BitLocker Encryption

Transcribed on July 10, 2025 at 9:07 AM by Minutes AI

Speaker 1 (00:00)

Bienvenidos a esta nueva sesión.

Durante esta sesión vamos a explorar una de las herramientas más importantes en el mundo de la seguridad de datos en sistemas Windows y que además viene instalado por defecto, y es BitLocker.

¿En primer lugar, qué es BitLocker?

Bitlocker es una función de cifrado de disco completo que protege los datos almacenados en unidades de disco y en dispositivos USB.

¿Y qué significa esto?

Pues básicamente significa que BitLocker codifica todos los datos almacenados en el disco, asegurando que sólo aquellos que tienen la clave de cifrado adecuada pueden acceder a ellos.

Una de las características más destacadas de BitLocker es la seguridad, y es que utiliza un cifrado AES de 128 o de 256 bit, considerado actualmente altamente seguro.

De esta manera podemos proteger nuestros datos.

Además, BitLocker se integra de forma nativa en el sistema operativo Windows, lo que facilita enormemente su configuración y su uso para proteger nuestros datos de manera efectiva.

¿Y entonces, cómo funciona Bitlocker en la práctica?

BitLocker se puede activar en unidades de disco duro y en dispositivos usb desde el panel de control o bien utilizando la herramienta de administración de políticas de grupo.

Esto utiliza una combinación del tpm 1 pin o una contraseña o una llave usb para proteger la clave de cifrado, asegurando que solo aquellos autorizados pueden acceder a los datos.

Bitlocker además ofrece varios modos de operación.

Por ejemplo, el modo tpm utiliza el tpm para almacenar ahí y para proteger las claves de cifrado, proporcionando una protección adicional contra los ataques físicos.

Por otro lado, el modo de autenticación usuario requiere que los usuarios proporcionen una contraseña o una llave USB para desbloquear la unidad cifrada.

¿Cuáles son entonces los casos de uso de Bitlocker?

Bitlocker es ideal para proteger los datos sensibles en dispositivos de almacenamiento local, garantizando además el cumplimiento de normativas de seguridad en entornos empresariales y proporcionando un respaldo seguro de los datos en dispositivos extraíbles, comunidades u.

Sin embargo, antes de implementar BitLocker hay algunas consideraciones importantes a tener en cuenta.

Por ejemplo, es fundamental verificar la compatibilidad del hardware y el software con BitLocker antes de activarlo.

Además, se recomienda realizar copias de seguridad de las claves de recuperación de BitLocker para evitar la pérdida de acceso a los datos de forma permanente e irrecuperable.

Vamos a pasar a ver de forma práctica cómo podemos activar y configurar BitLocker para Windows.

Me encuentro en una máquina con Windows 11 donde vamos a activar el BitLocker y vamos a ver cómo se realiza este proceso de configuración.

Para empezar, nos vamos a dirigir directamente a la búsqueda y vamos a poner Bitlock.

Ya por BitLocker vamos a ver cómo desde el panel de control, en la sección de seguridad nos aparece.

Aquí tenemos que tener en cuenta varias cosas, y es que aunque es cierto que es compatible con sistemas operativos anteriores, hay un elemento bastante importante que si no lo tenemos, pues vamos a tener que buscar alguna alternativa de poder hacerlo, y hablo del tpm.

Fijaos que por aquí podemos ver la administración del tpm y esto nos va a decir si tenemos el tpm listo o no.

Si tenemos un dispositivo que no disponga de este hardware, la manera de hacerlo va a ser distinta.

En primer lugar deberíamos configurar las políticas de grupo para permitir que se pueda activar bitlocker sin necesidad de tener un tpm, pero es que además, para poder almacenar las claves se deberá disponer de una memoria usb extraíble, ya que si no BitLocker se va a quejar y no nos va a dejar activar el BitLocker de manera correcta.

Tras esto, pues si tuviésemos distintos pendrive conectados, nos aparecerían aquí abajo y se nos indicaría si están cifrados o no con BitLocker.

Y en este caso donde queremos llegar es a BitLocker, que lo queremos activar en este caso sobre la propia unidad del sistema, sobre la unidad c.

Básicamente tendríamos que darle aquí a activar Bitlocker.

Esto va a hacer una serie de preparación para comprobar que efectivamente nuestro hardware y software es compatible con Bitlocker y se nos va a indicar de qué manera queremos guardar una copia de seguridad de las claves de recuperación, ya que si perdemos estas claves de recuperación nos será imposible poder recuperar el contenido en el caso de que se nos olvide la contraseña.

En este caso se nos dan tres opciones posibles.

Por un lado, si tenemos vinculada una cuenta de Microsoft podemos salvarla de esta cuenta.

Por otro lado lo podemos guardar directamente en un fichero o también nos da la opción de que podríamos imprimir esta clave de recuperación.

Podemos elegir la opción que más se adapte a nuestras necesidades, pero en este caso vamos a darle a que nos la imprima.

Nos la va a imprimir desde luego aquí en un PDF para que veamos cuál sería este papel y qué es la información que contiene este papel.

Así que lo vamos a guardar en el escritorio, vamos a guardarlo como key PDF, que es el tipo que ya tenemos.

Lo guardamos, ya lo podemos ver aquí en el escritorio y bueno, básicamente si lo abrimos se nos da toda la información y es que básicamente esta clave va a proporcionarnos un identificador para la cual es válida, es decir, si nuestro identificador cuando vamos a hacer el destif de esta unidad se corresponde con esta de aquí, pues va a ser posible luego poder recuperar el contenido en el caso de que se nos olvide la clave que le vamos a indicar ahora.

