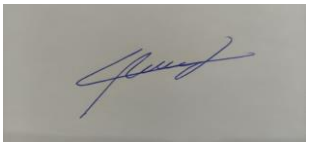
PRÁCTICA : E2 - Asegurar la CONFIDENCIALIDAD de los datos en Windows **MF0486_3 : Seguridad en Equipos Informáticos**	**Fecha**	07 / 03 / 2022
	Página 1 de 3	

Curso	**7.1. MF0486_3 Seguridad en equipos informáticos**	**Plan de Formación**	FC-2021.1/II.000/1914256

Nombre y Apellidos:	**PRUNELL ACOSTA, JAVIER**	**Firma del Alumno:**	
DNI:	54056004W	**Firma del Profesor:**	

Apto: ☐ **No Apto:** ☐ **Calificación:** ☐

Instrucciones Generales

La puntuación máxima será de 10 puntos.
Esta prueba tendrá una duración máxima de 420 minutos
(Temporalizados durante la Unidad de Aprendizaje)

El alumno/a deberá acatar las siguientes normas durante la duración de la práctica:

- Rellene el encabezado con su nombre, apellidos y D.N.I.
- Firme en todas y cada una de las hojas entregadas, incluidas las que estén en blanco.
- Usar exclusivamente bolígrafo azul o negro
- Guardar los ficheros generados en una carpeta con nombre **MF0486_E2**
- El docente le indicará al final como entregar el contenido de dicha carpeta
- Al finalizar el ejercicio y antes de entregarlo **comprueba tus respuestas**, en caso de duda consulta al docente.

Equipo y material

- Bolígrafo azul.
- Folios.
- Ordenadores.
- Conexión a Internet. (Para buscar información a modo de ayuda)
- **EFS :** Sistema operativo Windows 2000 (Virtualizado)
- **Bitlocker :** Sistema operativo Windows 8 pro (virtualizado)
- Pendrive.

Instrucciones específicas

El objetivo de esta práctica guiada será como se puede asegurar la **confidencialidad** de los datos en sistemas Windows, mediante la encriptación de archivos y carpetas.

Condiciones de realización:

La actividad se llevará a cabo en el aula y el alumnado contará en todo momento supervisión del docente.

El alumnado contará con una duración de 420 minutos para realizar la práctica.
Se podrá realizar en varias partes con una duración cada una de 60 minutos.

El alumno podrá hacer uso de internet para su realización, y se detallan a continuación algunas webs de ayuda.

Páginas webs :

EFS (Encrypting File System)

https://es.wikipedia.org/wiki/EFS
https://technet.microsoft.com/en-us/library/cc700811.aspx

BitLocker (BitLocker Drive Encryption)

https://es.wikipedia.org/wiki/BitLocker_Drive_Encryption

En ella se valorará la utilización de herramientas para la gestión del tiempo y secuenciación del uso de las aplicaciones necesarias. Y se observará especialmente la autonomía del alumnado a la hora de ejecutar y tomar decisiones. Como también la estructuración del ejercicio en donde se solicitará, orden, coherencia y limpieza.

Una vez terminado la práctica se le notificará al docente y pasará a su evaluación.

Descripción de la práctica

En esta práctica, vamos a cifrar archivos con la finalidad de mantenerlos seguros ante cualquier intrusión y así mantener un nivel de confidencialidad e integridad de los datos de una forma técnica y segura. Tendremos dos opciones principales, dentro de las herramientas de Windows, tenemos los dos sistemas de seguridad cifrada; EFS y la herramienta Bitlocker (solamente disponible a partir de la versión Windows Pro o posteriores).

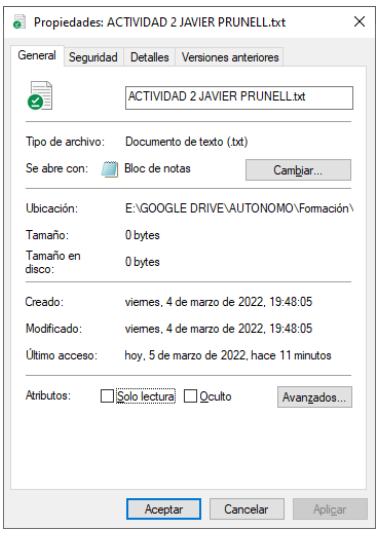
DIFERENCIAS ENTRE EFS Y BITLOCKER, ¿CUÁL ELEGIR?

