2011-2012

Documentación Seguridad Lógica

José Jiménez Arias

IES Gregorio Prieto

2011-2012

ÍNDICE

a) Realizar una **copia de seguridad con herramientas del sistema**:
En GNU/Linux: tar y crontab, rsync.
En Windows: Copias de seguridad y Restaurar Sistema.

b) Realizar una **copia de seguridad con aplicaciones específicas**:
En Windows: Cobian Backup
En GNU/Linux: fwbackup.

c) Utiliza una **herramienta de recuperación de datos:**
En Windows: Recuva.
En GNU/Linux: TextDisk, Foremost, Scalpel.

d) Realiza **un informe sobre los diferentes programas que existen** en el mercado informático que permite crear **imágenes de respaldo de tu equipo.**

e) Realiza **un informe con los servicios de almacenamiento que ofrecen las empresas:**
HP, Dell y ESABE:
www.hp.com www.dell.es www.esabe.com

f) Realizar en un entorno simulado un **medio de almacenamiento RAID 1 con máquinas virtuales Windows Server**.

g) Control de acceso lógico: Realiza la creación de una cuenta de usuario y su contraseña (política fuerte de contraseñas - modo comando y modo gráfico) que permite posteriormente acceder o no al sistema en sistemas Windows y sistemas GNU/Linux.

h) Verifica la auditoria de control de acceso "Visor de sucesos" de dicho usuario en Windows y Linux.

i) Descargar el programa de evaluación **CryptoForge para Sistemas Windows** en la dirección de Internet: **http://www.cryptoforge.com.ar/ y encripte y desencripte varios ficheros de tu ordenador,** utilizando diferentes sistemas de cifrado.

j) Encriptar y desencriptar ficheros de texto en sistemas GNU/Linux utilizando el comando tr que permite realizar sustituciones carácter a carácter, utilizando la ayuda del manual.

a) Realizar una copia de seguridad con herramientas del sistema:

En GNU/Linux: tar y crontab, rsync.

TAR

En el terminal

```
josejimenez@josejimenez:~/Escritorio$ tar cvf  copia.tar /home/josejimenez/Escritorio
```

```
josejimenez@josejimenez:~/Escritorio$ tar xvf  copia.tar
home/josejimenez/Escritorio/
home/josejimenez/Escritorio/hola
josejimenez@josejimenez:~/Escritorio$
```

Otro ejemplo del comando tar en este caso con extensiones .tar.bz2

```
root@josejimenez:/home/josejimenez# tar -jcvf copiatar.tar.bz2 /home/josejimenez
tar: Eliminando la `/' inicial de los nombres
/home/josejimenez/
/home/josejimenez/.sudo_as_admin_successful
/home/josejimenez/.ICEauthority
```

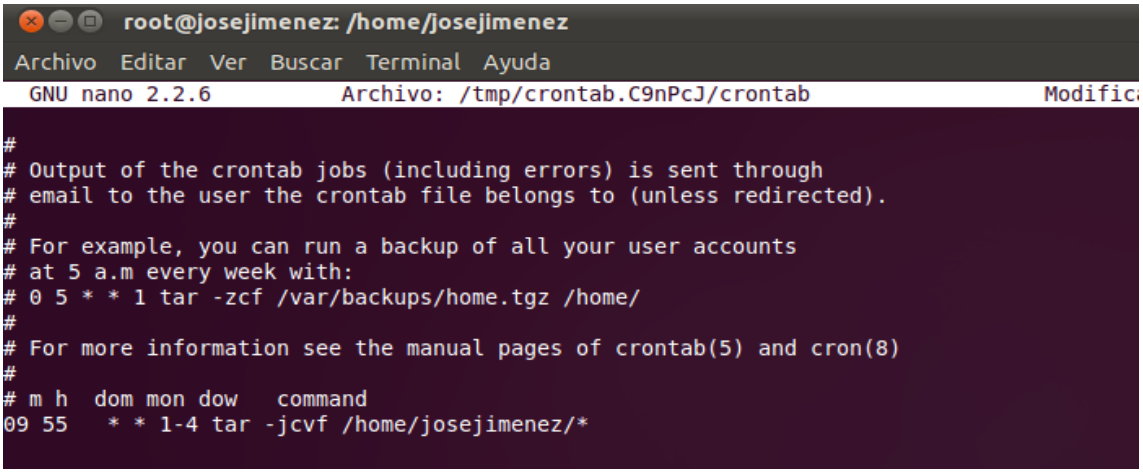
copiatar.tar.bz2

CRONTAB

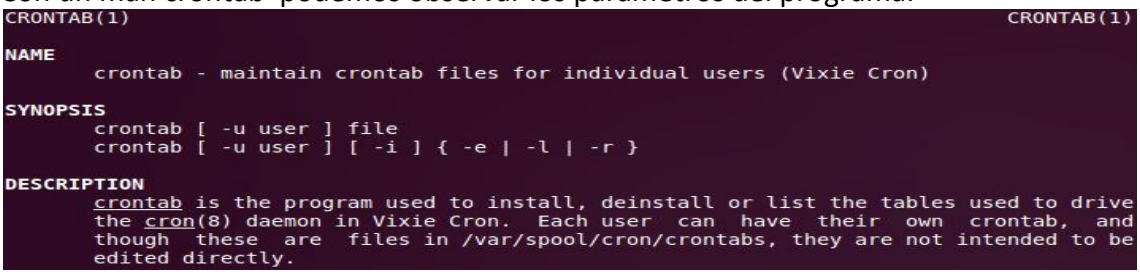
Para editar el fichero de programar la copia hemos de escribir en una terminal: *crontab –e*

A continuación se abre el siguiente archivo que hemos de configurar con los parámetros deseados.

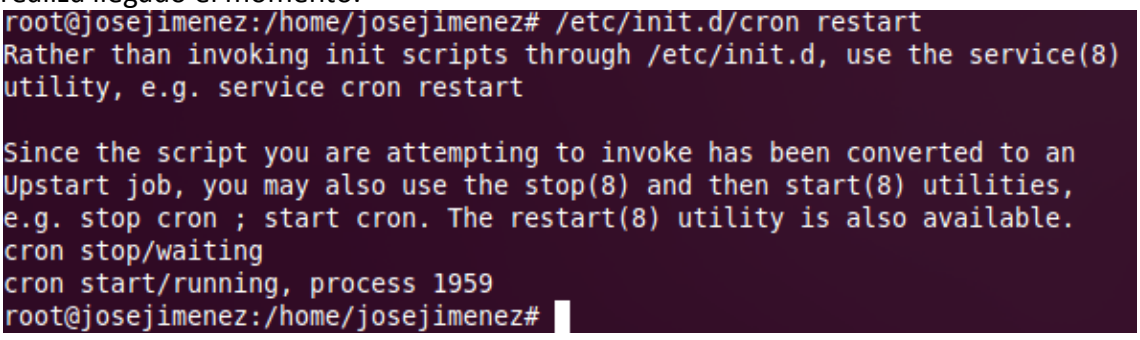
En mi caso configuro la siguiente copia:
Realice la copia a las *09:55,* que la realice de lunes a jueves, que la realice con tar, la opción del *tar* será *jcvf* y que realice una copia de los archivos que contenga el directorio */home/josejimenez*



Con un man crontab podemos observar los parámetros del programa.

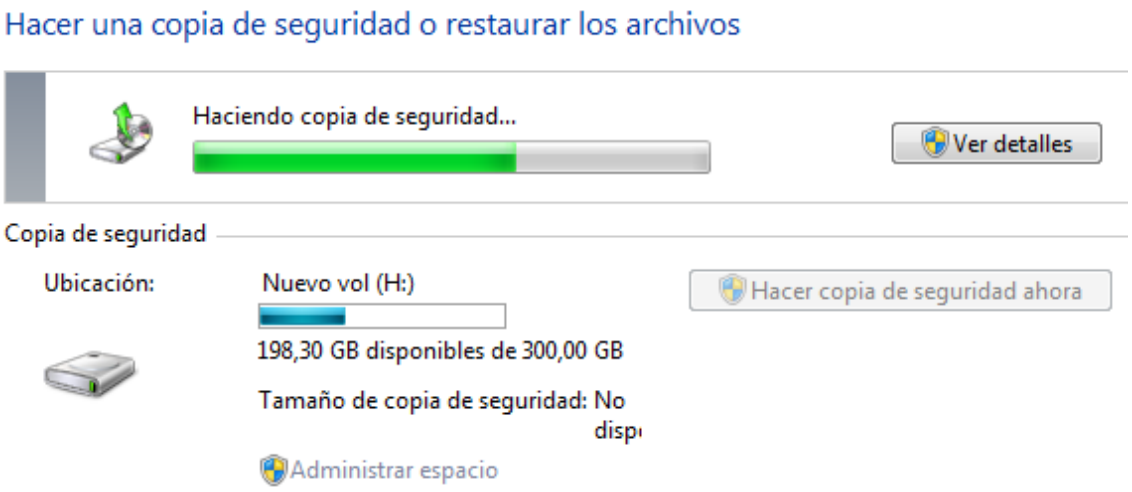


A continuación reiniciamos los servicios, vemos que está iniciado y que la copia se realiza llegado el momento.

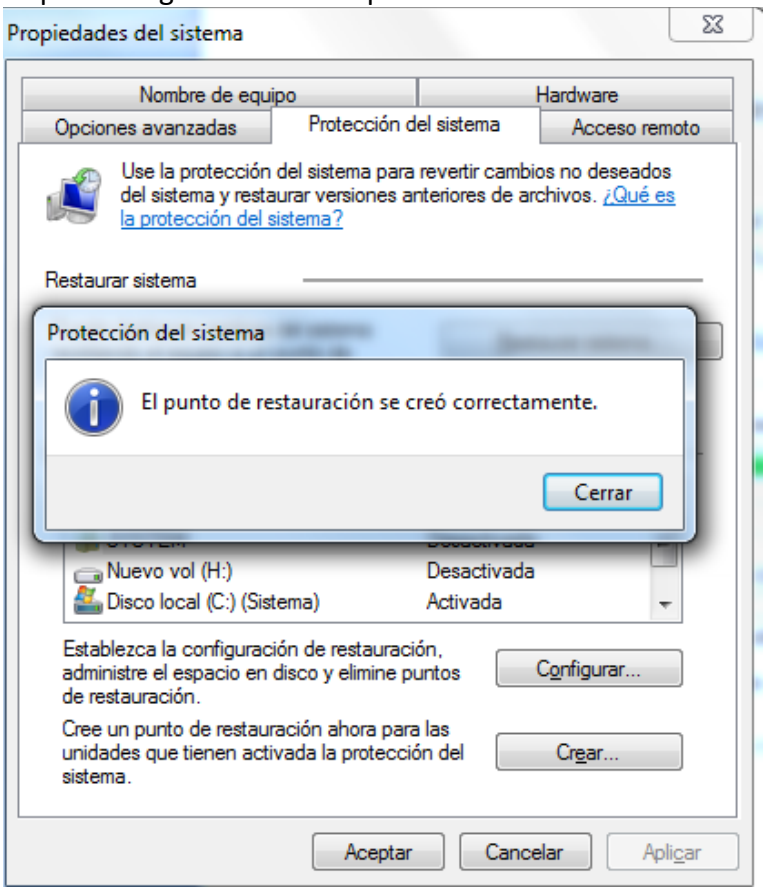


En Windows: Copias de seguridad y Restaurar Sistema.

Copia de Seguridad:
En primer lugar vamos a panel de control, copias de seguridad y restauración.
Hacer una copia de seguridad ahora.

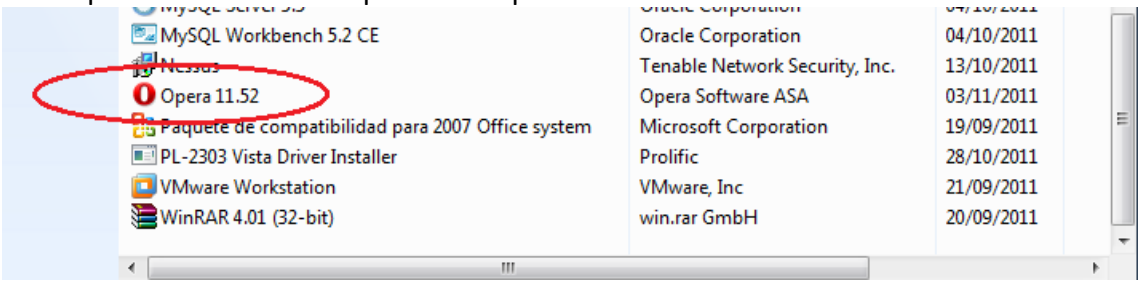


Restaurar Sistema:
En primer lugar creamos un punto de restauración.

