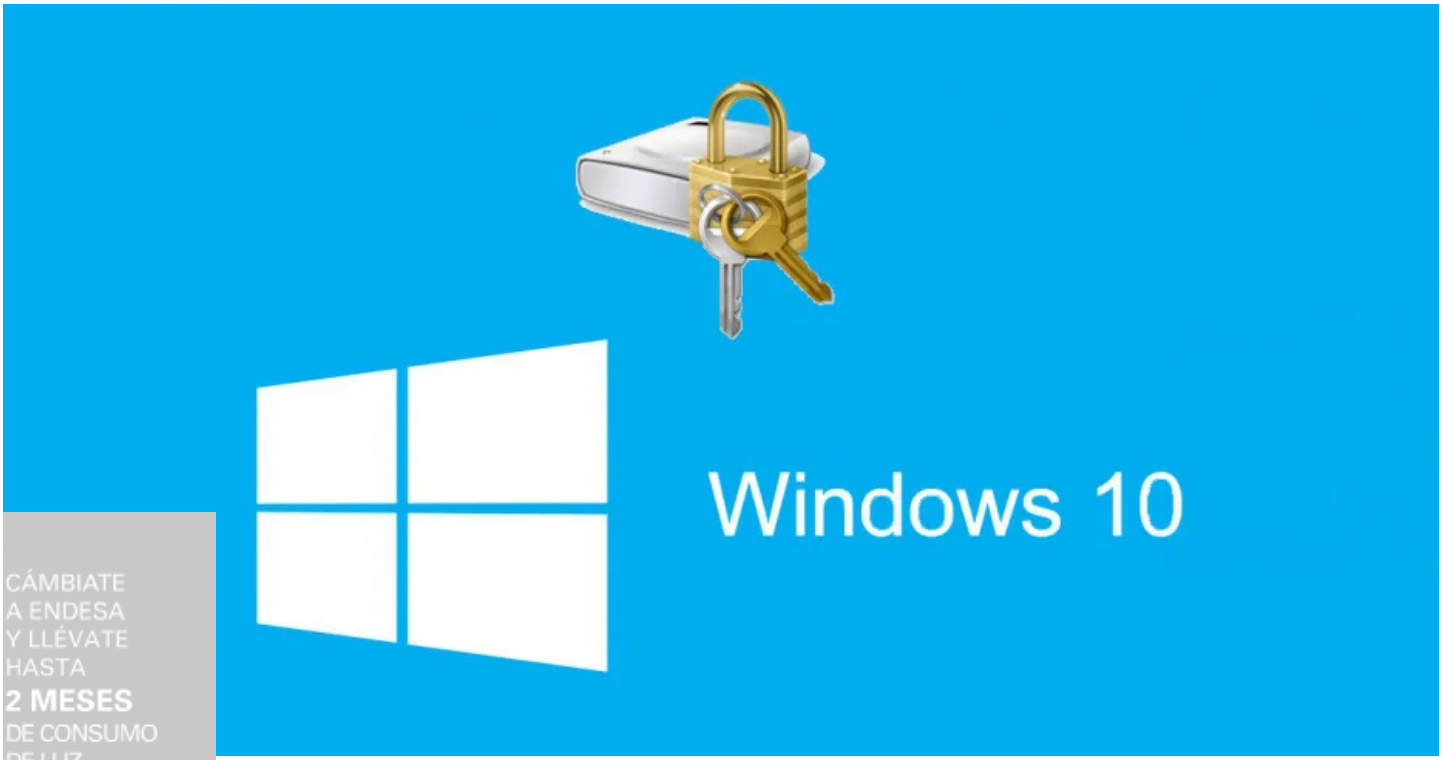
BitLocker: Tutorial completo para cifrar discos en Windows



CÁMBIATE
A ENDESA
Y LLÉVATE
HASTA
2 MESES
DE CONSUMO
DE LUZ
GRATIS
Y 1 AÑO DE
amazon prime
¡DE REGALO!
*Ver condiciones.
SABER MÁS
What's your power?
endesa

ente consideramos que los datos contenidos en los discos duros de ordenadores se encuentran protegidos por la contraseña de inicio de to es así hasta cierto punto, pero ¿qué ocurre si nos dejamos una sesión si perdemos o nos roban el ordenador o nuestro disco duro? Los datos os en los discos duros están a disposición de cualquier persona, bastaría disco duro de un ordenador y conectarlo a otro mediante un adaptador a USB, y tendríamos acceso a toda la información contenida en los Es decir, el sistema operativo protege el contenido de nuestros discos está funcionando, pero no cuando el ordenador está apagado o l proceso de arranque. Hoy en RedesZone os vamos a hablar sobre , la herramienta de Microsoft para Windows que nos permitirá cifrar estros datos.

BitLocker es una herramienta ofrecida por Microsoft en las versiones Profesional y Enterprise de su sistema operativo Windows y que permite cifrar el contenido de los discos duros internos, discos de arranque, discos externos y también los pendrives que conectemos a nuestro ordenador. De esta forma, aunque los conectemos a otro orden

BitLocker: Tutorial completo para cifrar discos en Windows

Índice:

1. ¿En qué consiste cifrar una unidad de almacenamiento?
2. Cómo modificar el método y la intensidad (seguridad) del cifrado mediante directivas de grupo en BitLocker
3. Activación de BitLocker en una unidad de almacenamiento interno
4. Realizar copia de seguridad de la clave de recuperación
5. Seleccionar cantidad de disco a cifrar
6. Configuración de BitLocker en unidades cifradas
7. BitLocker en unidades de disco del sistema operativo
8. BitLocker en unidades de almacenamiento externas o extraíbles
9. Procedimiento para utilizar BitLocker sin TPM
10. Procedimiento de desbloqueo de unidad de BitLocker con clave de recuperación
11. Acceso con escritorio remoto a unidades cifradas
12. Abrir unidades cifradas con BitLocker en Windows XP o Vista

1. ¿En qué consiste cifrar una unidad de almacenamiento?

El cifrado es un procedimiento por el cual mediante un algoritmo de cifrado y una clave determinada hace ilegible e incomprensible un mensaje a cualquier persona que no disponga de la clave. Esto se puede aplicar igualmente a los datos guardados en unidades de disco y memorias flash.

Esta herramienta permite cifrar el contenido de unidades de almacenamiento completas, para ello en su versión inicial utiliza el algoritmo de **cifrado estándar AES**, (Advanced Encryption Standard) con una clave de 128 bits que **puede ser cambiado a AES-256 usando las directivas de grupo**. En su última versión, Windows 10 incorpora el cifrado XTS-AES mucho más seguro.

Al cifrar el disco, tendremos que escribir una contraseña para proteger la información cifrada. No debemos perder ni olvidar esta contraseña pues tendríamos que utilizar la clave recuperación de cifrado de unidad o no podríamos volver a tener acceso a los datos. Cuando guardamos o copiamos un fichero a un disco cifrado, este se cifra automáticamente. Cuando copiamos o abrimos un fichero de un disco cifrado, este se descifra automáticamente.

2. Cómo modificar el método y la intensidad (seguridad) del cifrado mediante directivas de grupo en BitLocker

cifrado AES-CBC con una clave de 128 bits para las unidades externas y memorias flash USB. La diferencia entre estos dos métodos de cifrado XTX-AES y AES-CBC está en la forma en la que realizan el cifrado, su seguridad frente a ataques y en la rapidez con la que cifran y descifran datos.

- XTS-AES es el algoritmo de cifrado más reciente y tiene, como casi todo en informática, sus seguidores y detractores. Es el más rápido de los dos algoritmos y teóricamente el más seguro.
- AES-CBC es un algoritmo que todavía soporta Microsoft Windows y que es un poco más lento que el anterior, aunque prácticamente igual de seguro si se utiliza una contraseña adecuada.

La longitud de la clave es idéntica para los dos algoritmos, aunque se puede cambiar mediante directivas de grupo locales para utilizar **claves de 256 bits de longitud** en el cifrado de los discos **en lugar de claves de 128 bits**.

Normalmente se considera que cuanto más bits tiene una clave más difícil es romperla para descifrar los datos utilizando la fuerza bruta. ¿Por qué no se utilizan siempre claves lo más largas posibles? Pues fundamentalmente debido a que cuantos más bits tiene una clave, más se tarda en cifrar y descifrar, en criptografía siempre se busca obtener un cifrado suficientemente seguro a un coste razonable.

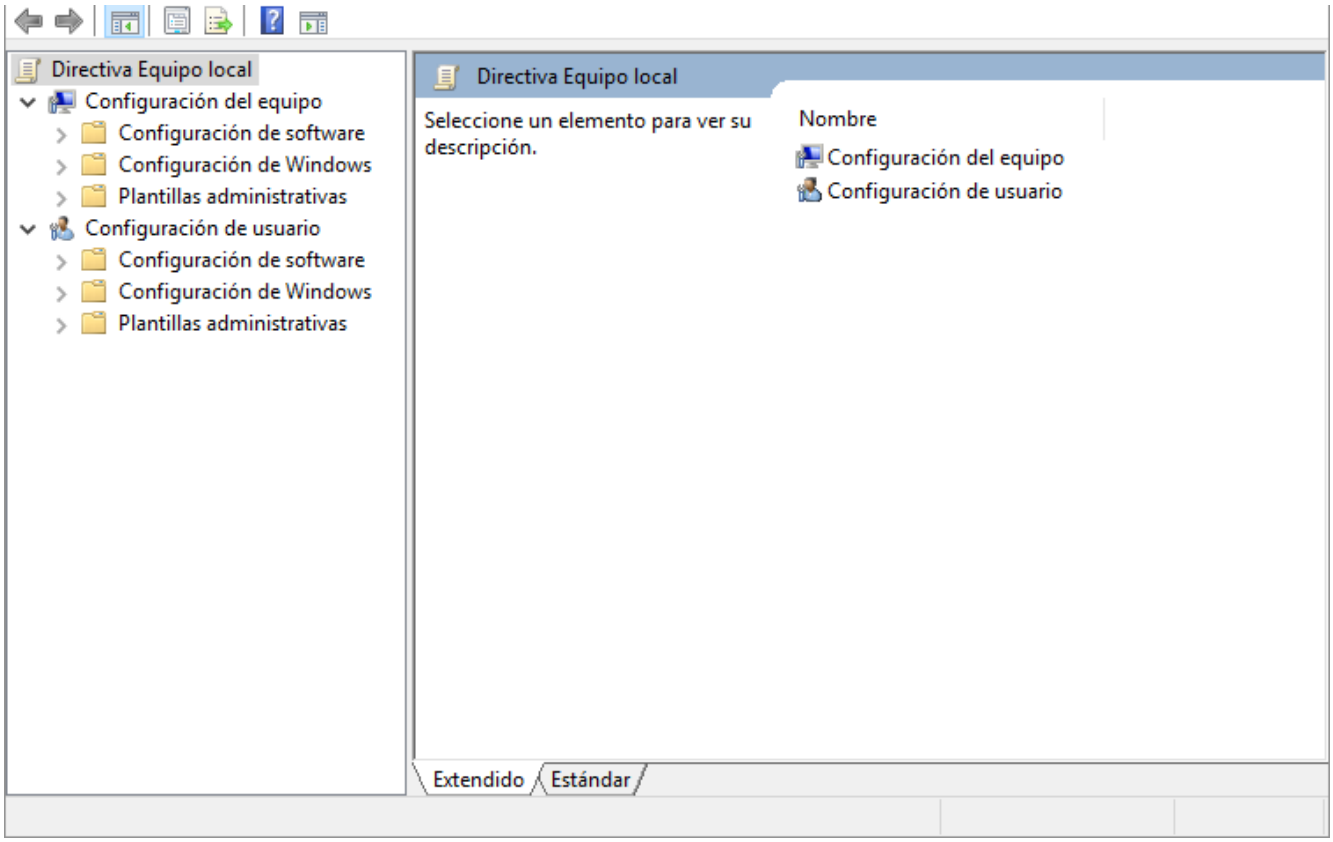
¿Qué es una directiva de grupo?

