	Asistencia 🗸	Buscar	Buscar	
Productos Soluciones Se	ervicios Asis	tencia Comunidad		
Soporte de productos Base de cono Solicitudes de servicio y estado del envío	ocimientos Ga Asistencia par	rantía y contratos a pedidos Póngase en contacto la asistencia		
☆ > <u>Asistencia</u> > Consulta de tema	as			

# ¿Cómo activar o desactivar BitLocker con TPM en Windows?

En este artículo, se describe el proceso de activación y desactivación de BitLocker en Windows 7/8/10 y cómo habilitar TPM para una funcionalidad adecuada.

### Índice:

- 1. Habilitar TPM
- 2. Activar BitLocker en el sistema operativo
- 3. Comprobar el estado de BitLocker (administrar la consola de BitLocker)
- 4. Verificar el estado de BitLocker (línea de comandos)
- 5. <u>Suspender BitLocker</u>
- 6. Desactivar BitLocker

### Activación y desactivación de BitLocker en Windows 7/8/10

Windows BitLocker se ha convertido en una solución cada vez más popular para que los usuarios aseguren sus datos. A continuación, encontrará información acerca de cómo activar y desactivar BitLocker mediante los métodos estándar.

Este artículo no contiene información acerca de la utilización de un USB como reemplazo de TPM y tampoco acerca de los cambios en las directivas de grupo para características avanzadas. Los cambios en la política de grupo a nivel de dominio y las configuraciones de BitLocker administradas en red fueron hechas con el mejor esfuerzo y están fuera del alcance del soporte. Las configuraciones compatibles se limitan a sistemas únicos y a las configuraciones de BitLocker administradas localmente.

NOTA: Los sistemas con chipsets Skylake necesitan una configuración muy específica para que BitLocker funcione correctamente. Si un sistema Skylake está solicitando la clave de recuperación, incluso con la siguiente configuración, ASEGÚRESE de que el BIOS esté actualizado, ya que se corrigió después de la versión.

- Todos los sistemas operativos configurados en el modo de inicio heredado deben utilizar TPM 1.2. Se recomienda que el BIOS también se actualice a la última revisión.
- Todos los sistemas operativos configurados en el modo de inicio de UEFI pueden utilizar TPM 1.2 o TPM 2.0. Se recomienda que el BIOS también se actualice a la última revisión.
- Si un sistema Windows 7 está configurado para el modo de inicio de UEFI, es posible que se deba aplicar este parche para utilizar TPM 2.0: Parche de Microsoft TPM 2.0
- Las excepciones a esto son Latitude 5175 y Latitude 7275, las cuales solo tienen TPM 2.0 y no pueden ser desactualizadas a 1.2.

NOTA: Para los requisitos completos y actualizados, consulte los requisitos de BitLocker de Microsoft aquí: <u>https://technet.microsoft.com/en-us/library/dd835565(WS.10).aspx</u>

## 1. Habilitar TPM

NOTA: Asegúrese de que el TPM esté Activado/Habilitado después de encenderlo, si tiene la opción. Encender el TPM no hará que se habilite de manera automática para establecer comunicación con el sistema operativo. Es necesario habilitar el TPM para que el sistema operativo asuma la propiedad del chip TPM para almacenar las claves de cifrado.

1. Encienda el equipo

- 2. Mientras la computadora realiza la prueba POST, presione la tecla de acceso rápido (por lo general, F2 o Supr) para ingresar al BIOS
- 3. Cuando esté en el BIOS, busque la sección para configurar la Security
- 4. En la sección de seguridad, busque la opción de TPM
- 5. Resalte la sección TPM 2.0/1.2 a la izquierda



- 6. Marque la casilla TPM a la derecha para encender el TPM
- 7. Después de conectar el TPM, seleccione la opción Activate/Enable para activar o desactivar el TPM.



8. Después de que el TPM se haya activado y habilitado, haga clic en Save changes and Exit en el BIOS.

Volver al principio

### 2. Activar BitLocker en el sistema operativo

1. Encienda el sistema.

2. Inicie sesión en el sistema operativo normalmente

3. Abra la sección de Administración de BitLocker de una de las siguientes maneras:

Windows 7

1. A través del Menú de Inicio

- a. Haga clic en el botón del Menú de Inicio de Windows
- b. En el cuadro de búsqueda, escriba "Administrar BitLocker"
- c. Presione Intro o haga clic en el icono Administrar BitLocker en la lista

#### 2. A través del Panel de control

- a. Haga clic en el botón del Menú de Inicio de Windows
- b. Haga clic en el Panel de control
- c. Haga clic en Sistema y seguridad
- d. Haga clic en cualquiera de las opciones de Cifrado de unidad BitLocker

#### 3. A través del disco duro

- a. Abra Equipo o Mi PC
  - De manera alternativa, haga clic en el icono del **Explorador de archivos** y seleccione el equipo
- b. Seleccione la unidad Encryption:\ (o sistema de Windows)
- c. Haga clic con el botón secundario en la unidad que resaltó
- d. Haga clic en Activar BitLocker (NOTA: Se omitirá la pantalla inicial de BitLocker)

