Actividad. Cifrado en Windows y Linux.

Las herramientas de cifrado permiten garantizar la **confidencialidad**, **autenticidad** e **integridad** de los datos, mediante la conversión de los datos originales a un formato codificado. De esta manera, si otras herramientas de seguridad son superadas por amenazas, el cifrado refuerza esta seguridad.

Cifrado en Windows

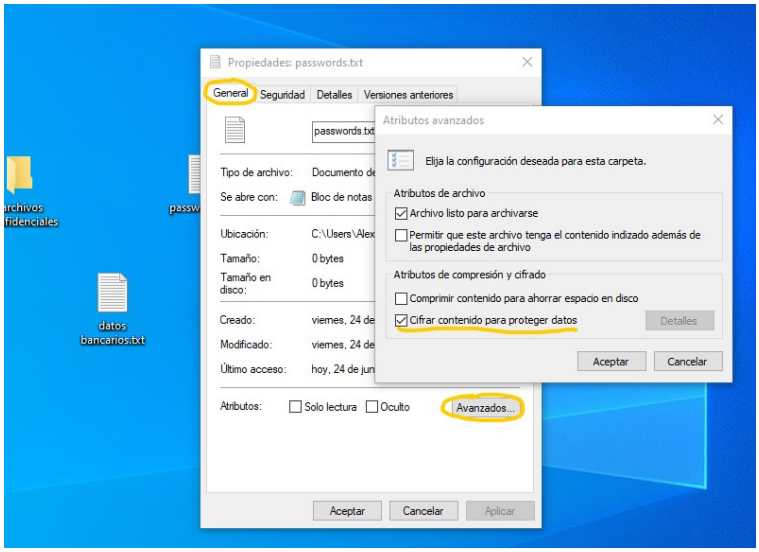
Windows ofrece cifrado EFS (Encrypting File System) sobre el sistema de archivos NTFS en versiones avanzadas. EFS no es compatible con la compresión, no obstante, garantiza que los archivos se cifren de manera individual , vinculándose al usuario que los cifró, estando disponible la información para éste pero no para el resto.

¿Cómo ciframos un archivo o carpeta?

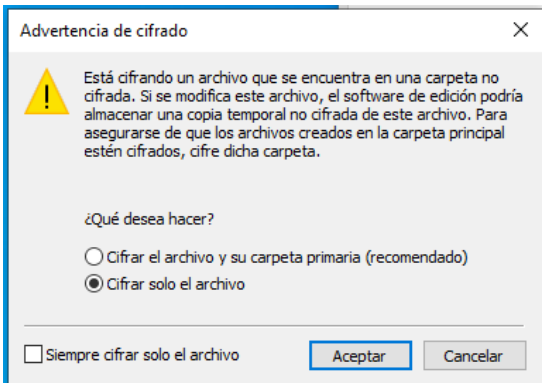
Accedemos a Propiedades → Avanzados(General) → Cifrar Contenido para proteger datos.

En caso de cifrar archivos y no su carpeta contenedora, Windows recomienda cifrar esta última mediante una advertencia. Y, una vez efectuado el cifrado, mediante el botón **"Detalles"** de la misma ventana anterior, permite añadir otros usuarios que puedan tener acceso.

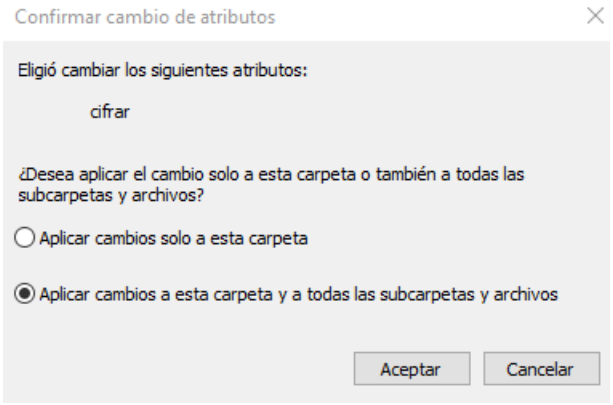
Además también avisará con la recomendación de crear una copia de seguridad de la clave de cifrado EFS.