Las directivas en el sistema operativo Microsoft Windows son la forma de editar y modificar configuraciones. Mediante directivas, podemos controlar múltiples tareas y funciones del sistema operativo, tanto a nivel de máquina como a nivel de usuario.

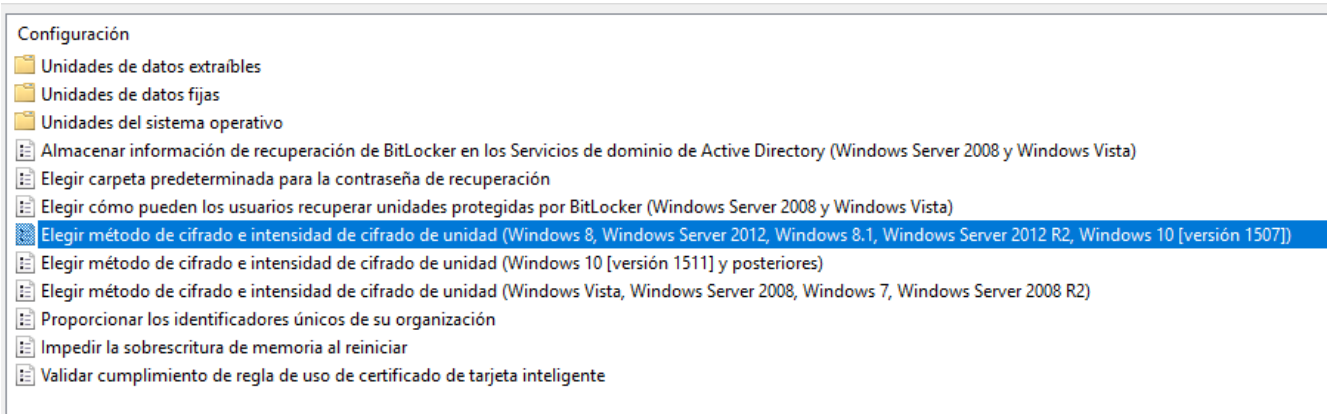
Modificando las directivas de grupo

Para cambiar el algoritmo de cifrado y la longitud de la clave mediante directivas de grupo **ejecutamos el comando gpedit.msc** desde la opción ejecutar de Windows, (pulsamos la tecla **Windows + R** para abrir la opción ejecutar). Este comando nos abre una consola de Microsoft donde podemos editar las directivas de grupo local.

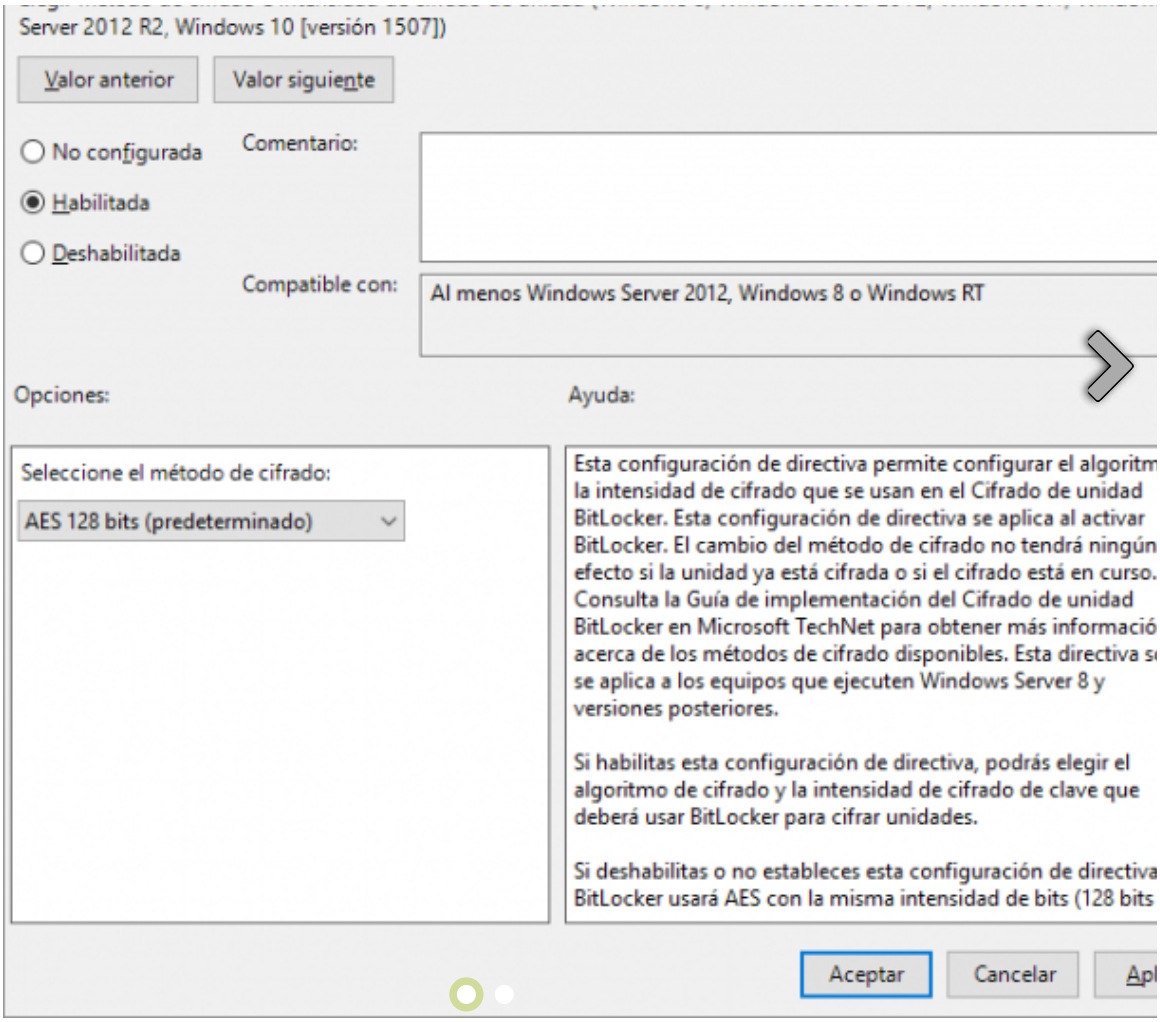
Dentro de la consola del **editor de directivas de grupo** seguimos la siguiente ruta de navegación: **Directiva de Equipo local / Configuración del equipo / Plantillas Administrativas /Componentes de Windows / Cifrado de unidad BitLocker**.



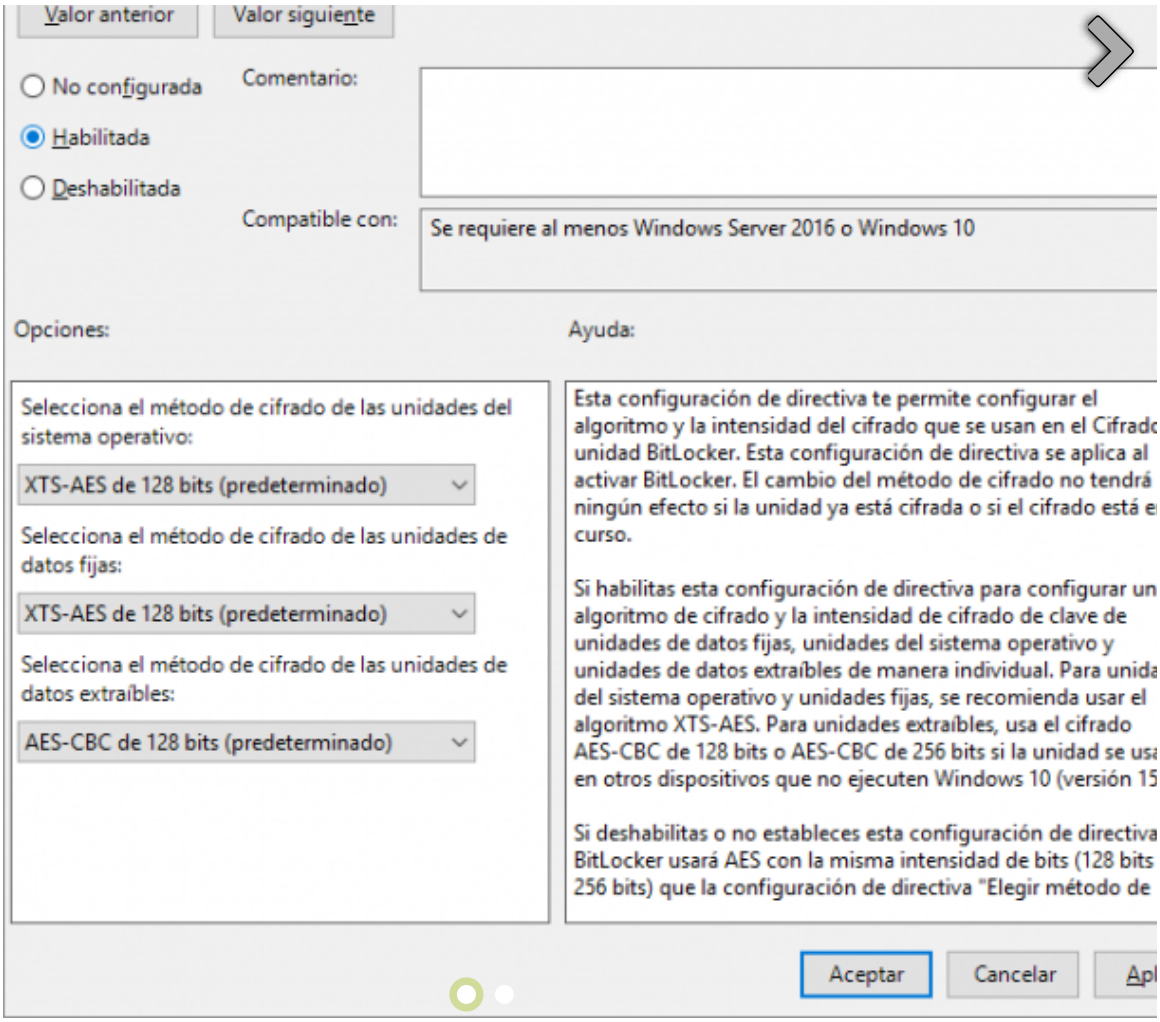
En esta categoría tenemos tres directivas:



Elegir método de cifrado e intensidad de cifrado de unidad para (Windows 8, 8.1, 10 [versión 1507] y Windows Server 2012, y 2012 R2), permite modificar la longitud de la clave de cifrado y escoger el cifrado AES con o sin el método difusor. El difusor es un método de cifrado que se aplica para proporcionar protección adicional a los datos cuando se pasa de la forma en claro a la forma cifrada.

