|  |  |  |  |
| --- | --- | --- | --- |
| **Nombre y Apellidos:** | **RUNE BRITO NUÑEZ** | **Firma del Alumno:** |  |
| **DNI:** | 78852907Y | **Firma del Profesor:** |  |

|  |  |  |
| --- | --- | --- |
| **Apto:** | **No Apto:** | **Calificación:** |

**Instrucciones Generales**

La puntuación máxima será de 10 puntos.

Esta prueba tendrá una duración máxima de 100 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.

**Descripción de la práctica**

**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 100 minutos para realizar la práctica.

Se podrá realizar en cuatro partes con una duración cada una de 25 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://es.wikipedia.org/wiki/EFS%20)

<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.

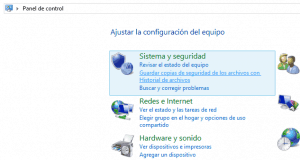
**RUNE BRITO NUÑEZ**

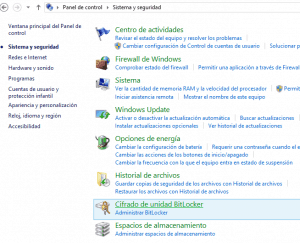
**SEGURIDAD INFORMATICA**

**MF0486\_3. PRACTICA E2**

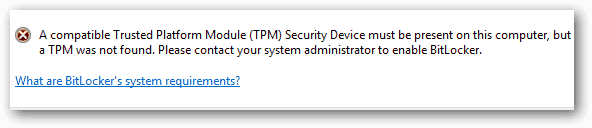
Lo primero que se realizó fue instalar el Windows 8.1 en el virtual box y a su vez se creó un disco duro con etiqueta RBN en D:/

Se intenta activar BitLocker en Windows 8.1, se hizo desde el Panel de Control/Sistema y Seguridad/Cifrado de unidad BitLocker y dar clic en Activar Bitlocker.

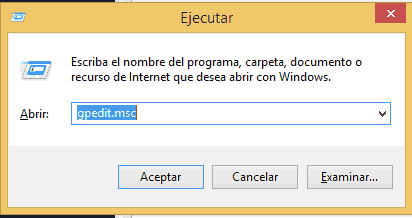




En el proceso, apareció un mensaje, el cual no, nos permite su activación; ya que Windows no tiene un módulo TPM que permita su activación por estar en modo virtual.

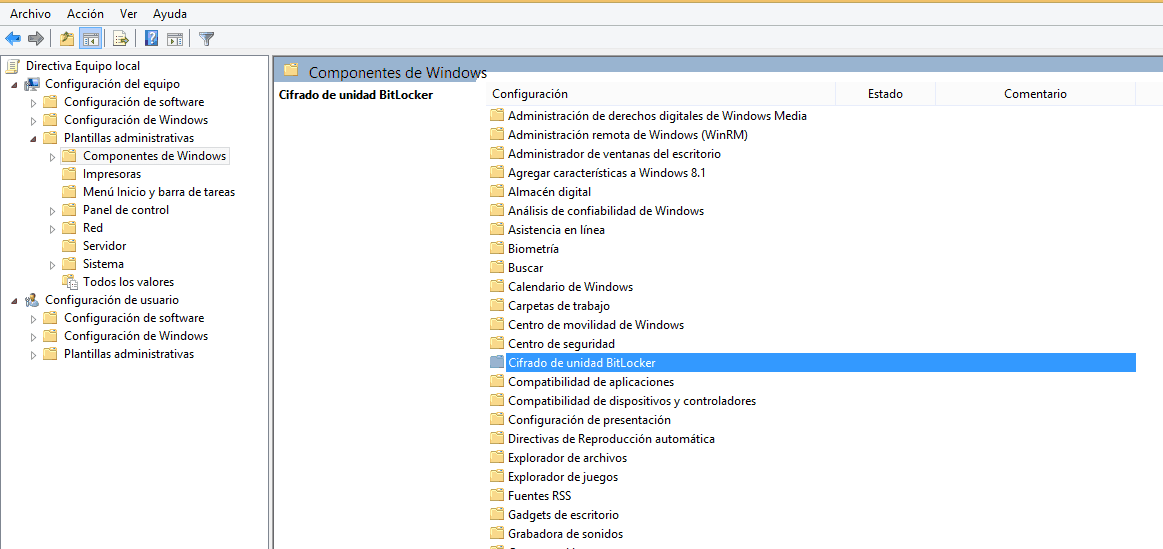


Para darle una solución, se ejecutó el comando “qpedit.msc” y solventar el incidente.

