

Caso práctico

Ada después de investigar en la web las distintas alternativas para realizar copias de seguridad, cifrado y RAID, y compensar las ventajas que proporcionan, frente al gasto económico que representa, ha decidido llevar a cabo una serie de pasos para aumentar la seguridad del sistema.



Ada es consciente que no sólo hay que realizar copias de seguridad, si no que una buena configuración es importante para que todo los equipos funcionen adecuadamente, además a ella le gusta que toda la información esté segura y si ocurre alguna incidencia se puede recuperar toda la información fácilmente. Por eso se preocupará que no sólo ella conozca todo lo necesario para trabajar con copias de seguridad de forma óptima, si no que intentará que el resto de trabajadores y trabajadoras de la empresa también hagan tareas de cifrado y monten sistemas RAID en sus equipos



[Ministerio de Educación y Formación Profesional](#). (Dominio público)

Materiales formativos de FP Online propiedad del Ministerio de Educación y Formación Profesional.

[Aviso Legal](#)

1.- Copias de seguridad. Backup de datos.

Caso práctico

Carlos va a ver a Juan.

—Hola Juan, mira me han encargado instalar muchos equipos iguales y la verdad es que me va a llevar mucho tiempo. ¿Conoces algún truco para ayudarme?—Sí claro, ahora mismo estoy viendo una herramienta que me permite clonar discos duros. La idea es que instalas y configuras bien un equipo, y luego le haces una copia al disco duro y la pones en todos los ordenadores. Así lo realizarás todo mucho más rápido.—¡Qué bien! Además, me gustaría que me expliques también cómo realizar copias de seguridad en Windows y Linux. ¡Me quedo contigo y así aprendo cómo se hace!



El objetivo de un backup o copia de seguridad es guardar las carpetas y archivos de los usuarios. En estas copias, no importa la instalación del sistema, sino que los datos estén guardados en más de un sitio, para evitar su pérdida. Por ese motivo, lo habitual es guardar las copias de seguridad en dispositivos externos o en otros ordenadores a través de la red, para evitar su pérdida en caso de mal funcionamiento del equipo.

Las copias de seguridad se planifican y automatizan con la programación de tareas del sistema operativo.

1.1.- Copias de seguridad en Windows.

Existen distintos tipos de copias de seguridad:

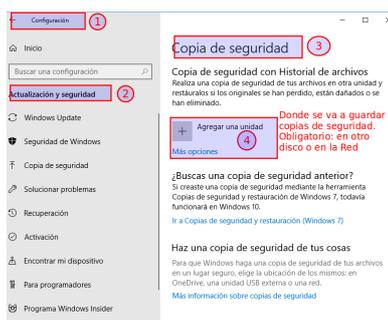
- ✓ **Completas:** Realiza la copia de todo el contenido de la carpeta seleccionada.
- ✓ **Incrementales.** Realiza la copia de los ficheros que hayan cambiado desde la última copia completa o incremental.
- ✓ **Diferenciales.** Realiza la copia de los ficheros que hayan cambiado desde la última copia completa.

Herramienta "Copias de seguridad de Windows"

En Windows tenemos la herramienta llamada "Copias de seguridad"

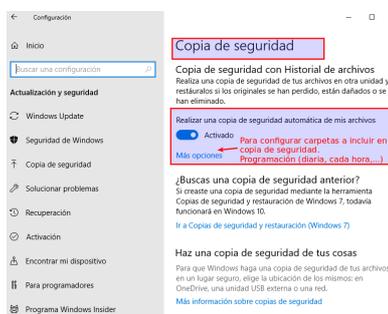
Para llegar a ella, ir a Configuración / Actualización y Seguridad / Copias de Seguridad. Una vez dentro de la herramienta de copias de seguridad se seguirán los pasos siguientes:

Agregar una unidad. Es obligatorio guardar la copia de seguridad en otro disco (interno, externo o pendrive) o en la red.



Miguel Ángel García Lara (CC BY-NC-SA)

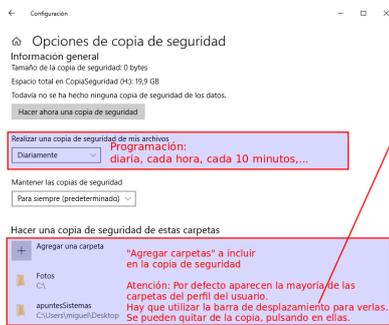
Una vez agregada la unidad, aparece Activado "Realizar una copia de seguridad..." Pulsar en "Más opciones" para seleccionar carpeta y programación de la tarea.



Miguel Ángel García Lara (CC BY-NC-SA)

En la ventana que se abre, se configuran varios aspectos:

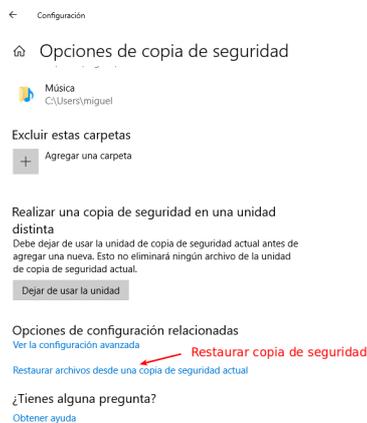
- ✓ Periodicidad de la copia de seguridad: cada pocos minutos, horas o una vez al día.
- ✓ Durante cuánto tiempo se realizarán las copias.
- ✓ Pulsar en "Agregar una carpeta" para seleccionar los archivos y carpetas a incluir en la copia de seguridad. Windows por defecto introduce las carpetas del usuario, si se quieren quitar, pulsar en ellas para eliminarlas (observar barra de desplazamiento).



Miguel Ángel García Lara (CC BY-NC-SA)

Para restaurar una copia de seguridad:

En la misma ventana de copias de seguridad, abajo del todo, se encuentra la opción “Restaurar copia”.



Miguel Ángel García Lara (CC BY-NC-SA)

También hay herramientas externas para realizar copias de seguridad como Ghost y Acronis. Estos mismos programas también los nombraremos en el capítulo 2, cuando hablemos de clonaciones.

1.2- Copias de seguridad en Linux.

En Linux, tenemos bastantes herramientas de copias de seguridad: tar, rsync, scp y dump. Todas ellas se usan en modo comando. En modo gráfico se puede utilizar tar.

Empaquetar y comprimir archivos con tar

La herramienta tar se utiliza para:

- ✓ Crear copias de seguridad
- ✓ Para empaquetar y comprimir archivos, siendo equivalente a los archivos zip o rar que conocemos en Windows.
Llamamos empaquetado porque un montón de archivos y directorios lo empaquetamos en un solo archivo.
- ✓ Para crear copias de carpetas idénticas a la original
 - ¿Por qué se utiliza tar para este fin?
Cuando copiamos una carpeta, cambian muchas propiedades de los archivos:
El usuario propietario es quien ha realizado la copia, independientemente de quien fuera el propietario del archivo original.
Los permisos serán los que se crean por defecto en los archivos nuevos y no los de los originales.
La copia tiene como fecha de creación la hora en la que se ha realizado dicha copia. Muchas veces queremos guardar la hora en que se modificó el archivo. Si por ejemplo copiamos una carpeta con fotos, en la copia parecerá que todas las fotos se han realizado en este momento.
En terminal, se puede utilizar `cp -p` (p de preservar) para hacer una copia idéntica. Pero en gráfico esta opción no existe.

Extensiones utilizadas para la herramienta tar

Igual que en Windows hablamos de archivos “.rar”, “.zip”, “.arj”, en Linux vamos a hablar de archivos “.tar”, “.gz” y “.tar.gz”

Archivos .tar significa que están empaquetados.

Archivos .gz significa que están comprimidos.

Archivos .tar.gz significa que están empaquetados y comprimidos.

Empaquetado y compresión con tar

Ejemplo: Obtener una copia de seguridad de todos los directorios \$HOME de los usuarios y guardarla y descomprimirla en una nueva carpeta llamada /copia_home

```
#cd /home
```

```
#tar -cvzf home.tar.gz * #Crea home.tar.gz empaquetado y comprimido con todo lo que hay (*) en el directorio actual
```

```
#Este archivo home.tar.gz empaquetado y comprimido lo podríamos guardar en cualquier sitio, como copia de seguridad.
```

```
#En este caso, ahora vamos a descomprimir y desempaquetar en otro sitio
```

```
#Para ello, creamos el directorio destino, nos cambiamos a ese directorio y movemos el archivo .tar.gz
```

```
#mkdir /copia_home
```

```
#mv /home/home.tar.gz /copia_home  
#cd /copia_home #tar -xvzf home.tar.gz #Se descomprime y desempaqueta donde estemos  
situados
```

El programa tar admite más sintaxis por si solo se quiere comprimir o empaquetar, aquí se ha reflejado la sintaxis principal.

Para saber más

Otras herramientas: rsync, dump, scp

La ventaja de rsync y dump para realizar copias de seguridad, es que realizan copias incrementales. La herramienta dump se utiliza de modo local, sin embargo rsync se puede utilizar tanto en equipo local como en equipo remoto; para ello antes de enviar la información por la red, comprime la información para optimizar los envíos. La utilidad scp es un programa para realizar copias en la red que incorpora el servicio ssh; que es un servicio de acceso remoto que se estudiará en la unidad 10. Más información de [rsync](#) y [dump](#)

2.- Clonaciones e imágenes de discos duros y particiones.

Caso práctico

Ada decide que ahora lo que interesa es realizar un backup del sistema operativo y software instalado, y no de los datos concretos de los usuarios. Por lo tanto pide que se realicen imágenes y clonaciones de particiones o discos duros completos.



2.1.- Conceptos. Herramientas.

Imágenes del sistema: creación y restauración

Cuando se instala un PC por primera vez, se necesita un tiempo para instalar el sistema operativo, drivers, configuración y el software que se vaya a utilizar. Nos interesa crear una imagen de ese sistema instalado, para que en el futuro, ante posibles errores o simplemente porque se quiere tener un sistema limpio, se pueda restaurar esa imagen, y volver al sistema tal como se tenía instalado el primer día.

Las opciones sobre imágenes son:

- ✓ **Crear una imagen de una partición:**

Crear una imagen de un sistema instalado en una partición, se trata de empaquetar y comprimir toda la información de la partición en un único archivo (o pocos archivos). Estos archivos, que son la imagen la podemos guardar en otro disco (interno o externo), en un equipo de la red o en otra partición del mismo disco.

