Cifrado de datos y particiones en Windows

Cifrado de datos y particiones

La confidencialidad de los datos almacenados en una unidad es fundamental. Windows originalmente integraba un sistema de encriptación denominado EFS, que aportaba seguridad en el acceso sólo permitiéndoselo al usuario que realizaba la operación.

En este caso iremos un paso más adelante y veremos una aplicación para cifrar y ocultar en el ordenador datos que el usuario considere reservados o confidenciales.

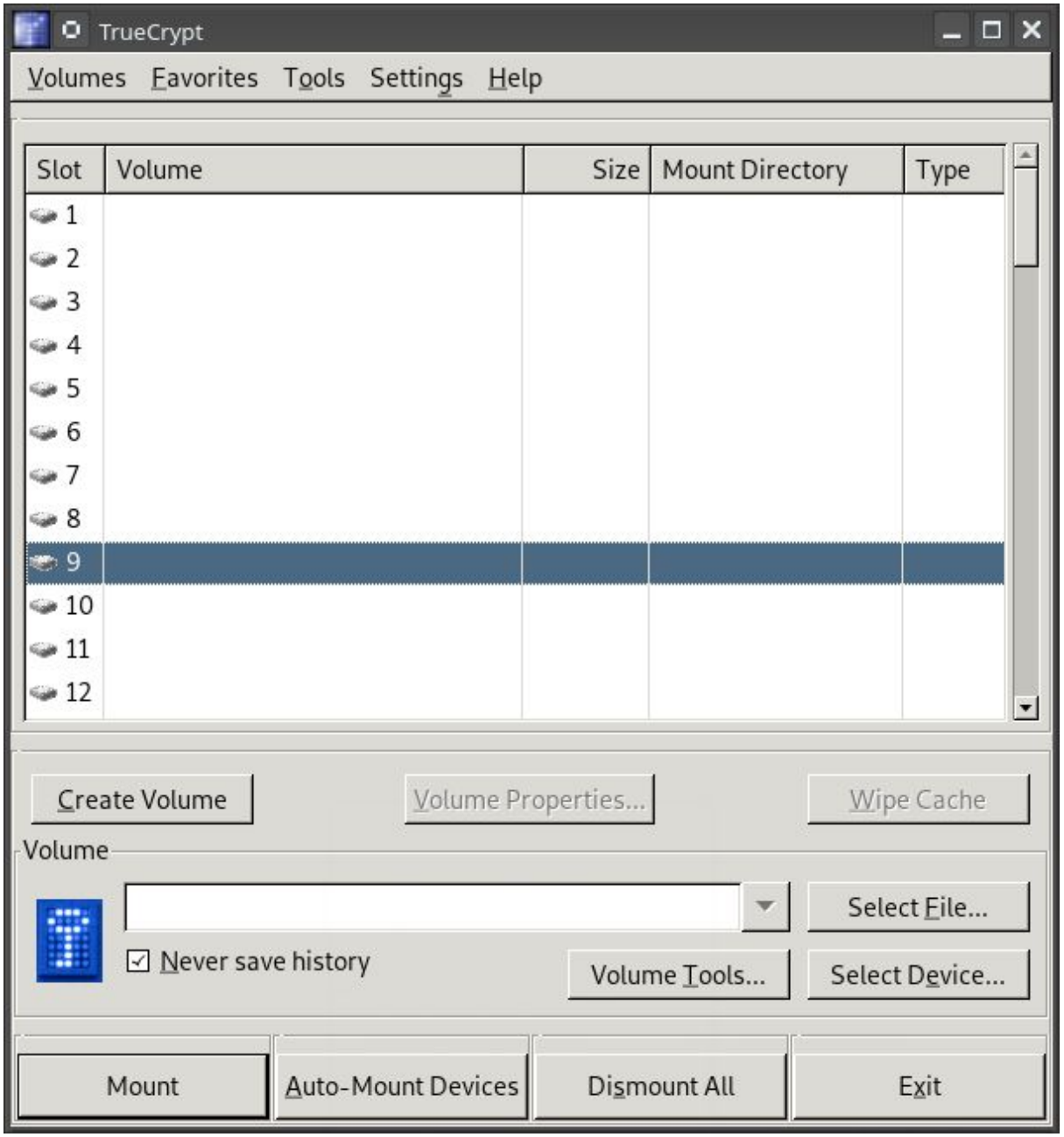
TrueCrypt

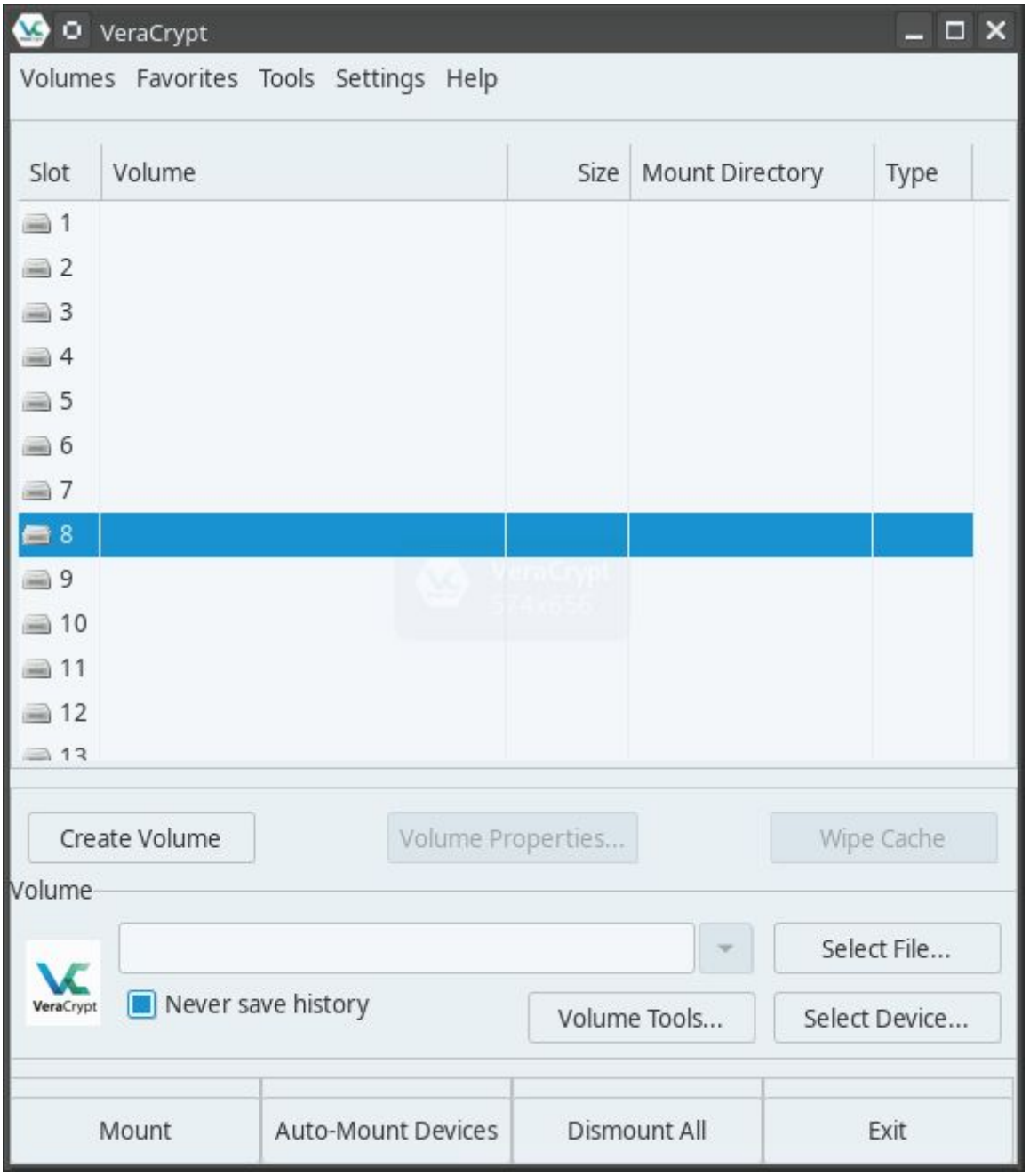
TrueCrypt ofrece la posibilidad de crear discos virtuales o aprovechar una partición ya existente para guardar ficheros cifrados, pudiendo escoger entre varios algoritmos de cifrado, como AES, Serpent o Twofish, y determinar de qué capacidad será la unidad virtual. Allí podremos guardar cualquier documento de forma segura y cómoda.

