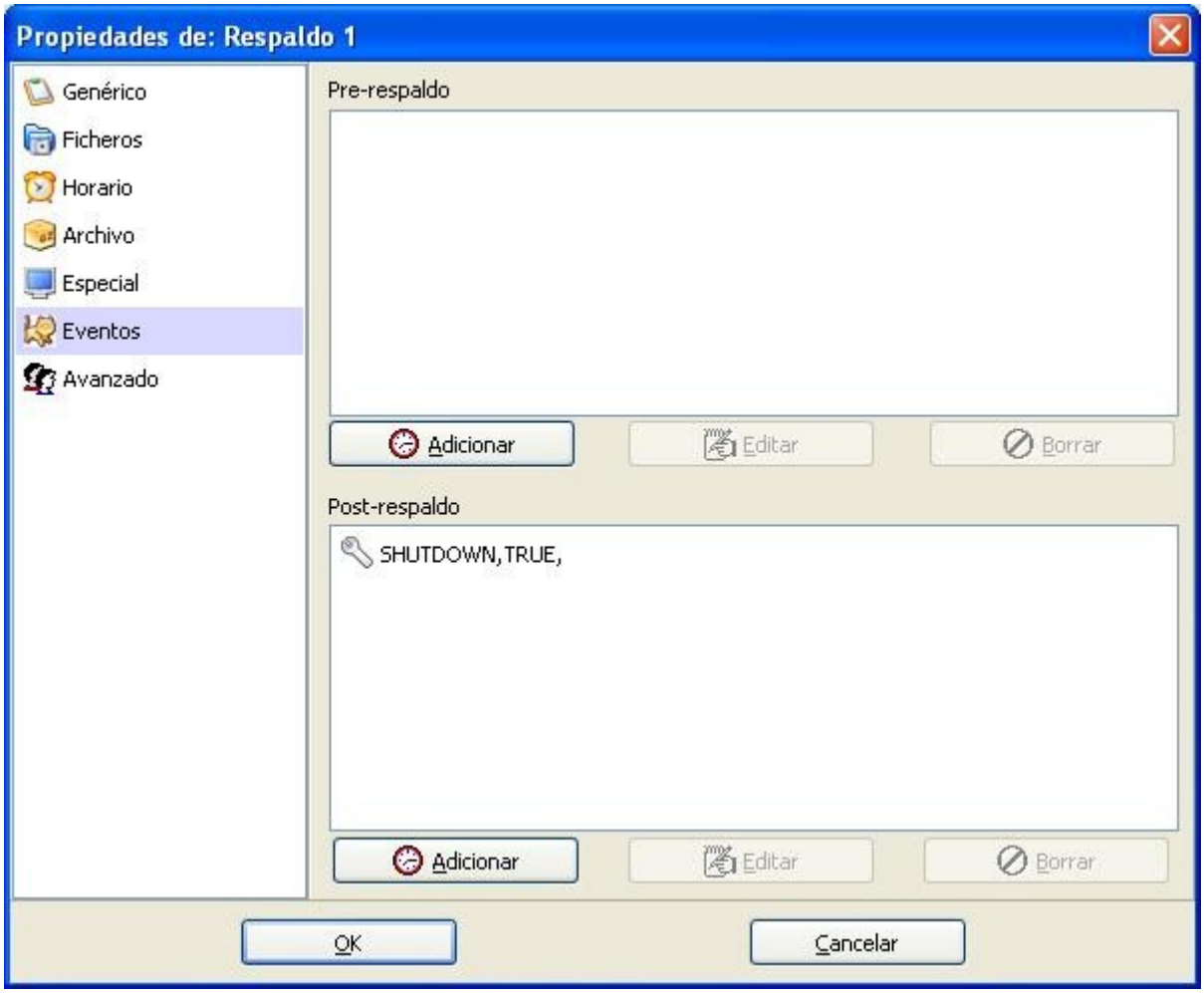


Máscaras de ficheros a no copiar:

.mp3,.avi,*.wmv,*.wma,*.mpeg,*.mpg,*.mov,*.wav

Añadimos la mascará tal y como hemos puesto arriba separando por comas las diferentes extensiones. En el ejemplo siguiente excluimos los mp3.

Por último en la sección Eventos añadimos el evento de Post-respaldo de apagar el equipo.



Esto es ideal si se quiere que las copias se hagan ha cierta hora y no hay nadie delante del equipo.

6.6.4 Configuración Cliente Linux

Aunque el proyecto esta orientado para Windows, aquí especificiamos como realizarla para clientes con Linux.

La forma mas sencilla de configurar el cliente linux es mediante un shellscript que se ejecute periodicamente en el cron de forma similar a como realizamos el backup de cinta.

/usr/local/bin/backup-linux.sh

```
#!/bin/bash
yafc ftp://admin01:admin01@172.26.0.70/home/admin01 < /usr/local/bin/texto1
```

El contenido de texto1 es el siguiente

```
put -f -e -r *.*
exit
```

y para ejecutarlo todos los dias lo editamos con el crontab

crontab -e

```
MAILTO=”informatica@iesgrancapitan.org"
# ejecuta a las 9:30 de lunes a viernes
10 15 * * 1,2,3,4,5 /usr/local/bin/backup-linux.sh
```

7.- Recursos

7.1.- Herramientas hardware

Ordenador IBM eServer xSeries 206

Las características técnicas del ordenador son entre otras.

