2021

Francisco Javier

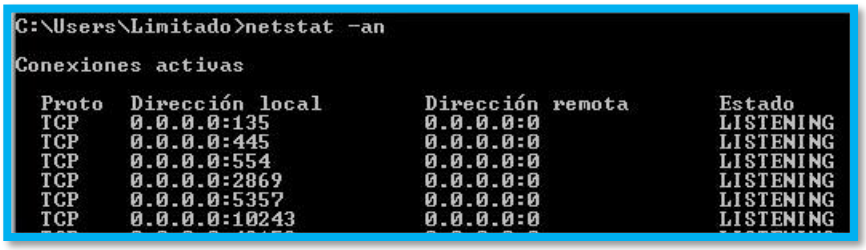
FRANCISCO JAVIER LÓPEZ CALDERÓN

PRACTICAS SEGURIDAD ACTIVA T_7

A partir de las explicaciones dadas en cada una de las prácticas siguientes, comprobad todos los apartados que se piden, capturando las imágenes necesarias, de forma que se demuestre de forma clara la comprensión de cada una de las actividades.

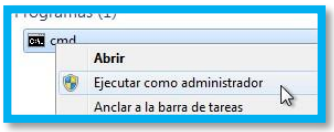
1. Ejecutar aplicación con **elevación de privilegios** en W7/W10.

- Crear una cuenta en W7 con un usuario con cuenta limitada (no administardor).
- Desde cmd. Introducimos **netstat –an** para ver todas las conexiones, se ejecuta con normalidad.

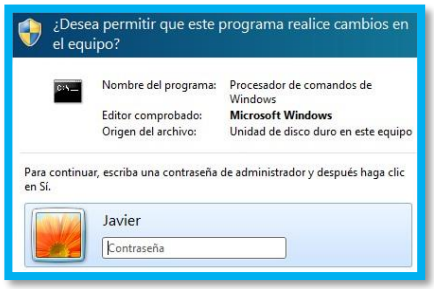


Pero si añadimos el parámetro b para mostrar el programa asociado a cada conexión, el sistema nos avisa de que necesitamos privilegios **Netstat –abn**

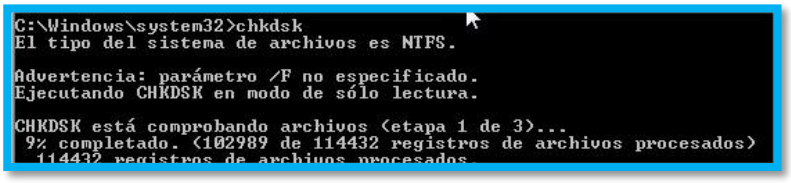
- Salimos de esa ventana y volvemos a lanzar la ventana de comandos, pero ahora no pulsamos directamente el botón derecho, para poder elegir Ejecutar como administrador



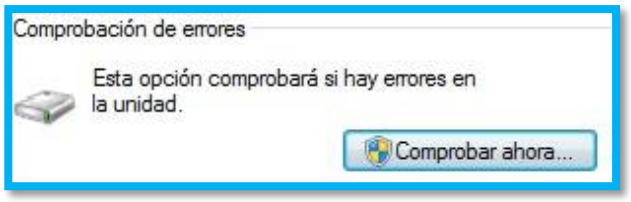
El sistema nos contesta solicitando una nueva autenticación para proceder a la ejecución. Nos ofrece el nombre de un usuario administrador y nos pregunta por su clave.



- Si se introduce correctamente, aparecerá la ventana de comandos y podremos ejecutar el comando netstat –abn y cualquier comando **chkdsk.**. Pero si cerramos esa ventana y la intentamos abrir de nuevo como administrador, nos pedirá de nuevo la contraseña.



- Este proceso se repite en cualquier menú o botón de Windows donde aparezca un escudo a la izquierda; indica que esa operación necesita elevación de privilegios. Por ejemplo, si abrimos el desfragmentador de disco (inicio>desfrag) la ventana se abre, pero cualquier operación posterior solicitará elevación.

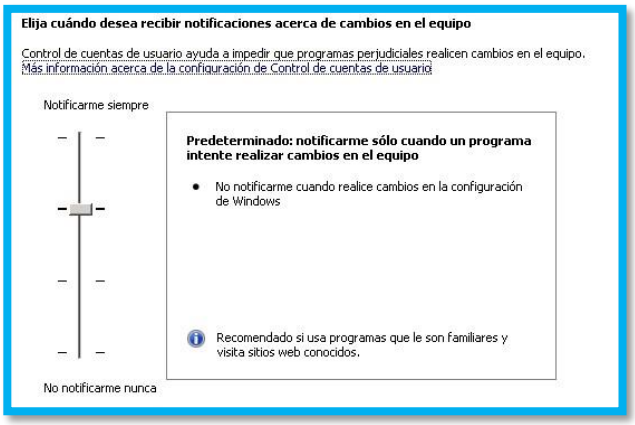


- Salgamos del usuario con cuenta limitada y entrar como usuario administrador. Podemos repetir los pasos anteriores y la única diferencia es que ya no nos pregunta por la contraseña. Simplemente nos avisa de que vamos a realizar algo potencialmente peligroso.

