Cifrado en Windows

Transcribed on August 4, 2025 at 3:27 PM by Minutes AI

Speaker 1 (00:03)

Bienvenidos a esta nueva sesión.

En esta sesión vamos a tratar del tema del cifrado en Windows.

Vamos a hablar de los servicios que tenemos para el cifrado en Windows de forma nativa y entre ellos hablaremos del sistema de cifrado de archivos FS y de BitLocker.

También vamos a hablar sobre cómo BitLocker nos puede ayudar a proteger el sistema de arranque en el dispositivo.

Tiene en sus propios componentes del sistema operativo servicios para el cifrado de datos.

Entre ellos tiene el sistema de cifrado de archivos conocido como EF S, que está basado en el sistema de archivos del disco duro, en el sistema de archivos NTFS.

Va a permitir que los usuarios, sin ninguna configuración previa, sin instalar nada, puedan cifrar carpetas y archivos y de esta manera asegurarse de un acceso no autorizado a esos elementos.

Bizlocker está orientado a cifrar volúmenes, puede servirnos para cifrar un volumen entero.

Podemos cifrar también el volumen de sistema y tenemos un componente en algunas versiones de Windows que se llama bitlockergo que nos sirve para cifrar dispositivos extraíbles tipo Es una característica del sistema.

En los equipos cliente de Windows ya viene instalada y en Windows Server es una característica que hay que instalar.

Requiere un chip TPM, es decir, necesita utilizar un chip criptográfico en el que pueda almacenar claves y secretos y de esta manera nosotros podemos guardar, por ejemplo, las claves de bitlocker en ese chip criptográfico y de esta manera podemos habilitar la funcionalidad de cifrar la parte de sistema.

Cuando nosotros ciframos el volumen de sistema hay un momento donde en la parte de arranque se necesita descifrar una serie de archivos para poder arrancar el propio sistema operativo.

Entonces necesitamos ese chip criptográfico para almacenar esas clases y que de esta manera bitlocker pueda funcionar y pueda cifrar el volumen de sistema.

El sistema de cifrado de archivos es el más conocido.

Nos permite de una forma sencilla proporcionar a los usuarios la posibilidad de cifrar tanto archivos como carpetas.

Si nosotros ciframos una carpeta, automáticamente se van a cifrar todos los archivos que tenemos dentro de esa carpeta, pero también tenemos la posibilidad de cifrar un determinado archivo.

Cuando se hace esta operación lo que se utiliza es el sistema de certificados del propio usuario con un sistema de clave privada y clave pública y se utiliza una clave simétrica y esa clave simétrica después se cifra mediante la clave pública del certificado digital del usuario y de esta manera queda protegido.

Esas claves van a estar almacenadas en la cabecera del archivo y el cifrado por defecto de EFS utiliza el algoritmo AES, de tal forma que es un cifrado bastante seguro.

Igual que tenemos EFS para el cifrado de archivos y el cifrado de carpetas.

Cuando nosotros ciframos los archivos o las carpetas, eso va a depender de que el usuario tenga iniciada sesión, es decir, cuando el usuario tiene iniciada sesión va a poder acceder a todo ese contenido sin hacer nada previamente.

Pero si un atacante o una persona que no tiene acceso a ese dispositivo, no tiene acceso autorizado ese dispositivo, coge ese dispositivo con una sesión abierta, pues va a poder acceder también a todo ese contenido.

Tenemos otro elemento que es BitLocker.

BitLocker lo que hace es que va a cifrar el volumen completo.

Bitlocker cifra el volumen completo y se va a necesitar conocer la clave para poder descifrar ese volumen.

Es decir, que aunque nosotros nos hiciéramos con la identidad del usuario o con el token del usuario, pudiéramos extraer las credenciales de ese usuario e iniciar sesión en ese dispositivo, si no conocemos la clave con la que se ha cifrado ese dispositivo, pues no vamos a poder acceder a ese disco.