- ✓ **Crear una imagen de un disco:**

También se puede crear una imagen de un disco duro completo. En esa imagen se guardarán todas las particiones en el estado actual. Esa imagen la podemos guardar en otro disco o en la red, pero nunca en una partición del mismo disco.

- ✓ **Restaurar una imagen en una partición:**

Cuando el sistema operativo, en un futuro vaya lento o no arranque, utilizaremos el mismo software para restaurar la imagen.

Al restaurar una partición, será necesario que esa partición exista; lo cual es lógico (al restaurar una imagen en una partición, nos tendrá que preguntar disco y partición de destino). Dará lo mismo si la partición de destino tiene un sistema de archivos u otro, si tiene datos o no, la partición se reescribirá volcando la imagen, dejando la partición tal como estaba cuando se creó la imagen.

- ✓ **Restaurar una imagen en un disco:** De la misma forma, al restaurar un disco nos dará lo mismo su estado actual, si el disco tiene particiones o no.

Clonaciones

Cuando se habla de clonaciones, se está hablando de volcar la misma información de una partición o de un disco en otra partición o disco, dejándolo igual. Por ejemplo, si clonamos una partición a otra, si en la partición origen hay 100 carpetas y 1500 archivos, en el disco destino se tiene esa misma cantidad de carpetas y archivos.

Las opciones sobre clonaciones son:

- ✓ Clonar un disco a otro disco
- ✓ Clonar una partición a otra partición

Herramientas para crear imágenes y clonaciones

Las herramientas que se muestran aquí, se pueden utilizar tanto en Windows como en Linux.

Clonezilla

La herramienta Clonezilla, es software libre basada en GNU-Linux, aunque se pueda utilizar también en Windows.

Se utiliza un CD o pendrive de arranque. Existe una versión para realizar las imágenes o clonaciones en la red conocida como DRBL-Clonezilla

Comando dd de GNU-Linux

El comando dd sirve para clonar discos duros, particiones, crear imágenes, copiar dvd. Su versatilidad es impresionante.

Ejemplo:

Clonar toda la información de un disco origen (suponer sda) en otro disco destino (suponer sdb). Por supuesto el disco destino, tiene que ser igual o más grande que el origen (una vez clonado, se podrían redimensionar las particiones con Gparted)

```
miguel@portatil:~$ sudo dd if=/dev/sda of=/dev/sdb bs=1M
```

```
..... #hasta que no aparezca línea del shell, no ha terminado la copia. Se ha clonado un 31229607936 bytes (31 GB) copiados, 2583,43 s, 12,2 MB/s #pendrive a otro.
```

```
miguel@portatil:~$
```

Se pueden ver más ejemplos de utilización de dd en:

[Ejemplo 1](#)

[Ejemplo 2](#)

Otras aplicaciones privativas o comerciales:

- ✔ Norton Ghost
- ✔ Acronis

Tal vez las más utilizadas en las empresas por su facilidad de uso. Más orientadas a los usuarios de Windows por su entorno gráfico.

Con respecto a Clonezilla, tienen la ventaja de que si el origen es un disco más grande que el destino, redimensionan las particiones de destino de forma automática, mientras que en Clonezilla, es necesario que el destino siempre sea igual o más grande que el origen.

Recordar en todo caso, que las 4 aplicaciones contadas en este apartado, admiten crear imágenes y clonaciones tanto en Windows como en Linux.

Páginas oficiales de [Ghost](#) y [Acronis](#):

2.2.- Ejemplo. Crear una imagen con Clonezilla.

Este apartado corresponde a un ejercicio de la tarea, por lo que se debe obtener las capturas correspondientes para su entrega.

Paso 1. Preparación inicial de la máquina de Windows.

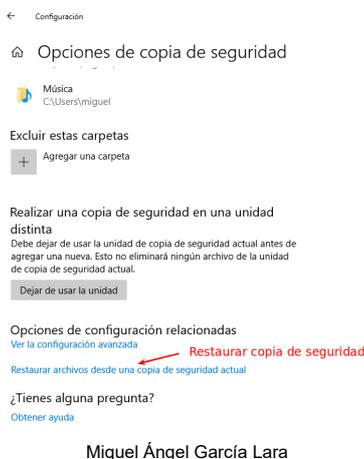
Se va a crear una imagen de la partición del primer Windows instalado en la unidad 1. Para tener un disco bastante limpio, restaura la instantánea creada en la tarea SI01.

Sino creaste esa instantánea, utiliza el administrador de discos para eliminar las particiones creadas para segundo Windows y posteriores. Se parte de una situación parecida a la siguiente:

Disco de 100 GB con 2 particiones y espacio libre:

- ✓ Partición de 550MB con el espacio reservado para Windows.
- ✓ Partición de 50000MB con primer Windows instalado en tarea SI01.
- ✓ Espacio libre en resto del disco.

Con el administrador de discos de Windows crear una partición de 40000MB en espacio libre con sistema de archivos NTFS. La situación del disco será aproximadamente:



Paso 2. Descarga de Clonezilla.

La descarga de Clonezilla, se realiza desde [enlace de descarga](#).

Descargar la versión estable (stable 2.6.0.37 en el momento de la realización de este material). El archivo a descargar, es el archivo iso correspondiente al CD de Clonezilla.

Para su descarga, seleccionar archivo iso de 32 o 64 bits, según Windows instalado. En principio, la de 64 bits será más eficiente en PC de 64 bits, pero sin embargo la de 32 bits funcionará en todos los PC.



Como se dijo en epígrafe anterior, estos programas se ejecutan desde autoarranque, por lo que siempre tendremos un archivo iso para grabar en CD o ponerlo en un pendrive de autoarranque con Yumi como hicimos en la tarea de la unidad 2.

En nuestro caso, vamos a realizar la práctica en VirtualBox, por lo que solo hay que descargar el archivo iso y montarlo como CD en la máquina virtual.

Paso 3. Inicio de Clonezilla.

Apagar la máquina Windows y poner como CD la iso descargada de Clonezilla.

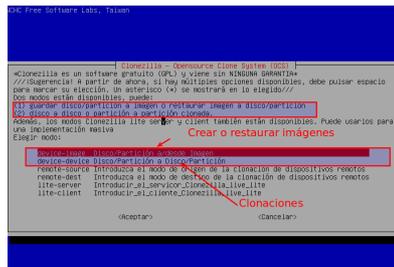
Iniciar la máquina con Clonezilla.

Van apareciendo pantallas sucesivas, ir respondiendo:

- ✓ Clonezilla live
- ✓ Idioma español
- ✓ Mantener la distribución del teclado
- ✓ Iniciar Clonezilla

Paso 4. ¿Imagen o clonación?

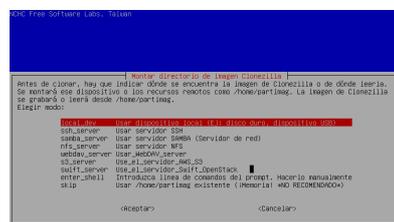
En la siguiente ventana, aparece la primera opción importante. En nuestro caso seleccionar la primera opción "Disco particion a/desde Imagen", pues queremos crear una imagen. Fijarse que la segunda opción sería para realizar clonaciones.



Miguel Ángel García Lara (CC BY-NC-SA)

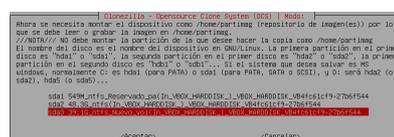
Paso 5. Seleccionar particion donde vamos a guardar o leer la imagen

La ventana siguiente es muy importante interpretarla bien. Solo hay que pulsar Intro, pero tenemos que entender que vamos a seleccionar el disco y partición donde tenemos o vamos a guardar la imagen, en nuestro caso habrá que seleccionar la partición 3 donde guardaremos la imagen. De momento, pulsar Intro con la opción por defecto.



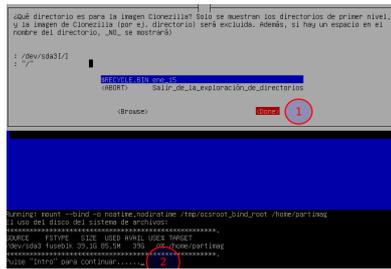
Miguel Ángel García Lara (CC BY-NC-SA)

En la siguiente ventana, como solo hay un disco duro, nos pregunta directamente la partición. Seleccionamos sda3 que es donde vamos a guardar la imagen.



Miguel Ángel García Lara (CC BY-NC-SA)

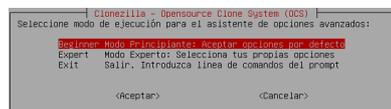
Al decirle que la imagen se va a guardar o se encuentra en sda3, explora la unidad y ve que no hay ninguna imagen, por lo que ya sabe que vamos a crear una imagen. De forma, que la siguiente pregunta es para decir en qué directorio guardamos, dejamos opciones por defecto. Pulsamos “Done” e “Intro”



Miguel Ángel García Lara (CC BY-NC-SA)

Paso 6. Seleccionar modo principiante

En la siguiente ventana simplemente seleccionamos modo principiante.



Miguel Ángel García Lara (CC BY-NC-SA)

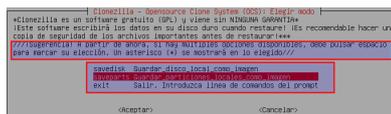
Paso 7. Seleccionar particiones a incluir en la imagen

Después se pregunta si queremos crear una imagen del disco o de particiones. En nuestro caso la creamos de particiones.

Recuerda que si quisiéramos crear una imagen del disco entero, deberíamos tener otro disco o pendrive, para guardar la imagen en otro sitio distinto.

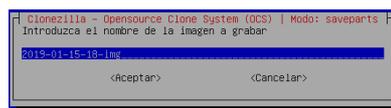
Marcamos “**Guardar particiones locales como imagen**”.

En la imagen se ha marcado un cuadro que se entenderá en posteriores ventanas.



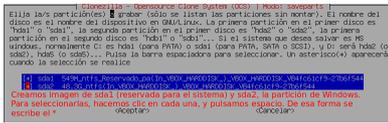
Miguel Ángel García Lara (CC BY-NC-SA)

El siguiente mensaje solo es informativo, se crea una carpeta con la fecha para guardar la imagen. Pulsamos Aceptar.



