LIEBHERR

Configuración Bitlocker

Contenido

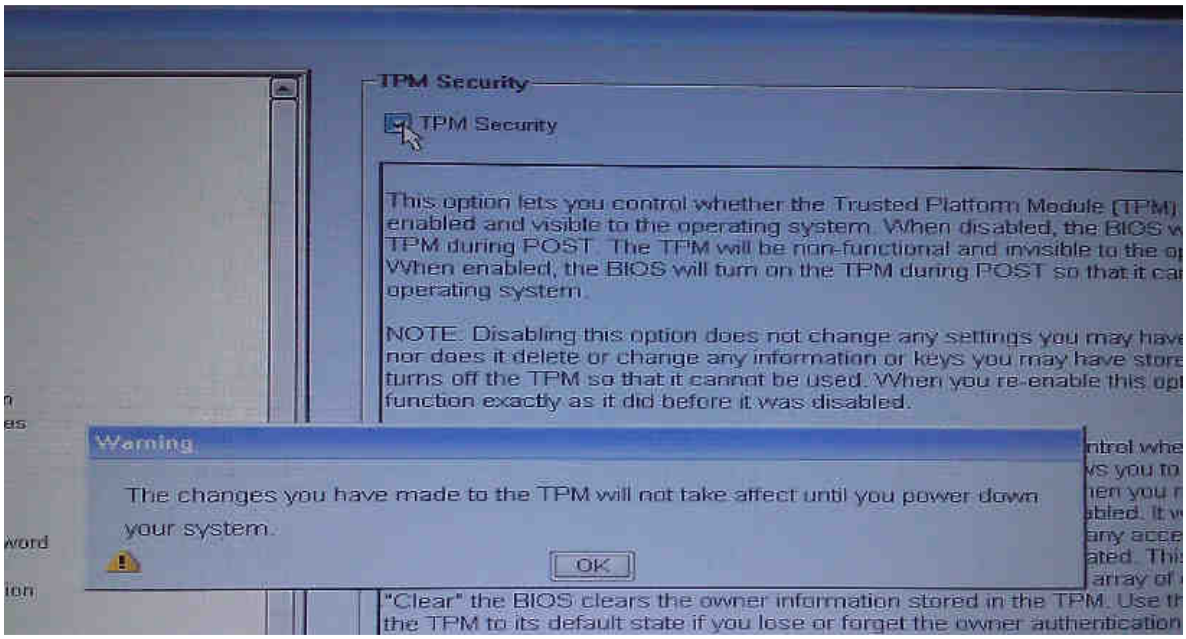
Preparación Equipo

Requisitos SO

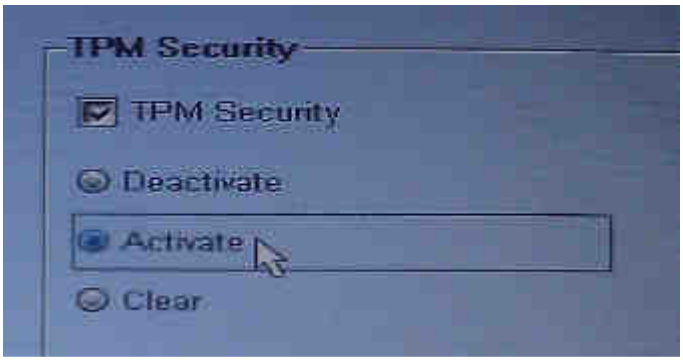
Sistema de encriptación válido sólo en computadores con módulo TPM y Windows 7 Ultimate/Enterprise, para todas las otras combinaciones se debe aplicar encriptación con McAfee (5.2.10).

Ajustes BIOS

Activar módulo en Settings > Security > TPM Security



Reiniciar el computador y activar la opción de seguridad para su uso:

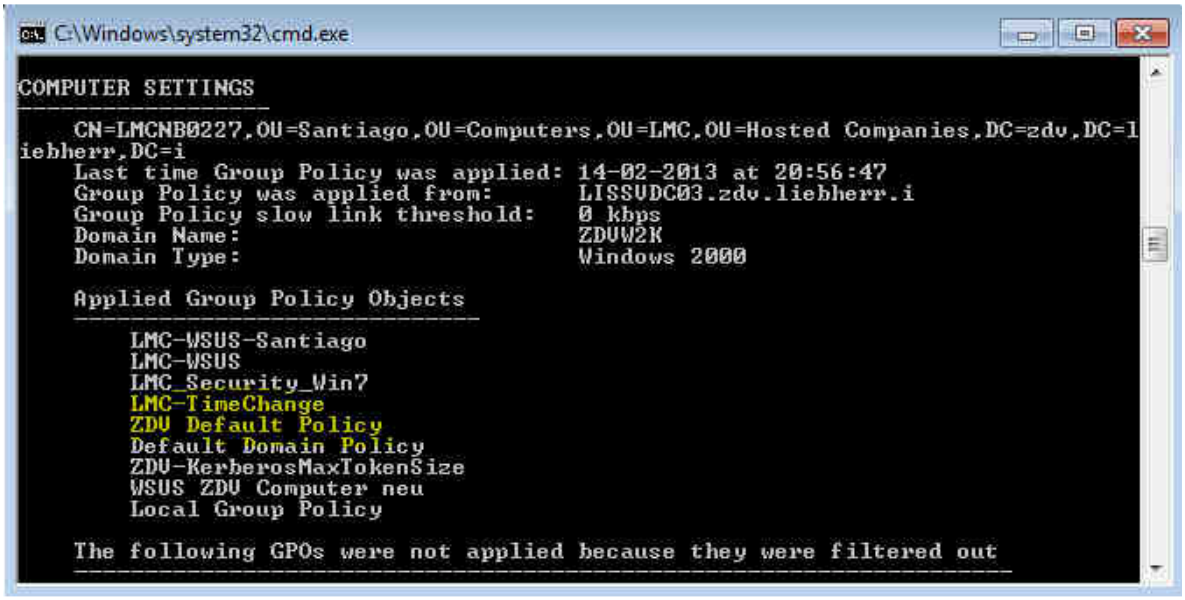


Ajustes Windows

Validar que se encuentra aplicado al menos uno de estos GPO en el computador:

- “ZDV Default Policy”, o
- “LMC-TimeChange”

Esto para que se cumpla el almacenamiento de la clave de seguridad en AD y manejo de bitlocker por parte de Windows, según política de seguridad de encriptación de computadores (ver apéndice A de ese documento).



Configuración que está en GPO:

System/Trusted Platform Module Services

Policy	Setting
Turn on TPM backup to Active Directory Domain Services	Enabled
Require TPM backup to AD DS	Enabled
If selected, cannot set or change TPM owner password if backup fails (recommended default). If not selected, can set or change TPM owner password even if backup fails. Backup is not automatically retried.	

Windows Components/BitLocker Drive Encryption

Policy	Setting	Comment
Store BitLocker recovery information in Active Directory Domain Services (Windows Server 2008 and Windows Vista)	Enabled	
Require BitLocker backup to AD DS	Enabled	
If selected, cannot turn on BitLocker if backup fails (recommended default). If not selected, can turn on BitLocker even if backup fails. Backup is not automatically retried.		
Select BitLocker recovery information to store:	Recovery passwords and key packages	
A recovery password is a 48-digit number that unlocks access to a BitLocker-protected drive. A key package contains a drive's BitLocker encryption key secured by one or more recovery passwords Key packages may help perform specialized recovery when the disk is damaged or corrupted.		

Windows Components/BitLocker Drive Encryption/Fixed Data Drives		
Policy	**Setting**	**Comment**
Choose how BitLocker-protected fixed drives can be recovered	Enabled	
Allow data recovery agent	Enabled	
Configure user storage of BitLocker recovery information:		
	Allow 48-digit recovery password	
	Allow 256-bit recovery key	
Omit recovery options from the BitLocker setup wizard	Enabled	
Save BitLocker recovery information to AD DS for fixed data drives	Enabled	
Configure storage of BitLocker recovery information to AD DS:	Backup recovery passwords and key packages	
Do not enable BitLocker until recovery information is stored to AD DS for fixed data drives	Enabled	

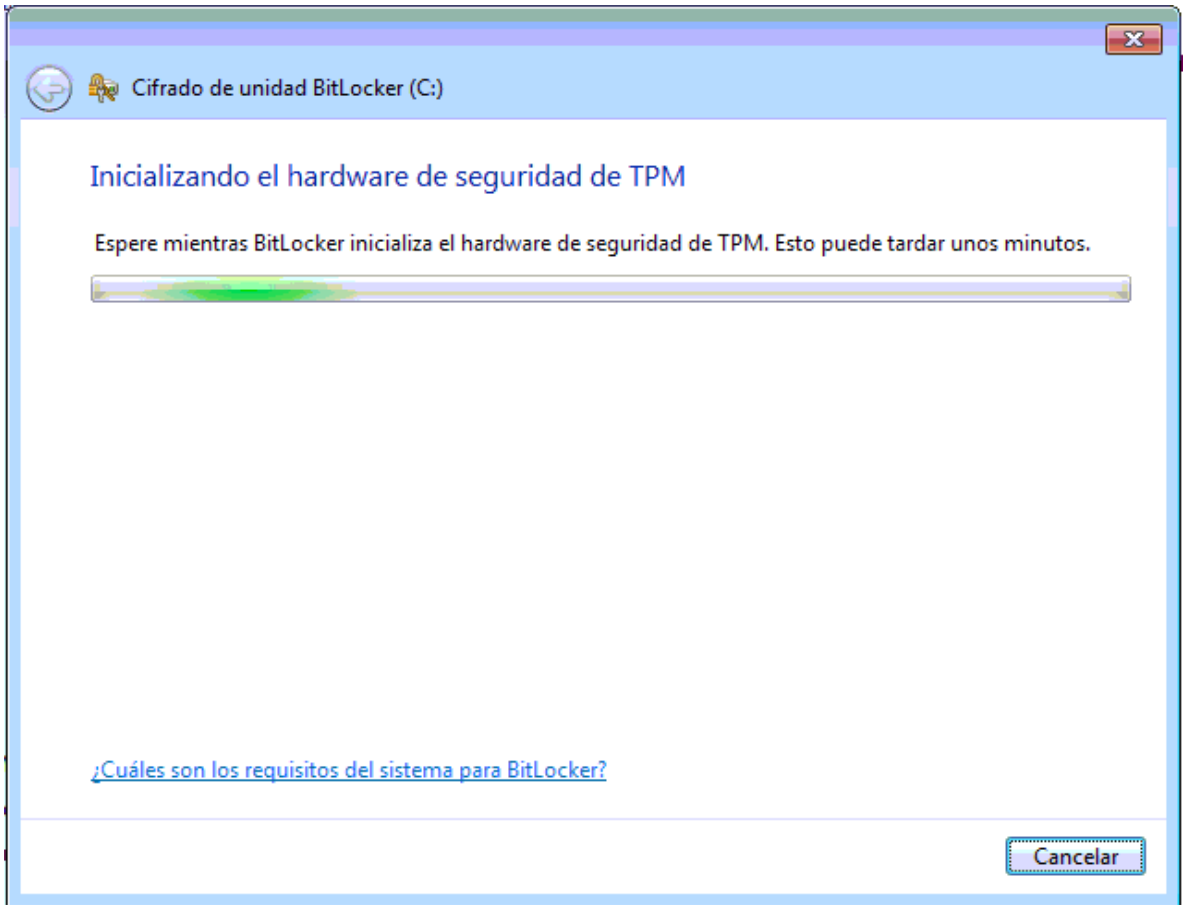
Windows Components/BitLocker Drive Encryption/Operating System Drives		
Policy	**Setting**	**Comment**
Choose how BitLocker-protected operating system drives can be recovered	Enabled	
Allow data recovery agent	Enabled	
Configure user storage of BitLocker recovery information:		
	Allow 48-digit recovery password	
	Allow 256-bit recovery key	
Omit recovery options from the BitLocker setup wizard	Enabled	
Save BitLocker recovery information to AD DS for operating system drives	Enabled	
Configure storage of BitLocker recovery information to AD DS:	Store recovery passwords and key packages	
Do not enable BitLocker until recovery information is stored to AD DS for operating system drives	Enabled	