Al ser administrador no se nos pedirá la contraseña del administrador, aunque, para algunas acciones se nos pedirá dar a “aceptar”

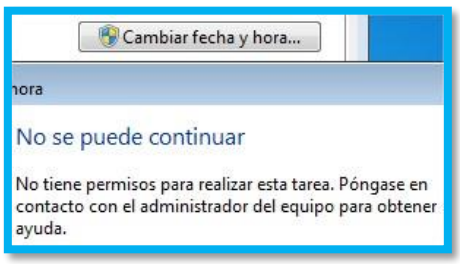
2. Configuración del UAC en W7

- Entramos en W7/w10 como administrador y comprobamos como está la configuración del UAC. Desde inicio buscamos UAC y ejecutamos el programa que nos ofrece.
  Configuración de Control de cuentas del usuario



En la ventana anterior vemos que hay una escala. Esta escala va desde notificame siempre hasta no notificar nunca. El valor por defecto es notificame siempre, porque permite operaciones sencillas, como cambiar la hora.
Si lo ponemos en notificame siempre y veremos que, tras cerrar la ventana, el cambio de hora nos pide confirmación.

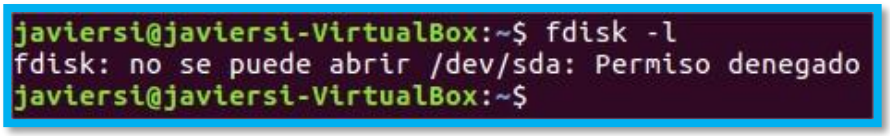
- Podemos probar a bajarlo hasta no notificarme nunca y comprobar que, después de reiniciar la máquina, el cambio de hora ya no pide confirmación.



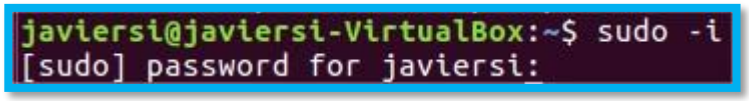
- Aunque no pide confirmación, no quiere decir que ya no sea una operación privilegiada. Si entramos con el usuario no administrador, seguimos sin poder cambiar la hora (con la diferencia de que ni siquiera nos ofrece la elevación de privilegios)

3. Elevación de privilegios en Linux

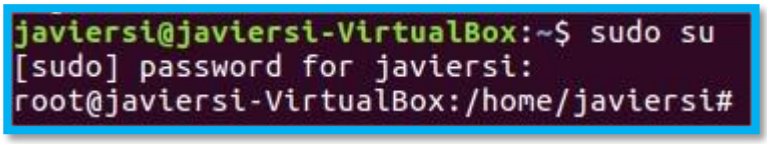
- Entramos en el sistema con un usuario registrado. abrimos una Shell y ejecutamos el comando fdisk –l /dev/sda. Nos aparece un mensaje de error porque no tenemos privilegios.



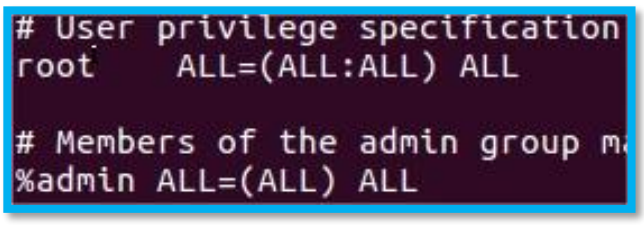
- Ejecutamos el comando sudo –i. Nos pedirá la contraseña. Si la introducimos correctamente, estaremos ejecutando una nueva Shell con permisos de administrador. Ahora si funciona el comando anterior funciona.



- El comando sudo permite ejecutar con privilegios el comando que pongamos a continuación (por ejemplo: **sudo fdisk –l /dev/sda**). Si vamos a ejecutar varios comandos, es más cómodo utilizar sudo –i



- Esto ha funcionado porque nuestro usuario cumple alguna de las condiciones que figuran en **el fichero /etc/sudoers**. En este fichero se pueden establecer limitaciones para un usuario concreto y para un grupo de usuarios. Las limitaciones pueden ser comandos concretos a todos. En nuestro caso se ha aplicado que nuestro usuario pertenece al grupo sudo, y este grupo tiene todos los comandos disponibles. En el fichero aparece esta línea
  %sudo ALL= (ALL : ALL) ALL.
  %sudo ALL= (ALL) ALLsudo usu



