

Seguridade Pasiva

Adrián Gómez Lois

Contenido

1. Obxectivos.....	3
2. Copias de seguridade con ferramentas do sistema.	4
3. Copias de seguridade con aplicación específicas.....	11
4. Comparativa de software de recuperación de datos.....	15
5. Actualización segura de sistema, virtualización de discos e borrado seguro.	18
6. Conclusións	22

1. Obxectivos.

Con estas prácticas chegaremos a ver as copias de seguridade, o clonado de unidades e o borrado seguro das mesmas.

As copias de seguridade permítenos salvagardar a información desexada en outras ubicacións ou dispositivos, dita información pode ser restaurada en calqueira punto.

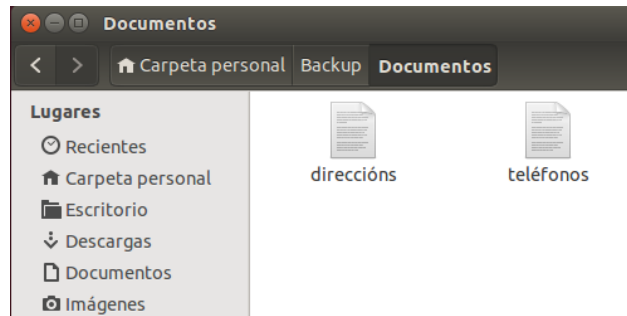
As clonacións son importantes para salvagardar os cambios actuais dun sistema e poder replicalo noutro equipo co fin de axilizarnos as labores de instalación e configuración inicial destes ou tamén usados en técnicas de análise forense.

Todo co fin de intentar protexer a nosa información almacenada. Tamén faremos borrado seguro da información o cal é un punto interesante e que se debería ter en conta en moitos casos, xa que a información sempre pode estar recuperable en calquer punto a menos que se faga o borrado seguro adecuado.

2. Copias de seguridade con ferramentas do sistema.

Realizaremos unha copia de seguridade en Linux coa utilidade tar, ferramenta a cal xa está incorporada nun sistema Ubuntu.

Creamos unha cartafol con dous ficheiros.



Realizamos a copia de seguridade da carpeta backup con tar -vcf.

```
adrian@adrian-VirtualBox: ~/Backup
adrian@adrian-VirtualBox:~/Backup$ sudo tar -vcf copiaTotal_01-12-15.tar Documentos/
adrian@adrian-VirtualBox:~/Backup$ ls -l
total 16
-rw-r--r-- 1 root root 10240 dic 16 18:51 copiaTotal_01-12-15.tar
drwxrwxr-x 2 adrian adrian 4096 dic 16 18:46 Documentos
adrian@adrian-VirtualBox:~/Backup$
```

Agora creamos un cartafol para o desempaquetado, e procemos con tar -xf.

```
adrian@adrian-VirtualBox: ~/Backup/Desempaquetado/Documentos
adrian@adrian-VirtualBox:~/Backup/Desempaquetado$ tar -xf copiaTotal_01-12-15.tar
adrian@adrian-VirtualBox:~/Backup/Desempaquetado$ ls -l
total 16
-rw-r--r-- 1 adrian adrian 10240 dic 16 18:53 copiaTotal_01-12-15.tar
drwxrwxr-x 2 adrian adrian 4096 dic 16 18:46 Documentos
adrian@adrian-VirtualBox:~/Backup/Desempaquetado$ cd Documentos/
adrian@adrian-VirtualBox:~/Backup/Desempaquetado/Documentos$ ls -l
total 0
-rw-rw-r-- 1 adrian adrian 0 dic 16 18:46 direccións
-rw-rw-r-- 1 adrian adrian 0 dic 16 18:45 teléfonos
adrian@adrian-VirtualBox:~/Backup/Desempaquetado/Documentos$
```

Temos que saber que podemos programar para así automatizar copias de seguridade.

Para iso aproveitando os ficheiros anteriores vamos facer o seguinte script. O cal fai uso de tar -cf para realizar a copia de seguridade.

```

root@adrian-VirtualBox: /home/adrian
GNU nano 2.2.6      Archivo: scriptBackups.sh      Modificado

#!/bin/bash
#      script de copia completa e incremental
#      a variable RESPALDAR indica o directorio/s a realizar os backups
RESPALDAR="/home/adrian/Documentos"

#      Directorio onde se gardarán os backups
BACKUP=/home/adrian/Backup

#      Directorio que gardará a fecha do último backup completo, variable FECHADIR
#      establécense as variables para os días da semana(DESEM), día e mes(DEM).
FECHADIR=/home/adrian/Backup
DSEM='date +%a'
DEM='date +%d%b'

#      Backup SEMANAL COMPLETO que sobrescribe o do mes anterior
if [ $DSEM = "" ]; then
tar -cf $BACKUP/copia_$DEM.tar $RESPALDAR
fi

^G Ver ayuda  ^O Guardar   ^R Leer Fich ^Y RePág.    ^K Cortar Text ^C Pos actual
^X Salir      ^J Justificar ^W Buscar    ^V Pág. Sig. ^U PegarTxt   ^T Ortografía

```

Vamos guárdalo en /usr/bin.

```

root@adrian-VirtualBox: /usr/bin
root@adrian-VirtualBox: /usr/bin# ls -l scrip*
-rwxr-xr-x 1 root root 13880 ago  5 04:20 script
-rwxr-xr-x 1 root root  579 dic 16 23:25 scriptBackups.sh
-rwxr-xr-x 1 root root  9712 ago  5 04:20 scriptreplay
root@adrian-VirtualBox: /usr/bin#

```

Agora con contrab automatizamos a lanzamento do anterior script nun día da semana e hora en cuestión, neste exemplo púxeno para que se executase o script.sh para realizar os bacukps todos os días da semana a 01:00 da mañá.

```

root@adrian-VirtualBox: /usr/bin
GNU nano 2.2.6      Archivo: /tmp/crontab.eBpPOM/crontab      Modificado

# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h dom mon dow   command
0 1 * * 0,6 /usr/bin/scriptBackups.sh

```

Simplemente quedaría darlle permisos de execución (+x) o script.sh.

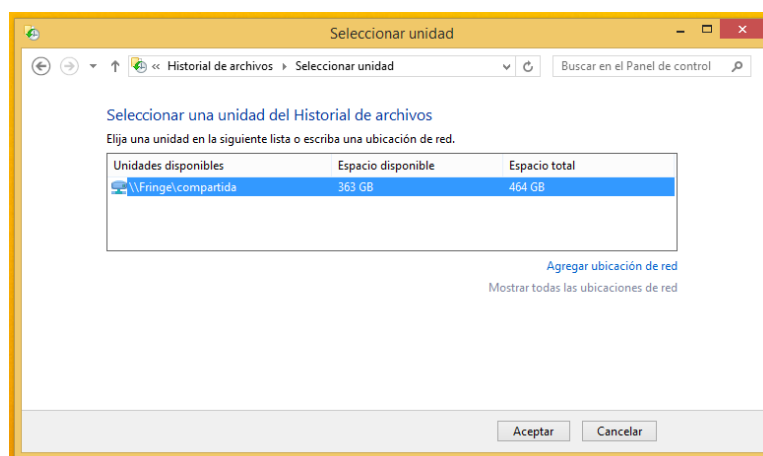
```
root@adrian-VirtualBox: /usr/bin
root@adrian-VirtualBox:/usr/bin# chmod +x scriptBackups.sh
root@adrian-VirtualBox:/usr/bin# ls -l scri*
-rwxr-xr-x 1 root root 13880 ago  5 04:20 script
-rwxr-xr-x 1 root root  579 dic 16 23:25 scriptBackups.sh
-rwxr-xr-x 1 root root  9712 ago  5 04:20 scriptreplay
root@adrian-VirtualBox:/usr/bin#
```

En Windows existe a posibilidade de facer copias de seguridade cunha ferramenta propiamente integrada.

