[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

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. 3/24

Almacenar información de re	cuperación de BitLocke	r en los S	Servicios de dominio de Active Directory (Windows Serv —	
Almacenar información de recupe Valor anterior Valor siguie	eración de BitLocker en ente	los Serv	rvicios de dominio de Active Directory (Windows Server 2008 y W	ndows Vista)
O No configurada Comentari	o:			
🔾 Habilitada				
🔿 Deshabilitada				w
Compatibl	e con: Windows Serv	/er 2008 y	3 y Windows Vista	
				T
Opciones:	Difference AD DC		Ayuda:	seguridad de
Requerir copia de seguridad de Si se selecciona, no se podrá activ de seguridad no se realiza correct predeterminado recomendado). Si no se selecciona, se podrá activ copia de seguridad no se realice o vuelve a intentar realizar la copia d automáticamente. Seleccionar la información de recu que debe almacenarse: Contraseñas de recuperación y pu Una contraseña de recuperación o	e BitLocker en AD DS var BitLocker si la copia amente (valor var BitLocker aunque la correctamente. No se de seguridad uperación de BitLocker aquetes de claves es un número de 48	~	 Lesta configuración de directiva permite administraria copia de los Servicios de dominio de Active Directory (AD DS) de la infor recuperación del Cifrado de unidad BitLocker. Esto proporciona administrativo de recuperación de datos cifrados por BitLocker evitar la pérdida de datos debida a la falta de información sobre configuración de directiva se aplica solo a equipos que ejecutar Server 2008 o Windows Vista. Si habilita esta configuración de directiva, se realizará una copia de la información de recuperación del BitLocker en AD DS, de fu automática y sin notificaciones, cuando BitLocker se active en u Esta configuración de directiva se aplica al activar BitLocker. Nota: para que la copia de seguridad de AD DS se realice correco probable que deba configurar primero extensiones de esquema la configuración de control de acceso en el dominio. En Micros encontrará más información sobre configuración de una copia en AD DS para BitLocker. 	Agundad de mación de un método con el fin de la clave. Esta i Windows de seguridad orma in equipo. tamente, es adecuadas y oft TechNet, de seguridad
			Aceptar Cancelar	Aplicar

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 —		\times
Elegir método de cifrado e intensidad Valor anterior Valor siguiente	de cifrado de	unidad (Windows 10 [versión 1511] y posteriores)		
O No configurada Comentario:				
 Habilitada 				
🔿 Deshabilitada				Ŧ
Compatible con:	Se requiere a	Il menos Windows Server 2016 o Windows 10		
				Ŧ
Opciones:		Ayuda:		
Selecciona el método de cifrado de las un sistema operativo: XTS-AES de 128 bits (predeterminado) Selecciona el método de cifrado de las un datos fijas: XTS-AES de 128 bits (predeterminado) Selecciona el método de cifrado de las un datos extraíbles: AES-CBC de 128 bits (predeterminado)	idades del idades de idades de idades de	Esta configuración de directiva te permite configu algoritmo y la intensidad del cifrado que se usan e unidad BitLocker. Esta configuración de directiva s activar BitLocker. El cambio del método de cifrado ningún efecto si la unidad ya está cifrada o si el cif curso. Si habilitas esta configuración de directiva para co algoritmo de cifrado y la intensidad de cifrado de unidades de datos fijas, unidades del sistema oper unidades de datos extraíbles de manera individual del sistema operativo y unidades fijas, se recomier algoritmo XTS-AES. Para unidades extraíbles, usa e AES-CBC de 128 bits o AES-CBC de 256 bits si la un en otros dispositivos que no ejecuten Windows 10 Si deshabilitas o no estableces esta configuración BitLocker usará AES con la misma intensidad de b 256 bits) que la configuración de directiva "Elegin cifrado e intensidad de cifrado de unidad (Window	irar el en el Cifrado se aplica al o no tendrá frado está en infigurar un clave de rativo y I. Para unida nida usar el el cifrado nidad se usa) (versión 151 de directiva, its (128 bits o método de <u>ws Vista</u>	de des rá 11).
		Aceptar Cancela	r Apli	car

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:

Q bitlocker	
Codo Aplicaciones Documentos	Web Configuración Carpetas 🕨 … 🧳
Mejor coincidencia	
Administrar BitLocker Panel de control	
Configuración	Administrar BitLocker
Copia de seguridad de la clave de > recuperación	Panel de control
Buscar en Internet	🖸 Abrir
Q bitlocker - Ver más resultados de la > búsqueda	
RitLocker Drive Encryption >	
Q bitlocker desactivar >	
Q bitlocker recovery key >	
Q bitlocker descargar >	
Q bitlocker usb >	
Q bitlocker windows 11 >	
Q Búsqueda	(*)

