Nombre y Apellido:

# LABORATORIO

# Hardware y Redes

**Experiencia: 09**

NOMBRE Y APELLIDO:

## Práctica de Laboratorio 09

Cifrando nuestro dispositivo de almacenamiento externo con Windows

## OBJETIVOS

1. Identificar el sistema operativo utilizado
2. Proteger los dispositivos de almacenamiento.

## MATERIALES

- ✓ Dispositivo de almacenamiento externo (pendrive, disco externo).
- ✓ Notebook o PC
- ✓ Equipos con Windows 10

## MARCO TEÓRICO

Bien sabemos la importancia de la protección de datos en la actualidad; también estamos en conocimiento que existen varias herramientas y métodos para hacerlos, pero muchas veces costosas. Confiar datos sensibles a empresas o personas muchas veces no es la solución más certera en cambio si uno posee un resguardo físico cerca suyo siempre estará más seguro de saber que esos datos importantes están ahí y protegidos.

Es muy interesante resaltar la importancia de esta herramienta que nos ofrece algunas de las versiones de este sistema operativo ya que el cifrado puede proteger los datos en el dispositivo haciendo que solo las personas con permiso o autorización tengan acceso a dichos dispositivos.

NOMBRE Y APELLIDO:

**PROCEDIMIENTOS**

Para desarrollar esta práctica se debe activar el cifrado de BITLOCKER en una unidad de datos extraíble y en la unidad del sistema operativo Windows 10. Dicha utilidad está desactivada de manera predeterminada y debe activarse para cada unidad que tenga que cifrar. Para activar y configurar nos vamos en PANEL DE CONTROL, en la vista de íconos pequeños, hacemos click en Cifrado de Unidad con BitLocker.

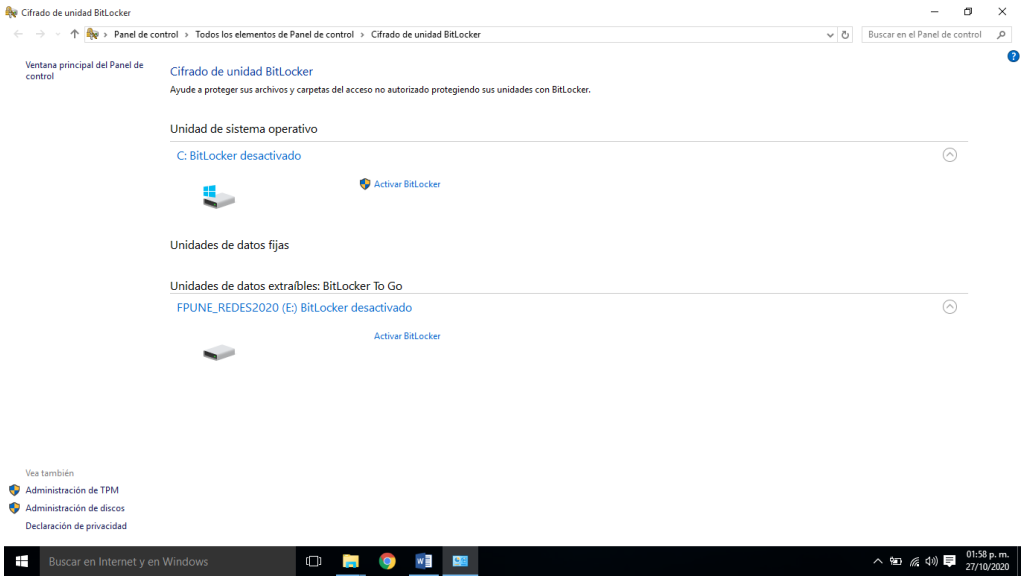


***Figura 1.1 Cifrado de Unidad BitLocker***

NOMBRE Y APELLIDO:

**Desarrollo del trabajo**

**Paso 1:**

Con la orientación del profesor instructor procedemos a activar BitLocker en las Unidades de discos extraíbles.