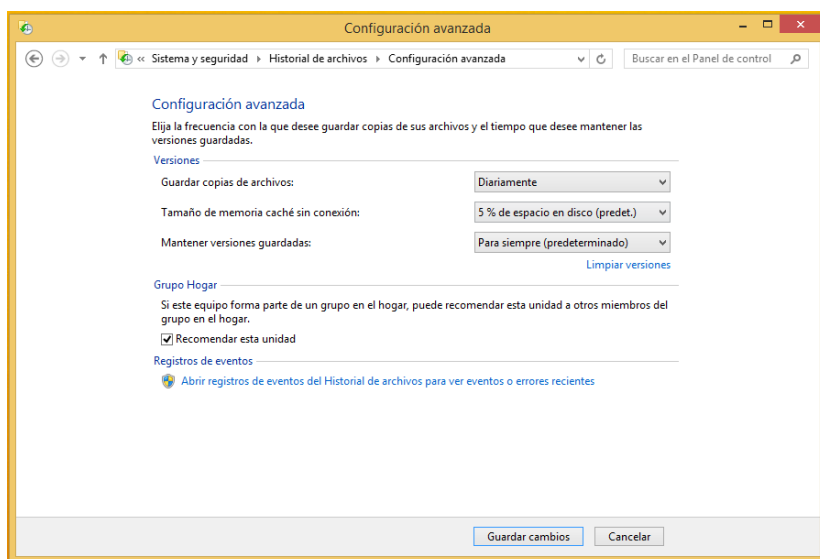
No panel de control de Windows podemos encontrar a utilidade chamada “Historial de ficheiros” (en Windows 8), no asistente pediranos unha ubicación onde almacenar a copia de seguridade.

Para facer neste exemplo dous pasos desta práctica empezarei por realizar a copia de seguridade nunha unidade de rede. Polo que selecciono outro equipo da e deixarei a copia nunha carpeta compartida.

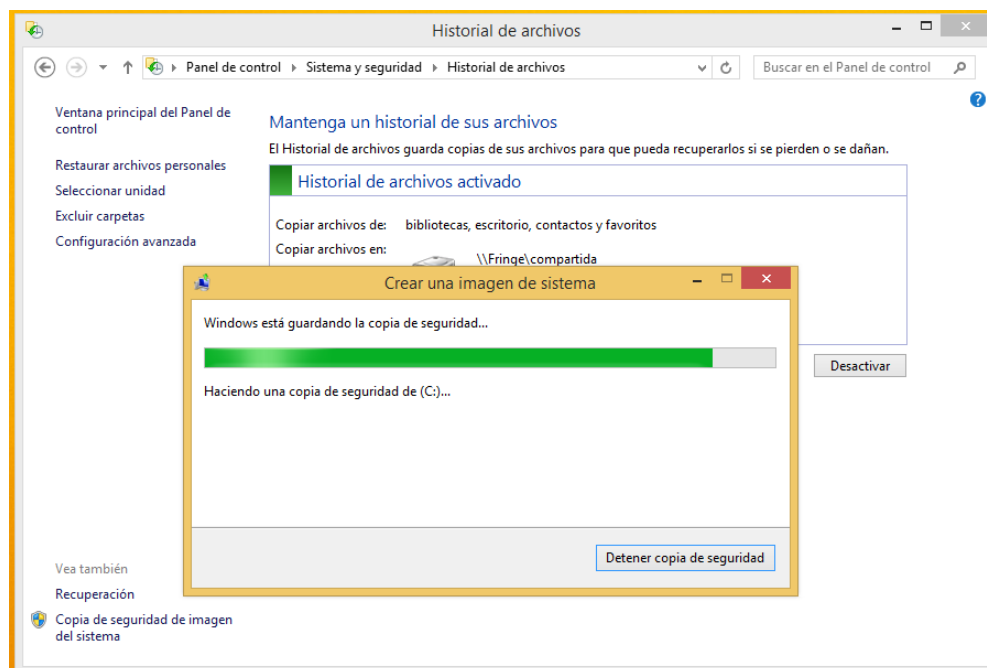
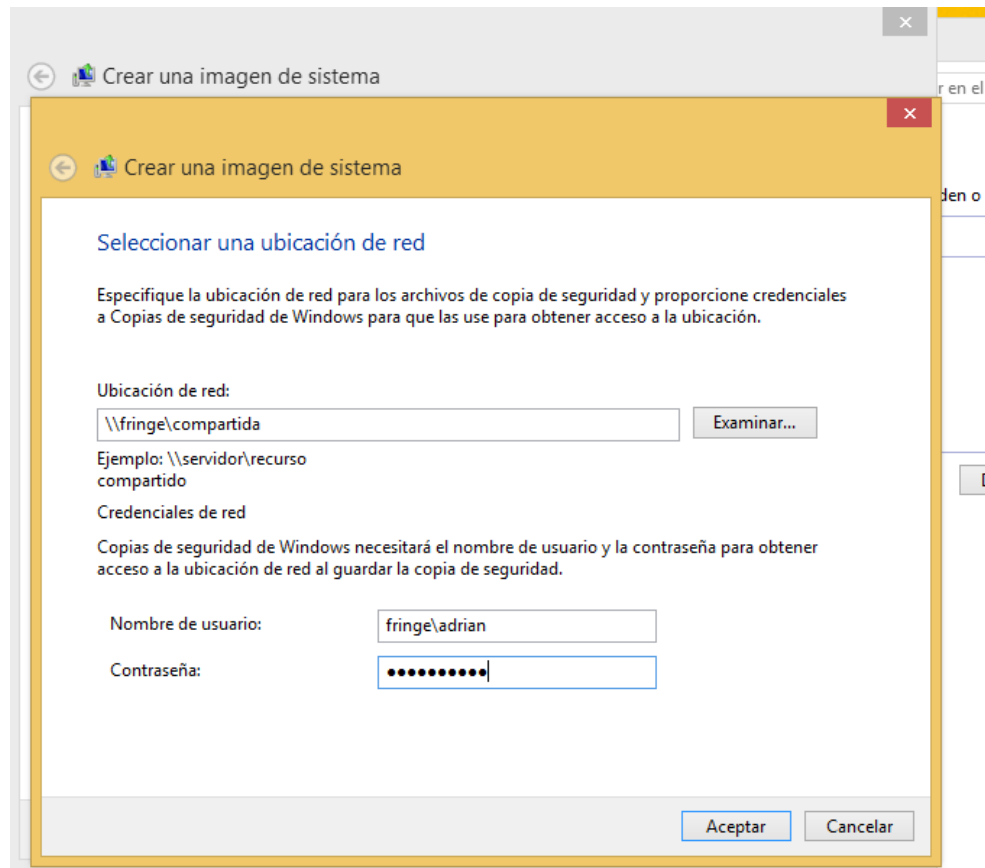
A copia contendrá unha imaxe do sistema actual completa.



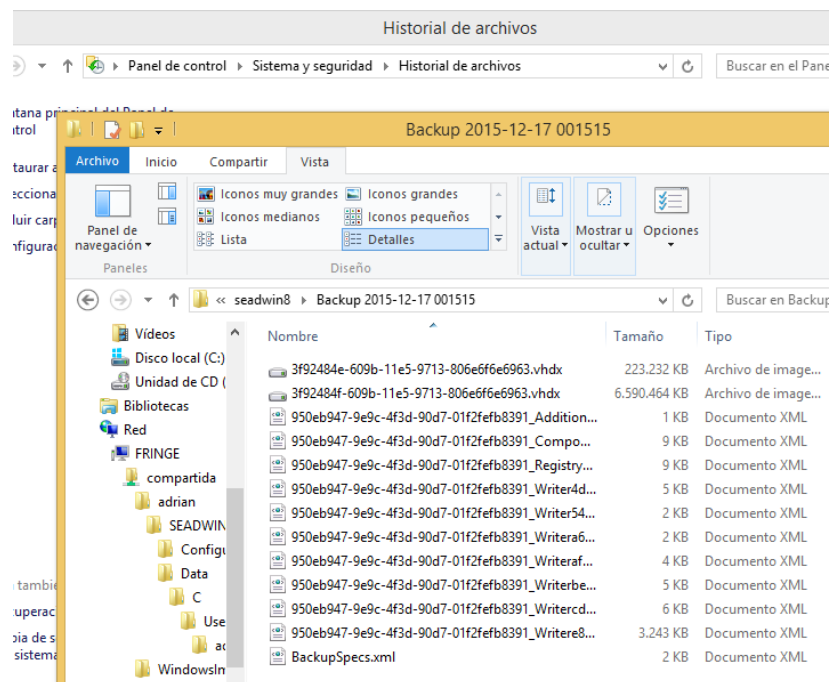
Configuro a copia como exemplo, para que se faga de forma diaria.



