

Utilidades para el mantenimiento de equipos informáticos

TEMA 8

Juan Carlos Moreno
Montaje y Mantenimiento de Equipos

INDICE

- 8.1 Clonación de equipos.
- 8.2 Utilidades para la compresión/descompresión de archivos y backup/restauración de sistemas.
- 8.3 RAID.
- 8.4 Antivirus.
- 8.5 Utilidades para el mantenimiento y reparación de los sistemas informáticos.



En este tema:

- Conocerás la importancia de la seguridad en un sistema informático.**
- Aprenderás a gestionar la seguridad de sistemas informáticos domésticos o de una pequeña/mediana empresa.**
- Aprenderás a utilizar herramientas para la clonación de equipos.**
- Conocerás los riesgos a los que están expuestos los sistemas informáticos en cuestión de malware y las herramientas a utilizar para proteger y recuperar los mismos.**

Conceptos básicos del tema:

- Debian
- Distribución
- Encriptación
- Imagen ISO
- Live CD/DVD
- Malware
- Overload
- Paridad
- SMART
- Privacidad
- Ratio de compresión
- Stripe



Ra-Ma[®]

8.1 Clonación de equipos.

Juan Carlos Moreno

Montaje y Mantenimiento de Equipos

¿Cómo conseguir Parted Magic?

1. Primero tienes que bajarte la ISO del CD Rom desde www.partedmagic.com o utilizar la versión del CD Rom de recursos (esta puede no ser la última versión).
2. Una vez descargada habrá que descomprimirla si está comprimida.
3. El último paso es grabar la imagen ISO a un CD (Un CD basta pues son menos de 100 MB).

Tu CD grabado estará disponible para arrancar desde el en un equipo.

Hostname: PartedMagic
 Linux Kernel: 2.6.29.2-pmagic
 CPU Details: i686, 2010 (MHz)
 CPU History: [graph]
 CPU Usage: 1% [graph]
 RAM Usage: 173.77MiB (17%)
 Available RAM: 997.84MiB

 Processes: 110 Running: 1
 (top 5 sorted by CPU usage)

NAME	PID	CPU%	MEM%
lxpanel	3297	0.41	0.81
Xorg	3261	0.20	1.09
mount-gtk	4726	0.00	0.83
pmagic_mount	4720	0.00	0.12
bash	4618	0.00	0.16

 Processes: (top 5 sorted by MEM usage)

NAME	PID	CPU%	MEM%
Xorg	3261	0.20	1.09
pcmanfm.bin	3364	0.00	0.99
xfce4-screensho	3919	0.00	0.97
mount-gtk	4726	0.00	0.83
notification-da	3332	0.00	0.81

 Tuesday, 19 May 2009, 14:01
 System Uptime: 0h 10m 16s

Parted Magic
 Partitioning Tool

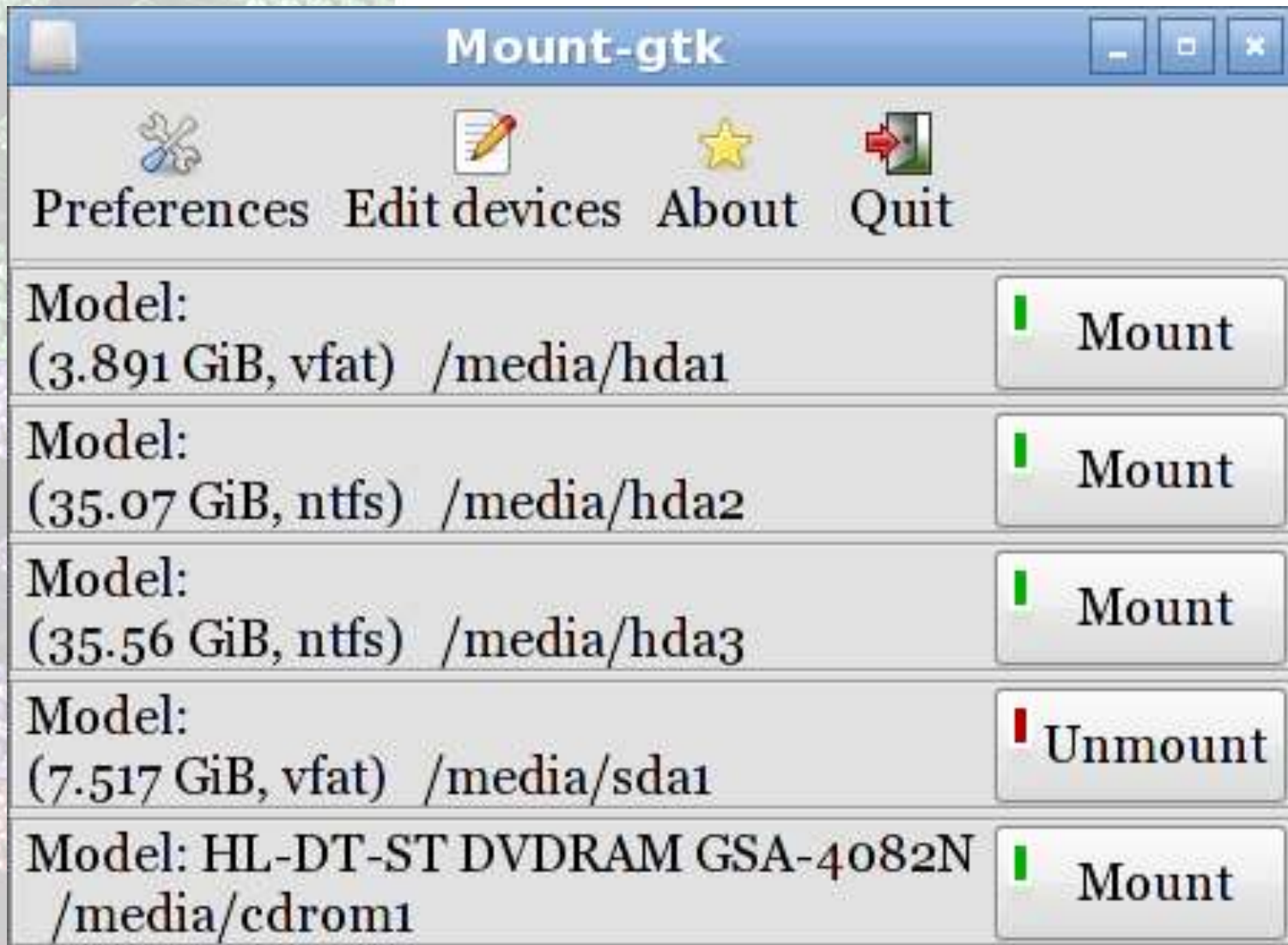
System Tools menu items:
 Erase Disk
 G4L
 GParted Partition Editor
 GSmartControl
 Grsync
 ISO Master
 Make Parted Magic USB
 Partition Image
 PhotoRec
 Saving Parted Magic
 System Profiler and Benchmark
 TestDisk
 TrueCrypt
 UDPCast Disk Cloning
 Xorg Configure
 Xvesa Configure

Taskbar: [sdb1] [Mount-gtk] 14:01

- Escritorio de la distribución Parted Magic

Ejecutar Parted Magic

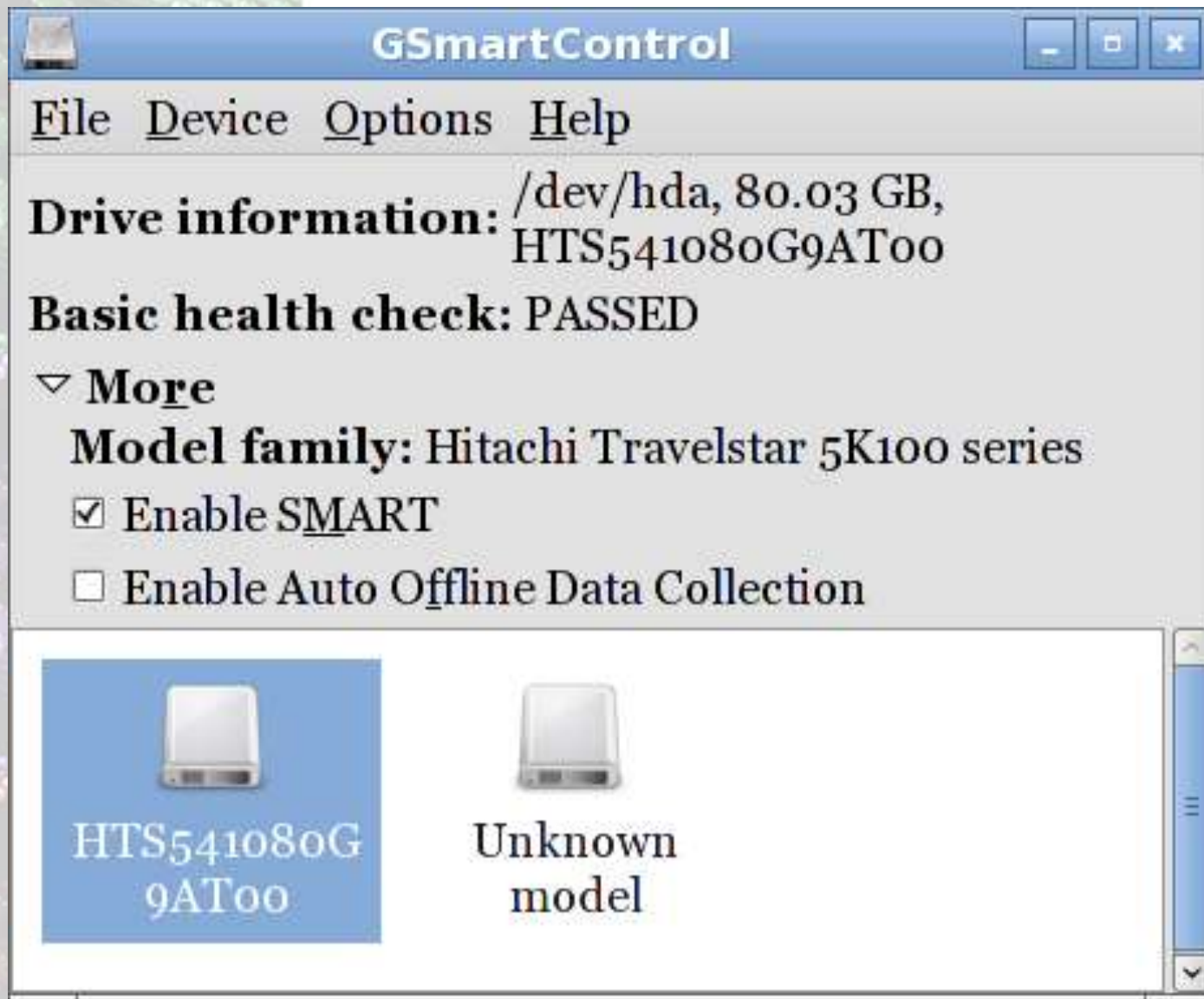
- Configurar el equipo para arrancar desde la unidad óptica.
- Una vez verificado este punto, introduce el CD en el lector y enciende el equipo.
- La mejor opción de arranque de Parted Magic es cargar el sistema en RAM (más rápida).



- **Herramienta Mount-gtk**

Herramientas de Parted Magic

- G4L. Ghost for linux.
- Gparted: Herramienta para realizar particionamiento.
- Partition Image: Herramienta para clonar particiones
- Make Parted Magic USB: Herramienta para hacer que funcione Parted Magic desde un dispositivo USB.
- Hardinfo. El Everest de Linux.
- GSmartControl.
- XArchiver. Herramienta para realizar copias de seguridad.
- Mount-gtk. Monta y desmonta dispositivos en el sistema.
- Y muchas más.



- Herramienta GSmartControl



Ra-Ma®

8.1 Clonación de equipos.

8.1.1 Clonación de particiones y de discos

Juan Carlos Moreno
Montaje y Mantenimiento de Equipos

¿Qué es una clonación?

Una clonación es una copia exacta de algo.
En nuestro caso será una copia exacta de un disco o una partición.

Para clonar un equipo deberás de hacer una réplica del disco/s y tendrás que asegurarte que **EL HARDWARE ES EL MISMO.**

Las clonaciones

- Sin sistema operativo → Basta con clonar las particiones
- Con sistema operativo → Clonar todo el disco. De esa manera se clonará el sector de arranque y se estará seguro de que si se sustituyen los discos el sistema funcionará perfectamente.
- Cuando se quiera volver el disco o partición a su estado anterior bastaría con restaurar el disco con la imagen creada.



Ra-Ma®

8.1 Clonación de equipos.

8.1.2 Clonación de particiones

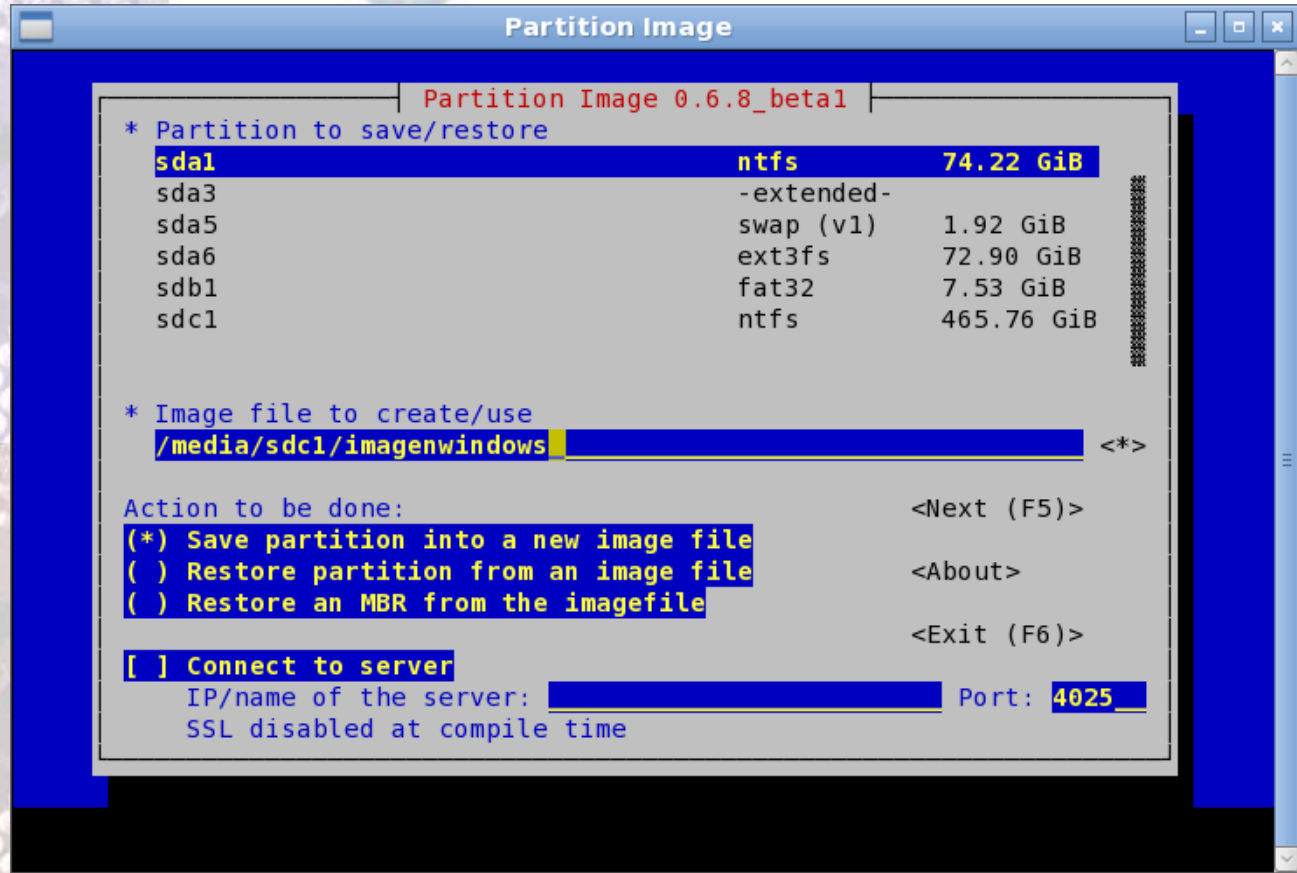
Juan Carlos Moreno

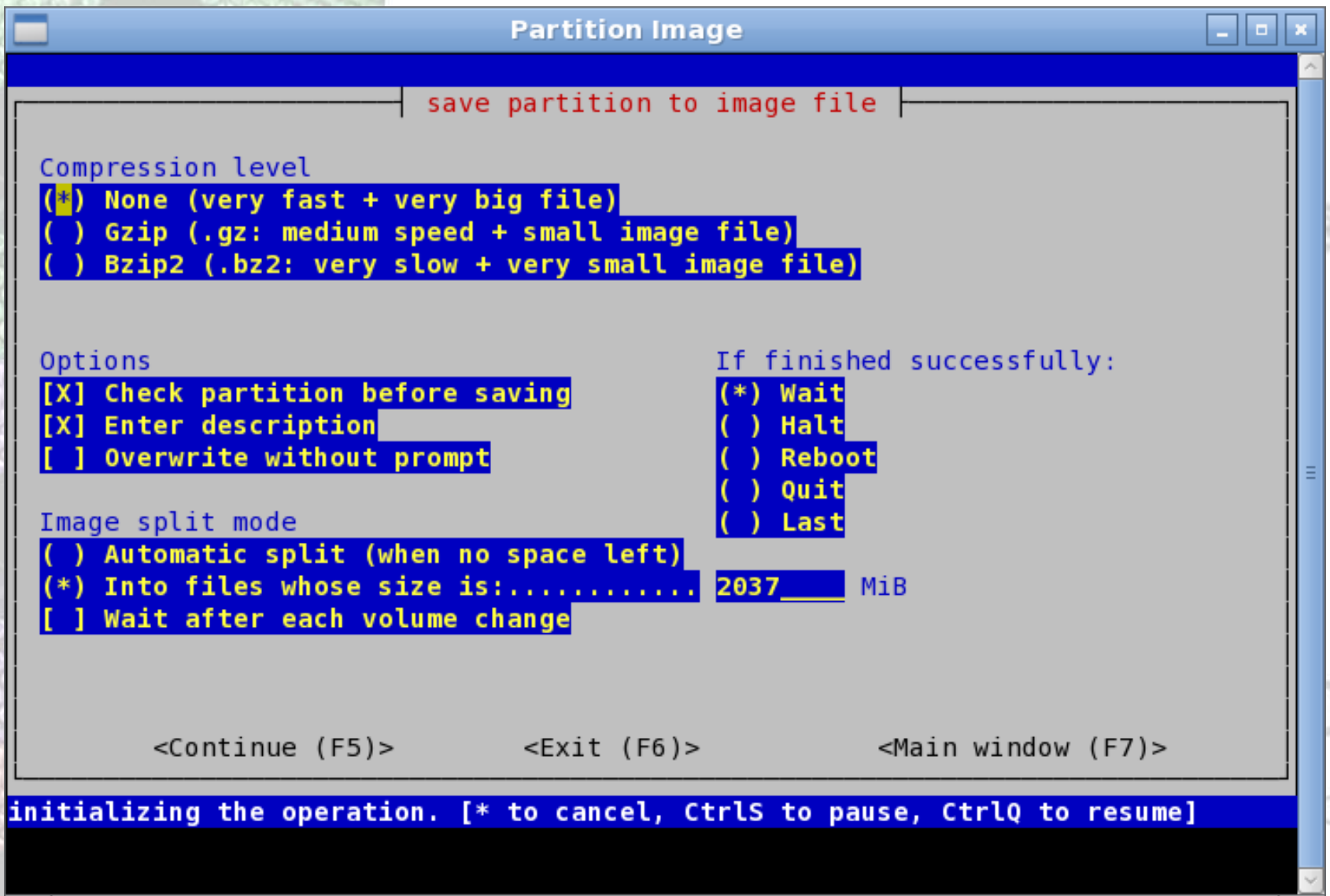
Montaje y Mantenimiento de Equipos

Creación/recuperación de una partición con Partition Image

Paso 1 Creación de la imagen

- El primer paso a dar es la elección de la partición a clonar.





- Paso 2 Elección de las opciones del proceso

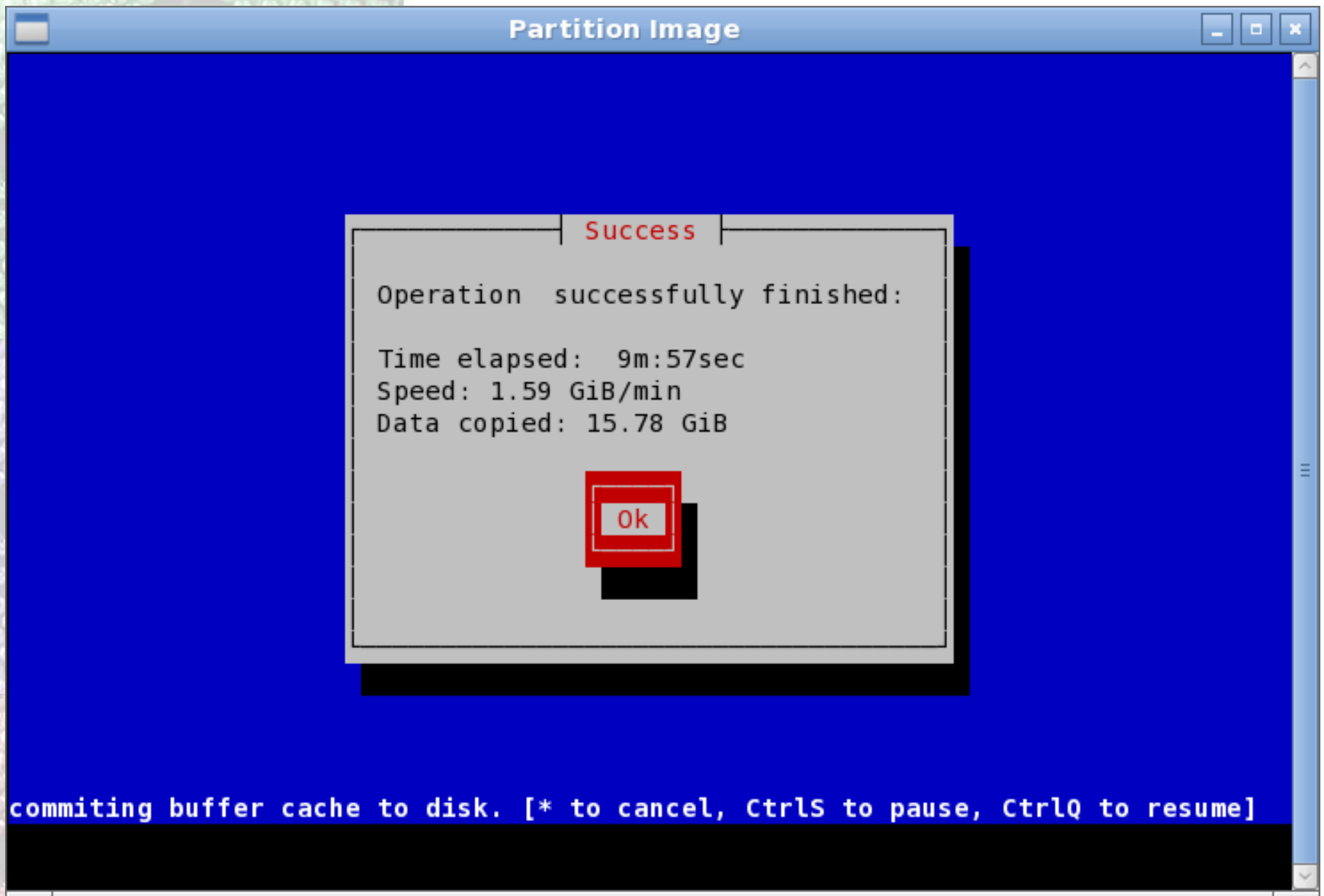
```
Partition Image
save partition to image file
Partition to save:...../dev/sda1
Size of the Partition:.....74.22 GiB = 79694705664 bytes
Current image file:...../media/sdc1/imagenwindows.000
Image file size:.....356.40 MiB
Available space for image:...465.21 GiB = 499516481536 bytes
Detected file system:.....ntfs
Compression level:.....None

Time elapsed:.....13sec
Estimated time remaining:.... 9m:40sec
Speed:.....1.60 GiB/min
Data copied:.....354.00 MiB / 15.78 GiB

2% 2 %

copying used data blocks [* to cancel, CtrlS to pause, CtrlQ to resume]
```

- **Proceso de creación de la imagen**



- **Proceso de creación de una imagen completado.**

• Paso 3 Restauración de la imagen

Hostname: PartedMagic
Linux Kernel: 2.6.29.2-rtmagic
2010 (MHz)

Partition Image

Partition Image 0.6.8_beta1

* Partition to save/restore

sda1	ntfs	74.22 GiB
sda3	-extended-	
sda5	swap (v1)	1.92 GiB
sda6	ext3fs	72.90 GiB
sdb1	fat32	7.53 GiB
sdc1	ntfs	465.76 GiB

* Image file to create/use

/media/sdc1/imagenwindows.000 <*>

Action to be done:

- Save partition into a new image file <Next (F5)>
- Restore partition from an image file <About>
- Restore an MBR from the imagefile <Exit (F6)>

Connect to server

IP/name of the server: Port:

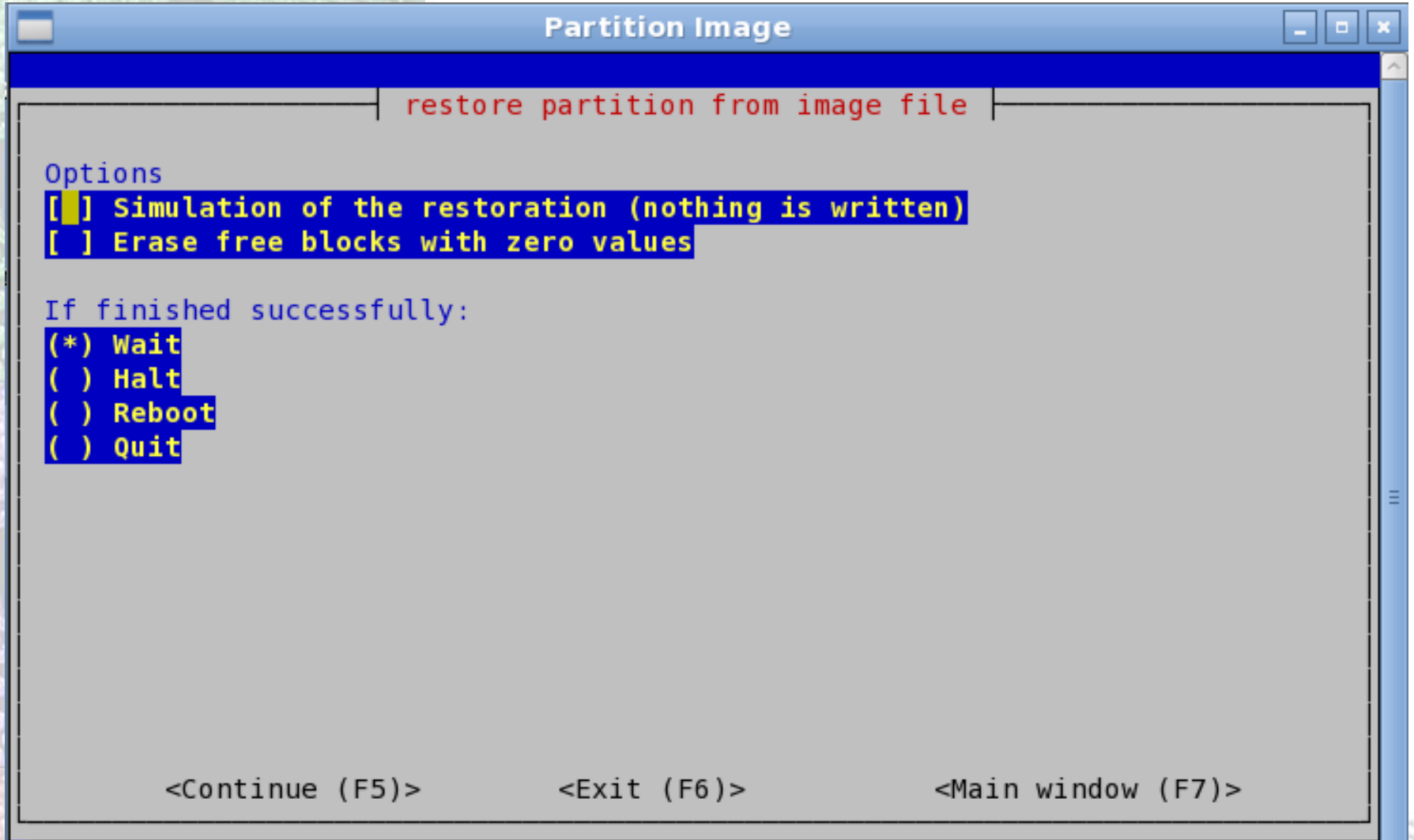
SSL disabled at compile time

imagenwindow imagenwindow imagenwindow
s.005 s.006 s.007

28 visible items (0 hidden) 15 visible items (0 hidden), Free space: 449.8 GB (Total: 465.8 GB)

Start Network

[ROX... sdb1 [media] media sdc1 Partiti... 14:29



- Una vez elegido la imagen a restaurar y el disco se eligen las opciones del proceso y se continua con el mismo

```
Time elapsed: 9m:33sec  
Speed: 1.65 GiB/min  
Data copied: 15.78 GiB
```



Ok

- El proceso finalizará mostrando un resumen de los datos copiados, velocidad y tiempo empleado.
- Ya solamente queda probar el sistema para corroborar que el proceso se ha realizado correctamente.



Ra-Ma®

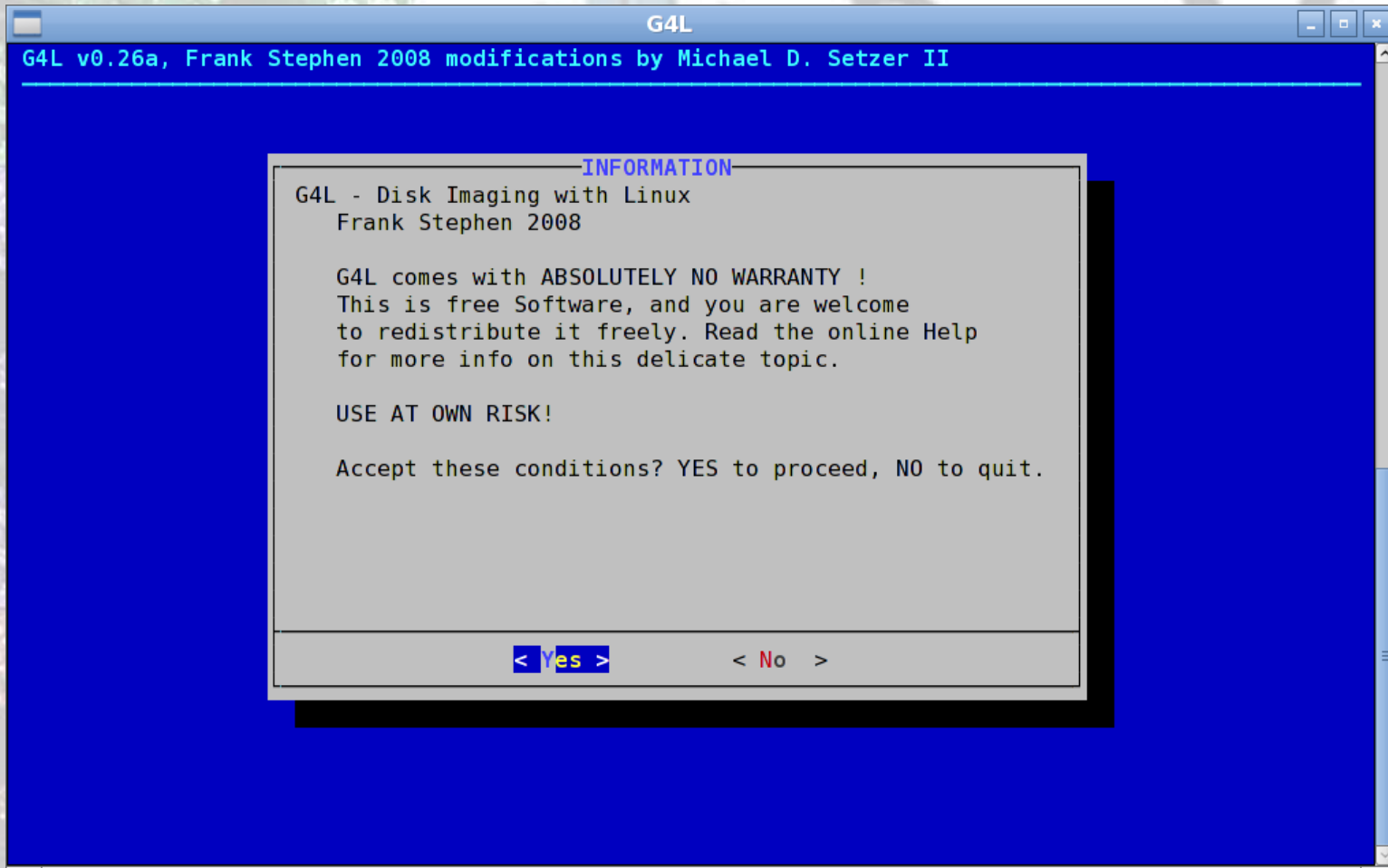
8.1 Clonación de equipos.

8.1.3 Clonación de discos

Juan Carlos Moreno

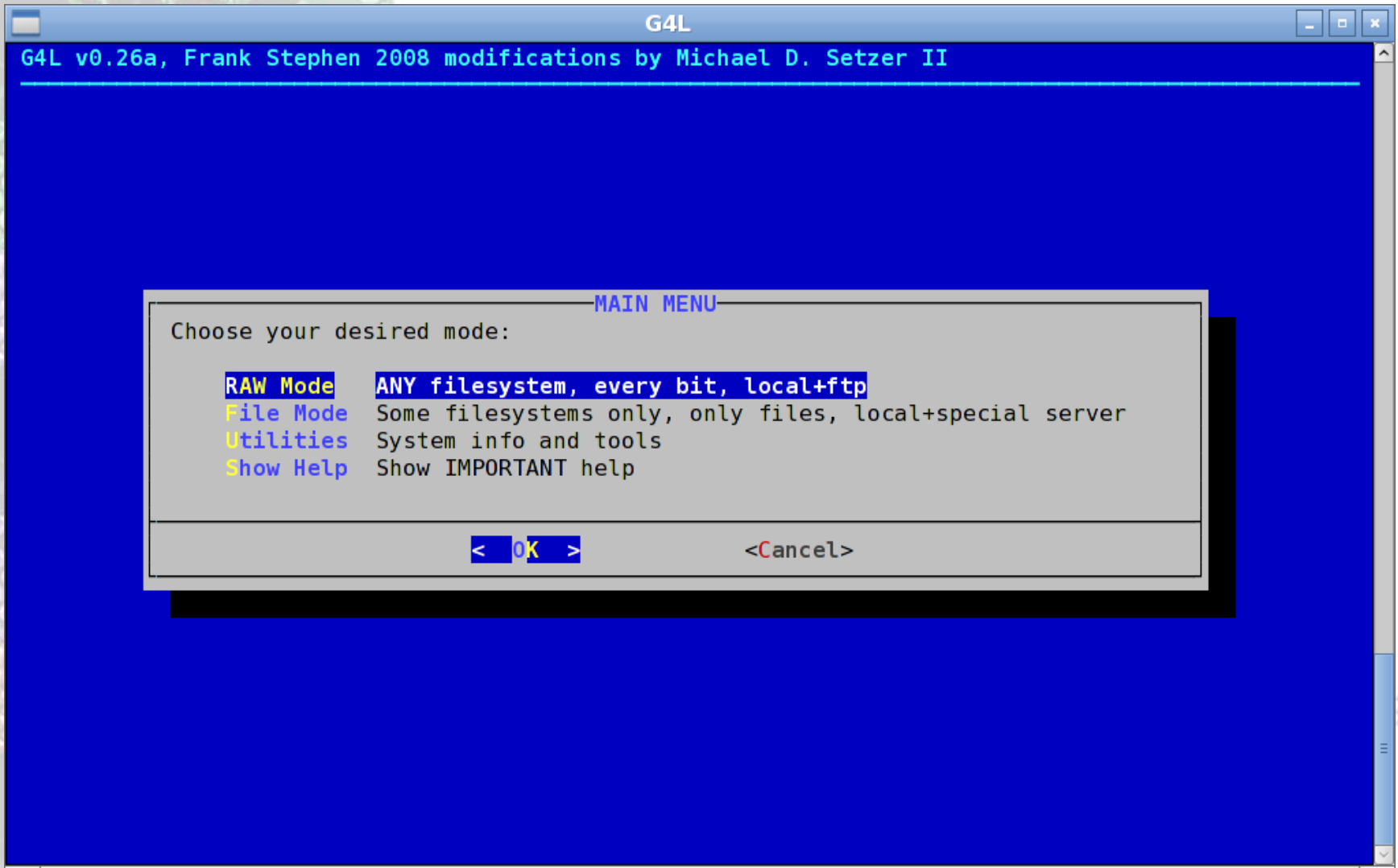
Montaje y Mantenimiento de Equipos

Ejercicio práctico: Creación y recuperación de un disco con G4L

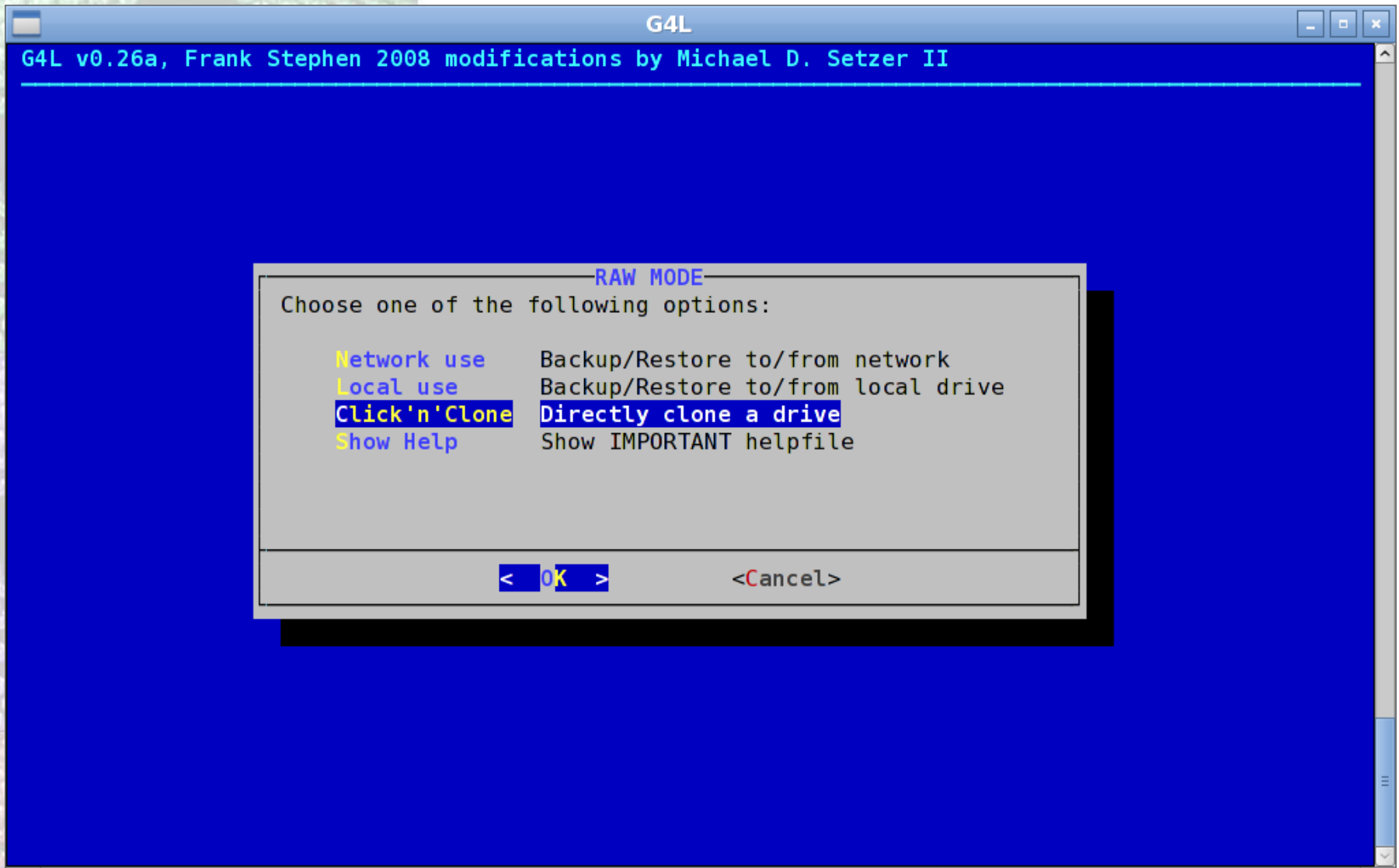


- **Herramienta Ghost for Linux**

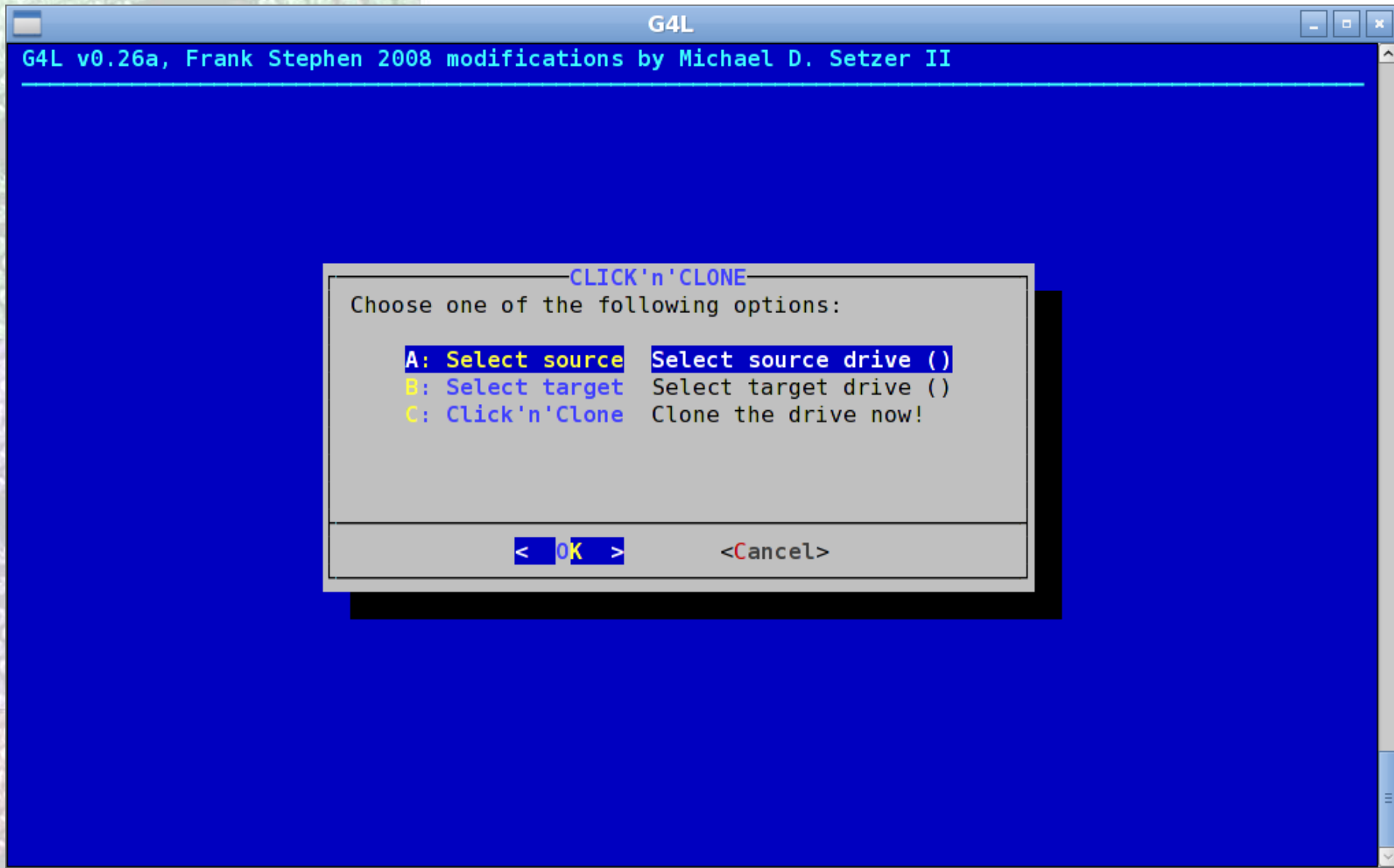
- Paso 1 Creación de la imagen



- Para la réplica de un disco se utilizará el modo RAW para copiar toda la información (todos los bits del disco).



- Elección de las opciones del modo crudo o raw. Se elige click'n'clone porque se va a hacer la imagen en un disco externo.



- Paso 2 **Elección del disco a clonar**

G4L

G4L v0.26a, Frank Stephen 2008 modifications by Michael D. Setzer II

SELECT SOURCE

Choose source drive to clone.
(Use Space Bar)

Select from:

- (*) **hda** **78150744--DISK**
- () **hda1** -----_4088511--Compaqdiagnostics
- () **hda2** -----36772785--HPFS/NTFS
- () **hda3** -----37286865--HPFS/NTFS
- () **sda** -----7897087--DISK
- () **sda1** -----7897056--W95FAT32

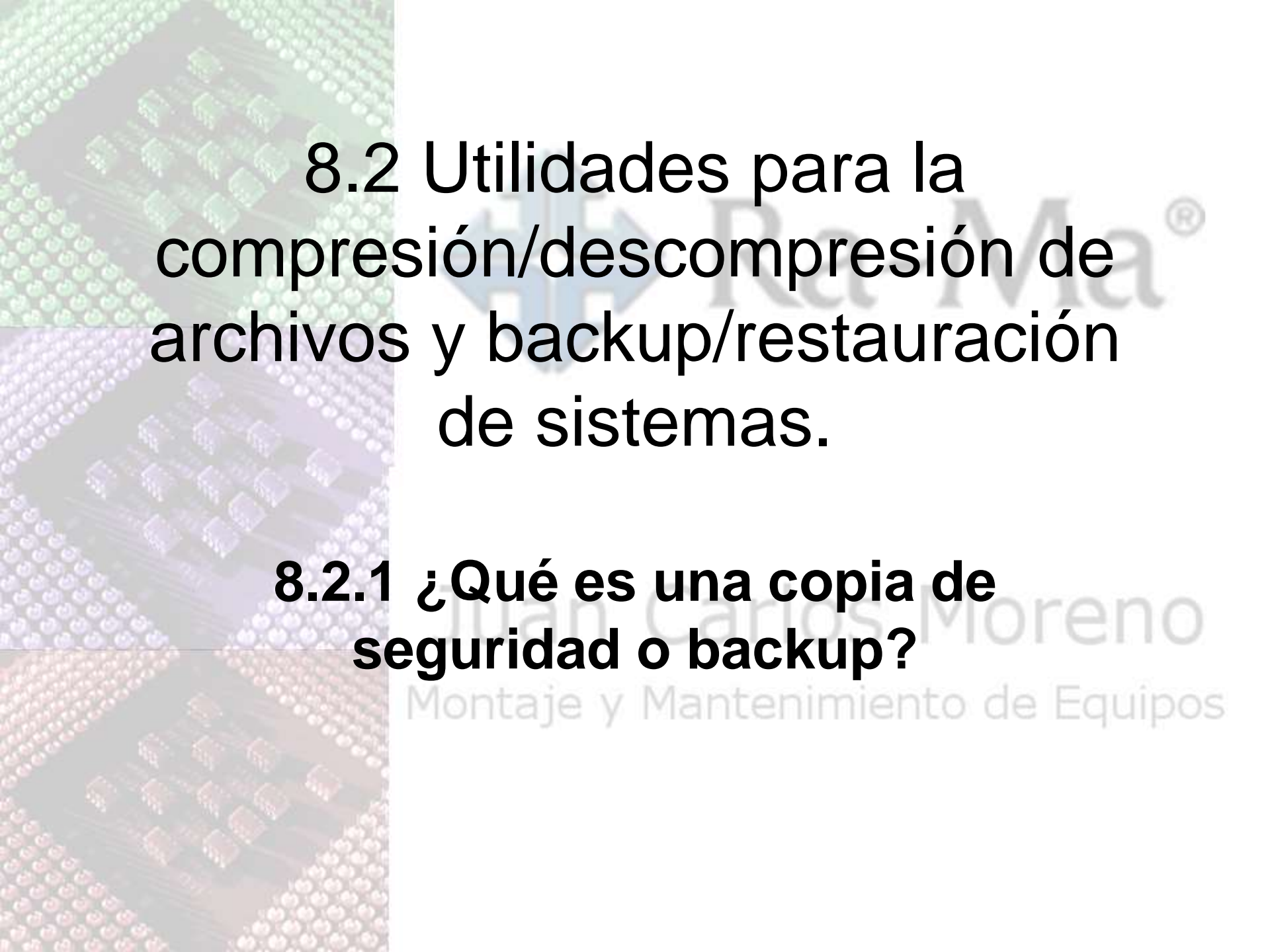
< **OK** >

<Cancel>

- Una vez elegido el disco a clonar deberemos de elegir el disco destino.
- El disco destino deberá de tener como mínimo la misma capacidad del disco origen.
- El resultado de este proceso es una réplica del disco que queríamos clonar.
- Se aconseja para la clonación discos de la misma capacidad.

RECUPERACIÓN DE UN DISCO O RESTAURACIÓN DE LA IMAGEN

- El proceso de restauración del disco es análogo al anterior.
- En este caso seleccionaríamos los discos origen y destino y haríamos la copia.
- Una vez realizado esto, ya solamente queda probar el sistema para corroborar que el proceso se ha realizado correctamente.



