Sistema de Archivos Encriptados

Transcribed on July 10, 2025 at 9:39 AM by Minutes AI

Speaker 1 (00:06)

Bienvenidos a esta nueva sesión.

En esta sesión vamos a hablar sobre el sistema de cifrado de archivos, también conocido como EF S.

Hoy vamos a explorar cómo EF S puede ayudarnos a proteger nuestros archivos sensibles en entornos Windows.

El sistema de fijado de archivos de Windows es una característica integrada en este sistema operativo que nos va a permitir cifrar archivos y carpetas para proteger su contenido contra accesos no autorizados.

En primer lugar, vamos a entender qué es exactamente y cómo funciona EFS.

Efs cifra archivos a nivel de archivo utilizando una clave de cifrado única asociada a cada archivo o carpeta.

Esta clave de cifrado se almacena en el sistema operativo y se protege mediante la infraestructura de ClE pública de Windows, o lo que es lo mismo, la PKI de Windows.

Si has trabajado alguna vez con algún apartado de cifrado Windows, quizás has visto o has configurado BitLocker.

¿Entonces, cuál es la diferencia entre EFs y BitLocker?

Una de las principales diferencias entre EFs y bitlocker radica en el nivel de cifrado que estos ofrecen.

Mientras que EFS cifra archivos a nivel de archivo, lo que permite cifrar archivos individuales, bitlocker lo que hace es cifrar todo el contenido, o mejor dicho, todo el disco o la unidad de almacenamiento completo.

Esto significa que, si bien EFS es más granular en términos de qué archivos se cifran, BitLocker proporciona una protección más integral a nivel de unidad.

Ahora pasemos a discutir algunas de las características clave de EFS.

Una de las ventajas principales es es que el cifrado se integra con los permisos de archivos ntfs, lo que significa que los archivos cifrados pueden compartirse de manera segura mientras se mantienen protegidos.

Además, Efs ofrece una funcionalidad transparente para los usuarios finales, lo que significa que el cifrado y el descifrado ocurren de manera automática y sin necesidad de tener que hacer una acción adicional por parte del usuario.

¿Y ahora, cómo implementamos y utilizamos Efs en la práctica?

Es importante seguir algunos pasos clave para activar y configurar EFs en un sistema Windows y ahora lo vamos a ver.

Una vez configurado, podemos cifrar y descifrar archivos de manera sencilla utilizando las opciones disponibles en el sistema operativo.

Si bien EFS ofrece muchas ventajas en términos de protección de archivos sensibles, también hay desafíos potenciales a considerar.

La correcta gestión de las claves de cifrado es fundamental para garantizar la seguridad de los archivos cifrados, y la pérdida de estas claves puede resultar en la pérdida permanente de acceso a los datos.

A continuación, vamos a verlo en directo.

Me encuentro en un sistema operativo Windows 11 y vamos a ver cómo aplicar el sistema de cifrado de archivos conocido como EFS en este sistema.

Esta explicación que vamos a ver podría aplicarse a otros sistemas más antiguos como es el caso por ejemplo de Windows 10.

En primer lugar lo que vamos a hacer va a ser crear una nueva carpeta.

Aquí vamos a crear por ejemplo una carpeta denominada test, vamos a definirla aquí y lo que queremos hacer es cifrar a nivel de carpeta o a nivel de archivo, así que también voy a escribir aquí un nuevo, vamos a crear un wordpack, por ejemplo, vamos a escribir un hello y vamos a guardarlo dentro de esta carpetita que acabamos de crear.

Lo siguiente que vamos a hacer es cifrar la carpeta, por supuesto que también podríamos coger y cifrar únicamente este documento, pero los pasos son los mismos, pero lo que vamos a hacer es venirnos aquí, darle al botón derecho y a la parte de propiedades.

En la parte de propiedades nos iremos a las opciones avanzadas de esta carpeta y encontramos ya directamente esta opción, apartado de la compresión y el cifrado, atributos de cifrado y lo que queremos hacer es darle a cifrar el contenido para proteger los datos.

De momento no nos deja acceder a los detalles, vamos a confirmar y vamos a darle a aplicar en este momento.

Ahora nos solicita este tipo de cifrado, a qué lo queremos aplicar, si lo queremos aplicar únicamente a este directorio o si por el contrario lo queremos aplicar al directorio, a los subdirectorios que se encuentren aquí y a los distintos archivos.

También se destaca de que si ciframos este directorio y todos los archivos, cuando metamos un archivo nuevo también se va a cifrar automáticamente.

Así que en principio vamos a cifrar todo lo que se vaya introduciendo aquí, no solamente el directorio sino también todos los subdirectorios y los archivos en sí.

Ahora lo siguiente que nos aparece es esta notificación, en principio ya el cifrado está hecho, de hecho podéis ver como nos aparece un candadito en este caso aquí en la carpeta, pero vamos a abrir esta notificación y vamos a ver qué es lo que nos indica.