Bizlocker puede ser configurado para proteger el sistema operativo, el sistema de arranque, en un escenario en el que tengamos un chip CL, un chip FM en el dispositivo, que en los dispositivos modernos es bastante habitual.

También podemos añadir segundos factores de autenticación, de tal forma que además de la clave se pida una llave o se pida un pin al usuario.

Podemos hacer que también se necesite instalar una llave USB para poder arrancar un determinado dispositivo.

Cuando BitLocker cifra el volumen de sistema, además de cifrar el volumen de sistema, va a proteger todos los archivos de arranque, entonces va a chequear y comprobar que no haya habido modificaciones en todos los archivos que tenéis en la diapositiva, en la parte de la BIOS, también en la ROM, en la Master Boot Record, en el sector de arranque de NTFS, en Windows Boot Manager y en Corel Root.

Estamos en la máquina virtual, tenemos aquí la carpeta confidencial, si damos botón derecho y nos vamos a la parte de propiedades de la carpeta confidencial, dentro de las opciones generales, en la parte de avanzado, tenemos aquí para cifrar el contenido de esta carpeta, damos a OK, damos aplicar, nos indica si queremos que se apliquen los cambios solo a esta carpeta o que se apliquen también a los archivos o carpetas que estuvieran dentro de esta misma carpeta.

Damos a OK y se va a cifrar el contenido de la carpeta.

Si nosotros ahora vamos a la carpeta dentro de este contenedor, nos vamos a encontrar con que tenemos señalizado en el icono de todos los documentos que estos documentos estarían cifrados.

Si nosotros abrimos cualquier documento, podemos abrir perfectamente cualquier tipo de documento, podemos escribir o modificar el documento y podemos cerrarlo porque nosotros estamos en este caso utilizando el usuario que se ha utilizado para cifrar esta carpeta.

Es decir, hay que entender muy bien qué medidas de seguridad nos aporta el sistema de cifrado de archivos.

Si otro usuario accede a los archivos de este usuario, no va a poder ver los documentos que estén cifrados.

Si alguien monta el disco y trata de acceder a las carpetas que están cifradas mediante EFS, no va a poder ver esos archivos, esos documentos.

Sin embargo, si alguien vulnera la seguridad del usuario y es capaz de iniciar sesión con este usuario, va a poder perfectamente ver todos los archivos y toda la documentación que está cifrado mediante EFS.

Entonces, nosotros siempre que ciframos algo mediante EFS, lo que estamos es protegiéndonos, siempre y cuando no se utilice la identidad de ese usuario, porque el usuario va a poder ver los archivos perfectamente.

Si nosotros volvemos a la parte de propiedades, nos vamos a la parte de avanzado y aquí tendríamos la parte de detalles relacionada con el uso del sistema de cifrado de archivos.

Si nosotros quitamos el check, damos a OK, damos aplicar, nos va a parecer lo mismo si queremos descifrar la carpeta o todo el contenido que hay en su interior.

Damos a OK.

Entonces, si ahora nosotros abrimos la carpeta, vamos a ver que esa carpeta no está cifrada y el contenido de esa carpeta no está cifrado.

Si nos vamos al explorador, nos vamos a la parte del equipo donde tenemos los diferentes volúmenes y nosotros podemos seleccionar un volumen, damos botón derecho y una de las opciones que nos aparece es la de iniciar bitlocker.

Si nosotros estuviéramos en Windows Server, tendríamos que previamente instalar la característica de bitlocker.

No viene en Windows Server habilitada por defecto seleccionamos Habilitar bitlocker y nos va a aparecer un asistente que nos va a guiar durante el periodo de activación de la característica.

Podemos utilizar una Smart Card para desbloquear el dispositivo o podemos utilizar una password que nosotros vamos a generar.

Damos a siguiente y nos va a decir dónde queremos que se almacene esa contraseña.

Esa contraseña es la que va a ser la clave de recuperación, es la que nos va a permitir descifrar el dispositivo en el caso de que nos olvidáramos la contraseña.