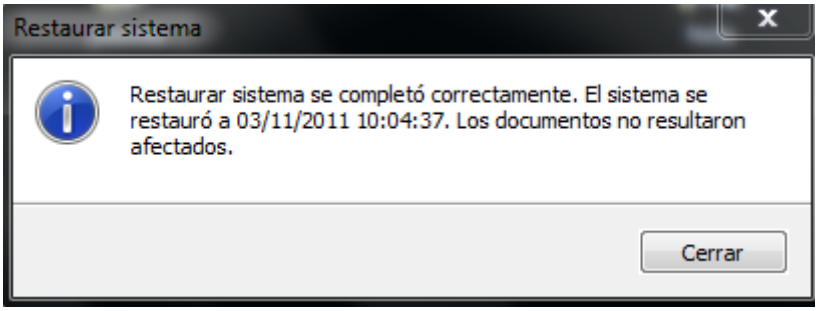


En segundo lugar instalamos un pequeño programita.
Elegimos el navegador opera.

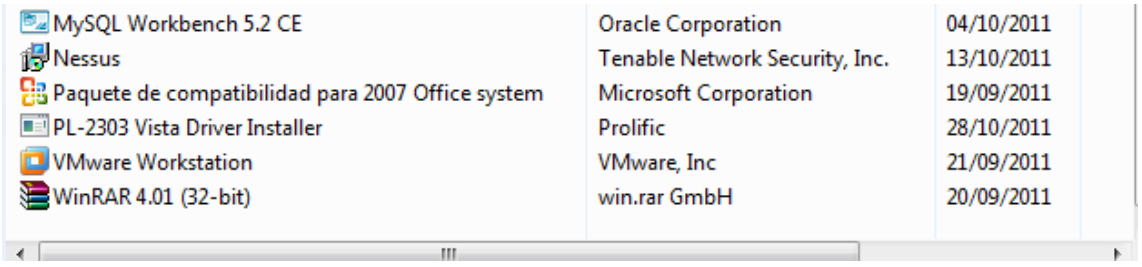
Desde panel de control comprobamos que está instalado.



Ahora restauramos el sistema para comprobar que ya no está el navegador opera instalado.



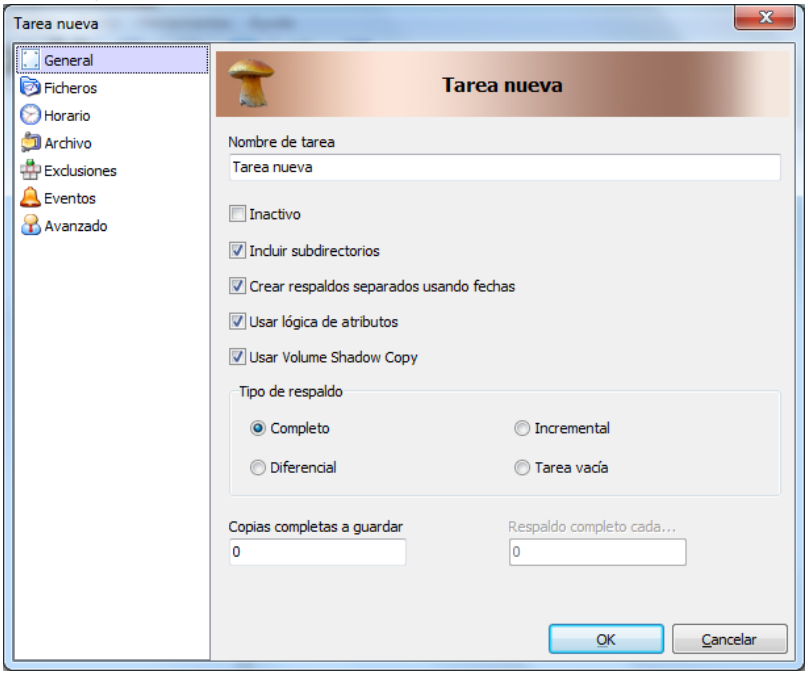
Ya no está instalado opera.



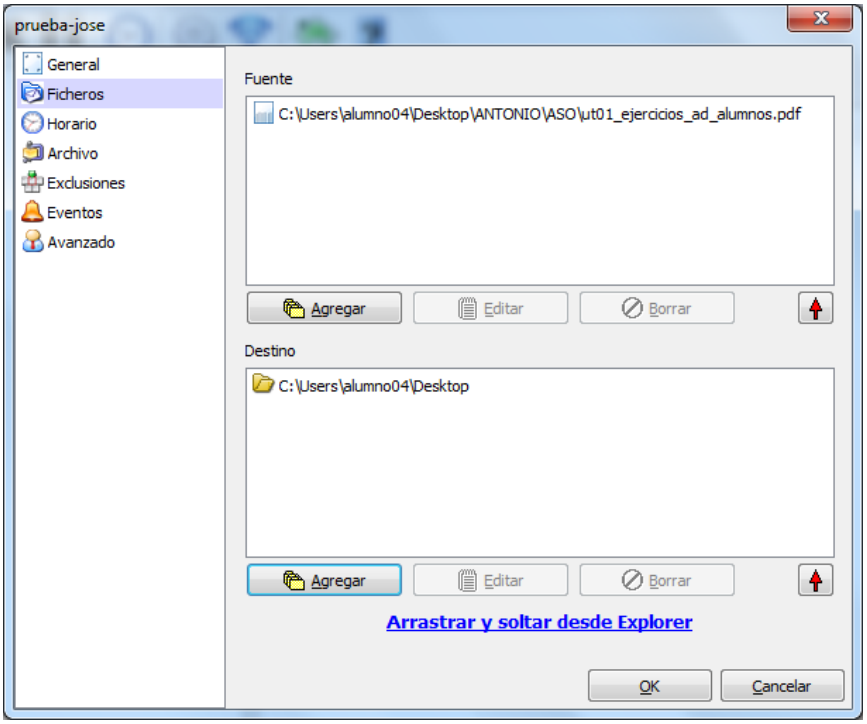
b) Realizar una copia de seguridad con aplicaciones específicas:

En Windows: Cobian Backup

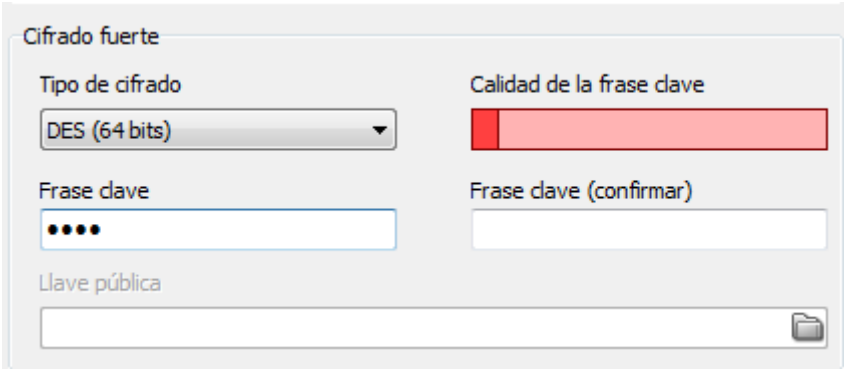
Es una aplicación bastante complete disponible en varios idiomas que permite realizar copias de seguridad.
Se basa en tareas. Para crear una debemos ir a tarea, nueva tarea.
Esta pestaña permite programar el tipo de copias, cuanto se realicen, que ficheros/directorios…



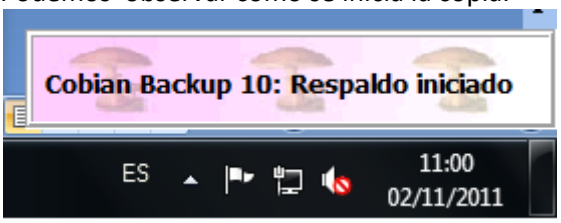
En la pestaña fichero, permite seleccionar el fichero/directorio del que hacer la copia y donde se alojará



Podemos proteger el archivo resultante de la copia comprimiéndolo y cifrándolo.



Podemos observar cómo se inicia la copia.



Cuando termina la copia muestra un fichero describiendo lo que ha realizado.

```
2011-11-02 11:00 Borrando la imagen de Volume Shadow Copy: "884292b9-1
2011-11-02 11:00 La imagen de Volume Shadow Copy ha sido borrada con é
2011-11-02 11:00 *** La tarea "prueba-jose" ha terminado. Ficheros pro
2011-11-02 11:00 ** El respaldo de "prueba-jose" ha terminado. Tiempo
2011-11-02 11:00
2011-11-02 11:00 El sistema puede ahora entrar en estado de descanso
2011-11-02 11:00 Tiempo total transcurrido en el respaldo de todas las
2011-11-02 11:00 *** Respaldo terminado. Ficheros procesados: 1. Fiche
```

En GNU/Linux: fwbackup.

Decidimos instalarlo en Ubuntu
En primer lugar descargamos el paquete de la página oficial.

- Source code (Linux): fwbackups-1.43.4.tar.bz2
- Fedora SRPM package: fwbackups-1.43.4-1.fc14.src.rpm
- Windows installer (Full*): fwbackups-1.43.4-Setup.exe
- Windows installer (Upgrade*): fwbackups-1.43.4-Lite_Setup.exe

Documentación instalación fwbackup en distintos sistemas operativos.
http://www.diffingo.com/oss/fwbackups/documentation/installation

En un nuevo terminal escribimos lo siguiente.
Instalamos los siguientes complementos.

```
sudo apt-get install gettext autotools-dev intltool python-crypto
python-paramiko python-gtk2 python-notify cron
```

```
tar xfj fwbackups.tar.bz2
cd fwbackups
```

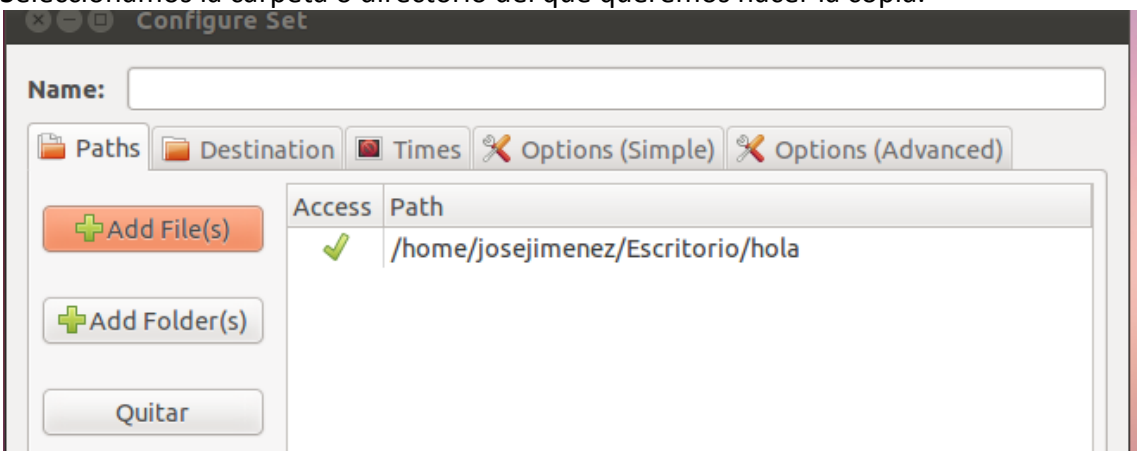
```
./configure
```

```
root@josejimenez:/home/josejimenez/Escritorio/fwbackups# ./configure
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /bin/mkdir -p
```

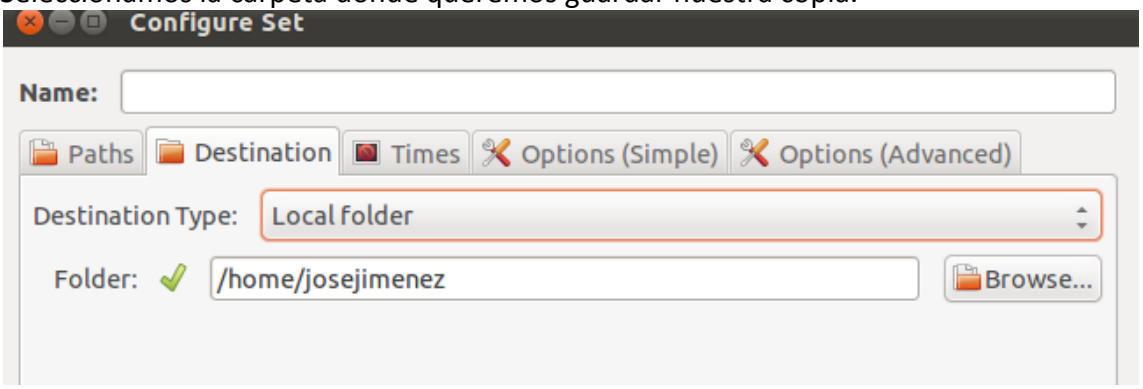
```
make && sudo make install
```

```
root@josejimenez:/home/josejimenez/Escritorio/fwbackups# make && sudo make install
Making all in bin
make[1]: se ingresa al directorio «/home/josejimenez/Escritorio/fwbackups/bin»
make[1]: No se hace nada para «all».
make[1]: se sale del directorio «/home/josejimenez/Escritorio/fwbackups/bin»
Making all in po
```

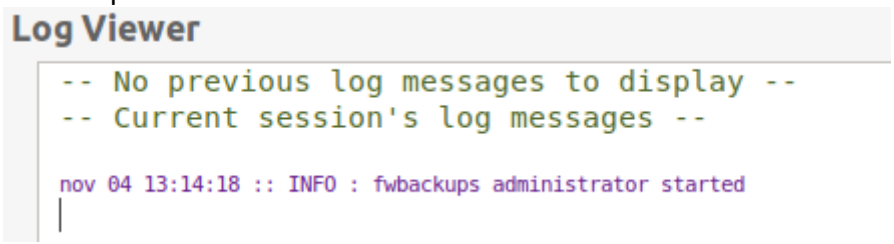
Realizamos la copia.
Pulsamos en file, new set.
Seleccionamos la carpeta o directorio del que queremos hacer la copia.