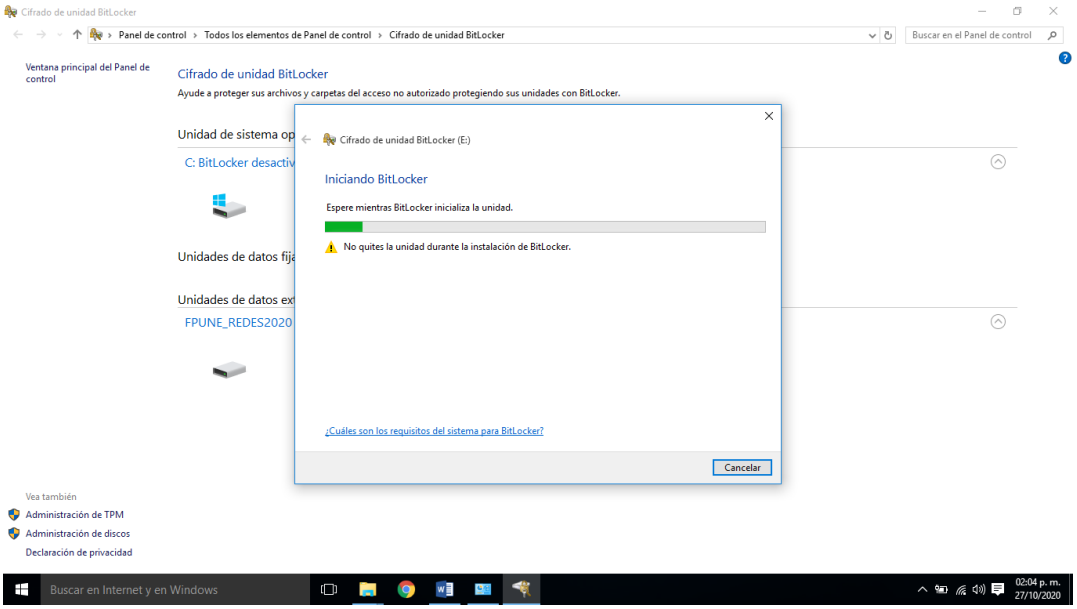


***Figura 1.2 Activando BitLocker***

NOMBRE Y APELLIDO:

**Paso 2**

Optamos como queremos desbloquear la unidad FPUNE_REDES2020 elegimos en este caso:

- Usar una contraseña para desbloquear la unidad
- Establecemos la contraseña y damos click en siguiente

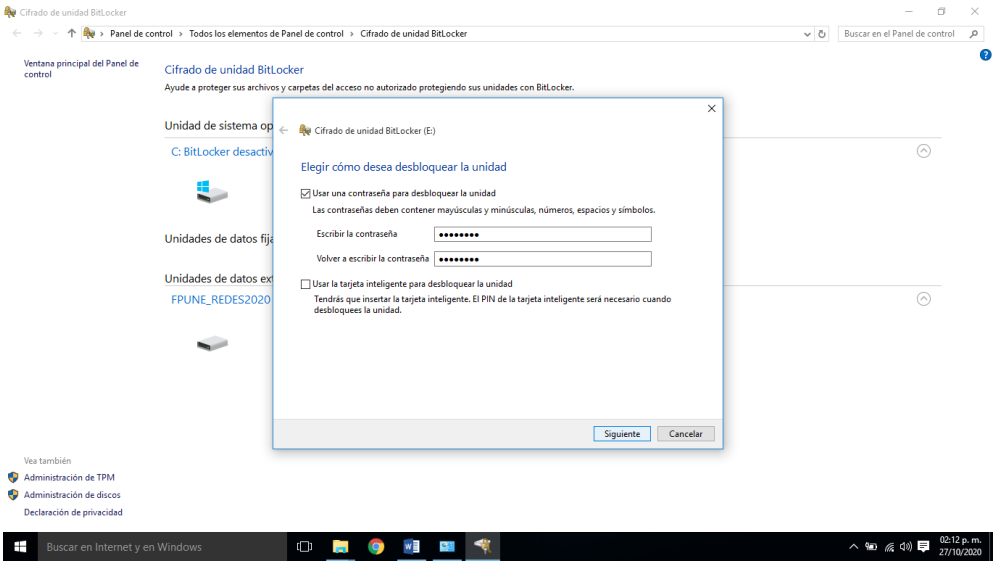


***Figura 1.3 Estableciendo contraseñas***

NOMBRE Y APELLIDO:

**Paso 3**

En este paso realizamos una copia de seguridad de la clave de recuperación en caso de que uno se olvida o pierde la contraseña asignada. Seleccionamos Guardar en un Archivo y luego Siguiente. Establecemos el nombre al archivo y luego Guardar.

