





Guía de Seguridad

Fecha de publicación: 04/08/2022

Tema: Guía de Controles y Prácticas de Seguridad en Dispositivos Extraíbles. **Objetivo**: Proveer una guía de prácticas para prevenir incidentes de seguridad relacionados con el uso indebido de dispositivos de almacenamiento extraíble.

Índice

Escenario 1 - Una organización que no tenga un controlador de dominio, ni antivirus	
corporativo	2
Bloquear el acceso del puerto USB:	2
Deshabilitar ejecución automática (autorun):	8
Cifrado de dispositivos:	. 11
Implementar una protección de antivirus:	. 20
Escenario 2 - Una organización mediana con un nivel de madurez medio, que cuenta c controlador de dominio y un antivirus centralizado.	on . 21
Deshabilitar USB a través de política de GPO:	. 21









Escenario 1 - Una organización que no tenga un controlador de dominio, ni antivirus corporativo.

Algunas buenas prácticas que pueden ejecutarse para este escenario son:

- Bloquear el acceso del puerto USB.
- Deshabilitar ejecución automática (autorun).
- Cifrado de dispositivo.
- Implementar una protección de antivirus.
- Implementar un controlador dominio:

Bloquear el acceso del puerto USB:

Se puede hacer esto bloqueando físicamente el acceso al puerto USB o deshabilitando los adaptadores USB a través del sistema operativo. Sin embargo, es probable que esta no sea una solución viable, ya que muchos teclados, mouse, impresoras y otros periféricos requieren acceso al puerto USB.

Para sistema operativo Microsoft Windows:

NOTA: Para realizar los siguientes pasos es necesario utilizar una cuenta con privilegios de administración.

Microsoft Windows puede evitar que los usuarios conecten dispositivos de almacenamiento extraíble USB a un sistema cambiando los permisos de acceso a los archivos de sistema **Usbtor.pnf** y **Usbtor.inf** Esto evitará que los usuarios instalen nuevos dispositivos de almacenamiento USB en los sistemas afectados. Para automatizar el proceso, puede implementar la directiva a través de un GPO de Windows:









1. Dispositivo de almacenamiento USB aún no está instalado en el equipo:

Si un dispositivo de almacenamiento USB aún no está instalado en el equipo, asigne al usuario o al grupo y a la cuenta **SYSTEM local** la propiedad *"Denegar permisos"* a los siguientes archivos:

- %SystemRoot%\Inf\Usbstor.pnf
- %SystemRoot%\Inf\Usbstor.inf

Al hacerlo, los usuarios no podrán instalar un dispositivo de almacenamiento USB en el equipo. Para asignar a un usuario o grupo denegar permisos a los archivos **Usbstor.pnf** y **Usbstor.inf**, siga estos pasos:

- a) Iniciar el Explorador de Windows y a continuación, buscar la carpeta **%SystemRoot%\Inf**.
- b) Hacer clic con el botón secundario en el archivo **Usbstor.pnf** y, a continuación, hacer clic en **Propiedades**.
- c) Hacer clic en la ficha **Seguridad**.
- d) En la lista **Nombres de grupo**, agregar el usuario o grupo para el que desee establecer permisos de denegación.
- e) En la lista **Permisos para Nombre de usuario**, hacer clic para activar la casilla de verificación **Denegar** situada junto a Control total.
- f) Agregar la cuenta del sistema a la lista **Denegar**.
- g) En la lista Nombres de usuario, seleccionar la cuenta SYSTEM.
- h) En la lista **Permisos para Nombre de usuario**, hacer clic para activar la casilla de verificación **Denegar** junto a **Control total** y, a continuación, **Aceptar**.
- i) Hacer clic con el botón secundario en el archivo **Usbstor.inf** y, a continuación, hacer clic en **Propiedades**.
- j) Hacer clic en la ficha Seguridad.









- k) En la lista **Nombres de usuario**, agregar el usuario o grupo para el que desee establecer permisos de denegación.
- I) En la lista **Permisos para Nombre de usuario**, hacer clic para activar la casilla de verificación **Denegar** situado junto a **Control total**.
- m) En la lista Nombres de usuario, seleccione la cuenta SYSTEM.
- n) En la lista **Permisos para Nombre de usuario**, hacer clic para activar la casilla de verificación **Denegar** junto a **Control total** y, a continuación, **Aceptar**.

Nota: Para obtener más información consulte el enlace

2. Dispositivo de almacenamiento USB que ha sido instalado en el equipo:

Si un dispositivo de almacenamiento USB ya ha sido instalado en el equipo e utilizado, se puede cambiar el **Registro** para asegurarse de que el dispositivo no funcione cuando el usuario se conecte al equipo.

Resolución Importante, este método o tarea contiene pasos que indica cómo modificar el **Registro**. Debe seguir estos pasos cuidadosamente para evitar algún inconveniente. Antes de realizar este método, se recomienda realizar una <u>copia de seguridad y restaurar</u> del **Registro en Windows**.