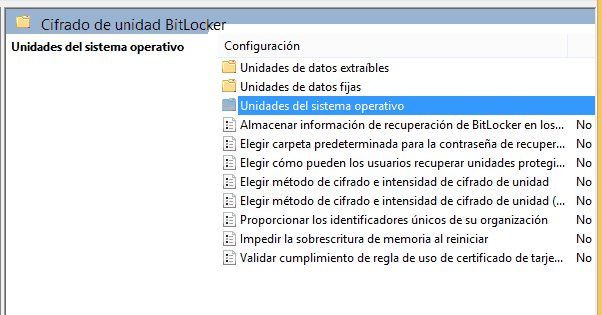


Y se buscó en el editor de directivas de grupo local, en el árbol, la siguiente ruta:  
**Configuración del Equipo/Plantillas Administrativas/Componentes de Windows/Cifrado de Unidad Bitlocker**

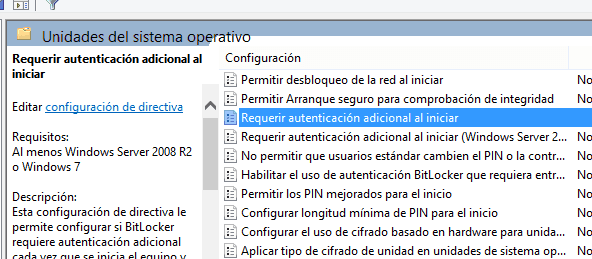
Al abrir esa carpeta nos mostrará lo siguiente:



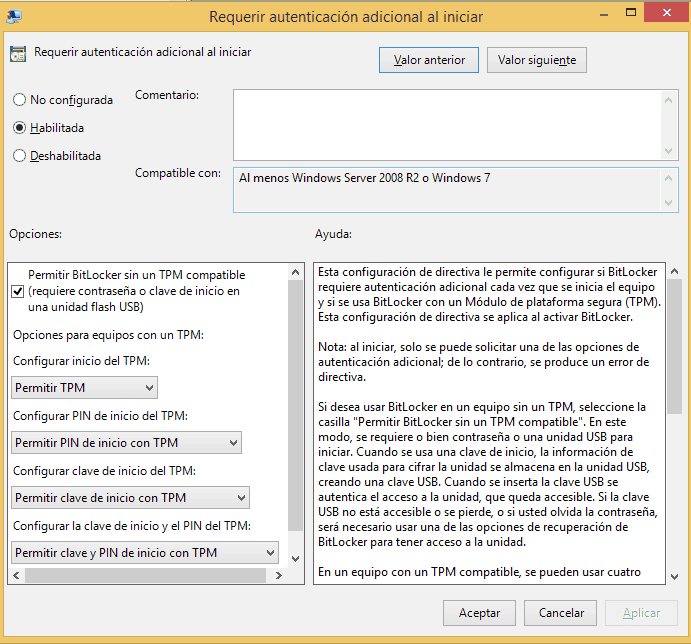
Ahí se abrió la carpeta: **Unidades del Sistema Operativo**