Gedit /etc/sudoers=➔ vemos el contenido

- Vamos a crear un usuario nuevo llamado limitado. Lo podemos hacer desde la misma ventana donde tenemos sudo –i con los comandos:
  Crear usuario desde entorno gráfico si da problemas
  #adduser limitado
  #passwd limitado

```
root@javiersi-VirtualBox:/etc# adduser limitado
Añadiendo el usuario `limitado' ...
Añadiendo el nuevo grupo `limitado' (1001) ...
```

- Si entramos en el sistema con el nuevo usuario e intentamos **fdisk –l /dev/sda**, fallará. Pero si intentamos **sudo –i,** no solo falla, sino que advierte de que avisará al administrador.

```
limitado@javiersi-VirtualBox:/$ fdisk -l
fdisk: no se puede abrir /dev/sr0: Permiso denegado
fdisk: no se puede abrir /dev/sda: Permiso denegado
```

```
limitado@javiersi-VirtualBox:/$ sudo fdisk -l /dev/sda
[sudo] password for limitado:
limitado no está en el archivo sudoers. Se informará de este incidente.
```

- Si volvemos a la sesión con privilegios y vemos las últimas líneas del **fichero /var/log/auth.log**, ahí aparecerá el intento fallido, junto con la fecha y la hora en la que lo hemos hecho. Ultiliza gedit para visualizar el fichero.

```
Feb 14 00:38:24 javiersi-VirtualBox sudo: limitado : user NOT in sudoer
s ; TTY=pts/6 ; PWD=/ ; USER=root ; COMMAND=/bin/su
Feb 14 00:38:38 javiersi-VirtualBox sudo: limitado : user NOT in sudoer
s ; TTY=pts/6 ; PWD=/ ; USER=root ; COMMAND=/sbin/fdisk -l /dev/sda
Feb 14 00:39:33 javiersi-VirtualBox su[6438]: pam_unix(su:session): ses
sion closed for user limitado
```

- Podemos permitir que el usuario limitado pueda hacer sudo solo con incluirlo en el grupo sudo. Por ejemplo, en la sesión de administrador ejecutamos el comando:
  #usermod –G sudo limitado
  La próxima vez que limitado entre al sistema ya podrá utilizar el mecanismo sudo

```
limitado@javiersi-VirtualBox:/$ sudo fdisk -l
Disk /dev/sda: 30 GiB, 32212254720 bytes, 62914560 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
```

4. Descarga el programa DiskCryptor instálalo en una M.V. Realizar la practica guiada del libro. **(pag 112 libro).CONSIDERAR VERSIONES ACTUALES.**

Queda como investigación por parte del alumno la utilización de otro programa diferente si así lo considera, que permita encriptar. En dicha práctica se deben poner las capturas de pantalla explicando su funcionamiento.

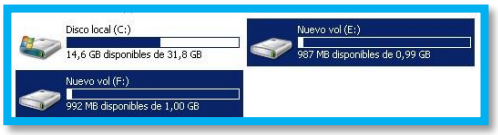
Otra herramienta utilizada en el ámbito empresarial es **BitLocker**

- Recordar que cuando añadimos el disco aparece un asistente para inicializar y convertir discos.
  - Cifrar una partición en Windows
  - El objetivo es proteger una partición de Windows para que la información no sea accesible para las personas que no conozcan la clave.
  - Para ello utilizaremos un programa de código abierto: DiskCryptor .

Para hacer la práctica vamos a seguir los siguientes pasos:

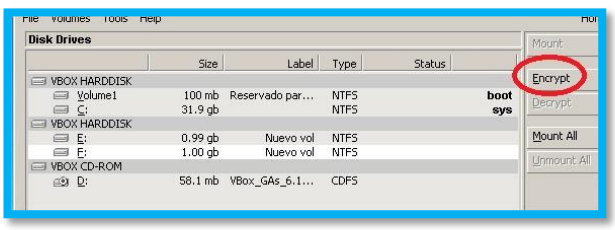
a. Añadir a la MV un nuevo disco duro de 2 Gb.

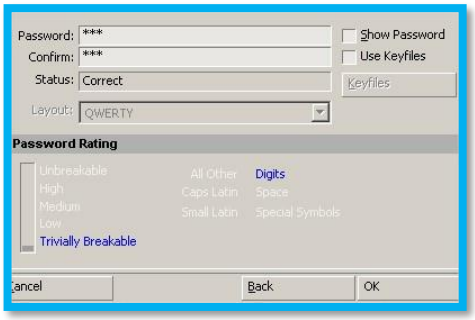
b. Hacer dos particiones de 1 Gb cada una.