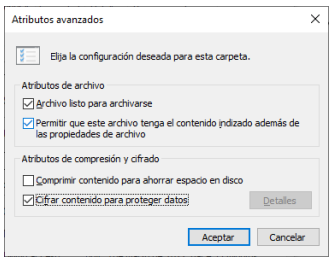
¿Cuál utilizar a la hora de cifrar?, tenemos que tener claro que los sistemas son diferentes. Principalmente el EFS, un sistema de cifrado que puede cifrar tanto archivos individuales como carpetas dentro del disco duro. El BitLocker se trata de un software capaz de cifrar toda una unidad para impedir que los usuarios no autorizados puedan acceder a los datos que contengan. Así que a la hora de cifrar, debemos de analizar previamente que debemos utilizar.

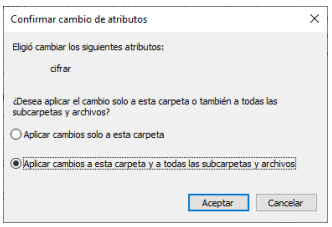
CIFRAR UN ARCHIVO MEDIANTE EL SISTEMA EFS

A grandes rasgos, el sistema EFS (Encrypting File System), está disponible desde Microsoft Windows 2000 que permite a los archivos contenidos ser cifrados en las particiones NTFS en donde esté habilitado para proteger datos confidenciales de personas con acceso físico a la computadora. EFS es incompatible con la compresión de carpetas.

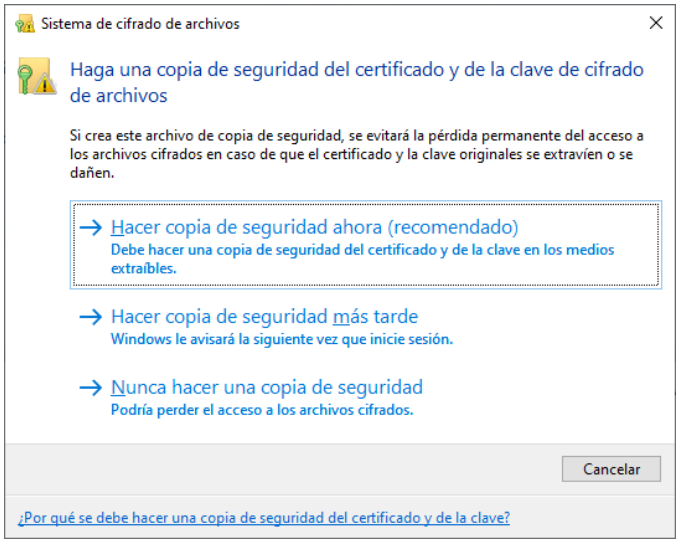
- Primeramente, vamos a seleccionar un archivo. Accedemos con el botón derecho a propiedades > Pestaña General > Avanzados > Cifrar contenido para proteger datos > Aceptar > Aplicar cambios a esta y a todas las subcarpetas y archivos.