Entonces debemos tener en cuenta que esa clave tiene que estar almacenada en un sitio que nos acordemos que la tenemos ahí almacenada, porque si nos olvidamos de la contraseña o tenemos un inconveniente con la contraseña y luego no sabemos encontrar esta clave, vamos a tener un problema porque vamos a perder los datos.

Pero además tenemos que almacenarla en un sitio seguro porque si alguien es capaz de acceder a esa clave va a poder descifrar lo que tengamos cifrado con bit.

Podemos grabarla en una cuenta de Microsoft cuando estamos utilizando sistemas online, una cuenta por ejemplo de Microsoft 365, podemos utilizar el almacén de credenciales de esa cuenta de Microsoft para guardarlo.

Podemos guardarlo en un USB de tal forma que lo guardamos en un dispositivo extraíble y luego ponemos a buen recaudo ese dispositivo extraíble o podemos grabarla en un archivo que cuando la grabamos en un archivo también la podemos poner en un elemento que sea extraíble.

Vamos a decir que la queremos guardar en un archivo y podríamos guardarla por ejemplo en un archivo OneDrive, de tal forma que lo tendríamos en la nube almacenado de forma segura y podríamos extraerlo de la nube o podríamos guardarlo en una ubicación.

Lo que no sería normal sería que nosotros lo guardáramos dentro del propio dispositivo como voy a hacer yo ahora.

Esto no sería correcto, pero para el ejercicio lo podemos hacer.

Una vez que seleccionamos dónde vamos a almacenar la clave para poder recuperar el sistema de cifrado, lo siguiente que nos pregunta es si queremos cifrar todo el volumen o solo la parte que estemos utilizando.

Cuando yo cifro todo el volumen, después cuando estoy utilizando ese volumen que ya está cifrado, pues va a ser mucho más ágil, pero va a tardar un poquito en cifrar todo el volumen, especialmente cuando es un volumen grande, cuando yo cifro el espacio de datos que está siendo utilizado, va a cifrarlo de una manera más eficiente, de una manera más rápida, aunque después cuando voy añadiendo datos, a la hora de almacenar esos datos, tiene que almacenar y cifrar esos datos.

Damos a siguiente y damos habilitar el sistema de cifrado.

Como veis, automáticamente nos aparece un candadito en el volumen y si yo ahora selecciono el volumen, ahora en vez de tener la opción de encender bitlocker, voy a tener la opción de administrar.

Entonces, cuando yo voy a la parte de administrar BitLocker, lo que me voy a encontrar es una pantalla de administración donde yo voy a tener una serie de opciones disponibles.

Entre ellas puedo hacer un backup de la clave de recuperación, puedo cambiar la password que voy a utilizar para la parte del cifrado, puedo puedo eliminar esa password, puedo añadir una smart car, puedo encender el autolog y puedo deshabilitar BitLocker.

Además puedo ver información sobre la administración del chip TPM, este chip criptográfico del que os estoy hablando constantemente.

Pues desde el propio administrador de BitLocker nos va a aparecer la posibilidad de ver el chip criptográfico que en este caso tendríamos en una máquina virtual.

Y después tendríamos también desde aquí las opciones de administrar discos, es decir, que vamos a abrir el administrador de discos desde el propio bitlocker.

Hemos visto el administrador de discos desde el administrador del dispositivo cuando aprendimos a formatear los diferentes discos y los diferentes volúmenes, montar sistemas reflejados o montar sistemas de RAID, etc.

Pues este mismo administrador de discos lo tendríamos disponible desde la consola de administración de BitLocker.

Si yo quiero habilitar BitLocker en otra unidad, en otro volumen, por ejemplo en el volumen de sistema, aquí me informa que en C, en el volumen del sistema, BitLocker estaría apagado y yo tendría la posibilidad de encender BitLocker en el volumen de sistema.

