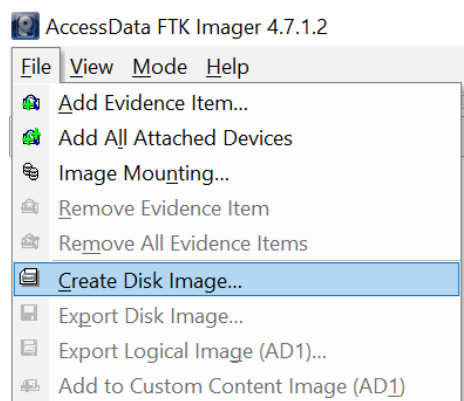


Práctica 4

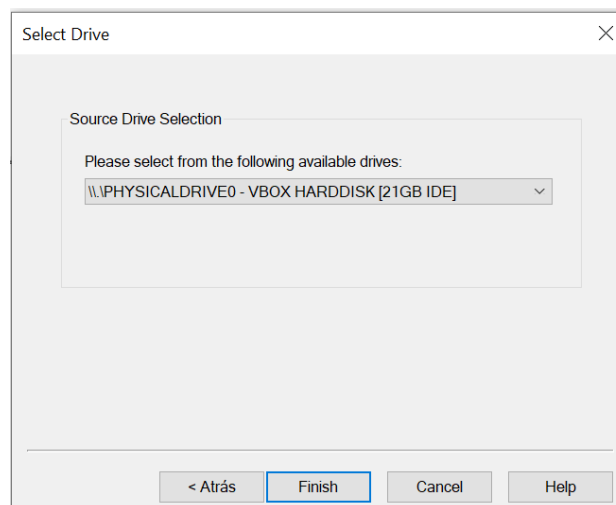
Adquisición de evidencia en maquina encendida

Nos enfrentamos a una situación en la que tenemos un ordenador encendido y no estamos seguros de poder acceder a él nuevamente si lo apagamos. En este contexto, llevamos a cabo la adquisición de evidencia en caliente con el equipo encendido, utilizando para ello el programa FTK Imager Lite.

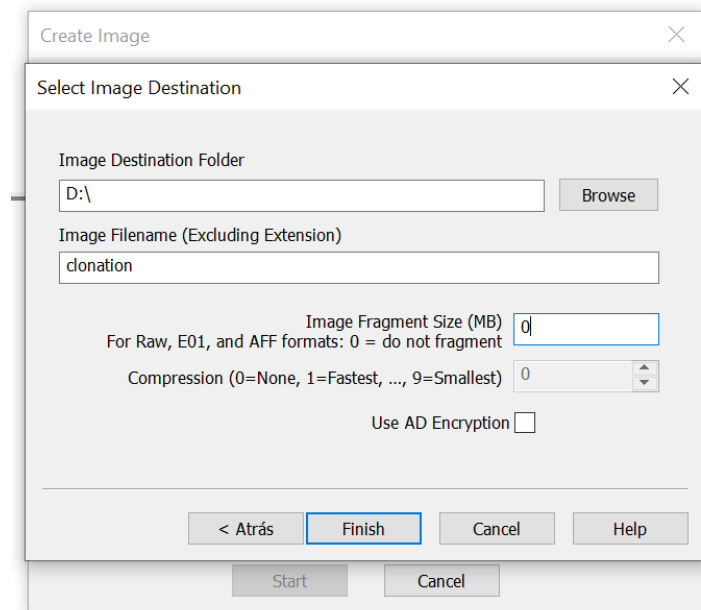
Este programa es portable, lo que significa que podemos llevarlo en un USB. Una vez que lo hemos abierto, nos dirigimos a la opción “**File > Create Disk Image...**”.



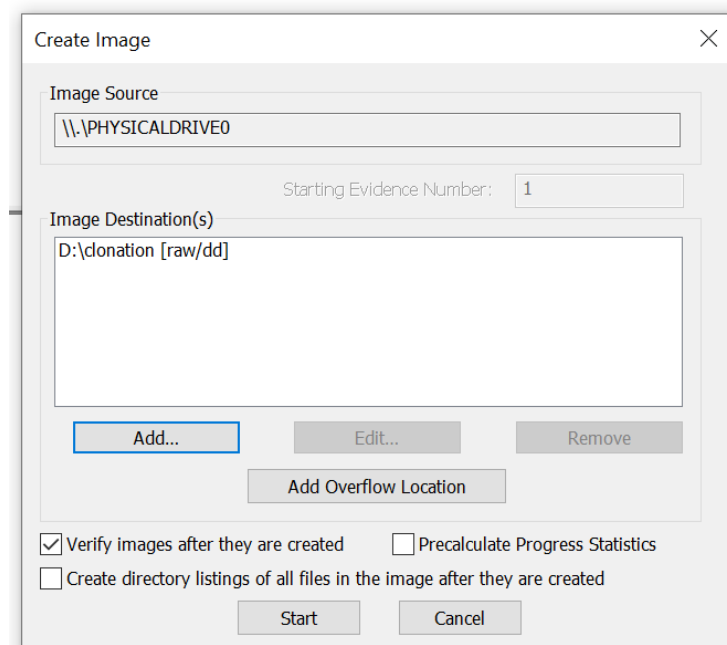
Seleccionamos el disco del cual deseamos realizar la clonación, en este caso, el disco C