Miguel Ángel García Lara (CC BY-NC-SA)

En la siguiente ventana, debemos seleccionar las particiones a incluir en la imagen. Seleccionamos sda1 y sda2, de esta forma estamos guardando la imagen tanto de la partición reservada para el sistema como de la partición de Windows. Para seleccionarlas, hay que hacer clic en cada una, y pulsar espacio. De esta forma aparece un * de que la partición está seleccionada.



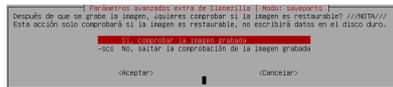
Miguel Ángel García Lara ([CC BY-NC-SA](#))

Paso 8. Últimas opciones

Las 2 ventanas siguientes preguntan si se quiere comprobar errores. En la primera pregunta si comprueba los errores de las particiones origen, le decimos omitir, pues ya dice la propia ventana que solo comprueba errores de sistemas de archivos de Linux.

En la segunda ventana, pregunta si se quiere comprobar errores de la imagen una vez creada. Le podemos decir que Sí y Aceptar. Esto alargará el tiempo de la creación de imagen, pero se sabrá que la imagen es correcta. Lo más importante, para tener éxito en la creación y restauración de imágenes, es que las particiones no tengan errores cuando se realiza la imagen, y que la última vez se haya apagado bien la máquina. Por ejemplo, es habitual ver la siguiente situación:

Se quiere clonar o crear una imagen. Se utiliza un CD o pendrive para arrancar el programa: Clonezilla, Acronis, Ghost,.. y al iniciar, se omite cambiar la BIOS para que inicie el CD (o pendrive). Windows empieza a arrancar, y se apaga a lo bruto, para iniciar el Cd. Ese estado del disco es inestable, si se crea la imagen así, lo normal es que falle.



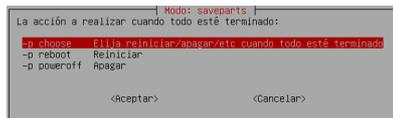
Miguel Ángel García Lara ([CC BY-NC-SA](#))

En la siguiente ventana, le decimos "No cifrar la imagen". Si la ciframos, nos pedirá una contraseña que tendríamos que usar al restaurar.



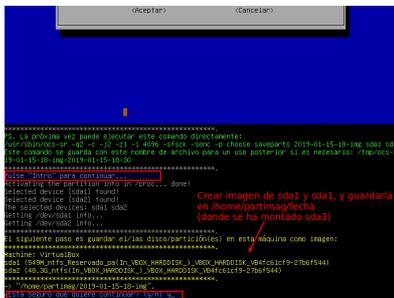
Miguel Ángel García Lara ([CC BY-NC-SA](#))

En la siguiente se pregunta que se quiere cuando se acabe de crear la imagen. Se ha seleccionado que presente un menú "Elija reiniciar/apagar...". Si prefieres, puedes pulsar Apagar.



Miguel Ángel García Lara ([CC BY-NC-SA](#))

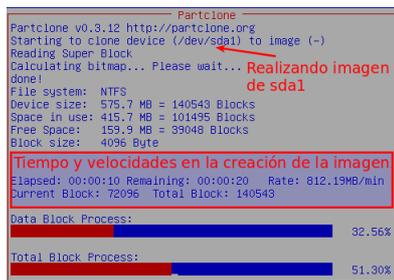
La siguiente ventana es informativa de las acciones que se van a realizar. Se pulsa Intro e y para continuar.



Miguel Ángel García Lara (CC BY-NC-SA)

Paso 9. Realizando las imágenes

Por fin se están realizando las imágenes de ambas particiones. Se pone captura del proceso en 2 instantes distintos.



Miguel Ángel García Lara (CC BY-NC-SA)



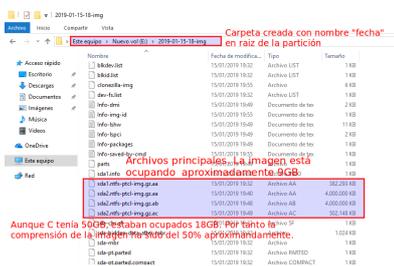
Miguel Ángel García Lara (CC BY-NC-SA)

Una vez acabada, volverá al menú, donde se selecciona apagar el equipo.

Paso 10. Imágenes finalizadas. Comprobación de la carpeta creada con la imagen.

Iniciamos de nuevo la máquina Windows Sistemas en Windows (comprobando previamente que no esté montada la iso de Clonezilla). Una vez iniciada, se comprueba que se ha creado la imagen. Se pone captura.

La partición de C tenía 50 GB, de los que estaban ocupados unos 18GB. Sin embargo la imagen ha ocupado 9 GB, es decir que la compresión es de un 50% aproximadamente.



Miguel Ángel García Lara (CC BY-NC-SA)

Si fallara Windows en un futuro, podríamos restaurar las particiones "Reservado para el Sistema" sda1 y la partición "C:" sda2 de una forma muy similar con algún pequeño cambio en los menús.

3.- Cifrado de archivos y particiones.

Caso práctico



descifrar.

Un tema que le preocupa a Juan es cómo cifrar archivos y particiones los recursos de equipos.

Porque poner todo a disposición de todos, que sería lo más fácil, puede suponer problemas de seguridad en la red y una mala gestión de los recursos. Así que será necesario, establecer una política de gestión de cifrado de archivos y particiones, de forma que solo los pueda leer la persona que conozca la clave para

En este capítulo se van a estudiar algunas herramientas que sirven para cifrar archivos y particiones, de forma que solo los pueda leer la persona que conozca la clave para descifrar.

3.1.- Cifrado de archivos en Windows con EFS “Encrypting File System”. Sistema de encriptación de ficheros.

Se comienza en este apartado con la herramienta EFS que ofrece Windows. Es importante aclarar, que esta herramienta servirá para cifrar una carpeta con sus archivos pero no particiones.

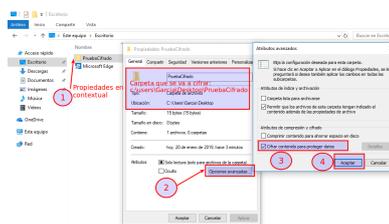
Éstas son algunas **características** destacadas de EFS:

- ✓ El cifrado es sencillo. Se realiza activando una casilla en las propiedades del archivo o de la carpeta.
- ✓ Ningún otro usuario que acceda a ese archivo, podrá abrirlo.
- ✓ El sistema EFS basa su seguridad en usuario, no en contraseña. El usuario, cuando cifra el archivo no escribe ninguna contraseña, y los puede abrir automáticamente. Sin embargo, si intenta acceder otro usuario no tendrá acceso.
- ✓ Se puede desactivar el cifrado del archivo, desactivando la casilla en las propiedades del archivo.
- ✓ Sólo se pueden cifrar archivos y carpetas en sistemas de archivos NTFS.
- ✓ Al cifrar archivos y carpetas comprimidos se descomprimirán.
- ✓ Los archivos marcados con el atributo del sistema no se pueden cifrar.
- ✓ EFS se instala de manera predeterminada en Windows 10 Profesional y superiores.

Procedimiento para cifrar un archivo o carpeta con EFS

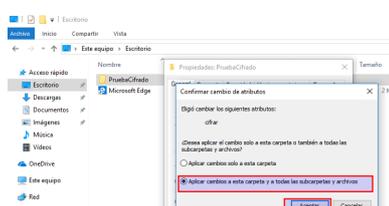
En el explorador de Windows, se selecciona Propiedades en el menú contextual del archivo o carpeta.

Se abre la solapa General / Avanzadas y se activa la casilla Cifrar contenido para proteger datos y Aceptar.



Miguel Ángel García Lara (CC BY-NC-SA)

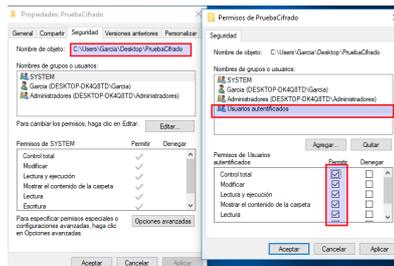
Si estamos cifrando una carpeta, nos preguntará si queremos cifrar todo el contenido o solo la carpeta.



La carpeta ya está cifrada. Se puede observar un candado pequeño en el nombre de la carpeta. El usuario no tendrá que introducir en ningún momento clave para acceder a ella, pero otro usuario no podrá acceder.

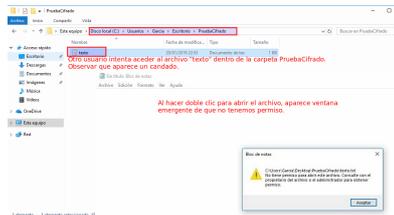
Comprobación de que otro usuario no tiene acceso a los archivos contenidos en la carpeta

Antes de comprobarlo, vamos a asegurarnos de que ese otro usuario va a poder acceder por permisos NTFS. Para ello, se ha incluido a "Usuarios autenticados" con permiso total en la carpeta, tal como se ve en la imagen.



Miguel Ángel García Lara (CC BY-NC-SA)

Al iniciar sesión con otro usuario, debería acceder a los archivos que hay dentro de la carpeta, pero al intentar abrir el archivo texto.txt dentro de la carpeta no se tiene permiso.



Miguel Ángel García Lara (CC BY-NC-SA)

Exportar certificado y clave

Una vez cifrada el archivo o carpeta, aparece en el área de notificaciones qué se debe hacer una copia de seguridad del certificado y la clave de cifrado en una unidad extraíble. Si la clave de cifrado se pierde o queda dañada y no tenemos copia de seguridad, no podremos recuperar los datos.

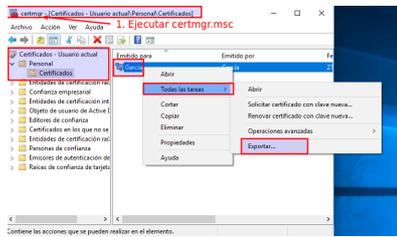
En el proceso de exportar certificado, se solicita una clave al usuario que tendrá que guardar en sitio seguro.

Si hubiera problema en el futuro con la clave original, habría que importar este certificado.

Procedimiento para exportar certificado y clave. Pasos.

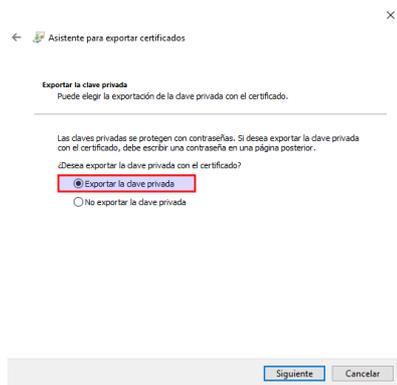
En vez de utilizar el proceso del asistente de notificaciones, se ha optado por mostrar el procedimiento general completo, que no depende de la notificación.