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

Last update: 2025/04/22 14:49

Ą	Cifrado de unidad Bi	itLocker		- 0		×
¢	\rightarrow \rightarrow \wedge \uparrow	褬 > Panel o	le control > Sistema y seguridad > Cifrado de unidad BitLocker ~ C	Buscar en el Panel de contr	ol ,C	þ
	Ventana principal de control	l Panel de	Cifrado de unidad BitLocker Protege tus archivos y carpetas del acceso no autorizado protegiendo tus unidades con BitLocker.			?
			Unidad de sistema operativo			
			Windows (C:) BitLocker desactivado	^		
			Activar BitLocker			
			Unidades de datos fijas			
			Unidades de datos extraíbles: BitLocker To Go Inserte una unidad flash USB extraíble para usar BitLocker To Go.			
•	Vea también Administración de Ti	PM				
•	Administración de di Declaración de priva	iscos cidad				

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

Comprobando la configuración del equipo

BitLocker está comprobando que el equipo cumpla los requisitos del sistema. Esto puede tardar unos minutos.

¿Cuáles son los requisitos del sistema para BitLocker?

Cancelar

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

 \times

Programa de instalación de Cifrado de unidad BitLocker

Al activar BitLocker, el equipo realiza los siguientes pasos:

Preparar la unidad para BitLocker Cifrar la unidad

¿Cuáles son los requisitos del sistema para BitLocker?

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.

Detalles

Precaución:

A 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.

Siguiente	Cancelar

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

Siguiente

Cancelar

-			-	
•		-4	e	
	۰.	e		
	~	×		

\leftarrow	Rev Cifrado de unidad BitLocker (C:)
	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:
	Preparar la unidad para BitLocker Cifrar la unidad
	<u>¿Cuáles son los requisitos del sistema para BitLocker?</u>

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

Х

Weight and the second state of th

¿Cómo desea realizar la copia de seguridad de la clave de recuperación?

El administrador del sistema administra ciertas configuraciones.

Se puede usar una clave de recuperación para acceder a los archivos y carpetas si tiene problemas para desbloquear su PC. Se recomienda tener más de una y conservarlas en un lugar seguro fuera de su PC.

→ Guardar en la cuenta Microsoft
→ Guardar en un archivo
→ Imprimir la clave de recuperación
Cómo puedo encontrar después mi clave de recuperación?

Siguiente Cancelar

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

🍕 Guardar clave de	recuperación de BitLocker como	>
\leftarrow \rightarrow \checkmark \uparrow	Este equipo > guardaAquiTuClave (F:) > clave	∽ C Buscar en clave ,
Organizar 👻 🛛 N	lueva carpeta	≣ ▾ 💡
🔀 Imágenes	Nombre Fecha de modificación Tipo	Tamaño
🕖 Música	Ningún elemento coincide con el criterio de b	úsqueda.
🔀 Vídeos	*	
 Este equipo Red 		
Nombre:	Clave de recuperación de BitLocker 201E5E8C-E1DE-40B8-B57B-84E8158A36B0	
Tipo:	Archivos de texto (*.bxt)	×
∧ Ocultar carpetas		Guardar Cancelar

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)

O Cifrar la unidad entera (más lento, pero mejor para unidades y PCs que ya se encuentran en uso)

juiente Cancelar	Siguiente	

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.

O 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)

Si	iguiente	Cancelar

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

Х

🔶 🛛 🏘 Cifrado de unidad BitLocker (C:)

¿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.

Continuar	Cancelar

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



c) Usa Veracrypt para crear un contenedor cifrado para el usuario dentro de su perfil

Para crear un contenedor cifrado primero debemos descargar e instalar veracrypt en nuestra máquina con windows 11. Tras eso se procede a abrir veracrypt:

🐱 VeraCrypt			_		\times
Volumes System Favorite	s Tools Settings	Help		Homep	age
Drive Volume A: B: B: G: H: I: J: K: L: M: N: O:		Size Encryption Algorithm	Туре		
<u>C</u> reate Volume	Volume	e Properties	<u>W</u> ipe C	ache	
Volume	nistory	Volume <u>T</u> ools	Select D	Eile Evice	
Mount V	<u>Auto-Mount Devices</u>	Di <u>s</u> mount All		E <u>x</u> it	