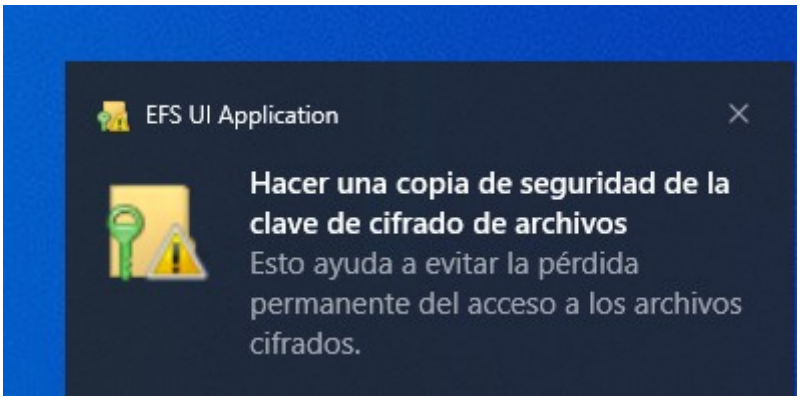


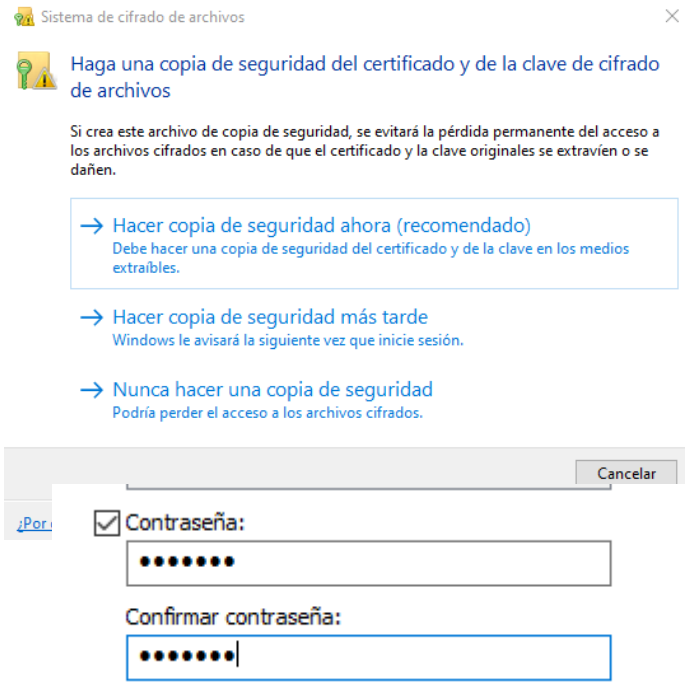
Si ciframos un archivo directamente:

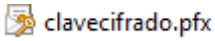


Si ciframos un directorio entero:



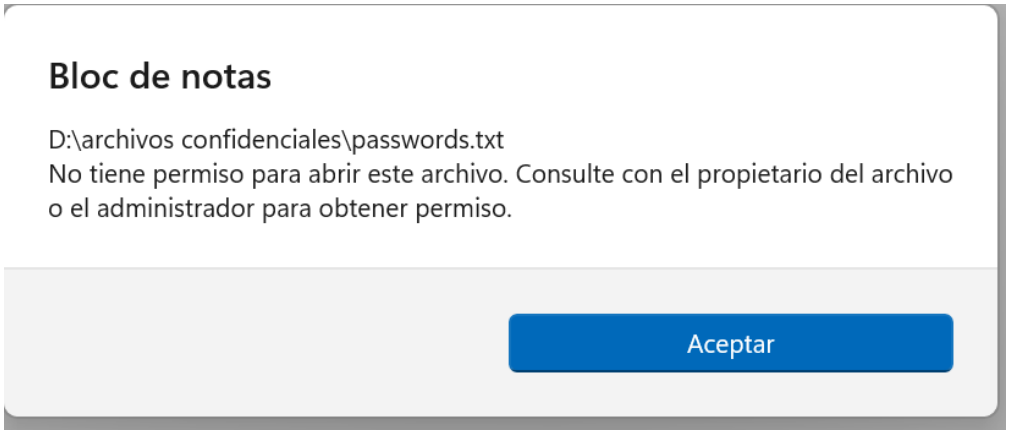






Ya tendría mi carpeta cifrada y guardada mi clave.

