



LABORATORIO 1: BITLOCKER Y BITLOCKER TO GO

Por: Jesús Padilla Crespo

Laboratorio 1: BitLocker y BitLocker To Go

Introducción

El cifrado puede proteger los datos en el dispositivo haciendo que solo las personas con autorización tenga acceso a ellos. Si la función de cifrado no está disponible en su dispositivo, es posible que pueda activar el cifrado de BitLocker estándar en su lugar.

Nota: BitLocker solo está disponible en estas versiones de Windows:

- Ediciones Ultimate y Enterprise de Windows 7
- Ediciones Pro y Enterprise de Windows 8 y 8.1
- Ediciones Pro, Enterprise y Education de Windows 10

En esta práctica de laboratorio, debe activar el cifrado de BitLocker en una unidad de datos extraíble y en la unidad del sistema informático.

Instrucciones

Parte 1: Utilizar BitLocker To Go

En esta parte, utilizará BitLocker To Go para cifrar una unidad de almacenamiento extraíble.

Paso 1: Cifre la unidad extraíble.

- Inserte una unidad extraíble, por ejemplo, una unidad USB, en la computadora.
- BitLocker está desactivado de manera predeterminada y debe activarse para cada unidad que tenga que cifrar. Para activar y configurar BitLocker, navegue hasta el **Panel de control**, en la vista de iconos pequeños, haga clic en **Cifrado de unidad con BitLocker**.
- En **Unidades de datos extraíbles**, expanda la lista según sea necesario. Seleccione **Activar BitLocker** para la unidad extraíble deseada.

LAB-1 (F:) BitLocker desactivado



Activar BitLocker

- En la ventana **Elija cómo desea desbloquear esta unidad**, marque la casilla de verificación **Usar una contraseña para desbloquear la unidad** e ingrese una contraseña. Haga clic en **Siguiente** para continuar.

Elija cómo desea desbloquear la unidad

☒ Usar una contraseña para desbloquear la unidad

Las contraseñas deben contener mayúsculas y minúsculas, números, espacios y símbolos.

Escribir la contraseña


••••••••

Vuelva a escribir la contraseña

••••••••

- e. En **Cómo desea realizar una copia de seguridad de la clave de recuperación**, seleccione **Imprimir o Guardar en un archivo** y, luego, haga clic en **Siguiente**.

¿Cómo desea realizar la copia de seguridad de la clave de recuperación?

 Se guardó la clave de recuperación.

Si olvida la contraseña o pierde la tarjeta inteligente, puede usar la clave de recuperación para acceder a la unidad.

→ Guardar en la cuenta Microsoft

→ Guardar en un archivo

- f. En la ventana **Elegir qué cantidad de la unidad desea cifrar**, seleccione **Cifrar toda la unidad** y haga clic en **Siguiente**.

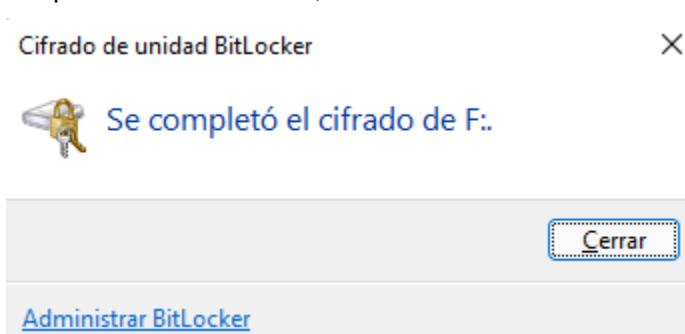
☒ Cifrar la unidad entera (más lento, pero mejor para unidades y PCs que ya se encuentran en uso)

- g. Si se abre la ventana **Elegir el modo de cifrado que desea usar**, seleccione **Modo compatible** y haga clic en **Siguiente** para continuar.

☒ Modo Compatible (recomendado para las unidades que se puedan mover de este dispositivo)

- h. En la ventana **¿Está listo para cifrar esta unidad?**, haga clic en **Iniciar cifrado**.

- i. Después de unos minutos, la unidad extraíble estará cifrada. Ahora puede extraerla.



Paso 2: Acceder a la unidad cifrada.