8.2 Utilidades para la compresión/descompresión de archivos y backup/restauración de sistemas.

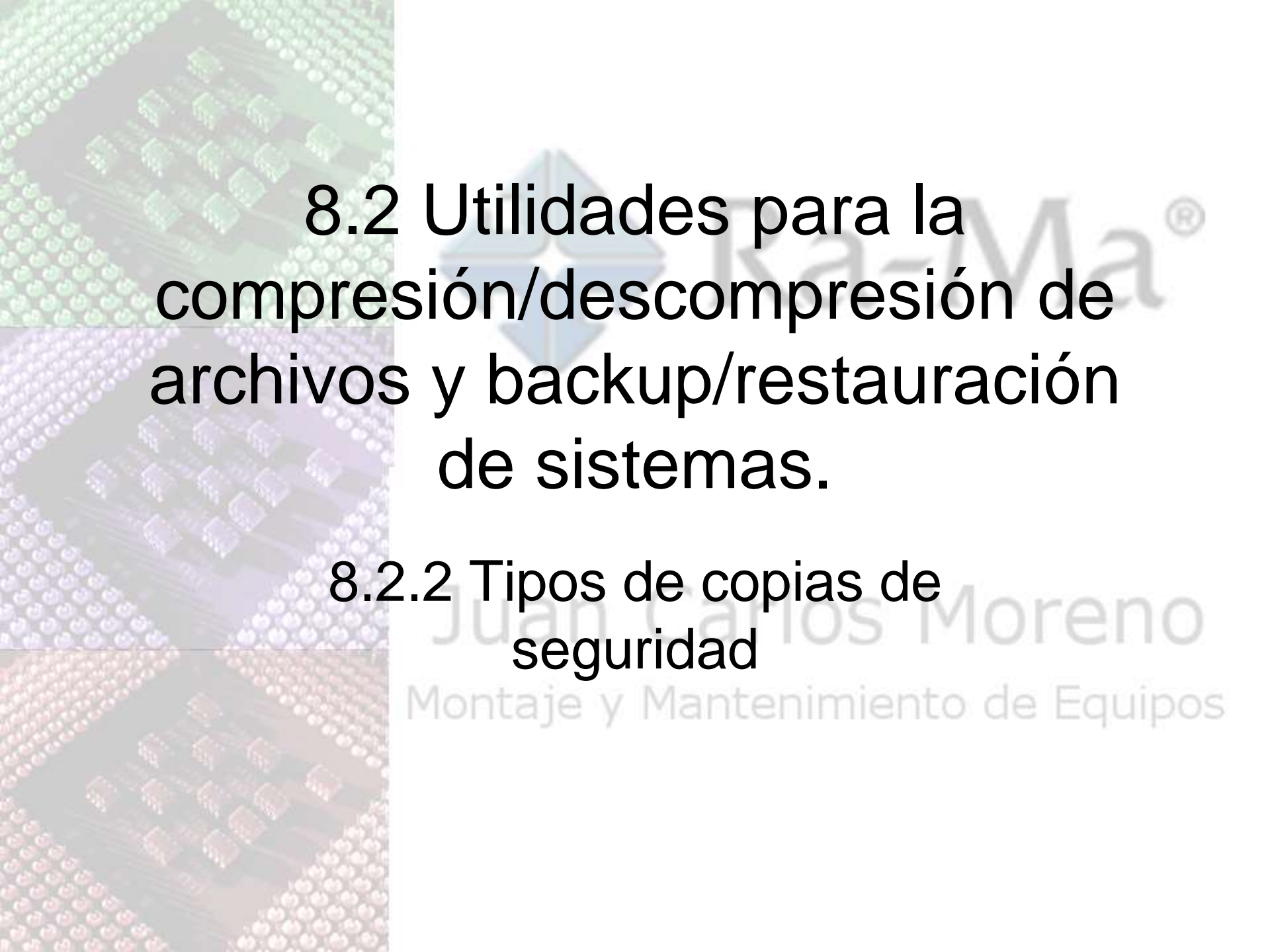
8.2.1 ¿Qué es una copia de seguridad o backup?

Juan Carlos Moreno
Montaje y Mantenimiento de Equipos

La copia de seguridad o backup

- Una copia de seguridad es hacer una duplicación de todo o parte del sistema.
- En caso de un fallo en el sistema se procederá a ejecutar el proceso de restauración del mismo.
- Las copias de seguridad no deberían de estar muy espaciadas en el tiempo.

Quando hay un fallo en el sistema se pierde la información existente entre el último backup y el momento del fallo.



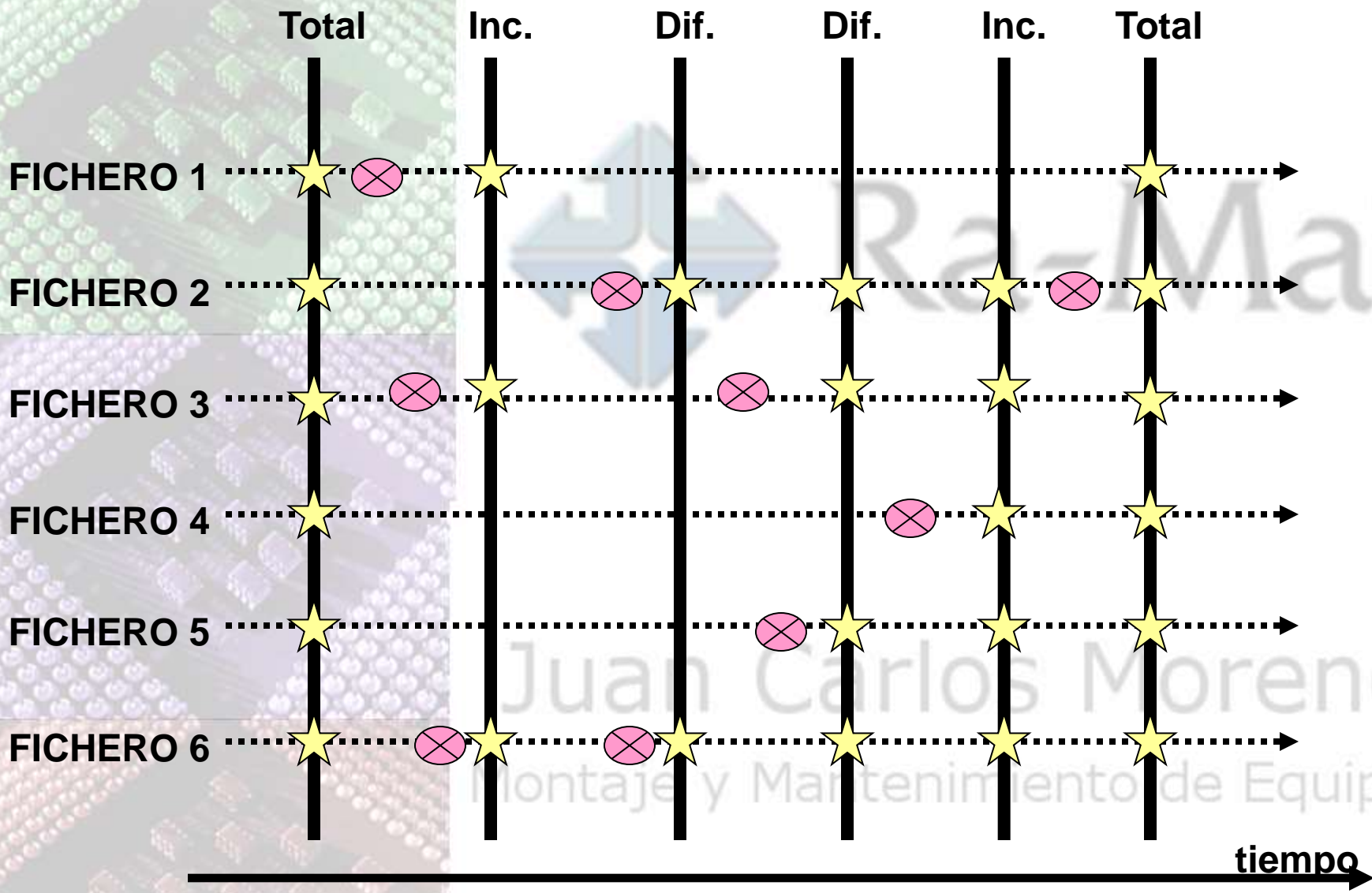
8.2 Utilidades para la compresión/descompresión de archivos y backup/restauración de sistemas.

8.2.2 Tipos de copias de seguridad

Juan Carlos Moreno
Montaje y Mantenimiento de Equipos

Tipos de copias de seguridad

- **Total o completa:** Es aquella que copia toda la información almacenada en el sistema. Desactiva el atributo de modificado a todos los archivos.
- **Incremental:** Copia solo los archivos que tienen el atributo de modificado activado. Una vez realizada la copia de seguridad ese atributo se desactiva.
- **Diferencial:** es igual que la incremental, lo único que el atributo modificado no se desactiva (este atributo se desactivará cuando se haga una copia de seguridad incremental o completa).

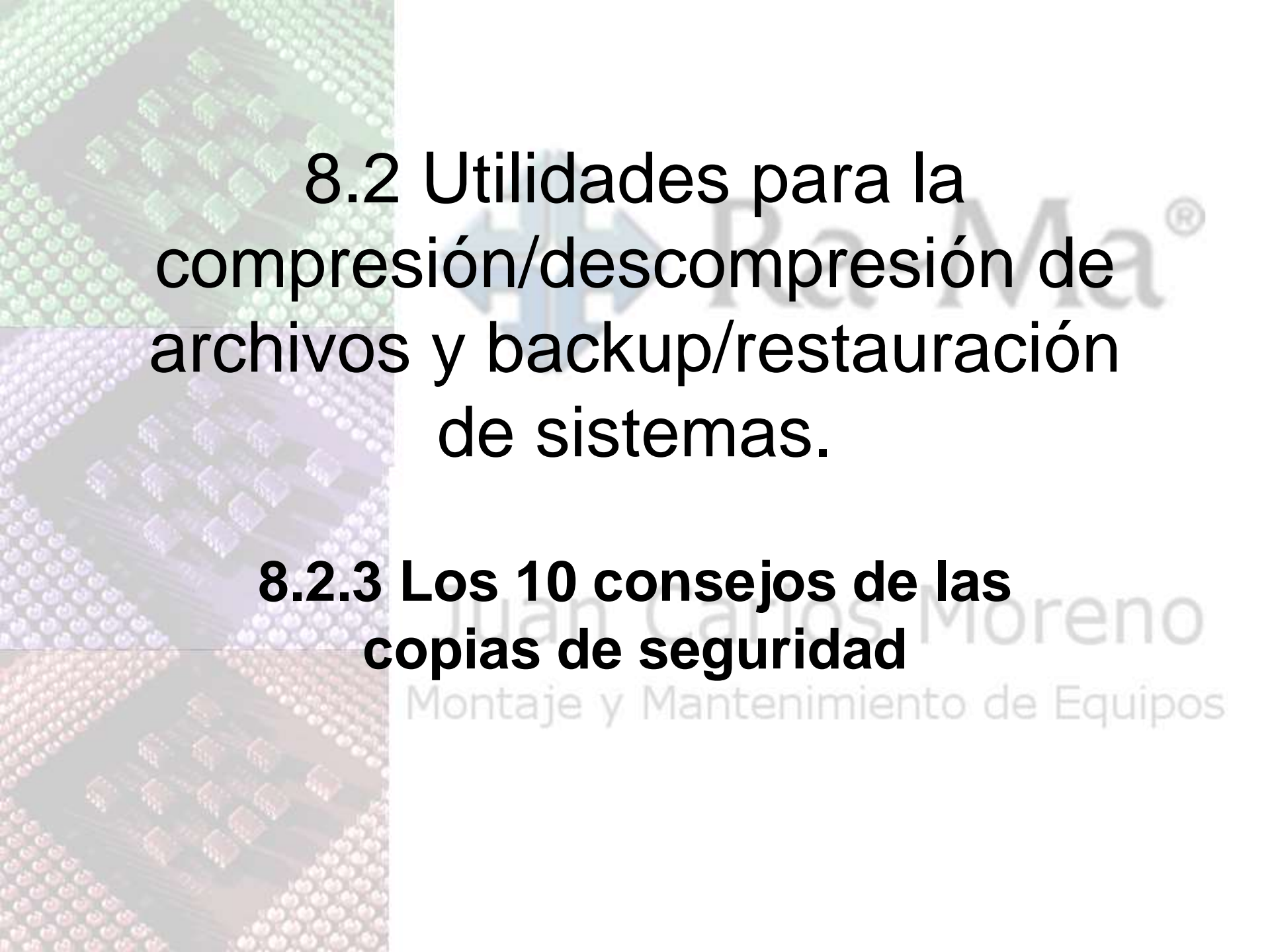


Ra-Ma[®]
 Juan Carlos Moreno
 Montajes y Mantenimiento de Equipos

Dif. = Diferencial
 Inc. = Incremental

El proceso de restauración

1. Restablecer la última copia de seguridad total.
2. Posteriormente se restauran desde la más antigua hasta la más moderna aquellas copias de seguridad incrementales desde la última exportación total.
3. Por último restablecer la última copia de seguridad diferencial realizada, siempre y cuando sea ésta la última copia realizada (no existe ninguna copia incremental ni total posterior).



8.2 Utilidades para la compresión/descompresión de archivos y backup/restauración de sistemas.

8.2.3 Los 10 consejos de las copias de seguridad

Juan Carlos Moreno
Montaje y Mantenimiento de Equipos

Los 10 consejos de las copias de seguridad (I)

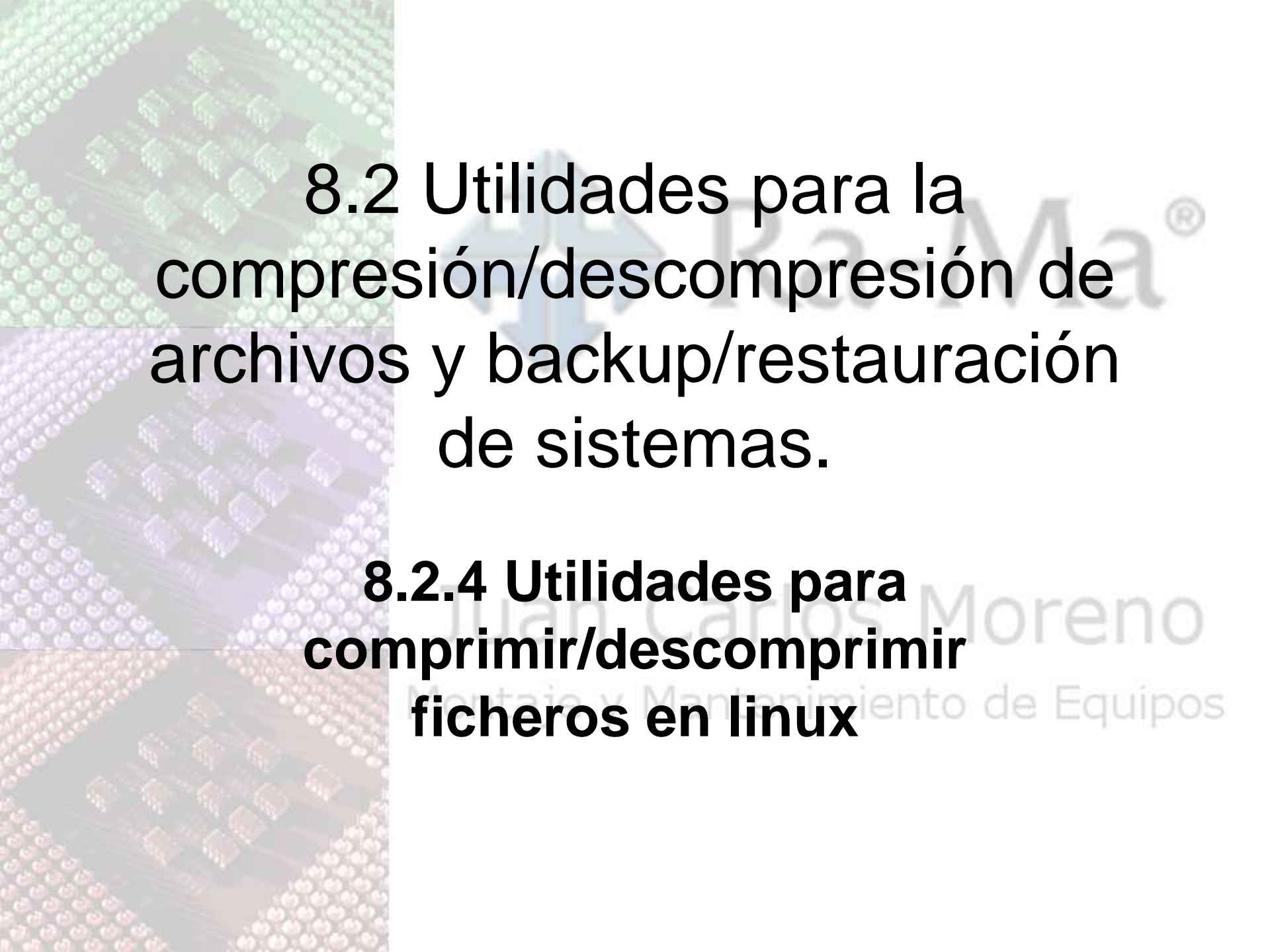
1. Realizar copias de seguridad de cuanto se pueda, como mínimo de los ficheros de datos.
2. Los backups deben ser comprobados para saber si funcionan. Deberán también de estar correctamente etiquetados y ordenados.
3. Mantener los backups en sitios diferentes a los que se encuentren los datos.
4. Realizar backups incrementales o diferenciales si no es posible realizar siempre backup total.
5. No demorar en el tiempo los backups.

Los 10 consejos de las copias de seguridad (II)

6. Automatizar los backups.
7. No fiarse de hacer copia de seguridad solo en otro PC.
8. Comprobar que el soporte en el que se hacen las copias de seguridad está en uso y no está obsoleto y proteger las copias de seguridad de su posible deterioro.
9. Hacer un simulacro de pérdida de información.
10. Las copias de seguridad tienen que estar protegidas.

Los CD's o DVD's hay que manejarlos por los bordes y conservarlos en un lugar fresco y seco.

Es prácticamente imposible garantizar la seguridad de un sistema al 100%, de todas formas si no se sigue una adecuada política de copias de seguridad la probabilidad de que algo ocurra al sistema se incrementa exponencialmente.



**8.2 Utilidades para la
compresión/descompresión de
archivos y backup/restauración
de sistemas.**

**8.2.4 Utilidades para
comprimir/descomprimir
ficheros en linux**

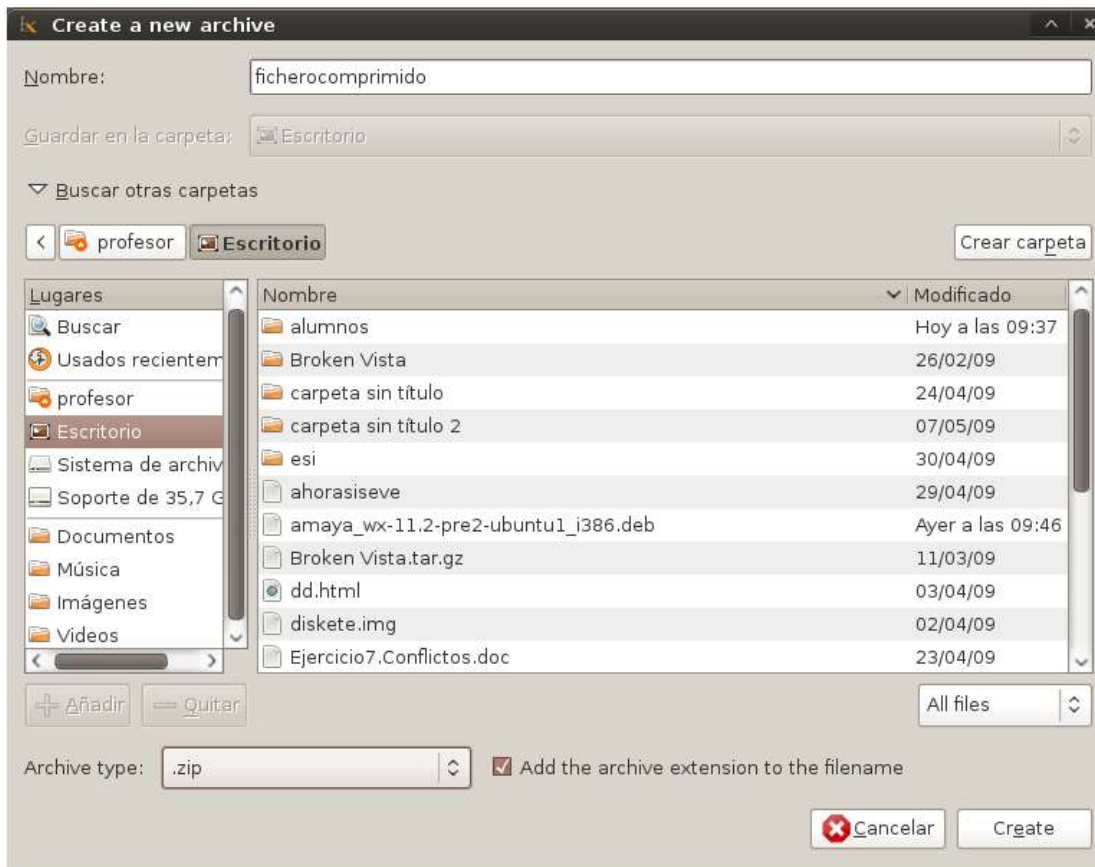
XArchiver para Linux

- Admite los formatos:
 - TAR
 - ZIP
 - 7-ZIP
 - JAR
 - LHA
 - SIT.
 - GZIP
 - BZip,
 - BZip2
 - Y otros

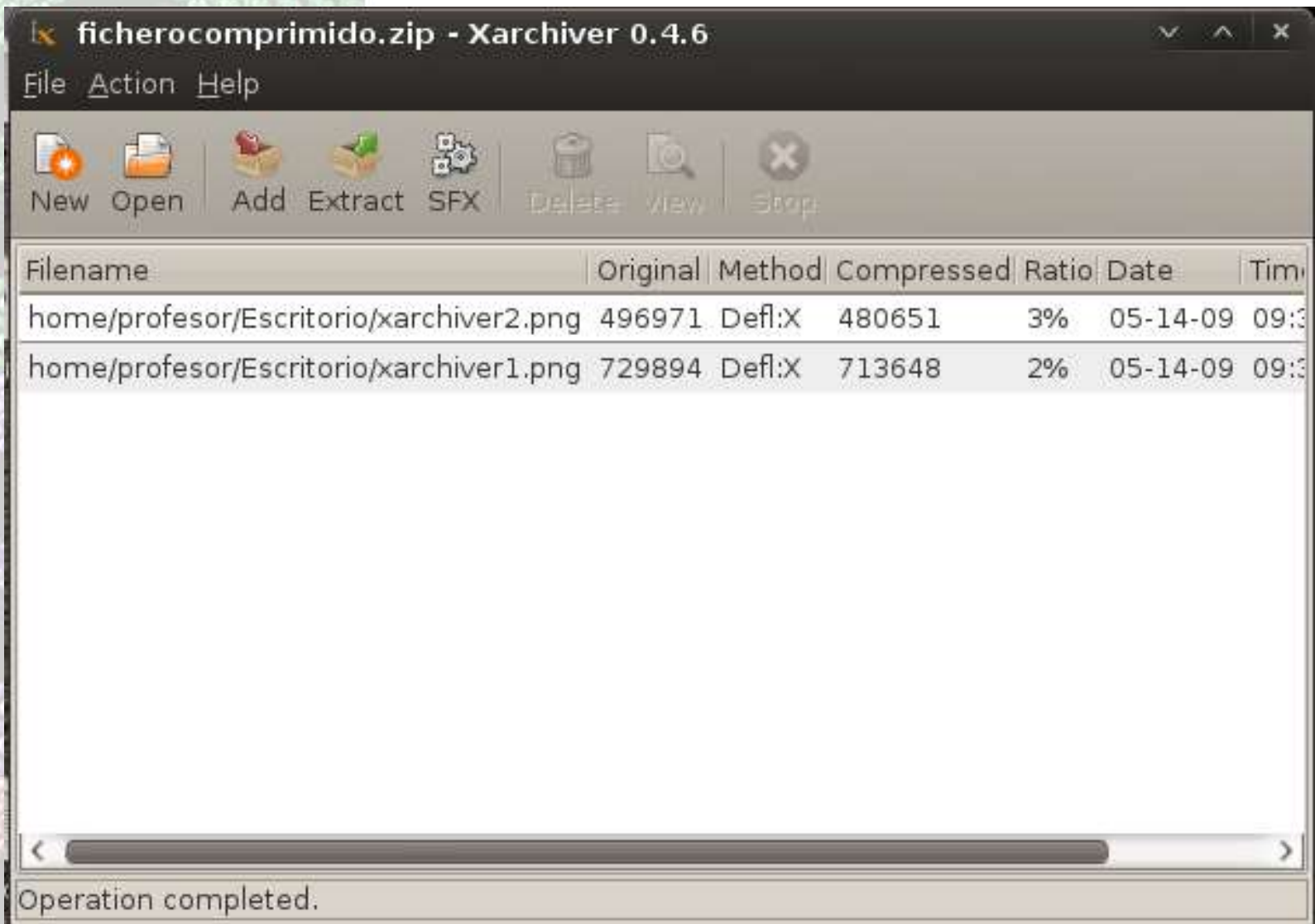
**XArchiver también
se puede ejecutar
desde la línea
de comando.**

```
profesor@profesor-desktop: ~  
Archivo Editar Ver Terminal Solapas Ayuda  
profesor@profesor-desktop:~$ sudo apt-get install xarchiver
```