Referencio un usuario e contraseña para ter acceso a ese recurso compartido e poder realizar a copia de seguridad.

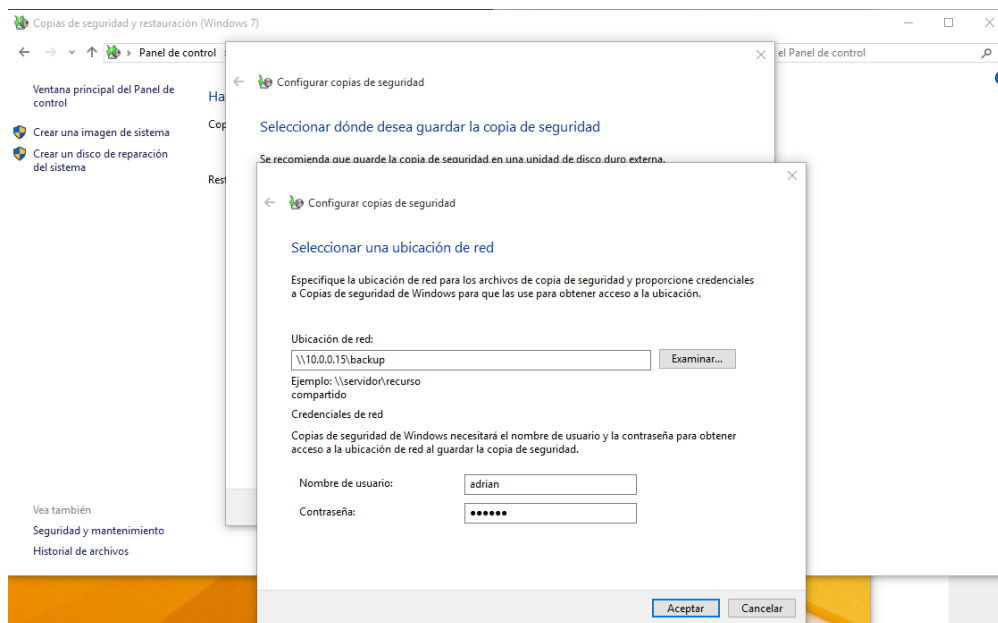


Vemos como se fixo correctamente o backup completo do sistema actual.

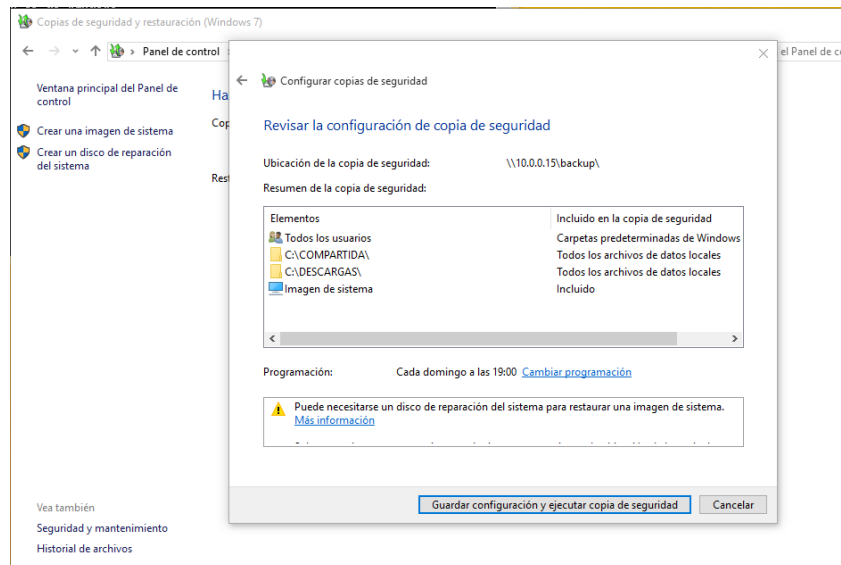
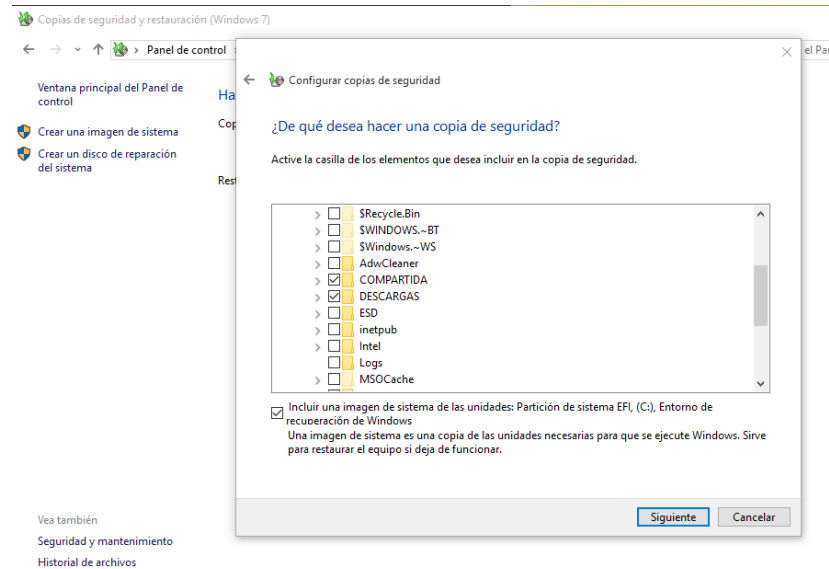


Neste outro exemplo farase unha copia de seguridade de determinadas zonas ou ficheiros internos pessoais.

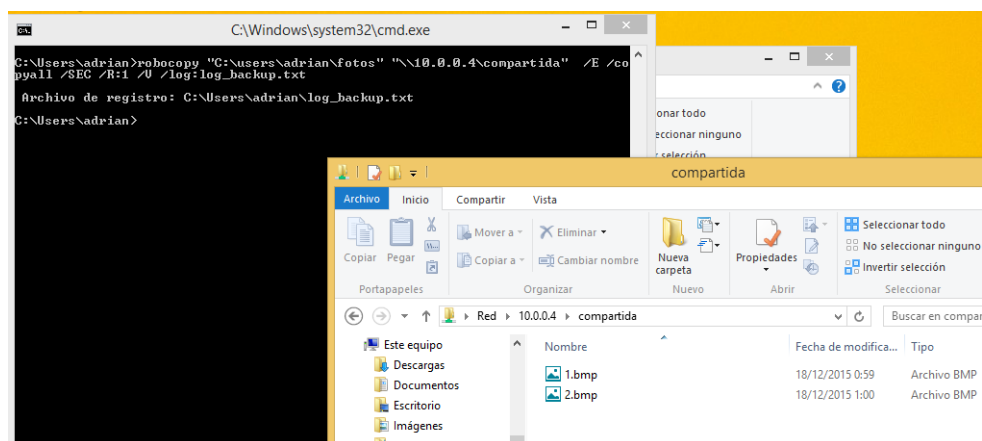
Neste caso ubicarei a copia de esos datos noutro equipo da rede.



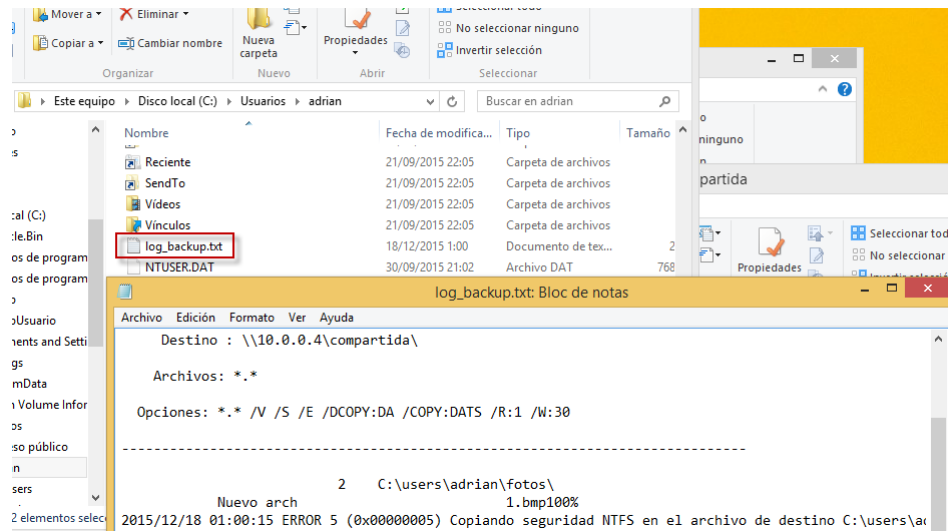
Eleximos os datos dos que queremos realizar o backup, a maiores xa lle indicamos a fecha/hora facer o backup, neste caso cada Domingo as 19:00.