- Inserte la unidad extraíble que acabamos de cifrar en el paso anterior en el puerto USB de la computadora.

BitLocker (F:)

Escriba la contraseña para desbloquear esta unidad.

Más opciones

Desbloquear

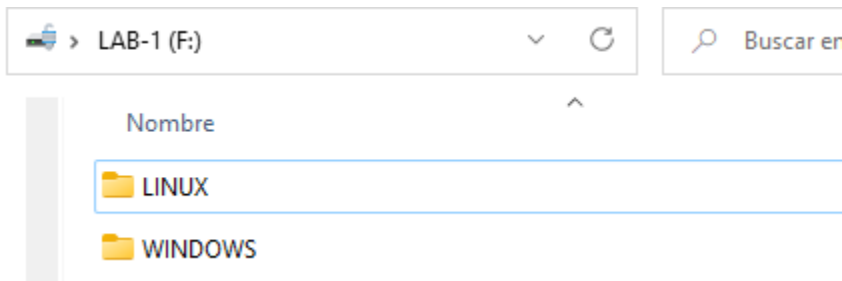
- Navegue hasta la unidad USB en el **Explorador de archivos** o **Windows Explorer** y abra la unidad USB. (Si no puede abrir la unidad USB, haga clic con el botón secundario en la unidad cifrada y en **Desbloquear unidad**).
- Haga clic en el botón **Más opciones**. Observe que hay una opción para ingresar la clave de recuperación. Si olvida la contraseña, se puede utilizar la clave de recuperación guardada o impresa en el paso anterior para desbloquear la unidad.

Pregunta:

¿Por qué es importante guardar una clave de recuperación de BitLocker?

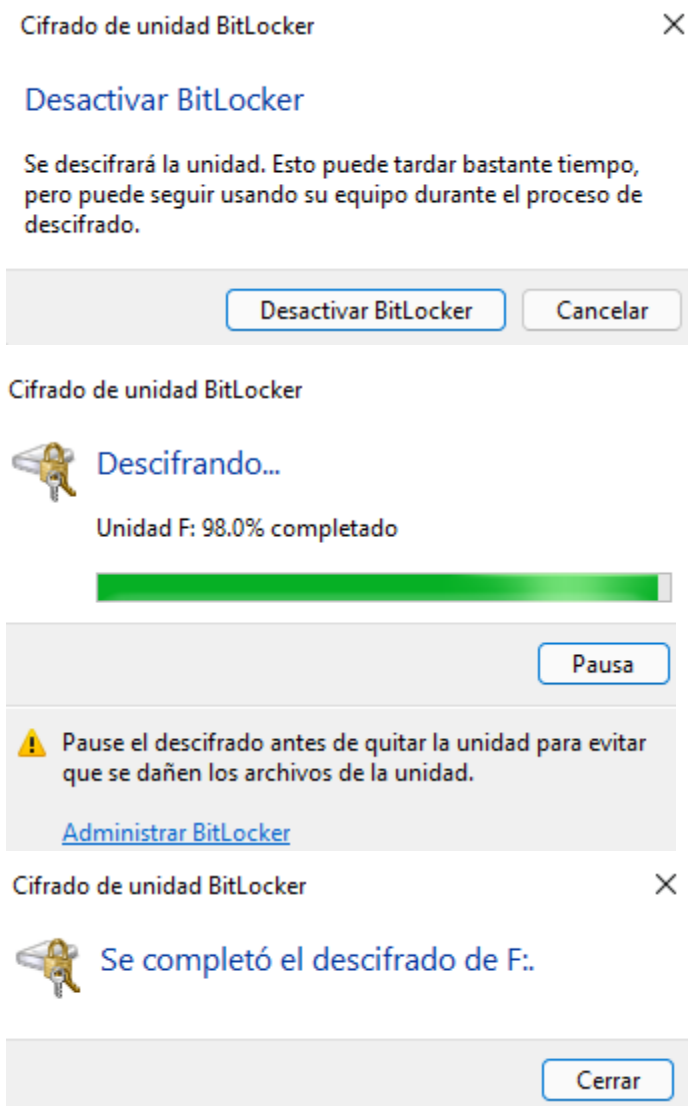
→ Como existe la posibilidad de olvidar una contraseña con el archivo de clave de recuperación añadimos un método seguro extra para poder desbloquear nuestra unidad en caso de haber olvidado la contraseña.

