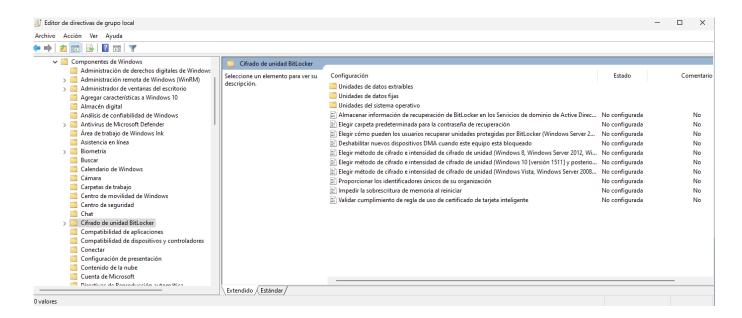
[FORT] Práctica 9: Fortificación de la información y auditoría de Windows 11

1. Cifrado de información con BitLocker

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

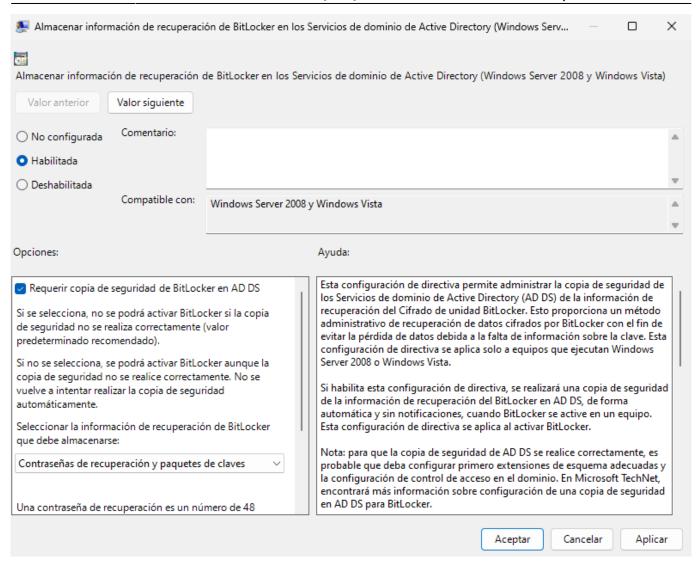


i. ¿Es necesario realizar algún ajuste para activarlo? ¿Es necesario realizar algún cambio para mejorar dicho cifrado?

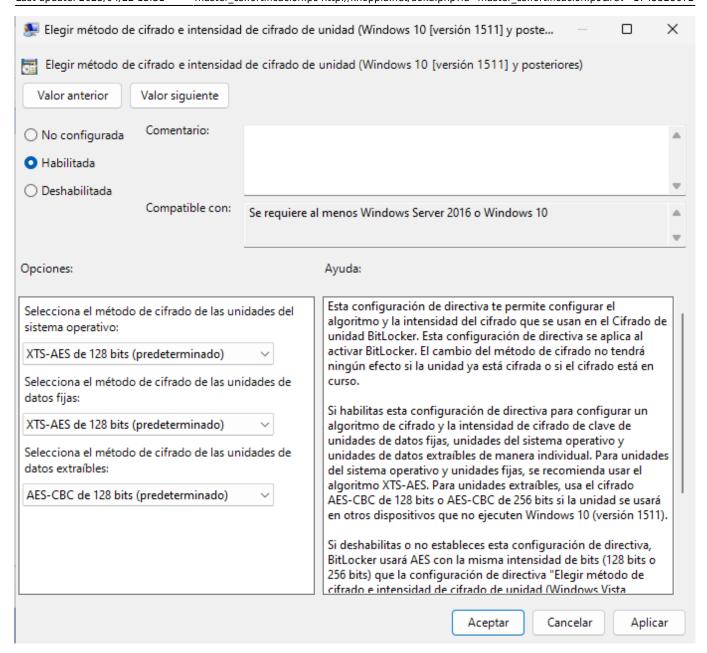
Para activar bitlocker mediante directivas de grupo local es necesario configurar donde está localizada la carpeta para la contraseña de recuperación

💽 Elegir carpeta predeterminada para la contraseña de recuperación — 🔻 🗆								×
Elegir carpeta predeterminada para la contraseña de recuperación Valor anterior Valor siguien								
○ No configurada	Comentario:							Δ
Habilitada								
Oeshabilitada			menos Windows Vista					
Opciones:			Ayuda:					
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.			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 la
					Aceptar	Cancelar	A	plicar

Si el equipo está en un dominio también se recomienda activar la opción "Almacenar información de Bitlocker en los Servicios de dominio de Active Directory" para almacenar la clave de recuperación en el servidor del dominio.



