



CEU

*Fundación San Pablo
Andalucía*

CENTRO DE ESTUDIOS PROFESIONALES

Glorieta Ángel Herrera Oria, s/n, 41930 Bormujos, Sevilla

HERRAMIENTAS DE CIFRADO: BITLOCKER



 Windows 10
BitLocker

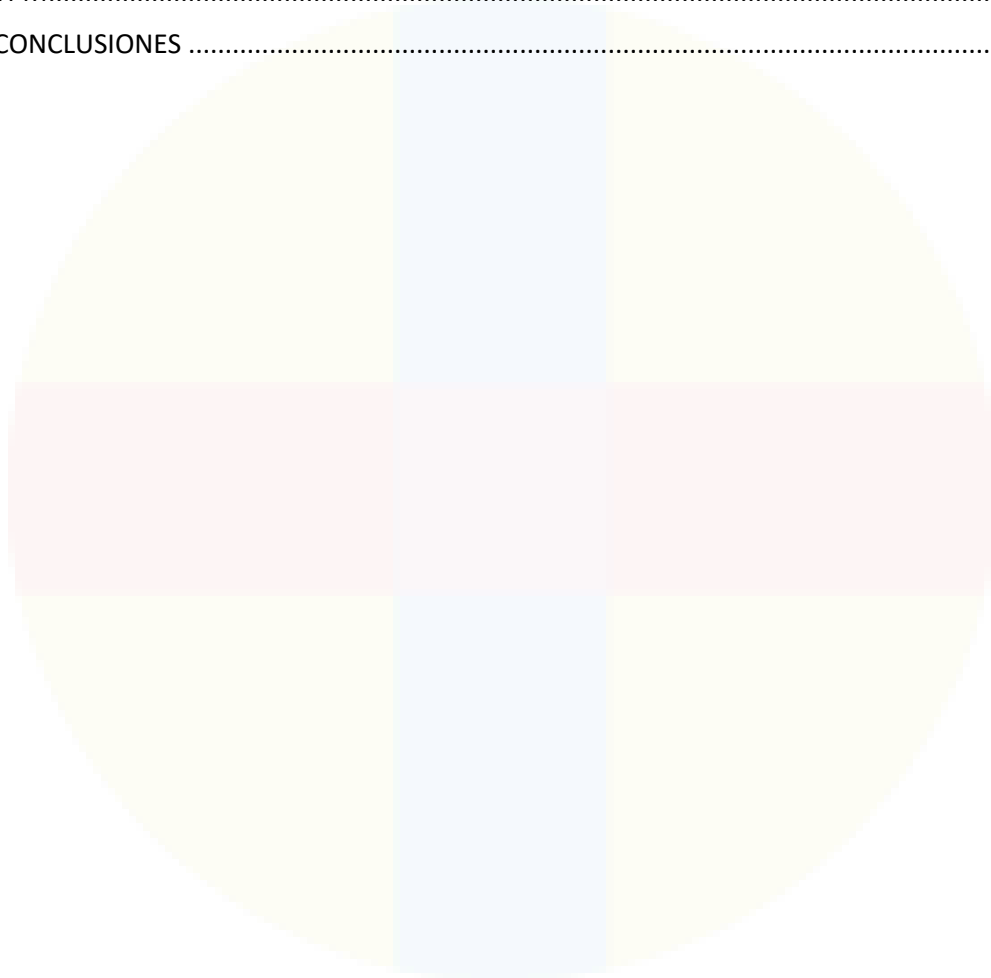
Realizado por:

Jhonatan Guzmán Panozo

1º DAW

ÍNDICE

HOJA DE CONTROL DEL DOCUMENTO	1
1. INTRODUCCIÓN	2
2. PRÁCTICA	2
3. TPM.....	11
4. CONCLUSIONES	12



HOJA DE CONTROL DEL DOCUMENTO

DOCUMENTO / ARCHIVO			
Fecha última Modificación	30/04/2024	Versión / Revisión	v01r01
Fecha Creación	30/04/2024		
Fecha Finalización	30/04/2024		
Ubicación Física	CLASE/CASA		

REGISTRO DE CAMBIOS		
Versión / Revisión	Página	Descripción
v01r01	1-13	Elaboración de la práctica

AUTORES DEL DOCUMENTO	
Apellidos, Nombre	Curso
Guzmán Panozo, Jhonatan	1º SSII DAW

PREPARADO	REVISADO	APROBADO
Jhonatan Guzmán Panozo	Jhonatan Guzmán Panozo	Rafael Madrigal Toscano

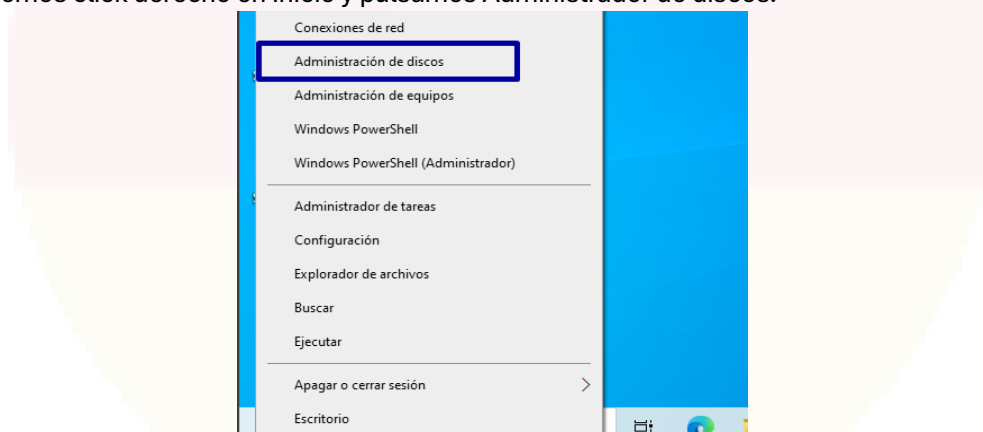
1. INTRODUCCIÓN

El cifrado de unidad BitLocker es una característica de protección de datos del sistema operativo, permite cifrar o encriptar los datos de un equipo para mantenerlo protegido, haciendo frente a amenazas como el robo de datos o la exposición en caso de pérdida, el robo o la retirada inapropiada de equipos.