Procesador: Pentium 4, 3.20Ghz

Memoria: RAM 1280Mb

Discos duros 2x: HD Maxtor 6Y080M0 SATA

LECTOR DE CD: CDROM HL-DT-ST GCR 8482B-PM

UNIDAD DE CINTA: IBM DDS GEN5, DAT 72

CONTROLADORA SCSI ADAPTEC 29320ALP

4 unidades de CINTA DAT 72

7.2.- Herramientas software

Debian Gnu Linux 4.0 etch

Windows 98, XP

Cobian Backup v7 y v8.

Proftpd

Programas de gestión de cintas: tar, mt, cron.

7.3.- Personal

- Usuarios de equipos.
- Responsable de copia.

7.4.- Presupuesto

Este sería un presupuesto aproximado, la infomación para realizarlo ha sido obtenida de Internet.

Costes Material:

IBM Eserver xSeries: 940,21 €

IBM DDS-5 / DAT 72: 410,0 €

Cinta DAT72: 15,38 € Clonica, 91,64 € IBM

Costes Mano de obra:

Costes número de horas: Dias 30 * 6 Horas * 6 € (Minimo) a 38 € (Maximo) : 1080 € - 6840 €

8.- Conclusiones

8.1.- Grado de consecución de objetivos

El El sistema se adecua a la legislación actual de protección de datos realiza una copia en cinta semanalmente y otra de forma diaria,salvo que no haya modificación en los datos. Falta en el aspecto legal que las cintas estén dentro del inventario identificando su localización que debe ser una ubicación diferente a la zona donde están, por ejemplo el departamento o la sala de comunicaciones.

El sistema es automatizado sobre todo en la parte cliente que es la que podía tener mayor complejidad. También el servidor realiza copias de forma automatizada en la cinta, es requisito que el responsable inserte la cinta todos los viernes.

Los respaldos se realizan de forma periódica, aunque en algunos casos la diferencia no es de 5 minutos sino que se realizan junto con otras tareas, esto es debido a que no existe posibilidad de realizarlo a otra hora o porque se este trabajando con el equipo.

Los clientes limitan las extensiones de ficheros a copiar y pueden modificarse cuando se estime necesario, aunque debe hacerse cliente por cliente.

El sistema envia correo de forma periodica, es posible que al realizar la copia el equipo se apague o reinicie y no lo envie hasta el dia siguiente por la mañana. Existe la posibilidad de que falle la red y no pueda enviar correo con lo cual la no recepción del correo ya es un sintoma de que el sistema no esta funcionando correctamente.

La solución esta basada en software libre o software de fuente abierta. Cobian utiliza la licencia Mozilla y no se esta haciendo uso comercial del mismo.

8.2.- Problemas encontrados

- Problemas la dificultad de realizar un trabajo en grupo.
- Desde el aula no podemos enviar correo al exterior.
- Hemos de evitar el bloqueo de relay o dominio no existente, para solventarlo utilizamos una cuenta ficticia del dominio y una cuenta existente en el dominio por ejemplo **informatica@iesgrancapitan.org**.
- Existe la posibilidad de redundancia de datos, en el caso de que cambien la ubicación dentro de la carpeta de la copia de seguridad a

otra subcarpeta de esta.

- Hemos optado por utilizar estas opciones porque es la menos costosa, es la que tiene menos mantenimiento, y es la mas sencilla de implementar.

8.3.- Futuras mejoras

- El servidor debería de llevar un sai, para que en caso de que se vaya la luz de tiempo al hacer una copia.

- El servidor debe llevar un mantenimiento, cada vez que finalice una evaluación debería chequearse el sistema de ficheros, además de borrar si es necesario las copias de seguridad del /home y crear un backup completo para tener información actualizada. De esto debe encargarse el administrador de copias.

- Deben borrarse los logs del proftpd localizados en */var/log/proftpd* periodicamente ya que es muy probable que ocupen bastante espacio.

- Si se quiere añadir un nuevo cliente solo es necesario añadir un usuario con adduser y configurar el equipo cliente.

- Para preservar la seguridad se deben de cambiar las claves de los usuarios por otras mas seguras.

9.- Referencias / bibliografía

- Antonio Villalón. "Seguridad en Unix y Redes". Versión 1.2 Digital - Open Publication License v.10 o Later. 2 de Octubre de 2000. http://www.kriptopolis.com
- http://es.tldp.org/Manuales-LuCAS/doc-como-seguridad-fisica/COMO-seguridad-fisica.html
- Ley de Protección de Datos: La nueva LORTAD. Editorial Díaz Santos. Madrid. 2000
- Ley Orgánica de Protección de Datos de Carácter Personal 13-12-1999, num. 15/1999 BOE 14-12-1999, num. 298 [pag. 43088].
- http://www.agpd.es
- http://www.map.es
- http://www.adso.net/AdsoUnidosis/legal/index.htm
- http://www.aui.es/biblio/documentos/proteccion_datos/resumen/resumen.htm
- http://www.agendaactiva.es/guia_lopd/
- Herramientas de backup: http://www.linux.org/apps/all/Administration/Backup.html
- Amanda: http://www.servitux.org/view.php/page/amanda
- Unison: http://www.cis.upenn.edu/~bcpierce/unison/docs.html
- Bacula: http://www.bacula.org/dev-manual/Contents.html
- Cobian: http://www.educ.umu.se/~cobian/cobianbackup.htm
- Uso de la cinta: http://www.linux-party.com/modules.php?name=News&file=article&sid=8
- Uso de Crond: http://www.linux-es.org/node/246
- Proftpd: http://www.proftpd.org/docs/example-conf.html
- PostFix: http://www.postfix.org/docs.html
- Seguridad Informática para empresas y particulares Editorial McGraw Hill [Ed. 2006].

10.- Anexos

10.1 Licencia

Este documento se distribuye bajo la licencia Creative Commons

http://es.creativecommons.org/licencia/