Se integra con el explorador de archivos que usemos, es fácil de usar, permitiendo crear hasta 32 unidades diferentes. Existen versiones para sistemas operativos Windows, Mac OS X, y GNU/Linux.

Como veréis en su web, se supone que está considerada como obsoleta y recomienda usar BitLocker. La polémica es que últimamente está bajo sospecha ya que se piensa que quizás su desarrollo se abandonó no por insegura, sino por todo lo contrario. Recientemente ha salido la noticia en España de las dificultades que tiene el CNI para descifrar los discos duros incautados al ex-comisario José Villarejo. En vez de usar TrueCrypt, también podés usar VeraCrypt, que es un sucesor libre de TrueCrypt. Es casi idéntico.

1. Descargaremos la aplicación (la descarga está al final de la página) y la instalaremos.


TrueCrypt
Volumes Favorites Tools Settings Help
Slot Volume Size Mount Directory Type
1
2
3
4
5
6
7
8
9
10
11
12
Create Volume
Volume Properties...
Wipe Cache
Volume
Select File...
Never save history
Volume Tools...
Select Device...
Mount
Auto-Mount Devices
Dismount All
Exit

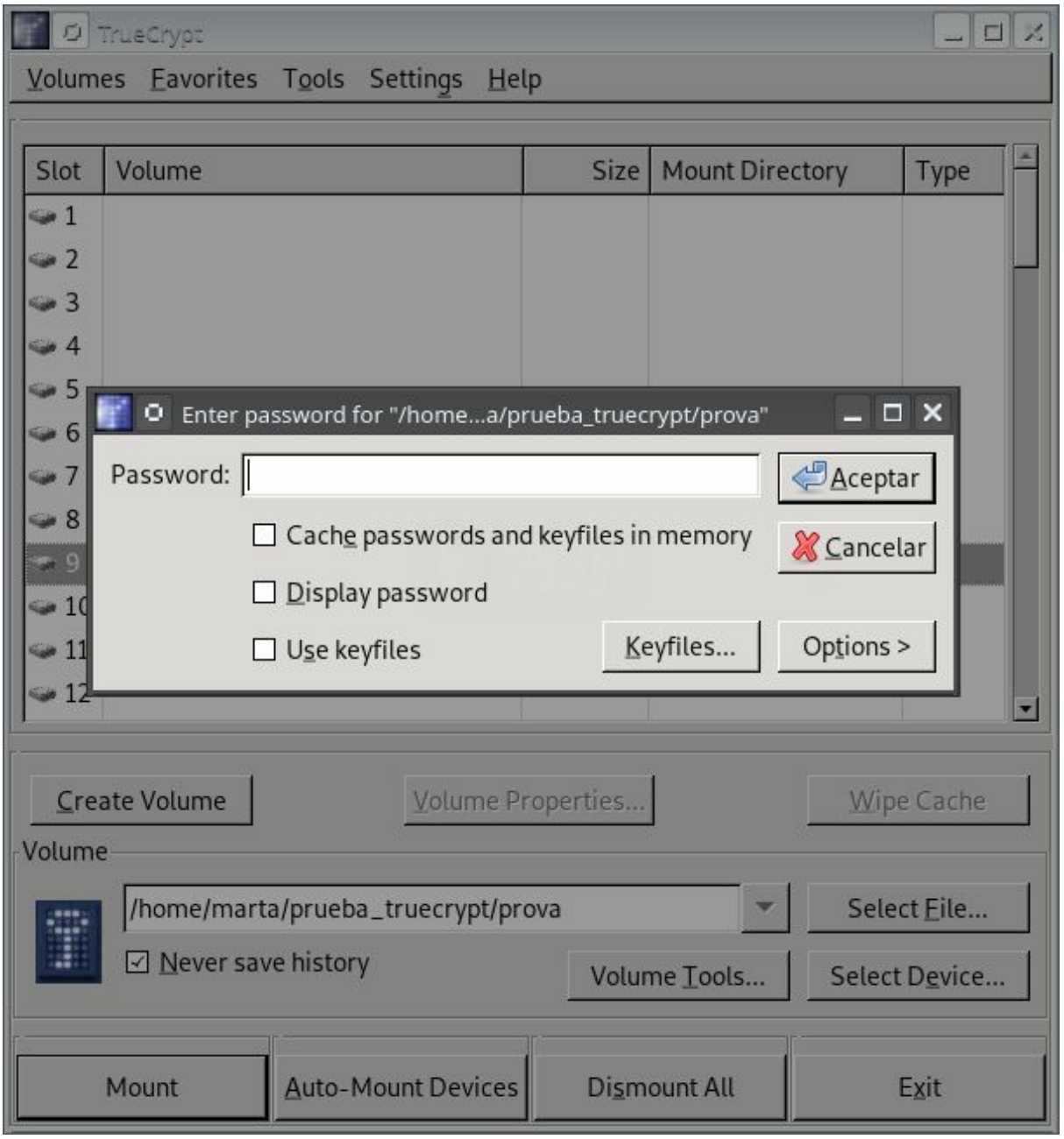


2. A continuación podremos crear un volumen normal (botón “Create Volume”), seleccionamos la opción en un archivo, que se creará en la ubicación que seleccionemos (indicaremos un nombre por ejemplo volumen_cifrado). Entre las opciones de encriptación podremos seleccionar entre diferentes algoritmos pudiendo ver una tabla comparativa con rendimientos en procesos de encriptación y desencriptación.