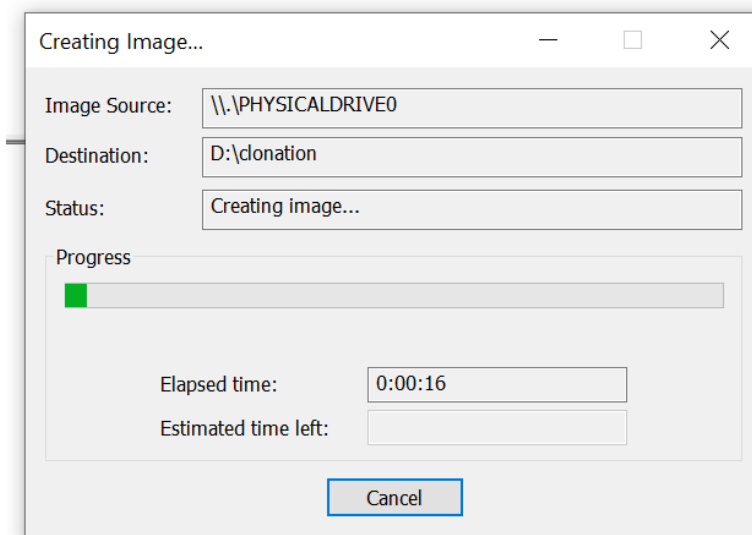
Seleccionaremos la ubicación donde se almacenará la clonación, en este caso, guardaremos la adquisición en el disco D.



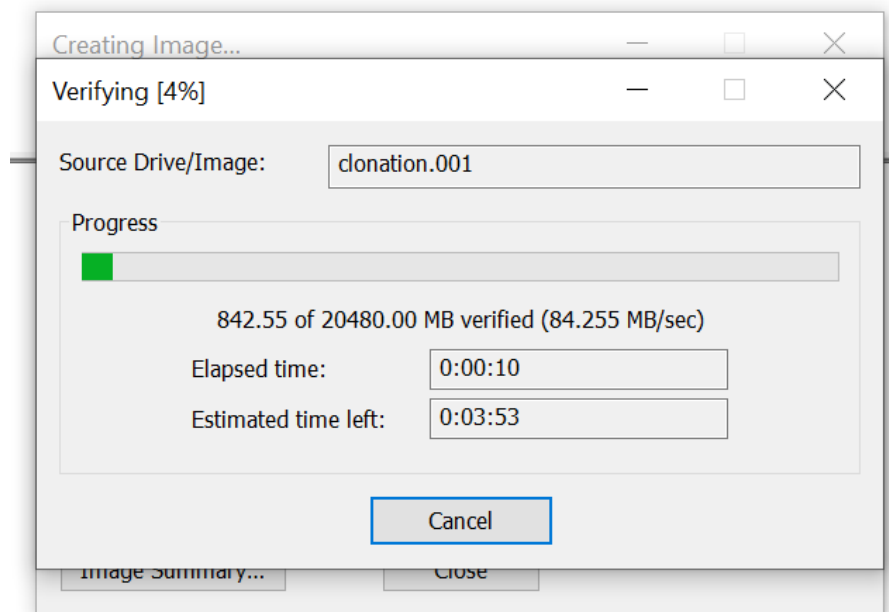
Una vez elegido el destino, podemos hacer clic en 'Start' para iniciar el proceso de clonación



Veremos el progreso con toda la información del proceso.



Una vez finalizada la creación de la imagen, se verificará la clonación para detectar posibles fallos.



Al concluir el proceso, se calculan los hashes MD5 y SHA-1, y se verifica la presencia de posibles errores.