Este método nos funcionaría sobre unidades externas. Si copiamos el archivo en un usb por ejemplo, lo llevamos a otro equipo y lo intentamos abrir nos encontraremos con el siguiente mensaje:

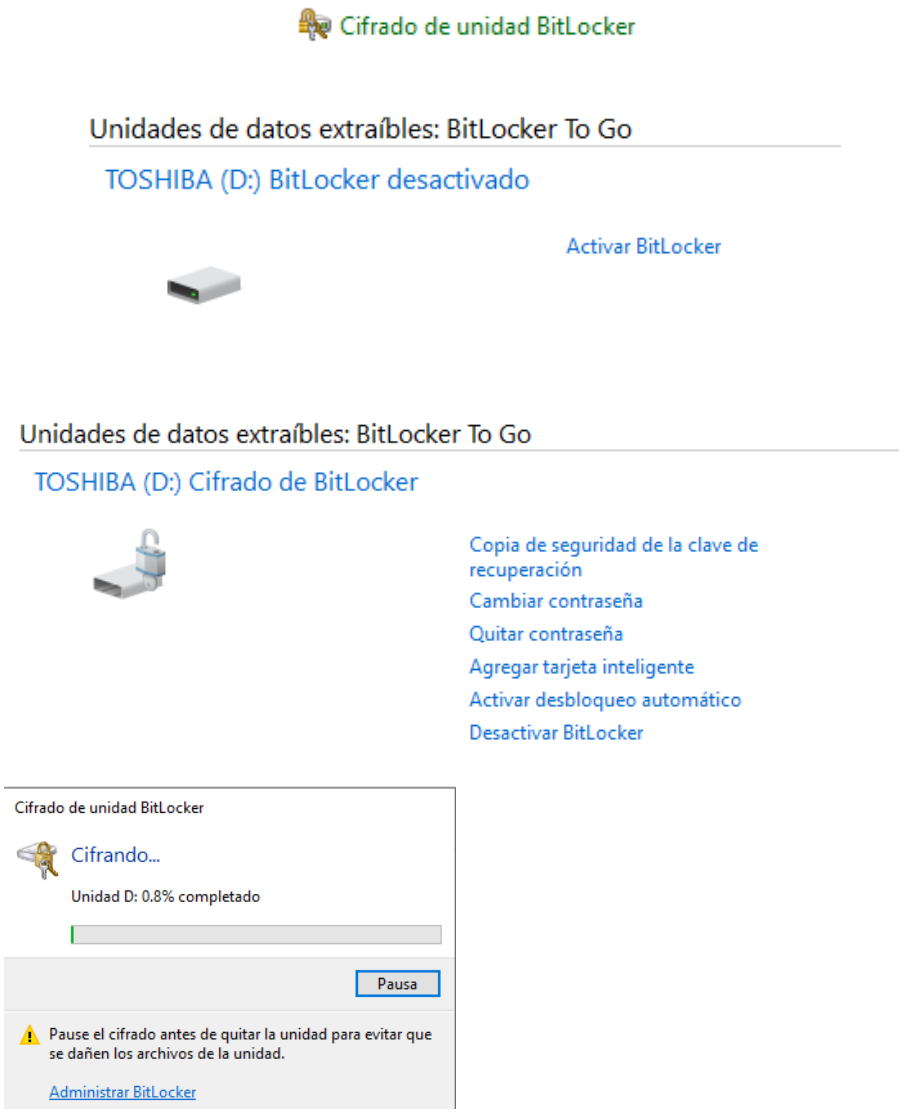


Nota: En sistemas de archivos NTFS, al mover archivos o carpetas a una carpeta cifrada, producirá que se cifre lo movido; sin embargo, esto no sucede al contrario.
Los archivos o carpetas cifrados se descifrarán si los movemos a un volumen que no sea NTFS.

Por lo tanto tampoco es un cifrado muy adecuado.

Otra manera de cifrado y solucionar los inconvenientes del cifrado EFS en Windows es a través de la herramienta BitLocker, que se encarga de asegurar la privacidad y la integridad en volúmenes enteros cifrando su contenido. Es más potente que EFS, ya que es independiente de los usuarios y puede emplear la tecnología de protección de datos TPM (Trusted Platform Module) para encriptar la información, así como una clave o tarjeta inteligente con PIN para su acceso. Se puede emplear solo en las versiones avanzadas de Windows.