- Introduzca la contraseña para desbloquear la unidad USB. Ahora puede acceder al contenido de la unidad cifrada.



Paso 3: Descifrar el archivo.

- Navegue hasta el **Panel de control** y, en la vista de iconos pequeños, haga clic en **Cifrado de unidad con BitLocker**.
- Seleccione la unidad extraíble cifrada. Si la unidad está bloqueada, ingrese la contraseña para desbloquearla. Haga clic en **Desactivar BitLocker**.
- Haga clic en **Desactivar BitLocker** cuando reciba el mensaje que le notifica que el proceso de descifrado podría tardar algún tiempo. Observe el mensaje de advertencia para no dañar el contenido de la unidad.



- Haga clic en **Cerrar** cuando termine el proceso de descifrado.

Parte 2: Cifrar la unidad del sistema operativo

En esta parte de la práctica de laboratorio, utilizará BitLocker para cifrar la unidad del sistema operativo.

Paso 1: Active BitLocker.

- Vuelva al **Panel de control > Sistema y seguridad > Cifrado de unidad con BitLocker** para Activar BitLocker para la unidad del sistema operativo.
- En **Unidad de sistema operativo**, seleccione **Activar BitLocker**.

Unidad de sistema operativo

"DISCO DURO" (C:) BitLocker desactivado



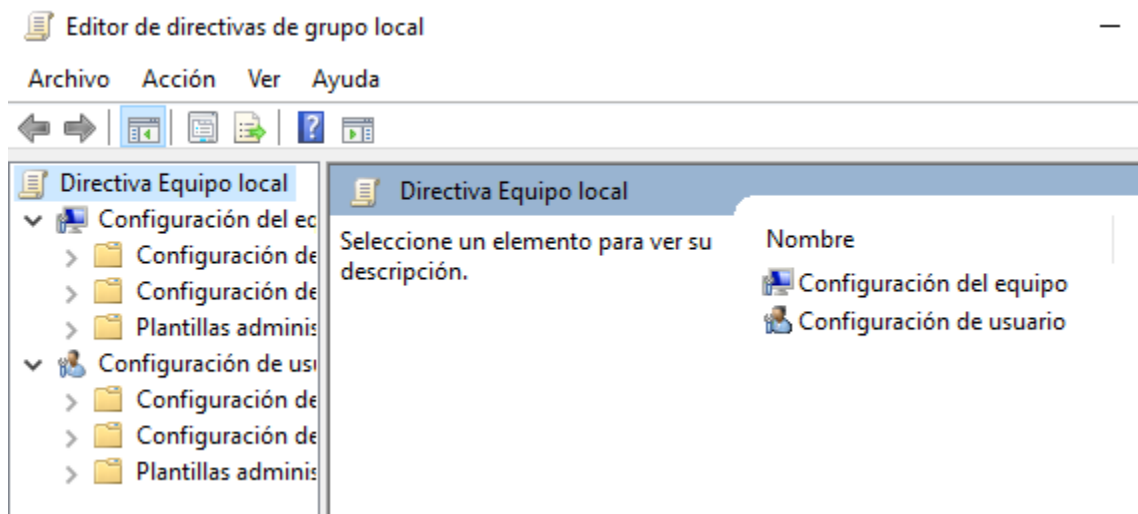
Activar BitLocker

Nota: Si aparece un mensaje de error que indica que el dispositivo no puede utilizar un módulo de plataforma confiable, deben seguirse algunos pasos adicionales para permitir la autenticación adicional en el inicio. Haga clic en **Cancelar** y siga estos pasos adicionales:

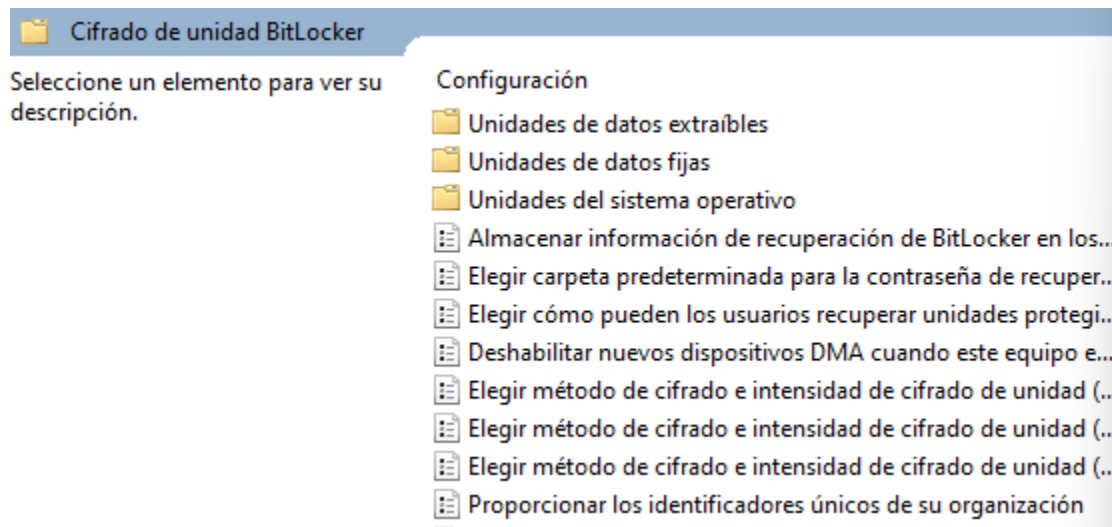
Iniciando BitLocker

- ❌ 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.

- Escriba **gpedit.msc** en el cuadro de **búsqueda de Windows** para abrir el **Editor de políticas de grupo locales**.



- 2) Expanda **Plantillas administrativas** en el panel izquierdo y haga clic en **Componentes de Windows**.
- 3) En la lista de componentes de Windows, seleccione **Cifrado de unidad con BitLocker**. Seleccione **Unidades de sistema operativo**. Seleccione **Requerir autenticación adicional en el arranque**.



- 4) Dentro de la ventana **Requerir autenticación adicional en el arranque**, seleccione el botón **Activado**, luego, haga clic en **Aplicar** y en **Aceptar** para cerrar la ventana.

Requerir autenticación adicional al iniciar

Requerir autenticación adicional al iniciar

Valor anterior Valor siguiente

☐ No configurada Comentario:

☒ Habilitada

☐ Deshabilitada

Compatible con: Al menos Windows Server 2008 R2 o Windows 7

Opciones:

Ayuda:

Permitir BitLocker sin un TPM compatible
☒ (requiere contraseña o clave de inicio en una unidad flash USB)

Opciones para equipos con un TPM:

Configurar inicio del TPM:
Permitir TPM

Configurar PIN de inicio del TPM:
Permitir PIN de inicio con TPM

Configurar clave de inicio del TPM:
Permitir clave de inicio con TPM

Configurar la clave de inicio y el PIN del TPM:

Esta configuración de directiva te permite configurar si BitLocker requiere autenticación adicional cada vez que se inicia el equipo y si se usa BitLocker con un Módulo de plataforma segura (TPM). Esta configuración de directiva se aplica al activar BitLocker.


Nota: al iniciar, solo se puede solicitar una de las opciones de autenticación adicional; de lo contrario, se produce un error de directiva.

Si deseas usar BitLocker en un equipo sin un TPM, activa la casilla "Permitir BitLocker sin un TPM compatible". En este modo, se requiere o bien contraseña o una unidad USB para iniciar. Cuando se usa una clave de inicio, la información de clave usada para cifrar la unidad se almacena en la unidad USB, creando una clave USB. Cuando se inserta la clave USB se autentica el acceso a la unidad, que queda accesible. Si la clave USB no está accesible o se pierde, o si olvidas la contraseña, será necesario usar una de las opciones de recuperación de BitLocker para tener acceso a la unidad.


Activar Windows
Ve a Configuración para activar Windows.

Aceptar Cancelar Aplicar

- 5) Cierre el **Editor de políticas de grupo locales** para volver a la ventana **Cifrado de unidad con BitLocker** y haga clic en **Activar BitLocker**.