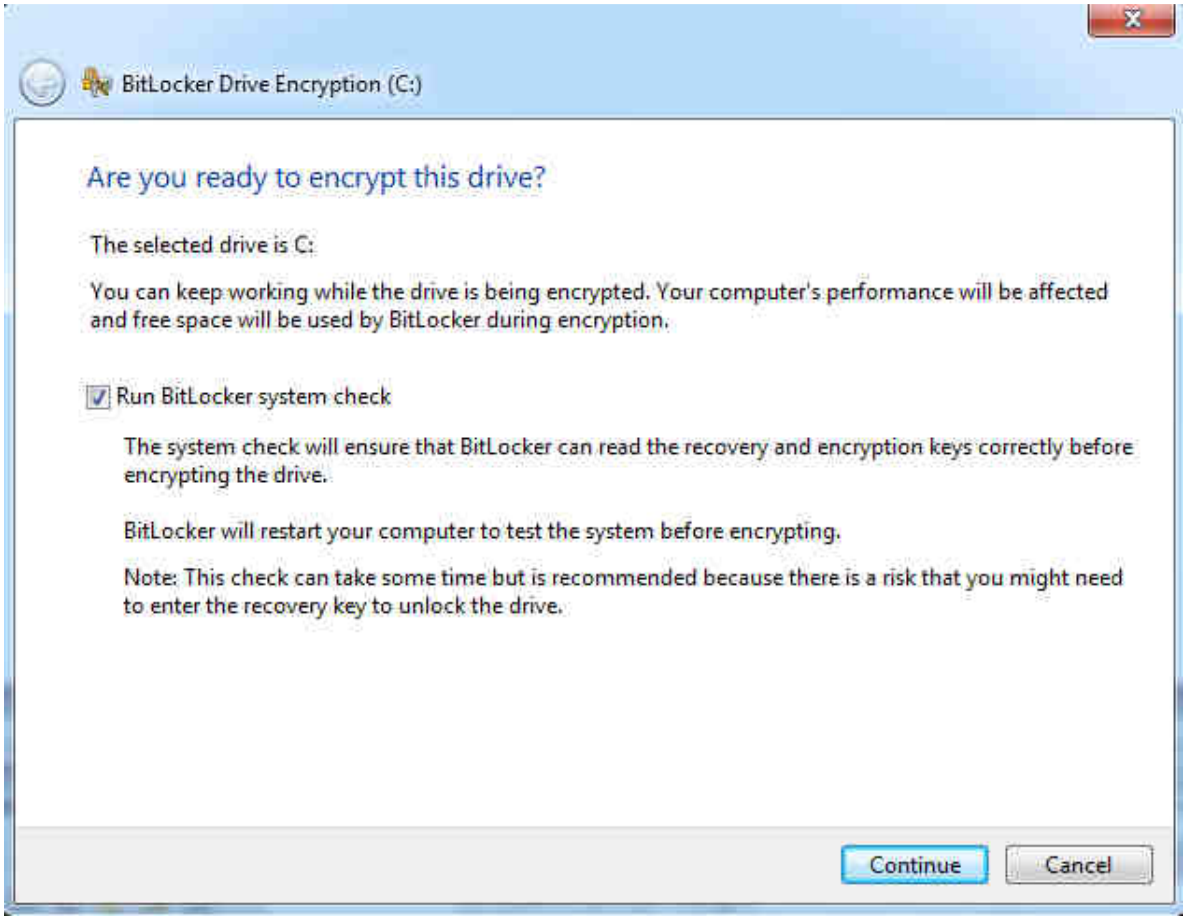
Luego de la validación de parámetros en el computador, recién se está en condiciones de activar el cifrado usando Bitlocker.