Drive/Image Verify Results	
Name	clonation.001
Sector count	41943040
MD5 Hash	
Computed hash	7e7206485f04c2a47efbde3d37d42e3d
Report Hash	7e7206485f04c2a47efbde3d37d42e3d
Verify result	Match
SHA1 Hash	
Computed hash	56a86c4b69afb6e440d15b492954b8d4136518c2
Report Hash	56a86c4b69afb6e440d15b492954b8d4136518c2
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

Este equipo > Disco local (D:)		Buscar en Disco local (D:)		
Nombre		Fecha de modificación	Tipo	Tamaño
do	clonation.001	30/11/2023 13:36	Archivo 001	20.971.52...
	clonation.001	30/11/2023 13:41	Documento de tex...	2 KB

Ahora procederemos a realizar la clonación de un directorio específico; en este caso, clonaremos el directorio 'Usuarios', donde suele almacenarse toda la información personal.

Select Source

Please Select the Source Evidence Type

☐ Physical Drive

☐ Logical Drive

☐ Image File

☒ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

☐ Fernico Device (multiple CD/DVD)

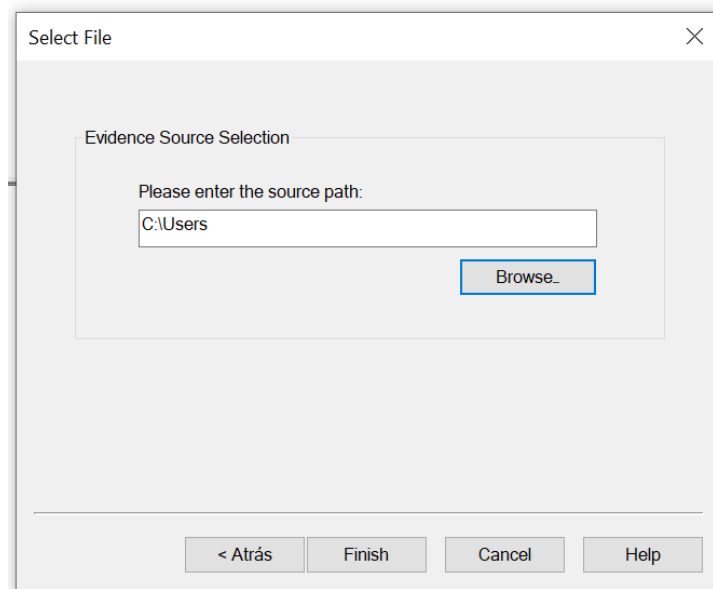
< Atrás

Siguiente >

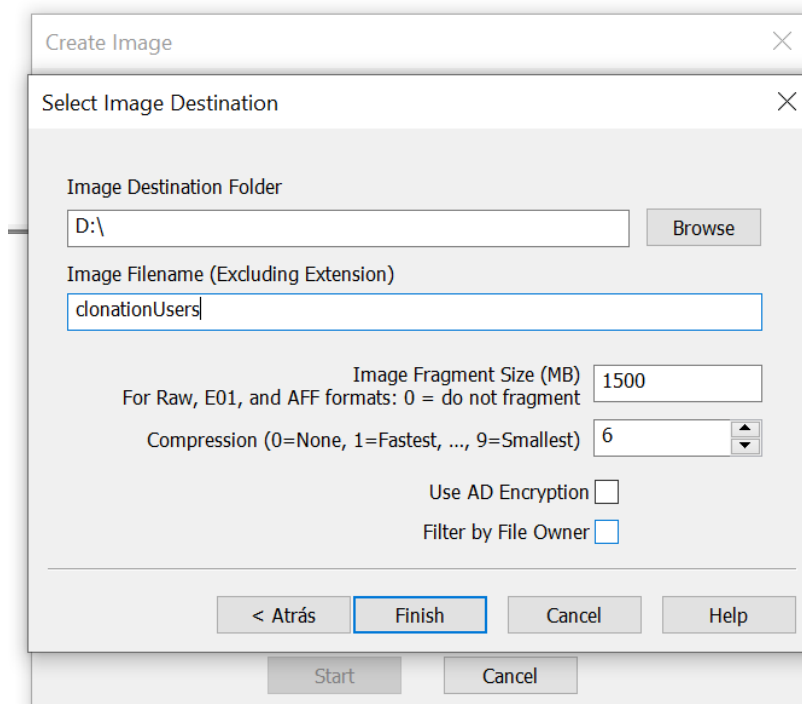
Cancel

Help

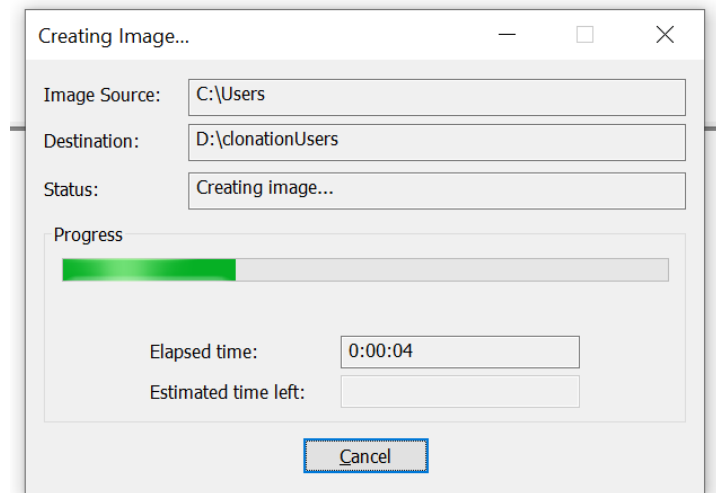
Seleccionamos el directorio 'C:\Users'.



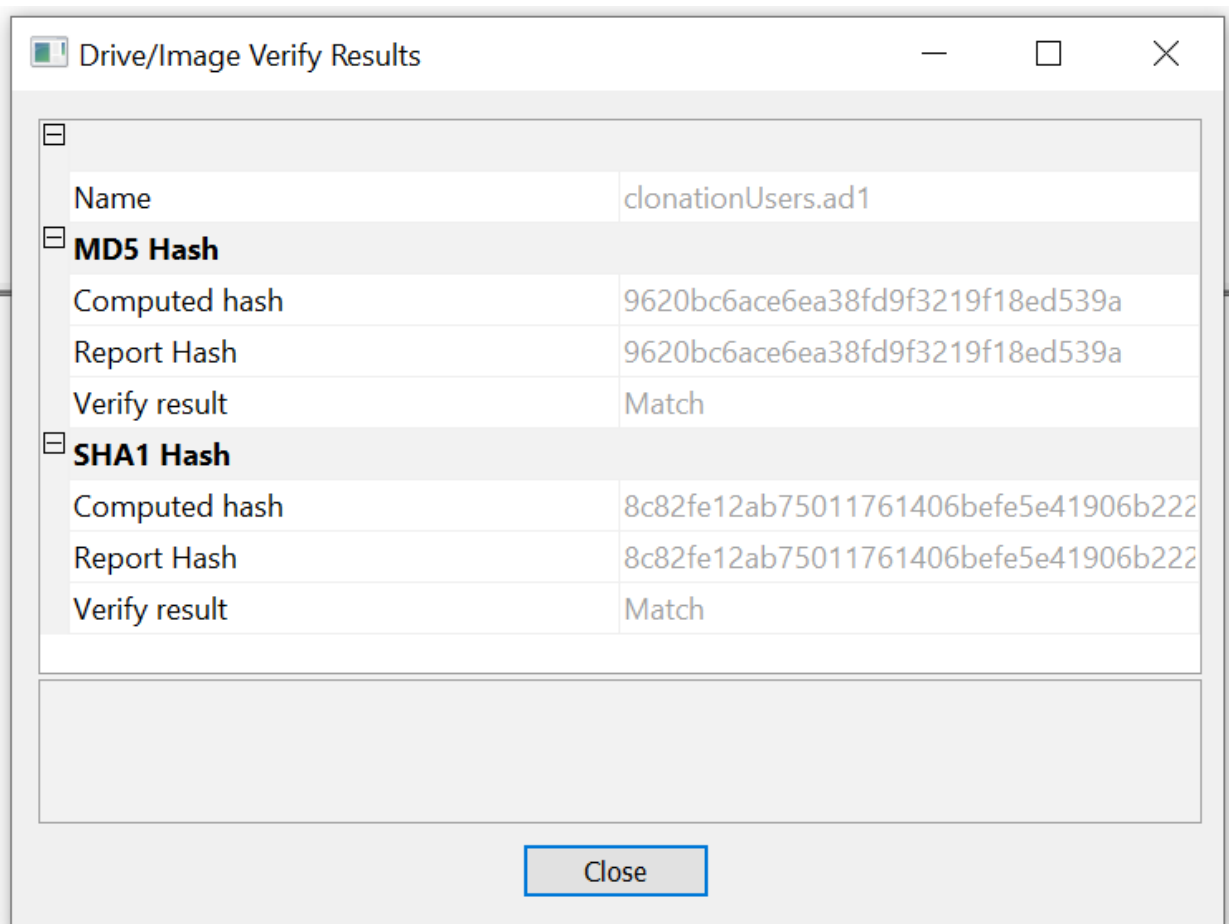
Seleccionamos el destino, en este caso el disco D.



De manera similar al caso anterior, hacemos clic en 'Start' y comenzará el proceso de clonación.



Al completar el proceso, se calcularán los hashes.