- ✓ Ejecutar el programa de certificados de Windows 10: certmgr.msc
- ✓ Ir a Certificados/Personal/Certificado. Aparecerá el certificado creado al cifrar una carpeta, con el nombre de usuario.
- ✓ Pulsar en menú contextual Todas las tareas / Exportar



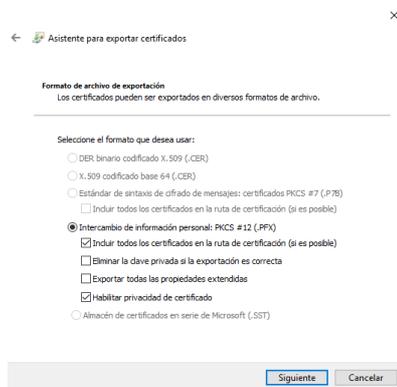
Miguel Ángel García Lara (CC BY-NC-SA)

✓ En la ventana siguiente, seleccionar “Exportar la clave privada” y pulsar Siguiente.



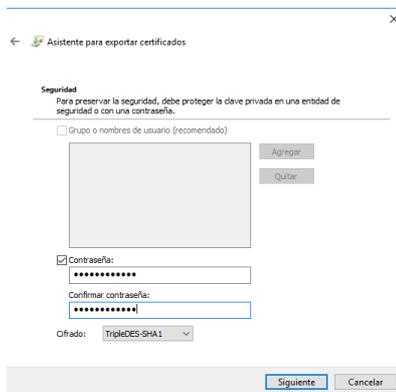
Miguel Ángel García Lara (CC BY-NC-SA)

✓ El archivo a exportar con el certificado, puede tener distintas extensiones. Dejamos opción por defecto, extensión pfx



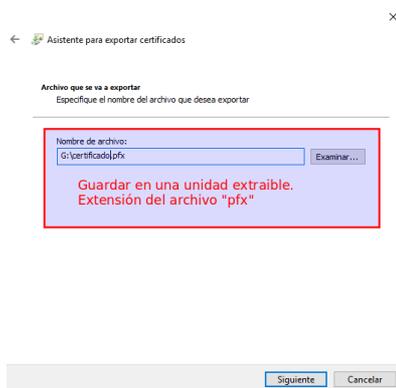
Miguel Ángel García Lara (CC BY-NC-SA)

✓ Hacer clic en Contraseña y escribirla 2 veces. Pulsar siguiente.



Miguel Ángel García Lara ([CC BY-NC-SA](#))

- ✔ Pulsar en examinar para guardar el certificado en una unidad extraíble.

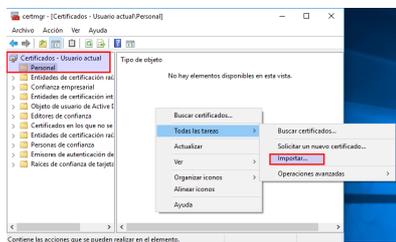


Miguel Ángel García Lara ([CC BY-NC-SA](#))

Importación de certificado

En caso de que el certificado original fallara, se importaría el certificado y clave de forma similar. Para ello:

- ✔ Ejecutar certmgr.msc
- ✔ Ir a Certificados / Personal y menú contextual "Todas las tareas / Importar"



Miguel Ángel García Lara ([CC BY-NC-SA](#))

- ✔ A partir de esta ventana solo queda buscar el certificado en la unidad extraíble.

3.2.- Cifrado de unidades lógicas en Windows con BitLocker.

BitLocker permite cifrar las unidades lógicas, incluso en la que está instalado el Sistema Operativo.

BitLocker en Windows 7 solo está disponible en las versiones Ultimate y Enterprise, pero en Windows 10 se encuentra disponible también en Windows 10 Profesional.

Para poder cifrar la partición del Sistema Operativo, es necesaria tener una partición reservada para el sistema. Por este motivo, cuando se instala Windows se crea automáticamente la partición de 550MB, por si en un futuro se quiere cifrar C; pues los archivos de sistema necesarios para el inicio no pueden estar cifrados.

BitLocker To Go, permite cifrar dispositivos de almacenamiento portátiles que se extravían fácilmente, como unidades flash USB y unidades de disco duro externas.

Para utilizar BitLocker es necesario que el hardware del PC incorpore el módulo TPM de seguridad (Trusted Platform Module, Módulo de Plataforma Confiable), en su defecto utilizaremos un medio de almacenamiento externo para almacenar la clave.

El objetivo de TPM es dar seguridad basada en hardware, más difícil de romper que la seguridad basada en software.

[Más información sobre TPM.](#)

Para abrir BitLocker ir a:

Panel de control / Sistema y seguridad / Cifrado de unidad BitLocker

Aparece la ventana de la imagen, en la que nos da la opción de activarlo en C y resto de particiones del disco, así como activar BitLocker To Go en las unidades extraíbles.



Miguel Ángel García Lara ([CC BY-NC-SA](#))

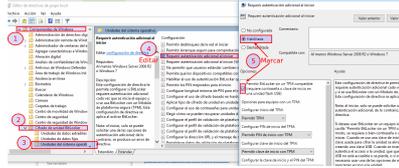
Se va a desarrollar el ejemplo de cifrar C. Este ejemplo se va a desarrollar en una máquina anfitrión Windows. Para la tarea se va a solicitar cifrar BitLocker To Go en un pendrive, para evitar manipulaciones en las máquinas anfitriones de los alumnos.

En la imagen se ha seleccionado **“Activar BitLocker en C”**. Al pulsar, se abre la ventana de que el PC no tiene el módulo TPM, por lo que hay que editar la directiva local “Requerir autenticación adicional al iniciar”



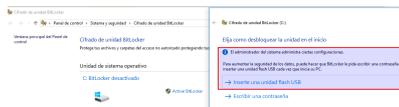
Miguel Ángel García Lara ([CC BY-NC-SA](#))

Tal como se vio en la unidad 4, abrimos el editor de directivas, ejecutando gpedit.msc. Para llegar y editar la directiva, seguimos los pasos de la imagen:



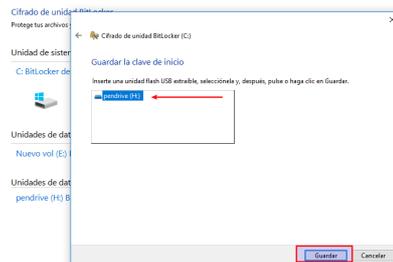
Miguel Ángel García Lara (CC BY-NC-SA)

Una vez realizado el cambio de directiva, volvemos al paso anterior para cifrar C. Ahora al seleccionar **“Activar BitLocker en C”** se abre la ventana siguiente. Seleccionar **“Inserte una unidad flash USB”**



Miguel Ángel García Lara (CC BY-NC-SA)

En la siguiente ventana, solo hay que **seleccionar nuestra unidad flash** y pulsar **Guardar**.

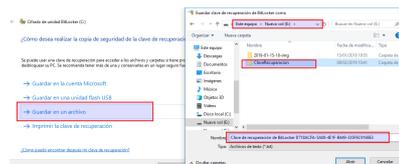


Miguel Ángel García Lara (CC BY-NC-SA)

En la siguiente ventana, se pregunta dónde queremos guardar la clave de recuperación. Es necesario explicar, que esta clave se necesitará en caso de desastre. Supongamos que en un futuro, fallara el pendrive, pues tendríamos esta clave guardada en un archivo de texto plano en otro sitio; como clave de rescate.

Por este motivo, en este caso se ha decidido **“Guardar en un archivo”**.

Al pulsar **“Guardar en un archivo”** hay que seleccionar donde guardar ese archivo. De momento, lo he guardado en el equipo local (tiene que ser en otra unidad distinta de la que se está cifrando, aunque lo coherente será guardarlo en otro extraíble distinto).

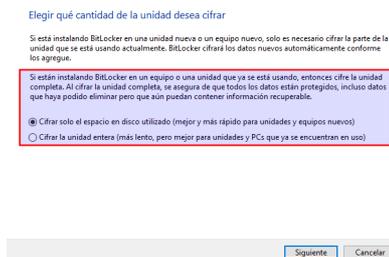


Miguel Ángel García Lara (CC BY-NC-SA)

En la siguiente ventana, se pregunta si queremos cifrar solo el contenido utilizado o toda la unidad. En este caso se ha decidido **“sólo espacio utilizado”** para tardar menos tiempo por ser un ejemplo didáctico, pero lo normal será **“Cifrar la unidad entera”**.

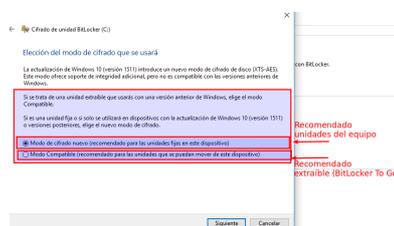
Explicar aquí, que cuando se borran los archivos, realmente no se borran, sino que se borra la entrada en el directorio. Para entenderlo, si se copia un archivo de 10 GB, se tarda un rato;

sin embargo si se borra, se tardan segundos. ¿Por qué?, porque realmente no se borra el archivo, sino que se borra la entrada al directorio; por eso en muchos casos se puede recuperar la información borrada en un PC. Un software para este fin es Recuva.



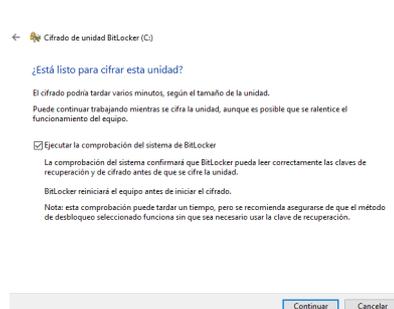
Miguel Ángel García Lara ([CC BY-NC-SA](https://creativecommons.org/licenses/by-nc-sa/4.0/))

En la siguiente ventana hay 2 opciones. La primera pensada si ciframos particiones del PC, la segunda si ciframos unidades extraíbles. Por tanto en este caso seleccionamos “**Modo de cifrado nuevo...**”



Miguel Ángel García Lara ([CC BY-NC-SA](https://creativecommons.org/licenses/by-nc-sa/4.0/))

Finalmente, aparece la ventana de que el sistema va a realizar las comprobaciones y el cifrado de la unidad. Una vez pulsado Continuar, habrá que **reiniciar el equipo**.