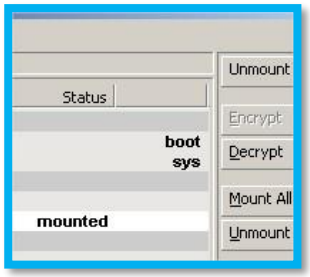
c. En una de ellas crear un fichero de texto

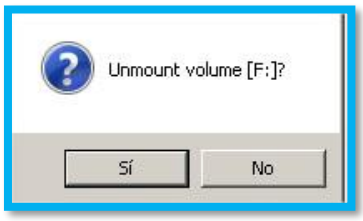
d. Encriptar con el programa DiskCryptor la partición donde está el fichero





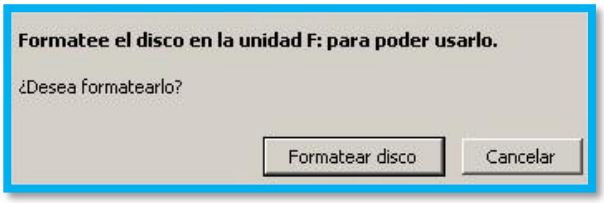
e. Comprobar que la partición está “montada” hay que quitar esta opción.





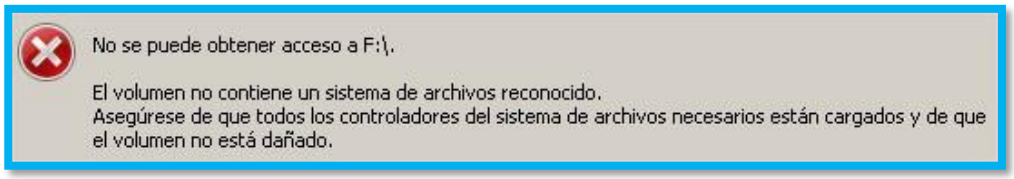
f. Comprobar el acceso a la partición encriptada y a su contenido. ¿Es lógico?

No se tiene acceso a la unidad desmontada



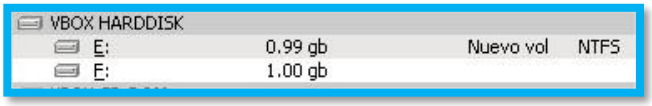
g. Reinicia el equipo

h. Comprobar el acceso a la partición encriptada y a su contenido. ¿Qué pasa?



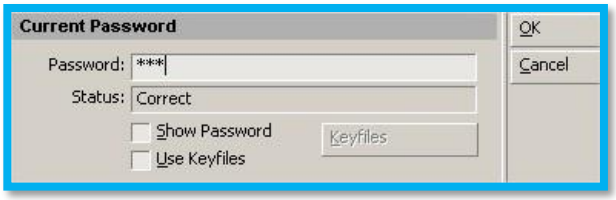
i. Abre el programa DiskCryptor. ¿Cuál es el estado de las particiones?

La partición encriptada se encuentra desmontada, ese sería su estado



j. ¿Qué puedes hacer para acceder a la partición encriptada?

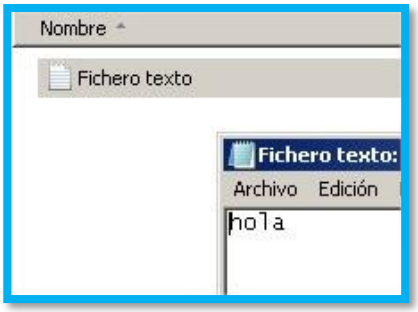
Se puede montar de nuevo la unidad.



k. Haz que otra MV de Windows acceda al disco duro con el que has trabajado hasta ahora. ¿A qué tienes acceso?, ¿bajo qué condicionantes? Comprobar la solución dada en este apartado

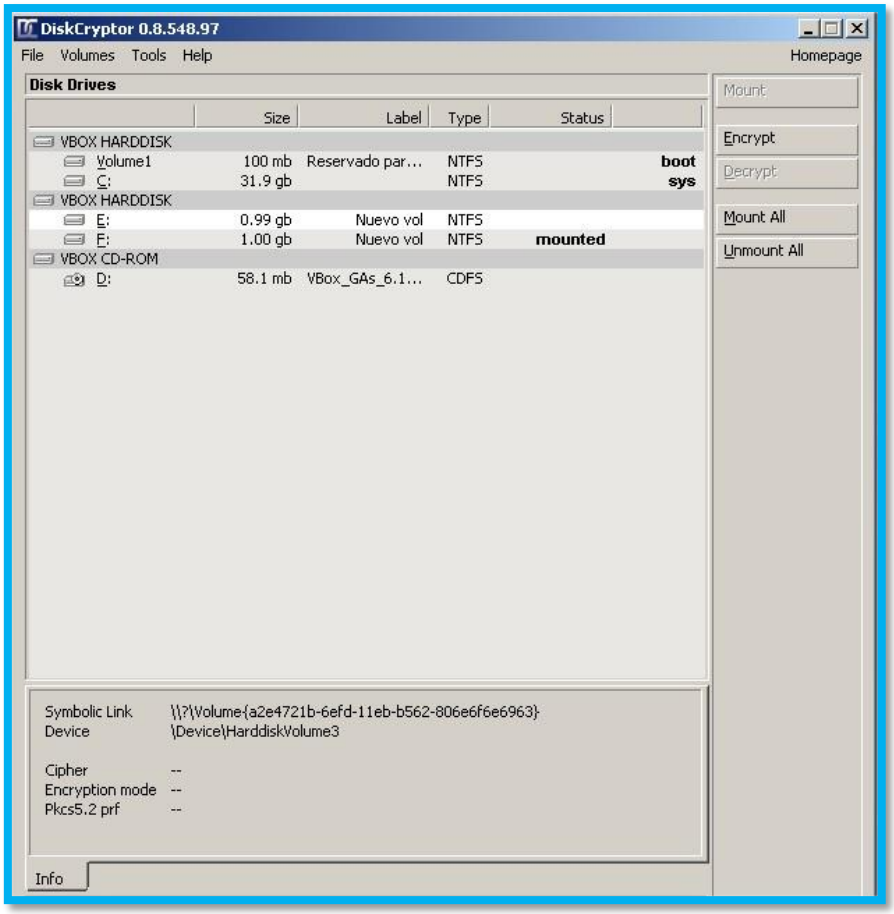
Sin el programa Diskcryptor es imposible acceder a la unidad, puedes formatearla.