Lo primero que se debe hacer es presionar en "Create Volume":

×

VeraCrypt Volume Creation Wizard



VeraCrypt Volume Creation Wizard Create an encrypted file container Creates a virtual encrypted disk within a file. Recommended for inexperienced users. More information Encrypt a non-system partition/drive Encrypts a non-system partition on any internal or external drive (e.g. a flash drive). Optionally, creates a hidden volume. Encrypt the system partition or entire system drive Encrypts the partition/drive where Windows is installed. Anyone who wants to gain access and use the system, read and write files, etc., will need to enter the correct password each time before Windows boots. Optionally, creates a hidden system. More information about system encryption Help < Back Next > Cancel

En la ventana que aparece seleccionamos "Create an encrypted container" y pulsamos en Next:



Seleccionamos Standard VeraCrypt Volume y le damos a next:

. .

🧏 VeraCrypt Volume Creation Wizard



Volume Locat	ion	_		×
	~	Sele	ct File	
Never save history				_
A VeraCrypt volume car on a hard disk, on a USI normal file (it can be, fo File' to choose a filenam the container to be creat WARNING: If you selec deleted and replaced w encrypt existing files (la are about to create now	t reside in a file (called VeraCrypt a flash drive, etc. A VeraCrypt co r example, moved or deleted as a e for the container and to select ated. t an existing file, VeraCrypt will N th the newly created VeraCrypt of ter on) by moving them to the Ve v.	container), v ntainer is jus any normal fil the location v OT encrypt it container. Yo raCrypt cont	which can re it like any le). Click 'Sel where you v t; the file wil u will be abl tainer that y	lect wish I be e to rou
are about to create nov	ν.			
Help	< Back Next	:>	Cance	4

Para almacenar el volúmen seleccionamos la carpeta de nuestro usuario:

🐱 Specify Path and Fi	le Name				×
$\leftarrow \rightarrow \checkmark \uparrow$	> Este equipo > Windows (C:) >	Usuarios > MCBS >	~ C [3uscar en MCBS	م
Organizar 👻 Nu	eva carpeta				≣ • 😗
🕖 Música 🦻	Nombre Favoritos	Fecha de modificación 30/03/2024 20:04	Tipo Tamaño Carpeta de archivos)	
	Imágenes	30/03/2024 20:22 30/03/2024 20:04	Carpeta de archivos Carpeta de archivos		
 Este equipo Red 	 Música OneDrive 	30/03/2024 20:04 30/03/2024 20:07	Carpeta de archivos Carpeta de archivos		
	Vídeos	04/04/2025 16:39 30/03/2024 20:04	Carpeta de archivos Carpeta de archivos		
Nombre: Tipo:	vol.hc All Files (*.*)				~
∧ Ocultar carpetas			(Guardar	Cancelar

Una vez seleccionada la ubicación le damos a next:

×

VeraCrypt Volume Creation Wiza



En la ventana que aparece se puede seleccionar el cifrado que se va a aplicar, una vez seleccionado se pulsa en siguiente:

🧏 VeraCrypt Volume Creation Wizard		-		×
	Volume Size			
VeraCrypt	 KB ● MB ● GB Free space on drive C:\ is 28.19 GiB Please specify the size of the container you want to create. If you create a dynamic (sparse-file) container, this parameter of maximum possible size. Note that the minimum possible size of a FAT volume is 292 KiB. size of an exFAT volume is 424 KiB. The minimum possible size of 3792 KiB. The minimum possible size of an ReFS volume is 642 M 	⊖ TB will specif The minir f an NTFS iiB.	y its num possi S volume i	ible s
	Help < Back Next >		Cancel	

Seleccionaremos el tamaño que va a tener el contanier y pulsaremos en siguiente:

🧏 VeraCrypt Volume Creation Wizard		- 🗆 ×
VeraCrypt	Volume Password: Password: Confirm: Display password Display password Use PIM It is very important that you choose a good password, one that contains only a single word that can be found combination of 2, 3, or 4 such words). It should not cor birth. It should not be easy to guess. A good password upper and lower case letters, numbers, and special chaetc. We recommend choosing a password consisting of longer, the better). The maximum possible length is 128	Keyfiles You should avoid choosing in a dictionary (or a tain any names or dates of is a random combination of racters, such as @ ^ = \$ * + 20 or more characters (the 3 characters.