Como último exemplo podemos realizar unha copia de seguridade con robocoy e que este a copia nunha unidade de rede.



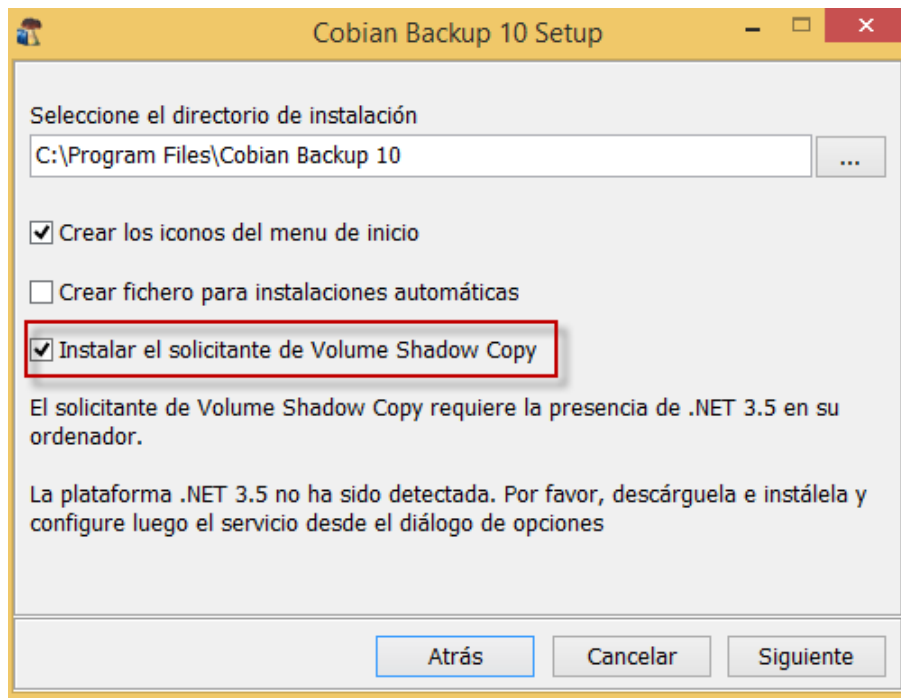
Podemos ter un control e monitoreo das nosas copias en todo momento, xa que se nos xenera un log no noso directorio persoal.



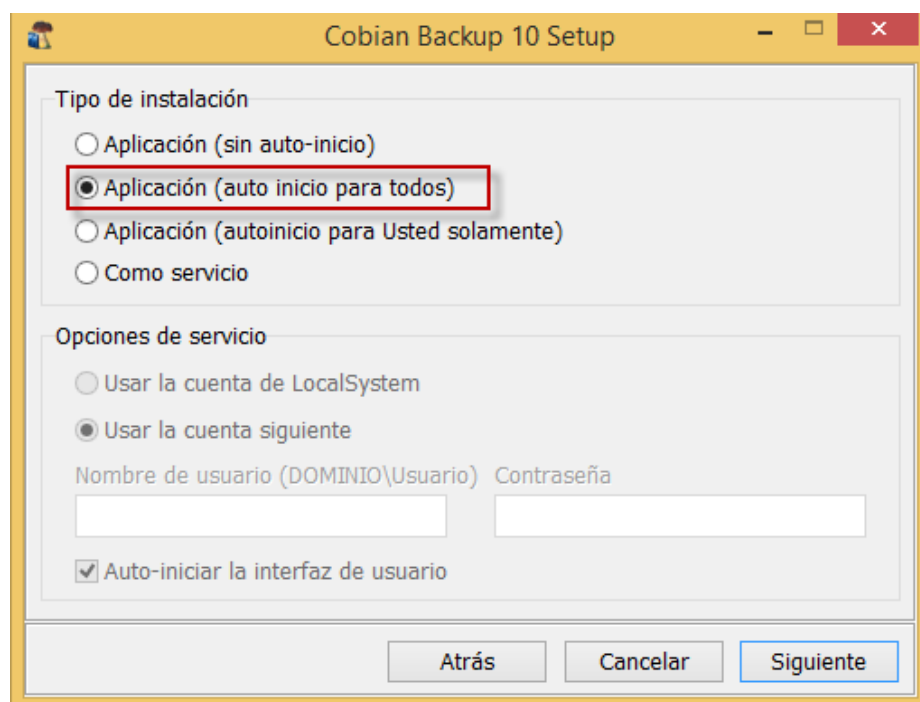
3. Copias de seguridade con aplicación específicas.

A parte das utilidades internas de cada sistema temos a opción de realizar copias de seguridade con ferramentas de terceiros.

No caso de Windows usaremos Cobian Backup 10, co solicitante de volumen ShadowCopy.

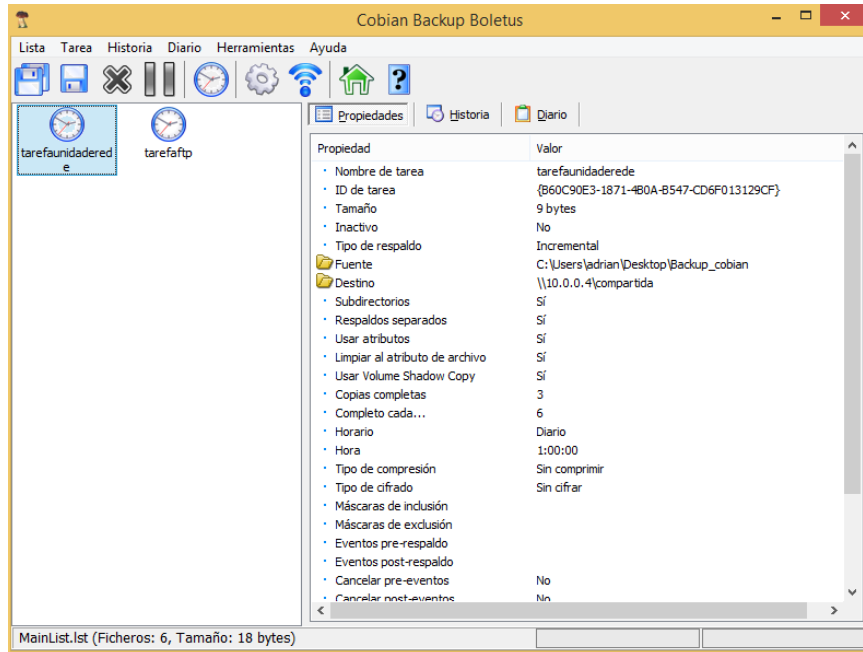


Marcamos que o instale para todos os usuarios e NON como servizo xa que de ese modo non funcionaría o ShadowCopy



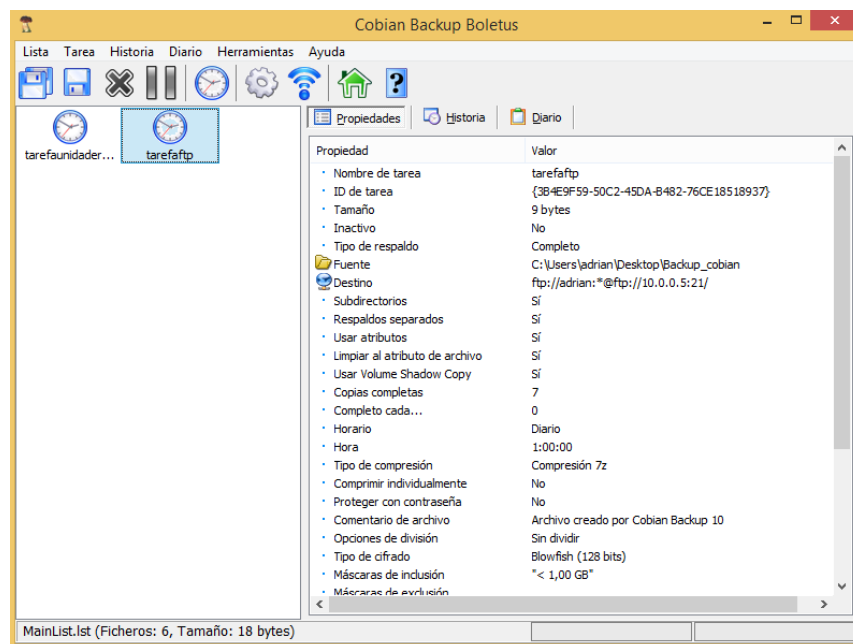
Creamos duas tarefas, a primeira chamada “tarefaunidaderedede”, cas características:

- Fará unha copia de seguridade incremental sen compresión nunha unidade de rede.
- Cada 6 copias incrementais para unha completa.
- Manteranse 3 copias completas.
- Cada copia farase diariamente ás 1.00 da mañá.