La protección de BitLocker en unidades del sistema operativo admite la autenticación de dos factores mediante el uso del Módulo de plataforma segura (TPM) junto con un número de identificación personal (PIN) o clave de inicio, así como la autenticación de un solo factor mediante el almacenamiento de una clave en una unidad flash USB o mediante el uso solo del TPM. El uso de BitLocker con un TPM proporciona una mayor protección a los datos y ayuda a garantizar la integridad del componente de arranque inicial.

2. PRÁCTICA

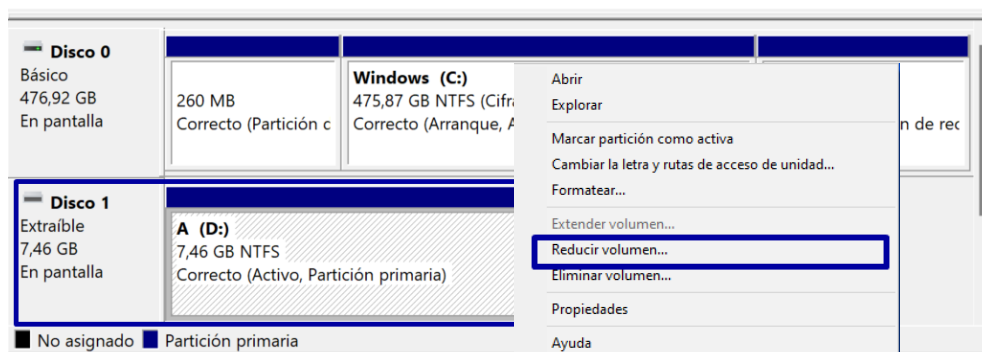
Hacemos click derecho en Inicio y pulsamos Administrador de discos.



Vamos hacer una partición de nuestro disco 1 A (D:). Click derecho>Reducir volumen.

Administración de discos

Volumen	Distribución	Tipo	Sistema de ...	Estado	Capacidad	Espacio ...	% disponible
(Disco 0 Partición 1)	Simple	Básico		Correcto (...)	260 MB	260 MB	100 %
(Disco 0 Partición 4)	Simple	Básico		Correcto (...)	813 MB	813 MB	100 %
A (D:)	Simple	Básico	NTFS	Correcto (...)	7,46 GB	7,44 GB	100 %
Windows (C:)	Simple	Básico	NTFS (Cifra...)	Correcto (...)	475,87 GB	285,31 GB	60 %



Ahora especificamos el tamaño de gigas que queremos.

Reducir D:

Tamaño total antes de la reducción, en MB:

7643

Espacio disponible para la reducción, en MB:

4519

Tamaño del espacio que desea reducir, en MB:

4519

Tamaño total después de la reducción, en MB:

3124

No se puede reducir un volumen más allá del punto en que haya algún archivo que no se pueda mover. Vea el evento "defrag" del registro de la aplicación para obtener información detallada acerca de la operación cuando se haya completado.

Vea "Reducir un volumen básico" en la Ayuda de Administración de discos para obtener más información

Reducir

Cancelar

Y nos aparece así

Administración de discos

Archivo

Acción

Ver

Ayuda

Volumen	Distribución	Tipo	Sistema de ...	Estado	Capacidad
(Disco 0 Partición 1)	Simple	Básico		Correcto (...)	260 MB
(Disco 0 Partición 4)	Simple	Básico		Correcto (...)	813 MB
A (D:)	Simple	Básico	NTFS	Correcto (...)	3,05 GB
Windows (C:)	Simple	Básico	NTFS (Cifra...	Correcto (...)	475,87 GB

Disco 0

Básico
476,92 GB
En pantalla

260 MB Correcto (Partición	Windows (C:) 475,87 GB NTFS (Cifrado con BitLocker) Correcto (Arranque, Archivo de paginación, Volc	813 M Correc
-------------------------------	--	-----------------

Disco 1

Extraíble
7,46 GB
En pantalla

A (D:) 3,05 GB NTFS Correcto (Activo, Partición pri	4,41 GB No asignado	
--	------------------------	--

No asignado

Partición primaria

Ahora sobre él, pulsamos click derecho y Nuevo volumen simple...

20,01 GB
No asignado

Nuevo volumen simple...

