Tema IV Ejercicio IV: Bitlocker

Nicolás A. Ortega Froysa

2 de diciembre de 2021

Índice

1. Hoja De Control Del Documento

Cuadro 1: Documento/Archivo

Fecha Última Modificación	2/12/2021	**Versión/Revisión**	v01r02
Fecha Creación	01/12/2021		
Fecha Finalización	2/12/2021		

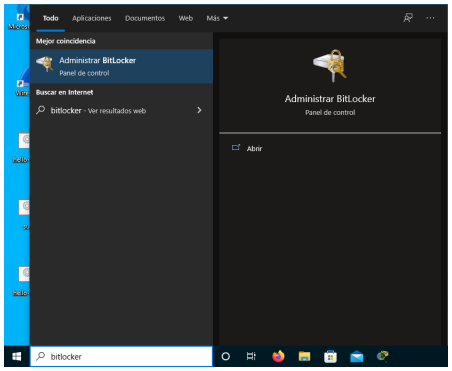
Cuadro 2: Registro De Cambios

Versión/Revisión	**Página(s)**	**Descripción**
v01r01	Todas	Creación y elaboración del documento.
v01r02	6-8	Completación de secciones 4-6.

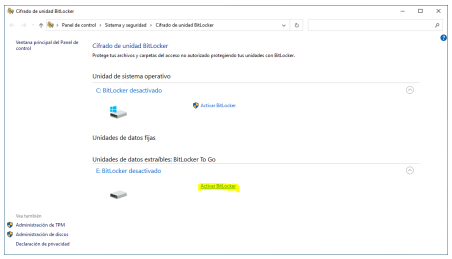
Cuadro 3: Autores Del Documento

Apellidos, Nombre	**Curso**
Ortega Froysa, Nicolás Andrés	1

Preparado	**Revisado**	**Aprobado**
Ortega Froysa, Nicolás Andrés		



(a) Despliegue de Bitlocker.



(b) Ventana de Bitlocker.

Figura 1: Inicio de Bitlocker.

2. ¿Qué es Bitlocker?

A menudo nos hace falta guardar unos datos de una forma segura, tal que sólo lo podemos abrir nosotros, pero también nos hace falta que sea portable. Para esto es ideal usar una herramienta como Bitlocker. Con esto, se cifra los datos que hay en una partición (de un *pendrive*), de forma que sólo se pueden acceder con la clave apropiada. Esto hace que puedas tener un dispositivo portable y (medianamente) segura.

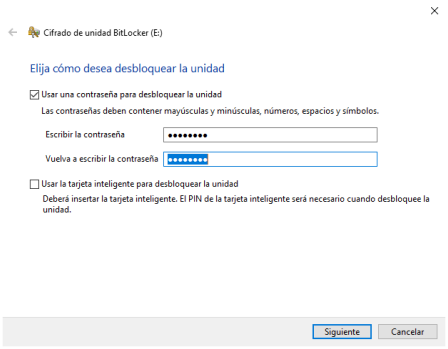
Esta herramienta se encuentra ya instalada en Windows 10, que no en Windows 7. De este modo, hay algunos pasos que ya no se aplican. Aquí veremos cómo usarlo en un sistema de Windows 10.

3. Cifrado de un Pendrive

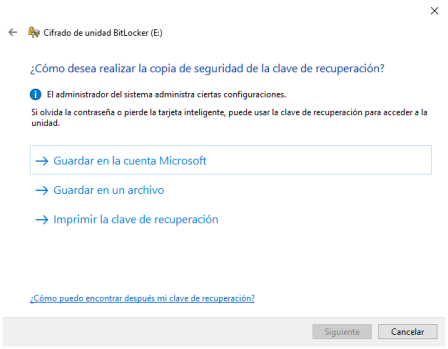
Al estar ya instalado en Windows 10, podemos abrirlo simplemente buscando «Bitlocker» en el menú (figura 1a). Al abrir la aplicación podemos ver los dispositivos disponibles para cifrar (figura 1b). Nos lo divide en varios apartados, pero dos importantes en los que nos fijaremos:

- **Unidad de sistema operativo**: unidades de almacenamiento que son usadas por el sistema operativo (e.g. `C:`).
- **Unidades de datos extraíbles: Bitlocker To Go**: unidades de almacenamiento que podemos fácilmente extraer del ordenador, como sería un *pendrive*.