Y se seleccionó: **Requerir autenticación adicional al iniciar**

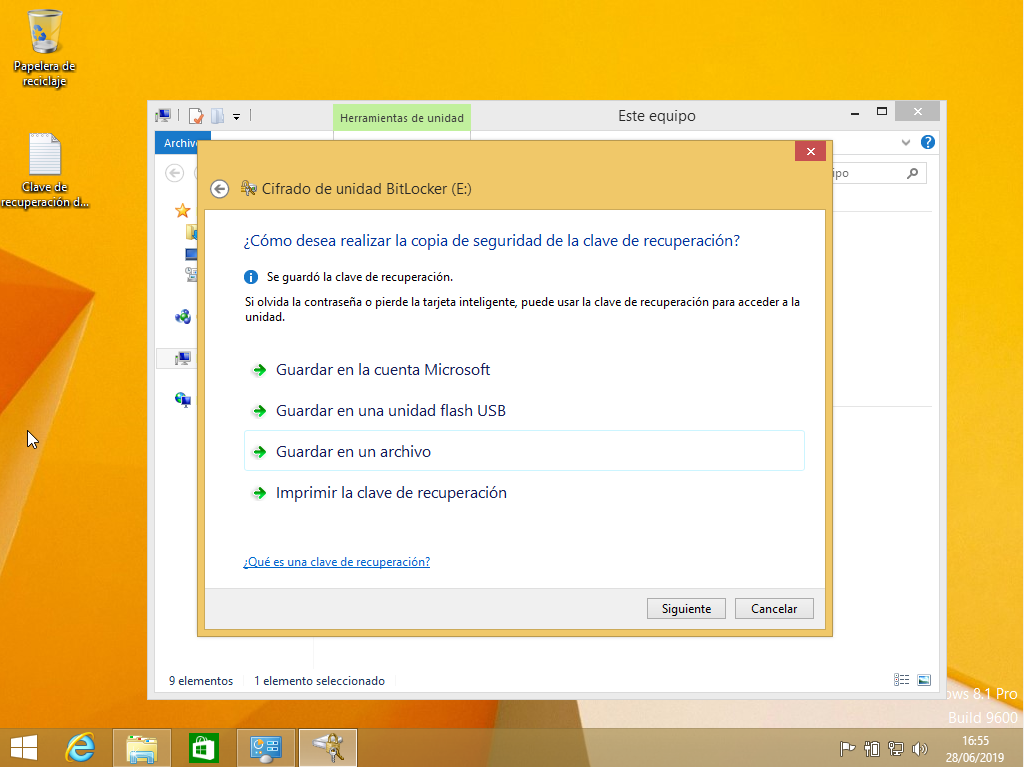


Por defecto esta directiva está como **No configurada**, solo hay que **Habilitarla** y verificar que la casilla con el texto: **Permitir Bitlocker sin un TPM compatible**, tal cual en la imagen