Activación de Bitlocker

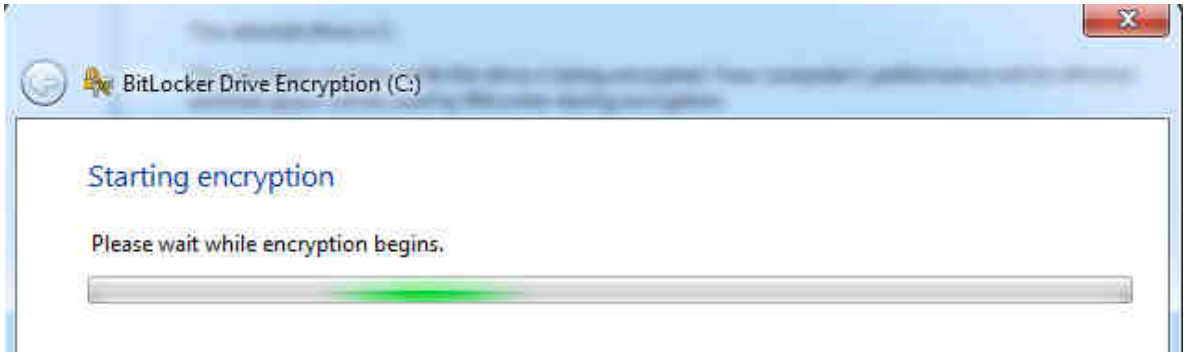
Para poder respaldar la información inicial de Bitlocker, es necesario que antes de iniciar se conecte el computador a la red.
Para activar Bitlocker, ir a Panel de Control > Cifrado de unidad Bitlocker > Activar Bitlocker

Activar Bitlocker y seleccionar la opción de validación, reiniciar cuando lo solicite.

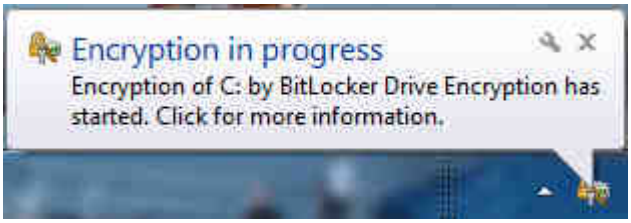


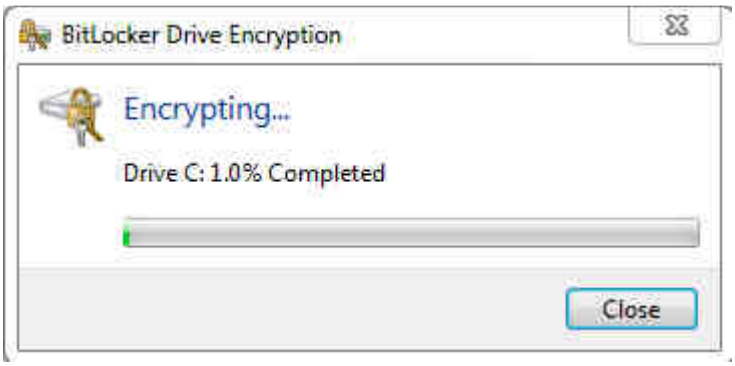

BitLocker Drive Encryption (C:)
Are you ready to encrypt this drive?
The selected drive is C:
You can keep working while the drive is being encrypted. Your computer's performance will be affected and free space will be used by BitLocker during encryption.
Run BitLocker system check
The system check will ensure that BitLocker can read the recovery and encryption keys correctly before encrypting the drive.
BitLocker will restart your computer to test the system before encrypting.
Note: This check can take some time but is recommended because there is a risk that you might need to enter the recovery key to unlock the drive.
Continue
Cancel


BitLocker Drive Encryption
The computer must be restarted
Restart now
Restart later

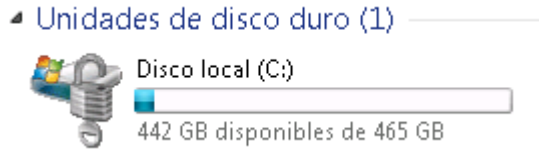

BitLocker Drive Encryption (C:)
Starting encryption
Please wait while encryption begins.

Luego del reinicio comenzará el cifrado del disco, esperar hasta que finalice.