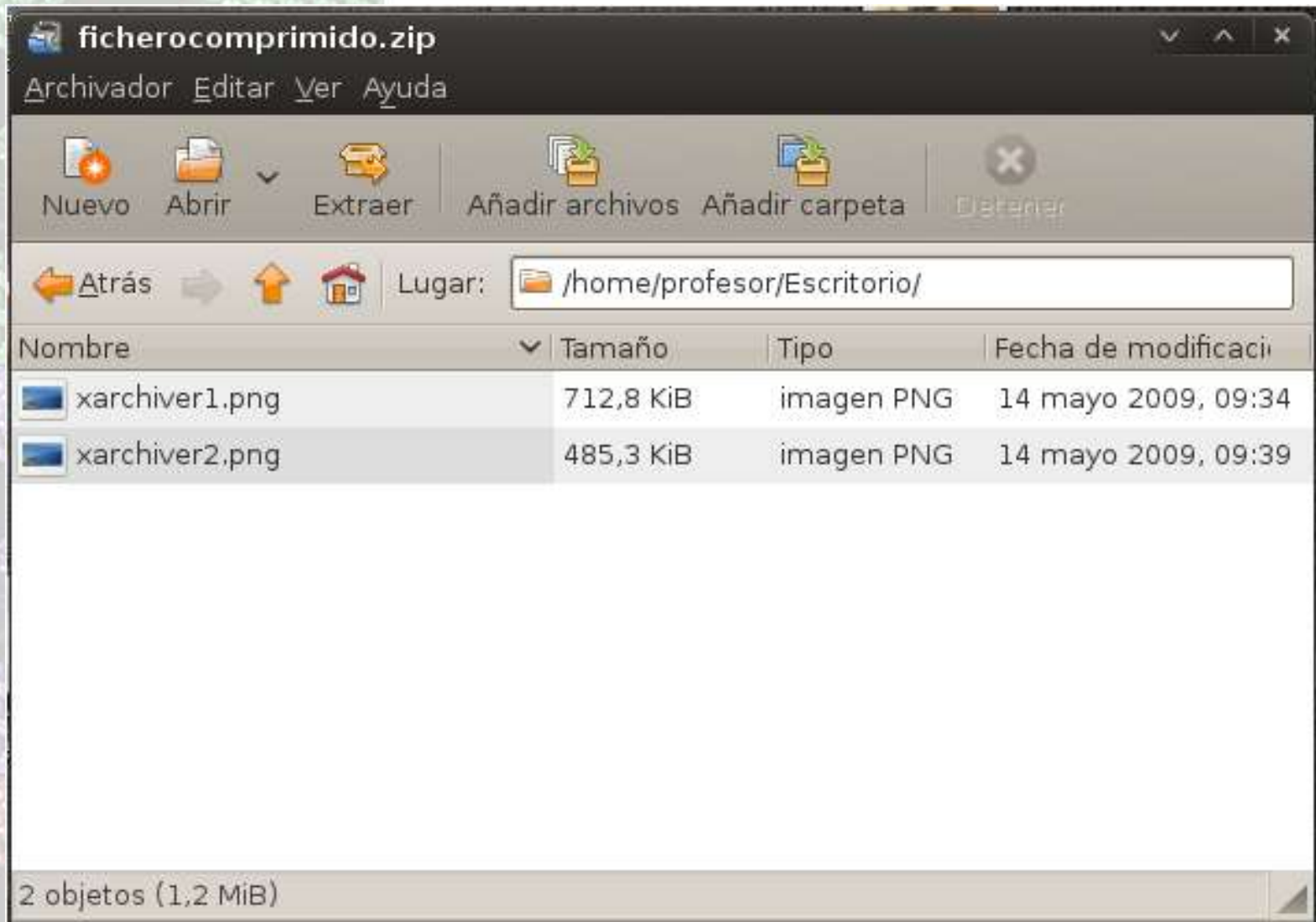
- Instalación de xarchiver



- Creación de un archivo comprimido



- **Detalles del fichero comprimido**

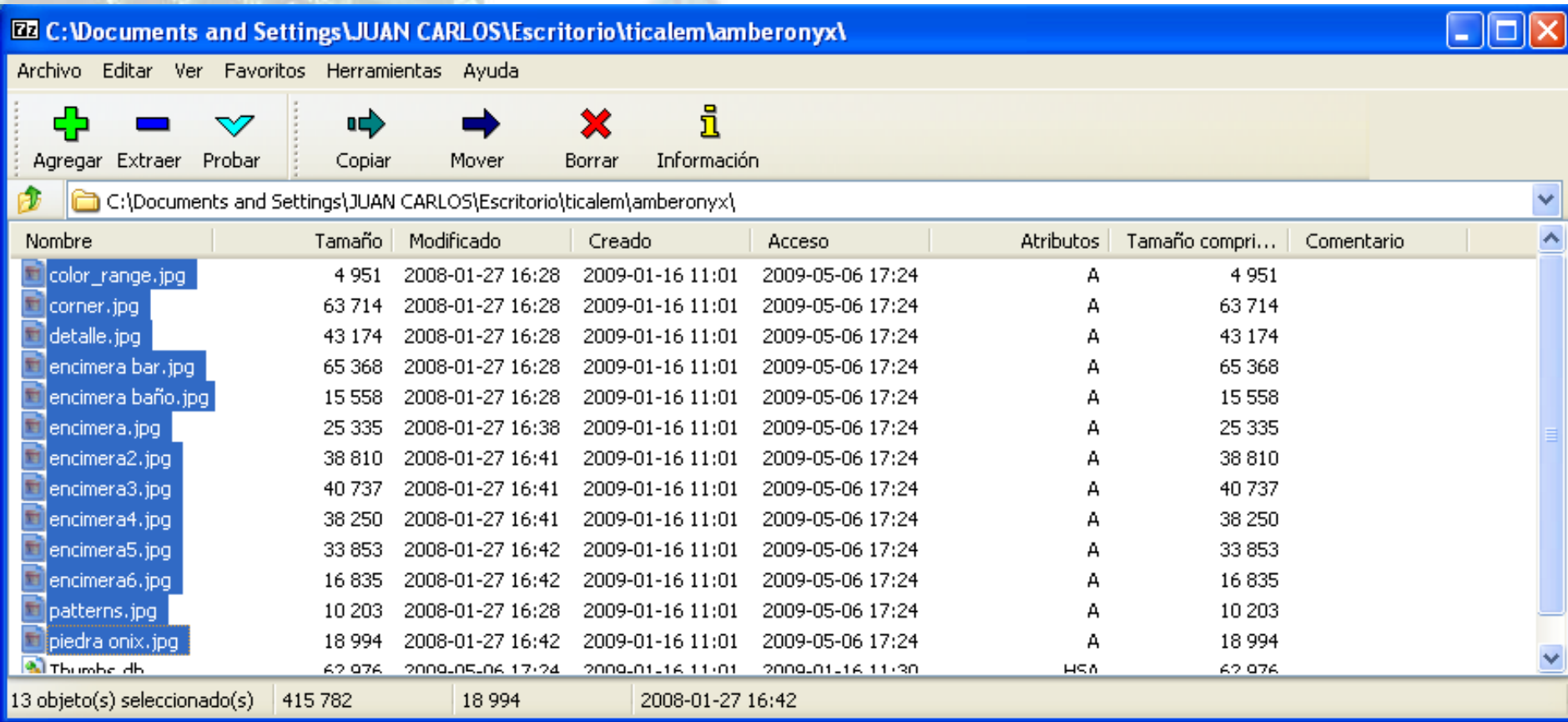


- **Abriendo el fichero comprimido con otra herramienta: File Roller.**

8.2 Utilidades para la compresión/descompresión de archivos y backup/restauración de sistemas.

8.2.5 Utilidades para comprimir/descomprimir ficheros en Windows

7zip



- Parecido a Winzip y Winrar pero libre

Añadir al archivo ✕

Archivo: ... ▼

Formato de archivo: ▼

Nivel de Compresión: ▼

Tipo de compresión: ▼

Tamaño de Diccionario: ▼

Tamaño de la Palabra: ▼

Tamaño de bloque compacto: ▼

Número de hilos de CPU: ▼ / 2

Memoria usada para Comprimir: 192 MB

Memoria usada para Descomprimir: 18 MB

Partir en fragmentos, bytes: ▼

Parámetros:

Modo de actualización: ▼

Opciones

Crear archivo SFX (auto-extraíble)

Comprimir archivos abiertos para escritura

Encriptación

Escriba la contraseña:

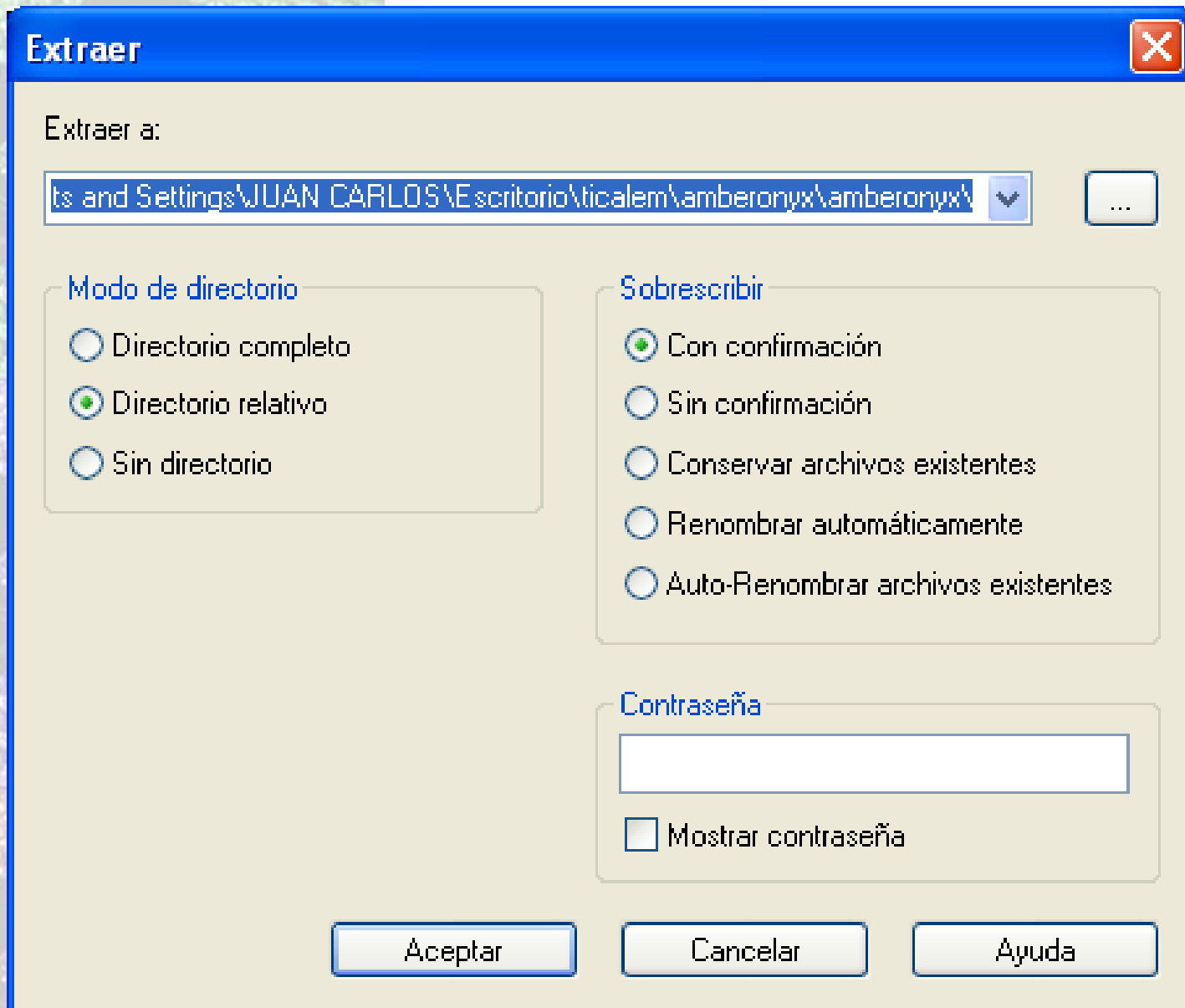
Escriba nuevamente la contraseña:

Mostrar contraseña

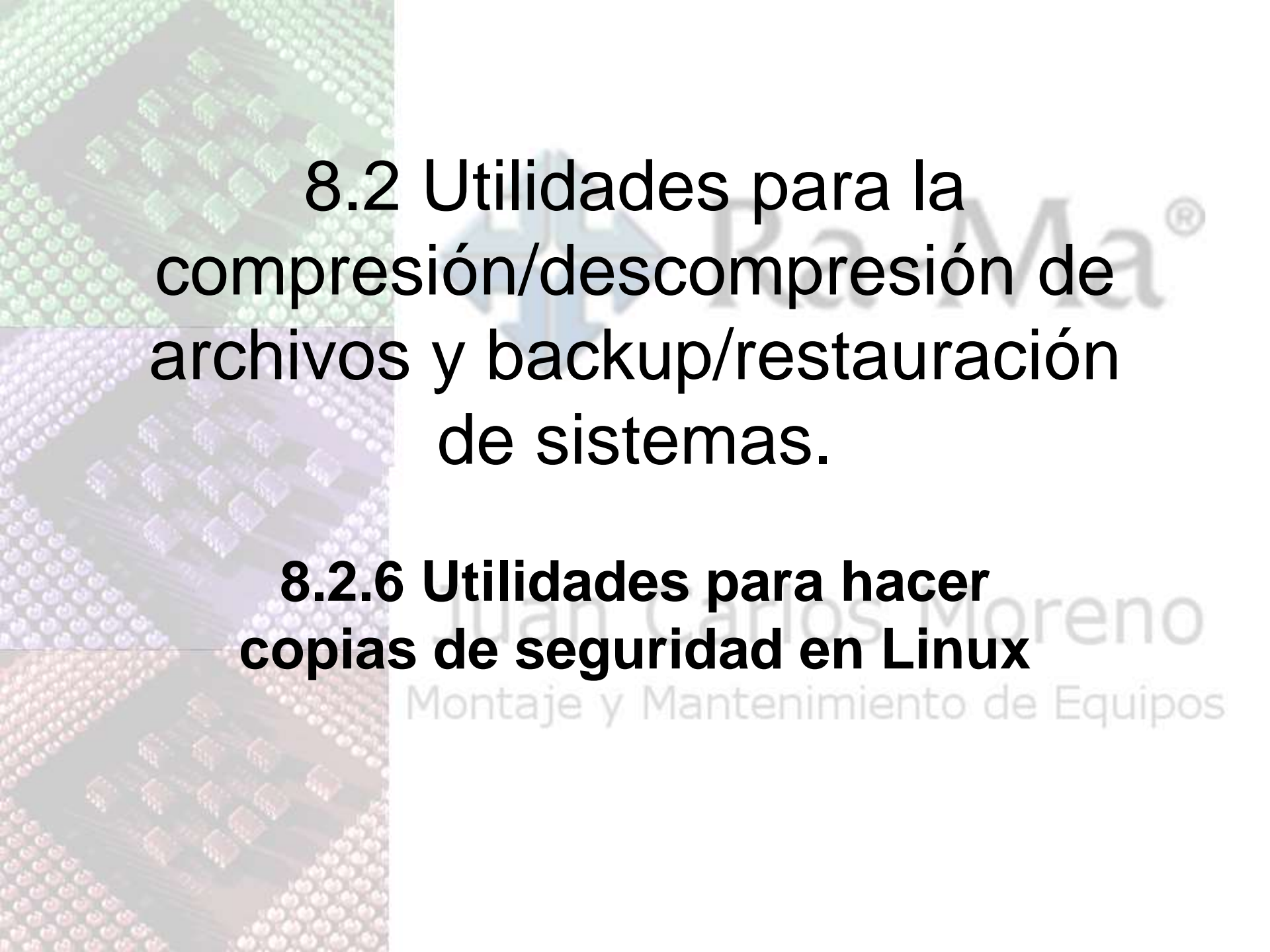
Método de Encriptación: ▼

Encriptar nombres de fichero

- **Opciones al crear un archivo.**



- **Extracción de un archivo.**



**8.2 Utilidades para la
compresión/descompresión de
archivos y backup/restauración
de sistemas.**

**8.2.6 Utilidades para hacer
copias de seguridad en Linux**

Juan Carlos Moreno
Montaje y Mantenimiento de Equipos

Linux tar (ejemplos I)

- 1. Empaquetar un directorio

```
dsl@box:~/datos$ tar cvf dir1.tar dir1
dir1/
dir1/datos2.txt
dir1/datos.txt
dsl@box:~/datos$ █
```

- 2. Empaquetar varios directorios y archivos

```
dsl@box:~/datos$ tar cvf dir1.tar dir1 fichero.txt
dir1/
dir1/datos2.txt
dir1/datos.txt
fichero.txt
dsl@box:~/datos$ █
```

quipos

Linux tar (ejemplos II)

- 3. Desempaquetar un fichero tar

```
dsl@box:~/datos$ tar xvf dir1.tar
dir1/
dir1/datos2.txt
dir1/datos.txt
fichero.txt
dsl@box:~/datos$ █
```

- 4. Empaquetar directorios y archivos de forma comprimida

```
dsl@box:~/datos$ tar cvzf dir1.tar.gz dir1
dir1/
dir1/datos2.txt
dir1/datos.txt
dsl@box:~/datos$ █
```

Linux tar (ejemplos III)

- 5. Desempaquetar un fichero tar que esté comprimido

```
dsl@box:~/datos$ tar xvzf dir1.tar.gz
dir1/
dir1/datos2.txt
dir1/datos.txt
dsl@box:~/datos$ █
```

- 6. Listar el contenido de un fichero tar

```
dsl@box:~/datos$ tar tvf dir1.tar
drwxrwxr-x dsl/staff      0 2009-05-13 15:31:53 dir1/
-rw-rw-r-- dsl/staff      9 2009-05-13 15:31:53 dir1/datos2.txt
-rw-rw-r-- dsl/staff      9 2009-05-13 15:31:50 dir1/datos.txt
-rw-rw-r-- dsl/staff     10 2009-05-13 15:35:59 fichero.txt
dsl@box:~/datos$ █
```

Linux tar (ejemplos III)

- 7. Listar el contenido de un fichero tar comprimido

```
dsl@box:~/datos$ tar tvzf dir1.tar.gz
drwxruxr-x dsl/staff      0 2009-05-13 15:37:18 dir1/
-rw-rw-r-- dsl/staff      9 2009-05-13 15:31:53 dir1/datos2.txt
-rw-rw-r-- dsl/staff      9 2009-05-13 15:31:50 dir1/datos.txt
dsl@box:~/datos$ █
```

Es el usuario quien tiene que ponerle la extensión al fichero comprimido.
Se suele utilizar **.tar.gz** o **.tgz**

Linux Sbackup

- Para la instalación de esta herramienta en Ubuntu, basta con ejecutar el siguiente:

comando: `sudo apt-get install sbackup`

- Una vez ejecutado este comando nos aparecerá en Sistema→administración el acceso a la configuración de las copias de respaldo y la restauración de las copias de respaldo.

General Incluir Excluir Destino Hora Purgando

Usar parámetros de copia de respaldo recomendados

Realizar copias de respaldo estandar.

Por defecto: incrementales diarios y copias de respaldo completas semanales en /var/backup de todos los archivos de usuario, /etc, /usr/ local y /var.

Los archivos multimedia, temporales y mayores a 100 Mb serán excluidos.


Usar ajustes de copia de respaldo personalizados


Generar copias de respaldo de acuerdo a lo definido en las páginas siguientes a este diálogo.

Solo copias de respaldo manuales

No realizar copias de respaldo de sus datos automáticamente. Nota: esto no previene la realización de copias de respaldo manuales.

 Acerca de

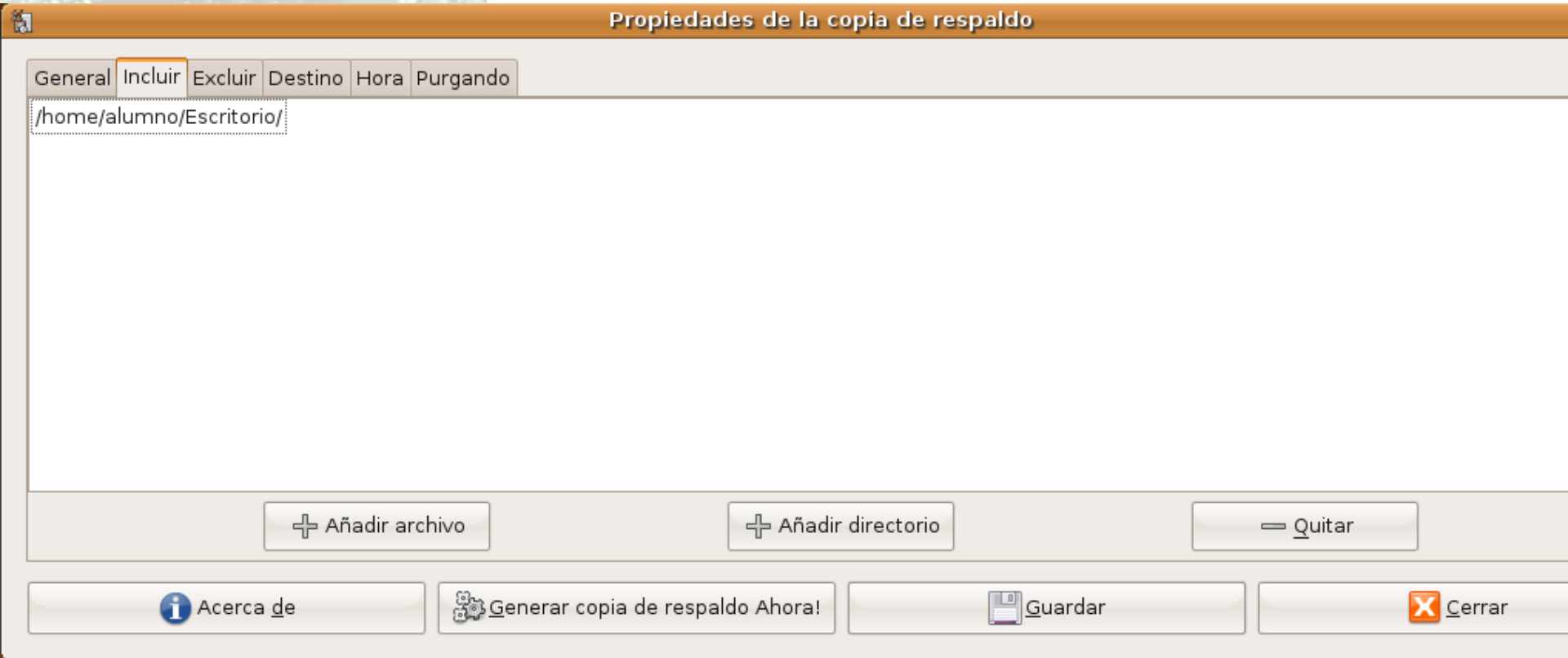
 Generar copia de respaldo Ahora!

 Guardar

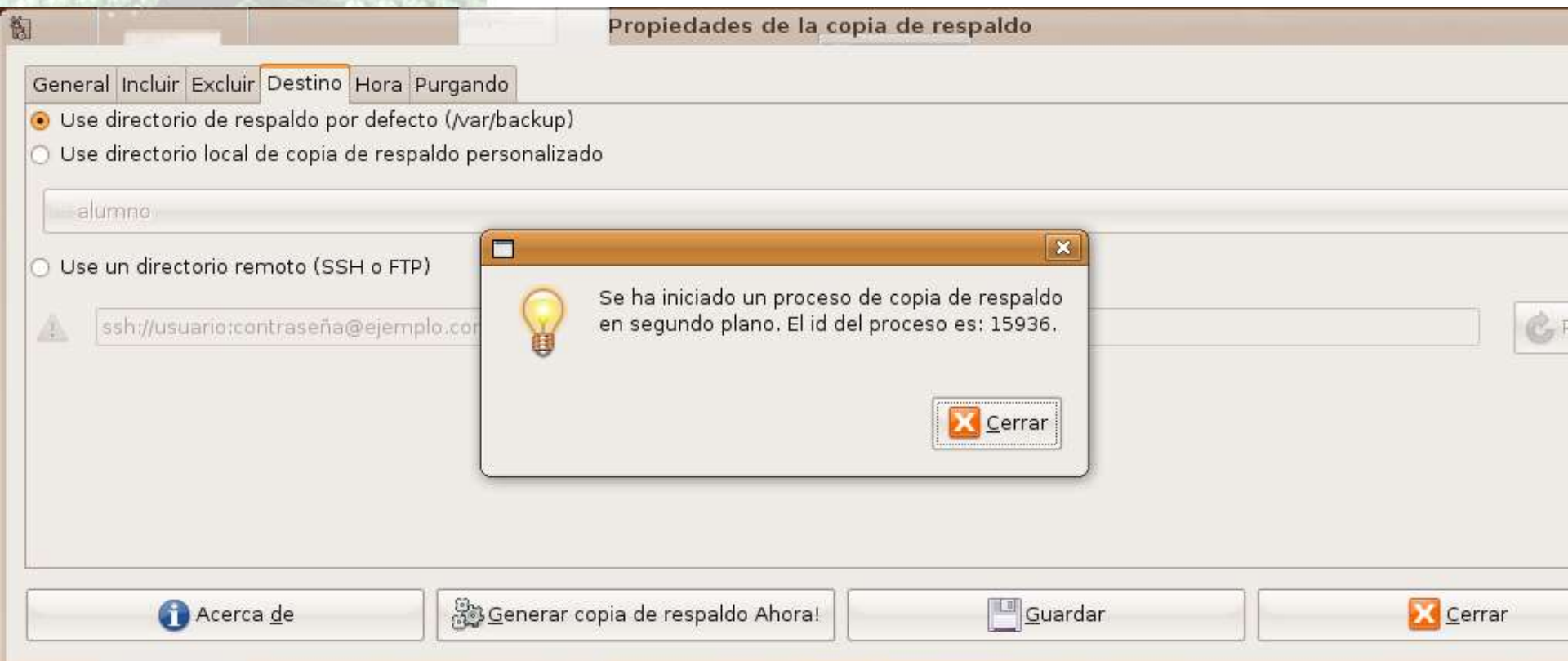
 Cerrar

Montaje y Mantenimiento de Equipos

- Se pueden hacer copias de seguridad manuales y automáticas



- Se pueden seleccionar los datos a incluir o excluir



Juan Carlos Moreno
Montaje y Mantenimiento de Equipos

- Generación de una copia de seguridad manual

General Incluir Excluir Destino **Hora** PurgandoRealizar respaldos simply **precisely** en

Día del mes:

Día de la semana:

Hora

Minuto

1	lunes
2	martes
3	miércoles
4	jueves


Definición de tiempo cron personalizado: 0 4 * * *

Realizar una copia de respaldo completa al menos una vez cada días

Puede configurar cuan frecuentemente empezar la ejecución de un proceso de respaldo y cuando hacerlo.