#### <u>Windows 8</u>

#### 1. A través de la pantalla de la aplicación

- a. Haga clic en el botón del Menú de Inicio de Windows
- b. Abra el cuadro de búsqueda y escriba "Administrar BitLocker"
- c. Presione Intro o haga clic en el icono Administrar BitLocker en la lista

#### 2. A través del Panel de control

- a. Haga clic en el botón del Menú de Inicio de Windows
- b. En el cuadro de búsqueda, escriba Panel de control
- c. Haga clic en Sistema y Seguridad o busque BitLocker en la ventana del Panel de control
- d. Haga clic en cualquiera de las opciones de Cifrado de Unidad BitLocker

#### 3. A través del disco duro

- a. Abra Equipo o Mi PC
  - De manera alternativa, haga clic en el icono del Explorador de archivos y seleccione el equipo
- b. Seleccione la unidad C:\ (o sistema de Windows)
- c. Haga clic con el botón secundario en la unidad que resaltó
- d. Haga clic en Activar BitLocker (NOTA: Se omitirá la pantalla inicial de BitLocker)

#### Windows 10

#### 1. A través del Menú de Inicio

- a. Haga clic en el botón del Menú de Inicio de Windows
- b. En el cuadro de búsqueda, escriba "Administrar BitLocker"
- c. Presione Intro o haga clic en el icono Administrar BitLocker en la lista

#### 2. A través del Panel de control

- a. Haga clic con el botón secundario en el Menú de Inicio de Windows
- b. Haga clic en el Panel de control
- c. Haga clic en Sistema y seguridad
- d. Haga clic en cualquiera de las opciones de Cifrado de unidad BitLocker

#### 3. A través de la configuración

a. Haga clic en el botón del Menú de Inicio de Windows

b. Haga clic en el icono de configuración

c. En el cuadro de búsqueda, escriba "Administrar BitLocker"

d. Presione Intro o haga clic en el icono Administrar BitLocker en la lista

4. A través del disco duro

a. Abra **Equipo** o **Mi PC** 

b. Seleccione la unidad C:\ (o sistema de Windows)

c. Haga clic con el botón secundario en la unidad que resaltó

d. Haga clic en Activar BitLocker (NOTA: Se omitirá la pantalla inicial de BitLocker)

4. En la pantalla de administración de BitLocker, haga clic en Activar BitLocker

¿Cómo activar o desactivar BitLocker con TPM en Windows? | Dell España

RitLocker Drive Encryption			-	×
🔶 🖂 🐇 🛧 🔍 Control Panel	> System and Security > BitLocker Drive Encryption v 0	Search Control Panel		,p
File Edit View Tools Help				
Control Panel Home	BitLocker Drive Encryption Help protect your files and folders from unauthorized access by protecting your drives with BitLocker. Operating system drive			U
	System (C) BitLocker off		$\odot$	
	Source Contraction Station			

5. BitLocker pasará por un proceso de inicialización reducido

_	/ //	
		×
• ÷	Ref BitLocker Drive Encryption (C:)	
ы	Charting Bitt order	
-	Starting BitLocker	
+	Please wait while BitLocker initializes the drive.	-
×		
e		
	What are Bitl or key's purteen requirements?	
	This are pricedule 5 system requirements:	
	Can	cel
_		

6. Seleccione una de las tres opciones para guardar la clave de recuperación

		×
(-	Ref BitLocker Drive Encryption (C:)	
	How do you want to back up your recovery key?	
	A recovery key can be used to access your files and folders if you're having problems unlocking your PC. It's a good idea to have more than one and keep each in a safe place other than your PC.	
	→ Save to your Microsoft account	
	→ Save to a file	
	$\rightarrow$ Print the recovery key	
	What is a recovery key?	
	Next Cancel	

Precaución: Esta clave debe guardarse en una ubicación segura. Si en algún momento

necesita acceder a la unidad, esta es la clave de recuperación que se usará para hacerlo. Si se pierde la clave de recuperación, no hay opción para recuperar datos de una unidad bloqueada y el sistema operativo deberá volver a instalarse. Esta clave es única para cada sistema y solo funcionará en el sistema para el que se creó.

BitLocker Recovery Key FC8EFCEF-33F3-40F0-8AE5-37CE3AD4030D - Notepad	-	0	$\times$
ile Edit Format View Help			
litlocker Drive Encryption recovery key			
To verify that this is the correct recovery key, compare the start of the following identifier with the identifier value displayed on your PC.			
Identifier:			
FC8EFCEF-53F3-40F0-8AE5-37CE3AD46300			
If the above identifier matches the one displayed by your PC, then use the following key to unlock your drive.			
lecovery Key:			
523787-716144-410300-132363-458865-458953-023155-580756			

If the above identifier doesn't match the one displayed by your PC, then this isn't the right key to unlock your drive. Try another recovery key, or refer to http://go.microsoft.com/fulink/RlinkID-260509 for additional assistance.