Seleccionamos la carpeta donde queremos guardar nuestra copia.



Témenos un fichero log donde podemos observar el sucesor relacionados con fwbackup.

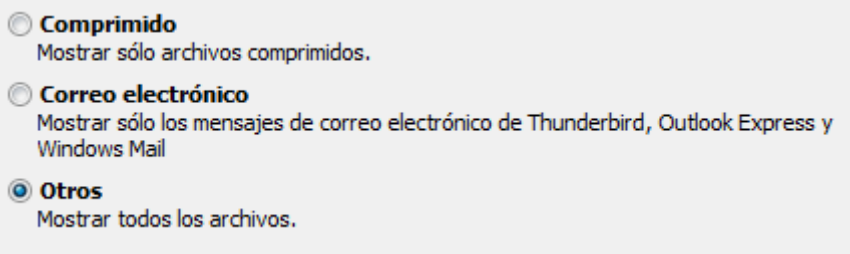


c) Utiliza una herramienta de recuperación de datos:

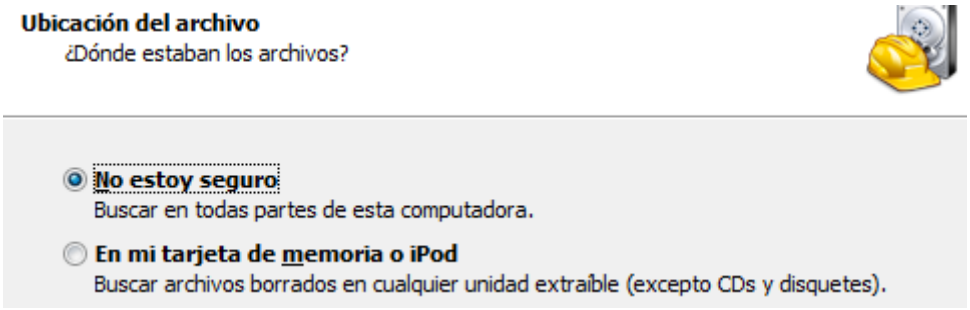
En Windows: Recuva.

Descargamos e instalamos Recuva.

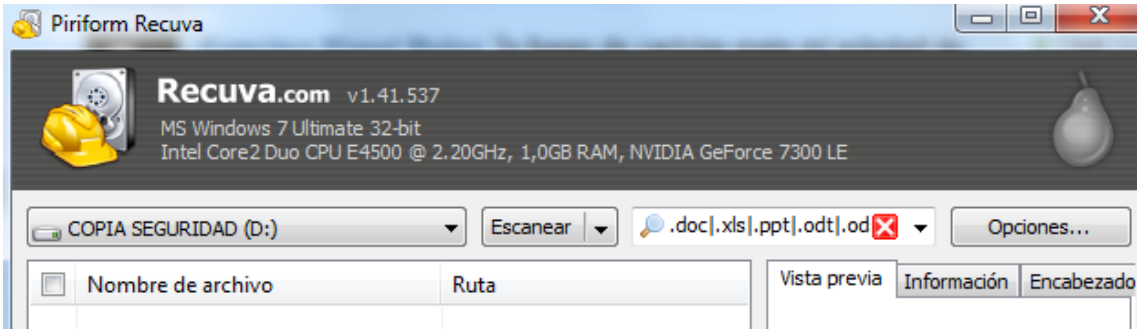
Se inicia el programa y en primer lugar nos pide el tipo de archivo que deseamos buscar.



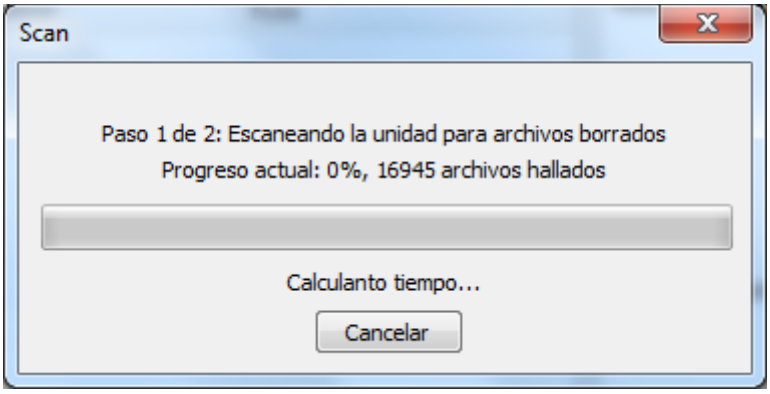
El lugar donde está ubicado:



También podemos utilizar el modo avanzado.



Iniciamos



En GNU/Linux: TextDisk, Foremost, Scalpel.

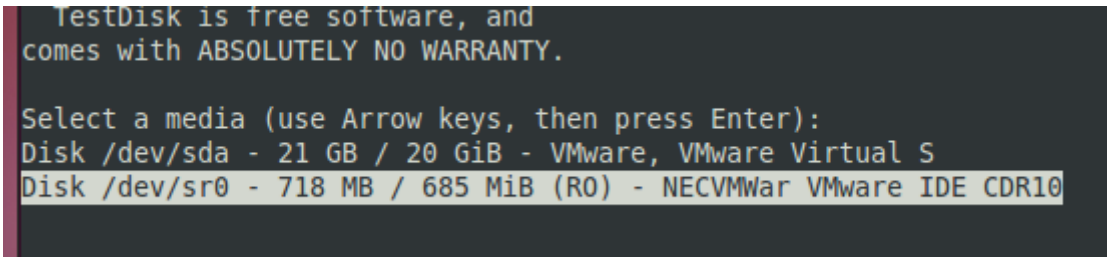
Testdisk

```
root@josejimenez:/home/josejimenez# apt-get install testdisk
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes NUEVOS:
  testdisk
0 actualizados, 1 se instalarán, 0 para eliminar y 299 no actualizados.
Necesito descargar 1596 kB de archivos.
Se utilizarán 4723 kB de espacio de disco adicional después de esta operación.
AVISO: ¡No se han podido autenticar los siguientes paquetes!
  testdisk
¿Instalar estos paquetes sin verificación [s/N]? s
```

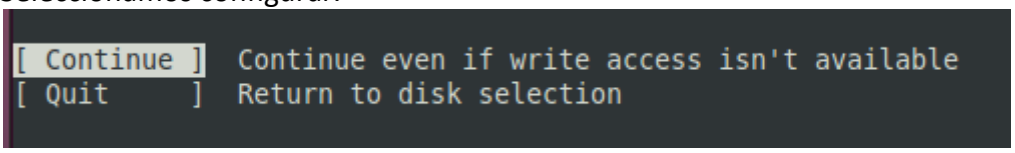
Para iniciar el programa escribimos testdisk
Muestra lo siguiente.
Pulsamos en create.

```
root@josejimenez: /home/josejimenez
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
TestDisk 6.11, Data Recovery Utility, April 2009
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org


TestDisk is a free data recovery software designed to help recover lost
partitions and/or make non-booting disks bootable again when these symptoms
are caused by faulty software, certain types of viruses or human error.
It can also be used to repair some filesystem errors.

Information gathered during TestDisk use can be recorded for later
review. If you choose to create the text file, testdisk.log , it
will contain TestDisk options, technical information and various
outputs; including any folder/file names TestDisk was used to find and
list onscreen.

Use arrow keys to select, then press Enter key:
[ Create ]  Create a new log file
[ Append ]  Append information to log file
[ No Log ]  Don't record anything
```

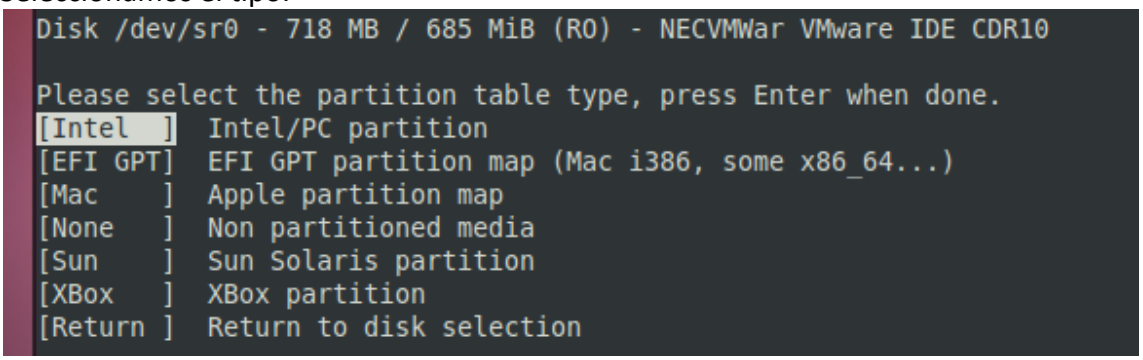
A continuación seleccionamos el disco o partición que necesitemos.



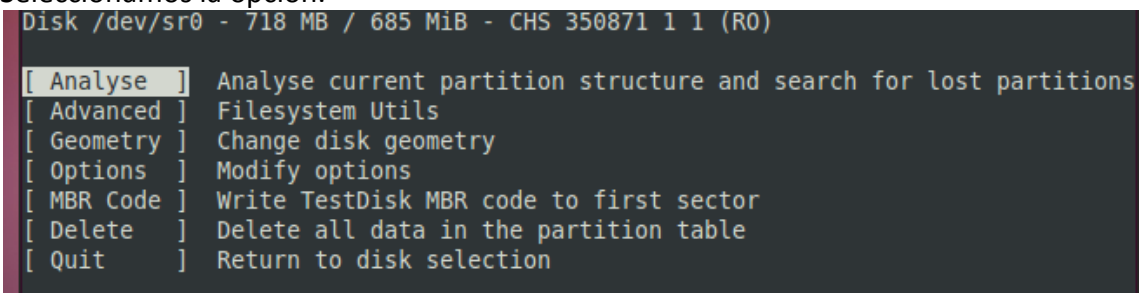
Seleccionamos configurar.

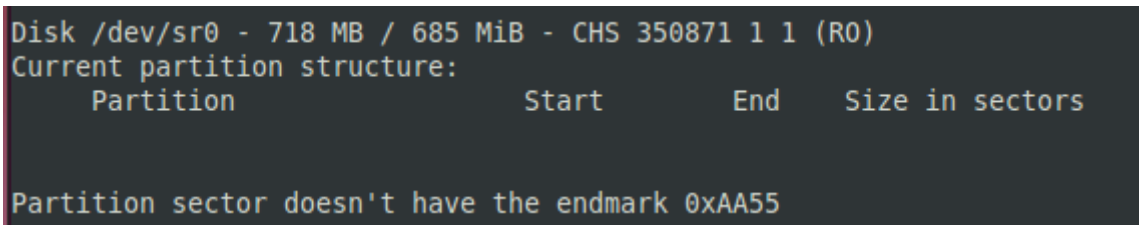


Seleccionamos el tipo.



Seleccionamos la opción.