Instalando el programa se puede acceder a las unidades, pero, se requiere la contraseña



l. Anota las conclusiones del funcionamiento de este programa

Es un programa muy interesante ya que nos permite cifrar particiones para mejorar su seguridad, un dato importante es que puedes "trasladar" una unidad a otro equipo que utilice Diskcryptor como hemos podido comprobar, utilizando una contraseña común, podemos acceder a esos datos.



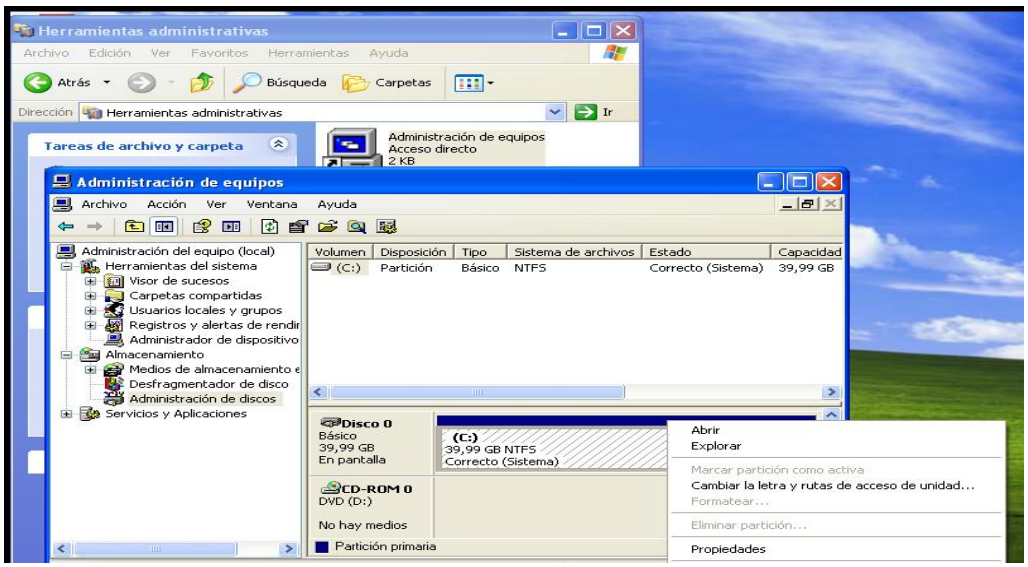
5. Cuotas de disco. Practica cuotas de disco en w7/W10 ACTUALIZAR INFORMACIÓN y las imágenes EN S.O. ACTUALES

La mayoría de los sistemas operativos poseen mecanismos para impedir que ciertos usuarios hagan un uso indebido de la capacidad del disco, y así evitar la ralentización del equipo por saturación del sistema de ficheros y el perjuicio al resto de los usuarios al limitarles el espacio en el disco.

Las cuotas de disco sólo pueden establecerlas los miembros del grupo Administradores en volúmenes con formato del sistema de archivos NTFS. Por tanto, la ficha Cuota no aparece si no pertenece al grupo Administradores, si el volumen no está compartido desde el directorio raíz del volumen o si el volumen no tiene formato NTFS.