Miguel Ángel García Lara ([CC BY-NC-SA](https://creativecommons.org/licenses/by-nc-sa/4.0/))

Al reiniciar el equipo, si no ha habido ningún problema, el equipo se encuentra cifrado. Una vez activado Bitlocker, cada vez que se inicie el equipo habrá que utilizar el dispositivo extraíble donde hemos almacenado la clave.

3.3.- Cifrado de archivos y unidades lógicas con VeraCrypt.

En Linux también hay herramientas propias de cifrado de particiones o unidades lógicas, pero en cambio de ver herramientas concretas para GNU-Linux, este apartado se va a dedicar a VeraCrypt.

TrueCrypt era una aplicación OpenSource para cifrar. En el año 2014, la aplicación se abandonó generando bastante controversia en el mundo informático, pues los estudios decían que era un software muy seguro, mientras que los propios desarrolladores en su página oficial, desviaban a utilizar BitLocker.

Abandonado TrueCrypt, nace VeraCrypt como bifurcación, utilizando el código abierto de TrueCrypt. VeraCrypt sigue obteniendo versiones mejoradas, solucionando errores y bugs encontrados y siendo software libre.

VeraCrypt tiene las siguientes ventajas:

- ✔ Se puede utilizar en Windows, GNU-Linux y MacOS
- ✔ Sirve tanto para cifrar particiones como archivos (para ello se creará un contenedor)

Si queremos cifrar una partición en una máquina Windows, será más razonable utilizar BitLocker. Pero si queremos cifrar una unidad extraíble, y la queremos utilizar en distintas máquinas, que tienen Sistemas Operativos Windows y sistemas GNU-Linux, tendremos que utilizar VeraCrypt por ser quien nos da dicha versatilidad. Comercialmente, muchos pendrives traen este tipo de software para cifrar, pero normalmente solo funciona en Windows.

Vínculos para obtener más información sobre [TrueCrypt](#) (discontinuado) y [VeraCrypt](#) (el relevo)

Ejemplo completo. Instalar VeraCrypt y crear un contenedor seguro en una unidad extraíble.

Este ejemplo, formará parte de la tarea SI07 a realizar.

Normalmente, tenemos pocos datos importantes. Por ejemplo, como profesor, me interesa una carpeta segura para las notas o los exámenes; pero el resto: apuntes, software, no me importa que caigan en manos de alguien. Por lo que suele ser suficiente tener un espacio pequeño encriptado.

El ejemplo que se detalla en este apartado, es crear un contenedor seguro en un pendrive. Este contenedor estará cifrado, e introduciremos dentro los archivos a esconder. El contenedor, realmente será un fichero que ocupará el espacio que le reservemos.

Montaremos el contenedor en un **volumen lógico** (una letra de partición)

Para realizar este apartado se han seguido algunos pasos de un manual muy completo de VeraCrypt en la [dirección](#).

Pasos:

Paso 1. Descarga VeraCrypt portable para Windows

Descargar el programa desde su [página oficial](#):

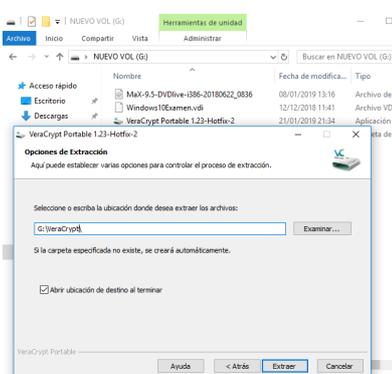
Podemos descargar versión estándar o versión portable. Si descargamos la versión estándar, tendríamos que instalarla en todos los equipos con Windows que vayamos a utilizar VeraCrypt.

En nuestro caso, vamos a descargar la versión portable, de forma que la instalaremos en el pendrive, y ya no tendremos que instalarla en el resto de equipos con Windows que queramos utilizar el contenedor.

[Vínculo](#) directo de descarga de la versión portable.

Paso 2. Instalar VeraCrypt.

La instalación no tiene dificultad, lo único a reseñar es que al descomprimir la aplicación, el destino será en una carpeta del pendrive. En la imagen, se ha dejado la carpeta por defecto.

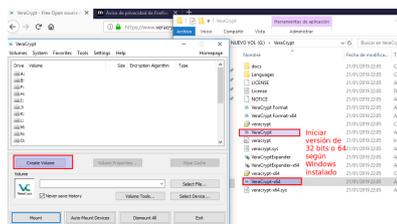


Miguel Ángel García Lar ([CC BY-NC-SA](#))

Al finalizar la instalación, el programa pregunta si se quiere realizar una donación para facilitar el mantenimiento del software al creador.

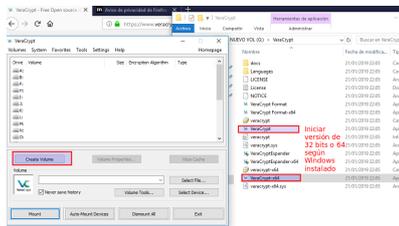
Paso 3. Abrir el programa

Se abre el programa con el ejecutable que se encuentra en la carpeta donde se ha instalado VeraCrypt. Se ejecuta el ejecutable adecuado (32 o 64 bits) según Windows instalado.



Miguel Ángel García Lara ([CC BY-NC-SA](#))

Una vez abierto, se pulsa en **“Create Volume”** para crear el contenedor donde se guardaran los ficheros a encriptar.



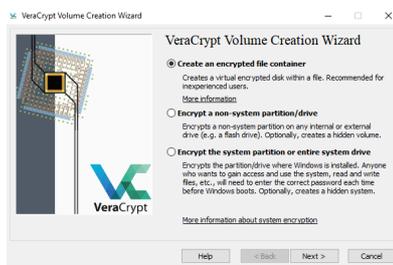
Miguel Ángel García Lara ([CC BY-NC-SA](#))

Paso 4. Crear volumen

Al pulsar Crear volumen, nos aparece una ventana, en la que se pregunta la opción que se desea:

- ✓ Crear un fichero contenedor
- ✓ Encriptar una partición o unidad que no tenga el Sistema Operativo
- ✓ Encriptar la partición o unidad completa con el Sistema Operativo

Se selecciona **“Crear un fichero contenedor”**.



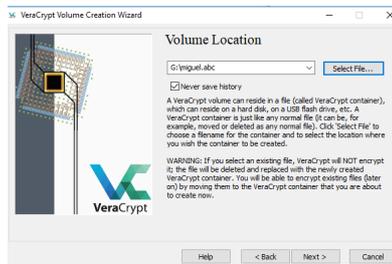
Miguel Ángel García Lara ([CC BY-NC-SA](#))

En siguiente ventana se pregunta si se quiere crear un “Volumen estándar” o un “Volumen oculto”. El volumen oculto, permite establecer 2 niveles distintos de visibilidad dentro del contenedor. En nuestro caso, seleccionar **“Volumen estándar”**.



Miguel Ángel García Lara ([CC BY-NC-SA](#))

En la siguiente ventana se selecciona el fichero que va a ser el contenedor. Se suele crear un fichero con un nombre que despiste, en este caso se ha decidido poner una extensión extraña al fichero **miguel.abc** de esta forma se despista en caso de perderse la unidad. VeraCrypt va a convertir este fichero en el contenedor.



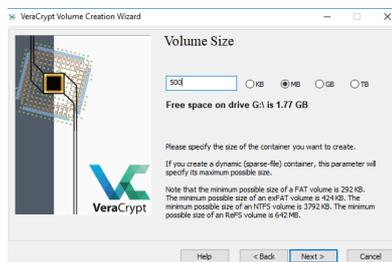
Miguel Ángel García Lara ([CC BY-NC-SA](#))

En la siguiente ventana, se pregunta qué algoritmos se van a utilizar para guardar la clave. Se dejan las opciones por defecto y se pulsa **Next**.



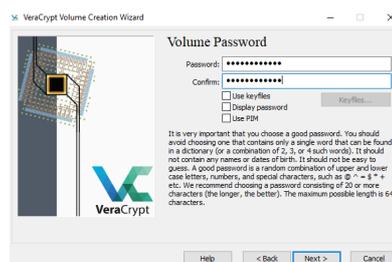
Miguel Ángel García Lara ([CC BY-NC-SA](#))

En la siguiente ventana, se pregunta **tamaño del fichero contenedor**.



Miguel Ángel García Lara ([CC BY-NC-SA](#))

Después escribimos el password que queremos utilizar 2 veces. VeraCrypt da mucha importancia a este tema, pues uno de los problemas habituales de la seguridad informática comienza por el mismo usuario, pues se tiene la mala costumbre de utilizar contraseñas fáciles de recordar.

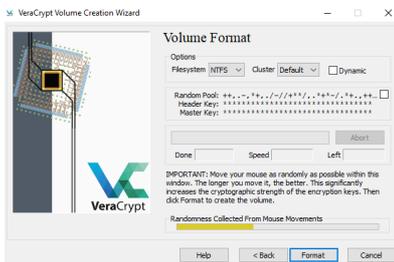


Miguel Ángel García Lara ([CC BY-NC-SA](#))

Ahora se pregunta con que sistema de ficheros se crea el contenedor: fat, ntfs. Si se selecciona NTFS, se debe tener en cuenta que los sistemas operativos posteriores que

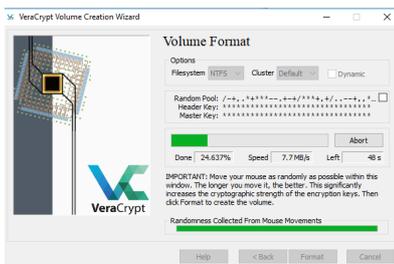
utilicemos con ese contenedor deben permitir leer y escribir particiones NTFS.

- ✓ Seleccionar NTFS (en nuestro caso, Ubuntu lee y escribe particiones NTFS)
- ✓ Después, mover el ratón por la pantalla contantemente. Hasta que aparezca en color verde la barra “Randomness...”
- ✓ Esto sirve para dar más fuerza a la password.
- ✓ Pulsar “Format”



Miguel Ángel García Lara (CC BY-NC-SA)

Se pone una imagen donde se está formateando la partición.



