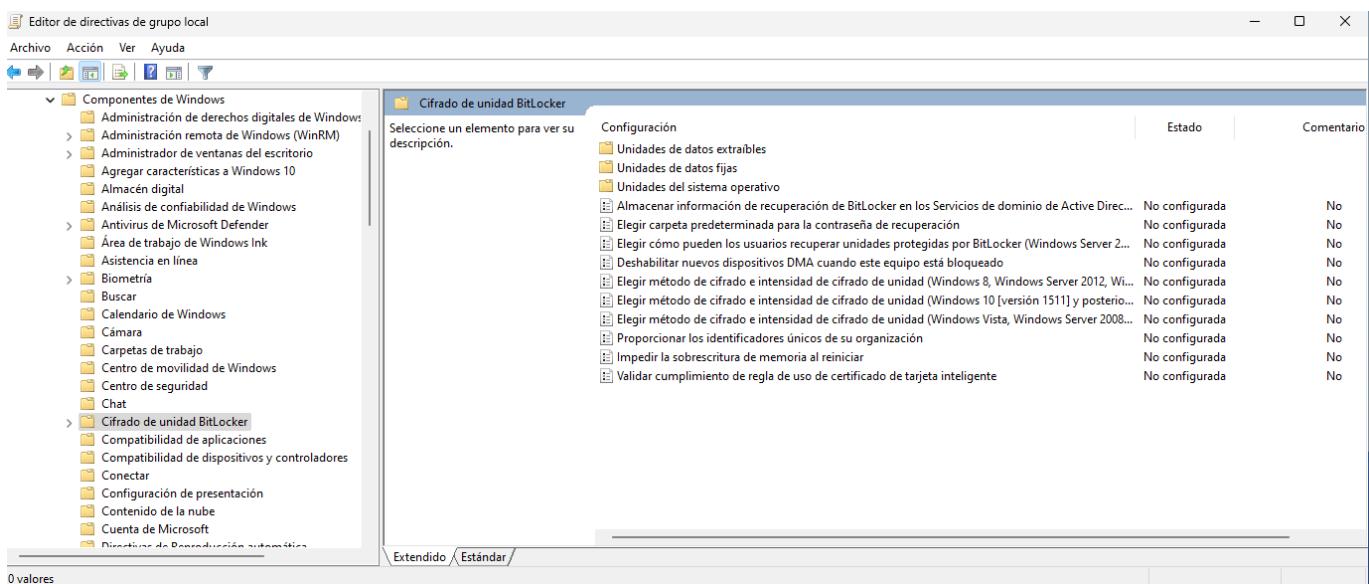


[FORT] Práctica 9: Fortificación de la información y auditoría de Windows 11

1. Cifrado de información con BitLocker

a) Revisa las políticas de seguridad de BitLocker que se encuentran en la configuración del equipo:



The screenshot shows the 'Editor de directivas de grupo local' (Group Policy Editor) window. The left pane shows a tree structure of Group Policy objects (GPOs). The 'Cifrado de unidad BitLocker' (BitLocker Drive Encryption) GPO is selected. The right pane displays the 'Configuración' (Configuration) tab for this GPO. The table lists various BitLocker configuration settings, all of which are currently set to 'No configurada' (Not configured) and marked with a 'No' in the 'Comentario' (Comment) column. The settings include: 'Unidades de datos extraibles', 'Unidades de datos fijas', 'Unidades del sistema operativo', 'Almacenar información de recuperación de BitLocker en los Servicios de dominio de Active Dire...', 'Elegir carpeta predeterminada para la contraseña de recuperación', 'Elegir cómo pueden los usuarios recuperar unidades protegidas por BitLocker (Windows Server 2...', 'Deshabilitar nuevos dispositivos DMA cuando este equipo está bloqueado', 'Elegir método de cifrado e intensidad de cifrado de unidad (Windows 8, Windows Server 2012, Wi...', 'Elegir método de cifrado e intensidad de cifrado de unidad (Windows 10 [versión 1511] y posterio...', 'Elegir método de cifrado e intensidad de cifrado de unidad (Windows Vista, Windows Server 2008...)', 'Proporcionar los identificadores únicos de su organización', 'Impedir la sobreescritura de memoria al reiniciar', and 'Validar cumplimiento de regla de uso de certificado de tarjeta inteligente'.

i. ¿Es necesario realizar algún ajuste para activarlo? ¿Es necesario realizar algún cambio para mejorar dicho cifrado?