↑





Este equipo > Disco local (D:)

▼

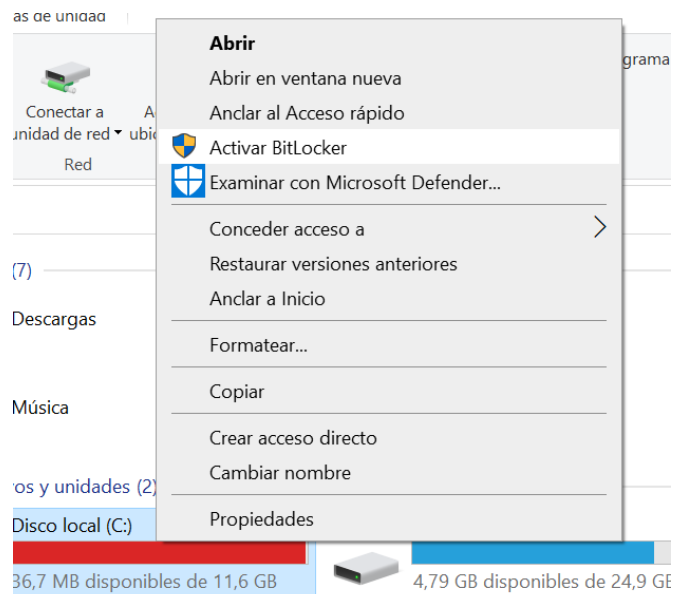
↺

🔍

Buscar en Disco local (D:)

	Nombre	Fecha de modificación	Tipo	Tamaño
rápido	 clonation.001	30/11/2023 13:36	Archivo 001	20.971.52...
rio	 clonation.001	30/11/2023 13:41	Documento de tex...	2 KB
gas	 clonationUsers.ad1	30/11/2023 13:49	Archivo AD1	149.182 KB
mentos	 clonationUsers.ad1	30/11/2023 13:49	Documento de tex...	83 KB
nes				

Una vez asegurada la clonación, procedemos a cifrar el disco C con BitLocker, lo que requerirá una contraseña al arrancar el sistema. Para ello, hacemos clic derecho en el disco a cifrar, en este caso, C, y seleccionamos **'Activar BitLocker'**.



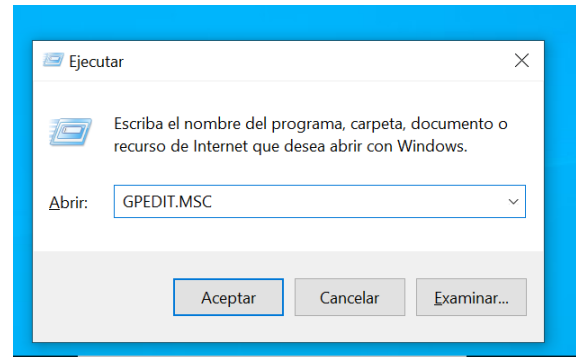
Aunque es posible que nos salga un error con este:

← Cifrado de unidad BitLocker (C:)