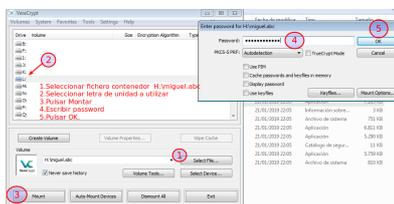
Miguel Ángel García Lara (CC BY-NC-SA)

Cuando acaba, aparece un mensaje de finalización de crear volumen.

Utilización del contenedor en Windows.

Una vez creado el volumen, ya se está en disposición de utilizarlo en cualquier máquina Windows. Además llevamos el programa instalado en la unidad extraíble, por lo que solo se abrirá el programa en cualquier PC y se siguen los pasos siguientes:

- ✓ Se selecciona el fichero contenedor **H:\miguel.abc**
- ✓ Se selecciona **una letra de unidad libre**, donde se va a montar el contenedor. En la imagen se ha seleccionado L.
- ✓ Se pulsa **“Mount”**.
- ✓ Se abre ventana donde **rellenamos el password** y pulsamos OK.

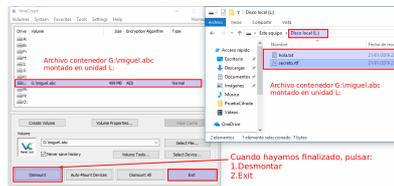


Miguel Ángel García Lara (CC BY-NC-SA)

A partir de ese momento, la unidad lógica L es como una partición más de nuestro sistema, donde podemos crear o copiar ficheros y carpetas de las formas habituales.

Cuando acabemos de utilizar la unidad, es importante seguir los 2 pasos siguientes:

1. Pulsar **Desmontar**
2. Pulsar **Exit**



Miguel Ángel García Lara (CC BY-NC-SA)

Instalación en GNU-Linux.

Para utilizar nuestro contenedor en una máquina Linux, tenemos que instalar el programa. Para ello, añadimos el repositorio y lo instalamos, tal como se explicó en la unidad 5.

Se ejecutan los 3 comandos siguientes:

```
#add-apt-repository ppa:unit193/encryption
```

.....

Pulse [ENTRAR] para continuar o Ctrl+C para cancelar la adición.

Añadimos el repositorio. A mitad de ejecución tenemos que pulsar Intro.

```
#apt update
```

Actualizamos los paquetes a instalar

```
#apt install veracrypt
```

Instalamos el programa

Utilización del contenedor en GNU-Linux.

Una vez instalado el programa, se puede utilizar tanto de forma gráfica como en terminal.

El funcionamiento del programa gráfico es idéntico a Windows, tanto en crear volumen como en montar el contenedor.

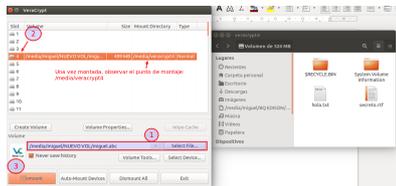
En el caso de GNU-Linux los contenedores se montarán en /media.

Para abrir el programa, escribir en terminal **veracrypt**. A continuación, como ya tenemos creado el volumen, solo tenemos que montar el contenedor:

- ✓ Seleccionar fichero contenedor
- ✓ Seleccionar número de montaje
- ✓ Pulsar "Mount"

Una vez montado, se abre gráficamente el explorador **nautilus** con el contenido de la unidad lógica.

En la imagen se muestra el programa, con el **contenedor montado en /media/veracrypt4**



Miguel Ángel García Lara ([CC BY-NC-SA](https://creativecommons.org/licenses/by-nc-sa/4.0/))

Autoevaluación

Si queremos cifrar un pendrive y utilizarlo en distintas maquinas Windows y Linux, ¿qué herramienta hay que utilizar?

- VeraCrypt
- dd
- EFS
- BitLocker

Respuesta correcta

Respuesta incorrecta.

Respuesta incorrecta.

Respuesta incorrecta.

Solución

1. Opción correcta
2. Incorrecto
3. Incorrecto
4. Incorrecto



4.- Sistemas RAID.

Caso práctico

Ada piensa que en los servidores se hace necesario imponer un sistema de forma que si falla un disco no se pierdan los datos. En el equipo ya se ha hablado de las copias de seguridad, que se suelen programar de forma automática para que se ejecuten a una hora determinada.

Ahora estudiarán la forma de implantar estas medidas de seguridad.



En esta unidad, vamos a hablar de RAID, que consiste en que varios discos duros funcionen como un solo disco, donde se almacenará información redundante (repetida), de forma que si un disco falla, el sistema pueda seguir funcionando sin pérdida de información de forma automática. Es decir, la primera ventaja de un RAID será su tolerancia a fallos.

Además, al almacenar la información entre varios discos también se incrementa la velocidad de transferencia, sea lectura o escritura, pues si repartimos los datos entre 3 discos, podremos escribir en todos a la vez incrementando su velocidad de transferencia.

Existen varios tipos de RAID, donde cada tipo exige un mínimo de discos duros e información redundante. A mayor cantidad de información repetida, se obtendrá mayor tolerancia a fallos (fiabilidad).

Para obtener las mejores prestaciones en los RAID, los discos duros serán de igual tamaño y con la misma geometría, pues si vamos a escribir en varios discos a la vez, lo ideal es que los retardos mecánicos de cambiar de cabeza o cilindro se produzcan a la vez.

4.1.- Sistemas RAID. “Redundant Array of Inexpensive Disks” (Matrices de discos Redundantes independientes).

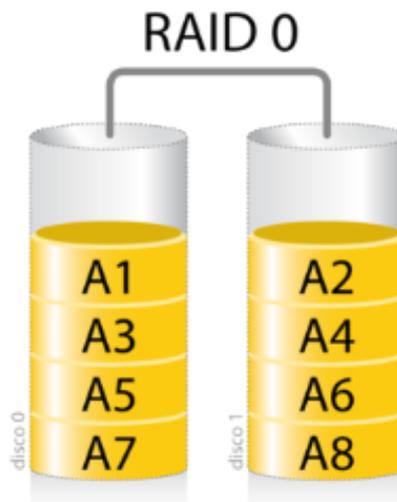
Tipos de RAID

Hay varios tipos de RAID. Los primeros que se estudian son RAID 0 y RAID 1 y van a servir para entender la tolerancia y velocidad de transferencia.

RAID 0. Data striping (Volumen seccionado)

Para construir un Raid 0 se necesitan 2 discos duros.

La información se divide en bloques de igual tamaño y se reparten los bloques entre los 2 discos de forma uniforme.



JaviMZN - Trabajo propio ([CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/))

De esta forma, se consigue la mayor velocidad de transferencia, pues se lee o escribe al doble de velocidad que con un solo disco duro, pues leemos o escribimos en los 2 discos a la vez. Pero no se obtiene mayor fiabilidad: en caso de que un disco falle, no se podrá recuperar la información.

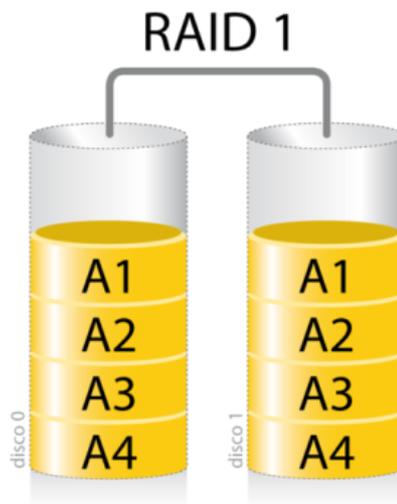
Si por ejemplo, se crea un RAID 0 utilizando 2 discos duros de 1 TB, se obtendrá un disco de 2 TB.

Para crear un RAID 0 se necesita un mínimo de 2 discos, pero se puede crear un RAID 0 de varios discos, incrementándose las velocidades de transferencia.

RAID 1. Mirroring (Volumen espejo)

Para construir un Raid 1 se necesitan 2 discos duros.

La información se divide en bloques de igual tamaño, pero se escriben todos los bloques en los 2 discos.



JaviMZN - Trabajo propio (CC BY-SA)

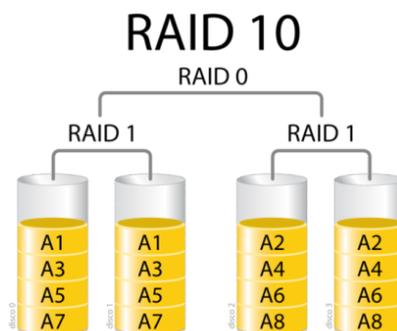
De esta forma, se consigue la máxima tolerancia a fallos, pues si se rompe un disco, el otro tiene toda la información. Pero no se gana velocidad en escritura, pues aunque se escriba a la vez en los 2 discos, se escribe toda la información en cada disco. Sí que se gana transferencia de lectura, pues al estar almacenada la misma información en 2 discos si se puede leer de ambos discos a la vez, leyendo por ejemplo del primer disco los bloques A1 y A2 y del segundo disco los bloques A3 y A4.

Si para crear RAID 1 se utilizan 2 discos duros de 1 TB, se obtendrá un único disco de 1 TB. RAID 1 desde el punto de vista económico es caro, pues de 2 discos duros, 1 se dedica a información redundante. Lo que es normal, pues la tolerancia a fallos o fiabilidad de los datos requieren un presupuesto económico.

Los siguientes RAID, van a ganar tanto en seguridad como en velocidad de transferencia.

RAID 10

Para construir un Raid 10 (también llamado RAID 1 +0) se necesitan 4 discos duros. Se trata de implantar tanto RAID 1 como RAID 0, para tener las ventajas de ambos.



JaviMZN - Trabajo propio (CC BY)

Si para crear un RAID 10 se utilizan 4 discos duros de 1 TB, se obtendrá un único disco de 2 TB. Se consigue una gran tolerancia a fallos y máxima velocidad de transferencia, pero el coste económico es muy alto, pues la mitad de los discos se utilizan para redundancia.

El mínimo de discos para crear RAID 10 es 4, pero también se podría crear un RAID 10 de 6 discos, creando 3 RAID 1 de 2 discos, y un RAID 0 con ellos.

RAID 5.

Para construir un RAID 5 se necesita un mínimo de 3 discos duros. La información se divide en bloques que se reparten entre todos los discos duros, pero en un disco se guarda información de paridad (información redundante). Esta información de paridad, servirá para

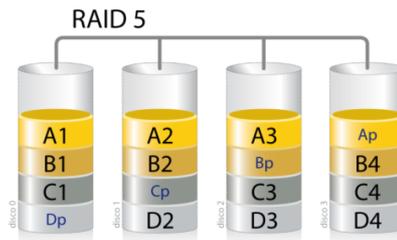
reconstruir la información si se rompe cualquier disco. Ver explicación de información de paridad.