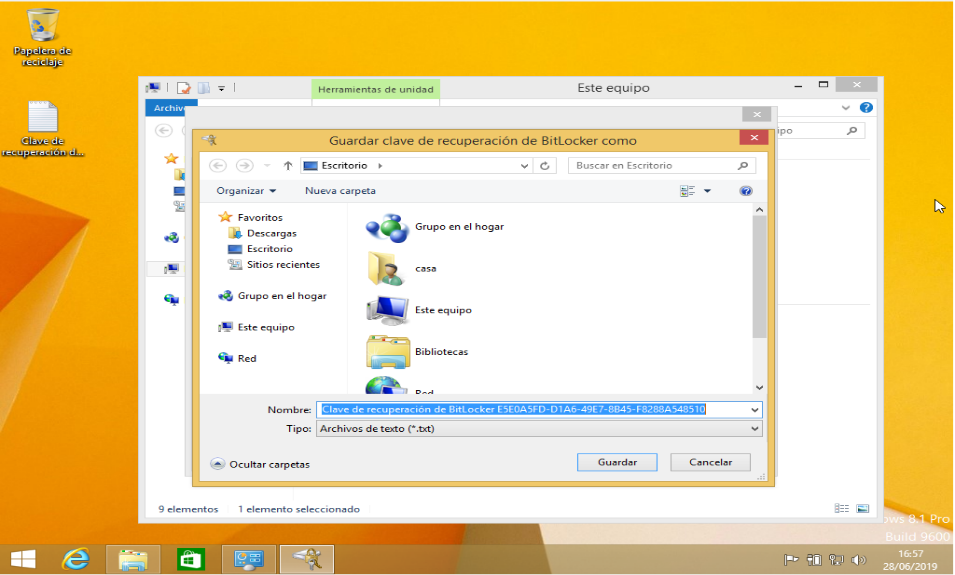


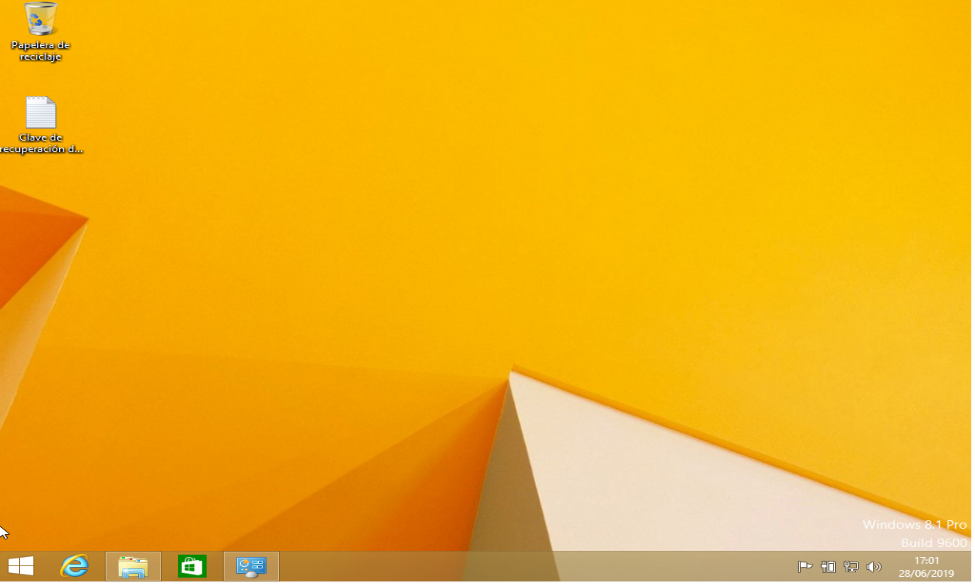
Una vez que nos cercioramos que está seleccionada, damos clic en **Aceptar** para poder iniciar la encriptación del disco.

A continuación, se procede con la encriptación del volumen RBN. Para ello se ejecutó el BitLocker en dicho volumen. Y nos pidió una forma de autenticarse entre varias opciones. Para este caso se generó un archivo con una contraseña en formato” TXT”

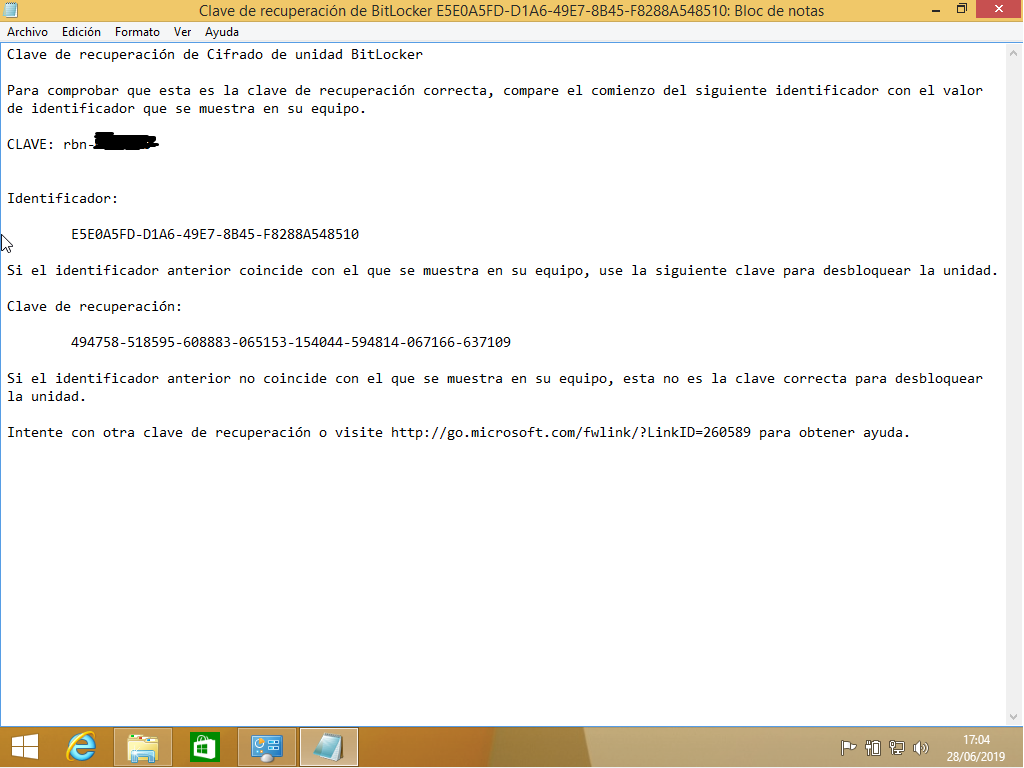


Después de este paso, el mismo Windows preguntó dónde guardar la información de recuperación de BitLocker, por si olvidamos la contraseña. Para ello, se seleccionó el escritorio como destino para el archivo “.TXT”





Una vez abierto el archivo, se verificó que contenía el identificador, y la clave de recuperación, por sí la clave original se extravía.



Por último, podemos observar que se crea la encriptación para todo el volumen RBN en D:/. Teniendo como icono un candado.