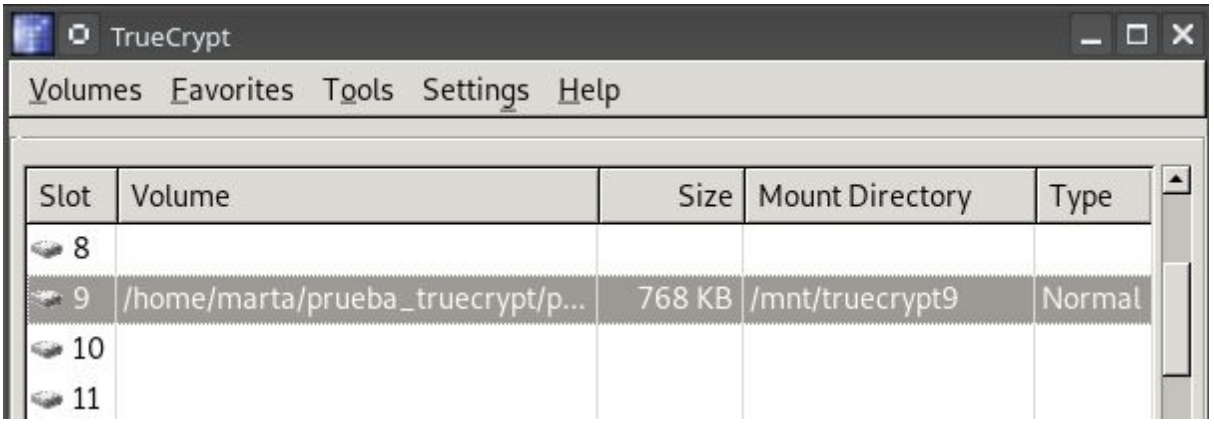
Una vez seleccionado, elegimos el tamaño de tu volumen cifrado y añadiremos una contraseña lo más segura posible.

Seleccionamos el sistema de ficheros (por ejemplo: NTFS por defecto) y nos indicará a continuación que el volumen ha sido creado.

3. Para utilizarlo debemos montar una unidad con el archivo creado. Seleccionamos una unidad disponible, por ejemplo K, y pulsaremos el botón Seleccionar archivo, donde navegaremos hasta la ruta del archivo creado para el volumen encriptado. Pulsaremos Montar y se nos pedirá nuestra contraseña:



Haciendo doble clic sobre la unidad accederemos a nuestro volumen cifrado.



Cualquier fichero que arrastremos hacia la unidad se guardará cifrado de forma transparente, y sin necesidad de que teclees de nuevo la contraseña (solo se te pide cuando montas la unidad). Puedes utilizar tu volumen cifrado TrueCrypt como otra unidad más de disco. Por último no olvidemos desmontar el volumen, pulsaremos el botón Desmontar.

Es recomendable realizar copia de seguridad del archivo ya que en caso de borrarlo perderemos la información contenida en él.

Haced pruebas y verificad que funciona correctamente y que es necesaria la clave para acceder al contenido. Podéis instalarlo también en Mac o Linux como he hecho yo.