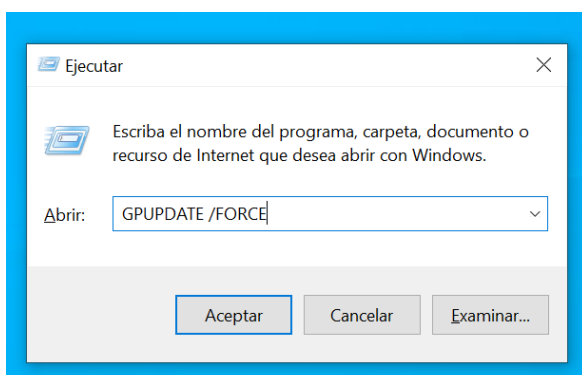
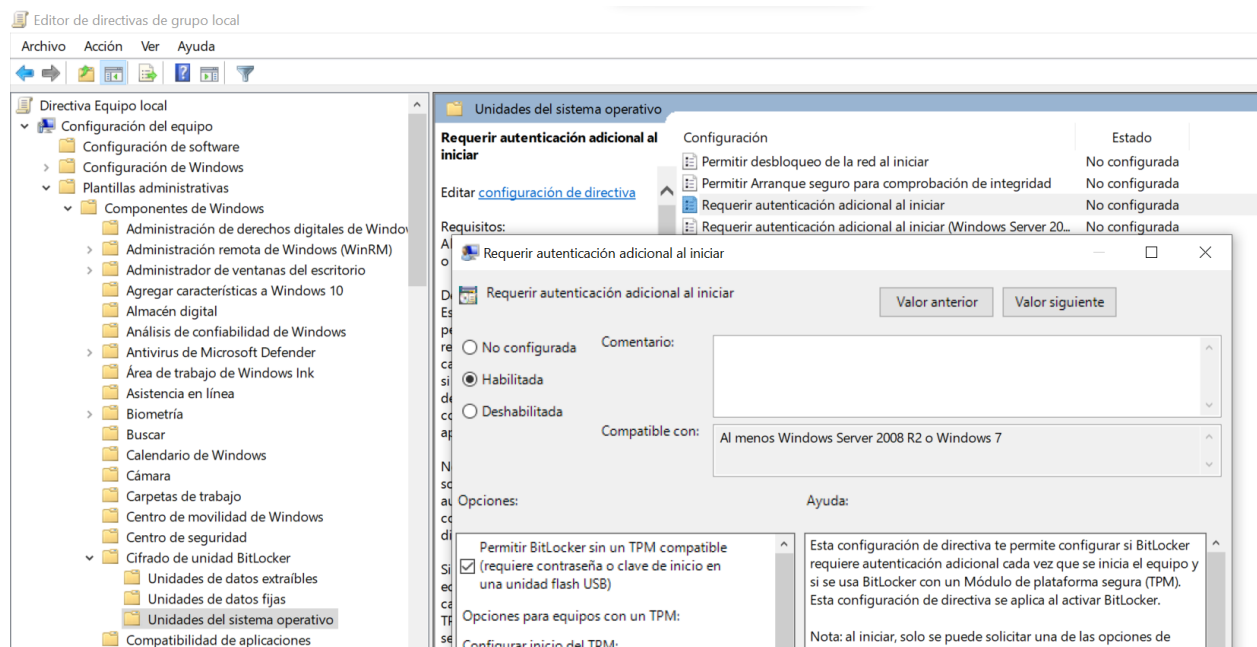
Iniciando BitLocker

- ❌ 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.

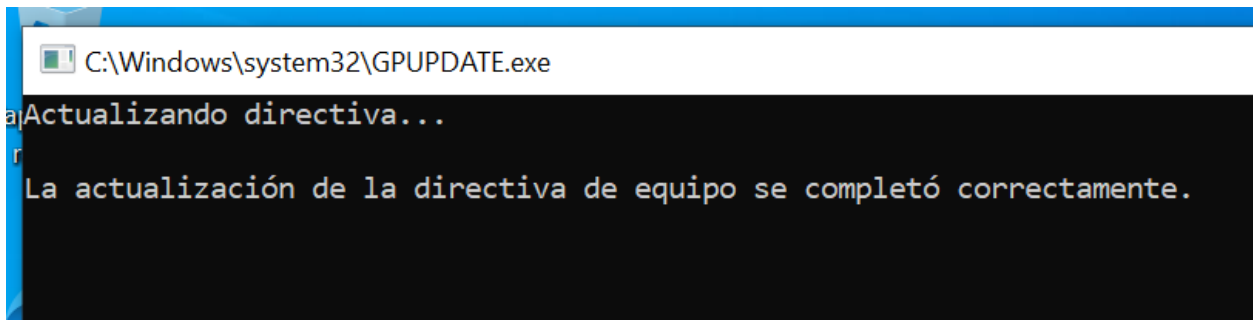
Para abordar el error anterior, presionamos “Windows + R” o buscamos 'Ejecutar' en el buscador, y ejecutamos el comando “**GPEDIT.MSC**”. Esto nos permitirá habilitar BitLocker sin requerir un TPM compatible”.



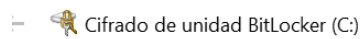
Se abrirá el Editor de directivas de Windows y nos dirigimos a “**Configuración del equipo\Plantillas administrativas\Componentes de Windows\Cifrado de unidad BitLocker\Unidades del sistema operativo**”. Luego, habilitamos la opción 'Requerir autenticación adicional al iniciar'.



Igual que en el paso anterior con la ventana de ejecutar, podemos utilizar el comando “**GPUPDATE /FORCE**”. Esto actualizará las directivas de Windows sin necesidad de reiniciar el equipo.



Una vez habilitada esta opción, podemos activar BitLocker para cifrar el disco C. Este proceso es sencillo y guiado. Podemos insertar una unidad USB; de este modo, si el USB no está conectado, no nos permitirá arrancar el PC. También tenemos la opción de utilizar una contraseña.



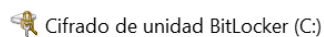
i El administrador del sistema administra ciertas configuraciones.

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

En este caso, seleccionaré la opción de contraseña, por lo que el sistema me solicita ingresar una contraseña.



