ManageEngine

Domina el cifrado: buenas prácticas para gestionar **BitLocker** con éxito

Tabla de contenido

Introducción

En la era digital, la información es poder... y también un blanco fácil. Cada día, la tecnología avanza a pasos agigantados, pero con ella, también evolucionan las amenazas cibernéticas.

¿Te imaginas perder tu computador portátil con documentos confidenciales? ¿O que alguien acceda a tus archivos personales solo porque tu disco duro no estaba protegido?

Aquí es donde entra en juego BitLocker, la herramienta de cifrado de Microsoft diseñada para blindar tus datos ante accesos no autorizados. Sin embargo, activarla es solo el primer paso. Una gestión deficiente del cifrado puede ser igual de peligrosa que no usarlo en absoluto.

En este ebook, descubrirás las mejores prácticas para gestionar BitLocker de forma eficiente, reforzar la seguridad de tu información y evitar que tus datos caigan en las manos equivocadas.

¿Qué es el cifrado de **BitLocker?**

BitLocker permite el cifrado completo de discos para proteger datos sensibles frente a pérdidas o robos.

Originalmente desarrollado bajo el nombre “Cornerstone” en 2004, formó parte de la arquitectura de la Base de Computación Segura de Próxima Generación de Microsoft. Antes de su lanzamiento oficial en Windows Vista, era conocido como Inicio Seguro.

Para reforzar la seguridad, esta herramienta incorpora el “Enraizamiento de Integridad de Código”, una función que verifica la integridad de los archivos críticos del sistema.

Por defecto, utiliza claves criptográficas para cifrar las unidades seleccionadas, asegurando que solo los usuarios autorizados puedan acceder a la información.

El contenido solo se desbloquea cuando se introduce la contraseña correcta o los datos del Módulo de Plataforma Segura (TPM, por sus siglas en inglés) coinciden, garantizando así una protección sólida y confiable.

¿Cómo gestionar el **cifrado de BitLocker?**

La gestión eficaz de BitLocker implica una serie de pasos y consideraciones para asegurar que el cifrado de datos se implemente y se mantenga correctamente.

Habilitación de **BitLocker en Windows**

1. Acceder a la configuración:

- Haz clic en el botón de Inicio de Windows y selecciona “Panel de control”.
- Navega a “Sistema y seguridad” y luego a “Cifrado de unidad BitLocker”.

2. Activarlo en la unidad deseada:

- Selecciona la unidad que deseas cifrar y haz clic en “Activar BitLocker”.
- Elige un método de autenticación:
  - **Contraseña:** ingresa una contraseña segura.
  - **Tarjeta inteligente:** usa una tarjeta inteligente compatible.
  - **Módulo de plataforma segura (TPM):** utiliza el TPM del dispositivo para una autenticación transparente.

3. Gestionar la clave de recuperación:

- Cuando se te solicite, selecciona una opción para hacer una copia de seguridad de tu clave de recuperación o almacénala en una bóveda de contraseñas (Password Manager Pro).

4. Iniciar el proceso de cifrado:

- Decide si cifrar solo el espacio utilizado o toda la unidad.
- Elige el modo de cifrado adecuado según tu entorno.
- Inicia el cifrado y espera a que se complete.

Administración del cifrado

Contenido relacionado: Seguridad de datos en los endpoints

Administrar BitLocker va más allá de simplemente activar el cifrado; es la clave para garantizar que la protección de tus datos sea realmente efectiva. Piensa en esta herramienta como un candado de alta seguridad para tu información, pero sin una gestión adecuada, sería como tener una llave para cada puerta de un edificio.

Aquí es donde Endpoint Central entra en acción, convirtiendo el cifrado básico en una solución inteligente que combina eficiencia, seguridad y cumplimiento normativo, todo en una sola consola.

Sin una herramienta de gestión de BitLocker tendrás que verificar manualmente tus dispositivos y solucionar problemas de cifrado uno por uno, lo que ocasionará la pérdida de información de seguridad crítica.

Beneficios de la gestión de **BitLocker en Endpoint Central**

Administración centralizada

Gestiona el cifrado de unidad BitLocker, el Módulo de Plataforma Segura (TPM) y otras configuraciones de protección desde una única consola. Automatiza actividades como la generación y el mantenimiento de claves de recuperación para un funcionamiento fluido.

Implementación de políticas granulares

Configura políticas flexibles para satisfacer requisitos de cifrado específicos y asigna políticas a grupos personalizados para aplicaciones específicas. Además, implementa políticas ligeras mediante comunicaciones seguras entre agente y servidor para mayor eficiencia.