Analiza la unidad.

```
Disk /dev/sr0 - 718 MB / 685 MiB - CHS 350871 1 1 (RO)
Analyse cylinder 163438/350870: 46%
```

A continuación pulamos L para el backup.

```
Disk /dev/sr0 - 718 MB / 685 MiB - CHS 350871 1 1 (RO)
Choose the backup you want to restore:
```

FOREMOST

Instalamos el programa

```
root@josejimenez:/home/josejimenez# apt-get install foremost
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes NUEVOS:
  foremost
0 actualizados, 1 se instalarán, 0 para eliminar y 299 no actualizados.
Necesito descargar 42,8 kB de archivos.
Se utilizarán 143 kB de espacio de disco adicional después de esta operación.
AVISO: ¡No se han podido autenticar los siguientes paquetes!
  foremost
¿Instalar estos paquetes sin verificación [s/N]? s
```

Ejecutamos el programa con la siguiente sentencia.
Los parámetros son que busque todo lo del direcorio /dev/sda1

```
root@josejimenez:/home/josejimenez# foremost -T all -i /dev/sda1
Processing: /dev/sda1
|***
```

Si el proceso va correctamente deberá aparecer una pantalla tal que así:

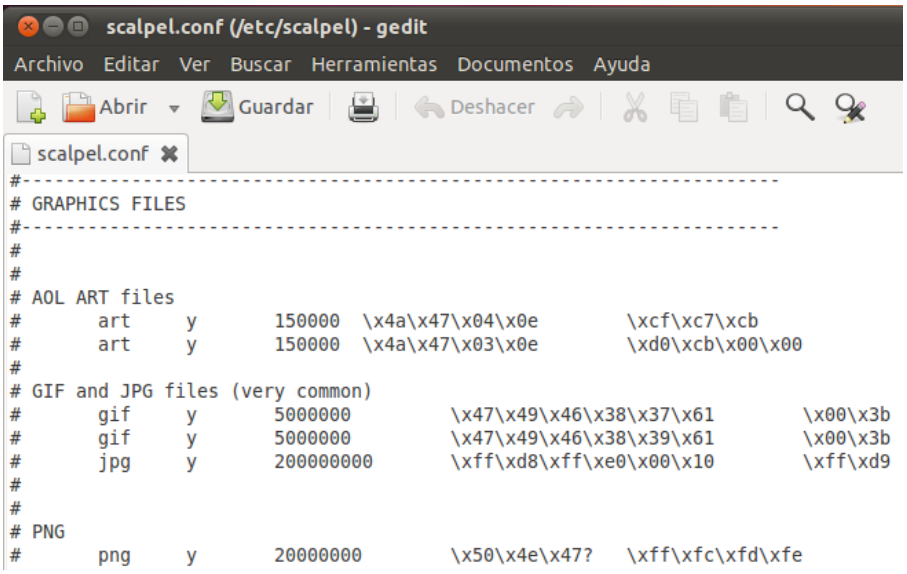
```
foundat=jsloader/resource/gre/modules/XPIProvider.jsm.binUT
foundat=jsloader/resource/gre/modules/nsFormAutoCompleteResult.jsm.binUT
foundat=jsloader/resource/gre/components/nsBadCertHandler.js.binUT
foundat=jsloader/resource/gre/components/nsURLFormatter.js.binUT
*****
```

SCALPEL

En primer lugar instalamos el programa.

```
root@josejimenez:/home/josejimenez# apt-get install scalpel
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes NUEVOS:
  scalpel
0 actualizados, 1 se instalarán, 0 para eliminar y 299 no actualizados.
Necesito descargar 34,9 kB de archivos.
Se utilizarán 131 kB de espacio de disco adicional después de esta operación.
AVISO: ¡No se han podido autenticar los siguientes paquetes!
  scalpel
¿Instalar estos paquetes sin verificación [s/N]? s
```

La configuración de Scalpel se encuentra en el directorio /etc, concretamente /etc/scalpel/scalpel.conf. En el momento que lo habrás verás que está dividido en secciones, y que está todo comentado, presentando un aspecto como éste:



Si quieres recuperar algún archivo, por ejemplo, archivos con formato “doc”, simplemente tienes que quitar la almohadilla del comienzo de la línea.

```
# Word documents
#
#       doc     y       10000000  \xd0\xcf\x11\xe0\xa1\xb1\x1a\xe1\x00\x00 \xd0\xcf
\x11\xe0\xa1\xb1\x1a\xe1\x00\x00 NEXT
#       doc     y       10000000  \xd0\xcf\x11\xe0\xa1\xb1
#
# Outlook files
#       pst     y       500000000       \x21\x42\x4e\xa5\x6f\xb5\xa6
#       ost     y       500000000       \x21\x42\x44\x4e
#
```

Por ejemplo, si queremos recuperar archivos comprimidos con formato “zip”, el archivo de configuración quedaría así:

```
# MISCELLANEOUS
#-----------------------------------------------------------------------
#
        zip     y       10000000        PK\x03\x04      \x3c\xac
#
#       java    y       1000000 \xca\xfe\xba\xbe
#
```

Una vez definido en el archivo de configuración lo que queremos recuperar, suponiendo que se encuentra en la partición /dev/sdh1, nos situaremos en otra unidad.

d) Realiza un informe sobre los diferentes programas que existen en el mercado informático que permite crear imagenes de respaldo de tu equipo.

Una imagen del Sistema, llamada también "imagen Ghost" o "Ghost" a causa de un programa bastante conocido, es una copia de respaldo de todo el contenido de una partición (incluso de un conjunto de particiones). Ninguna distinción es hecha en el contenido. Se puede decir que una imagen del sistema es una "copia fiel" de la partición en un instante T (siendo T la hora del respaldo).

Debemos hacer una distinción entre imagen del sistema y copia de respaldo de datos. Por lo general, las copias de respaldo son hechas de forma continua o de manera muy regular, seleccionando los directorios a respaldar y casi siempre de forma incremental.

En cambio, el sistema cambia muy poco por lo que no hay necesidad de crear una imagen frecuentemente. Para crear una imagen, debemos elegir la partición y no los directorios. La copia de seguridad incremental consiste en hacer una copia de respaldo de todo lo que se especificó la primera vez, luego solamente de los archivos modificados posteriormente, guardando aparte una copia del archivo original. Por lo tanto, copia de respaldo e imagen del sistema son dos cosas muy distintas en cuanto a sus objetivos y métodos.

WINDOWS

Norton Ghost es una utilidad que permite realizar copias de seguridad automáticas; podrás hacer backups de tus ficheros de música, fotografías, documentos, etc. El programa permite recuperar ficheros y directorios rápidamente, incluso si tu sistema operativo no se inicia. Es posible programar las labores de backup, optimizar el almacenamiento de medios y realizar backups manualmente.

Floppy Image es una aplicación con la que podrás crear y restaurar imágenes de disquetes. Podrás guardar las imágenes de los disquetes comprimidas, sin compresión o como un fichero de extracción automática (EXE); añadir descripciones y convertir ficheros de imágenes antiguos. Su interfaz es agradable y fácil de usar.

R-Drive Image crea imágenes de discos para hacer copias de seguridad o simplemente duplicarlos. La aplicación es capaz de restaurar esas imágenes en su disco original, otra partición o cualquier espacio libre del disco duro.

Winimage es una herramienta que te permite hacer imágenes de discos, extraer ficheros de esas imágenes, hacer una imagen vacía, copiar la imagen de un disco virgen y más.

GNU/Linux

Partimage es un software de código abierto de copia de seguridad de disco. Se ahorra particiones con un sistema de ficheros apoyado sobre una base sectorial a un archivo de imagen.

G4U crea imágenes clonadas de discos duros partiendo de un CD-ROM o un disquete usando el FTP. Fácil y eficaz, es capaz de crear imágenes de discos comprimidas y subirlas a un servidor FTP, lo que resulta tremendamente útil cuando se requiere instalar una misma configuración en un parque importante de servidores.

e) Realiza un informe con los servicios de almacenamiento que ofrecen las empresas:
HP, Dell y ESABE:

HP

Servidor HP ProLiant ML330 G6

HP ProLiant ML330 G6 ofrece a las compañías la tecnología de gestión integrada más potente de la industria, gracias a HP Integrated Lights-Out 2 (iLO 2), que les permite gestionar los servidores en cualquier momento y lugar.

- Intel® Xeon® E5606 (4 núcleos, 2,13 GHz, 8 MB L3, 80 W)
- 1x2GB(Udimms)
- 18 ranuras DIMM
- Incluye Smart Array P410
- 2 discos de 250GB LFF
- DVDRW
- fuente de 460W

Servidor/TV HP ProLiant DL320 G6 E5603 1P, 2 GB-E, 500 GB, SATA, 500 W, PS

- Intel® Xeon® E5603 (4núcleos, 1,60 GHz, 4 MB L3, 80 W)
- 2GB DDR3 (UDimms)
- 9 ranuras DIMM Plataforma de bastidor empresarial densa y de bajo coste.
- Disco de 500GB SATA
- DVDROM
- Fuente 500W

DELL

Dell EqualLogic PS4000XV

Controladores de almacenamiento
Dos controladores con un total de 4 GB de memoria alimentada por una pila
La memoria alimentada por pila proporciona hasta 72 horas de protección de datos

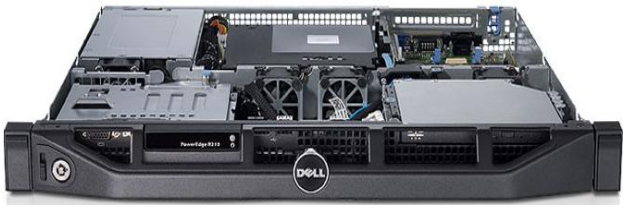
Unidades de disco duro
Dieciséis (16) unidades de disco duro SAS conectables en caliente

Capacidades de la unidad
Unidades SAS a 15.000 rpm de 300 GB, 450 GB, 600 GB

Capacidades del sistema
4,8 TB con dieciséis (16) unidades de disco SAS de 300 GB
7,2 TBcon dieciséis (16) unidades de disco SAS de 450 GB
9,6 TB con dieciséis (16) unidades de disco SAS de 600 G

PowerEdge R210 Servidor en rack

Entrada de Dell valor de 1 socket de servidor de 1U de rack, el Dell ™ PowerEdge ™ R210, ofrece capacidades avanzadas de gestión, el suministro de bajo voltaje de energía y opciones de conectividad externa de almacenamiento en un chasis muy pequeño.



- Ultracompacto de 15,5 pulgadas de profundidad de chasis para las opciones de implementación flexible en entornos de espacio limitado
- Los sistemas avanzados de gestión de la disponibilidad de Lifecycle Controller
- Puerto e-SATA para conexión añadido de almacenamiento externo

ESABE

Servicios byte pass *byte pass* es un servicio de backup eficiente
Una copia de seguridad puede ser suficiente pero, un buen backup, debe ser, además, eficiente para garantizar una buena seguridad informática, sobretodo en entornos empresariales. Un backup eficiente es el que se deriva de una política que incluye, además de la realización frecuente de copias de seguridad de los datos críticos, su externalización a la organización, comprobación periódica y disponibilidad permanente cumpliendo con el marco legal y las mejores prácticas. *byte pass*, es una solución completa para un problema complejo: El backup. El paradigma del beneficio de este servicio es que su empresa, sin tener que hacer backup, aumente la seguridad y disponibilidad de los datos, y en consecuencia fortalezca la seguridad de sus datos.

Los servicios que componen *byte pass*:

- Copia Local de respaldo.
- Réplica Remota para desastres.
- Réplica Local de datos para generar soportes externalizables.
- Copia Online para usuarios móviles y con necesidades de confidencialidad.
- Guarda y Custodia de Copias de Seguridad en soporte físico - Servicio BUNKER
- Destrucción Confidencial de Soportes y Documentación - Servicio DESCON

Copia Local
Mediante un dispositivo físico (appliance), conectado a la red del cliente, gestionado por ESABE y compuesto por servidor, discos y software, se consigue de una forma automática:

- Copiar todos los cambios producidos en los archivos informáticos (ficheros, bases de datos, correo, directorio activo y archivos abiertos).
- Mantener distintas versiones de los archivos respaldados.
- Recuperar inmediatamente la situación más reciente a cualquier contingencia. Disponer de un mecanismo de recuperación predictible (Fichero: 30'', Disco: 30').
- Restaurar completamente la imagen del Sistema con la opción Bare Metal Universal Restore.

Réplica Local

La transmisión de información a través de redes de comunicaciones exige disponer de anchos de banda adecuados. En casos en los que no se disponga de esa capacidad, byte pass ofrece la posibilidad de asegurar también la protección frente a desastres, posibilitando la realización de una réplica local, con similares características a la réplica remota y que sea externalizable.