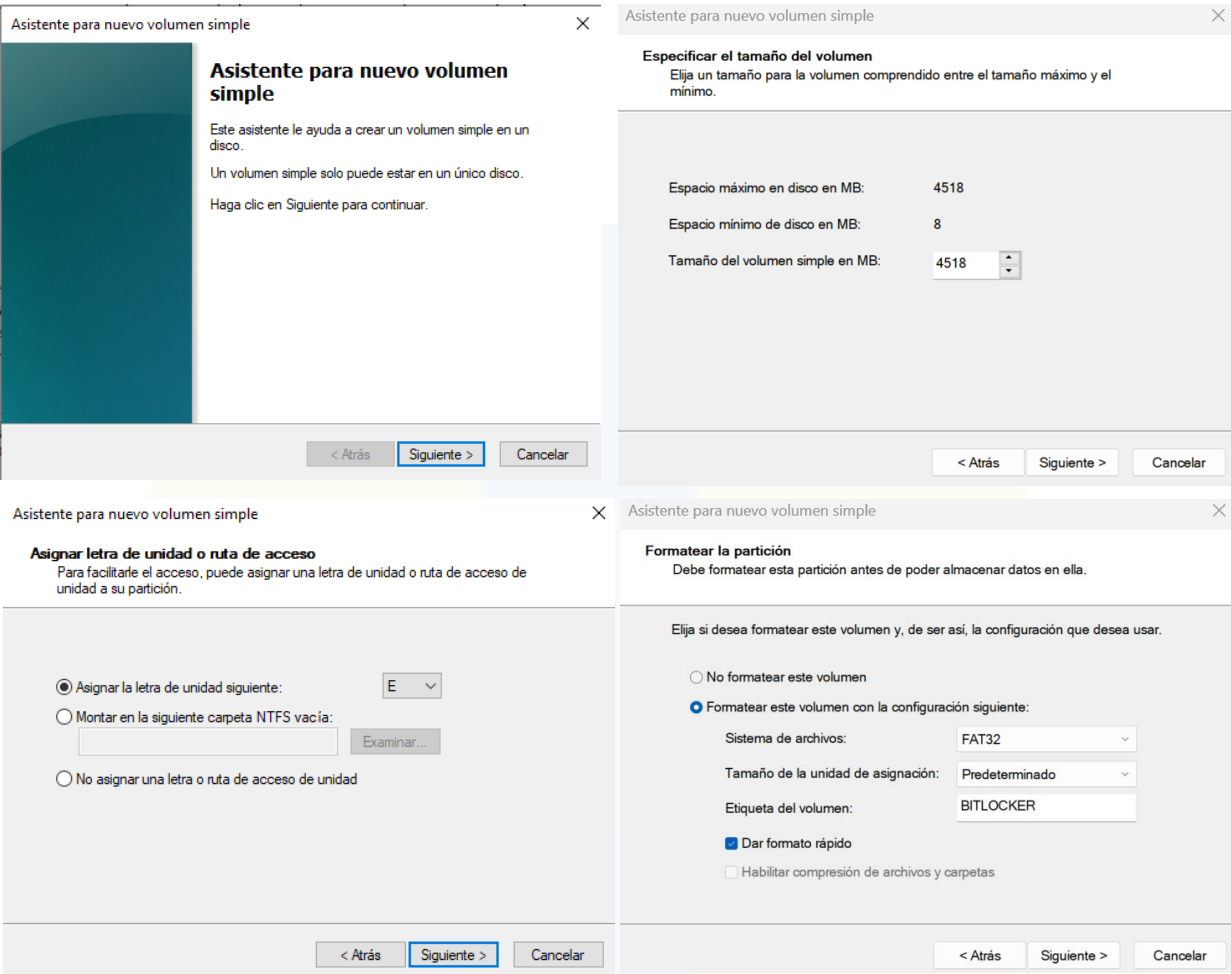
Nuevo volumen distribuido...

Nuevo volumen seccionado...

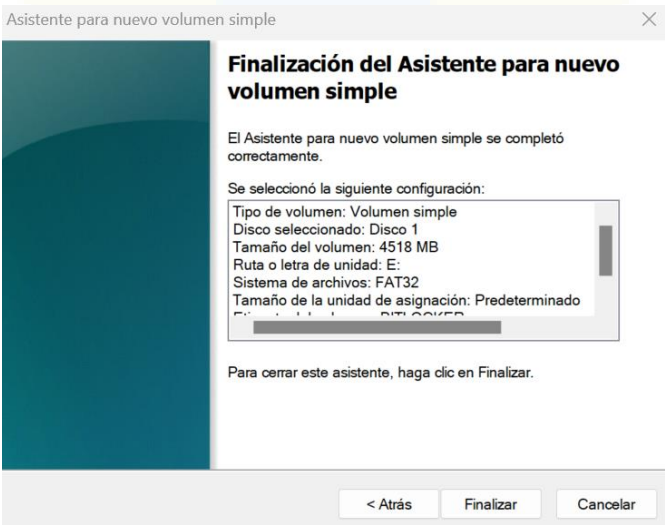
Propiedades

Ayuda

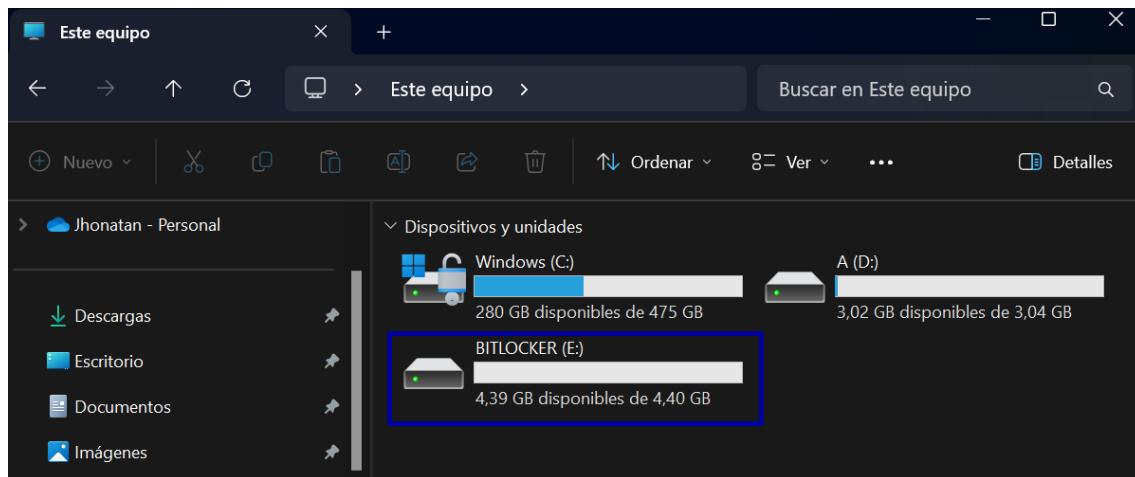
Y le damos Siguiente a todo.