Ahora estableceremos una contraseña y pulsaremos en siguiente:

 \times

VeraCrypt Volume Creation Wizard



Finalmente se selecciona el tipo de formateo que va a tener el container y se presiona en "Format"

🧏 VeraCrypt Volume Creation Wizard		– 🗆 X
VeraCrypt Volu	Defions Filesystem FAT Cluster Default Random Pool: ,,+,+-//+*,**/ Header Key: ************************************	Full Format
	/eraCrypt volume has been successfully created	d. d.
VeraCrypt	Acepta Randomness Collected From Mouse Movements	r ume.
	Help < Back	Format Cancel

Como resultado se obtiene un nuevo container de veracrypt.

d) Crea una carpeta con el sistema de cifrado EFS

i. Indica como sería el procedimiento

Para realizar un cifrado EFS de una carpeta debemos abrir el CMD como administrador y escribir el siguiente comando:

fsutil behavior set disableencryption 0

```
C:\Users\MCBS\Documents\Nueva carpeta≻fsutil behavior set disableencryption 0
DisableEncryption = 0 (El cifrado está HABILITADO)
Es necesario reiniciar el equipo para aplicar este cambio
```

Otra opción es ir a opciones avanzadas en propiedades de la carpeta y marcar la casilla de cifrar contenido para proteger los datos:

Atribute	tos avanzados	×
 Image: A start of the start of	Elija la configuración deseada para esta carpeta. Si hace clic en Aceptar o Aplicar en el diálogo Propiedades preguntará si desea también aplicar los cambios en todas subcarpetas.	;, se le las
Atribu	utos de índice y archivación	
Ca	arpeta lista para archivarse	
Pe co	ermitir que los archivos de esta carpeta tengan indizado el ontenido además de las propiedades de archivo	
Atribu	utos de compresión y cifrado	
	omprimir contenido para ahorrar espacio en disco	
🔽 Cif	ifrar contenido para proteger datos Detal	les
	Aceptar Can	celar

Como se puede observar la carpeta ahora está cifrada:

2025/04/22 14:51	21/24	[FORT] Práctica 9: Fortil	ficación de la información y auditoría de Windows 11
📒 Nueva carpeta	× +		- 0 X
\leftarrow \rightarrow \wedge C	🏠 > Documentos > 1	Nueva carpeta	Buscar en Nueva carpeta Q
🕀 Nuevo 🗸 🚺		↑↓ Ordenar ~ 🔲 Ver ~ ····	Detalles
 ♠ Inicio ▲ Galería > ▲ OneDrive 			
	oatata		
🔚 Escritorio 🛛 🖈			
🚽 Descargas 🛛 🖈			
📑 Documentos 🖈			
🔀 Imágenes 🛛 🖈			
🕖 Música 🛛 🖈			
🔀 Vídeos 🛛 🖈			
> 📃 Este equipo			
> 🛬 Red			
1 elemento			

ii. ¿Puede habilitar este sistema de cifrado un usuario limitado?

No, es necesario tener permisos de administrador para hacerlo

iii. ¿Podrían acceder varios usuarios al mismo fichero/carpeta compartida y crifrada?¿Cual sería el procedimiento?

Si, pero para ello habría que ir de nuevo a las propiedaddes, de la carpeta, opciones avanzadas y presionar en detalles al lado de la casilla de cifrar la carpeta y en la ventana que sale darle a añadir usuario.

2. Auditoría del sistema

a) ¿Está el sistema de auditoría de windows activado por defecto? ¿Como se puede activar el sistema de auditoría?

Por defecto la auditoría está desactivada, para activarla habría que ir al editor de directivas de grupo local "Configuración del equipo/Configuración de Windows/Configuración de Seguridad/Directivas Locales/Directivas de auditoría":



Aquí habría que activar la auditoría para cada elemento, donde podemos elegir que queremos auditar:



En este caso auditaremos los accesos correctos y erróneos para todo:

2025/04/22 14:51 23/24	[FORT] Práctica 9: Fortificación de la información y auditoría de Windows 11
Directiva	Configuración de seguri
🗓 Auditar el acceso a objetos	Correcto, Erróneo
📓 Auditar el acceso al servicio de directorio	Correcto, Erróneo
📓 Auditar el cambio de directivas	Correcto, Erróneo
📖 Auditar el seguimiento de procesos	Correcto, Erróneo
🔯 Auditar el uso de privilegios	Correcto, Erróneo
Auditar eventos de inicio de sesión	Correcto, Erróneo
📖 Auditar eventos de inicio de sesión de cuenta	Correcto, Erróneo
🔯 Auditar eventos del sistema	Correcto, Erróneo
Auditar la administración de cuentas	Correcto, Erróneo

b) ¿Qué categorías podemos auditar en un sistema operativo Windows 11?