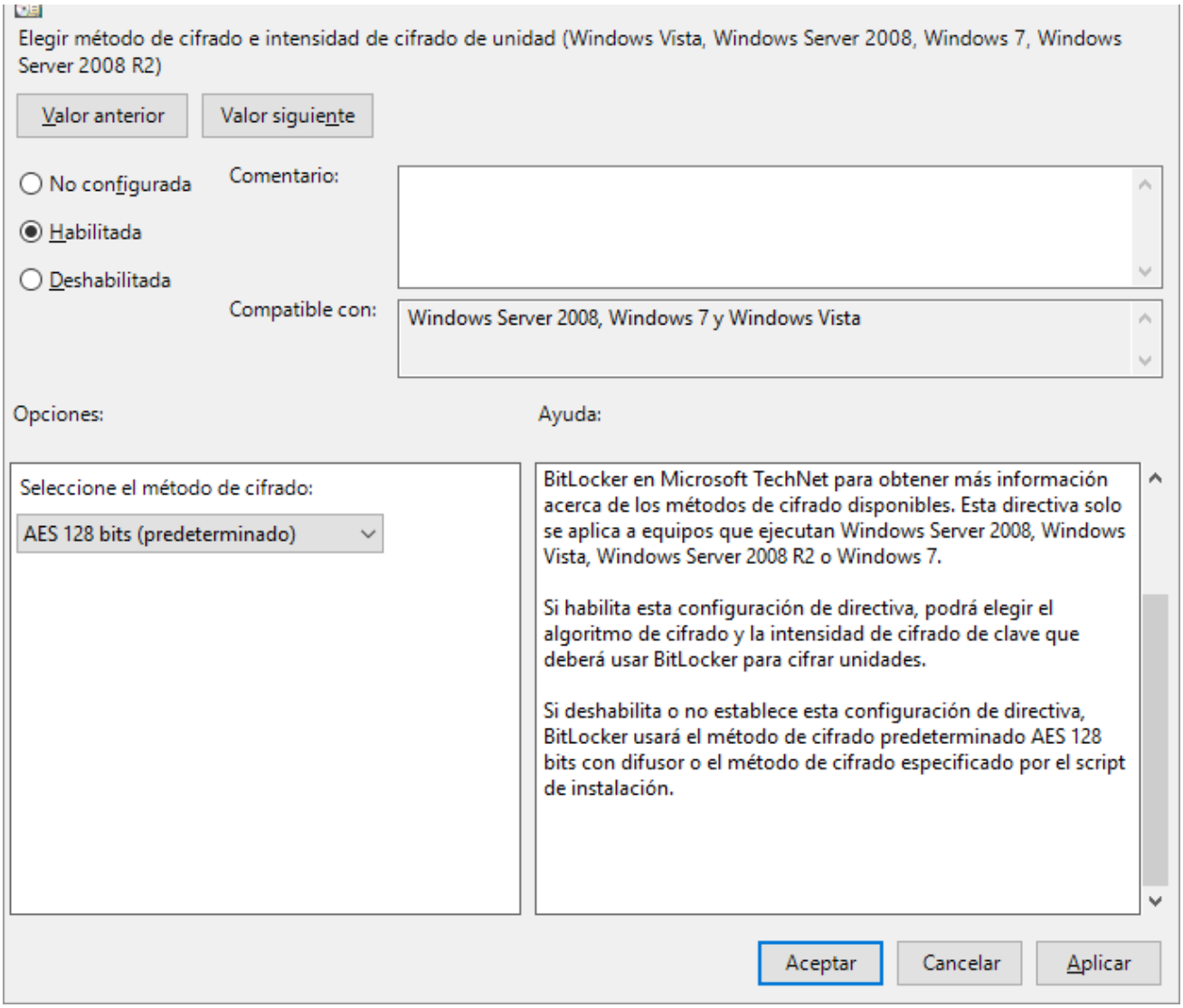


Elegir método de cifrado e intensidad de cifrado de unidad para (Windows 10 [versión 1511] y posteriores):

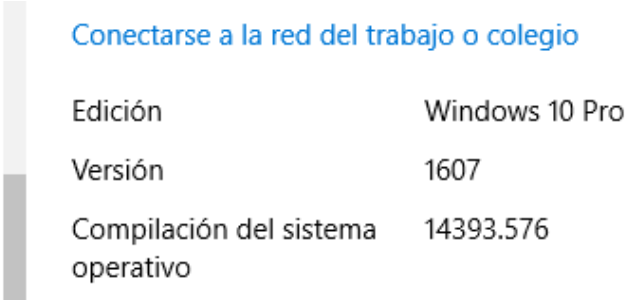


En esta directiva nos permite cambiar el algoritmo y la longitud de la clave de forma diferente para los discos internos de arranque, discos internos de datos y discos extraíbles y memorias flash USB.

Elegir método de cifrado e intensidad de cifrado de unidad para (Windows Vista, 7 y Server 2008 y 2008 R2):



Las posibilidades de configuración varían en función del sistema operativo y de su versión. Podemos ver la versión del sistema operativo abriendo el **Centro de actividades / Todas las configuraciones / Sistema / Acerca de**.



En cada una de ellas ofrece opciones de configuración del algoritmo y longitud de la clave de cifrado utilizado por BitLocker para el cifrado de las unidades. El cambio de

Estás directivas sólo se aplican en el caso de que coincida el sistema operativo y la versión con la que se está ejecutando en el ordenador. Al cambiar las opciones, las unidades que se cifren desde ese momento usarán la configuración nueva.

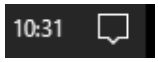
Activación de la directiva de grupo configurada

Una vez modificada una directiva de grupo, hay que esperar unos 90 minutos para que se apliquen los cambios; podemos pulsar la tecla Windows + R para abrir la opción ejecutar y escribir el comando "gpupdate /target:Computer /force" para que se apliquen los cambios inmediatamente y poder comprobar su resultado. Si ejecutas gpupdate.exe /? desde la consola de comandos podrás ver otras opciones del comando y explicación detallada sobre las mismas.

3. Activación de BitLocker en una unidad de almacenamiento interno

Vamos a ver el proceso de cifrado en una unidad de datos, es decir, sin sistema operativo, una unidad que no es de arranque.

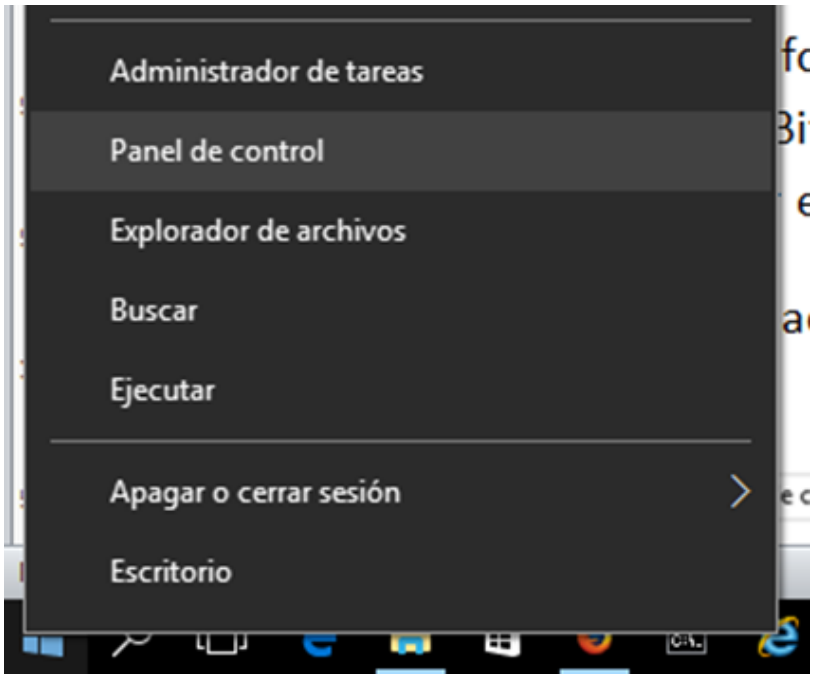
Para activar Bitlocker desde el menú de configuración de Windows 10, hacemos clic con el ratón sobre el icono del panel de notificaciones de la barra de tareas:



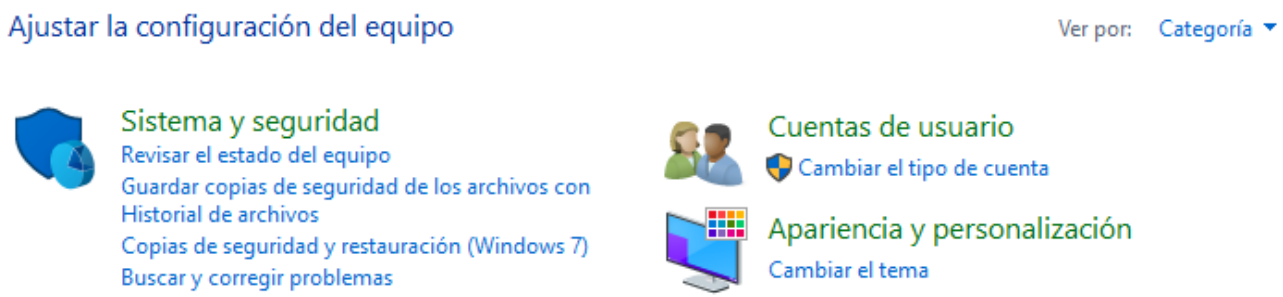
y escogemos la opción «Abrir el centro de Actividades»; pinchamos en «Todas las configuraciones» y en «Sistema»; pinchando en la última opción «Acerca de» accedemos a una ventana con información sobre nuestra instalación de Windows. En la parte inferior tenemos la opción «Configuración de BitLocker», al pinchar esta opción aparece una ventana en la que podemos activar, desactivar y gestionar BitLocker en nuestros discos y unidades extraíbles.

Para activar BitLocker desde el explorador de archivos, hacemos clic con el botón derecho del ratón sobre la unidad de disco a cifrar desde el explorador de archivos y en el menú de contexto de aparece escogemos la opción «**Activar BitLocker**«.

Para activar BitLocker desde el Panel de control, hacemos clic con el botón derecho del ratón sobre el icono de Windows en la barra de tareas.



En la ventana del «Panel de control» si el modo «Ver por» está configurado en «Categoría», pinchamos en «Sistema y seguridad».

