

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

HERRAMIENTAS DE CIFRADO:

BITLOCKER

Imagen que contiene Texto

Descripción generada automáticamente

Realizado por:

Jhonatan Guzmán Panozo

1º DAW

**ÍNDICE**

[**HOJA DE CONTROL DEL DOCUMENTO** 1](#_Toc165655523)

[1. INTRODUCCIÓN 2](#_Toc165655524)

[2. PRÁCTICA 2](#_Toc165655525)

[3. TPM 11](#_Toc165655526)

[4. CONCLUSIONES 12](#_Toc165655527)

# **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.

1. PRÁCTICA

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamenteInterfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamenteHacemos click derecho en Inicio y pulsamos Administrador de discos.

Interfaz de usuario gráfica, Texto

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

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamenteAhora especificamos el tamaño de gigas que queremos.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamenteY nos aparece así

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamenteAhora sobre él, pulsamos click derecho y Nuevo volumen simple…

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamenteInterfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamenteInterfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamenteInterfaz de usuario gráfica, Aplicación

Descripción generada automáticamenteY le damos Siguiente a todo.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamenteY Finalizar

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

Captura de pantalla de un celular

Descripción generada automáticamente

Captura de pantalla de un celular

Descripción generada automáticamenteEn nuestra carpeta BITLOCKER(E:) ponemos los archivos que queremos proteger.

Ahora click derecho sobre nuestra carpeta y Activar Bitlocker

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamenteEmpezará a cargar

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamenteY escribimos contraseña

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

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

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

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

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

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Y comienza el cifrado.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Gráfico, Gráfico de rectángulos

Descripción generada automáticamenteEn mi caso he guardado el archivo en el escritorio

Ahora podemos ver como queda con un candado abierto.

Interfaz de usuario gráfica

Descripción generada automáticamente

Para poder ver cambios, debemos reiniciar el ordenador.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamenteAhora para acceder debemos poner la contraseña de antes. Y ya estaría.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica, Aplicación, Teams

Descripción generada automáticamenteEn caso de haber olvidado la contraseña, le damos a más opciones.

Y abrimos nuestro archivo guardado para desbloquearlo.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Y desbloqueamos.

Tabla

Descripción generada automáticamente con confianza baja

Y ya podemos acceder a nuestra carpeta.

Captura de pantalla de un celular

Descripción generada automáticamente

1. 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:

Pantalla de computadora con fondo negro

Descripción generada automáticamente con confianza baja

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamenteY nos saldrá la siguiente información:

1. 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

Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto

Descripción generada automáticamente Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamenteInterfaz de usuario gráfica, Texto

Descripción generada automáticamenteY 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.