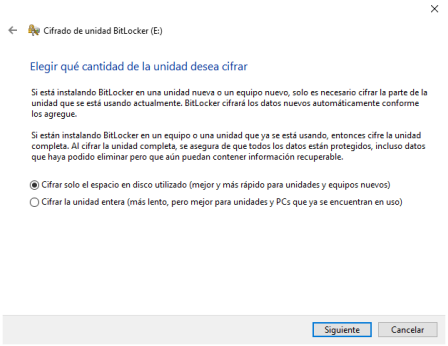
En nuestro caso, trabajaremos con los dispositivos extraíbles, y en particular con aquel dispositivo `E:`. Para empezar el proceso de configuración del



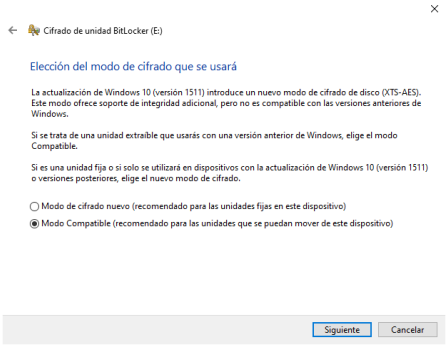
(a) Configuración de contraseña.



(b) Creación de una copia de respaldo.



(c) Cantidad de unidad a cifrar.



(d) Selección del tipo de cifrado.

Figura 2: Configuración del cifrado.

cifrado, pulsaremos sobre «Activar Bitlocker» al lado de nuestro dispositivo USB.

Al seleccionar la activación, debemos primero seleccionar el método que usaremos para desbloquear nuestro dispositivo (figura 2a). Aquí nos da dos opciones que se pueden combinar:

- **Contraseña**: quizá lo más obvio, cifras el contenido con una contraseña que se introducirá a la hora de descifrarlo.
- **Tarjeta Inteligente**: un dispositivo *hardware* para cifrado seguro.

No tenemos acceso a una tarjeta inteligente, así que nos aviaremos simplemente con la contraseña, que vale para nuestros requisitos.

A continuación nos pedirá hacer una copia de respaldo de la clave de recuperación del dispositivo (figura 2b). Esto es una buena idea por si se olvida la contraseña, o si se pierde la supuesta tarjeta inteligente. Nos da tres opciones:

- **Guardar en la cuenta de Microsoft**: si tienes una cuenta de Microsoft, puedes guardar la clave de recuperación en un ordenador de ellos.
- **Guardar en un archivo**: directamente la guardas en un archivo en tu máquina, aunque es mejor idea guardarlo en algún lugar seguro.
- **Imprimir la clave de recuperación**: imprimirlo y ponerlo en papel es quizá la opción más segura, aunque requiere que tengas impresora. Es más segura ya que existe como copia física al que se tiene que tener acceso y conocimiento de su existencia.

Elija la opción que mejor te convenga. Si no quieres entretenerte mucho, simplemente guárdalo en un archivo.

Después preguntará por el espacio que quieres cifrar (figura 2c). Realmente, la primera opción, de cifrar sólo el espacio usado, es la más rápida, y es la que vamos a usar, mas la otra opción es posible que sea más segura al cifrar el dispositivo entero.

Finalmente, debemos de elegir el tipo de cifrado…algo. Realmente no elegimos directamente el tipo de cifrado, sino si queremos que sea algo portable a otras máquinas. La primera opción es mejor si sólo se va a usar este dispositivo en la máquina en la que se cifra. Pero como estamos usando un *pendrive*, lo más normal es que lo usemos en otras máquinas, lo cual nos conviene mejor la segunda opción.

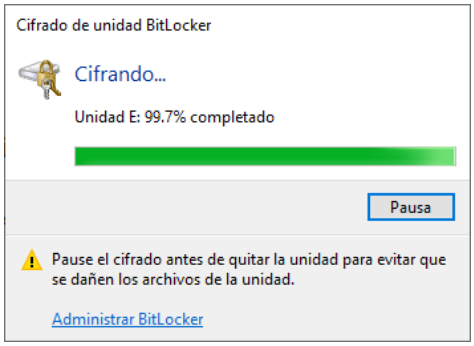
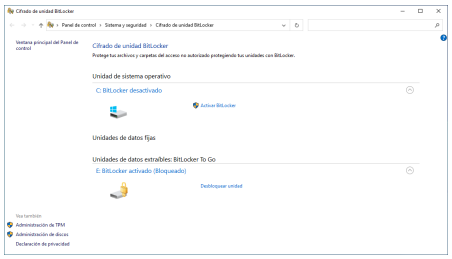
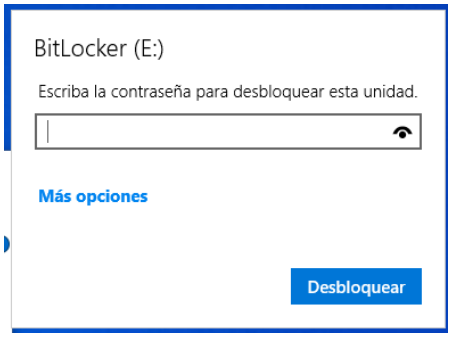