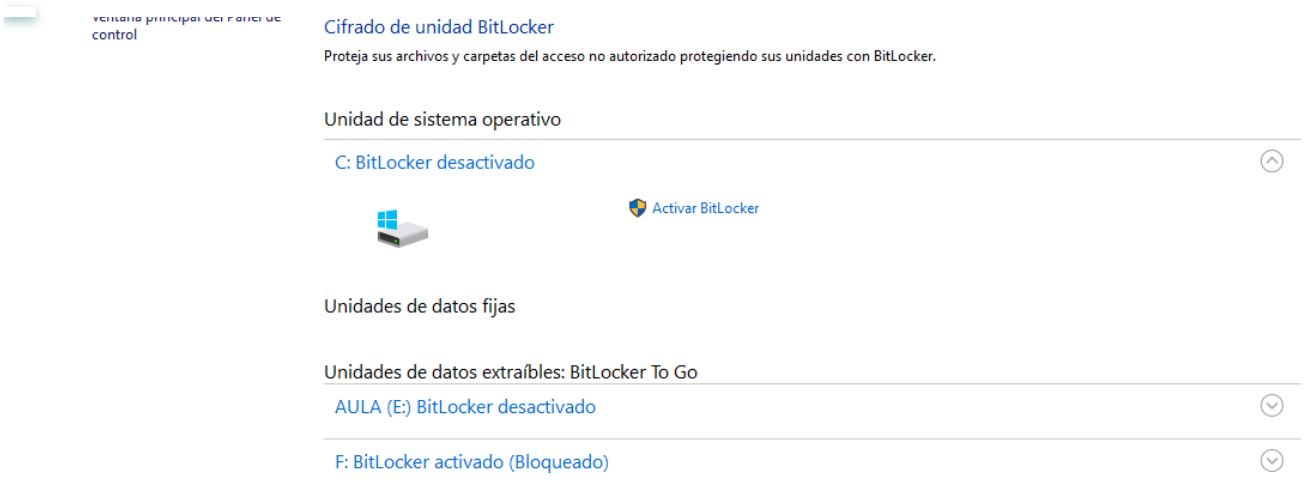


En la siguiente ventana ya podemos seleccionar la opción «Cifrado de unidad BitLocker».

BitLocker: Tutorial completo para cifrar discos en Windows

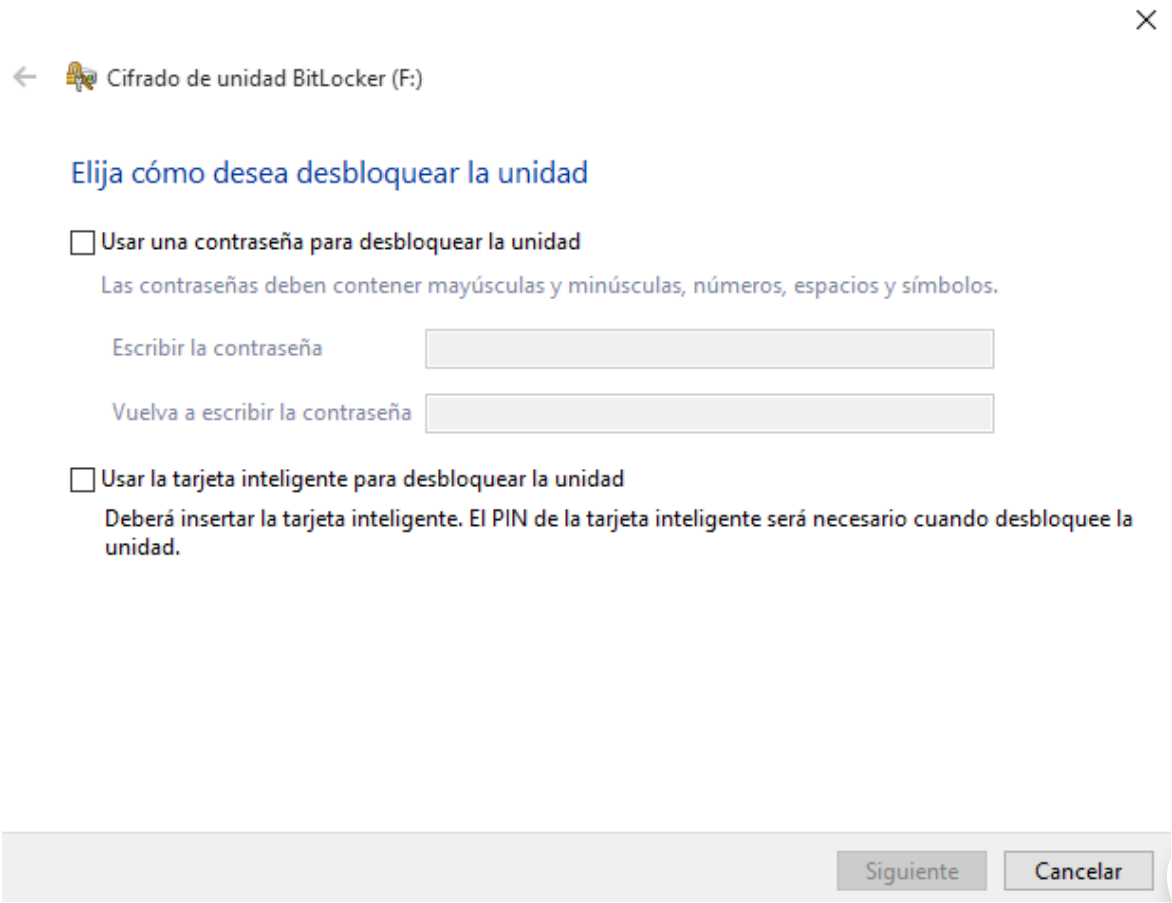
BitLocker muestra las unidades de almacenamiento agrupadas por categorías en función de cómo las ha detectado el sistema operativo. Solamente podemos utilizar BitLocker en unidades que están formateadas y con letra de unidad asignada.

En la imagen podemos ver un disco interno C: que contiene el arranque del sistema operativo en el que BitLocker está desactivado. Un disco externo con el cifrado también desactivado y un Pendrive con BitLocker activado.



Desplegamos las opciones de BitLocker para la unidad de disco a cifrar y nos muestra la opción «Activar BitLocker», pinchando sobre dicha opción nos aparece un asistente para configurar el cifrado en dicha unidad.

En primer lugar escribimos la contraseña para desbloquear la unidad una vez haya sido cifrada; la contraseña debe tener letras mayúsculas y minúsculas, números y símbolos especiales como el punto, la arroba, etc.

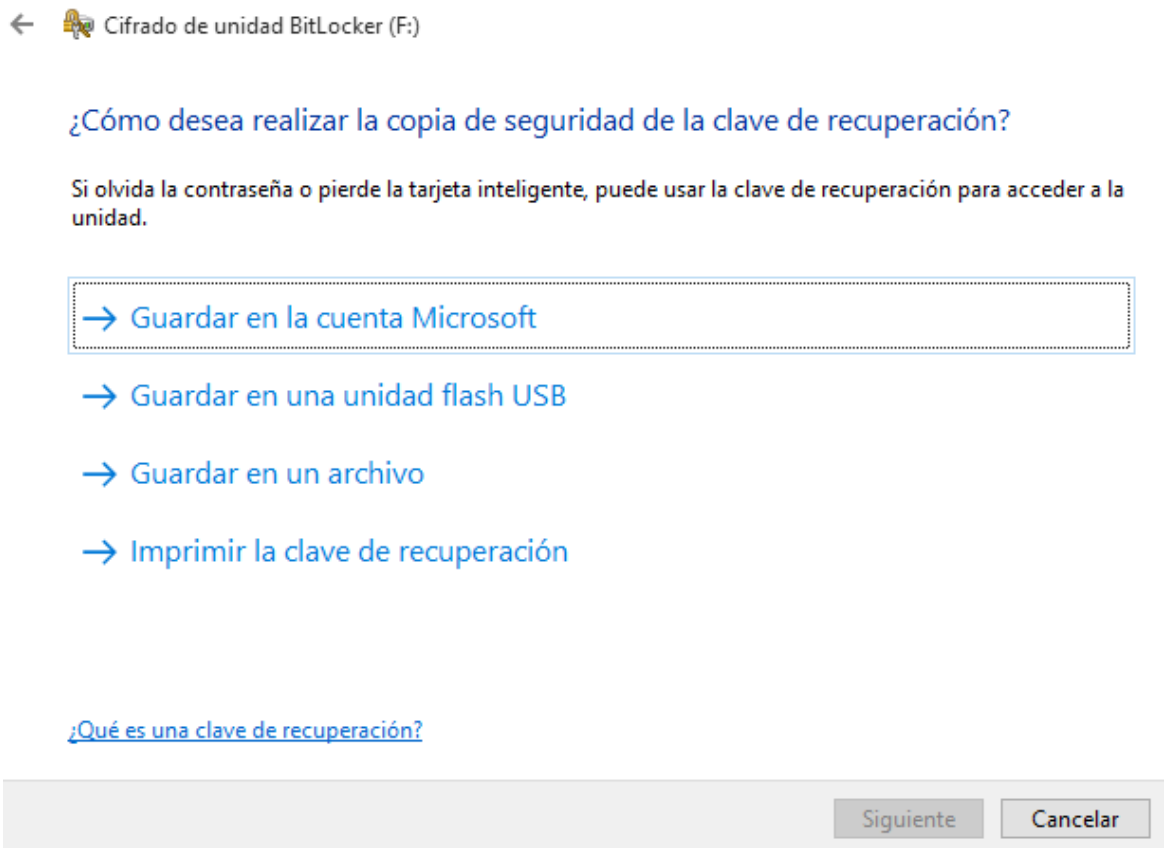


caso de que olvidemos la contraseña del punto anterior.

Al realizar una copia de seguridad de la clave de recuperación BitLocker crea una clave especial la primera vez que ciframos un disco. Una vez la unidad haya sido cifrada, podemos volver a generar una clave de recuperación desde el menú de configuración que aparece junto a la unidad cifrada en el cuadro de dialogo «Activar BitLocker».

Windows pedirá está clave de recuperación si durante el proceso de arranque de un ordenador con la unidad de disco del sistema operativo cifrada, detecta alguna situación extraña que impida desbloquear dicha unidad. También lo hará en el caso de hayamos utilizado BitLocker para cifrar una unidad de disco extraíble o una memoria flash y cuando no recordemos la contraseña de desbloqueo de una unidad cifrada.

El asistente de cifrado nos ofrece diferentes opciones para almacenar la clave de recuperación.



- **«Guardar en la cuenta Microsoft»:** Guarda la clave de recuperación en OneDrive, para poder usar esta opción es necesario haber abierto sesión en nuestro ordenador con una cuenta de Microsoft en lugar de con una cuenta local y que dicho ordenador no forme parte de un dominio de ordenadores.

Esta opción es la más recomendada por Microsoft para los ordenadores que no son miembros de un dominio.

Para configurar una cuenta de inicio de sesión de Microsoft en nuestro ordenador en lugar de una cuenta local, debemos tener una cuenta de Microsoft, (por ejemplo una cuenta de correo de Hotmail o de Outlook), y acceder al menú de «Configuración» del «Centro de Actividades», pinchar en la opción «Cuentas» y dentro del apartado «Tu Información», escoger el enlace «Iniciar sesión con una cuenta de Microsoft en su lugar».