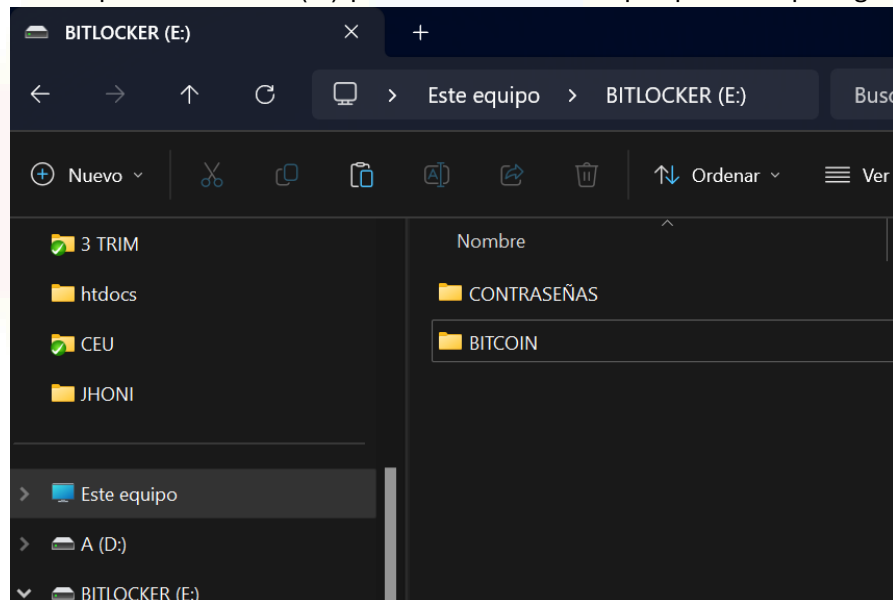
Y Finalizar



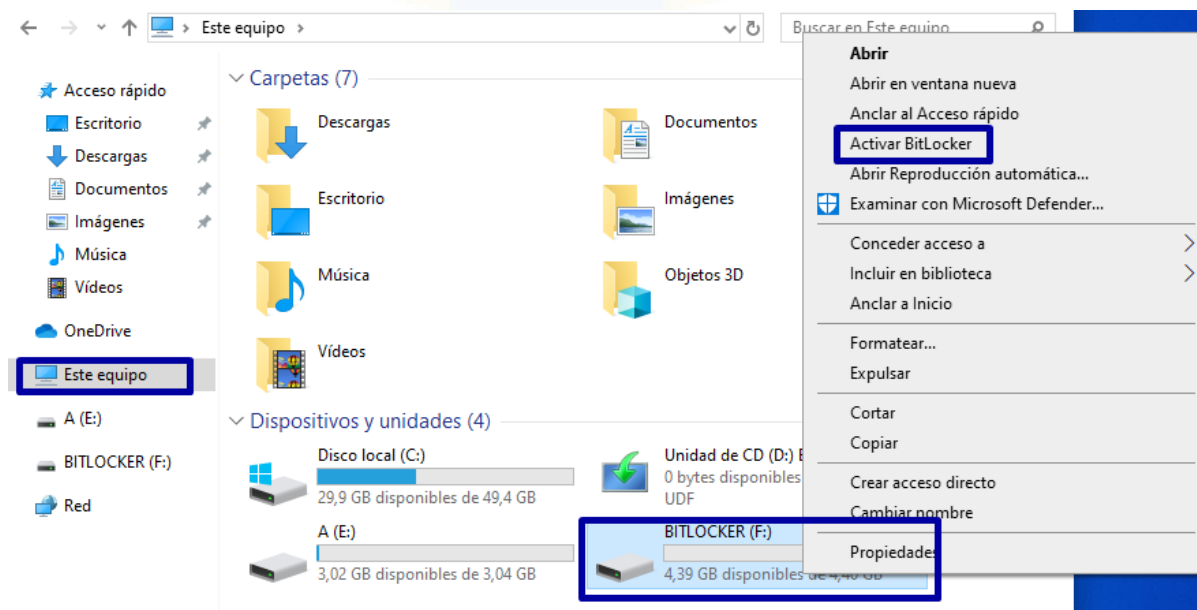
Una vez finalizado el proceso, nos aparecerá de la siguiente forma:



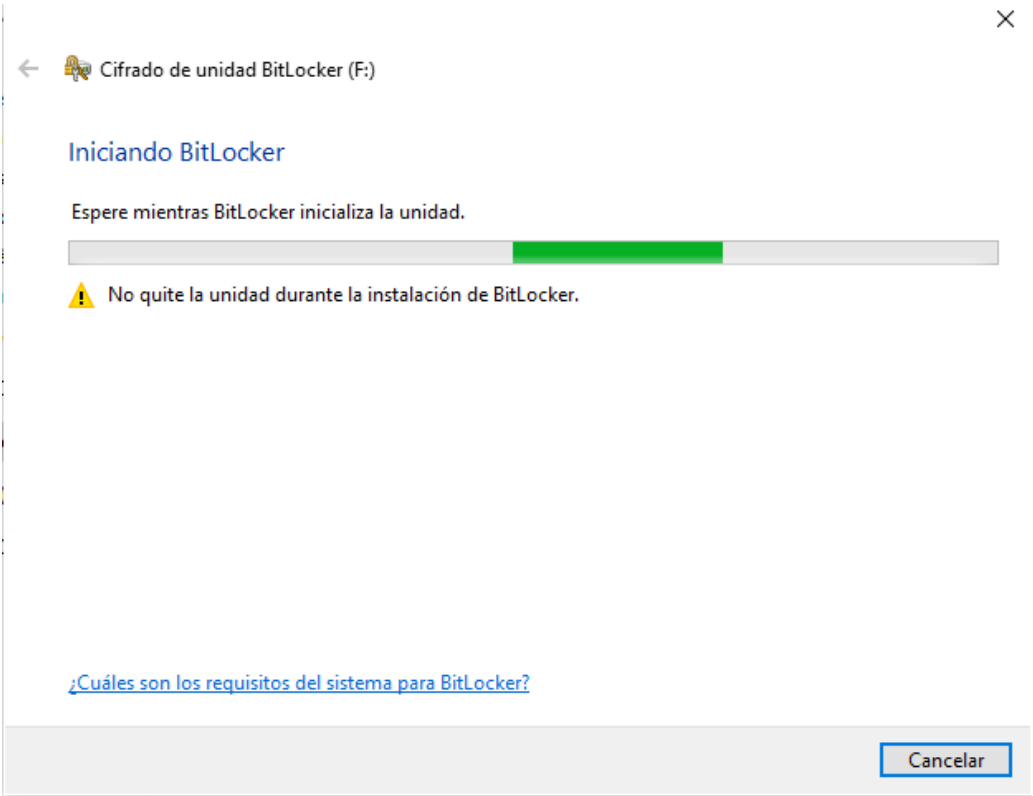
En nuestra carpeta BITLOCKER(E:) ponemos los archivos que queremos proteger.



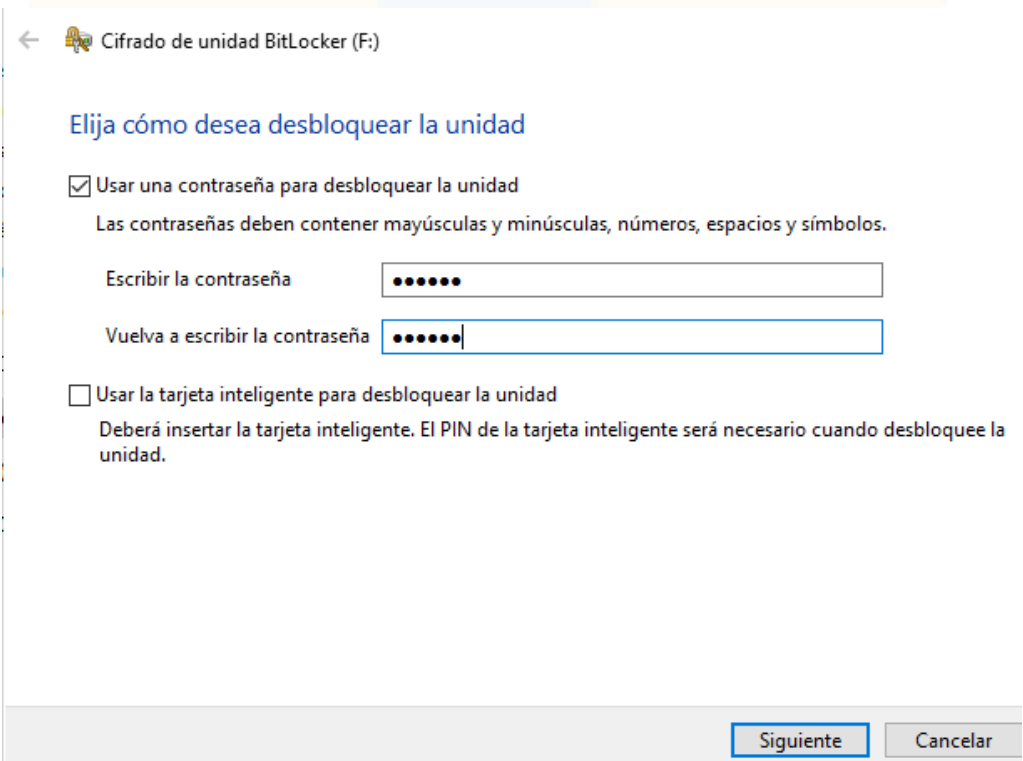
Ahora click derecho sobre nuestra carpeta y Activar Bitlocker




Empezará a cargar




Y escribimos contraseña



Elegimos donde guardar la contraseña en caso de que se nos olvide.

←  Cifrado de unidad BitLocker (F:)

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

 El administrador del sistema administra ciertas configuraciones.

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


→ Imprimir la clave de recuperación

[¿Cómo puedo encontrar después mi clave de recuperación?](#)

Siguiente

Cancelar

Elegimos el 1 que es más rápido pero el 2 es más seguro y más lento.

←  Cifrado de unidad BitLocker (F:)

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)

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

Siguiente

Cancelar

Elegimos el 2 porque es una unidad extraíble. El primero es para unidad interna.