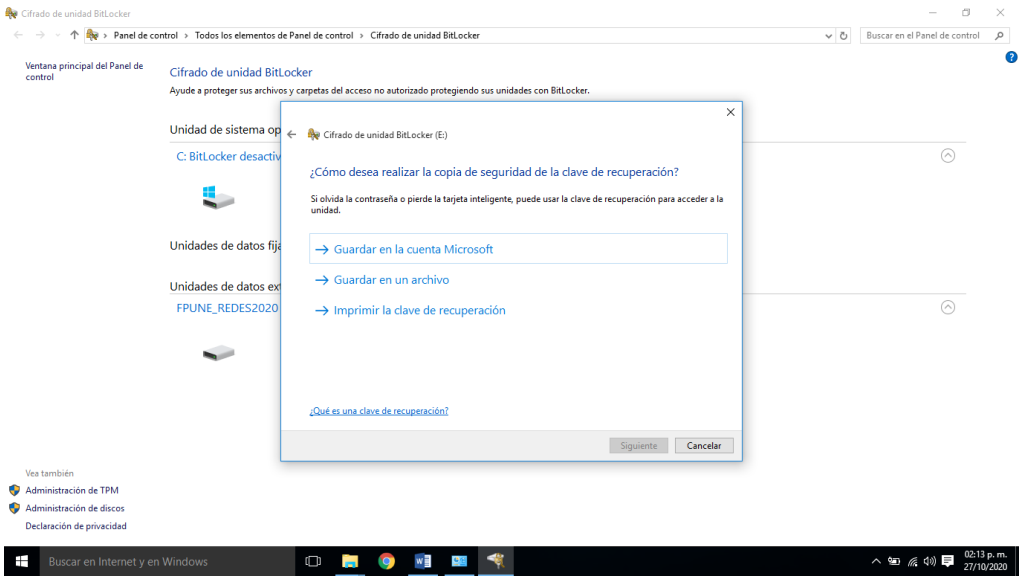


***Figura 1.4 Copia de Seguridad***

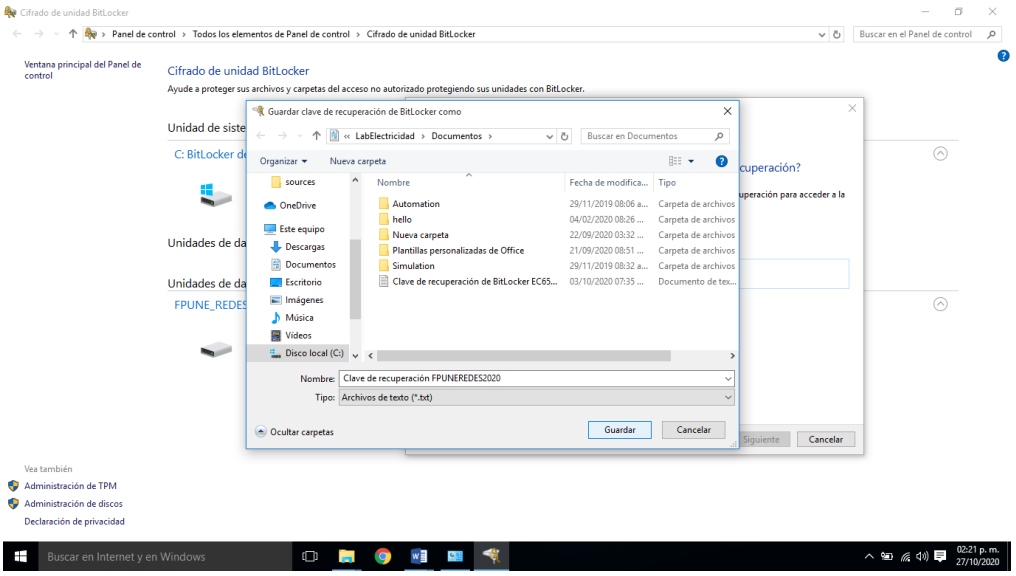


***Figura 1.5 Guardando el archivo***

NOMBRE Y APELLIDO:

**Paso 4**

En este paso elegimos la cantidad de la unidad que uno desea cifrar. Seleccionamos Cifrar la unidad entera y luego click en siguiente.