- **«Guardar en una unidad flash USB»:** utiliza un pendrive que para guardar dicha clave, el pendrive no puede estar cifrado con BitLocker.
- **«Guardar en un archivo»:** Crea un fichero de texto donde almacena dicha clave. Es el mismo archivo que genera con la opción anterior.
- **«Imprimir la clave de recuperación»:** Imprime dicha clave en una impresora. El texto es el mismo que el de los ficheros anteriormente generados.

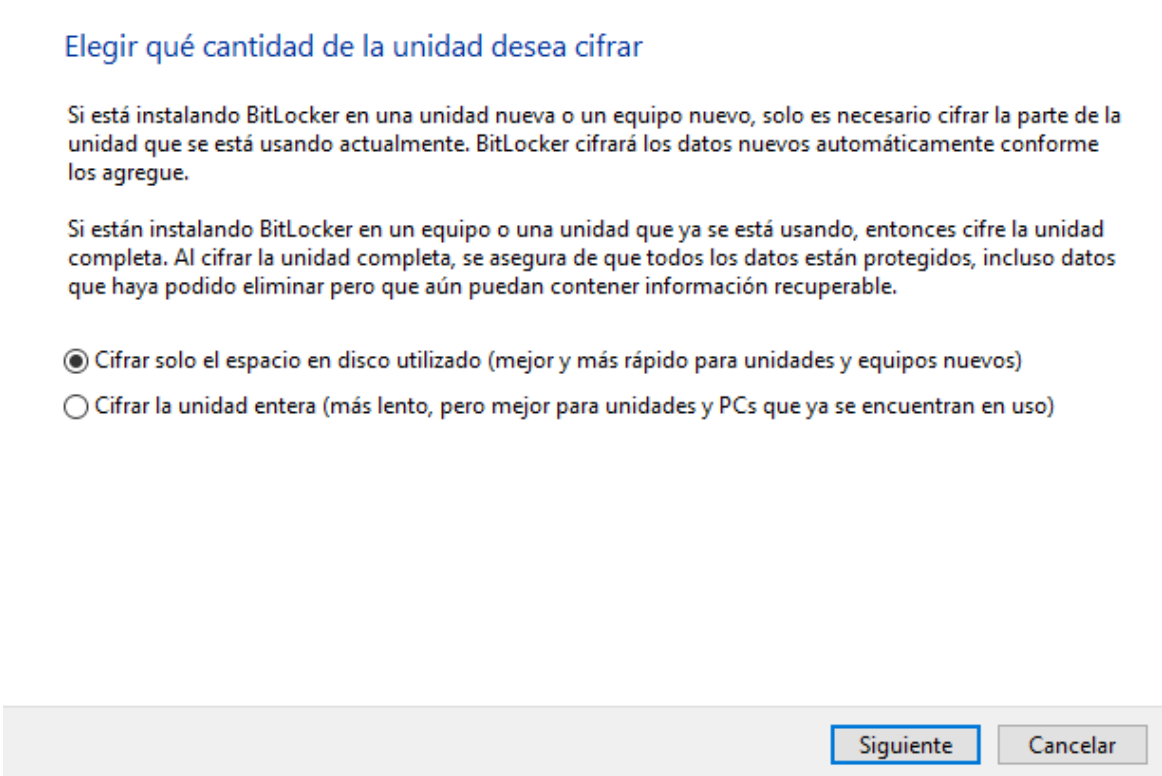
En el caso de que cifremos varios discos y tengamos varias claves de recuperación de cifrado, el nombre del archivo contiene un valor que debe coincidir con el que nos solicita el asistente de desbloqueo de unidad de BitLocker con clave de recuperación. Clave de recuperación de BitLocker **0555236F**-D828-4038-A990-DF3F90DA81A6.TXT

Escriba la clave de recuperación de 48 dígitos para desbloquear la unidad.
(Id. de clave: 0555236F)

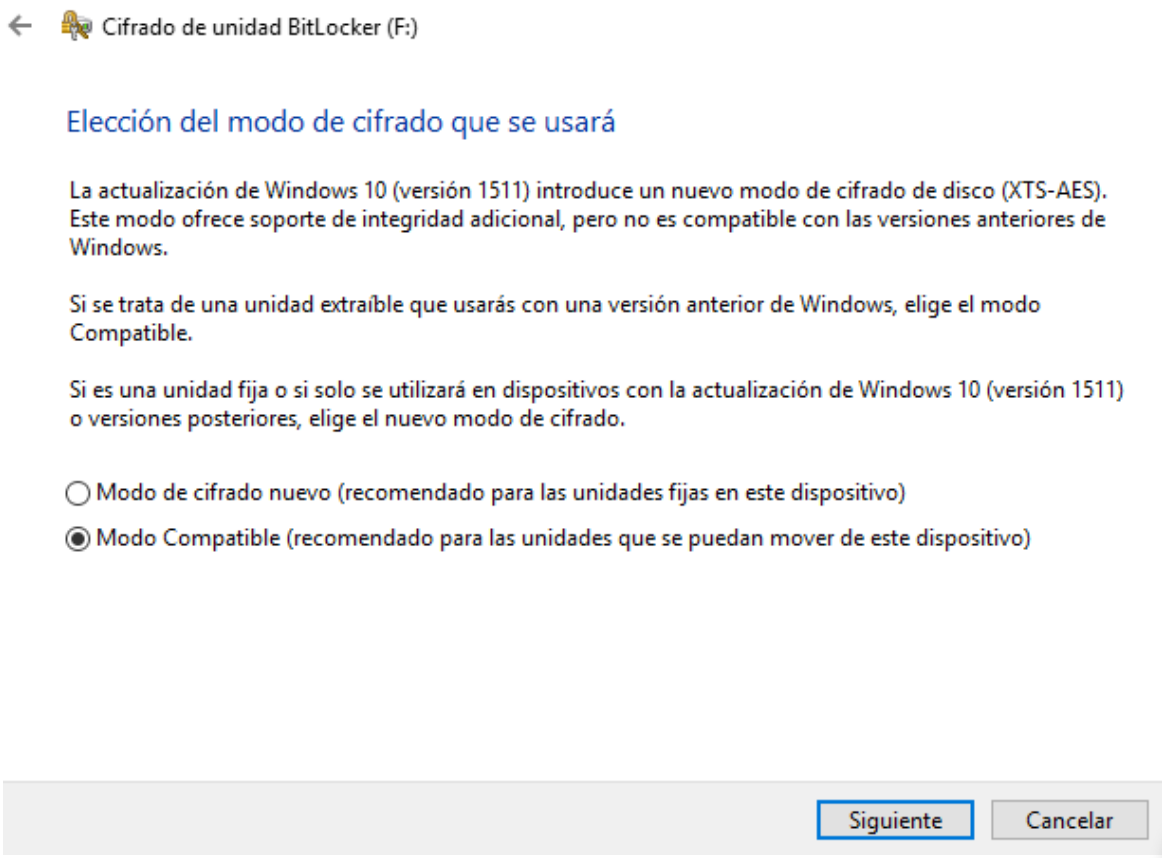
```
Clave de recuperación de Cifrado de unidad BitLocker

Para comprobar que esta es la clave de recuperación correcta, compare el comienzo del
siguiente identificador con el valor de identificador que se muestra en su equipo.

Identificador:

        0555236F-D828-4038-A990-DF3F90DA81A6

Si el identificador anterior coincide con el que se muestra en su equipo, use la siguiente
clave para desbloquear la unidad.

Clave de recuperación:

        164109-580635-109406-537933-420387-087450-051227-207449

Si el identificador anterior no coincide con el que se muestra en su equipo, esta no es la
clave correcta para desbloquear la unidad.
Intente con otra clave de recuperación o visite http://go.microsoft.com/fwlink/?
LinkID=260589 para obtener ayuda.
```

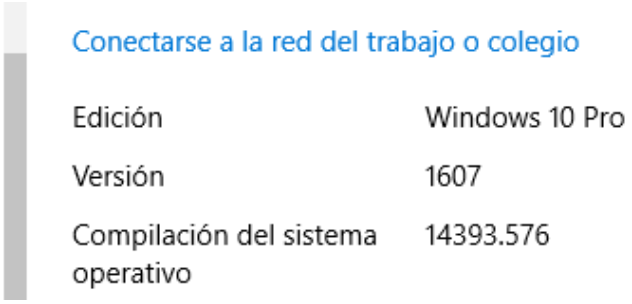
5. Seleccionar cantidad de disco a cifrar

En el siguiente paso nos pregunta si queremos cifrar sólo la parte de disco utilizada, (para discos nuevos, más rápida al cifrar menos cantidad de información), o cifrar todo el disco, (mejor opción para discos usados ya que aunque se hayan borrado ficheros, estos aún continúan en el disco y se pueden recuperar, es más lenta que la anterior).

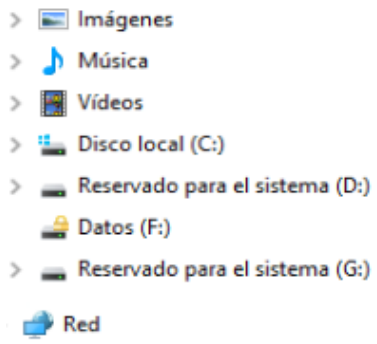


El siguiente cuadro de dialogo nos informa sobre la compatibilidad del cifrado de BitLocker con versiones anteriores de Windows 10.