BitLocker

Ya sabéis que desde Mayo de 2014 no se recomienda el uso de TrueCrypt debido a vulnerabilidades encontradas y se recomienda el uso de BitLocker que es una características aparecida a partir de Windows 7 en sus versiones Ultimate o

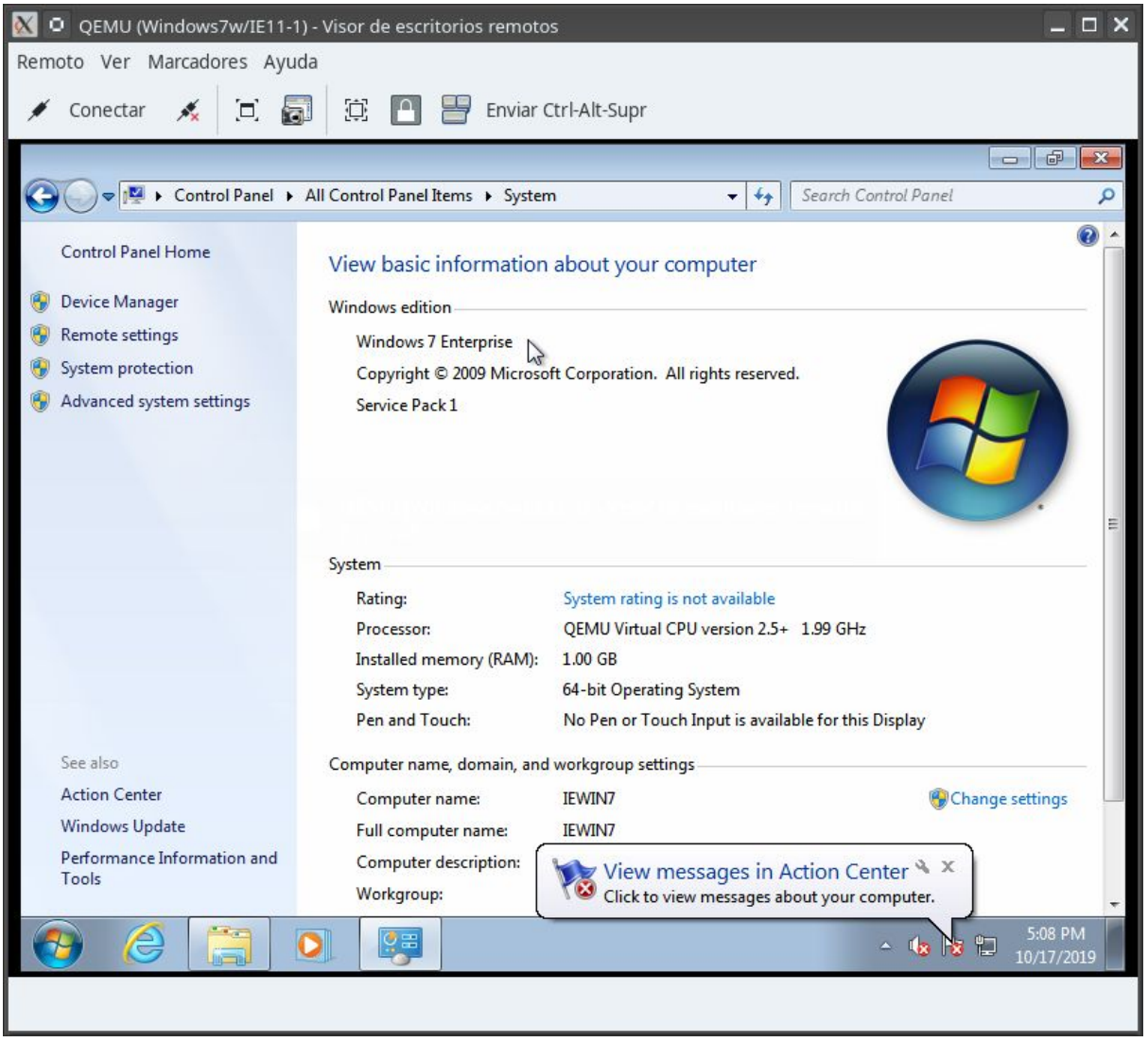
Enterprise.