Si quiero deshabilitar BitLocker, simplemente doy aquí, selecciono apagar BitLocker y veis que ahora este volumen dejaría de estar cifrado con bitlock.

Bueno, como conclusión, hemos visto que Microsoft tiene una serie de servicios de cifrado integrados dentro del sistema operativo que nos permiten proteger la privacidad de los datos, incluso aunque el dispositivo sea robado.

Como proposición de ejercicio debéis crear una carpeta que se llame Confidencial y cifrar esa carpeta con el sistema de cifrado de archivos EFS, luego adicional en la máquina virtual, aparte del disco de sistema para configurarlo como un volumen para datos y lo cifráis con bitlock.

Llegamos al final de la sesión, os esperamos en el siguiente vídeo.

Bienvenidos a esta nueva sesión.

En esta sesión vamos a resolver el ejercicio planteado en el vídeo anterior.

Pedíamos crear una carpeta llamada Confidencial, cifrar esa carpeta con el sistema de cifrado de archivos EFS, crear un disco adicional en la máquina virtual para un volumen de datos, darle formato y después cifrar ese volumen con bitlocker.

Estamos en la máquina virtual, si nos vamos al botón de inicio vemos que estamos con el usuario Ángel, nos vamos al explorador de archivos y en el explorador de archivos vamos a ir a un espacio común que pueda ser compartido con diferentes usuarios, es decir, nos vamos a ir en este caso a C, porque si nosotros generamos contenido dentro del escritorio, dentro de documentos o dentro de algún elemento del propio usuario, los otros usuarios no van a tener permiso para acceder.

Entonces cuando yo quiero crear contenido en un dispositivo para que puedan acceder todos los usuarios, tengo que hacerlo en un espacio en común, en este caso por ejemplo un volumen de datos o la unidad C.

Voy a crear una nueva carpeta que le voy a llamar Confidencial, voy a entrar dentro de la carpeta y crear un par de documentos de ejemplo, voy a crear por ejemplo un documento de texto y voy a crear una imagen.

Voy a copiar estos dos elementos y ahora voy a crear otra carpeta que se va a llamar Confidencial pero que no está cifrada como IFS.

Vamos a seleccionar esta carpeta y vamos a copiar los documentos.

Copiamos los documentos.

Ya tenemos una carpeta que es Confidencial y otra carpeta que va a ser Confidencial sin el cifrado DFS.

En este caso vamos a la parte de propiedades, vamos a la parte de avanzado, vamos a la parte de Cifrar, damos a OK, damos Aplicar, damos a OK y vamos a verificar en la carpeta confidencial que los elementos nos aparecen con el candadito, es decir, que están cifrados.

Lo siguiente que vamos a hacer es que vamos a ir al administrador de discos y dentro del administrador de discos.

Vamos aquí, vamos a dejar este disco como disco básico, vamos a convertir este disco a disco dinámico, el disco 2 lo convertimos a disco dinámico y vamos a dar formato a estos dos discos.

Vamos a crear un nuevo volumen simple que se va a llamar e, que es el disco básico y vamos a crear otro nuevo volumen simple que le vamos a dar también el sistema de archivos, se va a llamar f, le vamos a dar el sistema de archivos ntfs y ahora nos vamos a ir al explorador y nos van a aparecer aquí el volumen básico, e para datos y el volumen f, que es dinámico.

Si damos botón derecho sobre el volumen f, nos vamos a encontrar con que aquí no nos aparece la posibilidad de encender bitlocker, esto es porque hemos convertido el disco a dinámico, es decir, que cuando nosotros utilizamos discos dinámicos tenemos que tener en cuenta que esos discos dinámicos no los podemos proteger con vi si yo me voy al disco que hemos configurado como disco básico, sí que me aparecería para encender bitlocker, Entonces voy a encender en este volumen, en el volumen e, este disco de datos, voy a habilitar bitlocker, le voy a poner la contraseña, repetimos la contraseña, vamos siguiendo los pasos del asistente.