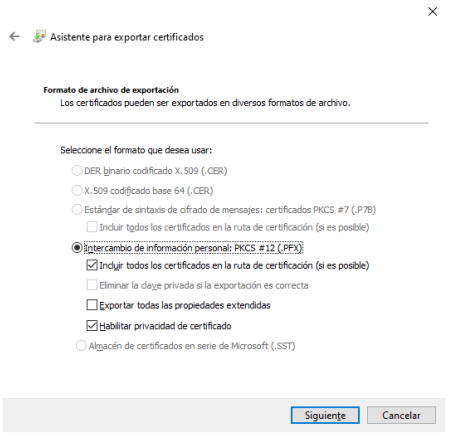




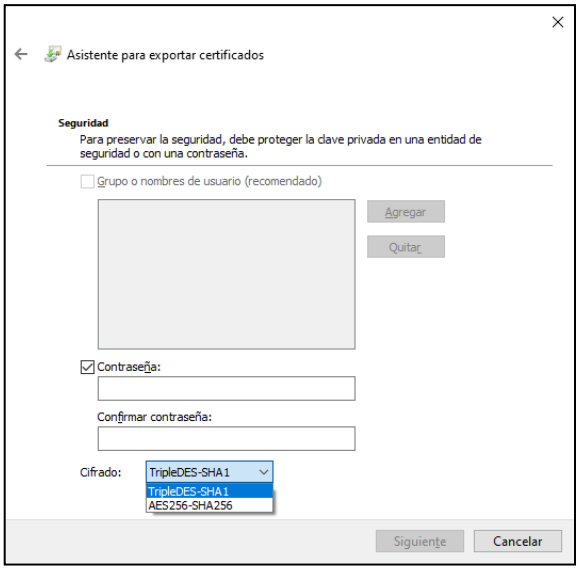


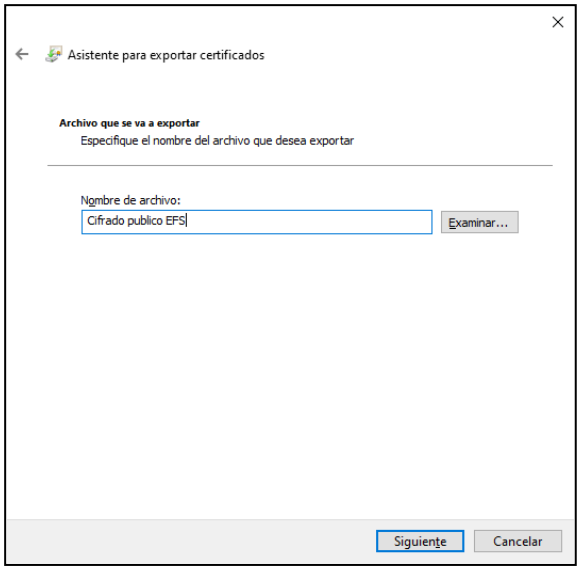
- Al terminar con el cifrado EFS, el sistema operativo te recomienda que realices una copia de seguridad de tu clave de cifrado.
- En este caso, vamos a seleccionar PKCS que es una clave publica EFS. El archivo exportado estará en formato (.PFX). Este formato también lo encontramos en los sitemas de certificados digitales o firma digitales del Estado.





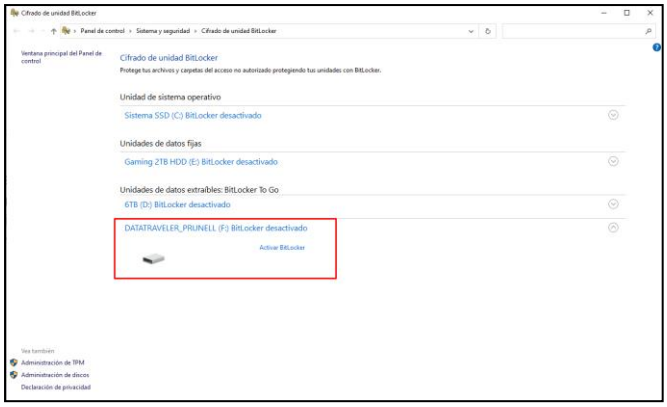
- Ahora nos pedirá la contraseña. En este caso, tendremos dos tipos de cifrados para ella. El cifrado DES está en desuso. Por lo tanto, cifraremos nuestra carpeta con AES256. En este caso, la contraseña será **ABCD1234.** Se introduce el nombre del archivo y guardamos finalizamos el asistente.