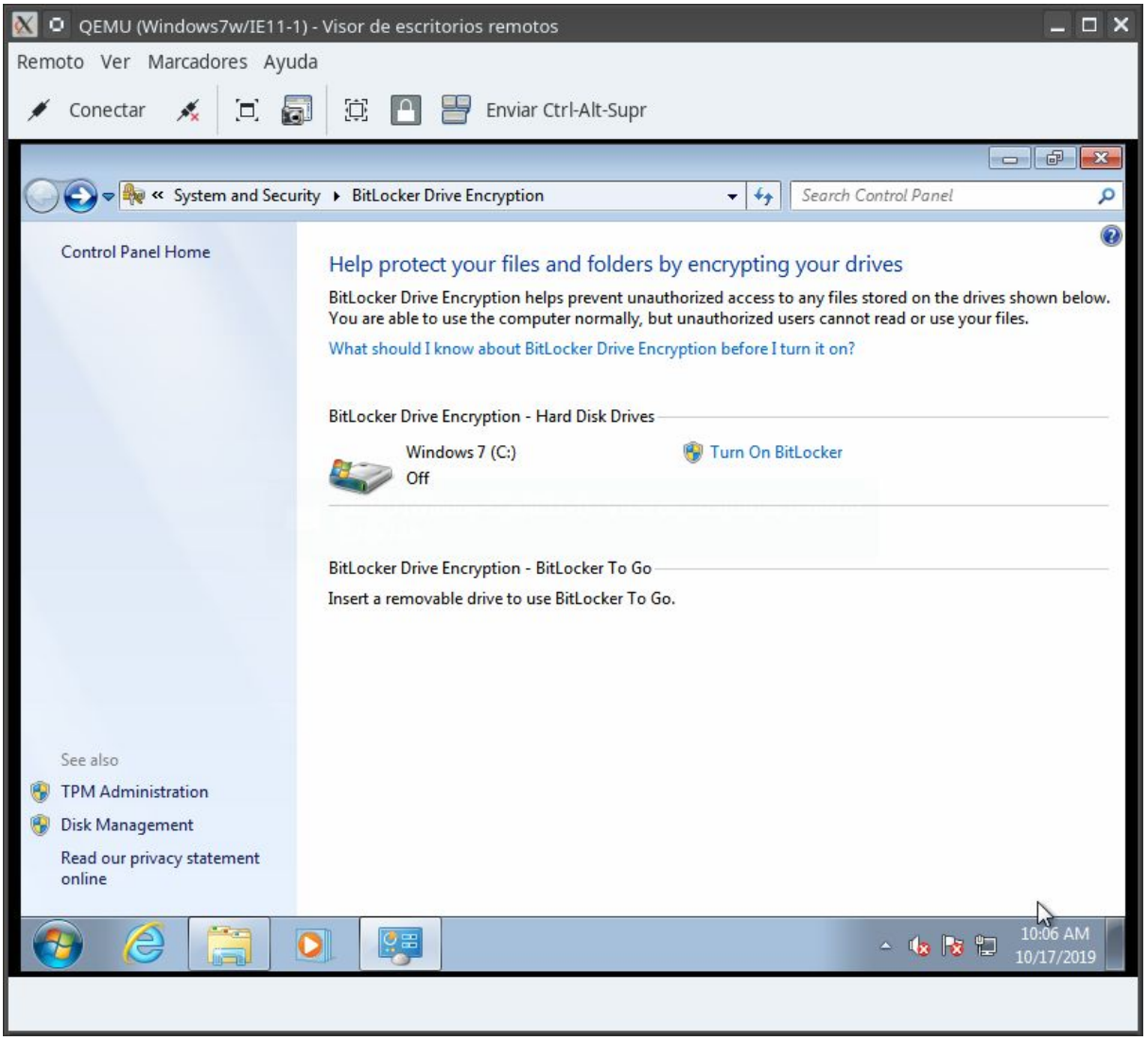
Vais a usar BitLocker para cifrar una partición de datos. También tenéis que aprender cómo descifrar la unidad.

Se puede cambiar el método de cifrado y su intensidad. Más información en el siguiente enlace.

Se recomienda usar una máquina virtual. Puede serte más fácil crear otro disco duro virtual en vez de una partición, para la práctica será indiferente.

Desde aquí podéis descargar Máquinas Virtuales de Microsoft que os pueden servir:





Documentad como de costumbre, con capturas de pantalla lo más claras posibles. Haced todo tipo de pruebas.