- Tener una copia externalizable en disco, de los datos críticos y con cifrado seguro.
- Disponer de un mecanismo de recuperación en caso de pérdida de los datos del appliance local.
- Disponer de un Soporte Técnico que nos ayude en la recuperación.
- Utilizar los servicios logísticos de ESABE para transportar y custodiar los discos de réplica en un búnker de seguridad e intercambiarlos periódicamente (semana) para garantizar su actualización.

Réplica Remota

Con la Copia Local ya tenemos la mejor protección para respaldo. Ahora debemos asegurarnos que, en caso de desastre, también tengamos la mejor protección. Para ello, byte pass ofrece esta opción con otro dispositivo gestionado por ESABE, en un Centro de Proceso de Datos seguro, que permite:

- Tener una copia remota de los datos críticos y con cifrado seguro.
- Utilizar la logística y transporte de ESABE para entregar una copia utilizable en el Centro de Proceso de Datos del cliente.
- Disponer de un mecanismo de recuperación predictible (Online y en menos de 24 horas).
- Disponer de un Soporte técnico que nos facilita la recuperación.

Copia Online

De forma totalmente automática, el servicio de Copia Online de *byte pass*, permite:

- Hacer copias de seguridad frecuentemente de forma programada desde cualquier dominio de Internet.
- Tener siempre una copia cifrada de los archivos más confidenciales fuera de los Sistemas Corporativos de su empresa.
- Recuperar su Copia de Seguridad sobre cualquier ordenador, conociendo su clave única de cifrado.

No hay nada que hacer, no tendrá que hacer copias en cintas y externalizarlas. Sus datos a salvo en instalaciones de seguridad, libres de sabotajes y accidentes. Los datos de alta confidencialidad son disponibles las 24 horas del día.
Para utilizar este servicio, sólo se requiere una línea ADSL, no se necesita una infraestructura informática o conocimientos de IT. Es una solución ideal para Pymes, autónomos, oficinas o delegaciones sin recursos informáticos, trabajadores con mucha movilidad geográfica y información de alta confidencialidad.

Pack de servicios de Nivel 1 de OFERTA COMPLETA PYMES: CL + RR

- Appliance modelo S1 (300 GB)
- 1 licencia byte pass Server + 4 licencias byte pass PC
- Réplica Remota en datacenter hasta 100 GB

Para asegurar que, en caso de desastre, también tengamos la mejor protección, byte pass ofrece el servicio de réplica remota gestionado por ESABE, que permite:

- Tener una réplica cifrada, remota y actualizada de los datos críticos.

- Utilizar la logística y transporte de ESABE para entregar una copia utilizable en el Centro de Datos del cliente.

- Disponer de un mecanismo de recuperación predictible (Online).

- Cumplir con los requerimientos de la LOPD.

Pack de servicios de Nivel 2 de OFERTA COMPLETA PYMES: CL + RR

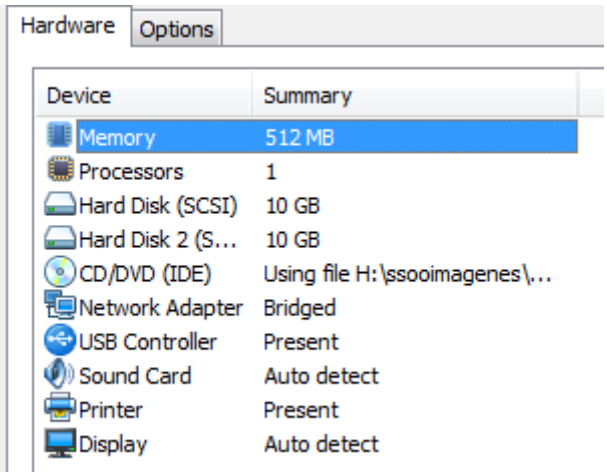
- Appliance modelo S1 (300 GB)
- 1 licencia byte pass Server + 4 licencias byte pass PC
- Réplica Local hasta 500 GB
- Servicio Bunker

La transmisión de información a través de redes de comunicaciones exige disponer de anchos de banda adecuados. En casos en los que no se disponga de esa capacidad, ***byte pass*** ofrece la posibilidad de asegurar también la protección frente a desastres, posibilitando la realización de una réplica local, con similares características a la réplica remota y que sea externalizable.

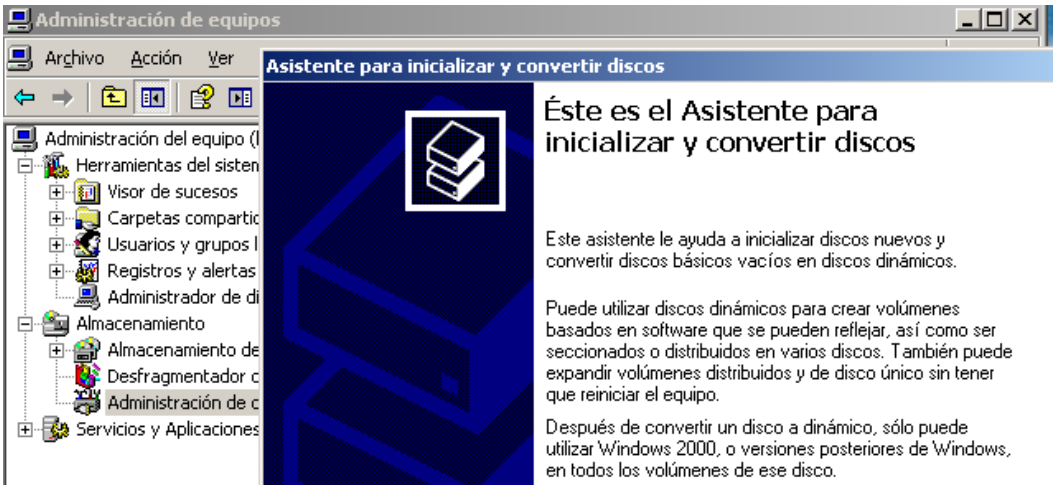
Con el servicio Bunker, su réplica será recogida en contenedor precintado y trasladado en una cámara de alta seguridad para su custodia, con disponibilidad 24/7.

f) Realizar en un entorno simulado un medio de almacenamiento RAID 1 con máquinas virtuales Windows Server.

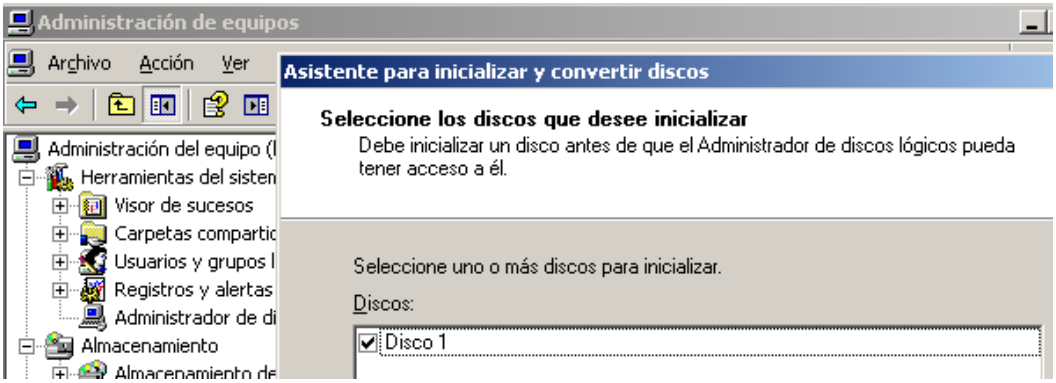
En primer lugar decir que para un raíz uno es necesario un mínimo de 2 discos duros.
Agregamos un segundo disco duro.



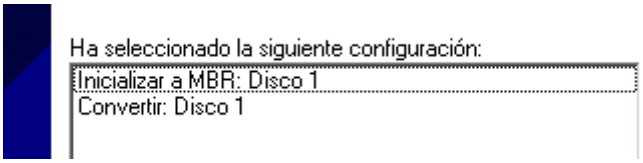
El siguiente paso es inicializar el nuevo disco.
Inicio, desplegamos el menú contextual sobre equipo, administrar, administrador de discos.
Se inicia el asistente.



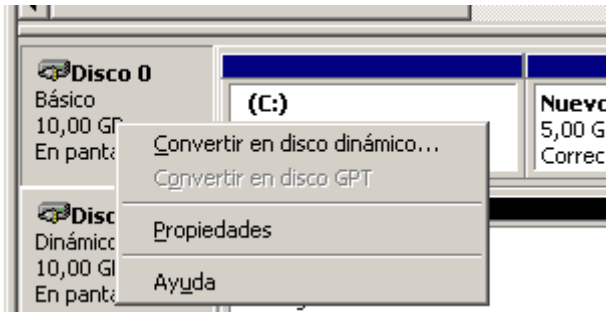
Seleccionamos el disco a inicializar. Al ser el segundo lo nombra como disco1 el disco0 el que el que existía.



Finalizamos la inicialización del disco1

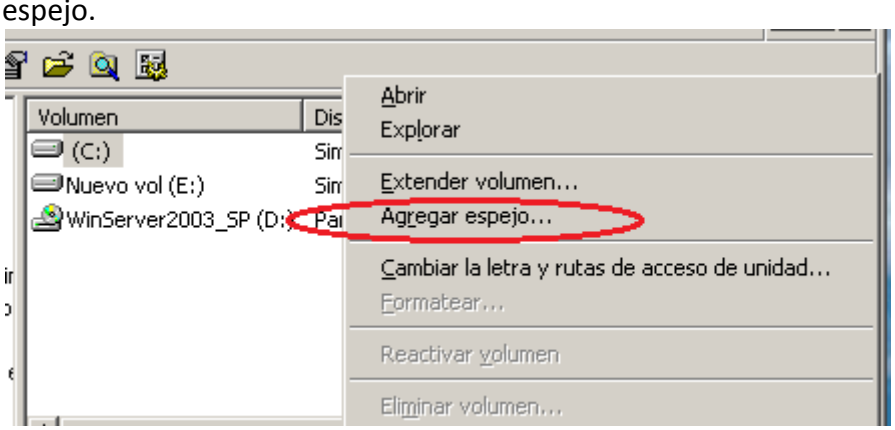


Posteriormente tenemos que convertir el disco que ya existía en disco dinámico.

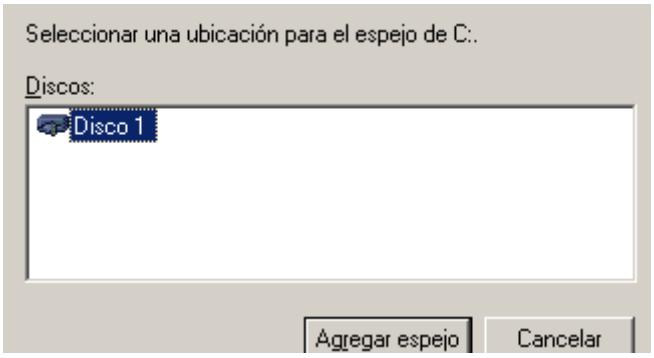


Una vez que ya tenemos ambos discos en dinámico podemos proceder a la creación del RAID1 o copia espejo.

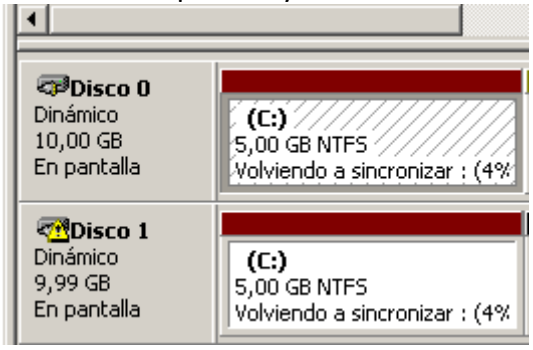
Sobre el disco primerio pulsamos con el botón derecho y seleccionamos agregar espejo.



A continuación seleccionamos donde en que disco queremos asignar el espejo. *Disco1 (el nuevo disco)*



Por último aceptamos y comienza la creación del RAID 1.