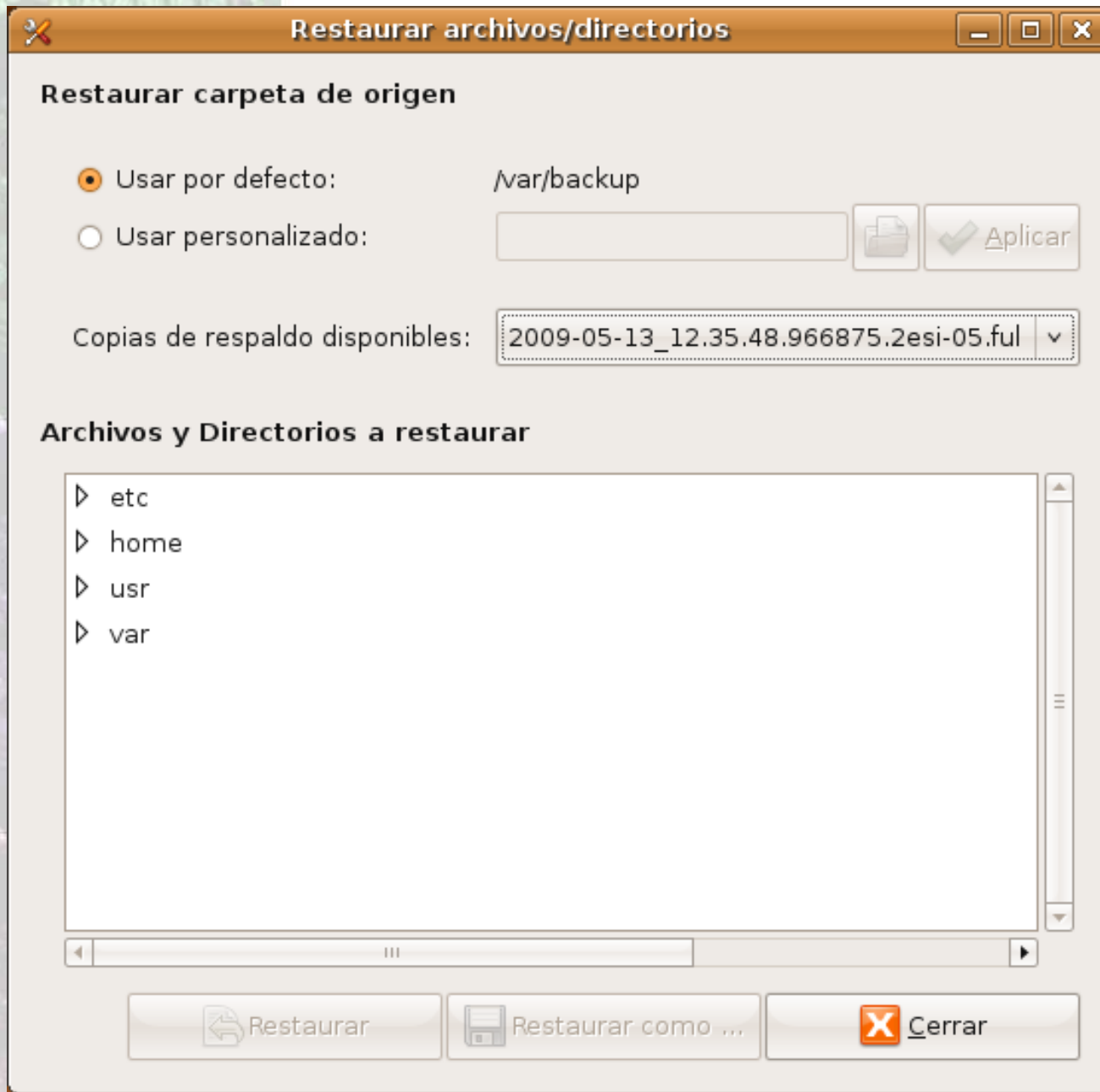
A menos que un número determinado de días hayan pasado desde el último proceso completado, se harán respaldos incrementales.

Vea "man 5 crontab" por la definición de tiempo en cron.

 Acerca de Generar copia de respaldo Ahora! Guardar Cerrar

Montaje y Mantenimiento de Equipos

- Programación de las copias de seguridad. Llama a la herramienta cron.



- Restauración de la copia de seguridad



Ra-Ma®

8.3 RAID

8.3.1 ¿Qué es la tecnología RAID?

Juan Carlos Moreno

Montaje y Mantenimiento de Equipos

Que es la tecnología RAID

- RAID = Redundant Array of Inexpensive Disks (matriz redundante de discos económicos).
- Es una matriz de discos compuesto de dos o más discos
- Los discos no tienen por que ser caros (podemos utilizar la tecnología SATA)
- La información está repetida.
- La repetición de esta información lo que implica es seguridad.

Sistemas RAID

- **Software**

- Es el sistema más económico pero menos eficiente.
- Normalmente se suele utilizar RAID para salvaguardar solamente los datos.

- **Hardware:**

- Es la forma más lógica de implementar RAID.
- Más rápido y efectivo.

Tipo de RAID	Ventajas	Limitaciones
RAID por software	Bajo coste. Solo se requiere un sistema operativo convenientemente configurado	Mucho menos eficiente que el RAID por hardware. Bajo rendimiento del sistema.
RAID por hardware	Más eficiente que el RAID por software. Menos carga de trabajo para el microprocesador	Más costoso, aunque con una placa base que incorpore RAID los costes se reducen.



Ra-Ma®

8.3 RAID

8.3.2 Complemento o no de las copias de seguridad

Juan Carlos Moreno
Montaje y Mantenimiento de Equipos

8.3.2 Complemento o no de las copias de seguridad

- RAID no sustituye a las copias de seguridad
- RAID nos da la tranquilidad de que ante cualquier fallo hardware podemos recuperar el sistema de una manera ágil y rápida
- No previene de un borrado accidental de los datos
- No previene de una corrupción de ficheros u otra desgracia por el estilo
- Es un complemento de las copias de seguridad



Ra-Ma®

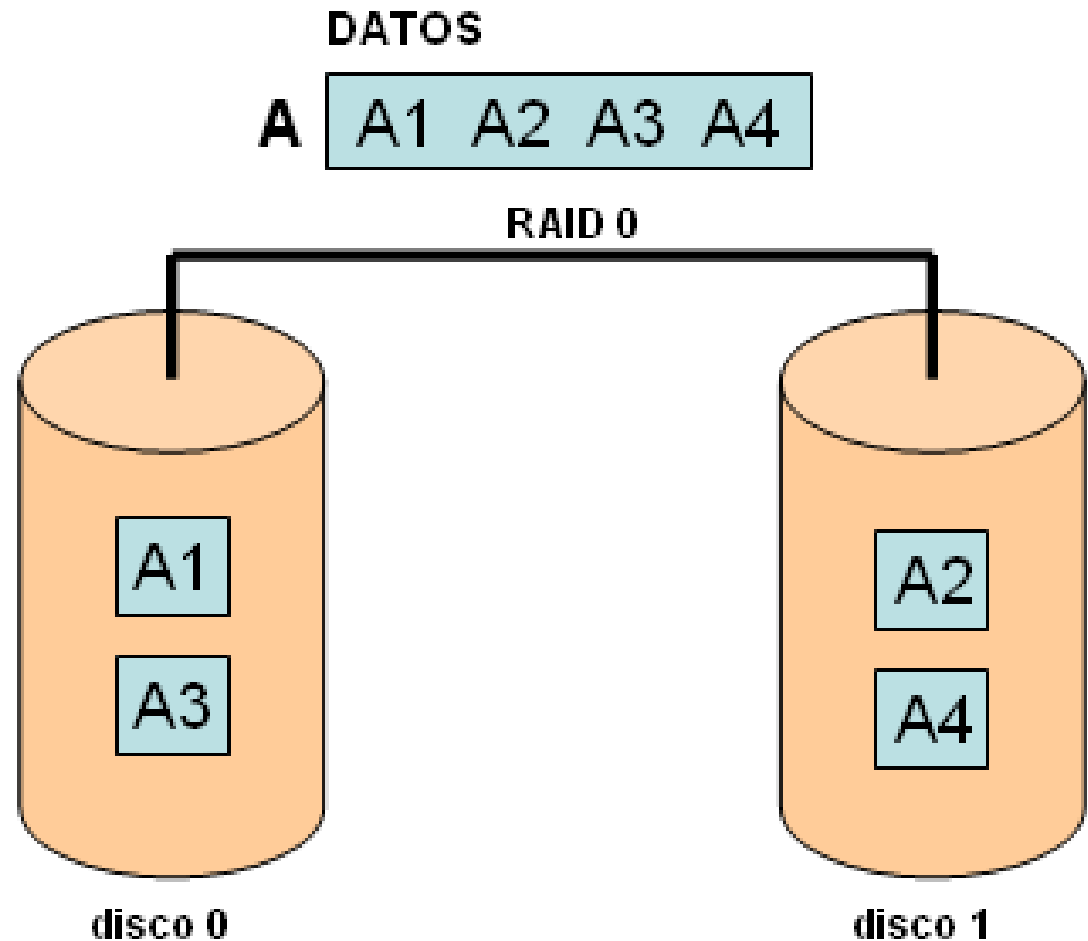
8.3 RAID

8.3.3 Tipos de RAID

Juan Carlos Moreno

Montaje y Mantenimiento de Equipos

RAID 0 (Striping o Duplexing)



RAID 0 (Striping o Duplexing)

- Striping = entrelazado.
- No hay implementado ningún mecanismo de seguridad.
- Se necesitan como mínimo dos discos.
- Objetivo : aumentar el rendimiento .
- No es aconsejable utilizar este sistema cuando la pérdida de información puede representar un problema grave.

**La pérdida o error en un disco de RAID 0
implica la pérdida de la información
en el sistema.**

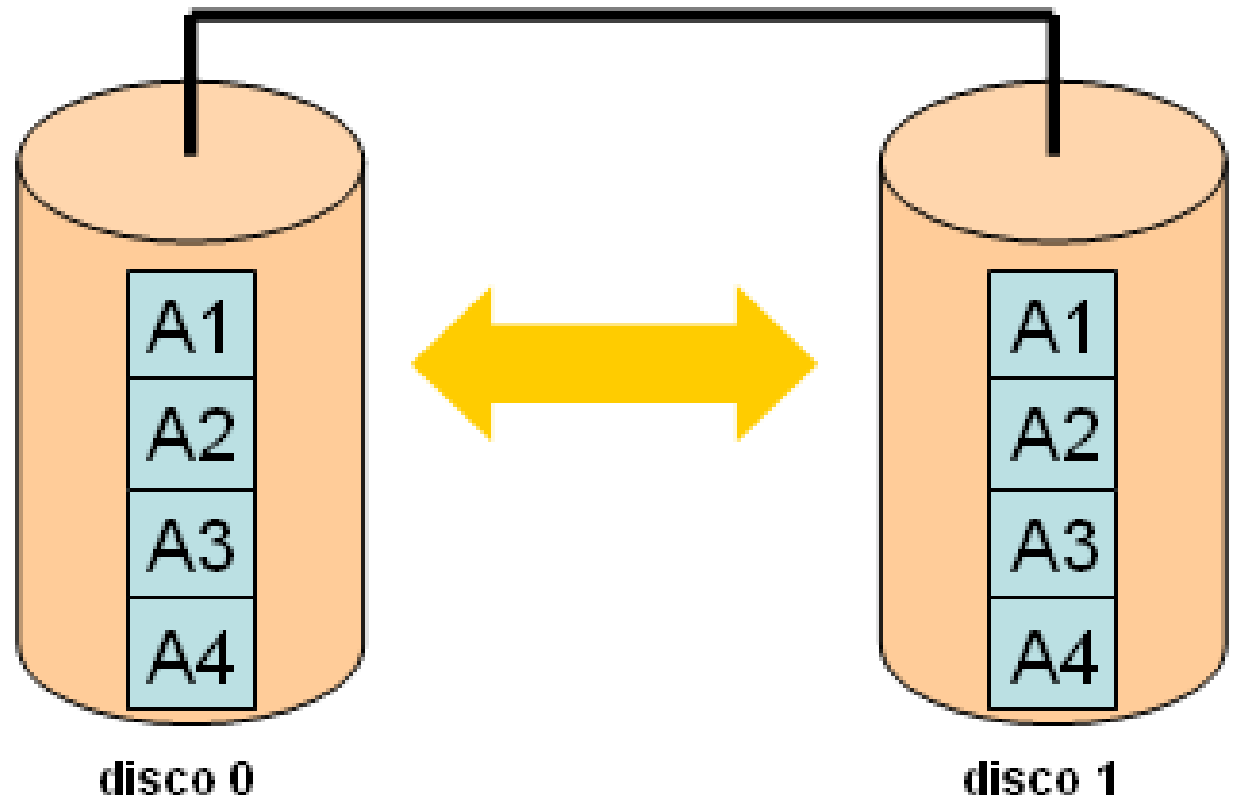
**Esta pérdida será definitiva
salvo que la información
se encuentre en algún backup.**

RAID 1 (Mirroring)

DATOS

A A1 A2 A3 A4

RAID 1



Se pueden utilizar en RAID 1
discos de diferentes capacidades
o velocidades.

Al final la pareja de discos
tendrá la velocidad del menor
y la capacidad del menor.

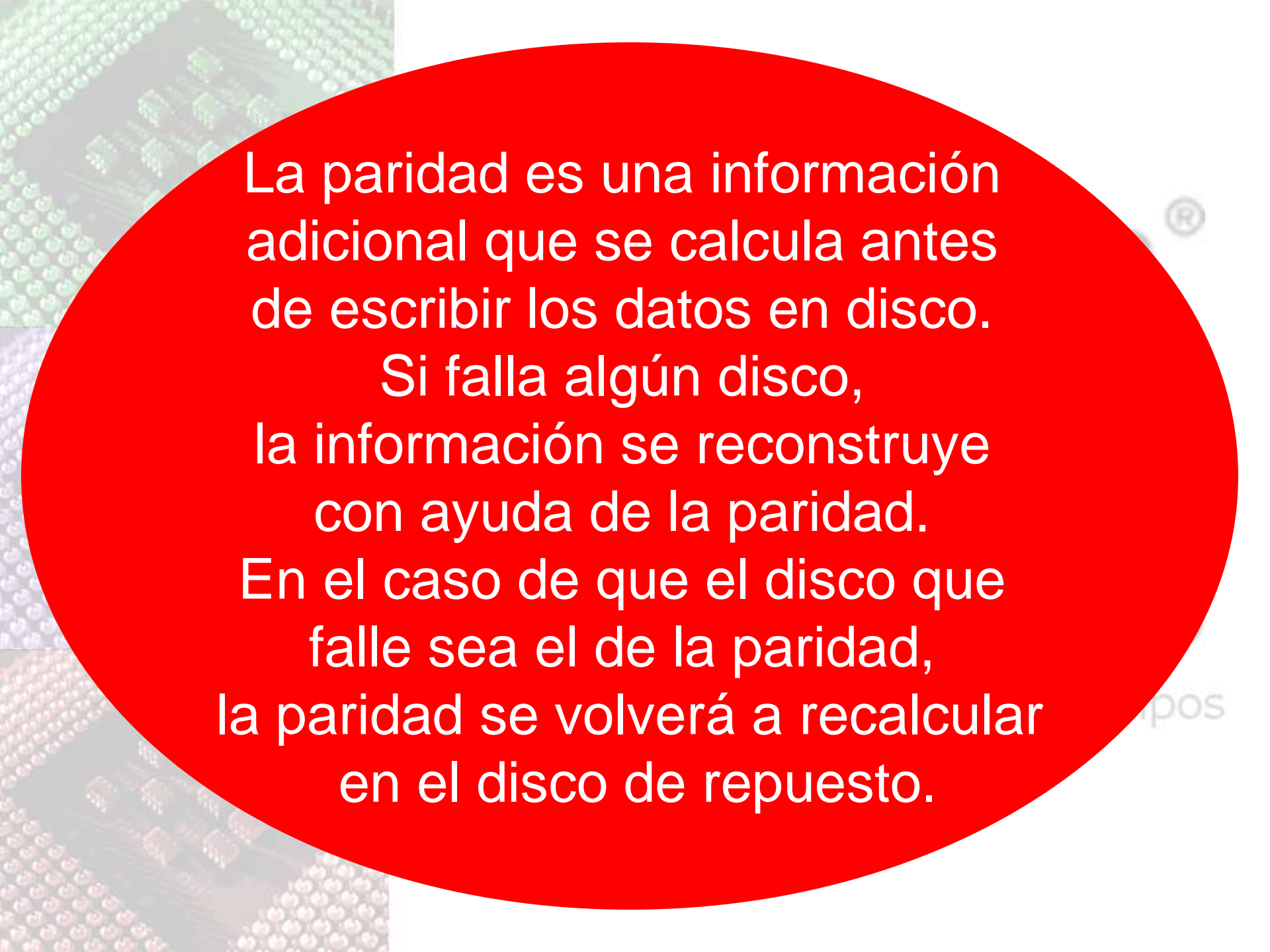
Aunque esto es posible, se aconseja
utilizar discos exactamente
iguales

RAID 1 (Mirroring)

- La sobrecarga u overload del sistema siempre será del 50%.
- Por cada disco se tendrá un disco extra, por lo tanto el sistema tendrá $2n$ discos.
- El rendimiento de lectura aumenta (hasta el doble como máximo) porque puede leerse de varios discos a la vez.
- El rendimiento de escritura permanece constante.

RAID 2 (Bit striping + Hamming Code)

- Utiliza una división de la información en bits por todos los discos del stripe y el código Hamming para la recuperación de errores.
- RAID 2 no se utiliza debido a que existen sistemas más avanzados y eficientes como RAID 4 o 5.



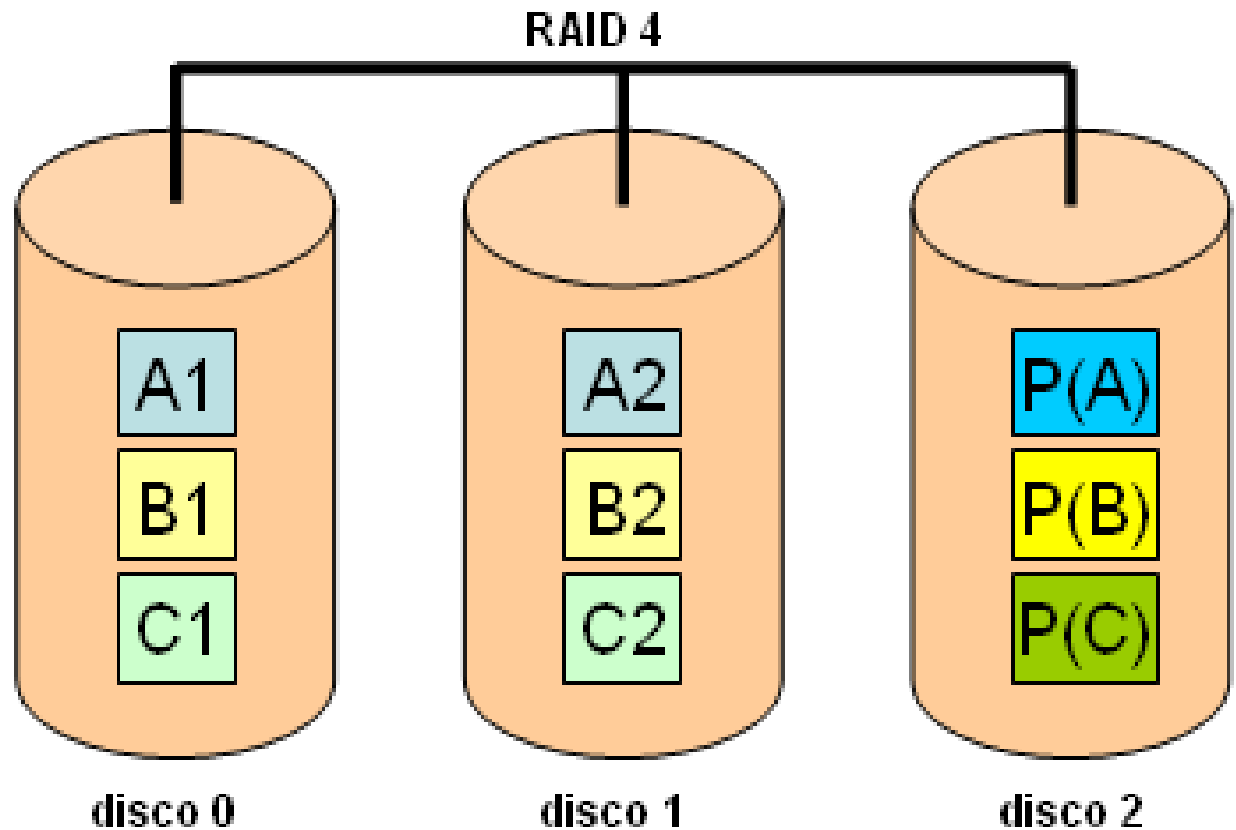
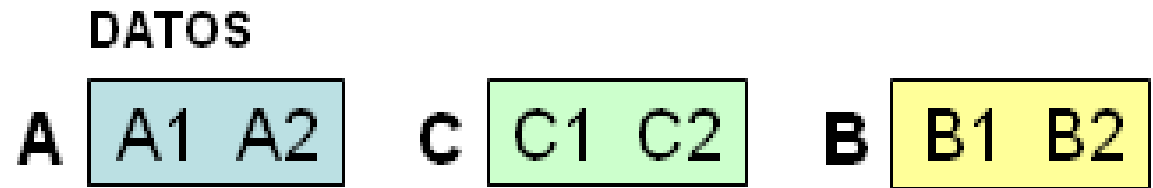
La paridad es una información adicional que se calcula antes de escribir los datos en disco.

Si falla algún disco, la información se reconstruye con ayuda de la paridad. En el caso de que el disco que falle sea el de la paridad, la paridad se volverá a recalcular en el disco de repuesto.

RAID 3 (Byte striping + Paridad)

- Utiliza una división de la información en bytes por todos los discos del stripe y la paridad para la recuperación de errores.
- La ventaja frente al RAID 2 es que la paridad ocupa menos que el código Hamming.
- RAID 3 no se utiliza debido a que existen sistemas más avanzados y eficientes como RAID 4 o 5.