Figura 3: Proceso cifrando.

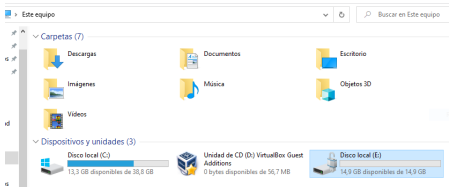
Al finalizar todo Bitlocker se pondrá a cifrar el dispositivo (figura 3). Este proceso puede tardar un tiempo dependiendo del tamaño y el tipo de cifrado.



(a) Ventana de administración Bitlocker.



(b) Entrada de contraseña para el desbloqueo.



(c) Disco cifrado desbloqueado.

Figura 4: Uso del dispositivo cifrado.

4. Abriendo un Pendrive Cifrado

Cuando tengamos hecho el cifrado, comprobaremos su correcto funcionamiento. Sacamos y volvemos a insertar el *pendrive*. Al hacer esto, nos dirá el navegador de archivos de Windows que «No se puede obtener acceso» al dispositivo. Para poder acceder a sus archivos, es necesario desbloquear el dispositivo con Bitlocker (figura 4a). Al seleccionar la opción de desbloquear nos pedirá la contraseña que le hemos puesto al dispositivo (figura 4b). Esta ventana aparecerá en la esquina superior diestra de la pantalla. Al introducir la contraseña, ya se podrá acceder al dispositivo de forma normal (figura 4c).

5. Desactivando Bitlocker

Es posible que queramos volver a desactivar el cifrado en nuestro dispositivo para que se pueda acceder de forma normal. Para esto podemos seleccionar la opción de «Desactivar Bitlocker» (figura 5a). Este proceso tardará un tiempo en finalizarse, dependiendo del tamaño del dispositivo. Al acabar el proceso, el dispositivo aparecerá igual que antes del cifrado (figura 5b), incluso con el mismo formateo (en este caso exFAT).

(a) Desactivar cifrado Bitlocker. (b) Dispositivo descifrado.

Figura 5

6. Conclusión

El cifrado es una herramienta bastante útil para guardar información de una manera segura, y Bitlocker es una de las muchas herramientas para hacerlo. También es algo universal, al menos para sistemas Windows, Mac, y Linux, ya que se encuentra disponible para las tres plataformas.[1]Diría que una de sus inconveniencias es el uso de interfaz gráfico. No lo digo por ser interfaz gráfico en sí, sino porque es una herramienta que lo más normal es que se quiera combinar con otras cosas, en cuyo caso es mejor trabajar desde la línea de comandos donde cada programa es un comando, que no en un interfaz gráfico donde se tiene que abrir una ventana nueva por cada programa. Imaginemos que quiero formatear un *pendrive* nuevo con cifrado. Haría falta particionarlo, formatearlo, y cifrarlo, lo que en la línea de comando podría ser tres instrucciones, en el entorno gráfico tardaría mucho más y sería más tedioso.

También le pongo falta a que no sea software libre, o al menos código abierto. Para las herramientas esto es importante, ya que si yo quisiera correr esto en un sistema BSD, por ejemplo, no podría. Al menos si fuera código abierto uno podría intentar portearlo al otro sistema.

No es una herramienta que usaría yo, ya que tampoco tengo necesidad de compatibilidad con sistemas Windows, y por lo tanto el cifrado LUKS me vale. Pero si tuviese que sugerir algún tipo de cifrado similar para Windows, Bitlocker no sería una opción mala.

[1] `https://www.easyuefi.com/bitlocker-for-linux/resource/access-bitlocker-drive-in-linux.html`

7. Derechos de Autor y Licencia