Cree una contraseña para desbloquear esta unidad

Deberá crear una contraseña segura que incluya mayúsculas y minúsculas, números, símbolos y espacios.


Escribir la contraseña

••••••••


Vuelva a escribir la contraseña

••••••••

Debemos elegir dónde deseamos guardar la clave de recuperación. Hay varias opciones; en mi caso, selecciono la opción 'Guardar en un archivo' y también en una 'unidad USB'.

 Cifrado de unidad BitLocker (C:)

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

 Se guardó la clave de recuperación.

Se puede usar una clave de recuperación para acceder a los archivos y carpetas si tiene problemas para desbloquear su PC. Se recomienda tener más de una y conservarlas en un lugar seguro fuera de su PC.

→ Guardar en la cuenta Microsoft

→ Guardar en una unidad flash USB

→ Guardar en un archivo

→ Imprimir la clave de recuperación

Como último paso, el sistema nos indica si estamos listos para cifrar la unidad. Al confirmar, reiniciará el equipo y realizará algunas comprobaciones. Si todo va bien, nos solicitará la contraseña y cifrará la unidad.

 Cifrado de unidad BitLocker (C:)

¿Está listo para cifrar esta unidad?

El cifrado podría tardar varios minutos, según el tamaño de la unidad.

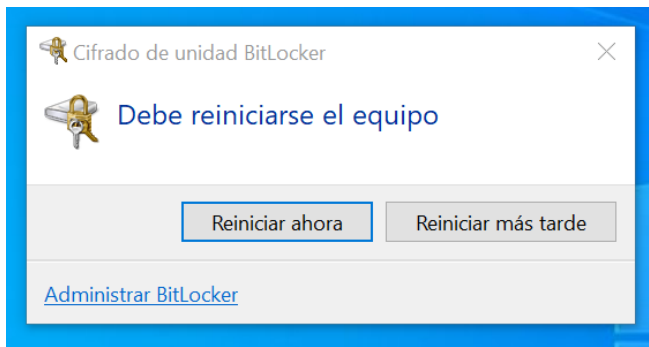
Puede continuar trabajando mientras se cifra la unidad, aunque es posible que se ralentice el funcionamiento del equipo.

☒ Ejecutar la comprobación del sistema de BitLocker

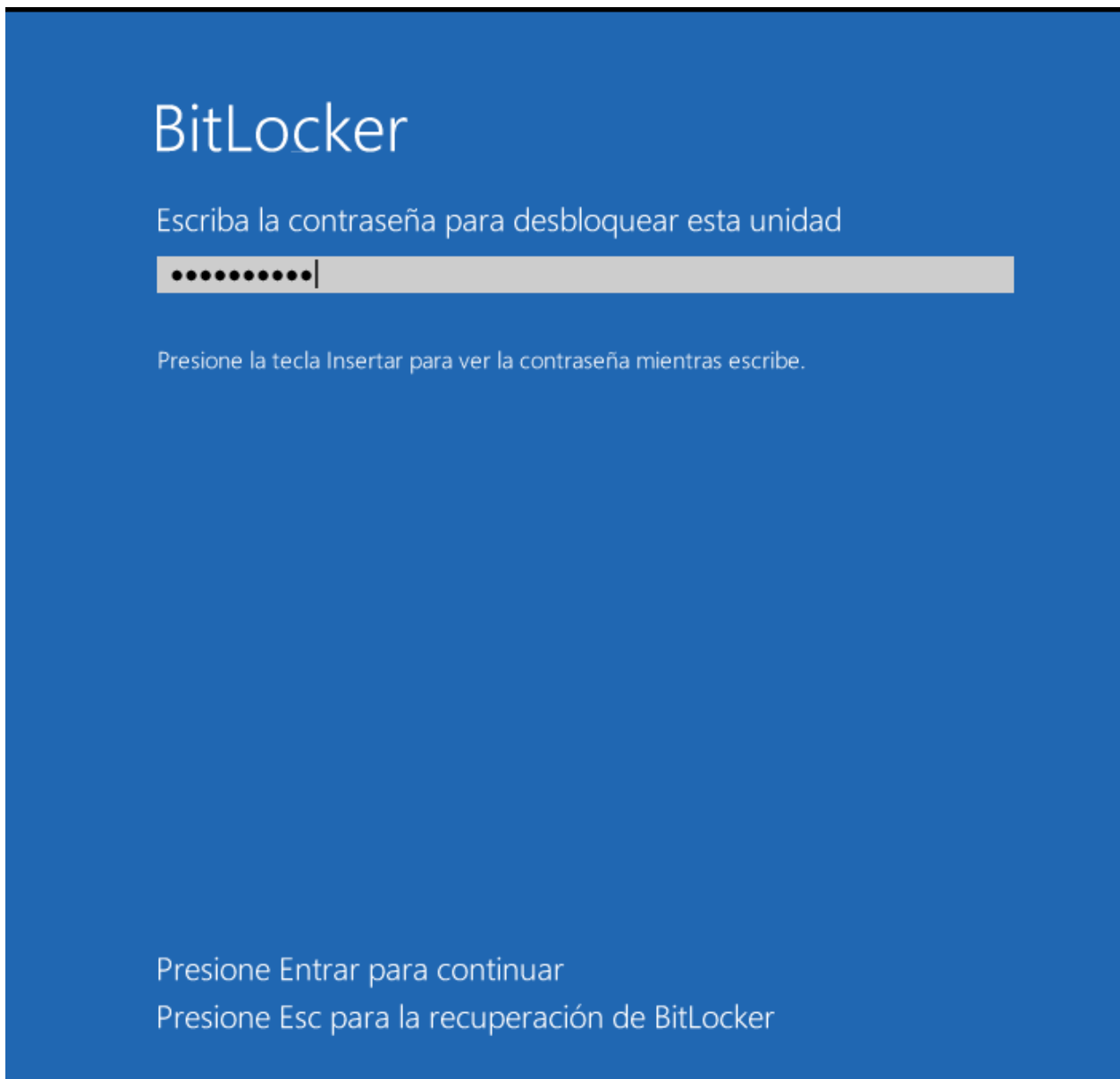
La comprobación del sistema confirmará que BitLocker pueda leer correctamente las claves de recuperación y de cifrado antes de que se cifre la unidad.