Pero bueno, que sepáis que esto sería la manera de poder tener la clave de recuperación, la podríamos imprimir en papel y almacenar de manera segura en algún sitio que sepamos que no vamos a perder.

Una vez que hemos definido esta parte le vamos a dar a siguiente y básicamente tenemos dos opciones de qué es lo que queremos cifrar.

Por un lado se nos da la opción de cifrar únicamente el disco que está ocupado, que en este caso nos indica que es más rápido y que es ideal para nuevos ordenadores y nuevas unidades de discos.

Aquí la recomendación es que esto se aplique por ejemplo a una memoria USB que está limpia y que está nueva.

En el caso de tener ya tiempo y hemos estado trabajando con el ordenador, vamos a tener que optar por la segunda opción, que básicamente consiste en cifrar el disco completo.

Esto va a ser más lento, pero va a ser mejor para un ordenador que ya tenga la unidad en U.

Así que vamos a darle a siguiente.

Aquí también se nos indica qué tipo de cifrado queremos utilizar.

Vemos como desde Windows 10 se nos añadió un nuevo tipo de cifrado, en este caso XTS con AES y podemos indicar cuál queremos, si le queremos el modo nuevo o bien el modo compatible, es decir, si estamos trabajando con memorias USB o unidades extraíbles que vamos a trabajar en otros ordenadores o versiones de Windows anteriores, quizás queremos utilizar el modo compatible para que precisamente lo podamos utilizar en esta sección serie de sistemas operativos más antiguos.

En este caso y para la prueba vamos a trabajar directamente ya con este modo nuevo porque vamos a trabajar con un Windows 11, así que seleccionamos el modo nuevo.

Por último se nos indica que el tamaño, o sea, que el tipo de cifrado, el tamaño depender, el tiempo va a depender en función del tamaño del disco.

Entonces veis que aquí nos dice vamos a ejecutar el System check para comprobar que todo está bien.

Por supuesto que esto nos va a tardar un poquito más, pero bueno, le podemos dar primero a chequear y después que hayamos comprobado que esto es compatible tenemos que hacer el reinicio de Windows.

Empezaremos a cifrar la unidad, así que voy a darle aquí, vamos a reiniciar y ahora vamos a seguir viendo qué ocurre.

Acabamos de reiniciar y veis que ya me dice que el cifrado está en marcha.

Por aquí nos ha aparecido el mensaje.

Bueno, básicamente en esta ocasión pues vemos cómo se se ha empezado ya con este tipo de cifrado de la unidad, que está todo en regla y que como veis pues nada, estamos ya empezando a cifrar la unidad.

Por supuesto que luego podremos quitar la unidad, desactivar el Bitlocker o bien hacer el backup del Recovery key.

En este caso, pues como veis vamos a obtener otra vez el nuevo menú de antes si queremos indicar la clave en un fichero o si la queremos dejar en un papel, que es el mismo que ya tenemos para recuperarla.

Una vez que ha terminado de cifrar todo el disco, ya podemos encontrar tres opciones en vez de dos, en la cual encontramos o bien suspender la protección temporalmente o bien apagar Bitlock.

Entonces se destaca que el Cifrado del Disco se va a realizar en el momento en el cargamos el inicio de sesión en la cuenta, que como habéis visto esto va a empezar a cifrar la unidad.

1 vez que la tenemos entera cifrada, pues ya podemos ver este menú que vemos aquí y por tanto ya estarían los datos protegidos, es decir, si este ordenador alguien es capaz de robar el disco duro, no va a poder leer el contenido aunque lo intente montar en otro sistema operativo distinto, ya que el contenido que tiene esos datos estará cifrado a través de BitLocker y por tanto, insisto, no se podrá acceder al contenido de manera externa.

Para finalizar vamos a ver las principales conclusiones de esta sesión.

La función de BitLocker que está integrada en sistemas operativos Windows y que nos brinda una capa adicional de seguridad mediante el cifrado de disco completo.

En primer lugar, Bitlocker nos ofrece una seguridad robusta gracias al cifrado AES de 128 o 256 bits que utiliza para proteger nuestros datos.

Esta tecnología nos brinda la tranquilidad de que nuestros datos están protegidos contra accesos no autorizados.

Destacamos que una de las ventajas clave de este BitLocker es su integración nativa en el sistema Windows, lo que facilita su configuración y su uso.

Como hemos visto, no necesitamos instalar ningún tipo de software adicional, lo que simplifica el proceso de la protección de los datos.

Además, BitDrocker es altamente flexible en su implementación.

Nos ofrece diferentes modos de operación como es el uso del TPM o la autenticación del usuario, lo que nos permite adaptarlo según nuestras necesidades específicas de seguridad.

Se pueden conocer diversos casos de uso de Bitlocker, desde proteger los datos sensibles en dispositivos de almacenamiento local, hasta garantizar el cumplimiento de normativas de seguridad en entornos empresariales e incluso respaldar de manera segura datos en dispositivos extraíbles como son unidades USB.

Sin embargo, antes de implementar Bitlocker es fundamental tener en cuenta algunas consideraciones importantes, como por ejemplo verificar la compatibilidad del hardware y del software que sea compatible con Bitlocker.

Además, también realizar las copias de seguridad de las claves de recuperación es un paso esencial para garantizar una implementación exitosa.

En resumen, BitLocker es una herramienta poderosa y versátil para proteger datos en sistemas Windows.

Nos proporciona una capa adicional de seguridad que ayuda a prevenir el acceso autorizado a los datos almacenados y además de eso, viene ya integrado por defecto de manera nativa en el sistema Windows.

Y con esto llegamos al final de la sesión.

Os esperamos en el siguiente vídeo.