Práctica Guiada: Confidencialidad de Datos en Windows mediante EFS

Introducción

La confidencialidad de los datos es uno de los pilares fundamentales de la seguridad informática. Garantiza que la información sensible solo pueda ser accesible por usuarios autorizados, protegiéndola frente a accesos no deseados o malintencionados.
En sistemas Windows, el **Encrypting File System (EFS)** permite cifrar archivos y carpetas en discos **NTFS**, asegurando que solo el usuario que cifra los datos pueda abrirlos o modificarlos.

Planteamiento de la práctica

El objetivo de esta práctica es que el alumno aprenda a:

- Configurar y activar EFS para proteger archivos y carpetas.
- Comprender cuándo y por qué es necesario cambiar la configuración de Windows para habilitar EFS.
- Evaluar los pros y contras del cifrado de archivos en Windows.
- Saber volver al estado anterior para desactivar el cifrado y evitar consumo de recursos innecesario.
- Desarrollar conciencia sobre la importancia de la confidencialidad y las buenas prácticas de seguridad en entornos personales y corporativos.

Definición combinada de NTFS y EFS

- **NTFS (New Technology File System):** sistema de archivos que organiza y protege datos en disco, permite permisos avanzados, registro de transacciones y compresión.
- **EFS (Encrypting File System):** función de cifrado que utiliza NTFS para proteger archivos y carpetas de manera individual, garantizando que solo el usuario autorizado pueda acceder a ellos.
- **En conjunto:** NTFS + EFS permite almacenar datos de forma **segura y confidencial** en Windows.

1. Cambiar configuración

Para usar EFS es necesario:

- Disco en **NTFS**.
- Edición de Windows **Pro, Enterprise o Education**. (cualquier otra edición requerirá cambiar la configuración Disco en NTFS)
- Servicio **EFS** activado y configurado en automático.

2. Por qué es necesario cambiarlo

- La opción de cifrado puede estar deshabilitada si: disco no es NTFS.

3. Pros y Contras

Pros

- Protege la **confidencialidad** de archivos y carpetas.
- Acceso exclusivo del usuario que cifra.
- Integrado en Windows, sin software adicional.
- Compatible con permisos NTFS.

Contras

- Solo disponible en Windows Pro/Enterprise/Education.
- Cifra archivos individuales, no todo el disco.
- Riesgo de pérdida de acceso si se pierden claves o certificados.
- Consumo de recursos al cifrar/descifrar.

4. Cifrar contenido (activar EFS)

Clic derecho sobre archivo/carpeta → **Propiedades**.
Opciones avanzadas → marcar **"Cifrar contenido para proteger datos"**.
Aplicar cambios → solo carpeta o toda la carpeta con subcarpetas/archivos.

5. Volver al estado anterior (desactivar cifrado)

Clic derecho sobre archivo/carpeta → **Propiedades** → **Opciones avanzadas**.
Desmarcar **"Cifrar contenido para proteger datos"**.
Aplicar cambios → solo carpeta o toda la carpeta con contenido.

6. Desactivar el servicio EFS (opcional)

Si no vas a usar más EFS y quieres volver al estado "de fábrica":

Presiona **Win + R**, escribe:

```
services.msc
```

Busca **Sistema de cifrado de archivos (EFS)**.
Haz clic derecho → **Detener**.
En **Tipo de inicio**, selecciona **Manual** o **Deshabilitado**.
Aplica y cierra.

EFS es una herramienta práctica para proteger la **confidencialidad de los datos** en Windows, pero requiere configuración manual y conocimiento de sus limitaciones. Activarlo o desactivarlo según necesidad permite un equilibrio entre **seguridad y rendimiento**, mientras se aplican buenas prácticas de protección de información sensible.

Preguntas de reflexión sobre EFS y certificados

Certificados y claves

A)¿Por qué no tuve que escribir una contraseña al cifrar el archivo?

B)¿Dónde está guardada la clave de cifrado que permite abrir mi archivo?

C)¿Qué ocurriría si pierdo el certificado asociado a mi usuario?

Finalidad del cifrado y Portabilidad del archivo cifrado

A) Si yo abro mi archivo cifrado en mi propia cuenta de Windows y lo veo sin problemas, ¿qué valor de seguridad me está aportando el EFS?

B)¿Qué pasaría si otra persona entra con su cuenta en el mismo ordenador e intenta abrir ese archivo?
Realiza la prueba.
Pon el archivo en disco compartido y prueba abrirlo. Exporta e importa el certificado. Vuelve a probar

C)¿Qué pasaría si me lo llevo a un disco externo?

D)Si envío el archivo cifrado por correo electrónico a otra persona, ¿podrá abrirlo sin mi certificado?

E)¿Qué pasa si intento abrir el fichero desde un programa para leerlo?

Copia este codigo en Python y ejecuta. ¿Qué ves?. Justifica tu respuesta

```
archivo = r"C:\Users\SAD_2\Desktop\Confidencial.txt.txt"
f = open(archivo, "br")
contenido = f.read()
print("Contenido: ")
print(contenido)
```

Instalación de Python:Ve a la web oficial: https://www.python.org/downloads/

Descarga la versión **estable más reciente** (por ejemplo, Python 3.13).

Durante la instalación, **marca la casilla "Add Python to PATH"** antes de hacer clic en "Install Now". Esto permite ejecutar Python desde la terminal.

Abre el **Símbolo del sistema (CMD)** y escribe:

```
python --version
```

Deberías ver algo como:

```
Python 3.13.7
```

Guarda tu archivo Python, por ejemplo abrir_efs.py.

Abre CMD y navega hasta la carpeta donde está el script:

```
cd C:\ruta\donde\esta\el\script
```

Ejecuta el script:

```
python abrir_efs.py
```

Comparación con otros métodos

¿En qué se diferencia EFS de comprimir un archivo con contraseña (por ejemplo, en un ZIP protegido)?

¿En qué se parece EFS a una firma digital en cuanto al uso de certificados?