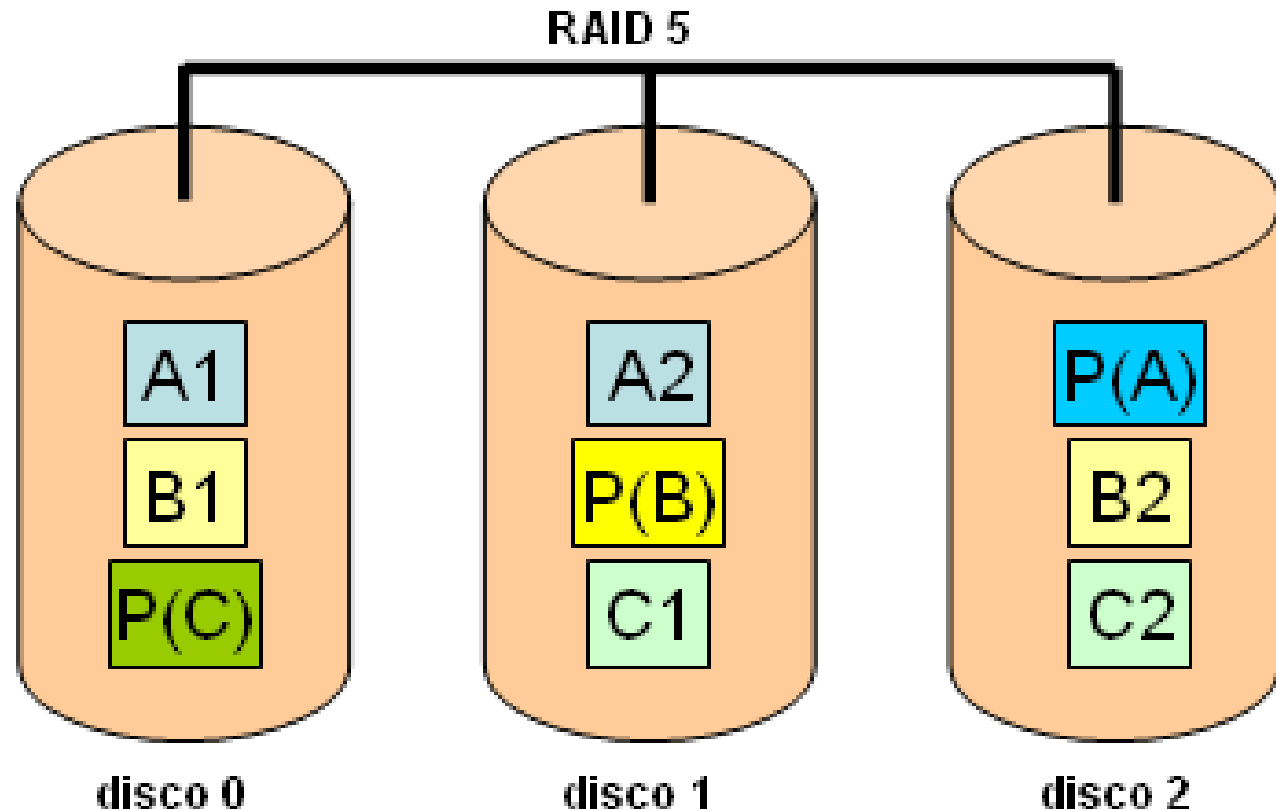
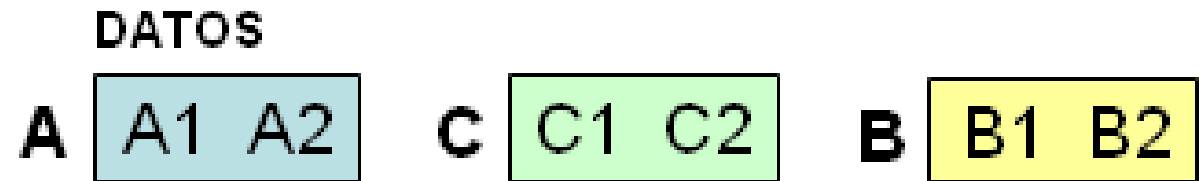
RAID 4 (Striping + Paridad)



RAID 4 (Striping + Paridad)

- Igual que RAID 3 pero en vez de distribuir la información por los discos por bytes, la distribuye por sectores. La paridad la almacena en un disco del stripe aparte de los datos.
- Tiene un rendimiento mayor que RAID 2 y 3.
- Necesita como mínimo 3 discos (2 para datos y uno para paridad).

RAID 5 (Striping + Paridad distribuida)



RAID 5 (Striping + Paridad distribuida)

- RAID 5 funciona igual que RAID 4, pero distribuye la paridad por cada uno de los discos del stripe o matriz.
- Tiene un rendimiento de escritura mucho mayor al escribir la paridad de forma distribuida.
- Se necesitarán como mínimo 3 discos.
- Con 4 discos el overload o sobrecarga es de un 25% .
- Sobrevive al fallo de un disco (no al de dos).
- Es el RAID mas utilizado al ofrecer un mejor equilibrio coste-rendimiento-protección.

Tipo de RAID	Nº Mínimo de discos	Ventajas	Limitaciones
RAID 0	2	Rendimiento	No existe protección de datos.
RAID 1	2	Buena protección de datos y alto rendimiento.	Alto coste. Se necesita duplicar el número de discos (2n). El overload es elevado, siempre un 50%.
RAID 5	3	Mejor relación rendimiento/precio · Necesita n+1 discos con un mínimo de 3 discos. Con 4 discos el overload es solo del 25% mientras que con RAID 1 sería del 50%.	Escritura más lenta que con RAID 0 o 1, dado que el sistema tiene que calcular la paridad para cada dato que escribe.



Ra-Ma®

8.3.4 Sistemas RAID anidados

8.3.4 Sistemas RAID anidados

Juan Carlos Moreno

Montaje y Mantenimiento de Equipos

RAID 0+1

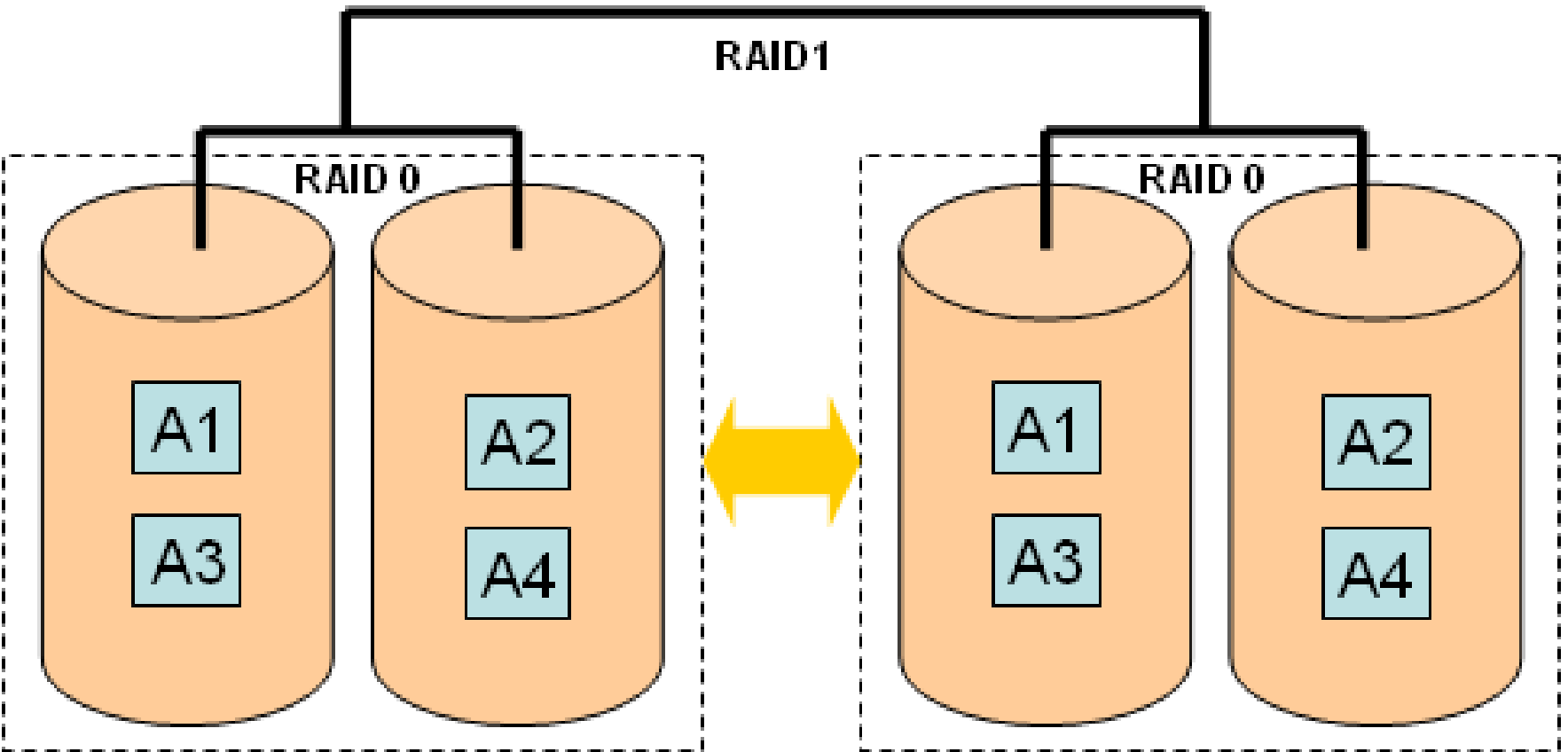
DATOS

A A1 A2 A3 A4

RAID1

RAID 0

RAID 0



RAID 0 + 1

- RAID 0 + 1 corresponde a implementar un stripe y duplicarlo en espejo.
- Se necesitarán como mínimo 4 discos.
- La sobrecarga u overload es de un 50%.

Juan Carlos Moreno

Montaje y Mantenimiento de Equipos

RAID 10 (1+0)

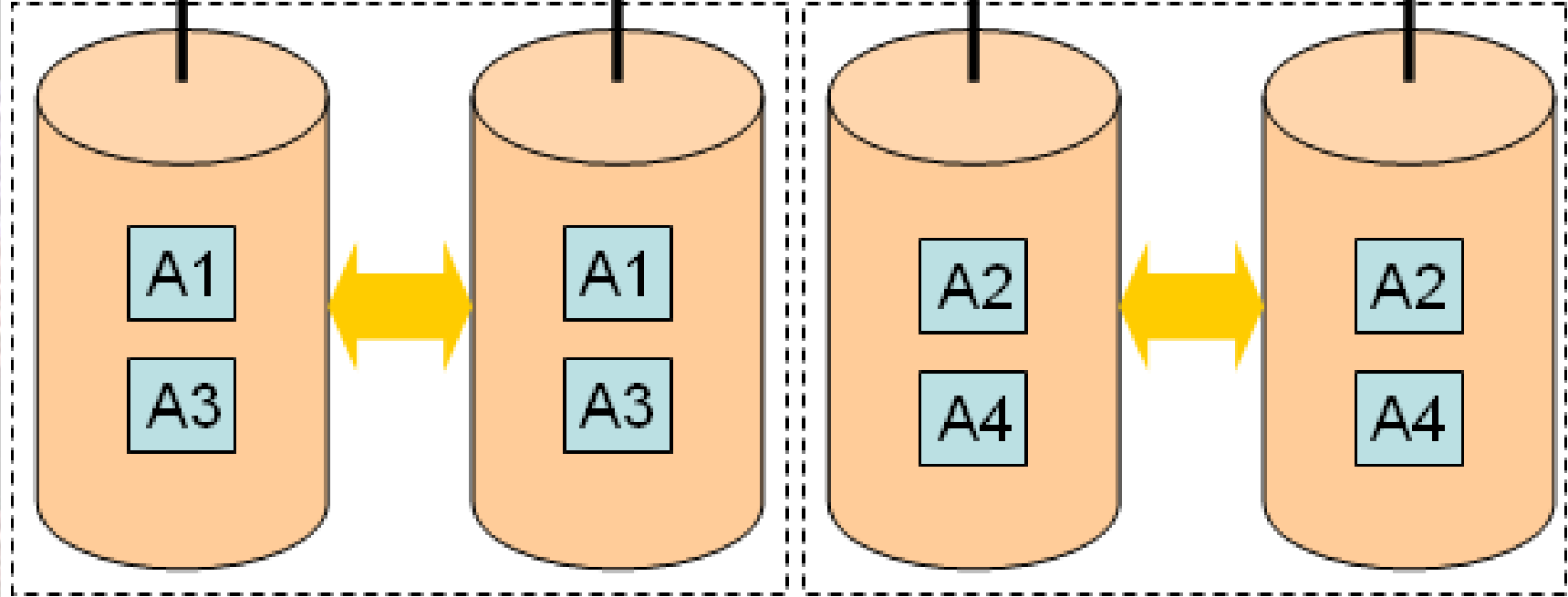
DATOS

A [A1 A2 A3 A4]

RAID 0

RAID 1

RAID 1



RAID 10 (1+0)

- RAID 10 corresponde a implementar varios espejos y luego realizar con ellos un stripe.
- Se necesitarán como mínimo 4 discos.
- La sobrecarga u overload es de un 50%.
- Es una configuración más usada que RAID 0+1 puesto que es ligeramente más tolerante a errores.
- Permite múltiples fallos siempre que se produzcan en un espejo distinto.

Niveles RAID mas utilizados

- **RAID 0, 1 y 10** para equipos normales, Workstation y servidores pequeños.
- **RAID 5 y 50** para grandes servidores.
También es común ver RAID 5 en equipos normales o servidores más pequeños.

Juan Carlos Moreno

Montaje y Mantenimiento de Equipos



Ra-Ma®

8.4 Antivirus.

8.4.1 Tipos de malware

Juan Carlos Moreno

Montaje y Mantenimiento de Equipos

virus

- Un virus es un programa software que se adjunta a un archivo del sistema para propagarse a otros equipos y dañar el sistema.
- Dependiendo del virus las consecuencias para el equipo serán de mayor o menor gravedad (igual que los virus humanos).

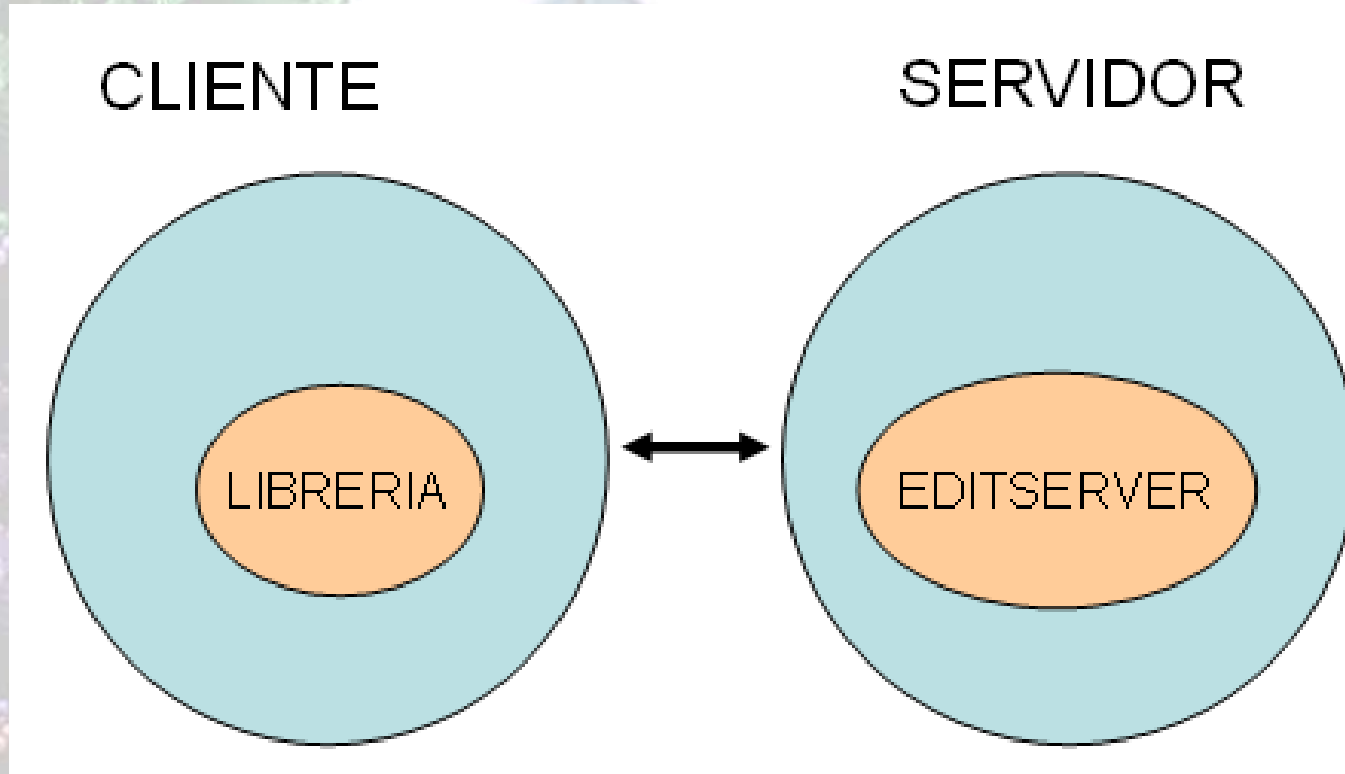
Nunca hay que abrir correos de desconocidos.

La mayoría de virus entran en los sistemas vía correo electrónico.

troyanos

- Los troyanos al revés que los virus no provocan daños en las máquinas anfitrionas.
- Su función es entrar en la máquina sin ser advertido de tal manera que levante la menor sospecha posible para así de esta forma conseguir información o controlar la máquina.

Estructura de un Troyano

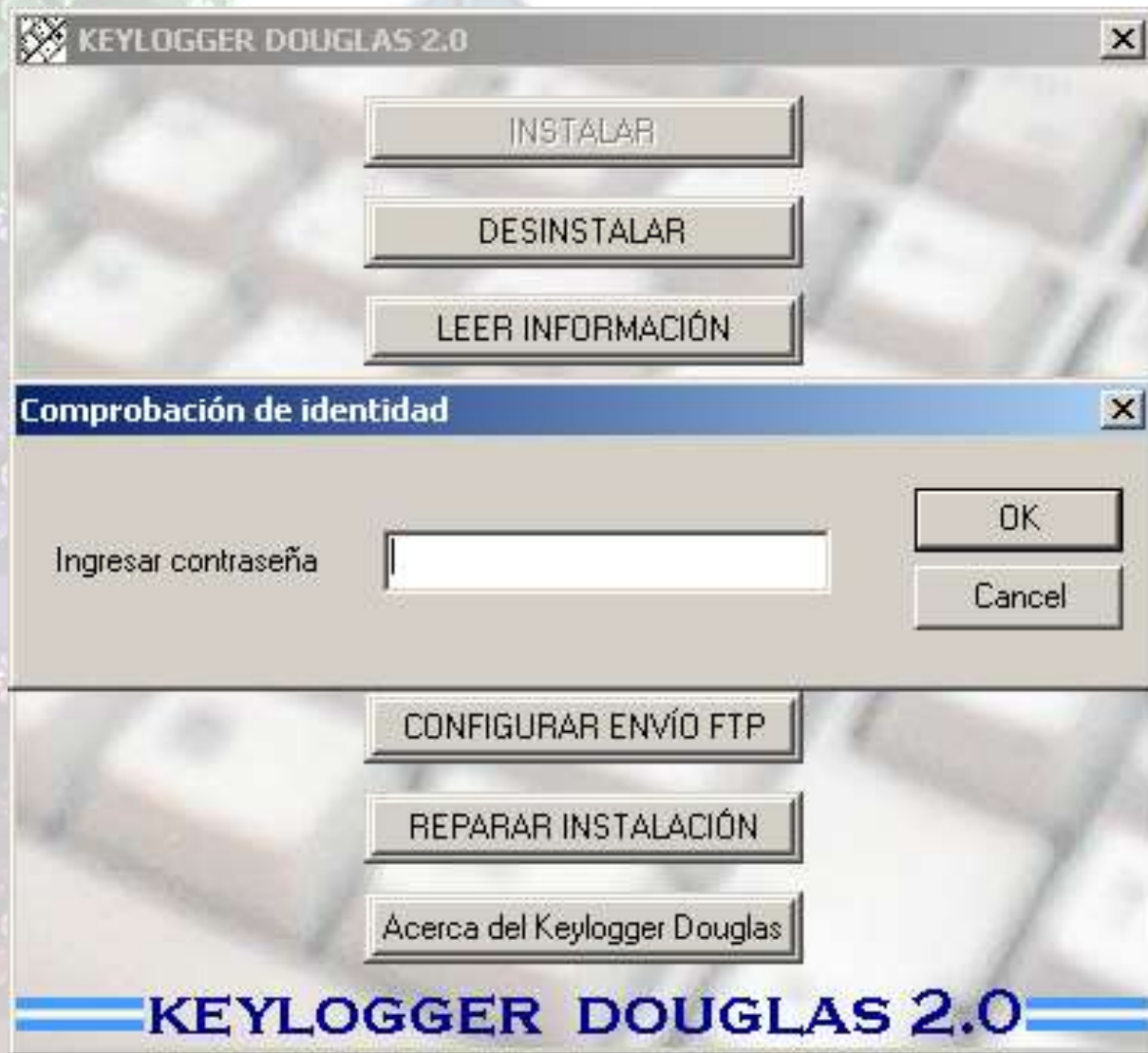


- **El servidor.** El servidor se encargará de enviar al cliente las acciones a ejecutar.
- **El cliente.** Alojado en la máquina anfitriona se encargará de realizar las acciones que le indique el servidor.

keylogger

- Un keylogger es un software o hardware que se encarga de registrar las pulsaciones producidas en el teclado.
- En el caso de un keylogger hardware, el dispositivo puede incorporarse al cable del teclado o bien se puede incorporar dentro del teclado mismo.
- Una vez registradas las pulsaciones del teclado estas se guardarán en un fichero o bien se enviarán por Internet al cracker.
- Existen sistemas antikeylogger.

Ejemplo de un keylogger



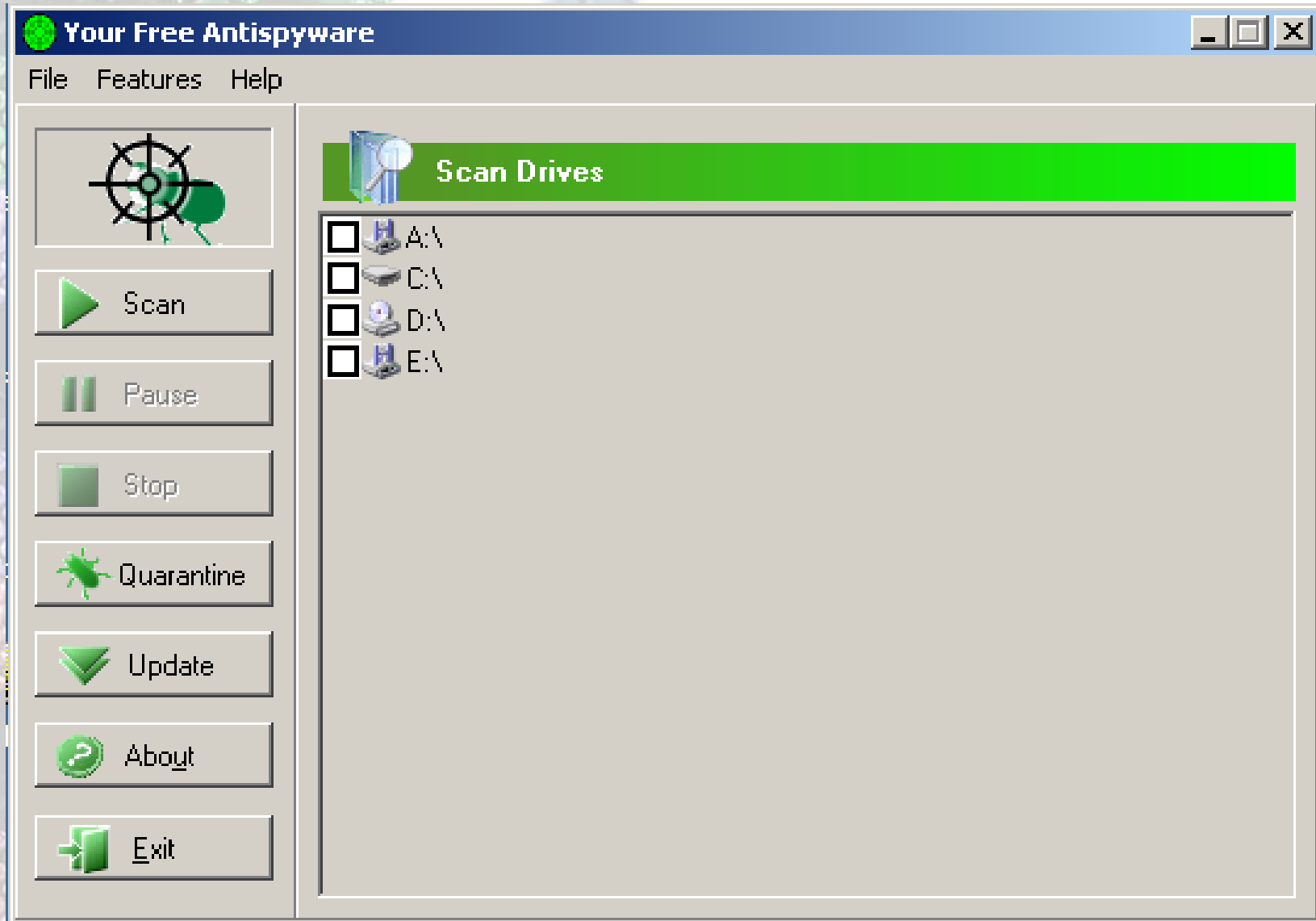
Spyware

- El spyware es un software que se encarga de recopilar información sobre el usuario o su equipo y la distribuye a alguien (normalmente empresas publicitarias o similares) con el fin de sacar beneficio de dicha información.
- Como es obvio esta información se distribuye vía Internet, por lo tanto parte del ancho de banda es “robado” para estos fines sin el consentimiento del usuario.

¿Cómo puedo estar seguro de que no tengo ningún Spyware?

- ¿Ha cambiado tu página de inicio (error, búsqueda...) en el navegador?
- ¿Brotan ventanas tipo “pop-up” en el navegador sobre temas comerciales o incluso pornográficos?
- ¿Se han modificado o cambiado valores del registro de Windows?
- ¿El navegador cada vez se hace más lento y da más problemas?
- ¿El equipo tarda mucho en arrancar?
- ¿Existen botones en la barra de herramientas que no se pueden quitar?
- ¿Brotan mensajes avisándote que tu sistema esta infectado incluso con vínculos para descargarte antispyware?
- ¿Tienes problemas con el correo electrónico o el messenger con funciones que antes funcionaban correctamente y ahora no?

Ejemplo de un antispysware





Your Free Antispyware



File Features Help



Scan

Pause

Stop

Quarantine

Update

About

Exit

Scanning...