←  Cifrado de unidad BitLocker (F:)

Elección del modo de cifrado que se usará

La actualización de Windows 10 (versión 1511) introduce un nuevo modo de cifrado de disco (XTS-AES). Este modo ofrece soporte de integridad adicional, pero no es compatible con las versiones anteriores de Windows.

Si se trata de una unidad extraíble que usarás con una versión anterior de Windows, elige el modo Compatible.

Si es una unidad fija o si solo se utilizará en dispositivos con la actualización de Windows 10 (versión 1511) o versiones posteriores, elige el nuevo modo de cifrado.


- ☐ Modo de cifrado nuevo (recomendado para las unidades fijas en este dispositivo)
- ☒ Modo Compatible (recomendado para las unidades que se puedan mover de este dispositivo)

Siguiente

Cancelar

Y comienza el cifrado.



←  Cifrado de unidad BitLocker (F:)

¿Está listo para cifrar esta unidad?

Podrá desbloquear esta unidad con una contraseña.

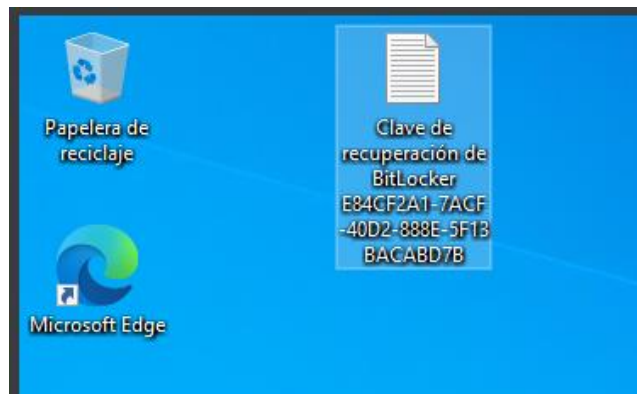
El cifrado puede tardar unos minutos en función del tamaño de la unidad.

Los archivos no estarán protegidos hasta que se haya completado el cifrado.

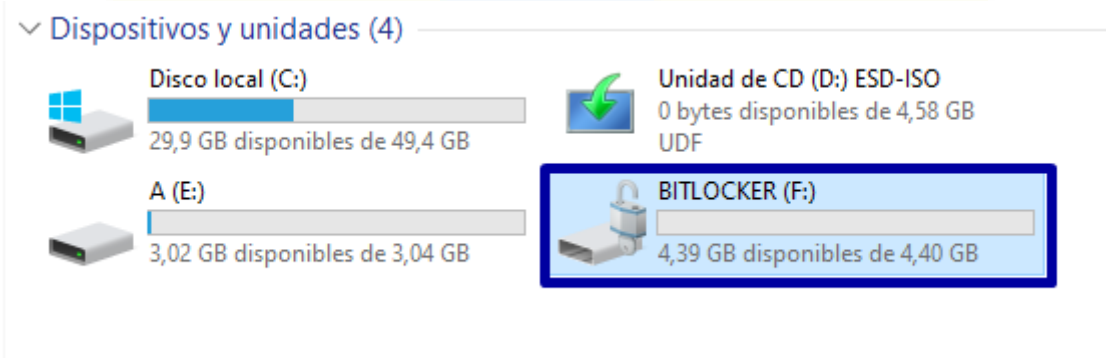
Iniciar cifrado

Cancelar

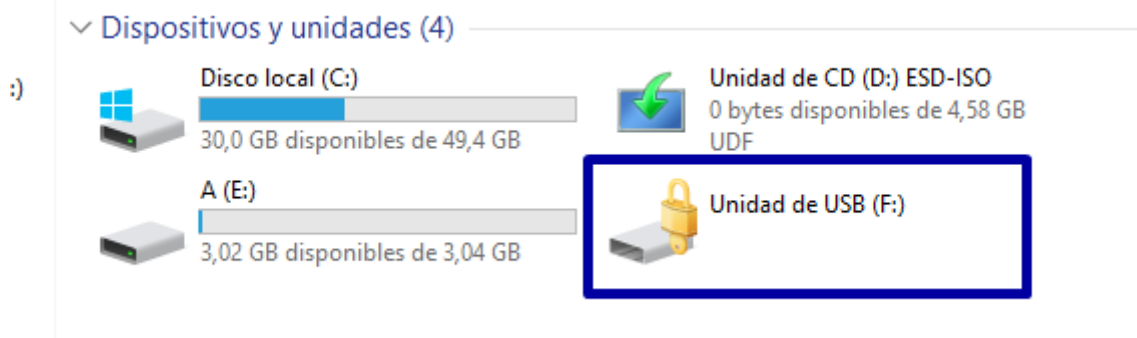
En mi caso he guardado el archivo en el escritorio



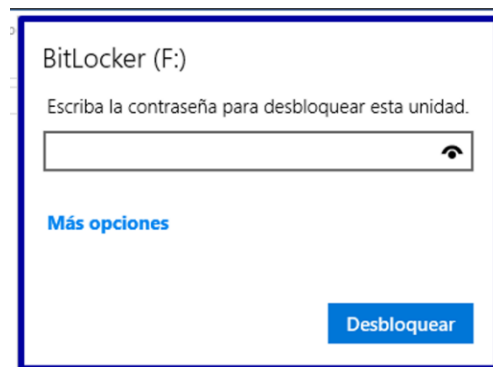
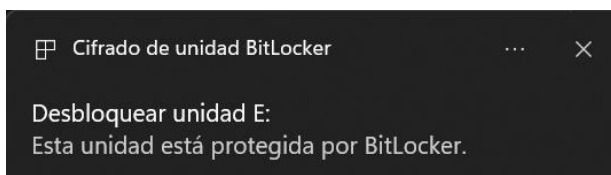
Ahora podemos ver como queda con un candado abierto.