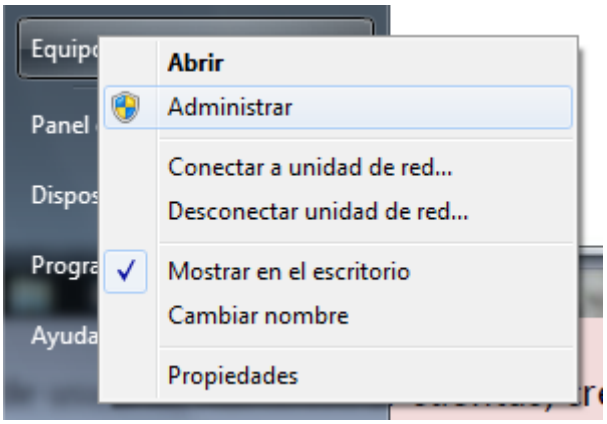


g) Control de acceso lógico: Realiza la creación de una cuenta de usuario y su contraseña (política fuerte de contraseñas - modo comando y modo gráfico) que permite posteriormente acceder o no al sistema en sistemas Windows y sistemas GNU/Linux.

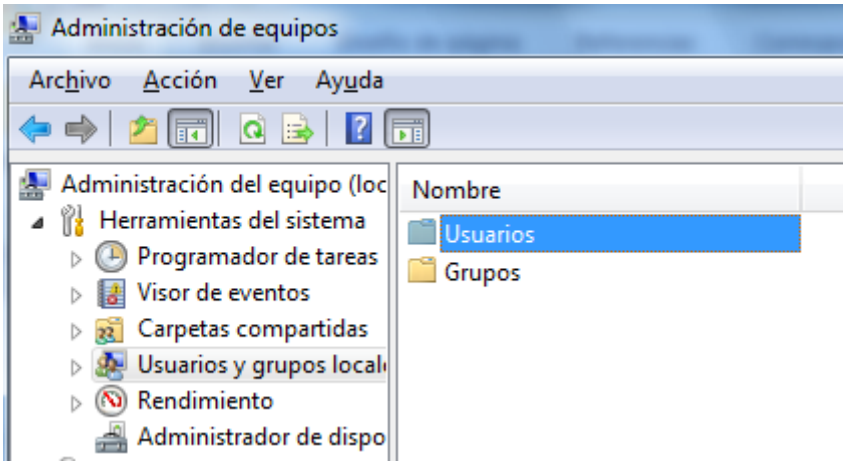
CREACIÓN USUARIO SISTEMA WINDOWS

MODO GRÁFICO

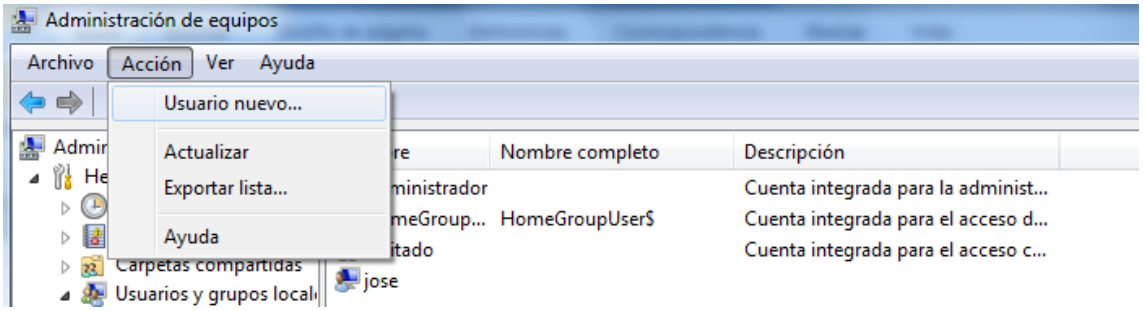
En primer lugar vamos a inicio, equipo, desplegamos el menú contextual y pulsamos en administrar.



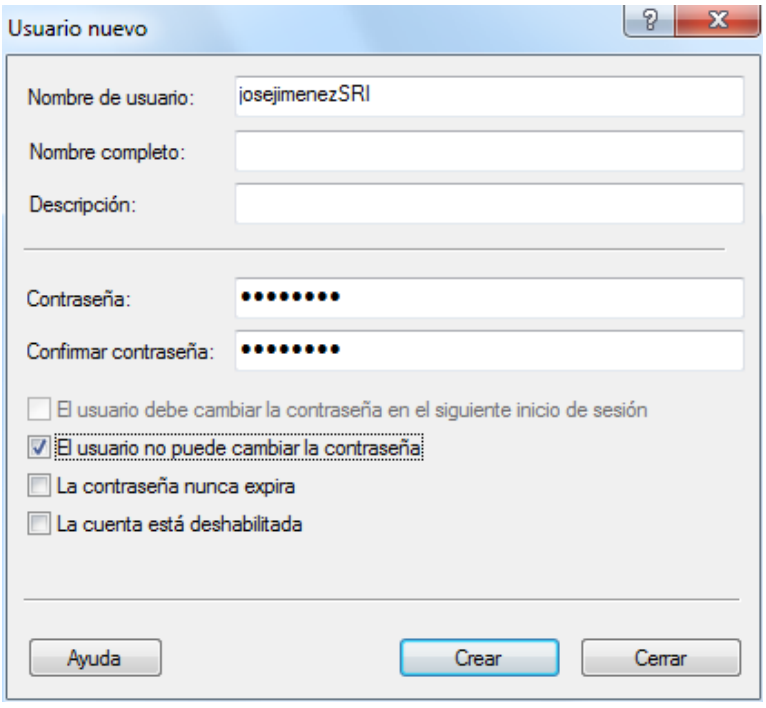
A continuación pulsamos en administración de usuarios y grupos > usuarios.



Posteriormente vamos a la segundas pestaña superior llamada Accion> nuevo usuario.

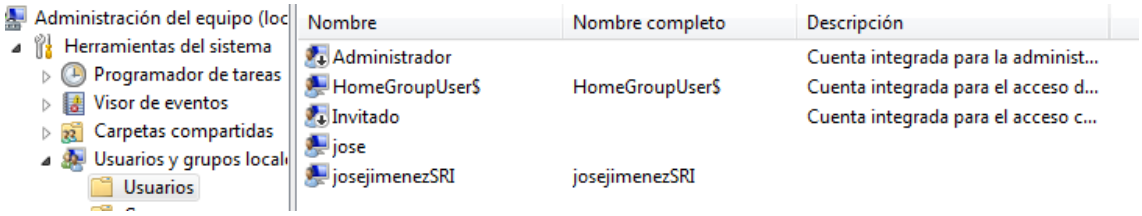


En cuarto lugar damos nombre a la nueva cuenta y una contraseña si lo creemos necesario.
También podemos configurar diversos parámetros en la parte inferior de la pantalla.
Y pulsamos en crear.



Nos aseguramos que la cuenta ha sido creada:

Bien desde la lista de usuarios.

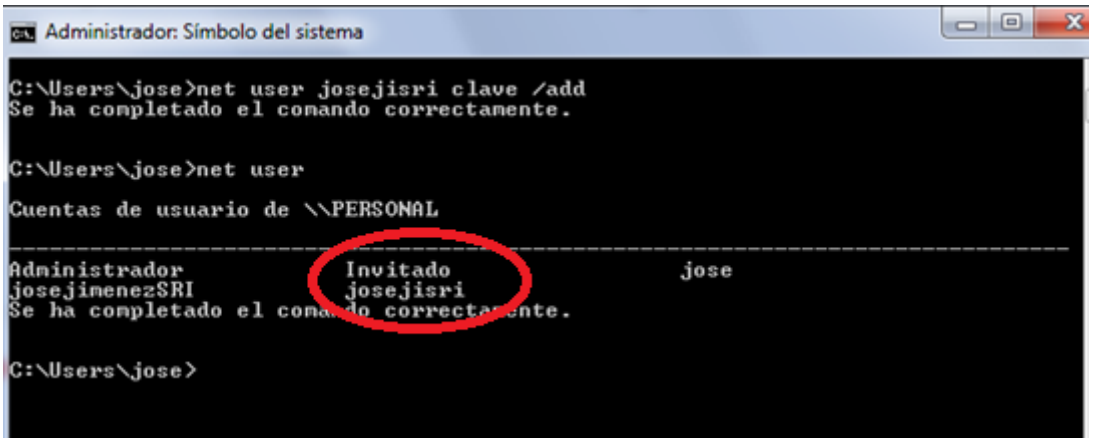


O desde el entorno de inicio de sesión:

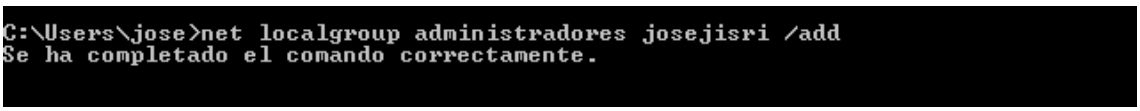
MODO COMANDO

En primer lugar abrimos símbolo del sistema como administrador.
Para agregar un usuario utilizamos la sentencia:
Net user nombredeusuario contraseña /add

Net user josejisri clave /add

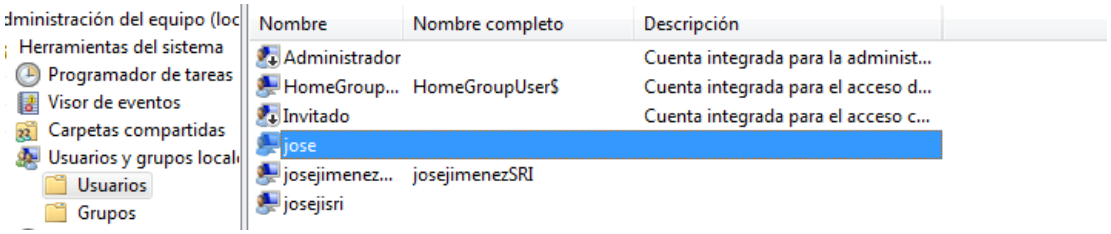


Para verificar las cuentas hacemos un net user. Como podemos ver en la pantalla anterior josejisri es una cuenta invitado, para agregarla al grupo administradores hacemos lo siguiente:



Nos aseguramos que la cuenta ha sido creada:

Bien desde la lista de usuarios.

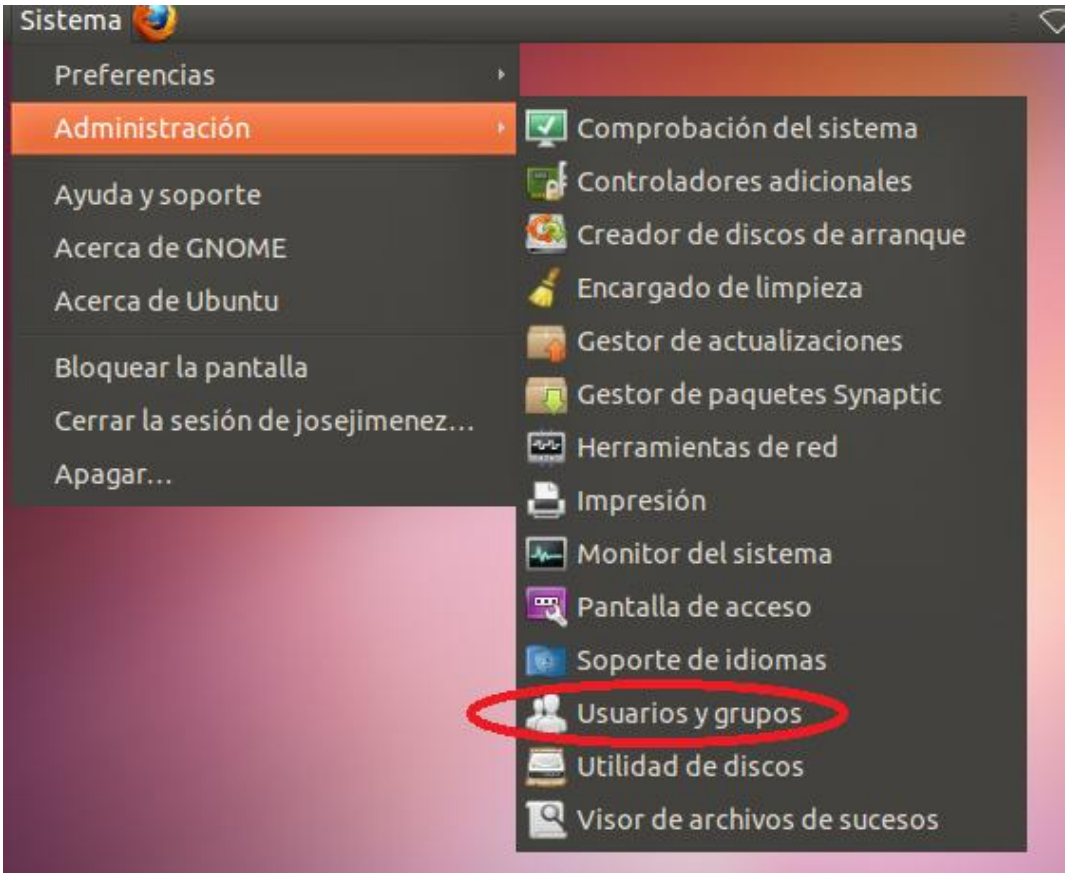


O desde el entorno de inicio de sesión:

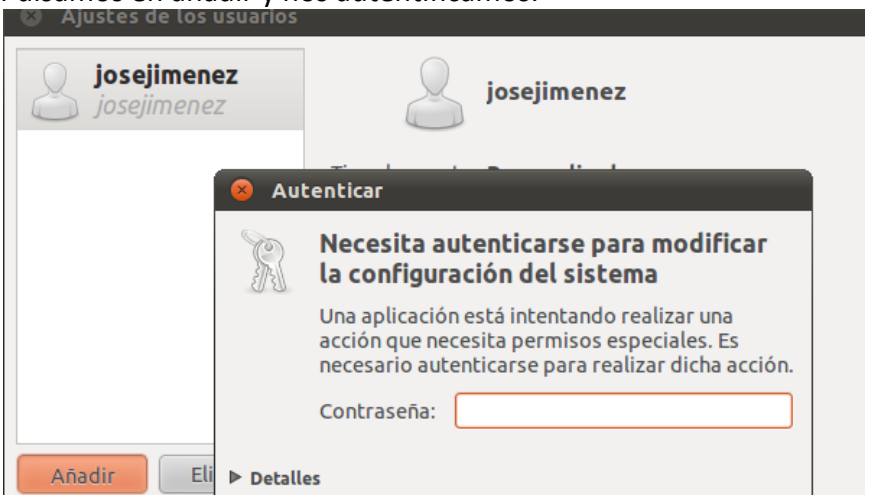
CREACIÓN USUARIOS EN SISTEMAS LINUX

MODO GRÁFICO

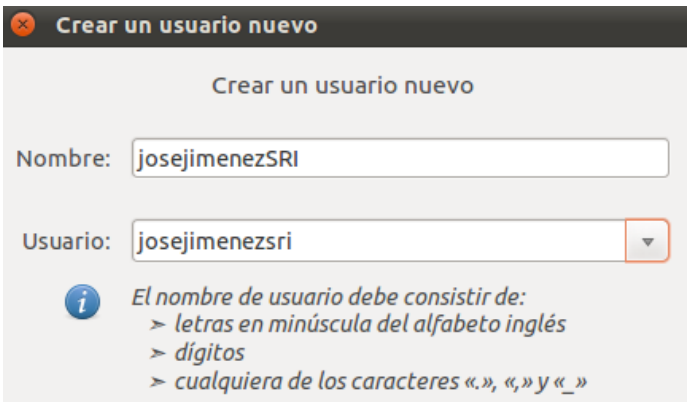
En primer lugar vamos a sistema, administración, usuarios y grupos.



Podemos observar que ya hay un usuario llamado josejimenez.
Pulsamos en añadir y nos autentificamos.

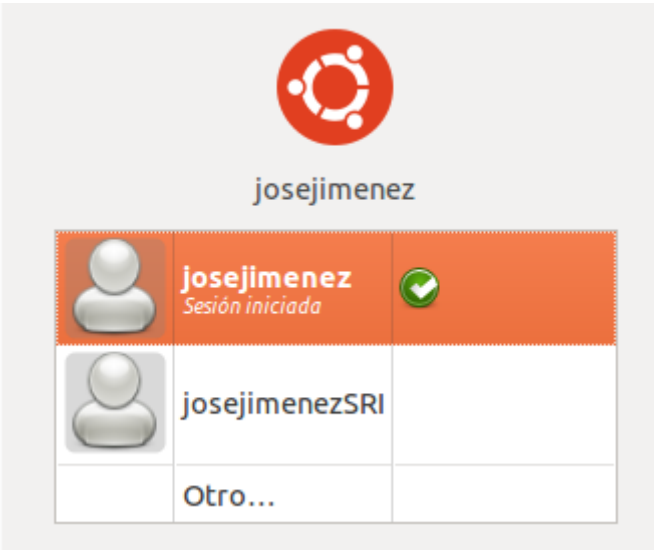


Escribimos en nombre del nuevo usuario.



En la siguiente pantalla podemos establecer una contraseña al usuario *josejimenezSRI*

Comprobamos que se ha creado correctamente y nos permite acceder al sistema.

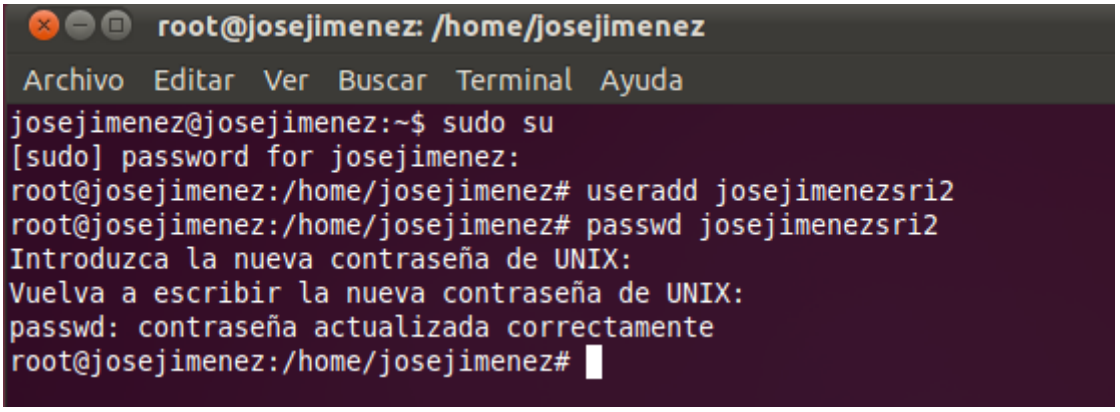


MODO COMANDO

Abrimos una nueva terminal y acreditamos que somos root.

Posteriormente creamos el usuario con *useradd josejimenezsri2*

A continuación establecemos una contraseña con *passwd josejimenezsri2*
Escribimos la contraseña 2 veces.



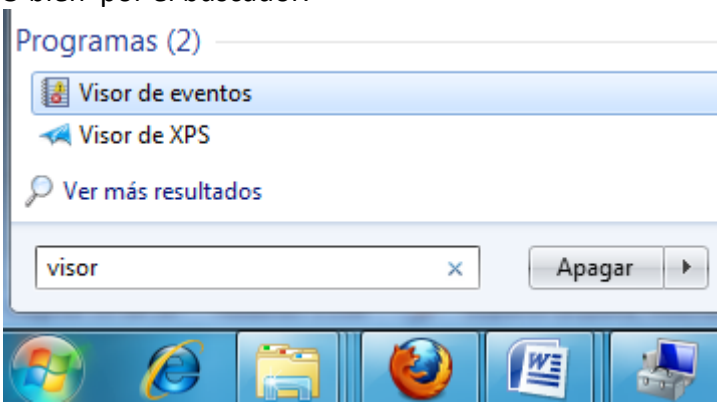
h) Verifica la auditoria de control de acceso “Visor de sucesos” de dicho usuario en Windows y Linux.

Definición: Aplicación que permite a los administradores y los usuarios ver los registros de sucesos en un equipo local o remoto.

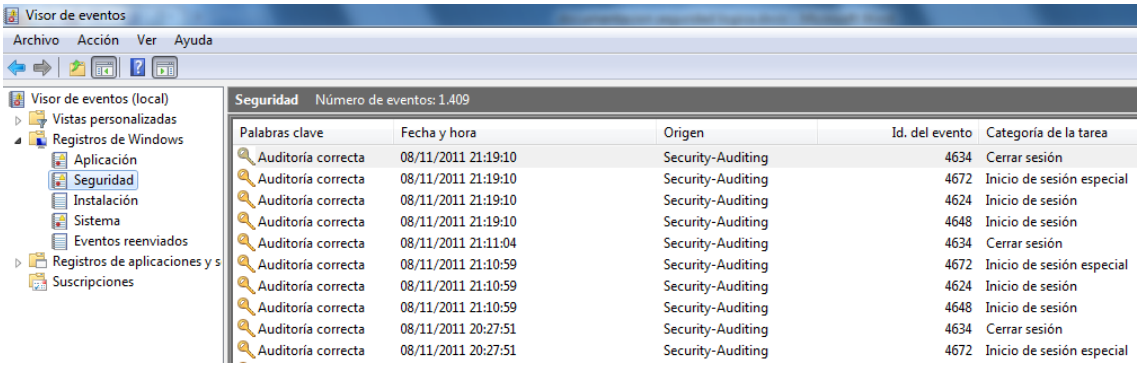
Visor de sucesos WINDOWS

A partir de la versión de Windows Vista se llama visor de eventos.
Podemos acceder a él mediante, panel de control, herramientas administrativas, visor de eventos.

O bien por el buscador.

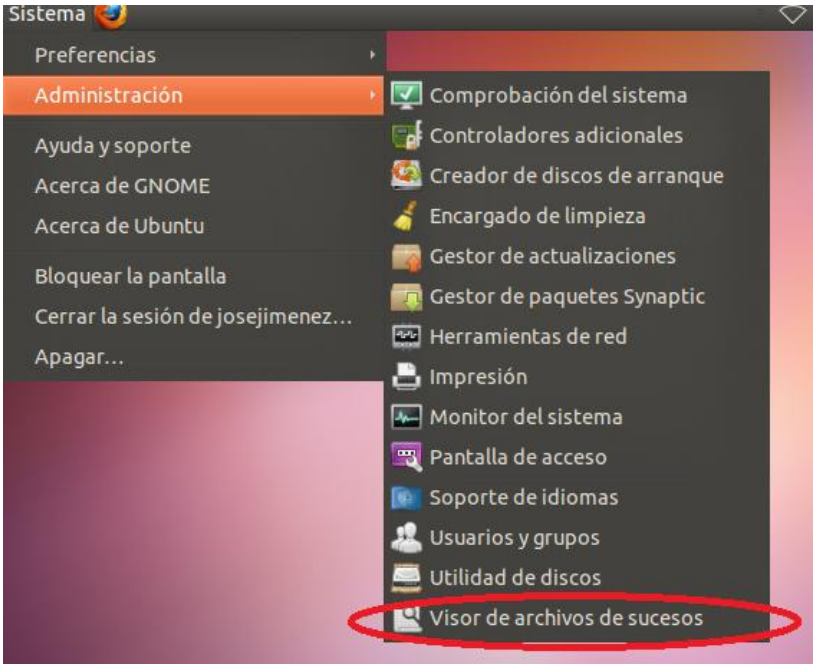


Tiene el siguiente aspecto:



Visor de sucesos LINUX

El visor de sucesos, no es otra cosa que un software que permite visualizar los ficheros log.

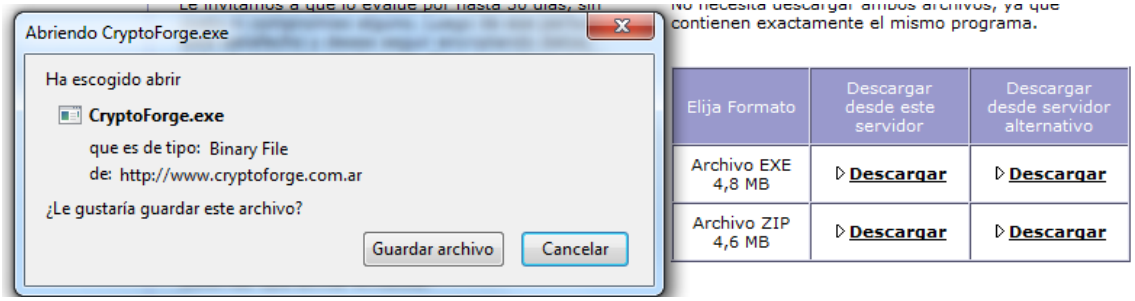


Esto es lo que aparece en el visor de sucesos.