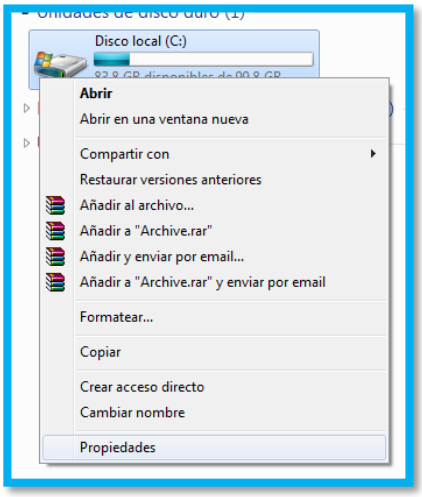
Activación y uso de cuotas de disco en Windows

Inicio/Panel de control/herramientas Administrativas/Administración de equipos/Administración de discos

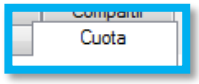


Para activar las cuotas de disco en una partición en Windows debemos seguir los siguientes pasos:

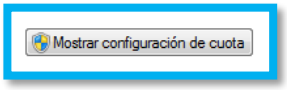
1. Haga clic con el botón secundario del ratón en el volumen para el que desee habilitar cuotas de disco y, a continuación, haga clic en **Propiedades**.



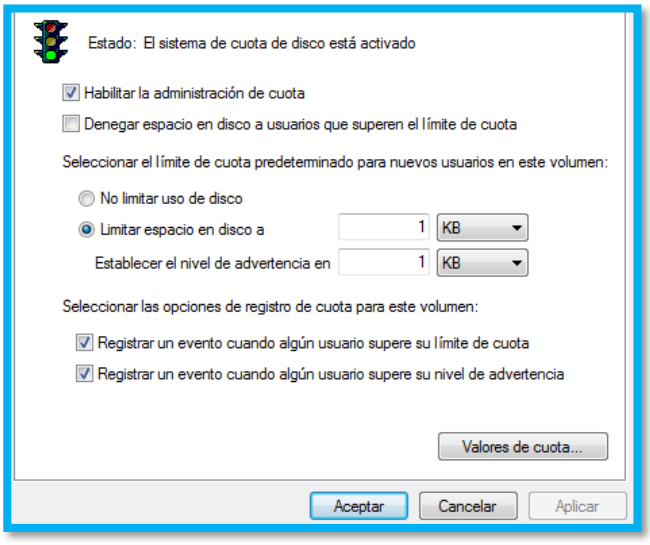
2. En el cuadro de diálogo **Propiedades**, haga clic en la ficha Cuota.



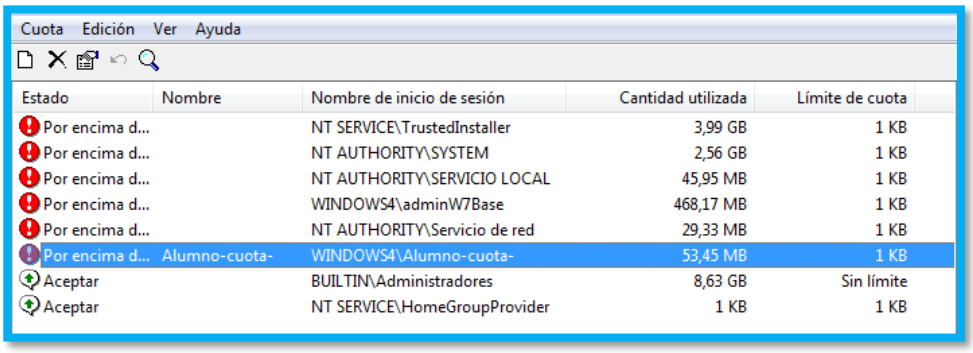
3. En la ficha **Cuota**, active la casilla de verificación **Habilitar la administración de cuota**.



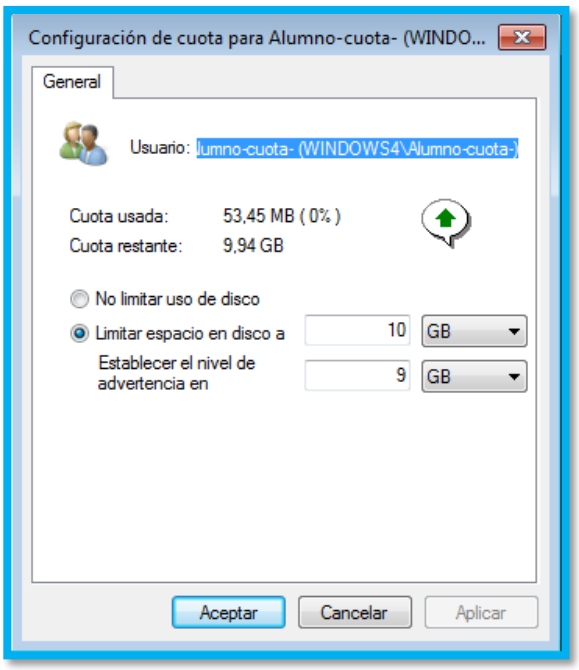
4. Seleccione una o varias de las siguientes opciones y, después, haga clic en **Aceptar**.



- Si lo que se desea es crear una cuota de disco personalizada se deberá seleccionar las dos primeras opciones y pulsar sobre el botón “Valores de cuota” para seleccionar el usuario concreto del sistema y limitar su acceso a disco.