Recordar que nosotros lo que vamos a hacer es guardar la clave de recuperación, en este caso la clave de recuperación pues la voy a guardar mismamente en el escritorio, Voy al escritorio, guardar aquí la clave, doy a siguiente, doy a cifrar el disco y comenzamos el cifrado del disco del volumen con Bizlock.

¿Ves que ya tenemos el disco cifrado?

Bueno, entonces ahora lo siguiente que vamos a hacer, vamos a cerrar todos estos elementos y voy a cerrar sesión con este usuario y vamos a iniciar sesión con otro usuario.

En este caso vamos a iniciar sesión con otro usuario del mismo dispositivo y vamos a verificar que no puede acceder a aquellos datos que son confidenciales, están cifrados y que no va a poder acceder a un volumen que está cifrado con bitlock.

Si nos vamos al otro usuario, iniciamos sesión con otro usuario.

Una vez que iniciamos sesión, si nosotros vamos al botón de inicio, vemos que estamos con otro y si nos vamos al explorador lo que vemos es que tenemos aquí un volumen que está cifrado con bitlocker.

Al tratar de acceder al volumen me va a pedir la contraseña y Aquí tendríamos también, si no nos acordáramos de la contraseña, la posibilidad de introducir la clave de recuperación.

Si yo pongo la contraseña y pongo una contraseña que no es correcta a la hora de desbloquear, aunque yo tengo un usuario válido del sistema, necesito conocer la contraseña para poder acceder al volumen.

Si yo meto una contraseña correcta a la hora de desbloquear el dispositivo, me va a permitir desbloquear el dispositivo y una vez que está desbloqueado el dispositivo ya podría acceder al volumen.

Entonces puedo entrar dentro del volumen y puedo ver los datos que estarían en ese volumen.

Si alguien roba el dispositivo, incluso si extrae el disco duro y trata de montar el disco duro con otro sistema operativo, con herramientas de análisis forense para poder extraer los datos de ese disco duro, ese volumen va a estar cifrado y va a ser muy complicado poder acceder a esos datos.

Si yo me voy al volumen C, dentro del volumen C vemos que tenemos la carpeta confidencial y la carpeta confidencial que no está cifrada mediante EFS.

Yo con este usuario como C sub espacio común, puedo acceder y puedo ver los documentos que tenemos almacenados en esta carpeta y podría modificar esos documentos o podría trabajar con esos documentos sin ningún problema.

Sin embargo, cuando yo tengo una carpeta que está cifrada con EFS, accedo a esa carpeta y entonces cuando yo voy a acceder a esta documentación, esta documentación está cifrada con la clave de otro usuario.

Entonces yo no voy a poder acceder a este tipo de recursos o no voy a poder acceder a esta documentación porque no tengo permisos para poder ver ese documento o no tengo permisos para poder ver esa imagen.

Entonces, como habíamos visto, el usuario que cifró unos datos pueda acceder a esos datos de forma totalmente transparente, no tiene que introducir en ningún momento una contraseña porque EPS identifica la contraseña del certificado del usuario, la utiliza para desbloquear esa contraseña compartida con todo lo que está cifrado con EPS y automáticamente el usuario puede utilizar toda la documentación que haya cifrado.

Sin embargo, esta documentación está protegida para cualquier otro usuario que aunque tenga acceso a esa documentación, aunque pueda haber esa información, no podría después acceder a esa documentación.

Como hemos podido comprobar, tenemos en Microsoft instalado por defecto en los sistemas Windows, dos sistemas de cifrado que son muy eficientes para ayudarnos a proteger los datos y la confidencialidad de aquellos recursos que tenemos almacenados en el dispositivo.

Es importante entender cómo funciona cada uno de ellos y qué propósito tiene cifrar las cosas mediante EFS y qué propósito tiene cifrar las cosas mediante bitlock.

Pero podemos combinar ambas tecnologías para tener un entorno mucho más seguro.

Llegamos al final de la sesión.

Os esperamos en el siguiente vídeo.