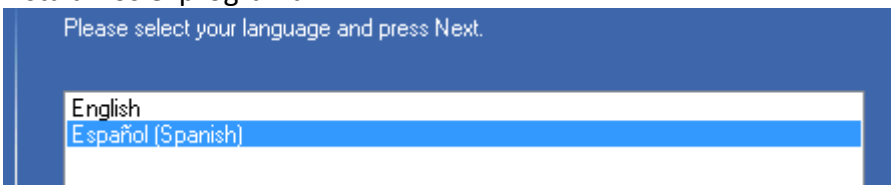
```
Oct 27 10:57:29 josejimenez dhclient: DHCPACK of 192.168.23.134 from 192.168.23.254
Oct 27 10:57:29 josejimenez dhclient: can't create /var/lib/dhcp3/dhclient.eth0.leases:
Oct 27 10:57:29 josejimenez dhclient: bound to 192.168.23.134 -- renewal in 746 seconds
Oct 27 11:09:55 josejimenez dhclient: DHCPREQUEST of 192.168.23.134 on eth0 to 192.168.
Oct 27 11:09:55 josejimenez dhclient: DHCPACK of 192.168.23.134 from 192.168.23.254
Oct 27 11:09:55 josejimenez dhclient: can't create /var/lib/dhcp3/dhclient.eth0.leases:
Oct 27 11:09:55 josejimenez dhclient: bound to 192.168.23.134 -- renewal in 825 seconds
```

i) Descargar el programa de evaluación CryptoForge para Sistemas Windows en la dirección de Internet: http://www.cryptoforge.com.ar/

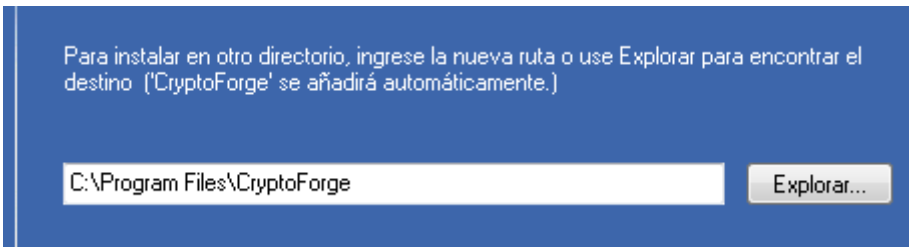
En primer lugar vamos a la página oficial y descargamos el software.



Instalamos el programa.

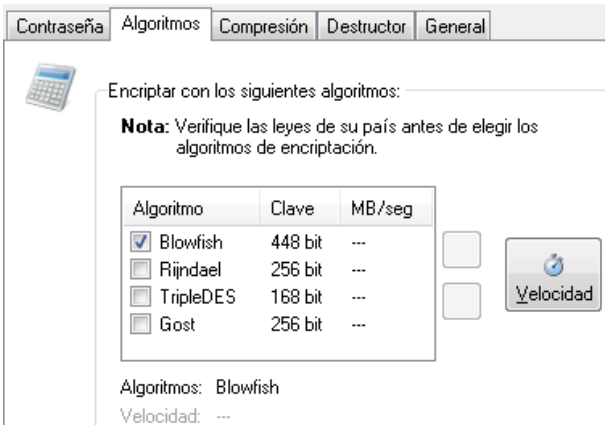


Seleccionamos el directorio.

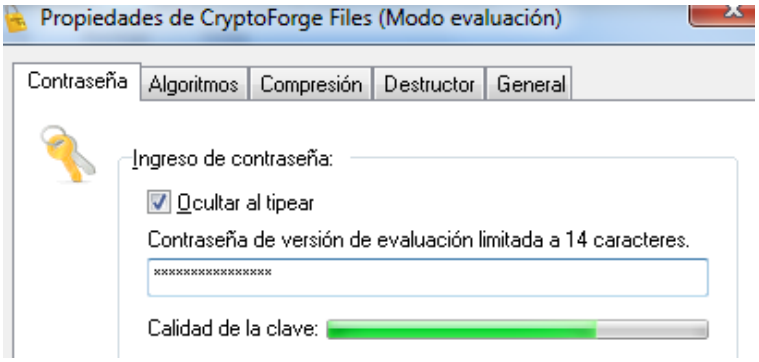


Y encripte y desencripte varios ficheros de tu ordenador, utilizando diferentes sistemas de cifrado.

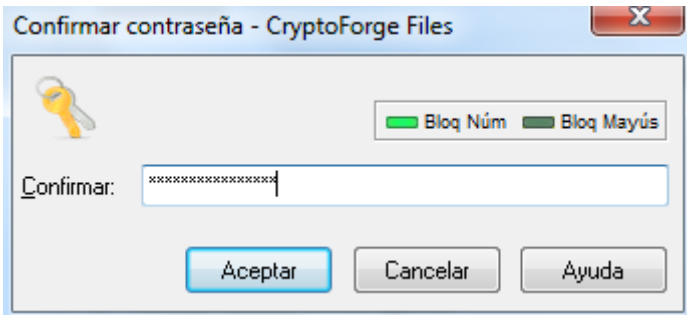
Arrancamos el programa y en la pantalla algoritmos observamos los diferentes sistemas de cifrado disponibles.



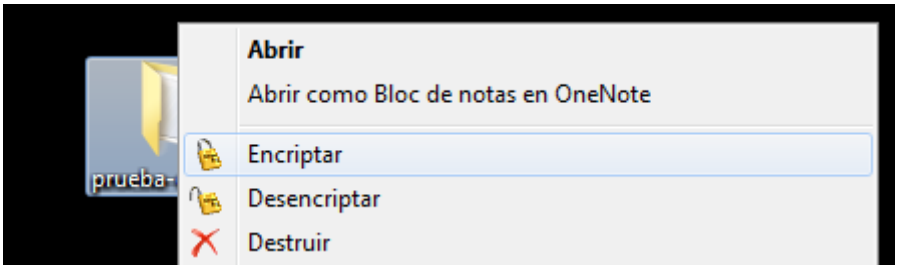
Ingresamos una contraseña, el software nos dice la calidad y seguridad de esta.



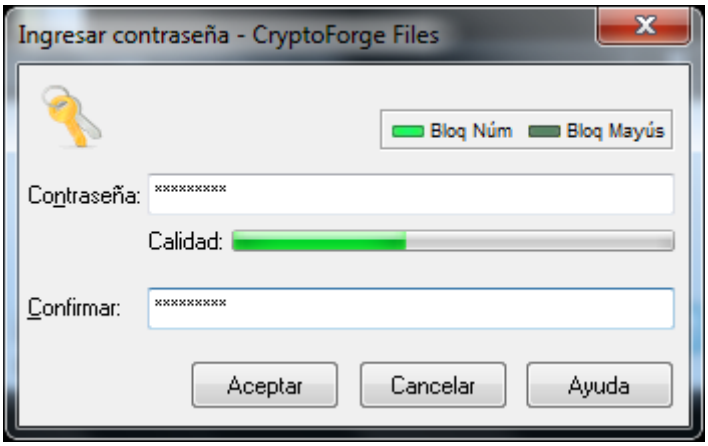
Pulsamos en aceptar y nos pide confirmar la clave.



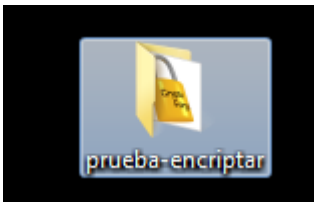
Encriptar/desencriptar:
Sobre el archivo que deseamos realizar la acción pulsamos con el botón derecho, encriptar.



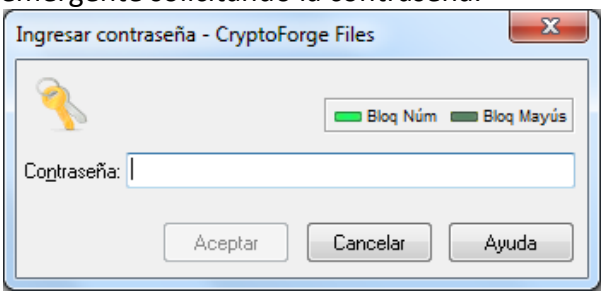
Ingrasamos la contraseña para cifrar el archivo.



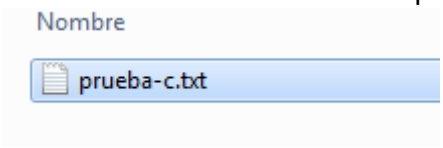
Si se ha realizado correctamente el fichero/directorio debe aparecer de la siguiente manera.



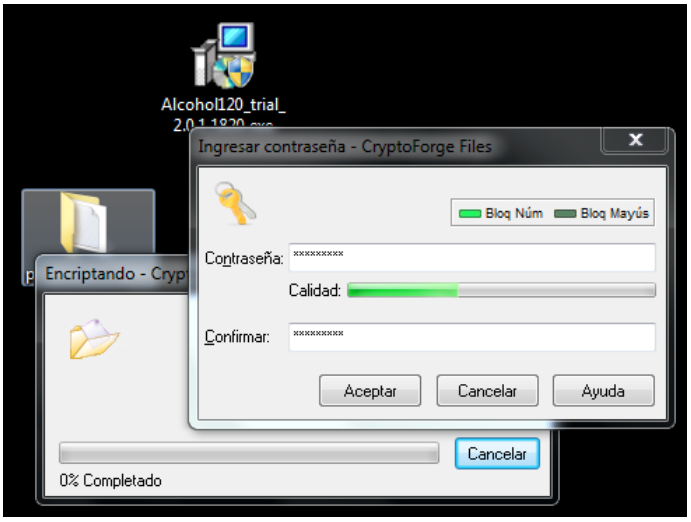
De tal modo cuando intentamos acceder al documento aparece una pantalla emergente solicitando la contraseña.



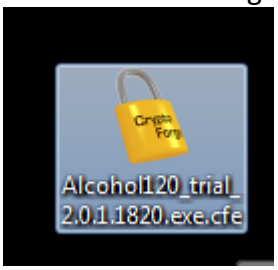
Si la introduces correctamente quita el cifrado al archivo y permite acceder a él.



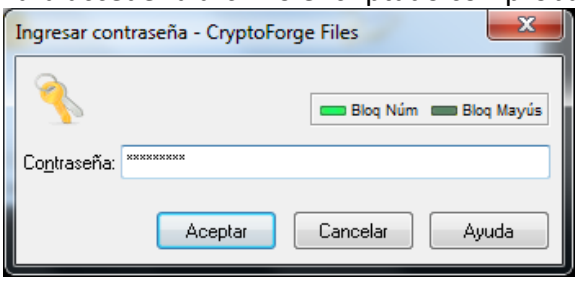
Siguiente prueba:
Seleccionamos todos los sistemas de cifrado y se lo aplicaremos a un archivo.exe



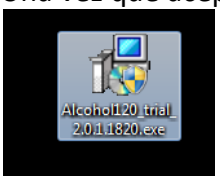
El resultado es el siguiente.



Para acceder a archivo encriptado comprobamos que nos solicita la clave.

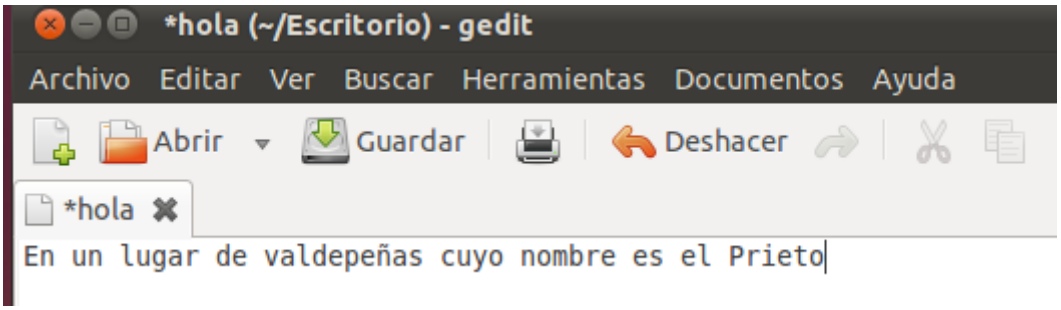


Una vez que aceptamos muestra el archivo tal y como estaba en su estado original.



j) Encriptar y desencriptar ficheros de texto en sistemas GNU/Linux utilizando el comando tr que permite realizar sustituciones carácter a carácter.

En primer lugar creamos un documento que será el que utilicemos para aprender.



Comenzamos abriendo una nueva terminal.

Un ejemplo de cómo funciona es el siguiente.

En el siguiente ejemplo cambiamos la vocales “e” por la letra “t”.

```
root@josejimenez:/home/josejimenez/Escritorio# cat hola
En un lugar de valdepeñas cuyo nombre es el Prieto
root@josejimenez:/home/josejimenez/Escritorio# cat hola | tr e t
En un lugar dt valdtptñas cuyo nombrt ts tl Pritto
root@josejimenez:/home/josejimenez/Escritorio#
```

Otro ejemplo.

```
root@josejimenez:/home/josejimenez/Escritorio# cat hola
En un lugar de valdepeñas cuyo nombre es el Prieto
root@josejimenez:/home/josejimenez/Escritorio# cat hola | tr vurñoe tedisoya
En en legad dy taldypyisas ceyo nombdy ys yl Pdiyto
root@josejimenez:/home/josejimenez/Escritorio#
```