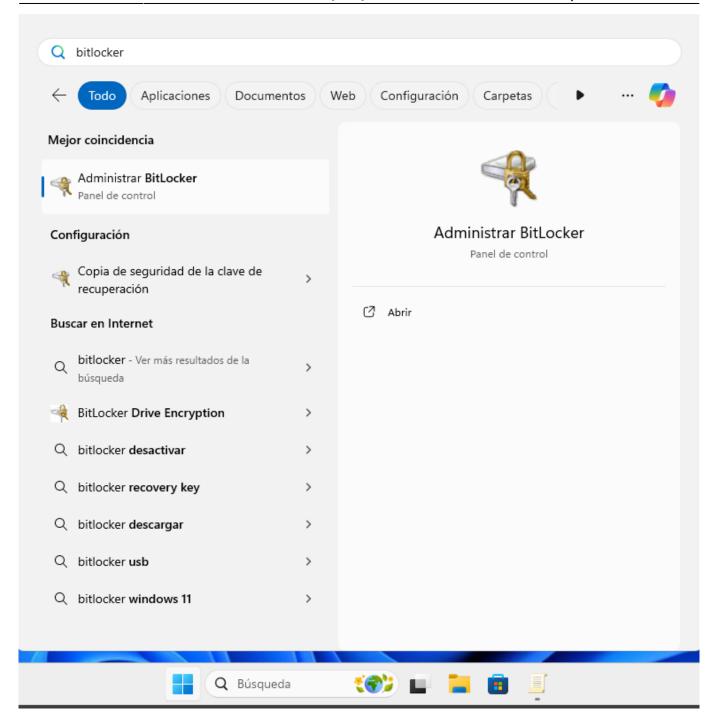
Para mejorar el cifrado podemos modificar la política de "Elegir método de cifrado e intensidad de cifrado de unidad" para sistemas de Windows 10 en adelante:



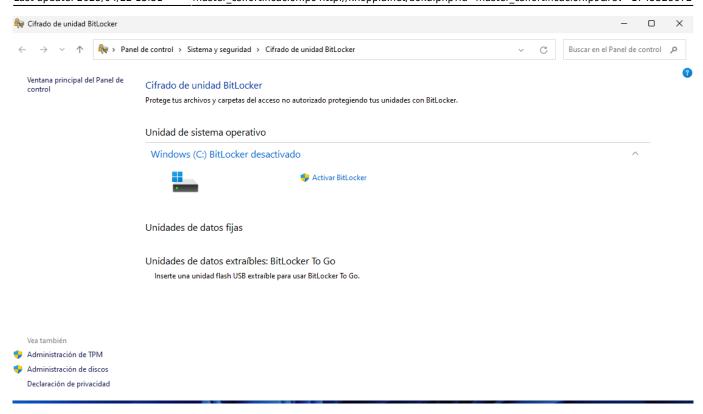
b) Realiza la activación de firado Bitlocker sobre C:\