Para explicar su funcionamiento, nos fijamos en la imagen siguiente, se tiene un RAID 5 de 4 discos, en la primera transferencia se ponen 3 bloques (A1, A2 y A3) de igual tamaño en los 3 primeros discos, mientras que en el cuarto disco se guarda la información de paridad.

En la segunda transferencia, se ponen 3 bloques (B1, B2 y B4) en los discos 1, 2 y 4, mientras en el tercer disco se guarda la información de paridad.

De esta forma hay un disco entero de paridad, o dicho de otra forma, hay 1 disco de información redundante.

La información redundante se reparte, pues se ha comprobado que es la forma más rápida de realizar las transferencias.



JaviMZN - Trabajo propio (CC BY)

Si para crear un RAID 5 se utilizan 4 discos duros de 1 TB, se obtendrá un único disco de 3 TB. De esta forma, con RAID 5 obtenemos la mejor relación rendimiento-coste, pues tenemos alta velocidad (en el ejemplo con 4 discos, triple de velocidad que con 1 disco duro sin RAID) y alta tolerancia, pues si se rompe un disco se puede recuperar la información y coste económico controlado. Claro, si fallan 2 discos no se podría recomponer la información.

En RAID 5 se necesitan un mínimo de 3 discos, pero se pueden poner varios discos, sabiendo que el esquema siempre será el aquí explicado, donde la información redundante es 1 disco.

Para saber más

Hay muchos más RAID: RAID 2, RAID 3, RAID 4, RAID 6, RAID 50. Todos buscan otras combinaciones, por ejemplo RAID 50 será la suma de crear un RAID 5 y un RAID 0. El RAID 6, mejora RAID 5 pues permite la posibilidad de fallo de 2 discos. Para más información, ver [otros sistemas RAID](#).

4.2.- Funcionamiento de un disco de paridad.

Se ha visto que en RAID 5 hay un disco de redundancia, también llamado disco de paridad. Este disco sirve para que si se estropea cualquier disco, se pueda reconstruir la información con el resto de discos.

Para entender como se explica en concepto de paridad. Se puede trabajar con 2 tipos de paridades: paridad par y paridad impar.

Paridad PAR significa que el número de 1 es par (puede haber 0 unos, 2 unos, 4 unos...)

Paridad IMPAR significa que el número de 1 es impar (puede haber 1 uno, 3 unos, 5 unos...)

Ejemplo con paridad PAR

Se suponen 3 discos duros de datos y el cuarto para paridad (tal como se ha visto en RAID 5)

En la tabla, se han puesto datos arbitrarios en los 3 primeros discos, en el cuarto se escriben 1 o 0 de forma que en cada columna tengamos un nº par de unos

Disco 1	1 0 0 0 0 1 0 1
Disco 2	0 1 0 0 1 1 0 1
Disco 3	1 0 1 1 1 0 0 1
Disco 4	0 1 1 1 0 0 0 1
Nº de unos	2 2 2 2 2 2 0 4

Reconstrucción de un disco

Si se estropea cualquier disco en un RAID por hardware, al poner un disco nuevo la misma controladora reconstruye la información.

La reconstrucción de los datos del disco se haría igual. Supongamos que se ha roto el disco 2. La información en el disco duro a sustituir, se calculará de la misma forma.

Disco 1	1 0 0 0 0 1 0 1
Disco 2	1 0 1 1 1 0 0 1
Disco 3	0 1 1 1 0 0 0 1
Disco 4	0 1 0 0 1 1 0 1
Nº de unos	2 2 2 2 2 2 0 4

Observar que el disco nuevo, tiene la misma información que el disco 2 original.

Por último, aclarar que en RAID 5, se distribuye la información de paridad en los distintos discos. Se realiza así para optimizar las lecturas y escrituras, pues la construcción del disco de paridad conlleva algunas manipulaciones, por lo que se reparte entre todos los discos. Pero eso, a la hora de recuperar la información no trae ningún problema.

4.3.- RAID por hardware o por software. Ejemplo.

Cuando se quiere crear un RAID, se puede crear por hardware o por software.

Por hardware, significa que el PC admite RAID (muchas placas base de PC de sobremesa lo admiten) o que utilizamos una tarjeta controladora RAID (PCI Express) donde se conectarán los distintos discos duros.

Por software, significa que tendremos varios discos, y bien con DiskPart en Windows o fdisk en Linux, se crea el RAID.

Las ventajas de un RAID por hardware son:

- ✓ Mejor rendimiento, pues la tarjeta controladora se encarga de las transferencias, librando al sistema operativo y procesador de esas funciones.
- ✓ Fácil de configurar
- ✓ Si se estropea un disco, se cambia y la controladora replica (reconstruye) la información.

Las desventajas de un RAID por hardware:

- ✓ El coste económico de la tarjeta
- ✓ Si se estropea la tarjeta controladora.
- ✓ El RAID hay que crearlo con los discos enteros, mientras que en un RAID por software también se puede crear con porciones (trozos) de discos duros.

Como es normal, las ventajas y desventajas de un RAID por software son las contrarias.

RAID por software en Windows. Discos dinámicos

Hasta ahora, siempre que hemos realizado particiones, han sido particiones en discos básicos. En la actualidad se habla de discos dinámicos. Si con los discos básicos hablamos de particiones y unidades lógicas, en los discos dinámicos hablamos de volúmenes dinámicos.

Un volumen dinámico, es que al crear el volumen se podrán utilizar trozos de distintos discos o del mismo disco que no estén contiguos.

Al crear volúmenes dinámicos en Windows, podremos seleccionar que se cree un RAID por software con ellos.

Este tipo de volúmenes pueden ser de 5 tipos:

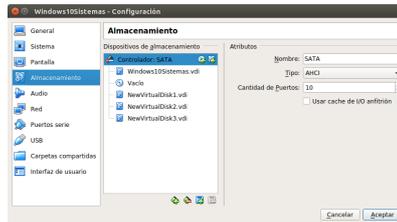
- ✓ **Volumen simple:** El volumen simple sirve para unir en un único volumen zonas no contiguas del mismo disco
- ✓ **Volumen distribuido:** sirve para unir en un único volumen zonas de distintos discos.
- ✓ **Volumen reflejado:** equivale a crear un RAID 1.
- ✓ **Volumen seccionado:** equivale a crear RAID 0
- ✓ **Volumen RAID 5:** como indica su nombre sirve para crear un RAID 5.

Ejemplo de creación de un RAID 0 por software en Windows

Este ejemplo formará parte de la tarea SI07.

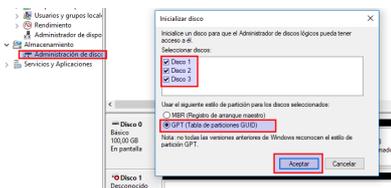
En máquinas virtuales solo se pueden crear RAID por software.

Se comienza insertando 3 discos duros nuevos en la máquina "Windows10Sistemas". Se ha insertado de 50 GB con tamaño dinámico.



Miguel Ángel García Lara (CC BY-NC-SA)

Iniciamos Windows y el Administrador de discos. Al iniciarlos, para crear discos dinámicos, los discos tienen que ser **GPT**.

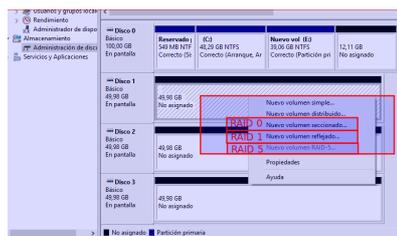


Miguel Ángel García Lara (CC BY-NC-SA)

Una vez iniciados los discos, pulsamos el menú contextual en el primer disco. Aparecen las opciones que admite GPT, tal como aparecen en la imagen y comentadas antes.

En nuestro caso seleccionamos "Nuevo volumen seccionado" para crear un RAID 0.

Se puede observar, que aunque tengamos 3 discos, el mínimo para crear un RAID 5, no aparece habilitada dicha opción. Eso es por una limitación de Windows 10 Profesional.

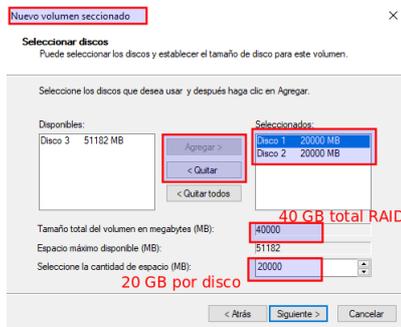


Miguel Ángel García Lara (CC BY-NC-SA)

Ahora hay que decir que los discos van a formar parte del RAID 0. Se van a utilizar los **discos 1 y disco 2**, para ello hay que **seleccionarlos** y pulsar **Agregar**.

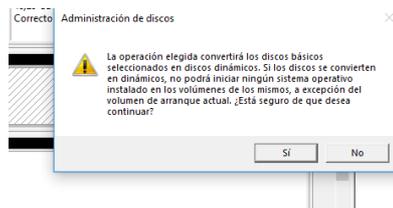
También se configura el tamaño, se ha decidido utilizar **20.000 MB** de cada disco por lo que el **volumen RAID 0** final va a ser de **40.000 MB**.

Pulsar Siguiente.



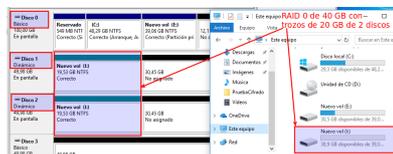
Miguel Ángel García Lara ([CC BY-NC-SA](#))

Aparece la ventana, que para crear volúmenes dinámicos, primero tiene que convertir los discos básicos en dinámicos.



Miguel Ángel García Lara ([CC BY-NC-SA](#))

Una vez convertidos los discos a dinámicos, y creado el RAID 0, aparece la ventana del administrador de discos con la misma letra en la partición de los 2 discos. Si se abre Equipo, se comprueba que el volumen resultante es de 40000 MB.



Miguel Ángel García Lara ([CC BY-NC-SA](#))

Para saber más

Finalmente, se añade un vínculo para crear RAID por software en GNU-Linux, donde hay que utilizar fdisk para crear las particiones de los discos, y mdadm como utilidad para crear el RAID.

[Creando un raid 0 para unir dos discos en linux.](#)

Autoevaluación

¿De qué RAID no se puede recuperar la información si se estropea un disco?