Informes exhaustivos

Consolida los datos de auditoría en informes detallados y visualiza el estado del cifrado mediante paneles intuitivos. Obtén visibilidad del estado del cifrado de la red para garantizar la seguridad de los datos.

Cifrado automático

Habilita la implementación automática de políticas de cifrado para múltiples usuarios sin intervención manual, simplificando la gestión del cifrado con una implementación de políticas en un solo paso.

Contenido relacionado: Gestión del cifrado de disco BitLocker

Monitoreo del estado de cifrado de todos los dispositivos

Endpoint Central proporciona una visión en tiempo real del estado del cifrado BitLocker de todos los dispositivos de la red. Esto ayuda a los administradores de TI a identificar y solucionar cualquier problema de encriptación de forma rápida y sencilla.

Gestión remota del cifrado

Esta herramienta de ManageEngine permite a los administradores de TI gestionar el cifrado BitLocker en dispositivos Windows de forma remota. Esto incluye tareas como cifrar y descifrar dispositivos, y restablecer la clave de recuperación de BitLocker.

¿Cómo deshabilitar el cifrado de **BitLocker?**

Cuando esta herramienta está activada, el sistema no puede identificar la ubicación exacta donde se almacenan los archivos dentro de la unidad cifrada. Esto puede generar problemas al crear imágenes del disco. Para garantizar un proceso de imagen eficiente, es necesario descifrar la unidad protegida con BitLocker antes de continuar.

Deshabilitar **BitLocker** a través del símbolo del **sistema de Windows**

Para desactivarlo mediante la línea de comandos, asegúrese de haber iniciado sesión como administrador. Sigue estos pasos para desactivar el cifrado mediante el símbolo del sistema:

1. Abre el símbolo del sistema en modo administrador.
2. Para comprobar el estado del cifrado de BitLocker en el sistema, ejecuta el comando: **gestionar-bde-estado**
3. Asegúrate de que los resultados para las unidades requeridas (C:, D:, etc.) sean los siguientes:

- **Estado de conversión:** completamente descifrado
- **Porcentaje cifrado:** 0,0%

4. Si el resultado es “Porcentaje cifrado: 100,0 %”, descifra el BitLocker de las unidades requeridas utilizando los comandos: **manage-bde -off <letra de unidad>:**

Por ejemplo: manage-bde -off C:

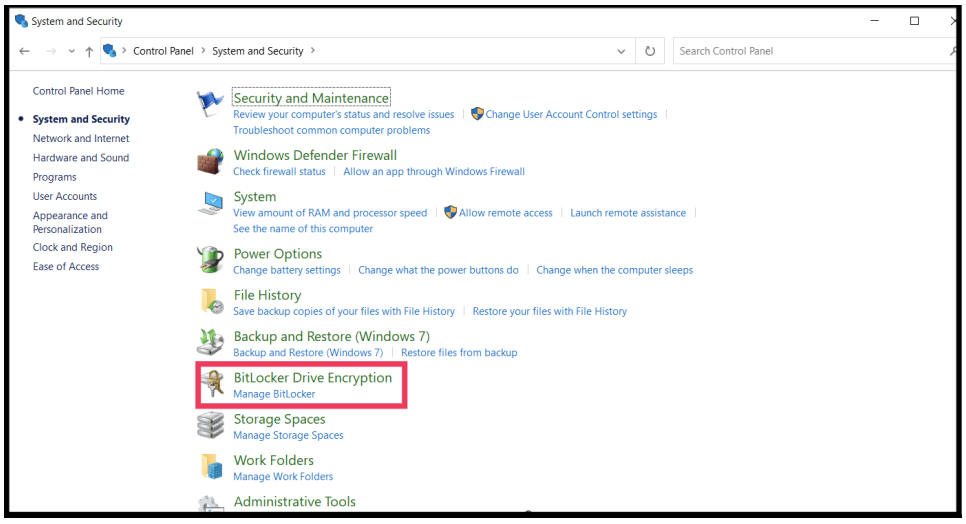
5. Verifica el estado de BitLocker después de deshabilitarlo usando el comando (**manage-bde -status**) y asegúrate de: **“Porcentaje cifrado: 0.0%”**