Como se puede observar en la anterior captura de pantalla se pueden auditar las siguientes categorías:

- Acceso a objetos
- Acceso al servicio de directorio

- Cambio de directivas
- Seguimiento de procesos
- uso de privilegios
- Eventos de inicio de sesión
- Eventos de inicio de sesión de cuenta
- Eventos del sistema
- Administración de cuentas

c) ¿Sobre que tipo de objetos podemos aplicar una auditoría de Windows 11?

Se puede aplicar una auditoría de windows a los siguientes obejtos:

- Archivos
- Carpetas
- Servicios

d) ¿Como podemos observar los resultados de una auditoría?

Podemos observarlos desde el Visor de eventos yendo a "Registros de Windows/Seguridad":

Archivo Acción Ver Ayuda	
Visor de eventos (local) Seguridad Número de eventos: 23.071 (!) Nuevos eventos disponibles Signa Sersonalizadas	
V 🕆 Registros de Windows Palabras clave Fecha y hora Origen Id. del evento Categoría de la tarea	
Aplicación 4673 Sensitive Privilege Use	
😰 Seguridad 🛛 🔒 Error de auditoría 22/04/2025 16:48:32 Microsoft Windows secu 4673 Sensitive Privilege Use	
📄 Instalación 🔰 Error de auditoría 22/04/2025 16:48:32 Microsoft Windows secu 4673 Sensitive Privilege Use	
🙀 Sistema 🛛 🔒 Error de auditoría 22/04/2025 16:48:32 Microsoft Windows secu 4673 Sensitive Privilege Use	
Eventos reenviados 🛛 🔒 Error de auditoría 22/04/2025 16:48:32 Microsoft Windows secu 4673 Sensitive Privilege Use	
> 📴 Registros de aplicaciones y s 🔒 Error de auditoría 22/04/2025 16:48:32 Microsoft Windows secu 4673 Sensitive Privilege Use	
🔝 Suscripciones 🛛 🔒 Error de auditoría 22/04/2025 16:48:32 Microsoft Windows secu 4673 Sensitive Privilege Use	
Arror de auditoría 22/04/2025 16:48:32 Microsoft Windows secu 4673 Sensitive Privilege Use	
Auditoría correcta 22/04/2025 16:48:26 Microsoft Windows secu 5158 Filtering Platform Connec	
Auditoría correcta 22/04/2025 16:48:26 Microsoft Windows secu 5158 Filtering Platform Connec	
Auditoría correcta 22/04/2025 16:48:26 Microsoft Windows secu 4689 Process Termination	
🔒 Error de auditoría 22/04/2025 16:48:26 Microsoft Windows secu 4673 Sensitive Privilege Use	
Auditoría correcta 22/04/2025 16:48:26 Microsoft Windows secu 4688 Process Creation	
Auditoría correcta 22/04/2025 16:48:26 Microsoft Windows secu 4670 Authorization Policy Cha	
Auditoría correcta 22/04/2025 16:48:26 Microsoft Windows secu 4670 Authorization Policy Cha	
🔒 Error de auditoría 22/04/2025 16:48:24 Microsoft Windows secu 4673 Sensitive Privilege Use	
🔒 Error de auditoría 22/04/2025 16:48:24 Microsoft Windows secu 4673 Sensitive Privilege Use	
Berror de auditoría 22/04/2025 16:48:24 Microsoft Windows secu 4673 Sensitive Privilege Use	
General Barror de auditoría 22/04/2025 16:48:24 Microsoft Windows secu 4673 Sensitive Privilege Use	
General Barror de auditoría 22/04/2025 16:48:24 Microsoft Windows secu 4673 Sensitive Privilege Use	
🔒 Error de auditoría 22/04/2025 16:48:24 Microsoft Windows secu 4673 Sensitive Privilege Use	
🔒 Error de auditoría 22/04/2025 16:48:24 Microsoft Windows secu 4673 Sensitive Privilege Use	
🖬 🔒 Error de auditoría 22/04/2025 16:48:24 Microsoft Windows secu 4673 Sensitive Privilege Use	
Error de auditoría 22/04/2025 16:48:20 Microsoft Windows secu 4673 Sensitive Privilege Use	
Evento 4673, Microsoft Windows security auditing.	×

General Detailer

From: https://knoppia.net/ - **Knoppia**

Permanent link: https://knoppia.net/doku.php?id=master_cs:fortificacion:p9



Last update: 2025/04/22 14:49