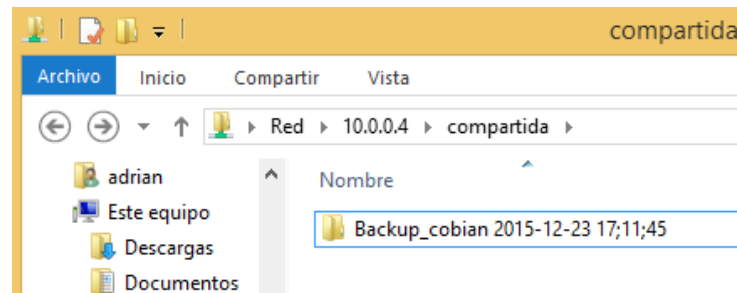


A segunda tarefa chamada “tarefaftp” terá as seguintes características principais:

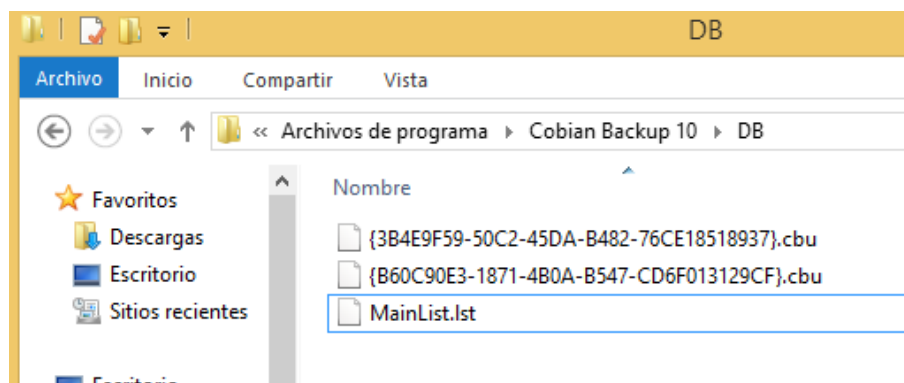
- Subirá a copia ao servidor FTP que teñades configurado.
- Fará unha copia de seguridade completa de forma manual.
- Manterá ata 7 copias completas.
- Aplica un filtro para que só almacene os arquivos de menos de 1GB.
- Estará comprimida e encriptada con AES 128 bits



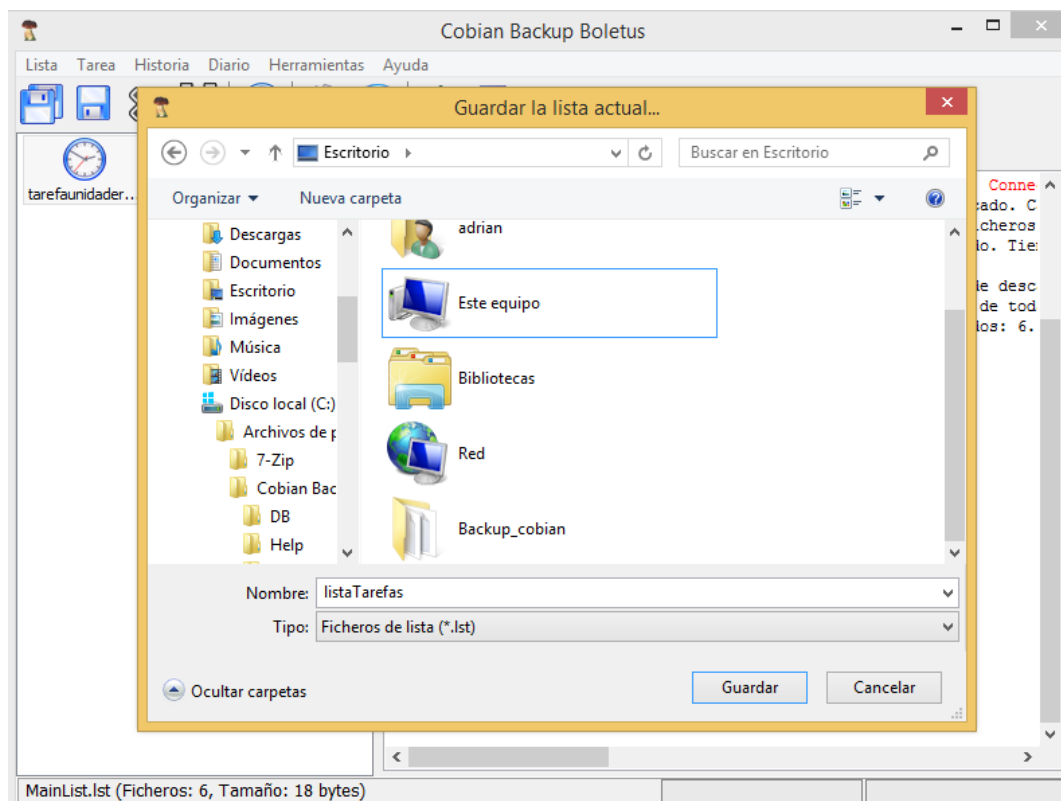
Como comprobante vemos que realizou esta copia de proba na unidade de rede indicada na primeira tarefa.



Agora gardaremos as tarefas nunha lista única. Por defecto xenérase na propia carpeta de instalación de “Archivos de Programa\Cobian Backup 10\DB” un .lst cos seus .cbu que sería os ficheiros que guardan a información de cada tarefa creada.



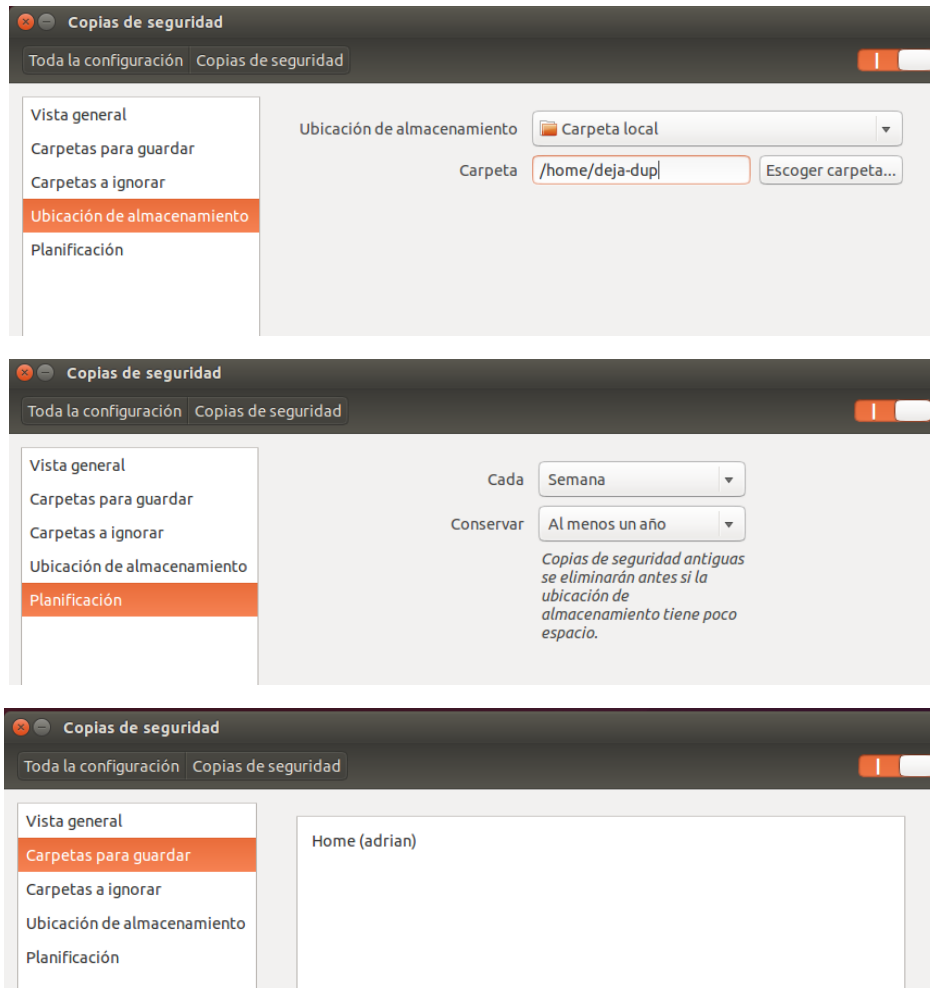
Ainda que temos tamén a posibilidade de gardar unha lista na ubicación que queiramos.