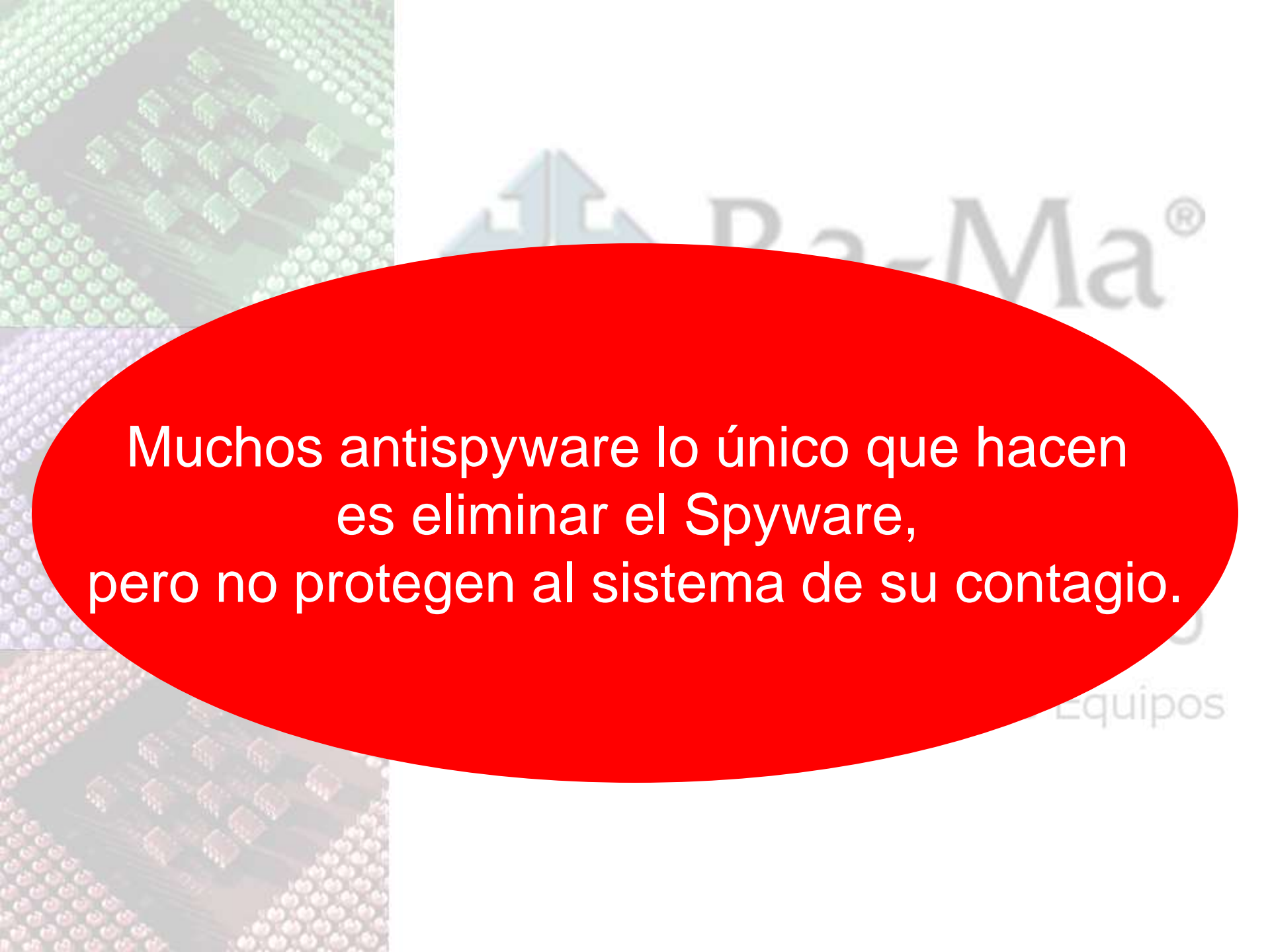
Scanned files (total):	46
Scanned (MB):	321
Infected:	0
Skipped:	0
Suspected:	0
Errors:	0

Information

Scan results: 0 infections found.

Complete





Muchos antispyware lo único que hacen
es eliminar el Spyware,
pero no protegen al sistema de su contagio.

Adaware

- El adaware o Advertising-Supported software consiste en que un software durante su ejecución muestra publicidad sobre productos, servicios...
- En ocasiones la publicidad permite la financiación del desarrollo y modificación del software que de otra forma desaparecería al no encontrar el programador ningún tipo de beneficio.
- En otras ocasiones el objetivo de estos programas es mostrar ventanas o publicidad molesta para el usuario sin ningún tipo de beneficio para el mismo y en este caso se consideraría un malware.

Cookies

- Las cookies son ficheros que se almacenan en el equipo del usuario y sirven para anotar y recordar información del usuario.
- El usuario en todo momento puede activar o desactivar el uso de estas cookies en las opciones de su navegador.
- No obstante, es posible que la información de las cookies se utilice con la finalidad de crear perfiles de usuarios.

Gusanos o Worms

- Un gusano es un malware residente en memoria que no modifica los archivos pero se va replicando de forma incontrolada, de tal manera que el sistema se ralentiza progresivamente debido al consumo de los recursos llegando en ocasiones a no poder ejecutar procesos normales.
- Los gusanos suelen provocar problemas en la red consumiendo ancho de banda propagándose entre los equipos que estén interconectados mediante IRC, SMTP u otros métodos.

Backdoor

- Backdoor o puerta trasera es un software que permite acceder al sistema saltándose los procedimientos habituales de identificación de tal manera que no se detecte este intrusismo.
- En ocasiones se produce un cambio en el software de forma malintencionada para crear una backdoor y así poder saltarse la seguridad del sistema.

Ransomware

- El ransomware es un malware que se propaga normalmente como un gusano y su objetivo es inutilizar el sistema o impedir al usuario el acceso a sus ficheros para luego pedir una recompensa por su liberación.
- Normalmente esta recompensa consiste en el envío de un SMS o la compra de algún programa para restablecer el sistema.

Web bug

- Un web bug es una imagen de tamaño muy pequeño (a veces 1 solo píxel) o invisible que se envía incrustada en una página web o email el cual permite saber si dicha imagen ha sido descargada (el usuario al leer el email o acceder a la página web descarga la imagen).
- Mediante este sistema se puede conocer si la página web ha sido descargada o el email leído.
- Otras formas de llamar a los web bug es:
 - Píxel tag
 - Tracking píxel
 - Tracking bug
 - Web beacon

Exploit

- Es un software que ataca un fallo o debilidad de un sistema.
- No tiene siempre por que ser un malware dado que puede evidenciar la existencia de agujeros de seguridad en un sistema (para corregirlos), pero si este va anexo a un malware como un gusano o bien se utiliza para inhabilitar el sistema o provocar fallos el resultado puede ser preocupante.

Rootkit

- Un rootkit es una herramienta software que se utiliza para tomar el control de un sistema y utilizarlo en beneficio propio.
- Generalmente los rootkits utilizan funciones para borrar huellas y no dejar evidencias de su uso.
- Una vez ganado el sistema es posible dejar puertas traseras o backdoors para propiciar futuros accesos al sistema o incluso exploits para atacar al sistema u otros sistemas.

Ejercicio: antirootkits

- Instala Rootkit Hook Analyzer en tu equipo desde el CD de recursos.
- Utiliza la ayuda para entender el funcionamiento del software y escanea el sistema en busca de rootkits conociendo los servicios a los que afecta.
- En el caso de encontrar algún rootkit elimínalo.

Dialer

- Los dialers son programas que mediante acceso telefónico realizan llamadas normalmente muy caras y en ocasiones sin avisar al usuario de que esta llamada se va a producir.
- Hoy en día la conexión a Internet mediante acceso telefónico no es muy común con lo cual la peligrosidad de este malware se ve reducida.

Leapfrog o ranas

- Las ranas entran en los sistemas descubriendo cuentas y contraseñas de correo para así de esta manera dar el salto y replicarse en otros sistemas.

Hoaxes, jokes o bulos

- Bromas que bajo la apariencia de parecer un virus el objetivo es preocupar al usuario y alarmarle para que tome precauciones y realice acciones que de otra forma no iba a hacer.
- En ocasiones el objetivo de estos bulos es que el usuario borre un archivo o realice alguna acción que provoque daños en el sistema.

Scumware o escoria

- El scumware es software que realiza varias acciones no deseadas como no permitir ser desinstalado, modificar el funcionamiento de los sitios web como redirigir páginas web hacia otras páginas, crear hiperenlaces no deseados o cambiar los banners de publicidad por otros.

Spam

- Prácticamente no hace falta explicar lo que es el spam pues los usuarios del correo electrónico lo sufren diariamente.
- Spam es todo el email basura que se recibe con múltiples finalidades, desde los email que muestran publicidad directamente hasta las famosas cadenas con niños que se están muriendo, animales abandonados o consejos que tienes que reenviar a “nosecuantos” amigos.

Honeypot

- Son sistemas que simulan ser vulnerables para propiciar el ataque de los cracker y así de esta forma conocer las técnicas y maneras de actuar de los mismos.
- También le sirven a los administradores para distraer a los cracker con máquinas que no son relevantes y de esta forma salvaguardar la seguridad de las máquinas importantes advirtiéndolo al administrador del problema producido.

Spyware enmascarado

- Suele ser un truco cruel que hace creer al usuario justo lo contrario que le va a ocurrir.
- Cuando haces caso a estas advertencias lo que ocurre después es que descargas e instalas el Spyware sin saberlo.





Ra-Ma®

8.4 Antivirus.

8.4.2 ¿Qué es un antivirus?

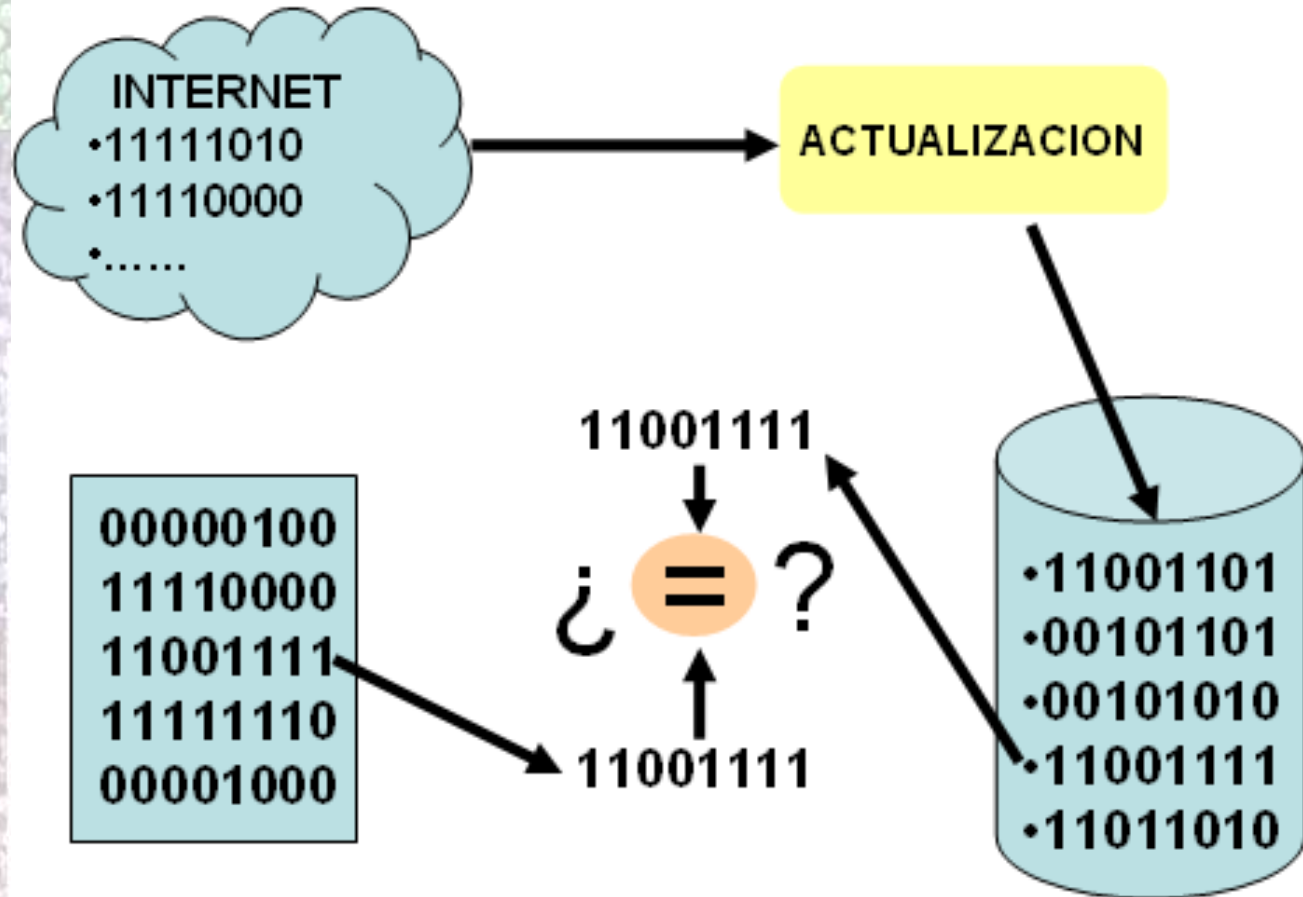
Juan Carlos Moreno

Montaje y Mantenimiento de Equipos

Las funciones de un antivirus son:

- Detectar los virus
- Prevenir las infecciones de los virus
- Analizar el sistema para comprobar la presencia de virus
- Eliminar los virus detectados en el sistema

¿Cómo funciona un antivirus? (I)



¿Cómo funciona un antivirus? (II)

- **Técnicas heurísticas**
- Monitorizar los programas en busca de comportamientos “sospechosos” propios de virus.
- El problema de esta técnica es que se puede sospechar de muchos programas que precisamente no son virus.
- Lo más común es encontrarnos en el mercado antivirus que combinen varias de estas técnicas para proteger el pc.

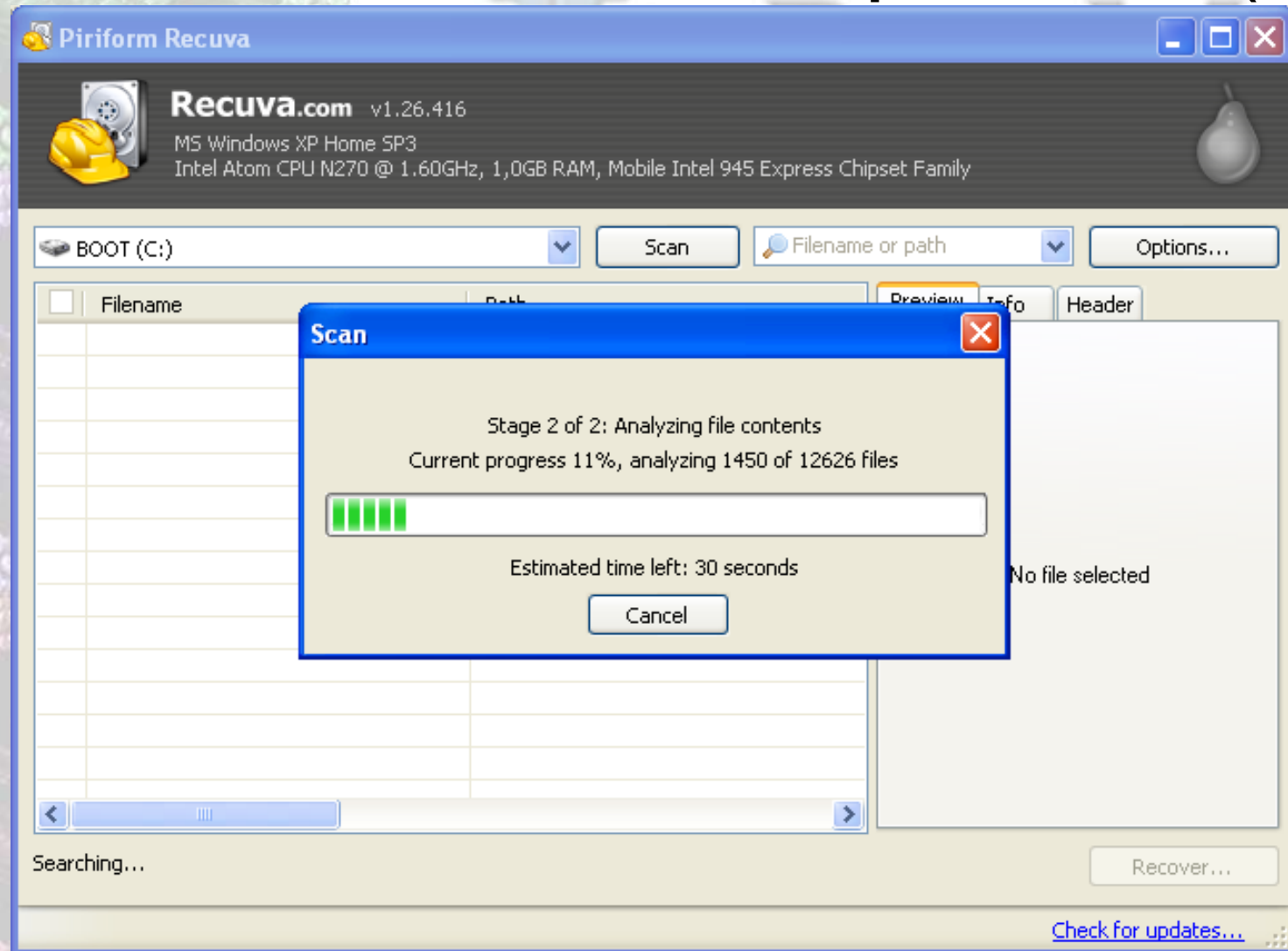
Hay que mantener el antivirus y el sistema operativo actualizado. De esa manera estaremos protegidos contra nuevos virus y agujeros de seguridad conocidos. Un antivirus o sistema no actualizado es un sistema vulnerable y fácilmente atacable por un virus.



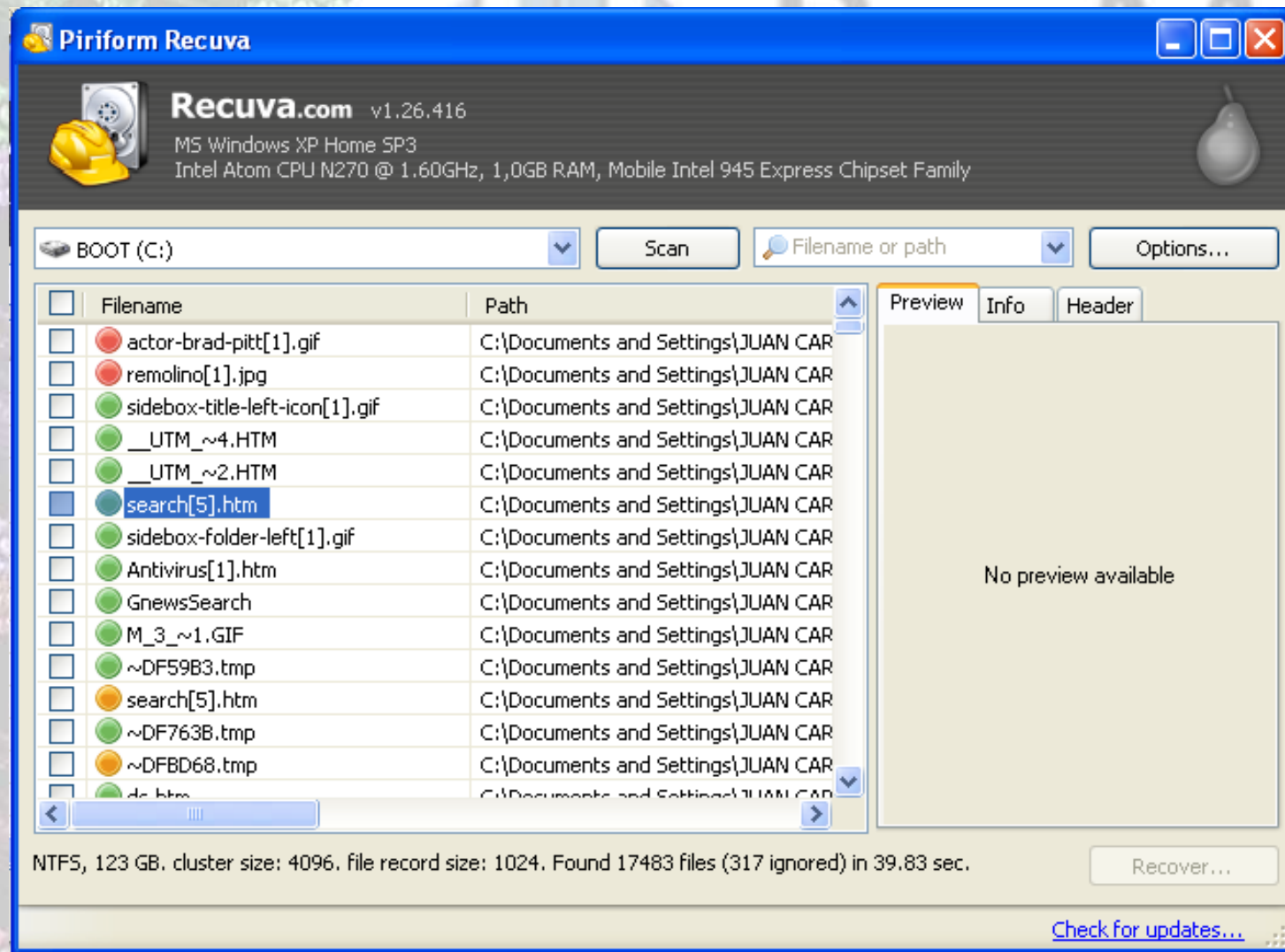
8.5 Utilidades para el mantenimiento y reparación de los sistemas informáticos.

8.5.1 Utilidades para la recuperación de ficheros

Ejercicio práctico: Recuperación de ficheros con Recuva portable (II)



Ejercicio práctico: Recuperación de ficheros con Recuva portable (III)



The screenshot shows the Piriform Recuva portable application window. The title bar reads "Piriform Recuva". The interface includes a header with the Recuva logo, version "v1.26.416", and system information: "MS Windows XP Home SP3" and "Intel Atom CPU N270 @ 1.60GHz, 1,0GB RAM, Mobile Intel 945 Express Chipset Family".

The main area displays a file list for the "BOOT (C:)" drive. The list has columns for "Filename" and "Path". The file "search[5].htm" is selected. To the right of the list is a preview pane with tabs for "Preview", "Info", and "Header". The preview pane currently shows "No preview available".

Filename	Path
<input type="checkbox"/> actor-brad-pitt[1].gif	C:\Documents and Settings\JUAN CAR
<input type="checkbox"/> remolino[1].jpg	C:\Documents and Settings\JUAN CAR
<input type="checkbox"/> sidebox-title-left-icon[1].gif	C:\Documents and Settings\JUAN CAR
<input type="checkbox"/> __UTM_~4.HTM	C:\Documents and Settings\JUAN CAR
<input type="checkbox"/> __UTM_~2.HTM	C:\Documents and Settings\JUAN CAR
<input checked="" type="checkbox"/> search[5].htm	C:\Documents and Settings\JUAN CAR
<input type="checkbox"/> sidebox-folder-left[1].gif	C:\Documents and Settings\JUAN CAR
<input type="checkbox"/> Antivirus[1].htm	C:\Documents and Settings\JUAN CAR
<input type="checkbox"/> GnewsSearch	C:\Documents and Settings\JUAN CAR
<input type="checkbox"/> M_3_~1.GIF	C:\Documents and Settings\JUAN CAR
<input type="checkbox"/> ~DF59B3.tmp	C:\Documents and Settings\JUAN CAR
<input type="checkbox"/> search[5].htm	C:\Documents and Settings\JUAN CAR
<input type="checkbox"/> ~DF763B.tmp	C:\Documents and Settings\JUAN CAR
<input type="checkbox"/> ~DFBD68.tmp	C:\Documents and Settings\JUAN CAR
<input type="checkbox"/> de.htm	C:\Documents and Settings\JUAN CAR

NTFS, 123 GB. cluster size: 4096. file record size: 1024. Found 17483 files (317 ignored) in 39.83 sec. Recover ...