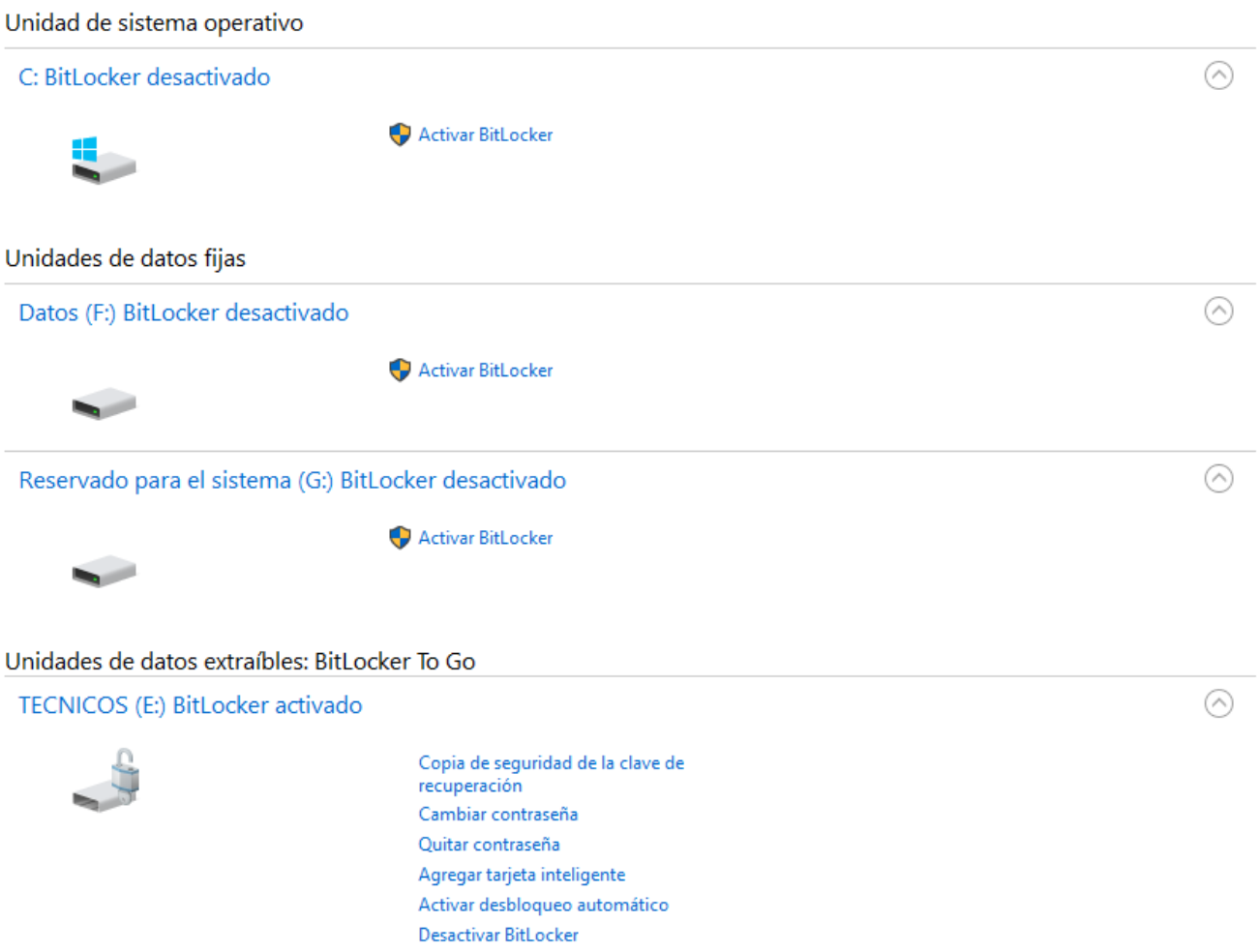


Si vamos a cifrar discos internos de nuestro ordenador, podemos utilizar la primera opción, pero si vamos a cifrar unidades de almacenamiento extraíbles es mejor utilizar la opción de compatibilidad para que no tengamos problemas a la hora de usar dicha unidad en sistemas con versiones sin actualizar de Windows 10. Seguidamente empieza el cifrado del disco, este proceso tendrá una duración determinada en función del tamaño del disco y de las opciones seleccionadas. Cuando finaliza el cifrado del disco, podemos ver un candado junto a la unidad de disco que está cifrada.



6. Configuración de BitLocker en unidades cifradas

Cuando tenemos unidades cifradas con BitLocker en nuestro ordenador nos aparece un menú de configuración debajo de la unidad cifrada.



La primera opción **«Copia de seguridad de la clave de recuperación»** sirve para volver a generar una clave de recuperación por si olvidamos nuestra contraseña de desbloqueo.

- **«Cambiar contraseña»** nos permite cambiar la contraseña de desbloqueo.
- **«Quitar contraseña»** Nos permite desactivar el desbloqueo mediante contraseña, habrá que habilitar otro método de protección del cifrado antes de que nos permita quitar la contraseña; BitLocker no se puede utilizar sin un método de autenticación.
- **«Desactivar BitLocker»** sirve para descifrar la unidad de almacenamiento.
- **«Agregar tarjeta inteligente»** permite utilizar un certificado o firma digital como dispositivo para desbloquear las unidades cifradas.
- **«Activar desbloqueo automático»** Tiene la misma función que la casilla de verificación del cuadro de dialogo de desbloqueo de unidad externa, no volver a pedir la clave de desbloqueo en un equipo determinado.

Si disponemos de la clave de desbloqueo podemos utilizar BitLocker en cualquier ordenador para descifrar el contenido de un disco o memoria USB.

ordenador arranque el disco que contiene el sistema operativo ha de estar desbloqueado, pero al mismo tiempo hay que proteger dicho disco por si se produce un arranque desde un live cd o un dispositivo USB.

BitLocker añade a la unidad de arranque una partición sin cifrar en la que almacena los ficheros que el ordenador necesita para arrancar y posteriormente desbloquea la partición donde se encuentra el sistema operativo para que pueda cargarse en memoria y arrancar el ordenador.

Es altamente recomendable realizar una copia de seguridad completa del disco de arranque antes de continuar con el cifrado del mismo por precaución.

Para conseguir la mejor protección del sistema BitLocker utiliza un dispositivo de hardware, (un chip), instalado en la placa base del ordenador llamado TPM, (Trusted Platform Module). El TPM genera claves de cifrado y almacena en su memoria parte de dicha clave y parte en el disco; TPM detecta cambios de hardware de forma que un atacante no pueda acceder al disco manipulando el hardware del ordenador mientras el sistema estaba sin conexión.

Si el ordenador tiene instalado el chip TPM lo podemos ver desde la ventana del administrador de dispositivos. Pulsando botón derecho del ratón sobre el icono de inicio de Windows accedemos al administrador de dispositivos y en dicha ventana aparecerá una categoría llamada “Dispositivos de seguridad” que indica que tenemos el chip TPM instalado.

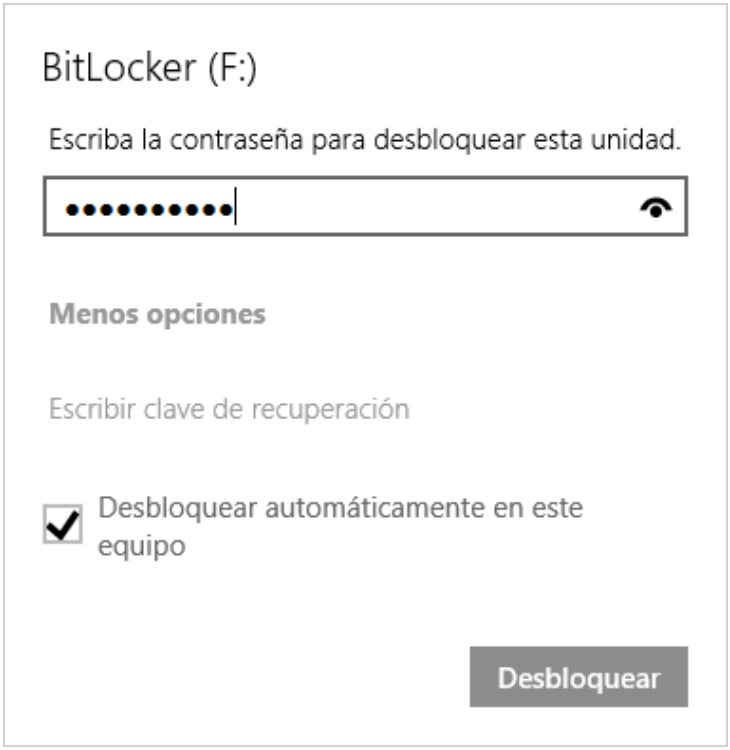
Si no disponemos de chip TPM aún podemos cifrar el disco de arranque de nuestro ordenador, al intentar activar BitLocker nos aparece la siguiente ventana en el que nos indica que podemos usar BitLocker si hacemos cambios en una directiva del equipo.

Iniciando BitLocker

Este dispositivo no puede usar un Módulo de plataforma segura. El administrador debe establecer la opción "Permitir BitLocker sin un TPM compatible" en la directiva "Requerir autenticación adicional al iniciar" para los volúmenes del sistema operativo.

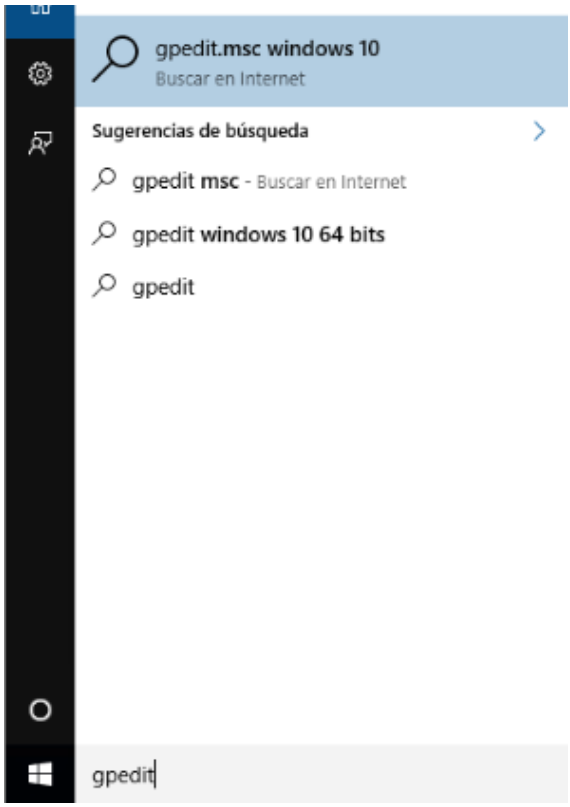
8. BitLocker en unidades de almacenamiento externas o extraíbles

En el caso de una memoria flash USB que esté cifrada, al pincharla en cualquier ordenador nos pide la contraseña de desbloqueo para poder acceder a ella. Tenemos la opción de marcar la casilla para que la unidad se desbloquee automáticamente en dicho equipo.



9. Procedimiento para utilizar BitLocker sin TPM

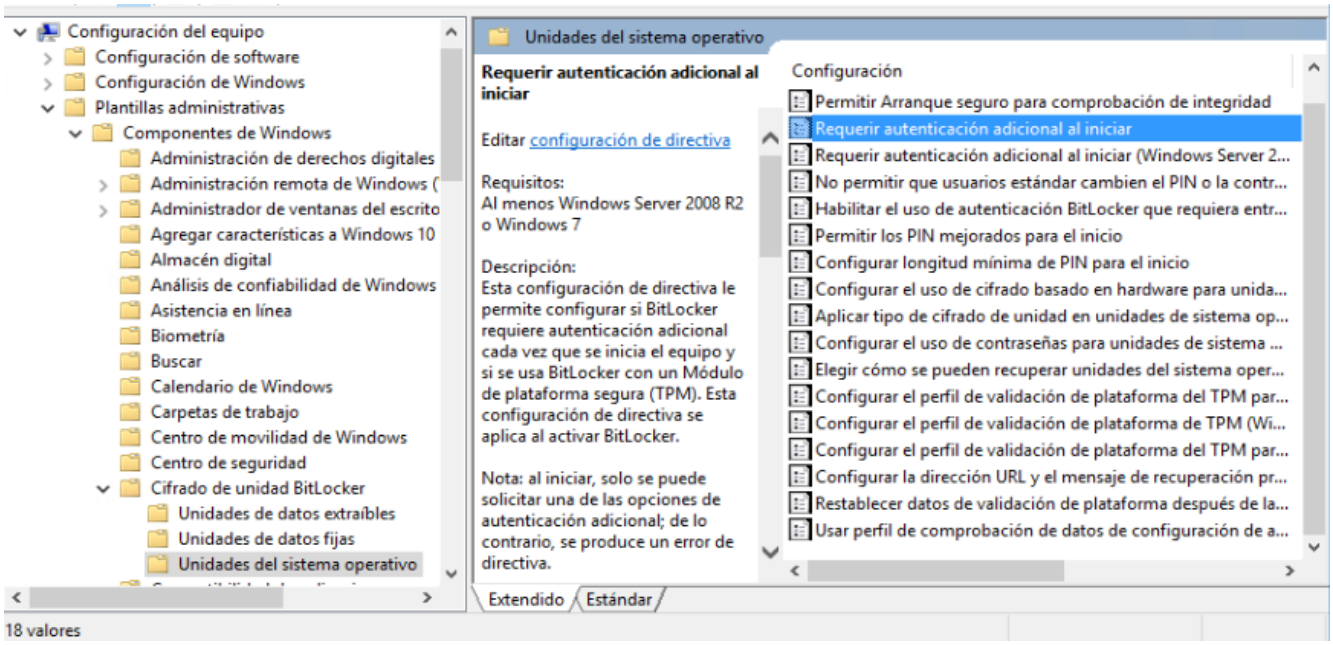
En la barra de búsqueda junto al botón de «Inicio» escribimos «gpedit.msc»:



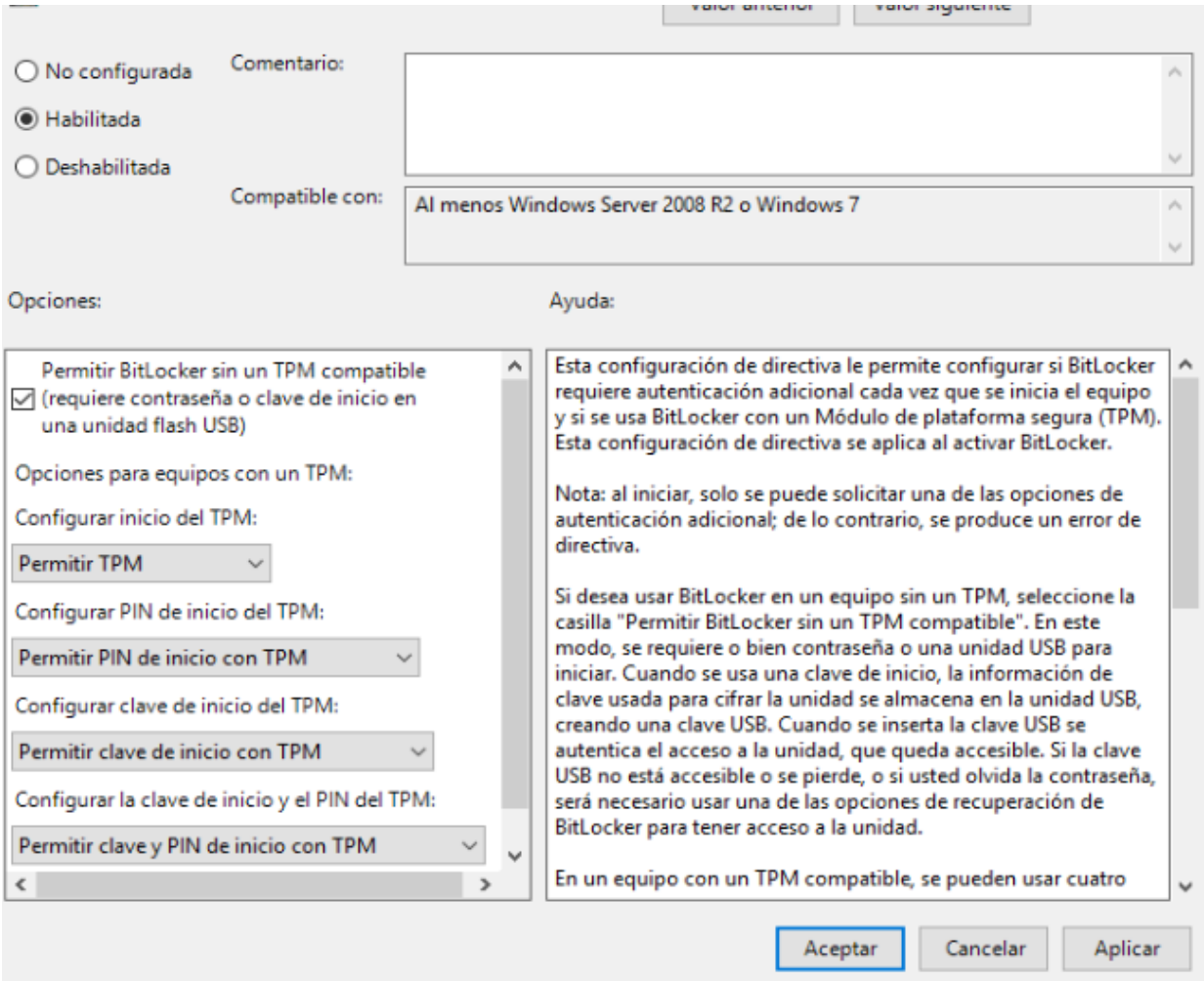
Hacemos clic sobre el enlace a «gpedit.msc Windows 10», con lo que se abre una consola del sistema operativo para la gestión de directivas del grupo local.

En el marco de la izquierda vamos haciendo clic en las opciones «Directiva Equipo local», Configuración del equipo / Plantillas administrativas / Componentes de Windows / Cifrado de unidad de BitLocker / Unidades del sistema operativo y en las opciones que aparecen en el marco de la derecha hacemos doble clic sobre «**Requerir autenticación adicional al iniciar**«:

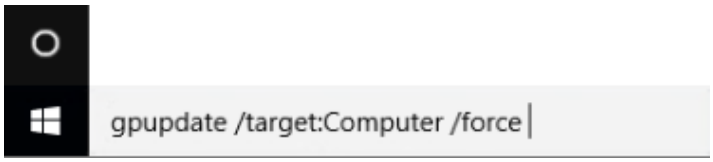
BitLocker: Tutorial completo para cifrar discos en Windows



En el cuadro de dialogo que aparece habilitamos la opción de «Requerir autenticación adicional al iniciar» y marcamos la casilla «Permitir BitLocker sin un TPM compatible».



Pinchamos en el botón Aceptar y ejecutamos el comando «gpupdate /target:Computer /force» para forzar la actualización de la directiva que acabamos de crear. Podemos ejecutar este comando desde la casilla de buscar junto al botón de «Inicio» de la barra de tareas.



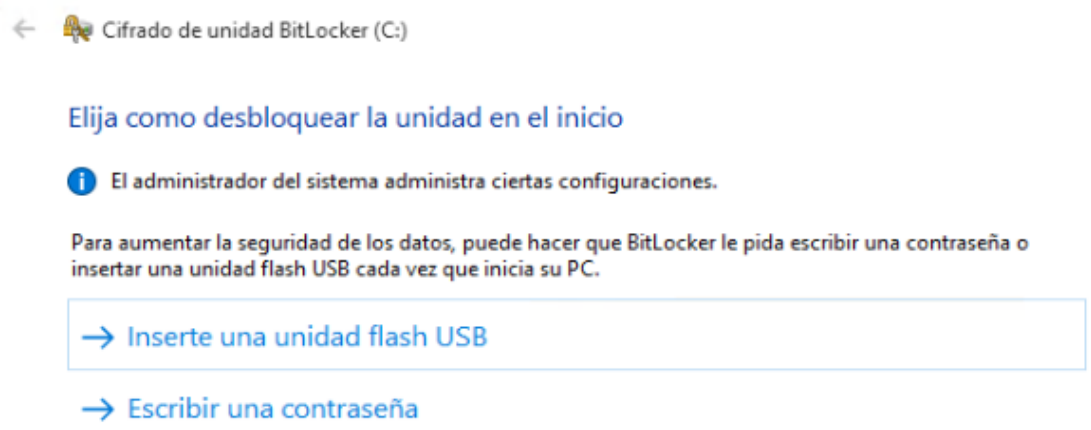
Volvemos a la ventana de Cifrado de BitLocker e intentamos volver a activar BitLocker en el disco de arranque. El asistente detecta que no tiene el chip TPM instalado y procede con lo configurado en la directiva y muestra un cuadro de dialogo en el que nos ofrece dos opciones:

- **Insertar una unidad flash USB**, donde almacenará la clave de desbloqueo del dis
  Esta unidad deberá estar insertada en el ordenador cada vez que intentemos arra

mayúsculas, minúsculas, números y símbolos especiales.

El asistente obliga a utilizar una unidad flash USB si considera que la configuración del sistema no es apropiada para utilizar la validación mediante contraseña. Es muy importante no retirar la unidad USB durante el proceso de cifrado y los reinicios del ordenador.

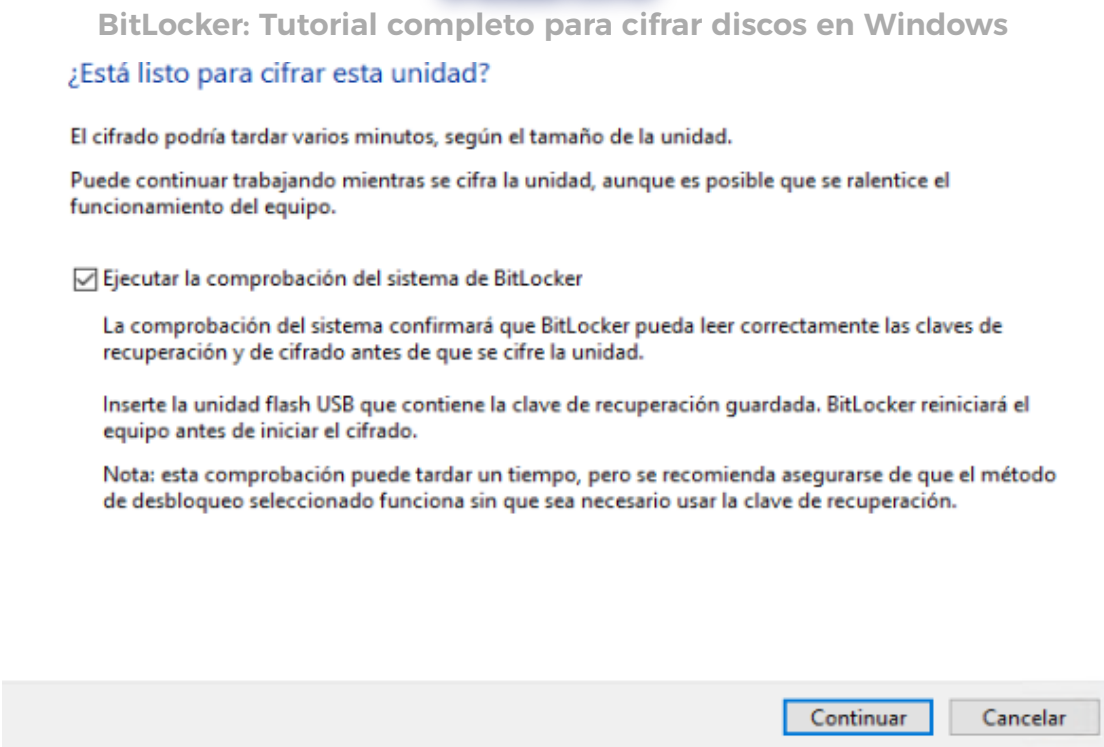
También es aconsejable cambiar el orden de arranque en el BIOS para que el ordenador no intente arrancar desde la memoria USB que estamos utilizando para almacenar la clave de desbloqueo.