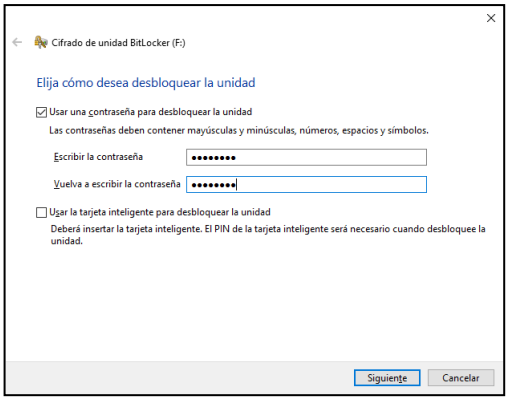




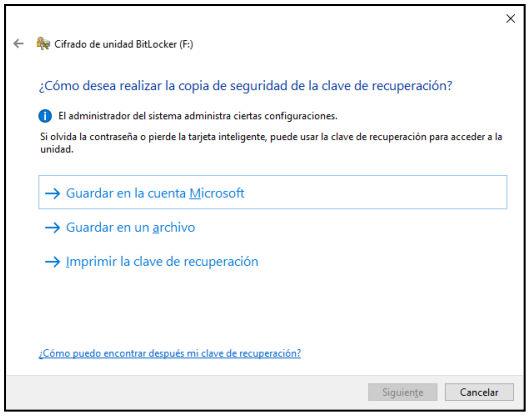
CIFRAR UN ARCHIVO CON BITLOCKER

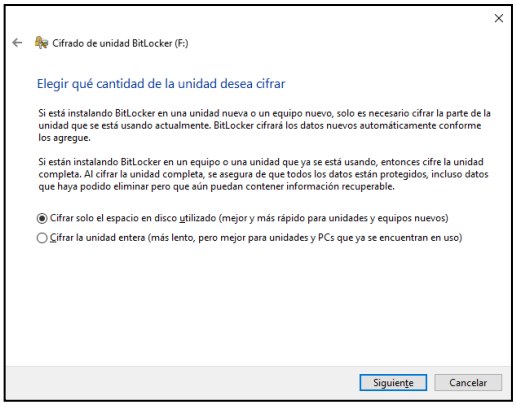
Para cifrar una unidad completa con Bitlocker, debemos recordar que solamente encontramos esta herramienta en algunas versiones de Windwos 10, en este caso, de Windows 10 Profesional en adelante. Primeramente, debemos elegir un sistema de almacenamiento de la información. En este caso, utilizaremos un pendrive para cifrar todo el contenido interno:

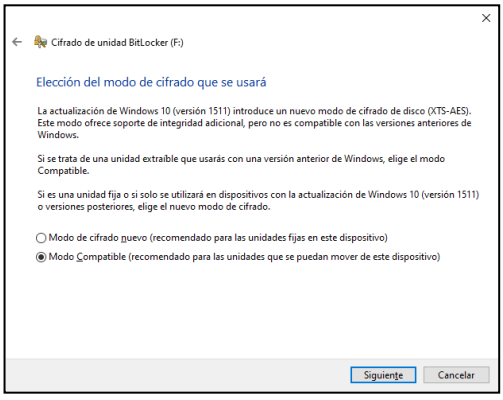




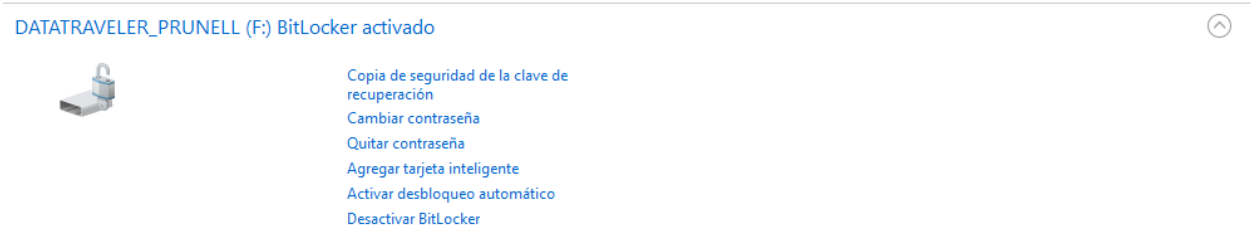
Vamos a utilizar la misma contraseña que antes en EFS; **ABCD1234.** Posteriormente, el Bitlocker nos ofrece tres posibilidades para recuperarla clave. Nosotros vamos a guardar la contraseña en un archivo txt. La siguiente pantalla, nos indica los dos modos; cifrado nuevo o modo compatible.







Por último, tenemos toda la unidad cifrada, y por lo tanto, podemos administrar la unidad con los siguiente elementos:



CIFRADO EN LINUX

Como dato externo a la práctica, no podemos olvidar el cifrado en Linux. El sistema EFS y el Bitlocker están centralizados en Windows, pero en Linux, podemos encontrarnos con el sistema GnuPG o GPG (GNU Privacy Guard) es un software desarrollado por la FSF (Free Software Foundation) para implementar un programa de compatibilidad con OpenPGP. Se pueden cifrar y descifrar mensajes en texto plano, ficheros, y hacer firmas digitales para asegurar el contenido que transferimos por correo electrónico o por cualquier otro servicio de red. Además, GPG es libre y gratuito bajo licencia GPL.