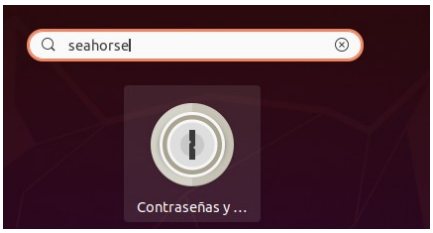
Para cifrar volúmenes con BitLocker lo haremos desde el panel de control accedemos a "Cifrado de Unidad BitLocker" y Activamos para un Volumen dado.

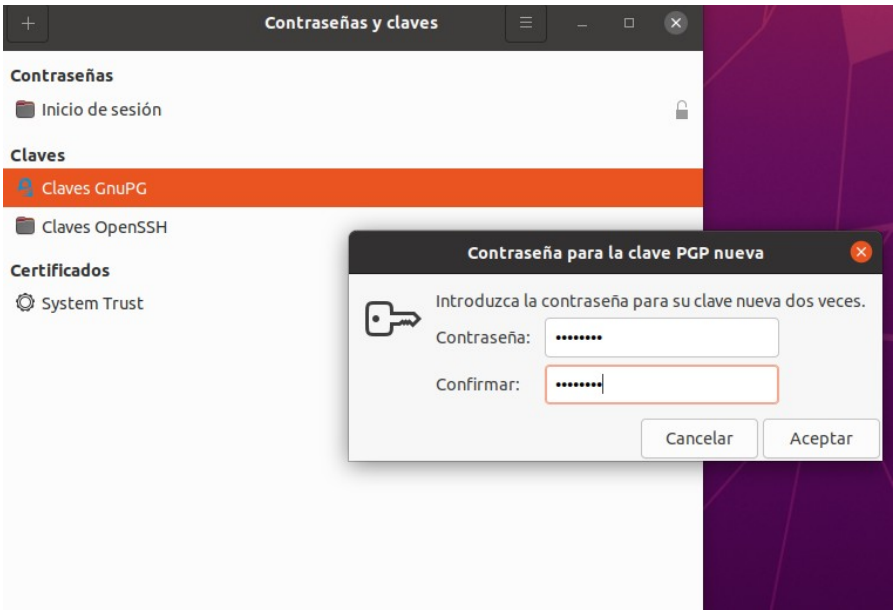


Cifrado Linux

Existen muchas herramientas de cifrado en sistemas operativos GNU/Linux. Una de ellas es GNU Privacy Guard (GPG). Emplea encriptación simétrica y asimétrica.
Ubuntu integra la aplicación Seahorse, que administra claves y contraseñas de cifrado, pudiendo gestionar claves GPG.

Para emplear esta utilidad cifrando carpetas o archivos, primero debemos crear las claves GPG desde **'+',** 'Nuevo' y 'Clave PGP'.





Para utilizar las herramientas integradas con el explorador de archivos Nautilus lanzamos las siguientes instrucciones desde el terminal:

```
alex@alex-VirtualBox:~$ sudo apt update
[sudo] contraseña para alex:
Obj:1 http://es.archive.ubuntu.com/ubuntu focal InRelease
Des:2 http://es.archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
Des:3 http://security.ubuntu.com/ubuntu focal-security InRelease [114 kB]
Des:4 http://es.archive.ubuntu.com/ubuntu focal-backports InRelease [108 kB]
Descargados 336 kB en 1s (407 kB/s)
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se pueden actualizar 46 paquetes. Ejecute «apt list --upgradable» para verlos.
alex@alex-VirtualBox:~$ sudo apt install seahorse-nautilus
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
El paquete indicado a continuación se instaló de forma automática y ya no es nec
esario.
  libfwupdplugin1
Utilice «sudo apt autoremove» para eliminarlo.
Se instalarán los siguientes paquetes adicionales:
```

De esta manera, ya podemos emplear la opción “Cifrar” desde el menú contextual al pulsar el botón secundario del ratón sobre los archivos o carpetas. Al cifrarse, se genera un archivo con extensión .gpg, por lo que, por seguridad, se debe eliminar el anterior archivo sin cifrar.