6. Reinicia tu computadora antes de continuar con el proceso de creación de la imagen.

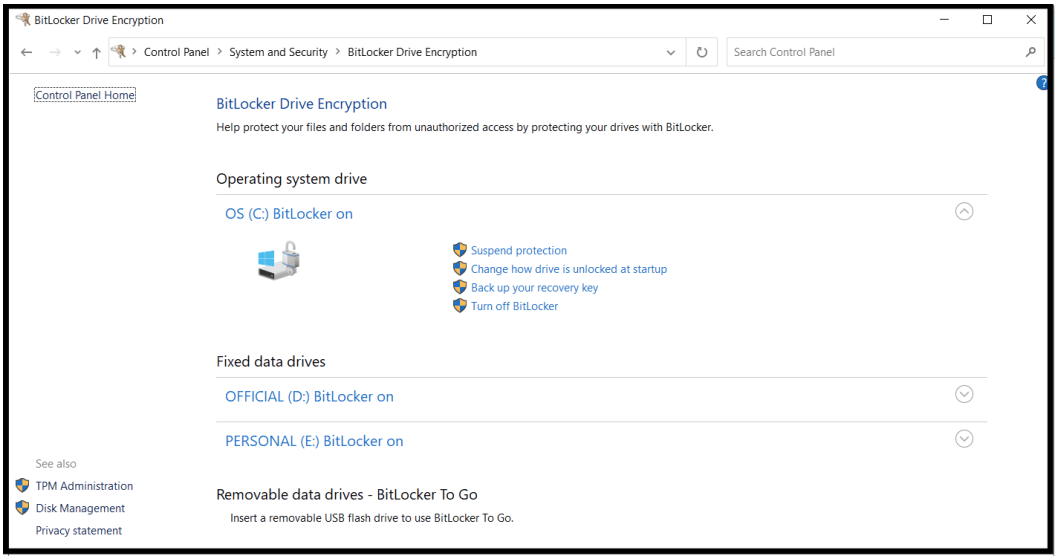
Deshabilitar BitLocker a través del modo **GUI de Windows**

Para eliminarlo mediante el modo GUI de Windows, asegúrate de tener credenciales de administrador para eliminar el cifrado de BitLocker. Siga los pasos a continuación:

1. Haz clic en **Inicio, Panel de control, Sistema y seguridad** y, por último, en **Cifrado de unidad BitLocker.**



2. Busca la unidad en la que deseas desactivar el cifrado de unidad BitLocker y haz clic en **Desactivar BitLocker.**



3. Se mostrará un mensaje indicando que la unidad se descifrará y que el proceso puede tardar un tiempo. Haz clic en Desactivar BitLocker/Descifrar la unidad para continuar y desactivar BitLocker en la unidad.

4. Reinicia tu computadora antes de continuar con la creación de la imagen. No olvides que puede que tarde un tiempo en descifrar la unidad y eliminar la protección de BitLocker.

¿Cómo asegurarse de que se elimine el cifrado de Bitlocker?

Puedes comprobar si el cifrado de BitLocker se ha eliminado, verificando si el icono del candado de BitLocker se ha eliminado en la unidad en cuestión, accediendo a ella. Puedes repetir los mismos pasos para desactivar el cifrado en otras unidades.

Deshabilitar **BitLocker a través de Windows PowerShell**

Para desactivar el cifrado a través de Windows PowerShell, debes tener instalada esta herramienta en tu sistema. De lo contrario, descarga e instala la versión correcta de PowerShell desde el sitio web de Microsoft.

Consulta también los requisitos del sistema de PowerShell antes de continuar con la instalación.

Si la partición con el sistema operativo contiene claves de desbloqueo automático, el cmdlet para deshabilitar el cifrado de BitLocker no funcionará. Puedes usar el cmdlet Clear-BitLockerAutoUnlock en la ventana de PowerShell para eliminar todas las claves de desbloqueo automático y deshabilitar BitLocker en la partición.

¿Cómo **deshabilitar Bitlocker** para todos los volúmenes?

1. Abre Windows Powershell en modo administrador y ejecuta los siguientes comandos:

- PS C:\>$BLV = Obtener-BitLockerVolume
- PS C:\>Deshabilitar-BitLocker -MountPoint $BLV

2. Verifica el proceso de descifrado utilizando el siguiente método:

- Ejecutar comando: PS C:\> Get-BitlockerVolume
- Verifica el progreso del descifrado en "**Estado del volumen**" y "Porcentaje de cifrado". Estos valores deben ser "**completamente descifrado**" y 100% para confirmar que el descifrado se ha completado.
- El progreso se puede ver en **Panel de Control → Sistema y seguridad → Cifrado de unidad BitLocker.**

3. Reinicia tu computadora antes de continuar con el proceso de creación de la imagen.

¿Cómo deshabilitarlo para un solo volumen?