i. Indica los pasos a seguir para realizar dicho cifrado

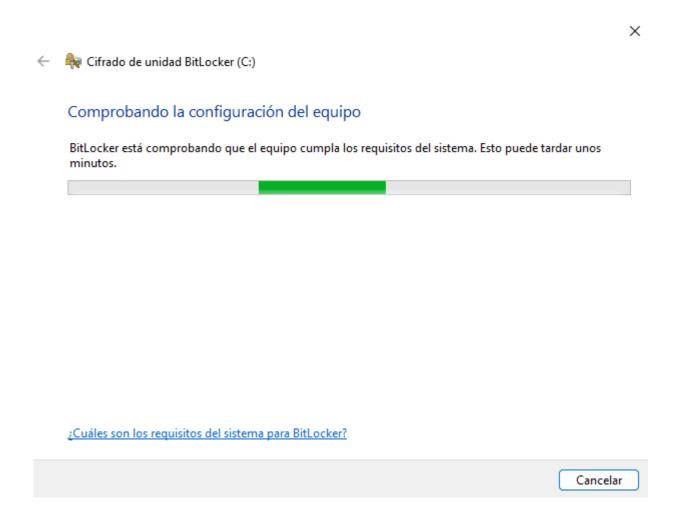
La forma más simple de realizar el cifrado del disco mediante bitlocker es pulsar el botón windows y buscar bitlocker:



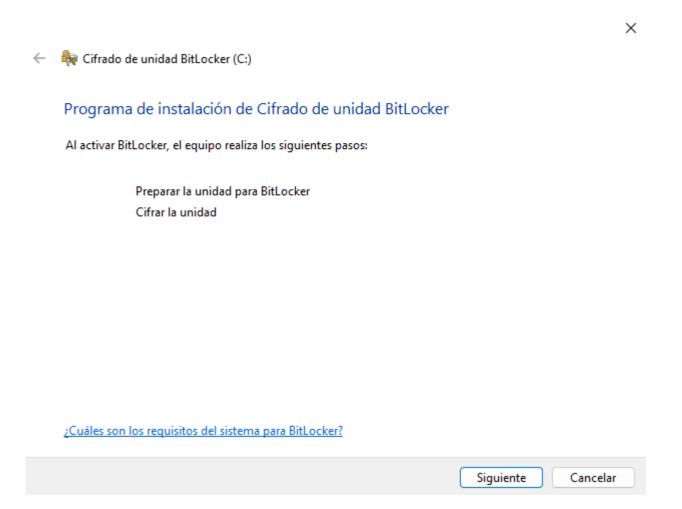
Una vez dentro de del administrador de cifrado de bitlocker se verá una ventana como esta:



Para activar Bitlocker simplemente debemos pulsar en donde pone "Activar Bitlocker"

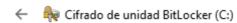


El sistema realizará una comprobación y si el sistema puede aplicar bitlocker veremos una ventana como esta:



Para proceder presionaremos en el botón de siguiente y nos aparecerá este aviso:





Preparación de la unidad para BitLocker

Se usará una unidad existente o espacio disponible sin asignar en la unidad de disco duro para activar BitLocker.



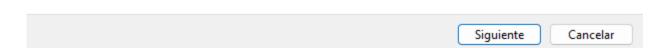
Precaución:



Se recomienda hacer una copia de seguridad de los archivos y datos imprescindibles antes de continuar.

Usar el historial de archivos para realizar una copia de seguridad

Este proceso puede tardar unos minutos, según el tamaño y el contenido de la unidad.



Presionaremos en siguiente, el sistema procederá a preparar el disco para su cifrado y tras eso aparecerá una ventana como la siguiente:

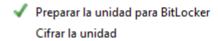




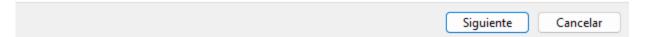
Programa de instalación de Cifrado de unidad BitLocker

Ya no podrá usar el Entorno de recuperación de Windows a menos que se habilite manualmente y se mueva a la unidad del sistema.

Al activar BitLocker, el equipo realiza los siguientes pasos:



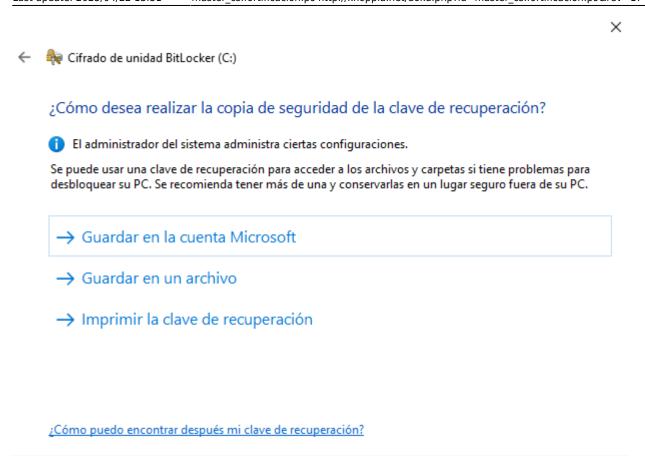
¿Cuáles son los requisitos del sistema para BitLocker?