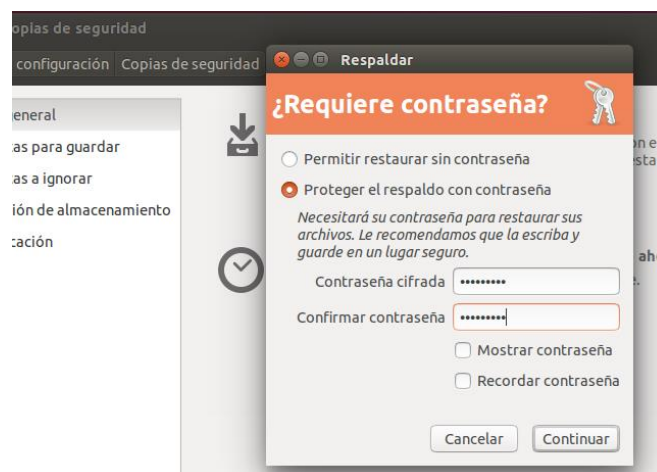
No caso de realizar copias de seguridade con software de terceiros para sistemas Linux.

Neste caso usaremos Dejà Dup, na nova versión de Ubuntu este pasa a ser “Copias de seguridade” nativamente no sistema.

Realiza un backup no propio sistema (en /home/deja-dup) de forma semanal e que se manteña 1 ano. Fai copia de /home/<<usuario>>



Adicionalmente establécese unha contrasinal para cifrar o backup.

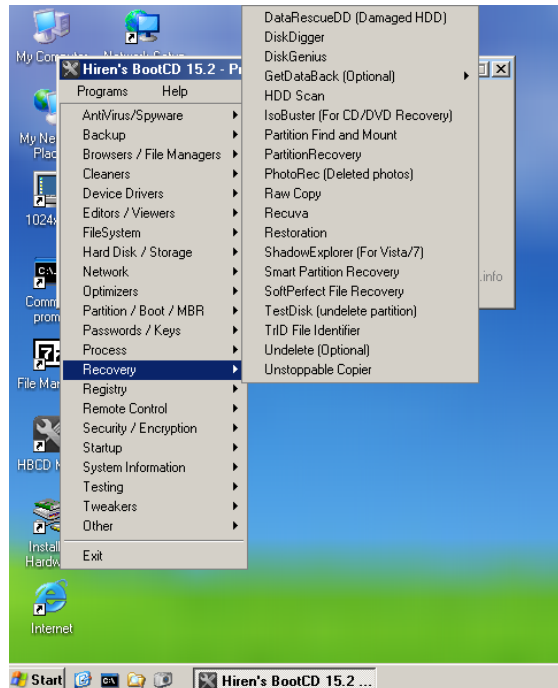


4. Comparativa de software de recuperación de datos.

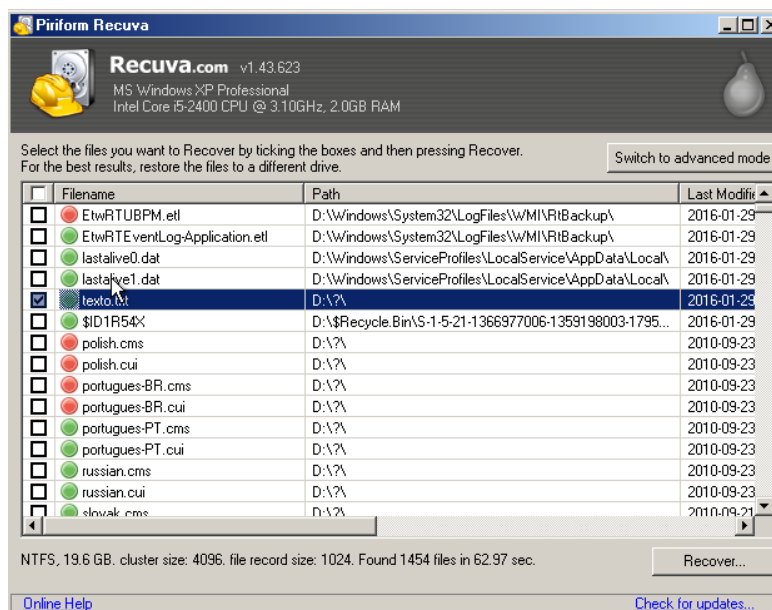
Para esta comparativa faremos uso de diversas ferramentas para a recuperación de información.

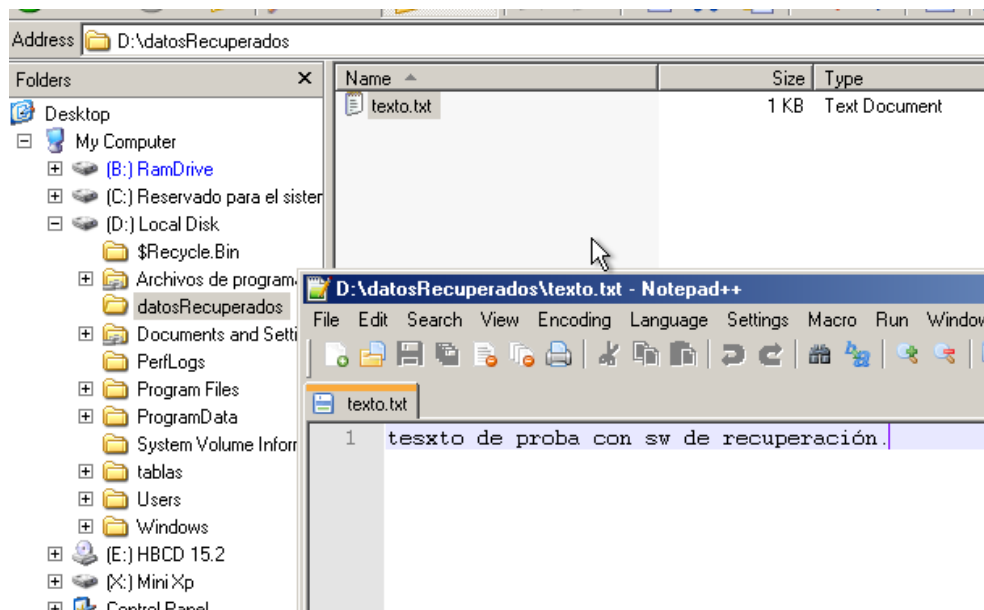
O normal nestes casos e facer uso de sistemas Live, xa que este cárgase na memoria RAM deste modo evitamos a posible alteración do disco propio do sistema o cal queremos recuperar os datos eliminados.

Comezaremos por **Recuva** executase a través de Hiren's Boot e ten unha interfaz amigable.



Neste exemplo para que se a búsqueda non tardase demasiado, creei un ficheiro de texto simple e borreino, o cal con Recuva despois de facilitarlle o path de búsqueda non lle levou demasiado tempo encontralo e recuperalo por completo.