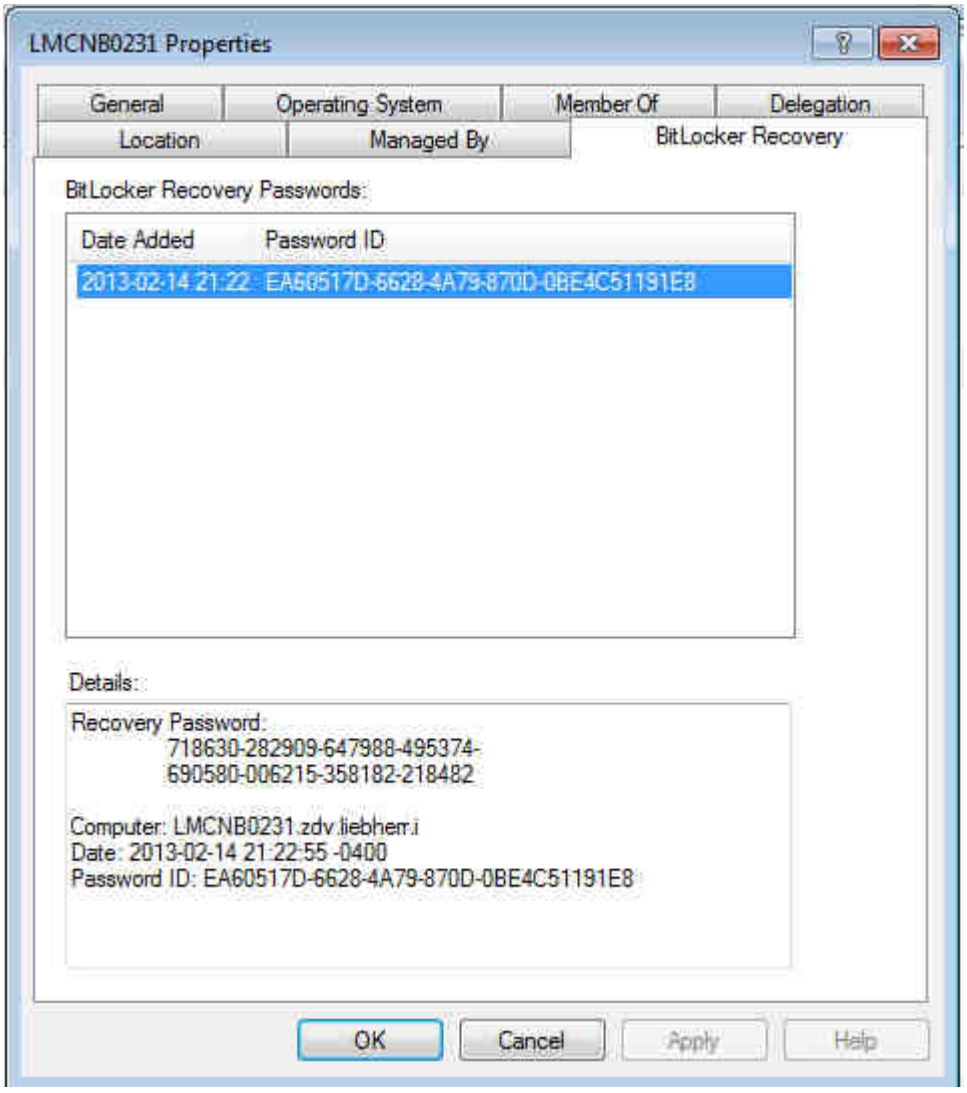




La imagen del disco cambiará en el explorador, ahora mostrará un candado.



La información de seguridad de la encriptación queda almacenada en el módulo TPM del computador y en la información del computador en el directorio (AD).



Configuraciones adicionales

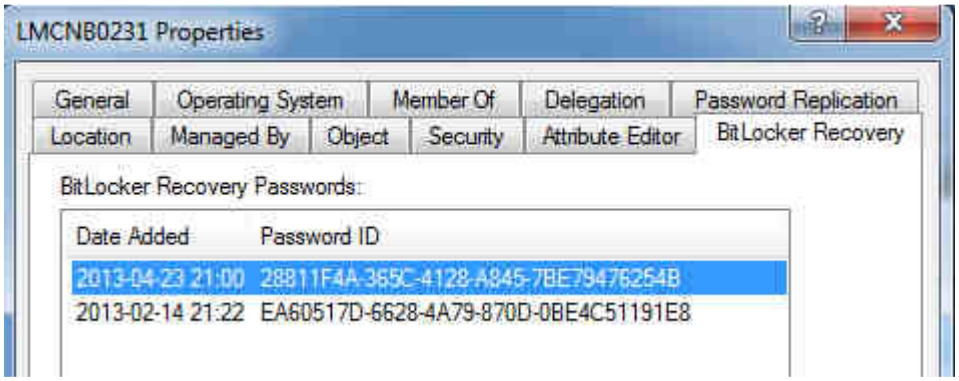
Respaldar manualmente clave de bitlocker en AD

En el caso de que no se haya respaldado la clave o al cambiar de nombre un computador registrado previamente en el dominio, se debe manualmente respaldar la clave en el directorio.
Para respaldar:

- Abrir consola como administrador.
- Ejecutar comando **"manage-bde –protectors –get C:"** para obtener el ID de la contraseña.

- Ejecutar comando **“manage-bde –protectors –adbackup C: -id <id contraseña obtenida anteriormente>”**

Ejemplo: Cambio de nombre en computador (TAG B6773R1) desde LMCNB0231 a LMCNB0232 para evitar conflictos con otro computador registrado con el mismo nombre.
Esto se debe realizar ya que el antiguo registro de bitlocker en AD para LMCNB0231 es reemplazado por la nueva publicación (nuevo computador con el mismo nombre).