BitLocker reiniciará el equipo antes de iniciar el cifrado.

Nota: esta comprobación puede tardar un tiempo, pero se recomienda asegurarse de que el método de desbloqueo seleccionado funciona sin que sea necesario usar la clave de recuperación.




Como podemos comprobar, nos solicita reiniciar el equipo y nos pide la contraseña para poder arrancarlo.




Ahora podemos observar que en el Disco local C aparece un candado, indicando que está cifrado. De igual manera, podemos verificar el estado de BitLocker y realizar modificaciones en el panel de control, específicamente en '**Sistema y seguridad\Cifrado de unidad BitLocker**'

Dispositivos y unidades (2)



Disco local (C:)


154 MB disponibles de 11,6 GB



Disco local (D:)

4,79 GB disponibles de 24,9 GB

Ubicaciones de red (1)

 > Panel de control > Sistema y seguridad > Cifrado de unidad BitLocker


Principal del Panel de

Cifrado de unidad BitLocker

Protege tus archivos y carpetas del acceso no autorizado protegiendo tus unidades con BitLocker.

Unidad de sistema operativo

C: Cifrado de BitLocker



Copia de seguridad de la clave de recuperación

Cambiar contraseña

Quitar contraseña

Desactivar BitLocker

Unidades de datos fijas

Finalmente, podemos repetir el proceso de clonación tanto del disco completo como de la carpeta de usuarios. Podremos comprobar que, a pesar de no haber realizado ninguna modificación en la unidad, el hash es diferente. Esto se debe al cifrado que acabamos de realizar en la unidad

Drive/Image Verify Results	
Name	clonation.001
Sector count	41943040
MD5 Hash	
Computed hash	51b0130b9c541da3800699fa346ef05d
Report Hash	51b0130b9c541da3800699fa346ef05d
Verify result	Match
SHA1 Hash	
Computed hash	c3686ce7e16a66e29bd7419677127c839dbf2777
Report Hash	c3686ce7e16a66e29bd7419677127c839dbf2777
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

Drive/Image Verify Results	
Name	clonationUsers.ad1
MD5 Hash	
Computed hash	83680279973d4b21b40961a1ae72cbe1
Report Hash	83680279973d4b21b40961a1ae72cbe1
Verify result	Match
SHA1 Hash	
Computed hash	a5f72b5fd0bcb7091803db1cce94ab19721t
Report Hash	a5f72b5fd0bcb7091803db1cce94ab19721t
Verify result	Match
Close	

Este equipo > Disco local (E:)				
	Nombre	Fecha de modificación	Tipo	Tamaño
ido	clonation.001	30/11/2023 14:15	Archivo 001	20.971.520 KB
o	clonation.001	30/11/2023 14:19	Documento de texto	2 KB
as	clonationUsers.ad1	30/11/2023 14:30	Archivo AD1	149.645 KB
ntos	clonationUsers.ad1	30/11/2023 14:30	Documento de texto	86 KB
as				