PhotoRec é outra ferramenta especializada na recuperación de ficheiros de tipo formato de imaxen. E por consola de comandos faise intuitivo interactuar con ela, nas probas realizadas como vemos, despois de seleccionar o directorio e os principais e habituais parámetros de búsqueda, xa empezou a recuperar ficheiros que previamente se eliminaran, o único pero é que é lenta a hora de recostruír e resturar os ficheiros encontrados.

```

C:\winufo\win-forensics-tools\Recovery\PhotoRec\PhotoRec.exe

PhotoRec 7.0-WIP, Data Recovery Utility, March 2014
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/sda - 500 GB / 465 GiB (R0) - Hitachi HDS721050CLA660
Partition      Start      End      Size in sectors
 4 P MS Data    67 111 45 60743 241 42 974768128 [Basic data parti
tion]

Pass 1 - Reading sector 4808960/974768128, 187 files found
Elapsed time 0h00m31s - Estimated time to completion 1h44m12
gz: 79 recovered
bmp: 36 recovered
txt: 20 recovered
exe: 18 recovered
a: 9 recovered
png: 8 recovered
jpg: 8 recovered
gif: 3 recovered
tx?: 3 recovered
lnk: 2 recovered
others: 1 recovered
Stop

```


Foremost é outra ferramenta de recovery data, na que como exemplo intento recuperar uns ficheiros de imaxe creados. Simplemente especificamos o tipo de ficheiro co modificador `-t`, e co `-o` especificamos a directorio de saída onde se gardarán os ficheiros recuperados. É sinxela de usar, o único inconveniente e quizás que tarda un chisco máis do normal para recuperar so dúas imaxes jpg de pouco tamaño.

```

root@adrian-sead: /home/adrian
root@adrian-sead:/home/adrian# foremost -t jpeg -i /home/adrian -o /home/adrian/
recuperadoForemost
Processing: stdin
|

```

Scalpel é outra ferramenta para usada para recuperación de datos, o interesante de esta ferramenta é que no ficheiro de configuración, por defecto `/etc/scalpel/scalpel.conf` podemos elixir entre que tipos de formato podemos incluír ou excluír nas búsquedas, de modo que así se axilize o tempo de da posible recuperación de datos.

A sintaxis sería sinxela o igual que `foremost`. O único inconveniente é que non se pode usar no mesmo sistema no que se queren recuperar os datos.

`sudo scalpel /home/usuario/documentos -o /home/cartafolRecupera`

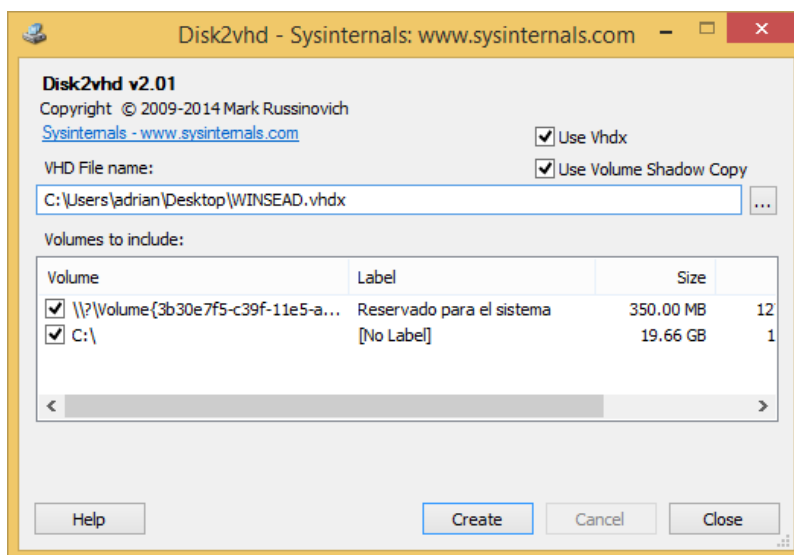
```

root@adrian-sead: /home/adrian
GNU nano 2.2.6      Archivo: /etc/scalpel/scalpel.conf      Modificado
#      art      y      150000  \x4a\x47\x04\x0e      \xcf\xc7\xcb
#      art      y      150000  \x4a\x47\x03\x0e      \xd0\xcb\x00\x00
#
# GIF and JPG files (very common)
#      gif      y      5000000  \x47\x49\x46\x38\x37\x61      \x00\x3b
#      gif      y      5000000  \x47\x49\x46\x38\x39\x61      \x00\x3b
#      jpg      y      200000000  \xff\xd8\xff\xe0\x00\x10      \xff\xd9
#
# PNG
#      png      y      20000000  \x50\x4e\x47?      \xff\xfc\xfd\xfe
#
# BMP (used by MSWindows, use only if you have reason to think there are
# BMP files worth digging for. This often kicks back a lot of false
# positives
#      bmp      y      100000  BM??\x00\x00\x00
#
^G Ver ayuda ^O Guardar ^R Leer Fich ^Y RePág. ^K Cortar Tex ^C Pos actual
^X Salir ^J Justificar ^W Buscar ^V Pág. Sig. ^U PegarTxt ^T Ortografía

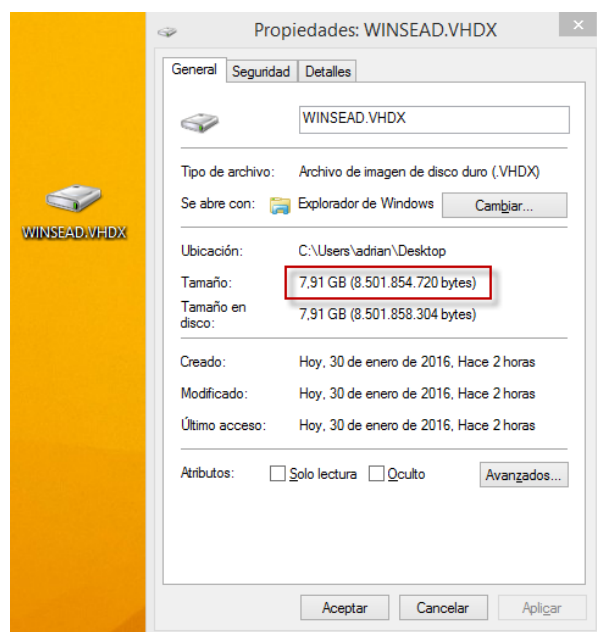
```

5. Actualización segura de sistema, virtualización de discos e borrado seguro.

Disk2vhd é unha ferramenta de sysinternal un partner importante de Microsoft, a cal está dispoñible de forma gratuita e que permite facer unha clonado do disco. Curiosamente podemos facer o clonado de dito disco co propio equipo correndo.



Vemos que aínda que todo o disco ocuparía uns 20GB, este aparece comprimido en apenas 8GB.



No caso de cargar esta imaxe nunha máquina virtual en virtualbox por problemas de compatibilidade drivers pode darse o caso de que nos falle o sector de arranque do sistema. Para recuperálo podemos seguir estos pasos:

<http://www.zonasystem.com/2014/02/recuperacion-de-arranque-en-windows-7.html>

DD (Dataset Definition) é a ferramenta por comandos usada en entornos Linux para poder facer copias exactas de unidades, cartafolios ou arquivos.

Neste exemplo copiase unha das unidades do sistema.

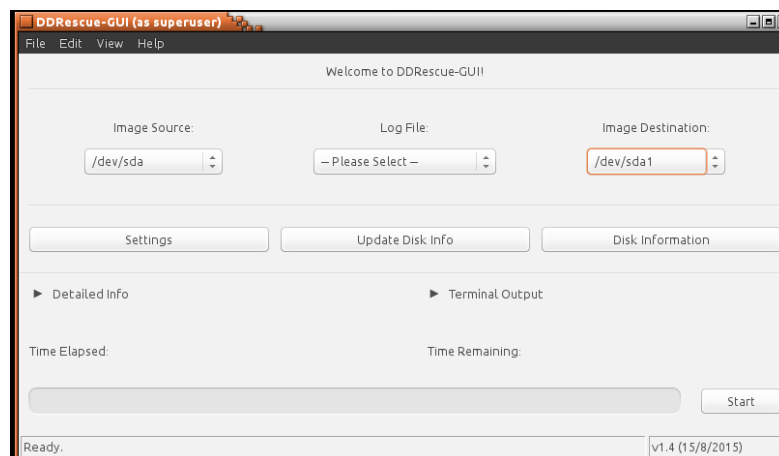
```
root@sead: /
root@sead: /# dd if=/dev/sda1 of=/backup/copia.iso
497664+0 registros leídos
497664+0 registros escritos
254803968 bytes (255 MB) copiados, 22,7244 s, 11,2 MB/s
root@sead: /#
```