Para poder ver cambios, debemos reiniciar el ordenador.



Ahora para acceder debemos poner la contraseña de antes. Y ya estaría.



En caso de haber olvidado la contraseña, le damos a más opciones.

BitLocker (E:)

Escriba la contraseña para desbloquear esta unidad.

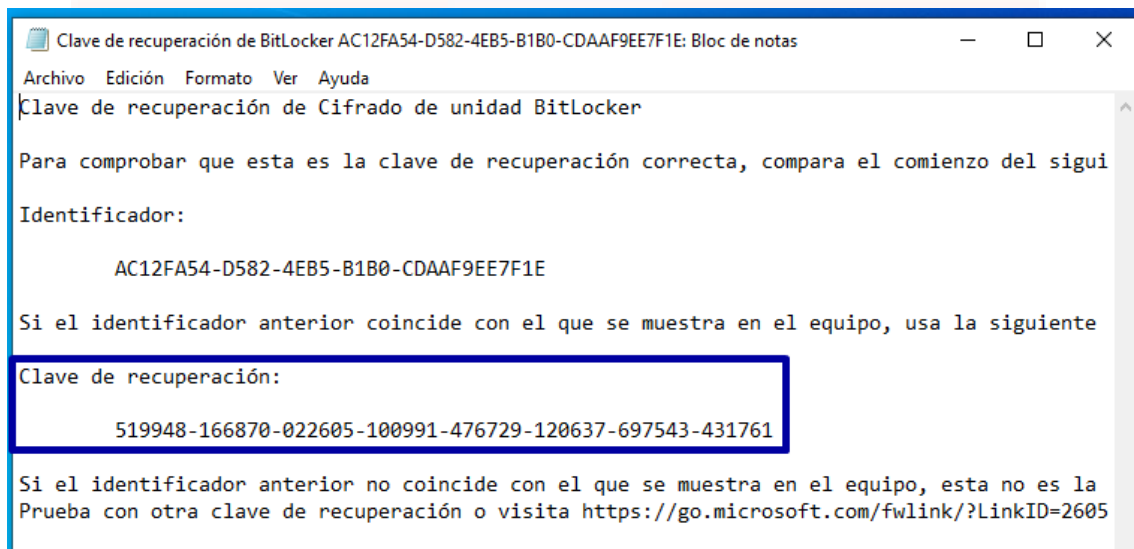
Menos opciones

Escribir clave de recuperación

☐ Desbloquear automáticamente en este equipo

Desbloquear

Y abrimos nuestro archivo guardado para desbloquearlo.



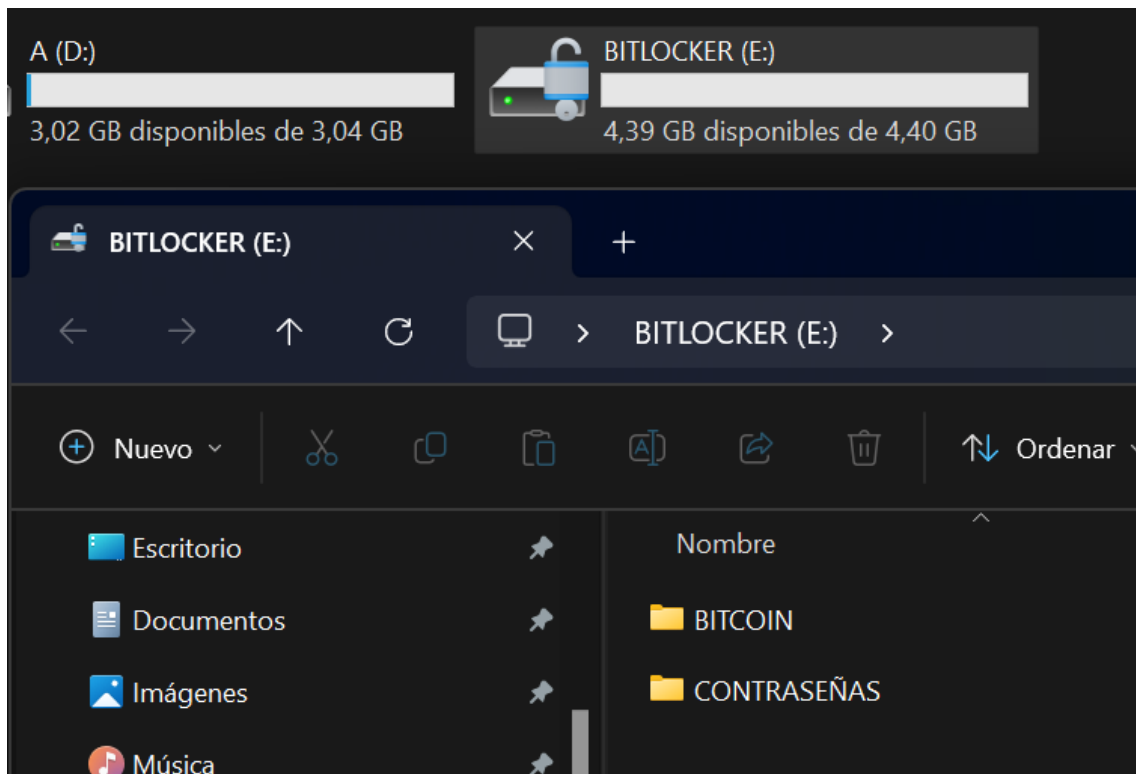
Y desbloqueamos.