1. Abre Windows Powershell en modo administrador
2. Deshabilitar BitLocker - Punto de montaje "C:"
3. Verifica el proceso de descifrado utilizando el siguiente método:

- Ejecuta el comando: PS C:\> Get-BitlockerVolume -MountPoint “C:”
- Verifica el progreso del descifrado en “**Estado del volumen**” y “**Porcentaje de cifrado**”. Estos valores deben ser “**completamente descifrado**” y 100% para confirmar que el descifrado se ha completado.
- El progreso se puede ver en **Panel de control → Sistema y seguridad → Cifrado de unidad BitLocker.**

4. Reinicia tu computadora antes de continuar con el proceso de creación de la imagen.
5. Espera hasta que se muestre que el cifrado de BitLocker está desactivado.

Otras buenas prácticas en la **gestión de BitLocker**

- Protege los datos de tus desktops, laptops y servidores usando cifrado de disco completo.
- Haz siempre un respaldo antes del cifrado de disco.
- Crea una contraseña o PIN con procedimientos de formulación de contraseñas robustos. Por ejemplo, usa una combinación de letras (tanto minúsculas como mayúsculas), números y caracteres especiales. Entre más larga sea la contraseña, más difícil será de adivinar.
- Mientras accedes a la red, usa siempre WPA2 y conéctate a una VPN, lo que ayudará a optimizar el tráfico mediante un túnel web definido.
- Realiza respaldos de manera regular luego de un cifrado de disco completo para mantener protegidos sus datos.
- Educa a los empleados sobre la importancia del cifrado y las mejores prácticas en el manejo de datos sensibles.
- Mantén el software y las políticas de seguridad actualizadas para proteger tus sistemas contra nuevas amenazas.

Riesgos de no gestionar con **eficacia BitLocker**

- Pérdida de acceso a datos críticos por claves de recuperación mal gestionadas.
- Filtraciones de información sensible debido a configuraciones inadecuadas o desactivación accidental del cifrado.
- Incumplimiento de normativas de seguridad como GDPR, HIPAA o ISO 27001, lo que puede derivar en sanciones.
- Mayor vulnerabilidad ante ataques cibernéticos, como el acceso no autorizado a dispositivos perdidos o robados.
- Problemas operativos y costos adicionales por falta de automatización y supervisión del estado de cifrado en los dispositivos.

Conclusión

proteger nuestros datos sensibles ya no es una opción, es una necesidad. Sin una estrategia de seguridad sólida, cualquier dispositivo puede convertirse en una puerta abierta para intrusos, poniendo en riesgo información valiosa.

BitLocker es una poderosa herramienta de cifrado, pero su verdadero potencial se desbloquea con una gestión eficiente. Siguiendo estas buenas prácticas, no solo reforzarás la seguridad de tus datos, sino que también garantizarás un acceso seguro y controlado, evitando pérdidas de información y asegurando el cumplimiento normativo.

En seguridad, la prevención es la clave. ¡No dejes tu información al azar y convierte BitLocker en tu mejor aliado!

Paola Andrea Quiroga

Marketing Analyst

ManageEngine LATAM

Acerca de **ManageEngine**

ManageEngine desarrolla el conjunto de software de gestión de TI más completo de la industria. Tenemos todo lo que necesita: más de **90 productos** y herramientas gratuitas para gestionar todas sus operaciones de TI, desde redes y servidores hasta aplicaciones, mesa de ayuda, Active Directory, seguridad para desktops y dispositivos móviles.

Desde 2001, los equipos de TI como el suyo han recurrido a nosotros para obtener un software asequible, rico en funciones y fácil de usar. Puede encontrar nuestras soluciones on-premises y en la nube que impulsan la TI de más de 180.000 empresas en todo el mundo, incluidas nueve de cada diez empresas de la lista Fortune 100.

A medida que usted se prepara para los desafíos de la gestión de TI que se avecinan, nosotros lideraremos el camino con nuevas soluciones, integraciones contextuales y otros avances que solo pueden provenir de una empresa dedicada singularmente a sus clientes. Y al ser una división de Zoho Corporation, seguiremos trabajando por establecer una estrecha alineación de TI con los negocios que usted necesitará para aprovechar las oportunidades en el futuro.

ManageEngine