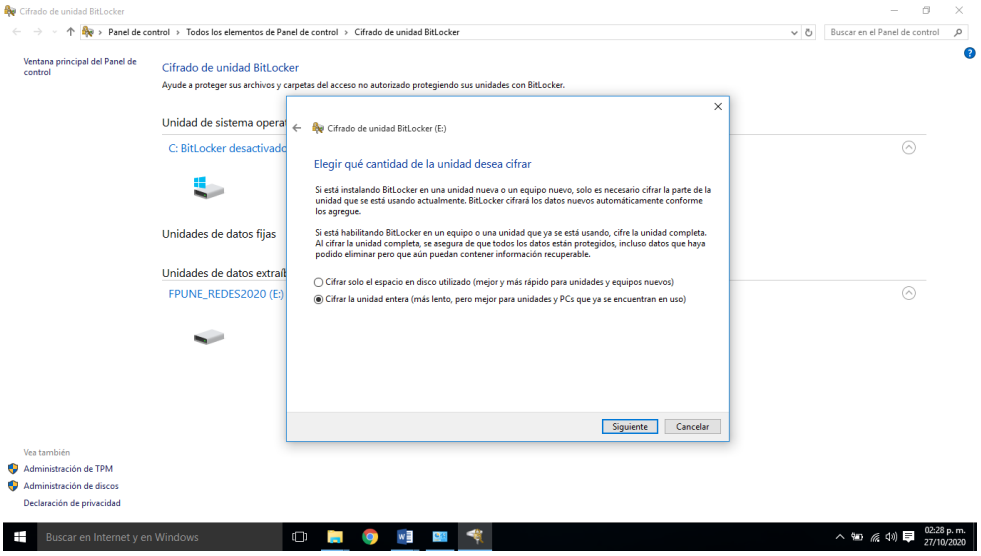


***Figura 1.5 Cantidad de la Unidad***

**Paso 5**

Esperemos a que realice el cifrado completo de la unidad. Damos click en Iniciar cifrado

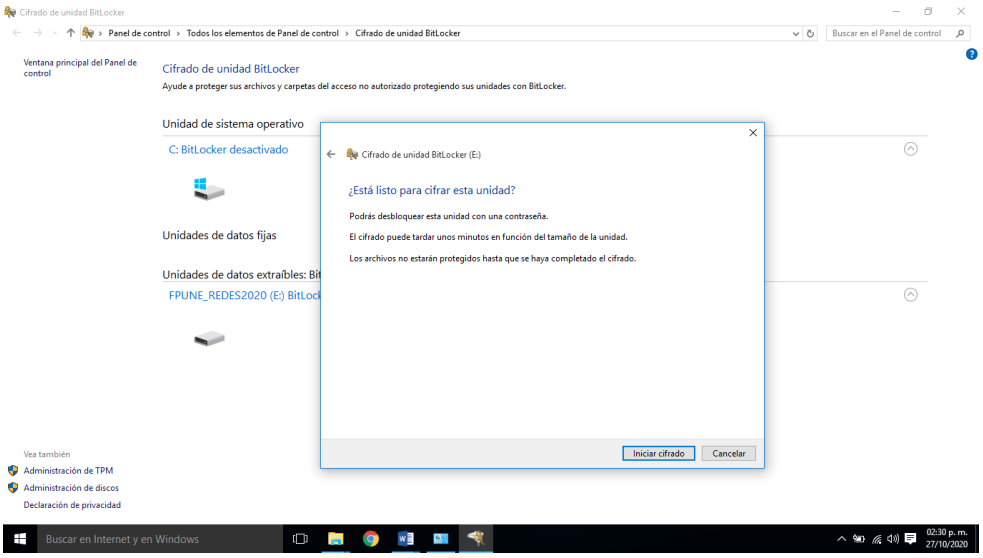


***Figura 1.6 Iniciando Cifrado***

NOMBRE Y APELLIDO:

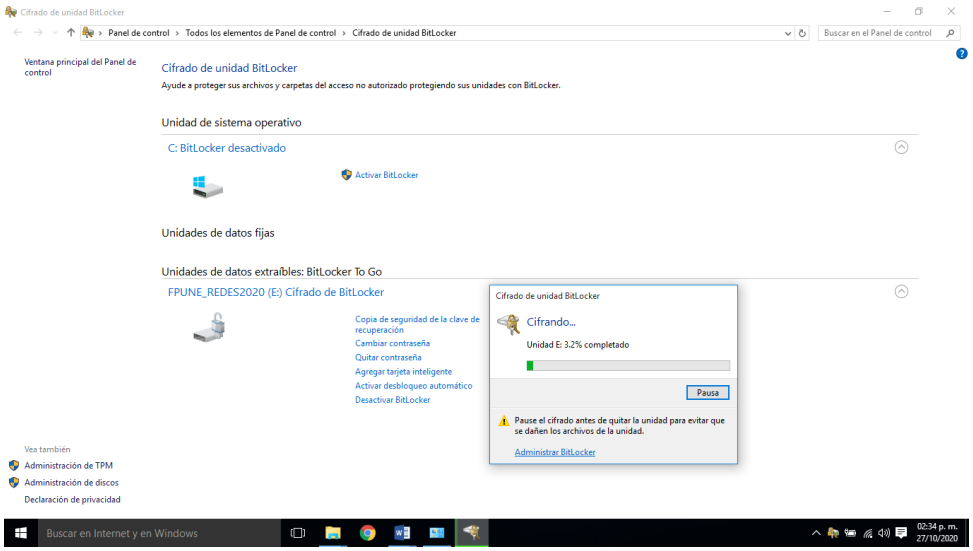


***Figura 1.7 Proceso de Cifrado***

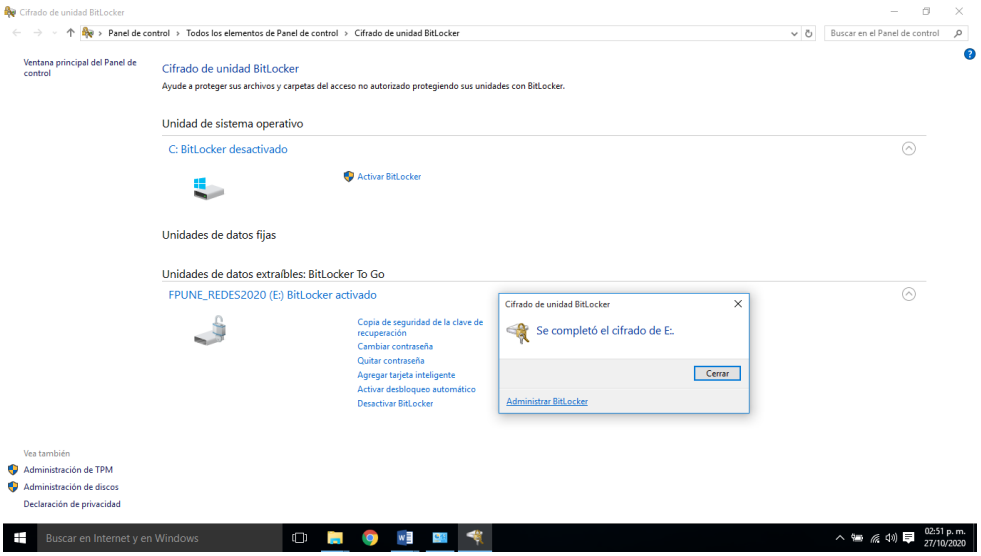


***Figura 1.8 Cifrado completo***

NOMBRE Y APELLIDO:

**Paso 6**

Accedemos a la unidad cifrada FPUNE_REDES2020; insertamos la unidad y navegamos hasta la unidad USB en el Explorador de archivos o Windows Explorer y abrimos la unidad USB (Si no logran abrir la unidad, click con el botón derecho y buscar la opción Desbloquear unidad)

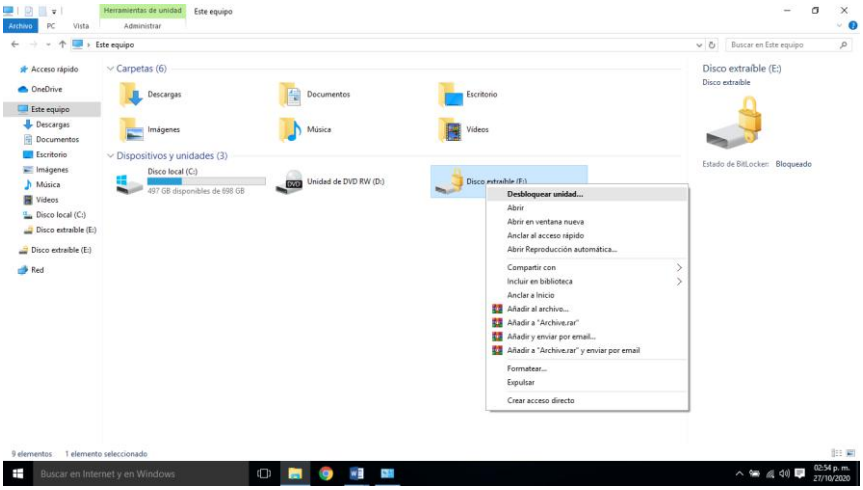


***Figura 1.7 Accediendo a la unidad cifrada***

**Paso 7**

Hacemos clic en el botón Más opciones. Observe que hay una opción para ingresar la clave de recuperación. Si olvida la contraseña, se puede utilizar la clave de recuperación guardada o impresa en el paso 3 para desbloquear la unidad.