- Después de guardar el archivo de contraseña o clave, haga clic en Siguiente
- Seleccione una de las opciones de cifrado de volumen
  - a. Cifrado completo del disco duro
    - Esto cifrará todo el espacio en el disco duro, independientemente de si se utiliza o no. Esto demora más en procesar el cifrado.
  - b. Cifrado en el espacio utilizado
    - Esto solo cifrará el espacio en el disco duro que esté lleno de datos y dejará el espacio libre sin cifrar. Esto se prefiere para el cifrado básico que es más rápido.



- Después de seleccionar la opción de cifrado, haga clic en Siguiente
- Seleccione el tipo de cifrado que se utilizará si tiene la opción para seleccionar el tipo de cifrado
  - El modo nuevo es el método de cifrado preferido para los sistemas nuevos



- Haga clic en Next (Siguiente)
- Marque la casilla etiquetada como "Ejecutar la comprobación del sistema de BitLocker"



Continue	Cancel

- Haga clic en **Continue** (Continuar)
- Reinicie el equipo después de verificar la configuración para iniciar el cifrado

**NOTA:** El cifrado puede demorar entre 20 minutos y un par de horas dependiendo de la cantidad de datos que están siendo cifrados, la velocidad del sistema, y si el proceso fue interrumpido por haber apagado o suspendido el sistema.

• El cifrado de BitLocker no se iniciará hasta que se reinicie la computadora. Si tiene trabajo por finalizar, es seguro completarlo y guardarlo antes de reiniciar



#### Volver al principio

## 3. Comprobar el estado de BitLocker (administrar la consola de BitLocker)

- 1. Abra la consola de Administración de BitLocker mediante alguno de los métodos descritos anteriormente.
- 2. Vea el estado que se informa en la consola
  - a. Si está en proceso de cifrado, el estado mostrará que BitLocker está cifrando
  - b. Si terminó de cifrar, el estado mostrará que BitLocker está activado y mostrará un icono de bloqueo



#### Volver al principio

### 4. Verificar el estado de BitLocker (línea de comandos)

- 1. Abra una ventana del símbolo del sistema
  - a. Haga clic en el botón de Inicio de Windows, escriba "cmd" y presione Intro
  - b. Presione y mantenga presionado el botón de Windows y R en el teclado, escriba "cmd" y presione Intro
- 2. En el símbolo del sistema, escriba "manage-bde -status" y presione Intro
- 3. Vea el estado de BitLocker en las unidades del sistema

Adminis	trator Comm	and Promot							
Adminis	rator: comm	and Prompt	S						
Microsoft	Windows	[Version	10.0	.1058	6]				
1-1 0045		-			-1-6-		F		

(c) 2015 Microsoft Corporation. All rights reserved.

C:\Windows\system32>manage-bde -status BitLocker Drive Encryption: Configuration Tool version 10.0.10011 Copyright (C) 2013 Microsoft Corporation. All rights reserved.

Disk volumes that can be protected with BitLocker Drive Encryption: Volume C: [] [OS Volume]

Size:	465.21 GB
BitLocker Version:	2.0
Conversion Status:	Encryption in Progress
Percentage Encrypted:	97.9%
Encryption Method:	XTS-AES 128
Protection Status:	Protection Off
Lock Status:	Unlocked
Identification Field:	Unknown
Key Protectors:	
TPM	
Numerical Passwor	đ

### 5. Suspender BitLocker

**NOTA:** Es posible que se deba suspender BitLocker temporalmente para ciertas actualizaciones y mantenimiento del sistema. Cuando actualice el BIOS, SIEMPRE debe suspender BitLocker antes de ejecutar la actualización. Si BitLocker está activo durante la actualización, se PERDERÁN todas las claves de recuperación almacenadas en el TPM.

- 1. Inicie el sistema
- 2. Inicie en el sistema operativo Windows
- 3. Abra las ventanas Administrar BitLocker mediante alguno de los métodos anteriores.
- 4. Haga clic en Suspender protección para la unidad deseada



5. Lea el mensaje de advertencia y haga clic en Sí para suspender BitLocker



6. Vuelva a la ventana para Administrar BitLocker para Reanudar la protección

Operating system drive	
C: BitLocker suspended	
	Resume protection
	Back up your recovery key
	STurn off BitLocker

Volver al principio

### 6. Desactivar BitLocker

**NOTA:** El cifrado puede demorar entre 20 minutos y un par de horas dependiendo de la cantidad de datos que están siendo cifrados, la velocidad del sistema, y si el proceso fue interrumpido por haber apagado o suspendido el sistema. El progreso se puede verificar en cualquier momento mediante uno de los métodos anteriores para comprobar el estado de BitLocker.

1. Inicie el sistema

2. Inicie en el sistema operativo Windows

3. Abra las ventanas Administrar BitLocker mediante alguno de los métodos anteriores.

4. Haga clic en Desactivar BitLocker



5. Confirme la decisión de desactivar BitLocker



6. Deje que el sistema se descifre



### Volver al principio



Puede encontrar más información y soporte para los sistemas operativos Windows en nuestra Página Web de soporte de Windows.

ID del artículo: SLN302845 Última fecha de modificación: 09/04/2020 09:51

https://www.dell.com/support/article/es-es/sln302845/cómo-activar-o-desactivar-bitlocker-con-tpm-en-windows?lang=es