⬅ BitLocker (E:)

Escriba la clave de recuperación de 48 dígitos para desbloquear la unidad.

(Id. de clave: AC12FA54)

Y ya podemos acceder a nuestra carpeta.

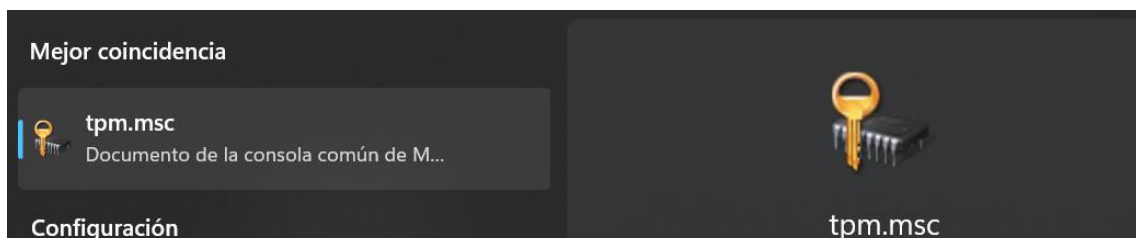


3. TPM

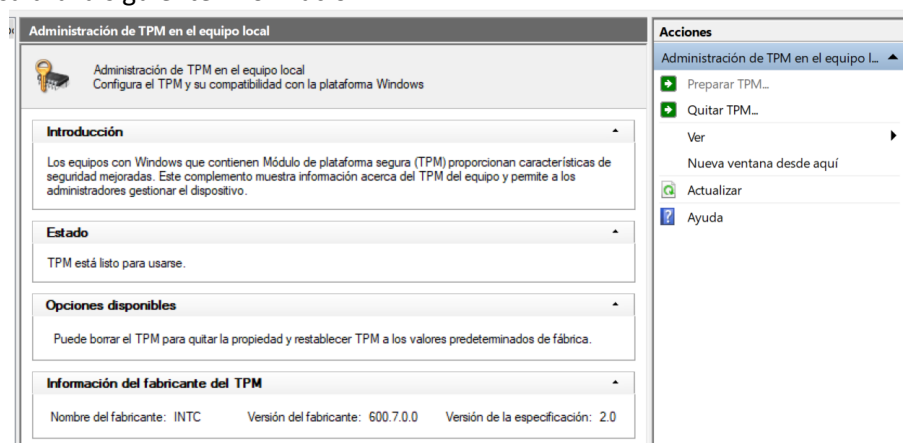
TPM significa Trusted Platform Module (Módulo de Plataforma de Confianza). Es un chip de hardware o un componente de seguridad en la placa base de un ordenador que proporciona funciones de seguridad críticas, como el almacenamiento seguro de claves criptográficas, la generación de claves aleatorias y la realización de operaciones criptográficas.

El TPM ayuda a garantizar la integridad del sistema y protege contra ataques como el robo de identidad, la manipulación de software y el acceso no autorizado a datos sensibles. Se utiliza en una variedad de aplicaciones, como la autenticación de usuarios, el cifrado de datos y la protección de la privacidad.

No todos los ordenadores tienen tpm, los más antiguos no lo poseen. Para verlo escribimos:

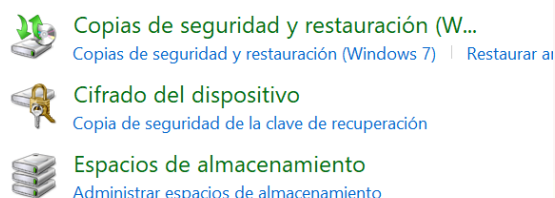


Y nos saldrá la siguiente información:



4. CONCLUSIONES

Este trabajo no era difícil, pero se me ha complicado bastante porque no me aparecía en mi ordenador la parte de bitlocker, solo me aparecía lo siguiente



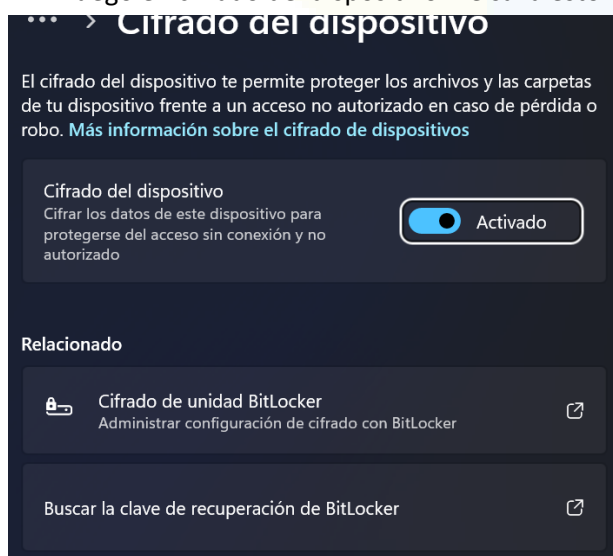
Unidad de sistema operativo

Windows (C:)



Copia de seguridad de la clave de recuperación

Y luego en cifrado del dispositivo me salía esto.



Lo tuve que hacer con virtualbox en windows 10 pro, ya que solo se puede usar en en windows 10/11 pro y en los demas no están disponibles.

Es una herramienta muy útil ya que, si te roban tu ordenador o unidad extraíble no van a poder acceder a él.