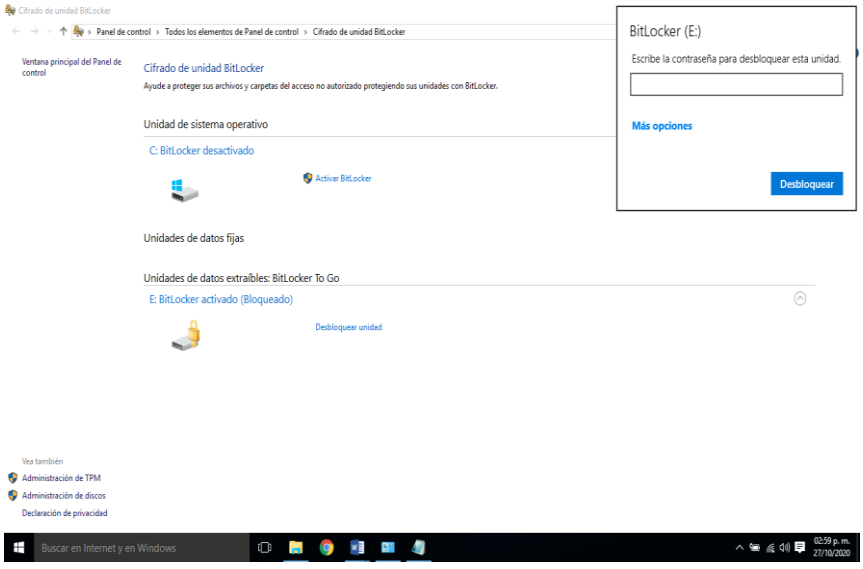


***Figura 1.8 Más opciones del Cifrado***

NOMBRE Y APELLIDO:

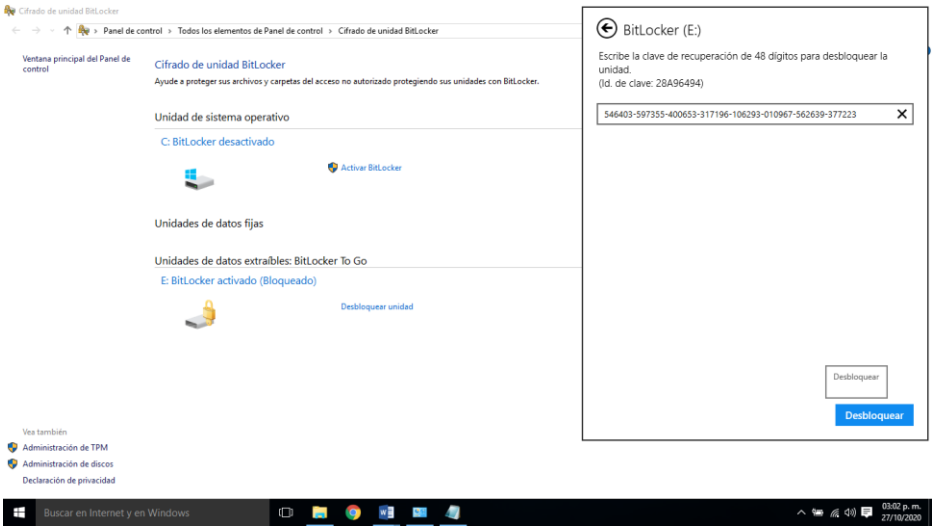


*Figura 1.9 Datos de recuperación*

**Paso 8**

Haga clic en **Desactivar BitLocker** cuando reciba el mensaje que le notifica que el proceso de descifrado podría tardar algún tiempo. Observe el mensaje de advertencia para no dañar el contenido de la unidad. Hacer click en Cerrar cuando termine el proceso de descifrado.