O contido do ficheiro .iso

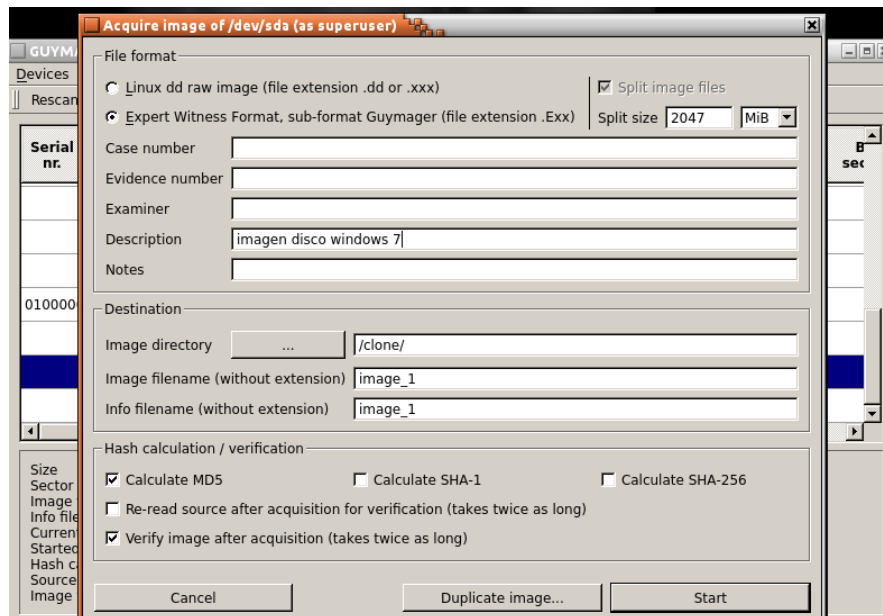
```
GNU nano 2.2.6           Archivo: /backup/copia.iso
c1017e30 t read_tsc
c1017e40 t calc_hpet_ref
c1017f00 t tsc_read_refs
c1017fb0 t calc_pmtimer_ref.part.0
c1018070 t tsc_refine_calibration_work
c1018240 T mark_tsc_unstable
c10182a0 t set_cyc2ns_scale
c1018460 t time_cpufreq_notifier
c1018550 T cyc2ns_read_begin
c1018560 T cyc2ns_read_end
c1018580 T native_sched_clock
c1018690 T sched_clock
c10186a0 T native_calibrate_tsc
c1018d00 T tsc_save_sched_clock_state
c1018d20 T tsc_restore_sched_clock_state
c1018e30 T unsynchronized_tsc
c1018e90 T calibrate_delay_is_known
c1018f20 T try_msr_calibrate_tsc
c1019040 T native_io_delay
```

Outra forma **sería a interfaz gráfica de DD** que a podemos encontrar en Caine, un LiveCD especializado con ferramentas de análise forense.

Seleccionando orixe e destino da imaxe a realizar, o destino pode ser un dispositivo extraíble.



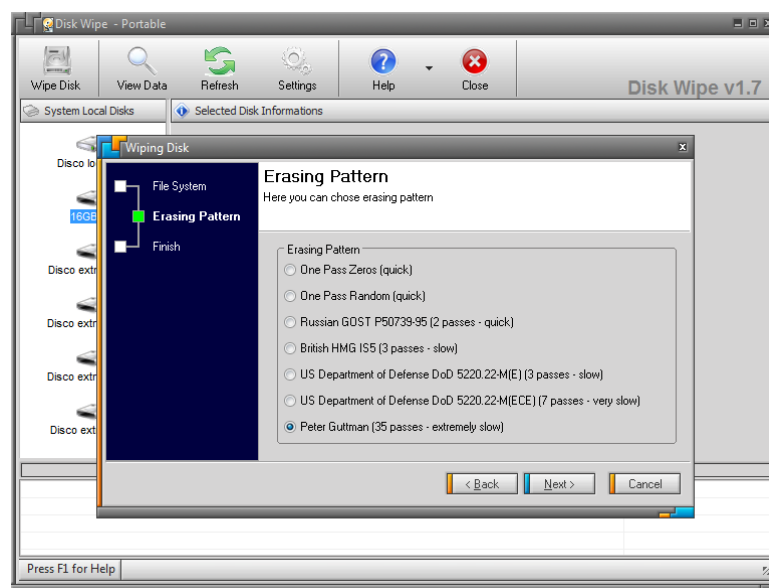
Dentro de Caine tamén podemos facer uso de **Guymager** outra ferramenta para crear imaxes ou clones de discos.



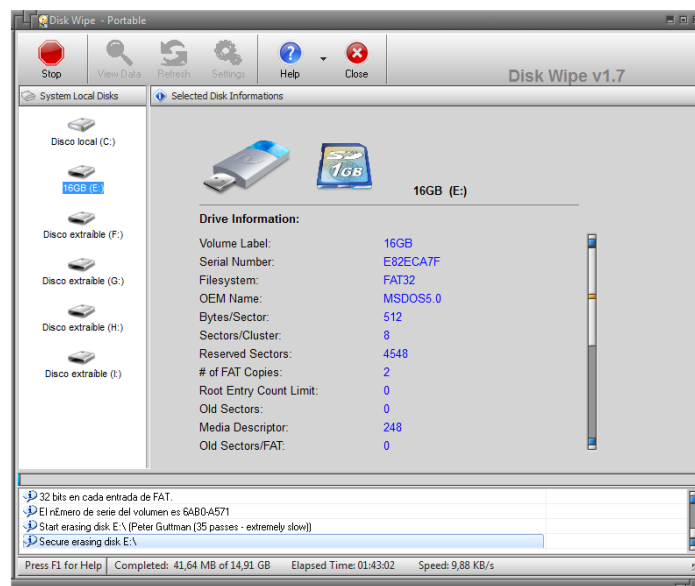
Borrado seguro de unidades.

Sempre que escribimos información nun dispositivo, aínda que o formateemos esta sigue permanecendo aí de forma oculta. Aconséllase o borrado seguro a un formateo e escribir un número de veces encima do eliminado, e dicir, basicamente unha sobreescritura, depende o número de veces será máis o menos difícil a súa recuperación.

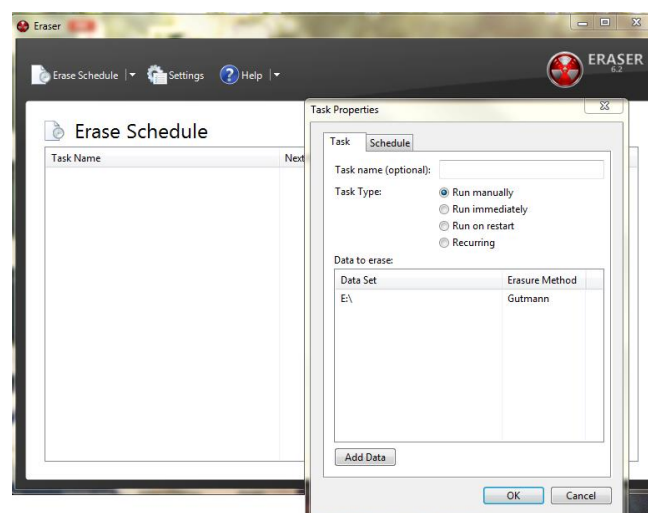
Disk Wipe é unha utilidade que nos permitirá facer un borrado seguro de dispositivos ou discos. Podendo establecer o tipo de técnica para a cantidade de veces de sobreescritura.



Neste caso realizase un borrado de 35 sobreescrituras nun pendrive de 16GB.



Eraser e outra utilidade para o borrado seguro, también con posibilidade establecer o tipo de técnica para o seu borrado seguro e a selección de unidades a borrar. Máis sinxela que Disk Wipe polo que estiven probando. Pero persoalmente quédome con Disk Wipe.



6. Conclusións

Chegamos as conclusións de que podemos facer backups de calqueira información que teñamos e as utilidades que os propios sistemas incorporan.

A información almacenada en unidades pódense replicar (clonar), recuperar información e borrar de forma segura con utilidades disponibles de forma gratuita, obviamente cas suas limitacións o tratarse de ferramentas free.

Técnicas como as de esta práctica úsanse sobretodo para o análise forense. Víronse utilidades a nivel software de sistema pero no mercado existen “station docks” de clonado nas que se fan copia bit a bit dun mesmo disco ou outro dispositivo suelen se usar a niveis profesionais debido o seu elevado coste.

Hai que entender con isto de que ninguna información está segura pese a ser borrada, e sempre hay posibilidade dunha posible recuperación da mesma, usando as utilidades axeitadas.