Luego de cambiar el nombre del computador antiguo a LMCNB0232, su información de bitlocker no queda almacenada como corresponde en el directorio aunque ya esté encriptado. Esto sucede debido a que Windows traspasa esa información sólo al momento de encriptar.

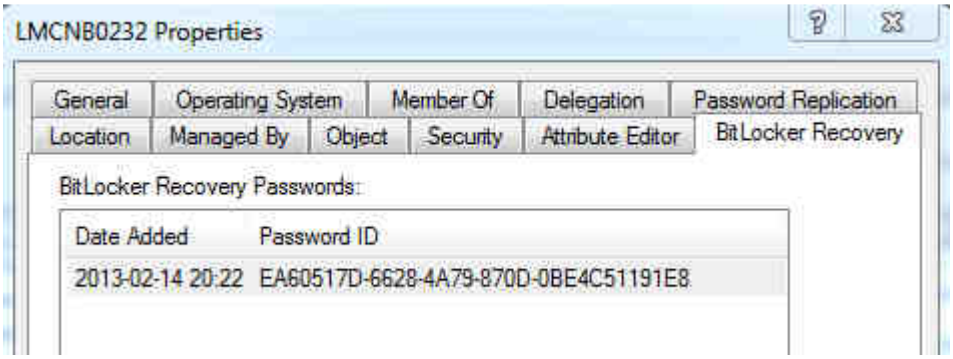
Para recuperar la información del computador y publicar, se debe abrir consola como administrador y ejecutar comando **“manage-bde –protectors –get C:”**

```
C:\>manage-bde -protectors -get c:
Cifrado de unidad BitLocker: versión de la herramienta de configuración 6.1.7601

Copyright (C) Microsoft Corporation. Reservados todos los derechos.

Volumen C: []
Todos los protectores de clave

    TPM:
      Id.: {E56E8C53-8046-4F64-A388-82E95D0F0E8C}

    Contraseña numérica:
      Id.: {EA60517D-6628-4A79-870D-0BE4C51191E8}
      Contraseña:
        718630-282909-647988-495374-690580-006215-358182-218482
```

En este caso, para publicar la información en AD se debe ejecutar el comando **"manage-bde –protectors –adbackup C: -id {EA60517D-6628-4A79-870D-0BE4C51191E8}"**. Cómo el código alfa numérico es largo, se recomienda copiar directo desde la consola (clic derecho > marcar > copiar > presionar enter) y luego pegar (clic derecho > pegar):

```
C:\>manage-bde -protectors -adbackup C: -id {EA60517D-6628-4A79-870D-0BE4C51191E
8}
Cifrado de unidad BitLocker: versión de la herramienta de configuración 6.1.7601

Copyright (C) Microsoft Corporation. Reservados todos los derechos.

Se hizo una copia de seguridad correcta de la información de recuperación en Act
ive Directory.
```

La fecha con la que queda el registro, corresponde a la fecha de creación de la clave en el computador, no a la fecha de publicación en el directorio.



Desactivar Bitlocker

Acá se presentan dos opciones, el suspender sin desencriptar y la desencriptación del disco.

Suspender Protección

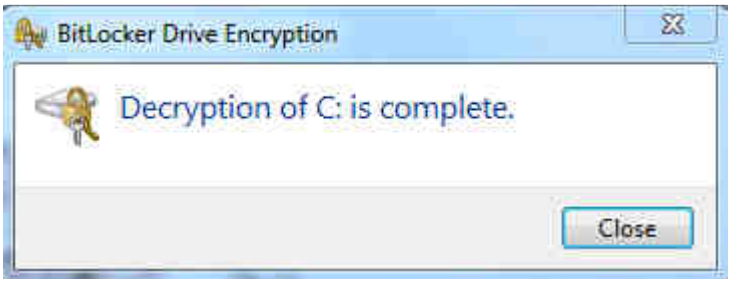
En el caso de necesitar hacer ajustes en la placa o actualizaciones de la BIOS luego de haber encriptado se debe suspender el uso del bitlocker, esto no desencripta el disco, sino que deja en espera la restricción hasta que se terminen los ajustes, luego se debe volver a activar para recuperar el estado de protección normal.
Para suspender, ir a Panel de Control > Cifrado de unidad Bitlocker > Suspender Bitlocker

Aceptar el mensaje y hacer los cambios que se necesiten.

Al finalizar los cambios se debe ingresar nuevamente al panel de control y presionar “Reactivar Protección”, mientras no se active esa opción los datos no estarán correctamente protegidos.

Desencriptar

En el caso de necesitar desencriptar la información y no sólo suspender momentáneamente el cifrado, ir a Panel de control > Bitlocker > Apagar bitlocker, eso desencripta el disco por lo que demora un tiempo en finalizar.