Para activar bitlocker mediante directivas de grupo local es necesario configurar donde está localizada la carpeta para la contraseña de recuperación

 Elegir carpeta predeterminada para la contraseña de recuperación

 Elegir carpeta predeterminada para la contraseña de recuperación

Habilitada

Deshabilitada

Comentario:

Compatible con: Al menos Windows Vista

Opciones: Configurar la ruta de acceso predeterminada de carpetas:
 Especifique una ruta de acceso completa o incluya las variables de entorno del equipo en la ruta de acceso. Por ejemplo, escriba "\\servidor\carpetaDeCopiaDeSeguridad", o "%variableDeEntornoDeUnidadSegura%\carpetaDeCopiaDeSeguridad". Nota: en todos los casos, el usuario podrá seleccionar otras carpetas donde guardar la contraseña de recuperación.

Ayuda: Esta configuración de directiva permite especificar la ruta de acceso predeterminada que se muestra cuando el asistente para la instalación del Cifrado de unidad BitLocker solicita al usuario que escriba la ubicación de una carpeta donde se guardará la contraseña de recuperación. Esta configuración de directiva se aplica al activar BitLocker. Si habilita esta configuración de directiva, puede especificar la ruta que se usará como ubicación de carpeta predeterminada cuando el usuario seleccione la opción de guardar la contraseña de recuperación en una carpeta. Puede especificar una ruta de acceso completa o incluir en la ruta las variables del entorno del equipo de destino. Si la ruta de acceso no es válida, el asistente para la instalación de BitLocker mostrará la vista de carpetas de nivel superior del equipo. Si deshabilita o no establece esta configuración de directiva, el asistente para la instalación de BitLocker mostrará la vista de carpetas de nivel superior del equipo cuando el usuario seleccione la opción de guardar la contraseña de recuperación en una carpeta.

Para mejorar el cifrado podemos modificar la política de "Elegir método de cifrado e intensidad de cifrado de unidad" para sistemas de Windows 10 en adelante:

Elegir método de cifrado e intensidad de cifrado de unidad (Windows 10 [versión 1511] y poste...)

Elegir método de cifrado e intensidad de cifrado de unidad (Windows 10 [versión 1511] y posteriores)

No configurada Comentario:

Habilitada

Deshabilitada Compatible con: Se requiere al menos Windows Server 2016 o Windows 10

Opciones: Ayuda:

Selecciona el método de cifrado de las unidades del sistema operativo:

XTS-AES de 128 bits (predeterminado)

Selecciona el método de cifrado de las unidades de datos fijas:

XTS-AES de 128 bits (predeterminado)

Selecciona el método de cifrado de las unidades de datos extraíbles:

AES-CBC de 128 bits (predeterminado)

Esta configuración de directiva te permite configurar el algoritmo y la intensidad del cifrado que se usan en el Cifrado de unidad BitLocker. Esta configuración de directiva se aplica al activar BitLocker. El cambio del método de cifrado no tendrá ningún efecto si la unidad ya está cifrada o si el cifrado está en curso.

Si habilitas esta configuración de directiva para configurar un algoritmo de cifrado y la intensidad de cifrado de clave de unidades de datos fijas, unidades del sistema operativo y unidades de datos extraíbles de manera individual. Para unidades del sistema operativo y unidades fijas, se recomienda usar el algoritmo XTS-AES. Para unidades extraíbles, usa el cifrado AES-CBC de 128 bits o AES-CBC de 256 bits si la unidad se usará en otros dispositivos que no ejecuten Windows 10 (versión 1511).

Si deshabilitas o no estableces esta configuración de directiva, BitLocker usará AES con la misma intensidad de bits (128 bits o 256 bits) que la configuración de directiva "Elegir método de cifrado e intensidad de cifrado de unidad (Windows Vista

Aceptar Cancelar Aplicar

From:

<http://knoppia.net/> - Knoppia

Permanent link:

http://knoppia.net/doku.php?id=master_cs:fortificacion:p9&rev=1745326982

Last update: 2025/04/22 13:03