[Check for updates...](#)



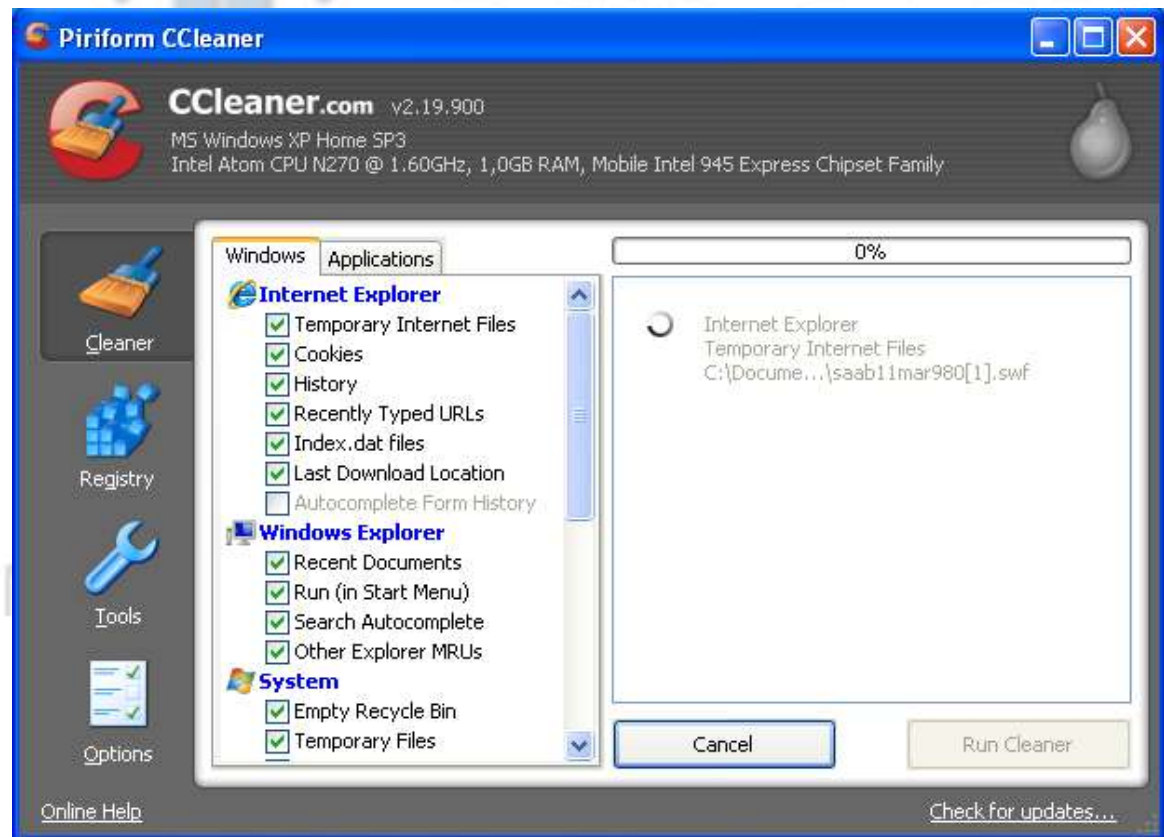
8.5 Utilidades para el mantenimiento y reparación de los sistemas informáticos.

8.5.2 Utilidades para la limpieza del registro de Windows

Juan Carlos Moreno
Montaje y Mantenimiento de Equipos

Ejercicio práctico: Limpieza del sistema con CCleaner portable

- CCleaner tiene 4 módulos principales:
 - Cleaner
 - Registry
 - Tools
 - Options





8.5 Utilidades para el mantenimiento y reparación de los sistemas informáticos.

8.5.3 Utilidades de disco

Juan Carlos Moreno
Montaje y Mantenimiento de Equipos

Gparted

OPERACIONES CON LAS PARTICIONES

DISCOS

PARTICIONES DEL DISCO

INFORMACION DE LAS PARTICIONES

OPERACIONES PENDIENTES

The screenshot shows the GParted application window titled "dev/hda - GParted". The menu bar includes "GParted", "Edit", "View", "Device", "Partition", and "Help". The toolbar contains icons for "New", "Delete", "Resize/Move", "Copy", "Paste", "Undo", and "Apply". A dropdown menu shows the selected device as "/dev/hda (74.53 GiB)". The main area displays a visual representation of the disk with three partitions: a small green partition, a large yellow partition labeled "/dev/hda2 35.07 GiB", and another large yellow partition labeled "/dev/hda3 35.56 GiB". Below this is a table with the following data:

Partition	File System	Mount Point	Label	Size	Used	Unused	Flags
/dev/hda1	fat32	/media/hda1	PQSERVICE	3.90 GiB	3.08 GiB	841.55 MiB	
/dev/hda2	ntfs	/media/hda2	ACER	35.07 GiB	34.09 GiB	1005.50 MiB	boot
/dev/hda3	ntfs	/media/hda3	DATOS	35.56 GiB	29.08 GiB	6.48 GiB	

The status bar at the bottom of the window displays "0 operations pending".

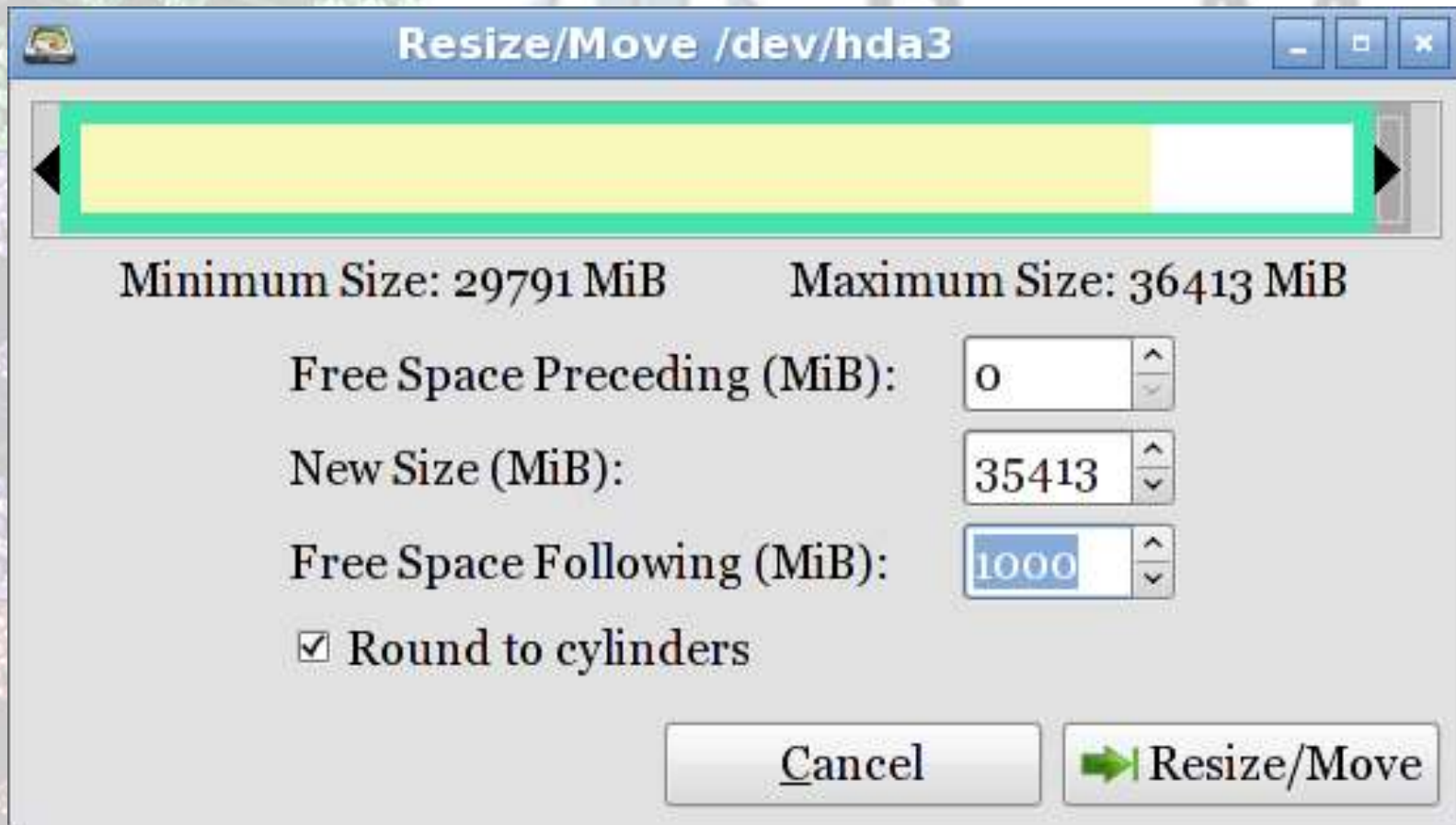
Ejercicio práctico: Redimensionamiento y formateo de una partición con Gparted (I)

Partition	File System	Mount Point	Label	Size	Used	Unused	Flags
/dev/hda1	fat32	/media/hda1	PQSERVICE	3.90 GiB	3.08 GiB	841.55 MiB	
/dev/hda2	ntfs	/media/hda2	ACER	35.07 GiB	34.09 GiB	1005.50 MiB	boot
/dev/hda3	ntfs	/media/hda3	DATOS	35.56 GiB	29.08 GiB	6.48 GiB	

0 operations pending

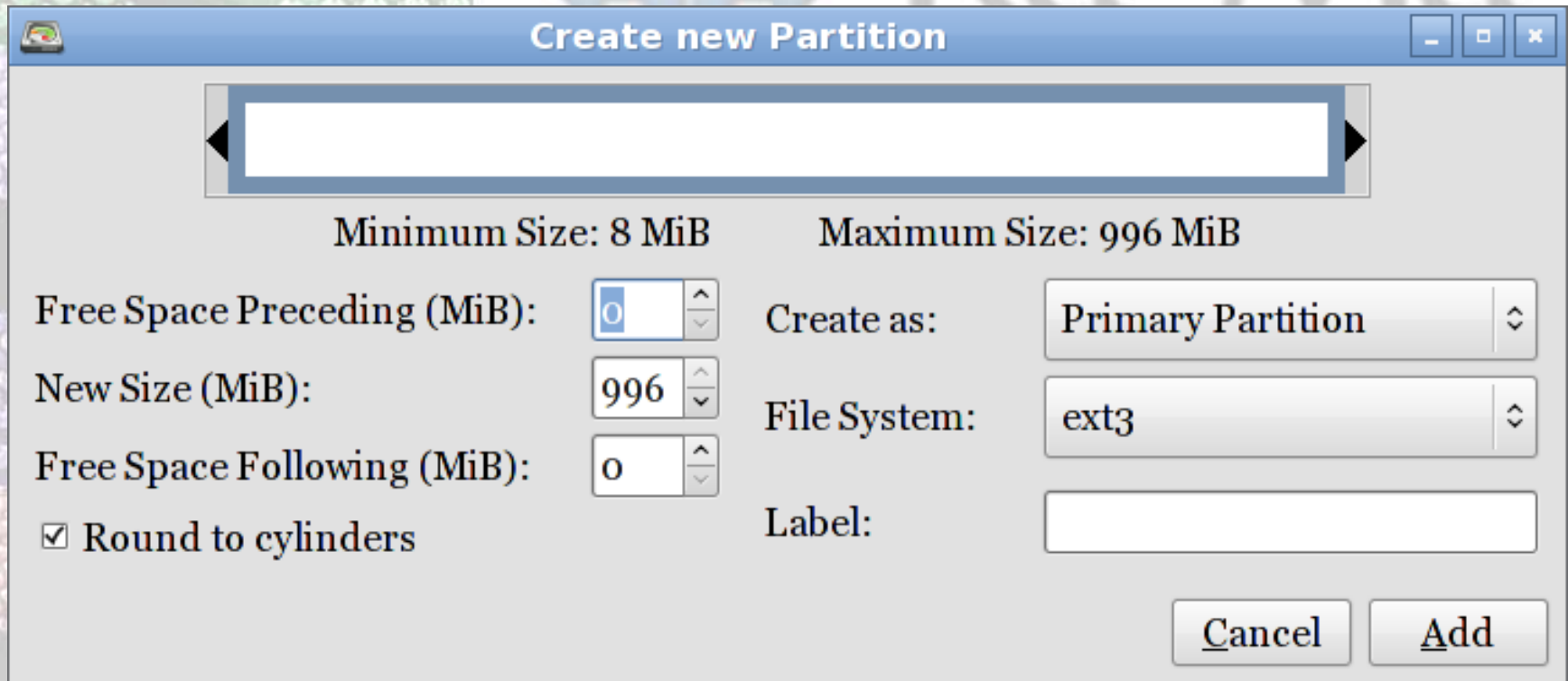
- Estado inicial del disco

Ejercicio práctico: Redimensionamiento y formateo de una partición con Gparted (II)



- PASO 1. REDIMENSIONAR LA PARTICION

Ejercicio práctico: Redimensionamiento y formateo de una partición con Gparted (III)



- PASO 2. Creación de una partición.

Ejercicio práctico: Redimensionamiento y formateo de una partición con Gparted (IV)

The screenshot shows the GParted application window titled "/dev/hda - GParted". The interface includes a menu bar (GParted, Edit, View, Device, Partition, Help) and a toolbar with buttons for New, Delete, Resize/Move, Copy, Paste, Undo, and Apply. A dropdown menu shows the selected device: /dev/hda (74.53 GiB). The main area displays a visual representation of the disk with three partitions: /dev/hda1 (3.90 GiB), /dev/hda2 (35.07 GiB), and /dev/hda3 (34.59 GiB). Below this is a table of partitions:

Partition	File System	Mount Point	Label	Size	Used	Unused
/dev/hda1	fat32	/media/hda1	PQSERVICE	3.90 GiB	3.08 GiB	841.55 MiB
/dev/hda2	ntfs	/media/hda2	ACER	35.07 GiB	34.09 GiB	1005.50 MiB
/dev/hda3	ntfs	/media/hda3	DATOS	34.59 GiB	29.08 GiB	5.51 GiB
New Partition #1	ext3			996.22 MiB	---	---

At the bottom of the window, a list of pending operations is shown:

- Shrink /dev/hda3 from 35.56 GiB to 34.59 GiB
- Create Primary Partition #1 (ext3, 996.22 MiB) on /dev/hda

The status bar at the bottom indicates "2 operations pending".

- Para finalizar el proceso deberemos de pulsar el botón "Apply".



8.5 Utilidades para el mantenimiento y reparación de los sistemas informáticos.

8.5.4 Utilidades para el apagado del sistema

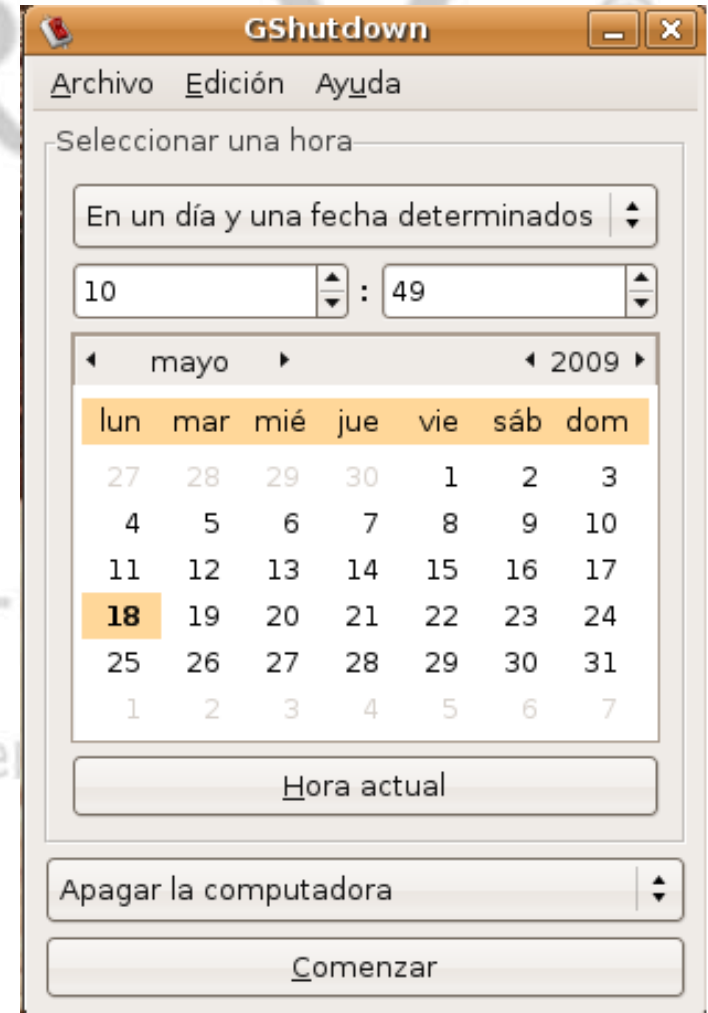
Juan Carlos Moreno
Montaje y Mantenimiento de Equipos

GShutdown para Linux

- Gshutdown es una herramienta que permite apagar/reiniciar/cerrar la sesión de nuestra computadora en Linux.

- Instalación:

sudo apt-get install gshutdown



Actividad propuesta

- Deja programado el equipo para que se apague dentro de 5 minutos y borre una carpeta temporal que hayas creado con ficheros que ya no vayas a necesitar nunca más.

Juan Carlos Moreno

Montaje y Mantenimiento de Equipos



8.5 Utilidades para el mantenimiento y reparación de los sistemas informáticos.

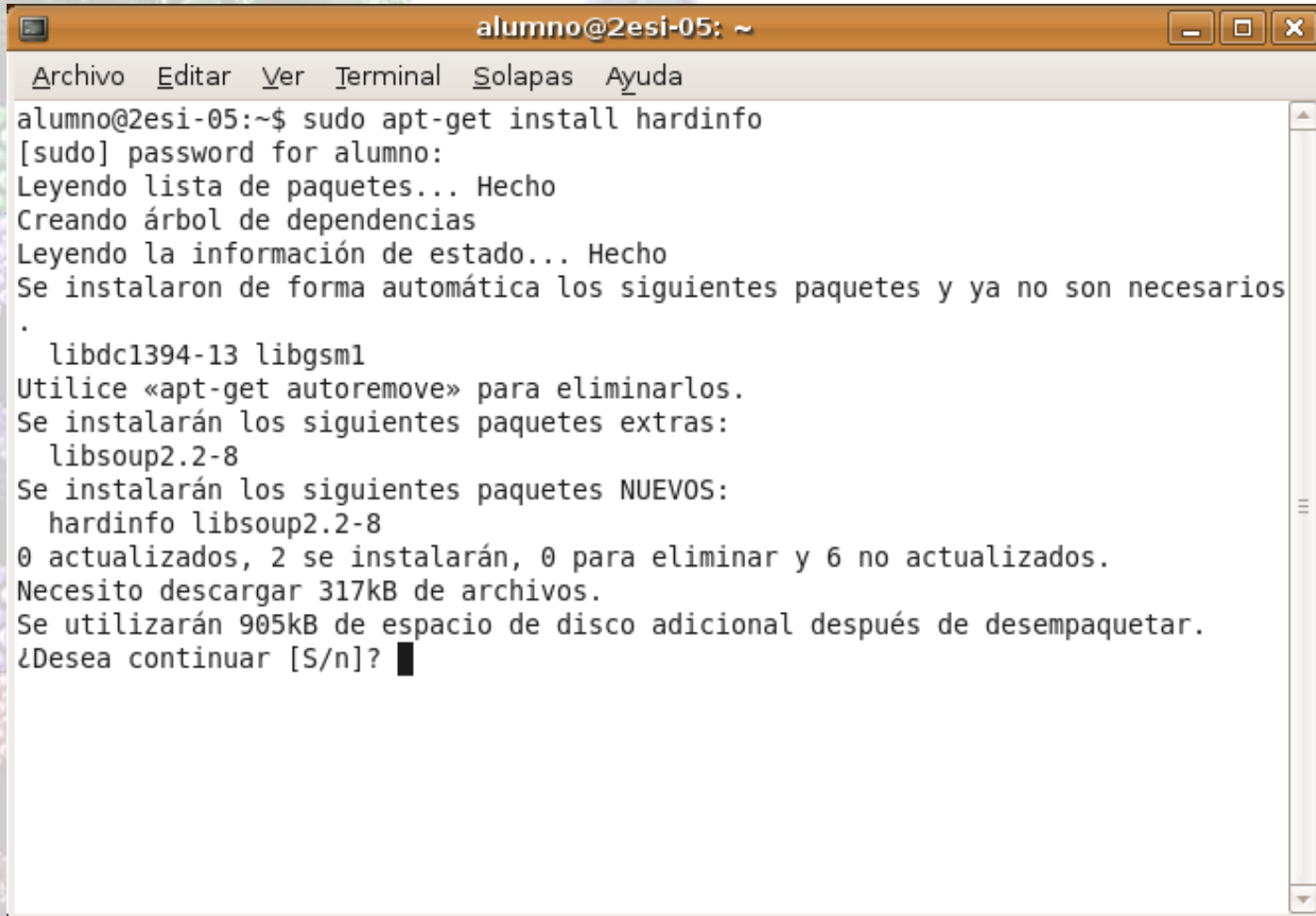
8.5.5 Utilidades de sistema

Juan Carlos Moreno
Montaje y Mantenimiento de Equipos

Hardinfo para Linux (I)

- Hardinfo es una utilidad de Linux parecida al Everest Edition® para Windows ®.
- Es GPL lo que nos permite utilizarla sin ningún tipo de problema en nuestros sistemas Linux y además de proporcionarnos toda la información respecto a nuestro hardware nos permite hacer pruebas de rendimiento del equipo.

Hardinfo para Linux (II)

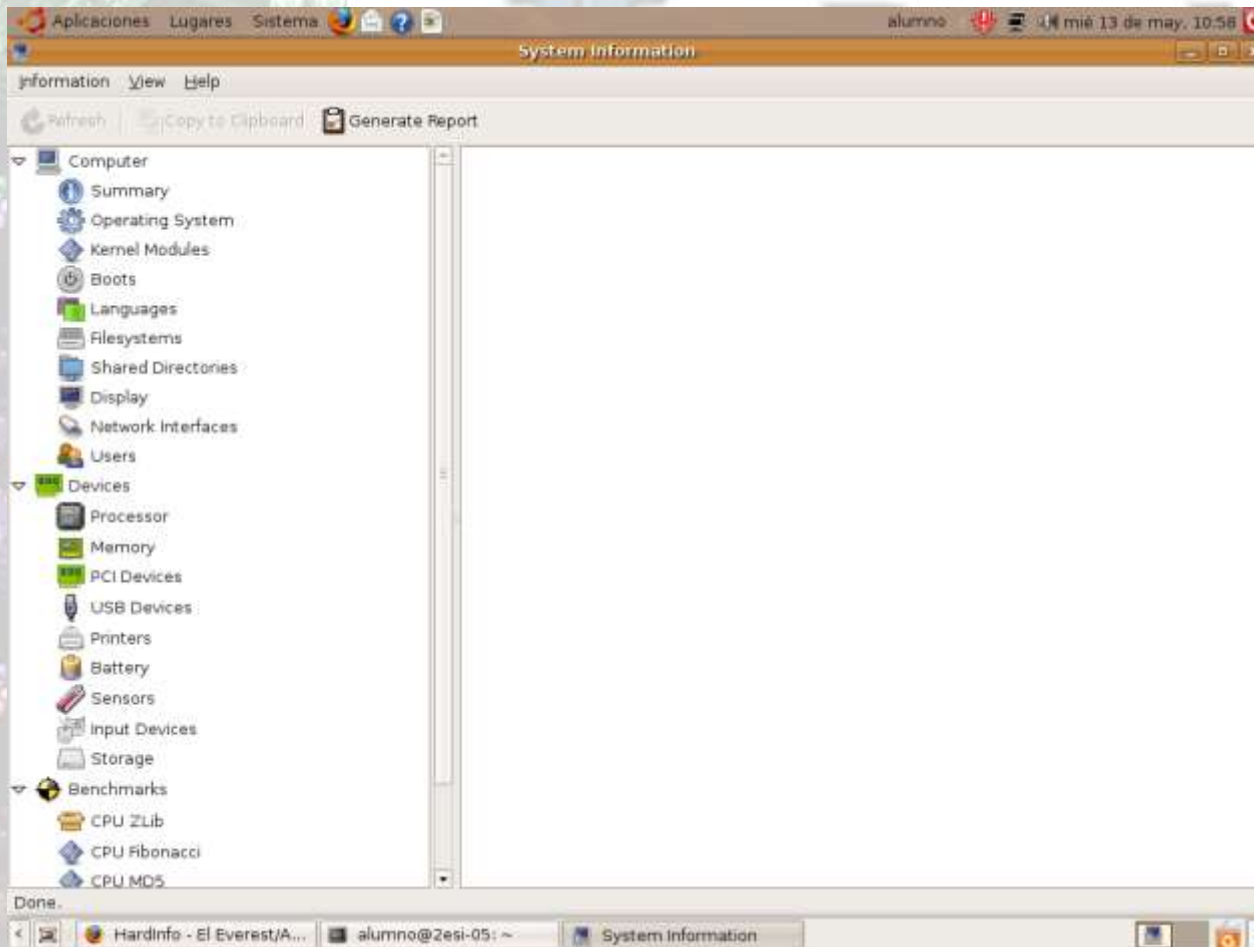


A terminal window titled 'alumno@2esi-05: ~' showing the command 'sudo apt-get install hardinfo' and its output. The output indicates that the package 'hardinfo' and its dependencies 'libsoup2.2-8' will be installed. It also shows the disk space requirements and asks for confirmation to continue.

```
alumno@2esi-05: ~  
Archivo Editar Ver Terminal Solapas Ayuda  
alumno@2esi-05:~$ sudo apt-get install hardinfo  
[sudo] password for alumno:  
Leyendo lista de paquetes... Hecho  
Creando árbol de dependencias  
Leyendo la información de estado... Hecho  
Se instalaron de forma automática los siguientes paquetes y ya no son necesarios  
.  
  libdc1394-13 libgsm1  
Utilice «apt-get autoremove» para eliminarlos.  
Se instalarán los siguientes paquetes extras:  
  libsoup2.2-8  
Se instalarán los siguientes paquetes NUEVOS:  
  hardinfo libsoup2.2-8  
0 actualizados, 2 se instalarán, 0 para eliminar y 6 no actualizados.  
Necesito descargar 317kB de archivos.  
Se utilizarán 905kB de espacio de disco adicional después de desempaquetar.  
¿Desea continuar [S/n]? █
```

- **Instalación de Hardinfo en Ubuntu.**

Hardinfo para Linux (III)



- **Herramienta Hardinfo**