Luego de eso los datos están sin encriptar

Cambio de placa madre / nuevo módulo TPM

Al hacer cambio de placa se debe cambiar la referencia de protección en Windows, donde dicho proceso de cambio de referencias comienza desde antes del cambio del hardware como tal.
Este cambio de hardware no implica la necesidad de desencriptar el disco, es posible hacer el cambio de forma rápida siguiendo estos pasos:

- Antes de cambiar el hardware, ingresar a Windows
- Abrir consola como administrador.
- Ejecutar comando “manage-bde –protectors –get C:” para obtener el id y la contraseña
    - Repetir este paso para todas las unidades encriptadas.
- Apagar computador
- Cambiar placa
- Encender computador e ingresar a la BIOS
- Activar módulo TPM, cambiar estado a “activo”
- Continuar inicio de windows. Acá se pedirá la clave de bitlocker, ingresar la anotada previamente
- Ir al panel de control > bitlocker > administrar TPM
    - Inicializar TPM usando contraseña automática
- Abrir consola como administrador.
- Ejecutar comando “manage-bde -protectors -delete C: -type tpm” para eliminar los datos antiguos
- Ejecutar comando “manage-bde -protectors -add C: -tpm” para registrar los datos nuevos

En el caso de que el cambio de placa sea porque ya no funciona y no es posible obtener copia de la clave de bitlocker, consultar por la información respaldada en el directorio para el computador específico.

Ejemplo:
Cambio de disco duro de un computador a uno nuevo manteniendo los datos del disco.
Por problemas de hardware se realiza cambio completo de computador, para evitar reconfigurar se cambia el disco duro del computador antiguo al nuevo.

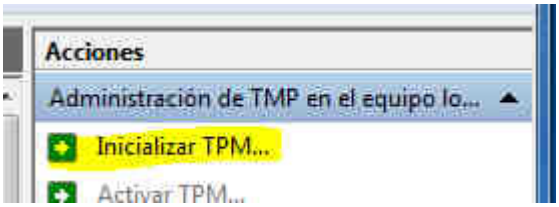
Desde el computador antiguo, se almacenan los datos de la contraseña de bitlocker donde sólo está la unidad C. Para tal efecto, se ejecuta el comando “**manage-bde –protectors –get C:”**

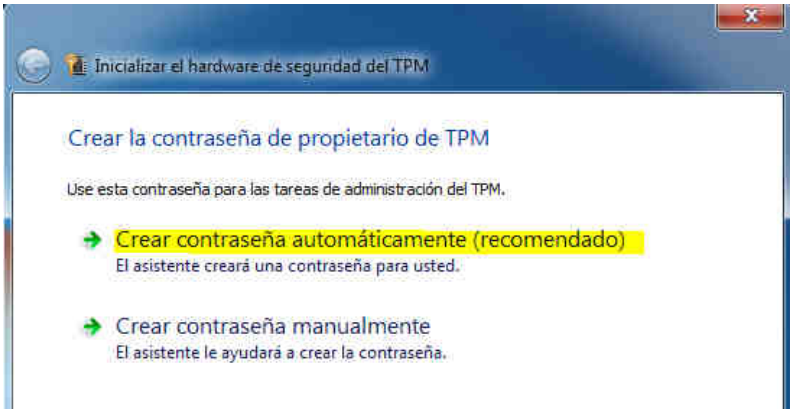
```
C:\Windows\system32>manage-bde -protectors -get C:
Cifrado de unidad BitLocker: versión de la herramienta de configuración 6.1.7601

Copyright (C) Microsoft Corporation. Reservados todos los derechos.

Volumen C: []
Todos los protectores de clave

    TPM:
      Id.: {3C6839BB-50D9-47D4-9426-322A50B7C01B}

    Contraseña numérica:
      Id.: {58D7A120-AC00-47A5-943A-C37205FAF5FE}
      Contraseña:
        067738-063833-671231-709357-083842-661705-428428-345499
```

Se apaga el computador y se mueve el disco al nuevo computador.
Se enciende el nuevo computador y se ingresa a la BIOS para activar el módulo TPM, se guardan los cambios y se continúa con el inicio de Windows.
Al encontrar un nuevo TPM, Windows solicita la contraseña de desbloqueo de bitlocker, acá se ingresan los datos rescatados anteriormente:

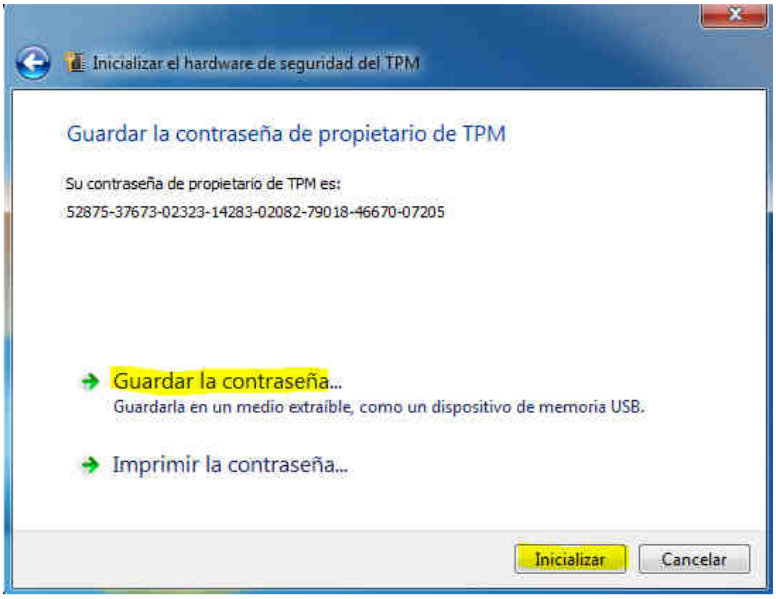
067738-063833-671231-709357
083842-661705-428428-345499

