

CENTRO DE ESTUDIOS PROFESIONALES  
[Glorieta Ángel Herrera Oria, s/n, 41930 Bormujos, Sevilla](https://goo.gl/maps/MeykttZYGNUCQCnK8)  
  
HERRAMIENTAS DE CIFRADO

****

Realizado por: Juan Gabriel Sánchez Vivero

**TABLA DE CONTENIDOS**

[1. ENUNCIADO 1](#_Toc165024117)

[2. EJERCICIO 1](#_Toc165024118)

[3. TPM 6](#_Toc165024119)

[4. CONCLUSIONES 7](#_Toc165024120)

HOJA DE CONTROL DEL DOCUMENTO

|  |  |  |  |
| --- | --- | --- | --- |
| DOCUMENTO / ARCHIVO | | | |
| Fecha última Modificación | 26/04/24 | Versión / Revisión | v01r02 |
| Fecha Creación | 25/04/24 |  | |
| Fecha Finalización | 26/04/24 |
| Ubicación Física | ------- |

|  |  |  |
| --- | --- | --- |
| REGISTRO DE CAMBIOS | | |
| Versión / Revisión | Página | Descripción |
| v01r01 | 1-5 |  |
| v01r02 | Resto |  |
|  |  |  |

|  |  |
| --- | --- |
| AUTORES DEL DOCUMENTO | |
| Apellidos, Nombre | Curso |
| Sánchez, Juan Gabriel | 1º Desarrollo de aplicaciones WEB |
|  |  |
|  |  |
|  |  |
|  |  |

|  |  |  |
| --- | --- | --- |
| PREPARADO | REVISADO | APROBADO |
| Sánchez, Juan Gabriel | Sánchez, Juan Gabriel | Sánchez, Juan Gabriel |

1. ENUNCIADO

En esta práctica, (según el sistema elegido) vamos a aprender a usar un sistema de encriptación (BitLocker), para cifrar una partición de datos, igualmente se aprenderá como descifrar la unidad.

1. EJERCICIO

Vamos a utilizar un disco duro externo para el cifrado. Para ello usaremos Bitlocker de Windows, abrimos Bitlocker de Windows y le damos a activar en el disco duro externo:

Interfaz de usuario gráfica, Sitio web

Descripción generada automáticamente

Se nos preguntará cómo deseamos desbloquear la unidad, seleccionamos la opción “Usar una contraseña para desbloquear la unidad”:

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Lo siguiente que se nos pregunta es cómo queremos hacer la copia de seguridad de la clave de recuperación. Existen los siguientes modos; “Guardar en la cuenta Microsoft”, “Guardar en un archivo” o “Imprimir la clave de recuperación”.

Nosotros elegiremos la opción “guardar en un archivo”:

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

A continuación, se nos da la opción de elegir qué cantidad deseamos cifrar, en la imagen puede verse las opciones, nosotros elegiremos “Cifrar la unidad entera”:

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

En el siguiente cuadro de diálogo, se nos pide el modo de cifrado, existen dos opciones, una para unidades fijas en el equipo y otra para unidades movibles del mismo (modo compatible).

Nosotros elegiremos la opción “modo compatible” ya que lo estamos haciendo en un disco duro externo:

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

y ya por último se nos pregunta si estamos listo para cifrar, le damos al botón “Iniciar cifrado”:

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Ahora comenzará el proceso de cifrado, las opciones que hemos elegido van a tardar bastante ya que cifraremos toda la unidad:

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Sitio web

Descripción generada automáticamente

Ahora tan sólo tenemos que desconectar y volver a conectar el disco usb y podremos ver como nos indica que está cifrado:

Captura de pantalla de computadora

Descripción generada automáticamente

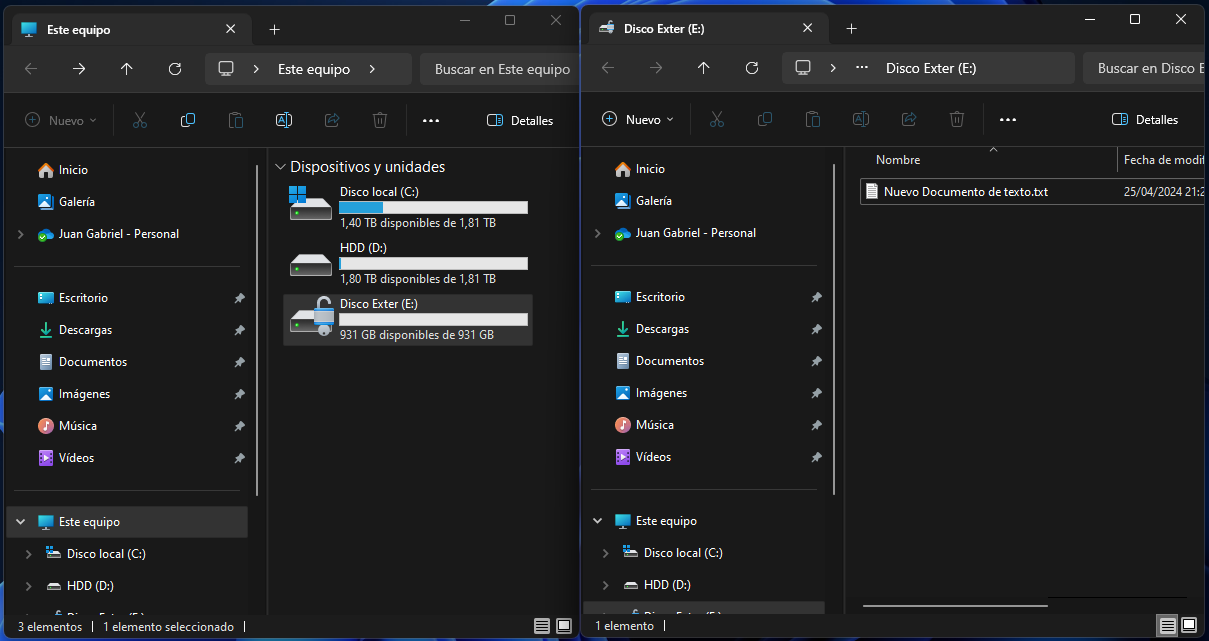
Presionamos en Mas opciones e introducimos la contraseña de recuperación:

Introducimos la contraseña que generamos anteriormente y guardamos en un archivo en el escritorio:

Captura de pantalla de computadora

Descripción generada automáticamente

Presionamos en desbloquear y ya podremos ver el contenido de nuestro disco:



1. TPM

TPM o módulo de plataforma de confianza, es un chip de seguridad que está en la placa base o en un procesador tiene funciones de seguridad para almacenar información confidencial.

TPM es un método de seguridad basado en hardware y software, forma parte del proceso de inicio de una computadora.

TPM tiene un número único pudiendo soportar los ataques lógicos y físicos para proteger las claves y credenciales almacenadas.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Para activarlo debemos comprobar si nuestra placa base lo soporta, aunque el sistema se implemento de forma obligatoria para la instalación de Windows11 y es relativamente moderno, muchas placas gracias a una actualización de BIOS pueden conseguir la compatibilidad con él.

1. CONCLUSIONES

Las herramientas de cifrado son muy útiles cuando queremos proteger nuestra información.

Recalcar la importancia de su uso en copias de seguridad y aunque no haya un método que sea infalible uno de los mas seguros es la clave física, en donde se necesite al usuario para poder desbloquear el cifrado.

TPM bajo mi opinión esta muy bien, ya que obtenemos mas seguridad para nuestro hardware y software, pero pienso que es una herramienta mas de control para los usuarios, teniendo u código único e identificativo y hasta donde sabemos inmodificable. Por lo que hace a tu equipo único.

En resumen, la seguridad de nuestro datos y equipos es muy importante, cosa que deberíamos de tomarnos en serio ya que estamos conectados a una gran red en la cual no creemos que seamos invisibles pero la cantidad de datos que compartimos es muy grande.