←  Cifrado de unidad BitLocker (C:)

Elija como desbloquear la unidad en el inicio

 El administrador del sistema administra ciertas configuraciones.

Para aumentar la seguridad de los datos, puede hacer que BitLocker le pida escribir una contraseña o insertar una unidad flash USB cada vez que inicia su PC.

→ Inserte una unidad flash USB

→ Escribir una contraseña

- c. Se abrirá la ventana **Elegir cómo desea desbloquear esta unidad**. En esta ventana, marque la casilla de verificación **Usar una contraseña para desbloquear la unidad**, seleccione **Introducir una contraseña** y, a continuación, introduzca una contraseña y haga clic en **Siguiente**.
- d. En **¿Cómo desea realizar una copia de seguridad de la clave de recuperación?**, seleccione **Imprimir** o **Guardar en un archivo** y, luego, haga clic en **Siguiente**.
- e. En la ventana **Elegir qué cantidad de la unidad desea cifrar**, seleccione **Cifrar solo el espacio utilizado en disco** y haga clic en **Siguiente**.

 Cifrado de unidad BitLocker (C:)

Elegir qué cantidad de la unidad desea cifrar

Si está instalando BitLocker en una unidad nueva o un equipo nuevo, solo es necesario cifrar la parte de la unidad que se está usando actualmente. BitLocker cifrará los datos nuevos automáticamente conforme los agregue.

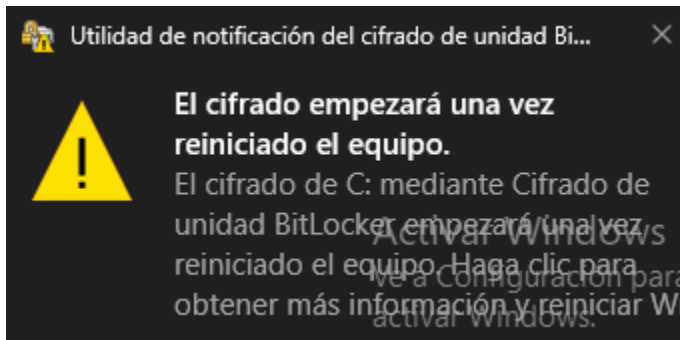
Si están instalando BitLocker en un equipo o una unidad que ya se está usando, entonces cifre la unidad completa. Al cifrar la unidad completa, se asegura de que todos los datos están protegidos, incluso datos que haya podido eliminar pero que aún puedan contener información recuperable.

☒ Cifrar solo el espacio en disco utilizado (mejor y más rápido para unidades y equipos nuevos)

- f. En la ventana **Elegir el modo de cifrado que desea usar**, seleccione **Nuevo modo de cifrado** y haga clic en **Siguiente**.

☒ Modo de cifrado nuevo (recomendado para las unidades fijas en este dispositivo)

- g. En la ventana **¿Está listo para cifrar esta unidad?**, asegúrese de que la casilla de verificación **Ejecutar sistema de BitLocker** esté seleccionada y haga clic en **Continuar**. Aparecerá un mensaje que indica que se debe reiniciar la computadora.



- h. Haga clic en **Reiniciar ahora** para reiniciar la computadora.
- i. Cuando se reinicie la computadora, se le solicitará que ingrese su contraseña para desbloquear la computadora.

Pregunta:

¿Cuál es la función de un TPM en relación con BitLocker?

→ Se trata de hardware cuya función principal es generar y comprobar claves criptográficas de manera segura que utilizará BitLocker para cifrar unidades. (Este hardware sólo es compatible con algunos dispositivos, aunque en la actualidad se está implementando una ley a las empresas que fabrican dispositivos para tener unas condiciones de seguridad obligatorias).

Paso 2: Desactive BitLocker.

- a. Para desactivar BitLocker, vuelva al **Panel de control > Sistema y seguridad > Cifrado de unidad con BitLocker**, y seleccione **Desactivar BitLocker**.
- b. Haga clic en **Desactivar BitLocker** para descifrar la unidad. Según el tamaño de la unidad, este proceso puede demorar un poco.

Unidad de sistema operativo

C: BitLocker desactivado



 **Activar BitLocker**