Vemos que en este diálogo se nos dan tres opciones, en este caso tendríamos hacer el backup, que obviamente es la opción recomendada y es lo que vamos a hacer, también nos lo podrían recordar un poco más tarde, es decir, la siguiente vez que se haga el login que nos vuelva a aparecer este aviso o bien no hacer el backup y por tanto si perdemos la clave vamos a perder el acceso a todo.

Nos dirige a un enlace donde podemos leer más en este enlace sobre por qué deberíamos hacer un Backup del Certificado y de la clave, nosotros vamos a ir directamente a hacer el certificado, hacer el backup, nos aparece este asistente y le vamos a dar a siguiente.

Ahora ya nos sale también esto por defecto y el formato que vamos a utilizar es el PKCS que sería Personal Information Exchange y con las opciones que ya tenemos por defecto le vamos a dar a siguiente, vamos a definir una contraseña, como podéis ver aquí se nos pide una contraseña así que asignamos una contraseña seguro y por último la última opción que tenemos es el tipo de cifrado que queremos aplicar o bien triple des con sha o bien AES con sha, dependiendo de las necesidades de cada uno pues eligiera un tipo de cifrado u otro.

Si hablamos de seguridad pues un cifrado más robusto y más avanzado que triple des por supuesto que es AES.

Así que esta es la opción que vamos a elegir, le daremos a siguiente y buscaremos en qué sitio queremos dejar este documento, en este caso en el escritorio lo vamos a guardar como key, le vamos a dar a guardar y le vamos a dar a siguiente.

Por último nos muestra este apartado con las distintas, con el resumen por así decirlo, así que le vamos a dar a finalizar y vemos como aquí tenemos este certificado.

Si posteriormente quisiéramos importar este certificado vamos a hacerle doble clic y nos está apareciendo este nuevo asistente para importar el certificado que nos dice que donde lo queremos almacenar, si en el current user o en la máquina local, aquí ya dependiendo también de cada uno lo configurará y ahora la importación de este celular cuando lo haya perdido y quiera recuperar el contenido del mismo.

Antes de terminar sí que quiero mostrar un par de cosas más y en primer lugar es que si aquí ahora nos vamos a la sección de propiedades y avanzado ya nos aparece disponible el botón de detalles y simplemente dándole aquí nos dice quién o qué usuarios tienen acceso a estos archivos y también información sobre el certificado que tenemos aquí.

Por último si quisiéramos poner este certificado porque se nos ha olvidado hacer el backup y queremos más tarde recuperar cómo hacer ese backup nos vamos a venir aquí y buscaremos sobre cifrado, en este caso sobre el encrypt y aquí vemos una sección que es device encrypt, así que si, perdonad, este es el bitlocker, aquí no lo tenemos, es este es el manage file Encryption certificate, si le damos aquí nos va a salir los certificados que tenemos con EFs como podemos ver y va a ser otra opción donde nosotros podamos hacer este backup.

Si le damos aquí a siguiente, veis aquí podemos ver información del Certificado, cuando lo hemos creado y hasta cuando va a ser válido, veis que nos está poniendo por bastante, bastante tiempo.

Y si le damos en este caso a siguiente, vemos cómo podríamos hacer esta contraseña, cómo podríamos hacer este backup asignando una contraseña.

Recuerdo de nuevo que esta contraseña se nos pedirá cuando queramos importar el certificado, como hemos visto ahora cuando le hemos dado aquí hacer la importación del kit que nos ha salido ese asistente.

Como veis, trabajar con EFs de manera práctica es sencillo y es una manera bastante rápida de poder aplicar un cifrado a nivel de carpeta o de archivo.

Llegamos ya al final de la sesión y a continuación vamos a definir las conclusiones principales que hemos ido viendo.

Por un lado, hemos aprendido que Efs es una característica integrada en los sistemas operativos Windows que nos permite cifrar archivos y carpetas de manera selectiva para proteger su contenido contra accesos no autorizados.

Efs cifra los archivos a nivel de archivo y se integra perfectamente con los permisos de archivos NTFS.

Esto significa que podemos compartir archivos cifrados de manera segura mientras se mantienen protegidos contra accesos no autorizados.

También hemos visto los pasos necesarios para implementar y activar EFS en un sistema Windows, así como la funcionalidad transparente que ofrece para los usuarios finales, donde el cifrado y el descifrado ocurren automáticamente sin requerir de una acción adicional.

Hemos contrastado las diferencias entre Efs y broker, destacando que Ecs cifra los archivos de manera individual, mientras que Bitlocker se encarga de cifrar las unidades completas.

Además, hemos destacado que la integración de EFs está integrada con los permisos de archivos NTFs.

Por último, se recomienda utilizar Efs como parte de una estrategia integral de seguridad en entornos Windows, precisamente para proteger archivos sensibles de una manera selectiva y para mantener la integridad dentro de su sistema de archivos.

En resumen, EFs es una herramienta poderosa para proteger archivos sensibles en entorno Windows, ofreciendo una protección granular y transparente para los usuarios finales.

Espero que esta sesión te haya proporcionado información valiosa sobre cómo implementar y utilizar ecs en estos entornos.

Y con esto llegamos al final de la sesión.

Os esperamos en el siguiente.