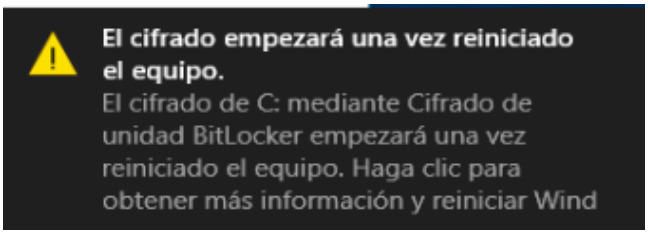
A partir de aquí el proceso es similar a cuando estamos cifrando un disco de datos:

- Nos pide un método para realizar una copia de seguridad de la clave de recuperación.
- Seleccionar si ciframos todo el disco o sólo la parte que contiene datos.
- Ejecutar una prueba compatibilidad del sistema con BitLocker.

El sistema nos ofrece la posibilidad de realizar una prueba al sistema para determinar que se puede realizar el cifrado y que BitLocker podrá acceder sin problemas a la clave de recuperación antes de proceder al cifrado del mismo.



Una vez pinchemos en el botón Continuar, el asistente nos dirá que es necesario reiniciar el sistema para comenzar el cifrado del disco.



Si al reiniciar el ordenador aparece el siguiente mensaje, es que no se ha podido completar el cifrado del disco, comprobar los puntos indicados en el mensaje y vuelva a intentarlo. Asegúrese de que el BIOS está configurado para que no arranque desde la memoria flash USB.

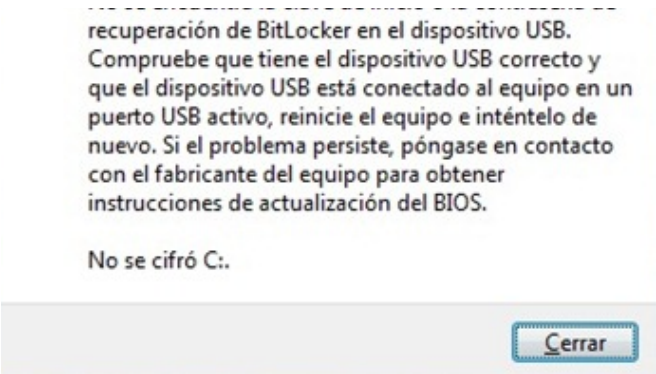
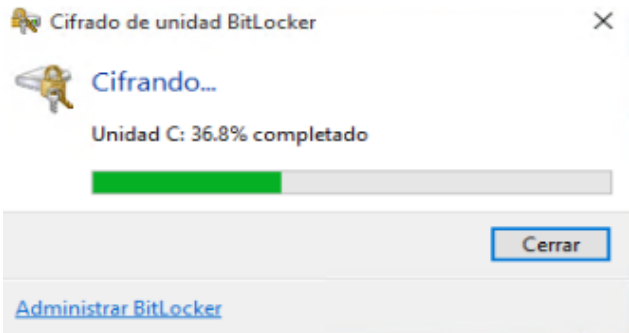


Imagen del proceso de cifrado que se realiza al reiniciarse el ordenador.



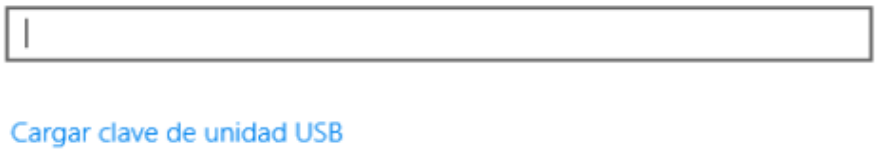
En la unidad flash USB BitLocker almacena un fichero cifrado con extensión BEK (BitLocker Encryption Key) que contiene la clave para desbloquear el disco de arranque del sistema. Es conveniente hacer una copia de seguridad de este fichero junto con el de la clave de recuperación en un lugar seguro.

10. Procedimiento de desbloqueo de unidad de BitLocker con clave de recuperación

Windows pedirá la clave de recuperación si durante el proceso de arranque con la unidad de disco del sistema operativo cifrada, detecta alguna situación anómala que impida desbloquear la unidad por algún motivo. También lo hará en el caso de hayamos utilizado BitLocker para cifrar una unidad de disco extraíble o una memoria flash, y no recordemos la contraseña de desbloqueo.

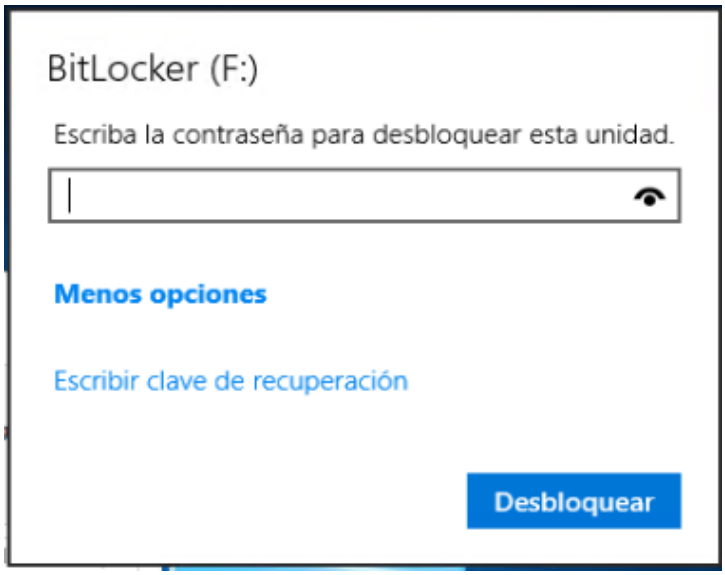
En el caso de que cifremos varios discos y tengamos varias claves de recuperación de cifrado, el nombre del archivo contiene un valor que debe coincidir con el que nos solicita el asistente de desbloqueo de unidad de BitLocker con clave de recuperación.

Clave de recuperación de BitLocker 0555236F-D828-4038-A990-DF3F90DA81A6.TXT



11. Acceso con escritorio remoto a unidades cifradas

Cuando accedemos mediante escritorio remoto a un ordenador que tiene unidades de almacenamiento cifradas con BitLocker, nos pide la contraseña de desbloqueo.



También nos ofrece una opción para escribir la clave de recuperación por si no recordáramos la contraseña de desbloqueo.

12. Abrir unidades cifradas con BitLocker en Windows XP o Vista

Windows XP o Windows Vista no reconocen automáticamente que una unidad extraíble está cifrada con BitLocker por lo que no permiten desbloquearlas. Microsoft tiene una herramienta llamada «**Lector BitLocker To Go**» que permite a los usuarios obtener acceso de sólo lectura a las unidades con formato de sistema de archivos FAT protegidas por BitLocker. Puedes **descargarla en este enlace**.

Hasta aquí hemos llegado con nuestro manual a fondo de BitLocker, si tenéis cualquier duda podéis ponernos un comentario y os responderemos lo antes posible.

Te puede interesar ...

Análisis de Acronis True Image 2021, ahora es una suite de ciberseguridad

Mejores herramientas gratuitas de informática forense

Seguridad

Prueba la nueva función de aislamiento de sitios

Seguridad

Javier Jiménez | Publicado el 26 de septiembre, 2020 • 10:00

0

Mozilla Firefox es, como sabemos, uno de los navegadores más populares y utilizados a nivel mundial. Está presente en múltiples sistemas operativos y dispositivos. Cuenta con una gran cantidad de extensiones, características y funciones que podemos utilizar. Sin embargo algo en lo que hacen mucho hincapié constantemente es en buscar mejoras relacionadas con la seguridad y privacidad. Ya sabemos que son factores muy importantes para los usuarios. En este artículo explicamos cómo usar la nueva función de **aislamiento de sitios en Firefox**.

Cómo activar la función de aislamiento de sitios en Firefox

Como hemos indicado, el navegador de **Mozilla** siempre ha contado con funciones y características a la vanguardia para intentar que la seguridad y privacidad estén presentes. Es precisamente a la hora de navegar por Internet cuando más problemas podemos sufrir de este tipo.

En esta ocasión se trata de la característica **Fission**, que ofrece la funcionalidad de aislar sitios y los iframes de terceros en el navegador web. De esta forma mejora tanto la privacidad como la seguridad de los usuarios.

De momento esta característica únicamente está disponible para Firefox Nightly, que como sabemos es la versión del navegador de Mozilla donde llegan primero los cambi

Lo primero que tenemos que asegurarnos es de contar con la última versión. Al menos es necesario tener Firefox Nightly 82.0a1. Una vez nos aseguremos de tener el navegador correctamente actualizado, debemos llevar a cabo los siguientes pasos:

En la barra de direcciones debemos ejecutar **about:config**. Nos pedirá permisos y debemos darle a aceptar los riesgos. Un paso previo para poder entrar en la configuración.

Posteriormente debemos buscar **fission.autostart**. De forma predeterminada veremos que viene en False, por lo que simplemente lo cambiamos a True. Básicamente eso lo que hace es activar la función.

Hecho esto tenemos que ir nuevamente a la barra de búsqueda y en este caso buscar **gfx.webrender.all**. Como en el caso anterior vendrá de forma predeterminada en False y simplemente lo cambiamos a True.

Una vez hayamos hecho estos dos pasos previos, simplemente reiniciamos el navegador para que los cambios tengan efecto. A partir de ahí ya debería estar disponible para u esta función.

activada correctamente en Mozilla Firefox. Para ello simplemente hay que abrir cualquier página web en el navegador y pasar el cursor del ratón por encima de la pestaña.

Veremos que, como aparece en la imagen de arriba que mostramos, junto al nombre del sitio aparece F. Eso quiere decir que está funcionando correctamente Fission.

Hay que tener en cuenta que Mozilla Firefox funcionará de la misma manera que antes de activar esta función. No vamos a notar **ningún cambio** al iniciar páginas webs. Eso sí, esta herramienta va a consumir algunos recursos más en el sistema. No obstante, no debería de ser algo que sea perceptible por el usuario.

También podemos navegar de forma normal, sin hacer uso de esta característica. Para ello tenemos que ir al menú y veremos la opción **New Non-Fission Window**. Simplemente tenemos que pinchar y se abrirá una nueva ventana del navegador Firefox pero esta vez sin hacer uso de la característica Fission.

En definitiva, siguiendo estos pasos que mencionamos podemos activar la función de **aislamiento de sitios webs y de iframes** de terceros en Mozilla Firefox. Como hemos visto simplemente hay que seguir una serie de pasos sencillos. De esta forma haremos que la privacidad y seguridad al navegar estén presentes y no tengamos ningún tipo de problemas. Ya sabemos que son dos factores que deben estar siempre en primer plano en todo tipo de sistemas operativos y dispositivos que utilicemos.

¡SÉ EL PRIMERO EN COMENTAR!

Te puede interesar ...

Habilita la protección contra el rastreo de redirección en Firefox

Evita que te rastreen con Gmail y Outlook