Se presiona en siguiente y se nos preguntará como queremos guardar la clave de recuperación:

Cancelar

Siguiente



Como no tenemos cuenta microsoft, en este caso se guardará la clave de recuperación en un archivo:



Una vez guardada la clave se puede proceder a pulsar en siguiente y se selecciona la opción de cifrar el espacio usado para que no lleve demasiado el proceso de cifrado de la unidad:







Elegir qué cantidad de la unidad desea cifrar

Si está instalando BitLocker en una unidad nueva o un equipo nuevo, solo es necesario cifrar la parte de la unidad que se está usando actualmente. BitLocker cifrará los datos nuevos automáticamente conforme los agregue.

Si están instalando BitLocker en un equipo o una unidad que ya se está usando, entonces cifre la unidad completa. Al cifrar la unidad completa, se asegura de que todos los datos están protegidos, incluso datos que haya podido eliminar pero que aún puedan contener información recuperable.

- O Cifrar solo el espacio en disco utilizado (mejor y más rápido para unidades y equipos nuevos)
- Cifrar la unidad entera (más lento, pero mejor para unidades y PCs que ya se encuentran en uso)



Tras eso le damos a siguiente y seleccionamos la opción de Modo de cifrado nuevo:





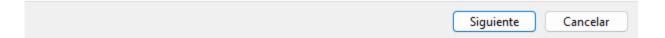
Elección del modo de cifrado que se usará

La actualización de Windows 10 (versión 1511) introduce un nuevo modo de cifrado de disco (XTS-AES). Este modo ofrece soporte de integridad adicional, pero no es compatible con las versiones anteriores de Windows.

Si se trata de una unidad extraíble que usarás con una versión anterior de Windows, elige el modo Compatible.

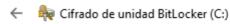
Si es una unidad fija o si solo se utilizará en dispositivos con la actualización de Windows 10 (versión 1511) o versiones posteriores, elige el nuevo modo de cifrado.

- Modo de cifrado nuevo (recomendado para las unidades fijas en este dispositivo)
- Modo Compatible (recomendado para las unidades que se puedan mover de este dispositivo)



Finalmente nos permitirá iniciar el cifrado, se recomienda marcar la casilla de ejecutar la comprobación del sistema de bitlocker:





¿Está listo para cifrar esta unidad?

El cifrado podría tardar varios minutos, según el tamaño de la unidad.

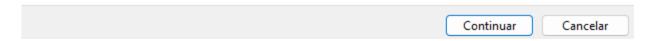
Puede continuar trabajando mientras se cifra la unidad, aunque es posible que se ralentice el funcionamiento del equipo.

Ejecutar la comprobación del sistema de BitLocker

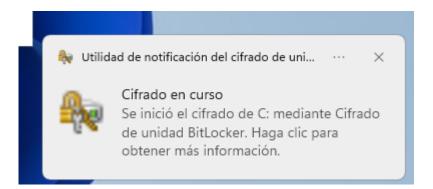
La comprobación del sistema confirmará que BitLocker pueda leer correctamente las claves de recuperación y de cifrado antes de que se cifre la unidad.

BitLocker reiniciará el equipo antes de iniciar el cifrado.

Nota: esta comprobación puede tardar un tiempo, pero se recomienda asegurarse de que el método de desbloqueo seleccionado funciona sin que sea necesario usar la clave de recuperación.



Una vez le demos a iniciar cifrado aparecerá una notificación indicando que se ha iniciado el cifrado y este se realizará en segundo plano:



From:

http://knoppia.net/ - Knoppia

Permanent link:

http://knoppia.net/doku.php?id=master_cs:fortificacion:p9&rev=174532867

Last update: 2025/04/22 13:31