De esta forma se creará una entrada de datos con el nuevo usuario al que se ha limitado una cuota y las características de éstas.



- **Denegar espacio de disco a los usuarios que sobrepasen su límite de cuota**

Los usuarios que sobrepasen el límite de sus cuotas recibirán un mensaje de error, indicando que no hay espacio suficiente en el disco, de Windows y no podrán escribir más datos en el volumen si no eliminan o mueven antes uno o varios archivos.

Cada programa trata este error de un modo específico. Para el programa, será como si el volumen estuviera lleno. Si desactiva esta casilla de verificación, los usuarios pueden sobrepasar el límite de cuota. Puede ser útil habilitar cuotas y no limitar el uso del espacio de disco cuando no se desea denegar a los usuarios el acceso a un volumen, pero sí realizar un seguimiento del uso del espacio de disco por parte de cada usuario. También puede especificar si debe registrarse o no un suceso cuando los usuarios superen su nivel de advertencia de cuota o su límite de cuota.

- **Limitar espacio de disco a**

Escriba la cantidad de espacio de disco que pueden utilizar a los nuevos usuarios del volumen y la cantidad de espacio de disco que debe utilizarse para que se escriba un suceso en el registro del sistema. Los administradores pueden ver estos sucesos en el Visor de sucesos. Es posible utilizar valores decimales (por ejemplo, 20.5). Por lo que se refiere a los niveles de espacio de disco y advertencia, seleccione las unidades apropiadas en la lista desplegable (por ejemplo, KB, MB, GB). Para obtener más información acerca del Visor de sucesos, consulte los Temas relacionados.

- **Registrar suceso cuando un usuario exceda su límite de cuota**

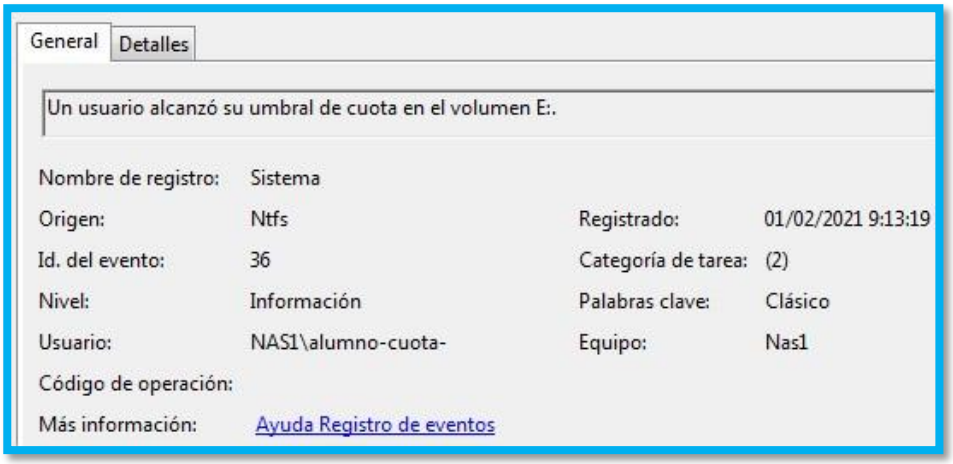
Si se han habilitado las cuotas, se escribe un suceso en el registro de sistema del equipo local cada vez que un usuario sobrepasa su límite de cuota. Los administradores pueden ver estos sucesos en el Visor de sucesos si aplican el filtro de sucesos de disco.

De forma predeterminada, los sucesos de cuota se escriben cada hora en el registro del sistema del equipo local.

Registrar suceso cuando un usuario exceda su nivel de advertencia

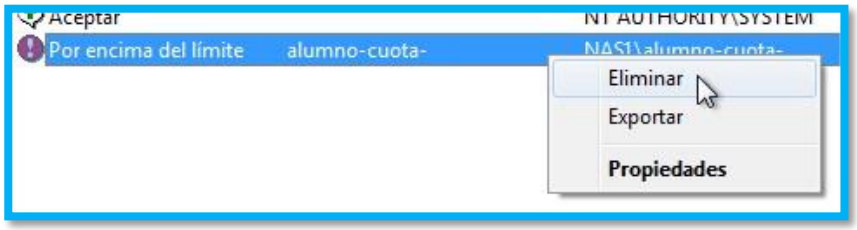
Si se han habilitado las cuotas, se escribe un suceso en el registro de sistema del equipo local cada vez que un usuario sobrepasa su nivel de advertencia.

- El usuario puede ver mediante el visor de sucesos dicha información.