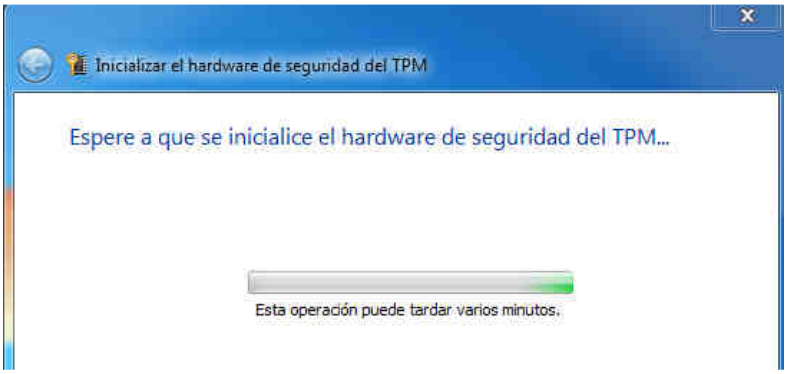
Al ingresar a Windows se abre la opción de administrar TPM desde Panel de control > Cifrado de unidad Bitlocker y se inicializa.

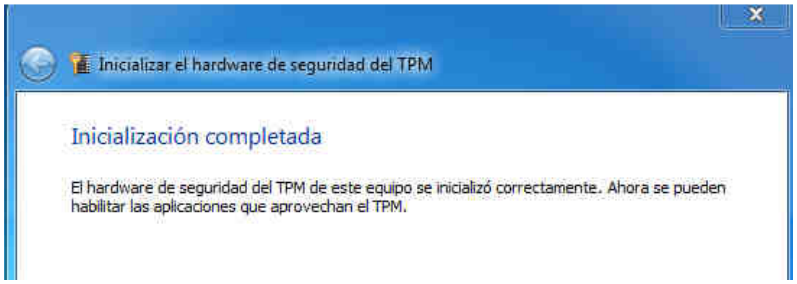




Al finalizar la creación, sólo es posible continuar si se guarda o imprime la contraseña creada.







Al terminar el proceso de inicialización de TPM, se debe cambiar la referencia de bitlocker para que utilice este nuevo TPM.
Desde consola de administrador se ejecutan los comandos de eliminación y respaldo:

manage-bde -protectors -delete C: -type tpm

```
C:\Windows\system32>manage-bde -protectors -delete C: -type tpm
Cifrado de unidad BitLocker: versión de la herramienta de configuración 6.1.7601

Copyright (C) Microsoft Corporation. Reservados todos los derechos.

Volumen C: []
Protectores de clave de tipo TPM

    TPM:
      Id.: {3C6839BB-50D9-47D4-9426-322A50B7C01B}

Se eliminó el protector de clave con el identificador "{3C6839BB-50D9-47D4-9426-
322A50B7C01B}".
```

manage-bde -protectors -add C: -tpm

```
C:\Windows\system32>manage-bde -protectors -add C: -tpm
Cifrado de unidad BitLocker: versión de la herramienta de configuración 6.1.7601

Copyright (C) Microsoft Corporation. Reservados todos los derechos.

Protectores clave agregados:

    TPM:
      Id.: {DD5D2AD8-256C-43A4-94D9-9C6CCA134DB2}
```

Para validar que el nuevo TPM quedó asociado de forma correcta:

manage-bde –protectors –get C:

```
C:\Windows\system32>manage-bde -protectors -get C:
Cifrado de unidad BitLocker: versión de la herramienta de configuración 6.1.7601

Copyright (C) Microsoft Corporation. Reservados todos los derechos.

Volumen C: []
Todos los protectores de clave

    Contraseña numérica:
      Id.: {58D7A120-AC00-47A5-943A-C37205FAF5FE}
      Contraseña:
        067738-063833-671231-709357-083842-661705-428428-345499

    TPM:
      Id.: {DD5D2AD8-256C-43A4-94D9-9C6CCA134DB2}
```

Ahí se puede confirmar que se mantienen intactos los datos de bitlocker y que tiene asociado el nuevo TPM (ID DD5D2AD8-256C-43A4-94D9-9C6CCA134DB2).
Luego de lo anterior es posible reiniciar sin tener que volver a escribir la contraseña de bitlocker cada vez que parta Windows.

Errores

Problemas en el disco

Ejecutar comando y reiniciar, luego de eso debiera continuar la encriptación.

Módulo TPM desactivado / no reconocido

En algunos casos al tratar de activar bitlocker Windows indica que no es posible acceder a la información del módulo TPM por estar desactivado, de ser así ir a la BIOS y verificar que el módulo se encuentra en modo activo, en caso de estarlo previamente, probar limpiar el módulo (opción “clear”) y volver a tratar de activar Bitlocker. Posiblemente luego de eso Windows mande un mensaje al módulo haciendo que aparezca un texto en el próximo reinicio pidiendo confirmación de la activación, tal como muestra la imagen:

Presionar F10 para activar.