- RAID 5
- RAID 1
- RAID 0
- En todos los RAID se puede recuperar la información.

Respuesta incorrecta.

Respuesta incorrecta.

Respuesta correcta.

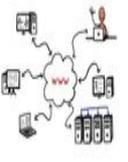
Respuesta incorrecta.

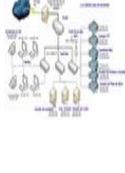
Solución

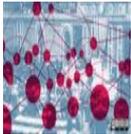
1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

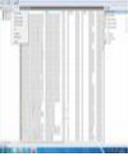
Anexo.- Licencias de recursos.

Licencias de recursos utilizados en la Unidad de Trabajo.

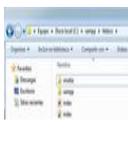
Recurso (1)	Datos del recurso (1)	Recurso (2)	Datos del recurso (2)
	<p>Autoría: BenSpark. Licencia: CC BY-NC-SA 2.0A. Procedencia: http://www.flickr.com/photos/a/bennett96/5000312736/</p>		<p>Autoría: Microsoft. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla de Windows 7.</p>
	<p>Autoría: Microsoft. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla de Windows 7.</p>		<p>Autoría: Microsoft. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla de Windows 7.</p>
	<p>Autoría: miniyo73. Licencia: CC BY-SA 2.0. Procedencia: http://www.flickr.com/photos/miniyo73/5663291297/sizes//in/photostream/</p>		<p>Autoría: Microsoft. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla de Windows 7.</p>
	<p>Autoría: ibuch. Licencia: CC BY-NC-SA 2.0. Procedencia: http://www.flickr.com/photos/ibuch/2861975307/sizes/t/in/photostream/</p>		<p>Autoría: Microsoft. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla de Windows.</p>
	<p>Autoría: pixle. Licencia: CC BY-NC-SA 2.0. Procedencia: http://www.flickr.com/photos/pixle/2000160844/sizes/t/in/photostream/</p>		<p>Autoría: Microsoft. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla de Windows 7.</p>
	<p>Autoría: Microsoft. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla de Windows 7.</p>		<p>Autoría: Microsoft. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla de Windows 7.</p>
	<p>Autoría: Microsoft. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla de Windows 7.</p>		<p>Autoría: Microsoft. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla de Windows 7.</p>

	Autoría: Microsoft. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla de Windows 7.		Autoría: Microsoft. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla de Windows 7.
	Autoría: Microsoft. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla de Windows 7.		Autoría: Microsoft. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla de Windows 7.
	Autoría: Microsoft. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla de Windows 7.		Autoría: davydubbit. Licencia: CC-BY-NC. Procedencia: http://www.flickr.com/photos/95745910@N00/3435484286
	Autoría: FlickrDelusions. Licencia: CC-BY-NC-SA. Procedencia: http://www.flickr.com/photos/27195496@N00/2366484391		Autoría: Jinho Jung. Licencia: CC-BY-NC-SA. Procedencia: http://www.flickr.com/photos/hploveme/3394511146/in/photostream/
	Autoría: Desconocida. Licencia: Dominio público. Procedencia: http://www.public-domain-photos.com/free-cliparts/computer/filesystems/folder2-1781.htm		Autoría: _rfc_. Licencia: CC-BY-NC-SA. Procedencia: http://www.flickr.com/photos/65124317@N02/5954920966
	Autoría: _rfc_. Licencia: CC-BY-NC-SA. Procedencia: http://www.flickr.com/photos/65124317@N02/5954920204		Autoría: _rfc_. Licencia: CC-BY-NC-SA. Procedencia: http://www.flickr.com/photos/65124317@N02/5954920204
	Autoría: _rfc_. Licencia: CC-BY-NC-SA. Procedencia: http://www.flickr.com/photos/_rfc_/5954919436/in/photostream/		Autoría: -. Licencia: Dominio público. Procedencia: http://www.public-domain-photos.com/free-cliparts/computer/applications/printer-1585.htm
	Autoría: Old Shoe Woman (Judy Baxter). Licencia: CC-BY-NC-SA. Procedencia: http://www.flickr.com/photos/3955435@N00/76127449		Autoría: Desconocida. Licencia: Dominio público. Procedencia: http://www.public-domain-photos.com/free-cliparts/computer/hardware/computer-aj_aj_ashton_01-1860.htm
	Autoría: Desconocida. Licencia: Dominio público. Procedencia: http://www.public-domain-photos.com		Autoría: Bull3t Hughes. Licencia: CC-BY-SA. Procedencia: http://www.flickr.com/photos/5

	<p>s.com/free-cliparts/computer/filesystems/folder2-1781.htm</p>		<p>6315780@N00/990866224</p>
	<p>Autoría: Desconocida. Licencia: Dominio público. Procedencia: http://www.public-domain-photos.com/free-cliparts/computer/applications/web-browser-1621.htm</p>		<p>Autoría: Desconocida. Licencia: Dominio público. Procedencia: http://www.public-domain-photos.com/free-cliparts/computer/applications/procman-1586.htm</p>
	<p>Autoría: David Boyle. Licencia: CC-BY-SA. Procedencia: http://www.flickr.com/photos/15513233@N00/330353975</p>		<p>Autoría: Rsms (Rasmus Andersson). Licencia: CC-BY-NC. Procedencia: http://www.flickr.com/photos/12281432@N00/376693138</p>
	<p>Autoría: opensourceway (opensource.com). Licencia: CC-BY-SA. Procedencia: http://www.flickr.com/photos/47691521@N07/4371001268</p>		<p>Autoría: Don Hankins. Licencia: CC-BY. Procedencia: http://www.flickr.com/photos/23905174@N00/1594411528</p>
	<p>Autoría: WebWizzard (Anthony Reeves). Licencia: CC-BY. Procedencia: http://www.flickr.com/photos/42623262@N03/3931165508</p>		<p>Autoría: hufse (Jon Moe). Licencia: CC-BY-NC-SA. Procedencia: http://www.flickr.com/photos/20771223@N00/15529699</p>
	<p>Autoría: Razza Mathadsa. Licencia: CC-BY. Procedencia: http://www.flickr.com/photos/60282136@N02/5539701673</p>		<p>Autoría: Desconocida. Licencia: Dominio público. Procedencia: http://www.public-domain-photos.com/free-cliparts/tools/weapons/shield_matt_todd_01-7449.htm</p>
	<p>Autoría: Avast Free Antivirus. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla de Avast Free Antivirus.</p>		<p>Autoría: Avast Free Antivirus. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla de Avast Free Antivirus.</p>
	<p>Autoría: Avast Free Antivirus. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla de Avast Free Antivirus.</p>		<p>Autoría: Avast Free Antivirus. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla de Avast Free Antivirus.</p>

	Autoría: Avast Free Antivirus. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla de Avast Free Antivirus.		Autoría: Avast Free Antivirus. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla de Avast Free Antivirus.
	Autoría: Avast Free Antivirus. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla de Avast Free Antivirus.		Autoría: Avast Free Antivirus. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla de Avast Free Antivirus.
	Autoría: Avast Free Antivirus. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla de Avast Free Antivirus.		Autoría: Avast Free Antivirus. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla de Avast Free Antivirus.
	Autoría: . Licencia: CC-BY-NC-SA. Procedencia: TechSoup for Libraries http://www.flickr.com/photos/9279573@N02/2590832103		Autoría: zstephen (Stephen Mackenzie). Licencia: CC-BY-NC-SA. Procedencia: http://www.flickr.com/photos/87463936@N00/399633721
	Autoría: Microsoft. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla de Windows 7.		Autoría: Microsoft. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla de Windows 7.
	Autoría: Microsoft. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla de Windows 7.		Autoría: Microsoft. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla de Windows 7.
	Autoría: Microsoft. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla de Windows 7.		Autoría: Microsoft. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla de Windows 7.
	Autoría: Microsoft. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla de Windows 7.		Autoría: Microsoft. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla de Windows 7.
	Autoría: Microsoft. Licencia: Copyright cita.		Autoría: Microsoft. Licencia: Copyright cita.

	<p>Procedencia: Elaboración Propia, captura de pantalla de Windows 7.</p>		<p>Procedencia: Elaboración Propia, captura de pantalla de Windows 7.</p>
	<p>Autoría: Microsoft. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla de Windows 7.</p>		<p>Autoría: Desconocida. Licencia: Dominio público. Procedencia: http://www.public-domain-photo.com/free-cliparts/tools/other/utensili_chiave_e_cacci_01-7410.htm</p>
	<p>Autoría: Comtrend. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla de interfaz de administración de Comtrend ADSL Router.</p>		<p>Autoría: Google y Comtrend. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla del buscador Google y de la interfaz de autenticación de Comtrend ADSL Router.</p>
	<p>Autoría: Desconocida. Licencia: Dominio público. Procedencia: http://www.public-domain-photo.com/free-cliparts/computer/mimetypes/encrypted-2223.htm</p>		<p>Autoría: Comtrend. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla de la interfaz de administración de Comtrend ADSL Router.</p>
	<p>Autoría: Microsoft. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla de Windows 7.</p>		<p>Autoría: Microsoft y Comtrend. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla del navegador MS Internet Explorer y de la interfaz de administración de Comtrend ADSL Router.</p>
	<p>Autoría: Microsoft. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla de una ventana de MS-DOS.</p>		<p>Autoría: Microsoft y Comtrend. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla del navegador MS Internet Explorer y de la interfaz de administración de Comtrend ADSL Router.</p>
	<p>Autoría: Microsoft. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla de Windows 7.</p>		<p>Autoría: Microsoft. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla de Windows 7.</p>
	<p>Autoría: Microsoft. Licencia: Copyright cita.</p>		<p>Autoría: Microsoft. Licencia: Copyright cita.</p>

			
	Autoría: Microsoft. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla de Windows 7.		Autoría: Microsoft. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla de Windows 7.
	Autoría: Xampp. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla de Xampp.		Autoría: Xampp. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla de Xampp.
	Autoría: Xampp. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla de Xampp.		Autoría: Xampp. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla de Xampp.
	Autoría: Xampp. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla de Xampp.		Autoría: Xampp. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla de Xampp.
	Autoría: Xampp. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla de Xampp.		Autoría: Xampp. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla de Xampp.
	Autoría: Xampp. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla de Xampp.		Autoría: Xampp. Licencia: Copyright cita. Procedencia: Elaboración Propia, captura de pantalla de Xampp.