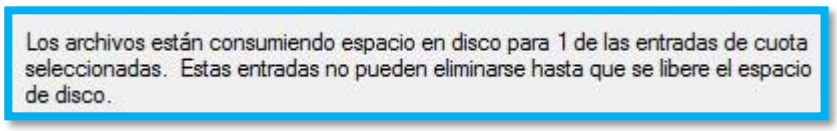


Eliminar una cuota personalizada

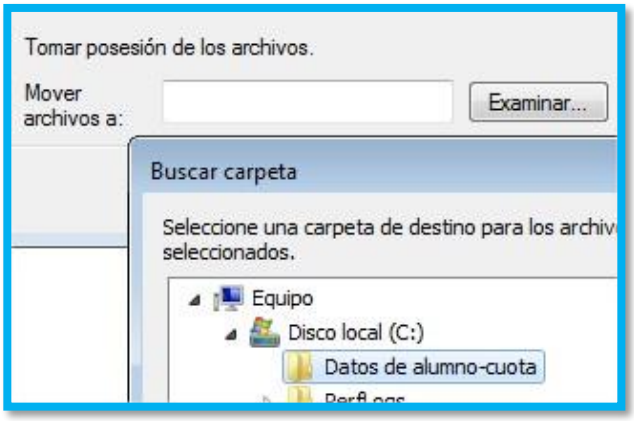
Si desea eliminar una entrada de cuota, lo primero que debe hacer es eliminar todos los archivos de ese usuario en el volumen en que quiere eliminar la entrada de cuota o en su defecto cambiarles el propietario a los archivos.



No podemos eliminar la cuota hasta que movamos los archivos del usuario o los borremos



Podemos mover los archivos desde la cuenta "administrador" en este caos los moveremos a la carpeta "Datos de alumno cuota" en C:



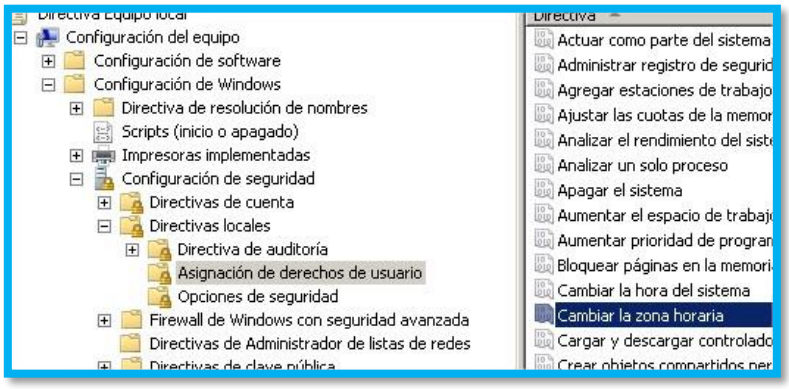
Otra opción es "tomar" los archivos como propios del usuario administrador

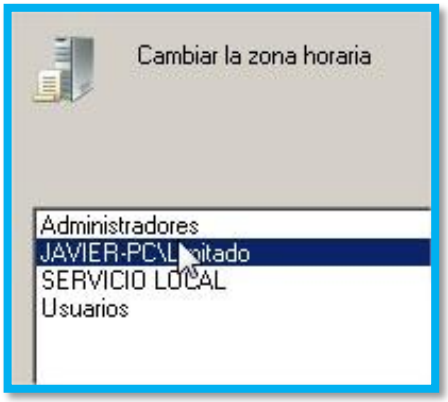
Cómo ultima opción, podemos eliminar los archivos

6. Suponiendo que tenemos un usuario Administrador, crear un usuario con cuenta limitada.

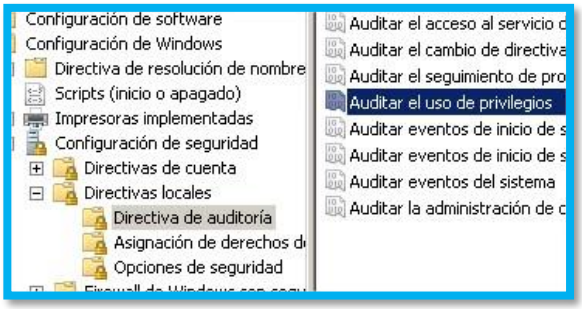
Desde un usuario con rol administrador, agregar la posibilidad a la cuenta limitada creada anteriormente de cambiar:

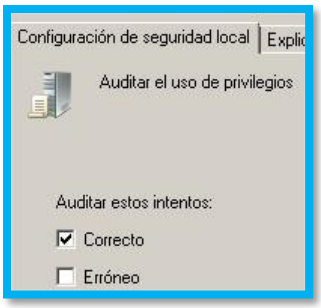
- La fecha/hora.





- Activar el archivo de sucesos o *log* de sucesos asociados a esos privilegios.





Acceder como usuario rol-limitado y verificar privilegios y limitaciones. Acceder como usuario rol-administrador y verificar el archivo de suceso o log.

¿Los usuarios con cuenta limitada pueden acceder a la configuración de directivas locales? ¿Es lógico?