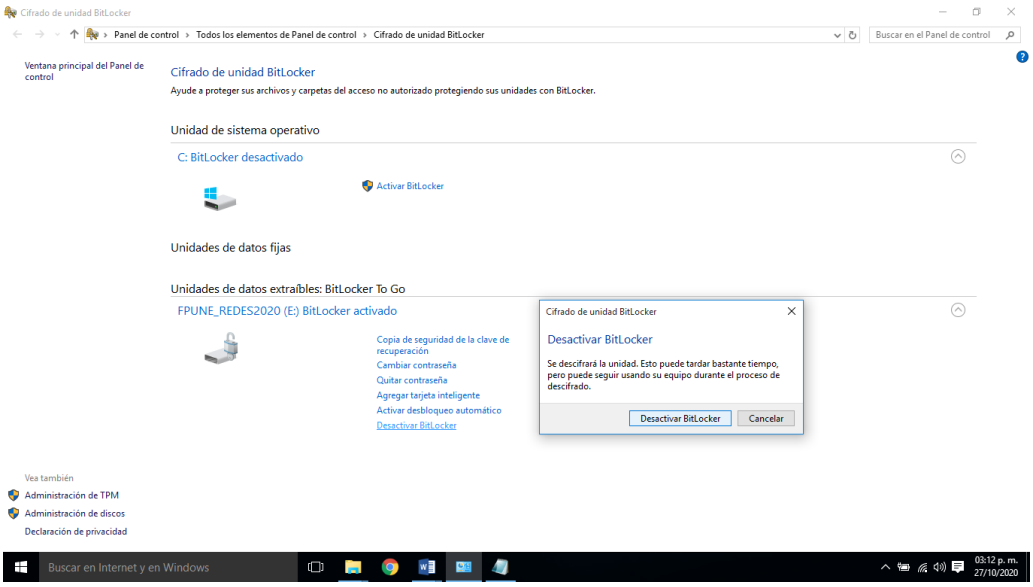


*Figura 1.10 Proceso de descifrado*

NOMBRE Y APELLIDO:

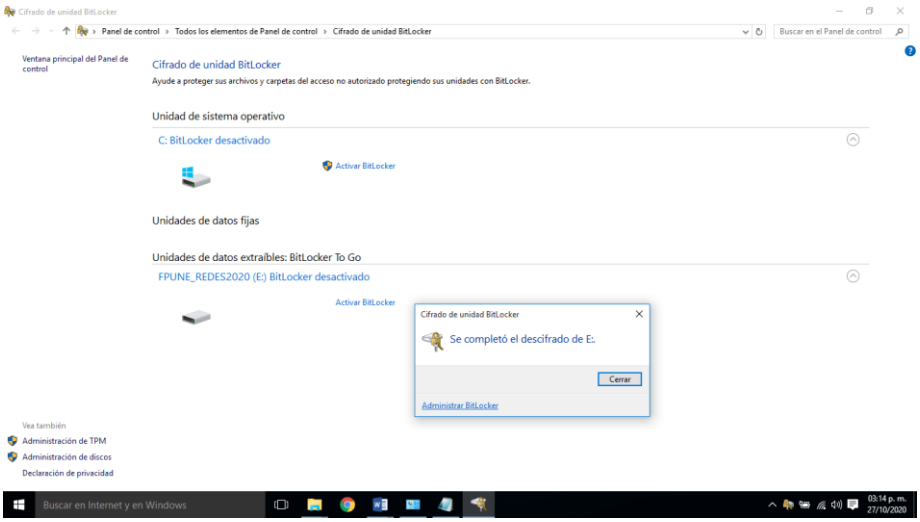


***Figura 1.11 Descifrado completo***

**Reflexiones**

Estos métodos de seguridad aplicable son de mucha importancia; tal vez una de las desventajas seria la disponibilidad en los sistemas operativas; estamos también informados que los sistemas operativos inferiores a Windows 10 ya no cuentan con soporte por este motivo surge la gran necesidad de actualizarnos a dichos sistemas operativos para poder utilizar al máximo los beneficios que nos ofrecen.

**PREGUNTAS**

1. ¿Por qué es importante guardar una clave de recuperación de BitLocker?
2. ¿En qué versiones de Windows está disponible la BitLocker?
3. La clave de recuperación ¿Cuántos bits contiene?
4. Investigue. Políticas de seguridad aplicable a dispositivos externos en Sistemas Operativos Linux.