Secuencialmente, establecer el valor Inicio en la siguiente clave del Registro en "4":

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\UsbStor Al hacerlo, el dispositivo de almacenamiento USB no funciona cuando el usuario conecta el dispositivo al equipo. Para establecer el valor **Start**, siga estos pasos:

- a) Hacer clic en Inicio y, a continuación, Hacer clic en Ejecutar.
- b) En el cuadro Abrir, escribir regedit y, a continuación, Aceptar.
- c) Buscar y, hacer clic en la siguiente clave del Registro:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\UsbStor









- d) En el panel de detalles, Hacer doble clic en Inicio.
- e) En el cuadro **Información del valor**, escribir 4, Hacer clic en **Hexadecimal** (si aún no está seleccionado) y, a continuación, **Aceptar**.
- f) Salir del Editor del Registro.

Para sistema operativo Linux

NOTA: Para realizar los siguientes pasos es necesario utilizar una cuenta con privilegios de administración.

1. Comprobar si el controlador del dispositivo USB está presente en el Kernel de Linux

Para deshabilitar el soporte de medios USB en el servidor, en primer lugar, será necesario identificar si el controlador de almacenamiento está cargado en el Kernel de la distribución y validar el nombre del controlador responsable de este medio de almacenamiento. El siguiente tutorial está basado en distribuciones Linux basadas en Debian/Ubuntu.

Se deberá de tener en cuenta los siguientes pasos:

Paso 1. Ejecutar el comando "Ismod", ya que, se podrá validar que el módulo "usb_storage" está en uso por el módulo UAS.

lsmod | grep usb_storage



Fuente: https://www.solvetic.com/tutoriales/article/4801-bloquear-dispositivos-usb-con-comando-chmod-linux/









Paso 2. Descargar ambos módulos de almacenamiento USB del Kernel y verificar si el proceso de eliminación ha sido completado con éxito, para esto se debería de ejecutar los siguientes comandos:



2. Editar las políticas en Linux

Paso 1. Enumerar el contenido que hay en el directorio de módulos de almacenamiento USB del kernel o núcleo actual haciendo uso del siguiente comando:

ls /lib/modules/`uname -r`/kernel/drivers/usb/storage/

Paso 2. Identificar el nombre del controlador de almacenamiento USB el cual en la mayoría de los casos tiene el siguiente formato:











Paso 3. Para bloquear el módulo de almacenamiento de USB en el Kernel, será necesario cambiar la ruta de los módulos de almacenamiento USB del directorio al Kernel y luego renombrar el módulo usb-storage.ko.xz a usb-storage.ko.xz.blacklist o bien usb-storage.ko a usb-storage.ko.blacklist , usando los siguientes comandos:

cd /lib/modules/`uname -r`/kernel/drivers/usb/storage/
ls
sudo mv usb-storage.ko usb-storage.ko.blacklist
<pre>solvetic@solvetic-Ubuntu: /lib/modules/4.10.0-42-generic/kernel/drivers/usb/storage solvetic@solvetic-Ubuntu:~\$ cd /lib/modules/`uname -r`/kernel/drivers/usb/storage/ solvetic@solvetic-Ubuntu:/lib/modules/4.10.0-42-generic/kernel/drivers/usb/stora ge\$ ls uas.ko ums-eneub6250.ko ums-karma.ko ums-sddr55.ko ums-alauda.ko ums-freecom.ko ums-onetouch.ko ums-usbat.ko ums-cypress.ko ums-isd200.ko ums-realtek.ko usb-storage.ko ums-datafab.ko ums-jumpshot.ko ums-sddr09.ko solvetic@solvetic-Ubuntu:/lib/modules/4.10.0-42-generic/kernel/drivers/usb/stora ge\$ sudo mv usb-storage.ko usb-storage.ko.blacklist solvetic@solvetic-Ubuntu:/lib/modules/4.10.0-42-generic/kernel/drivers/usb/stora ge\$</pre>

Fuente: https://www.solvetic.com/tutoriales/article/4801-bloquear-dispositivos-usb-con-comando-chmod-linux/

Paso 4. En el caso de Debian debemos ejecutar los siguientes comandos para el bloqueo del módulo de almacenamiento USB:

```
cd /lib/modules/`uname -r`/kernel/drivers/usb/storage/
ls
sudo mv usb-storage.ko usb-storage.ko.blacklist
```

De este modo, cuando se conecte cualquier medio USB al equipo, el kernel no podrá cargar el módulo respectivo de entrada de controlador para el dispositivo de almacenamiento.

Paso 5. En el momento de revertir los cambios basta con renombrar el dispositivo a su nombre original ejecutando lo siguiente:

cd /lib/modules/`uname -r`/kernel/drivers/usb/storage/









mv usb-storage.ko.blacklist usb-storage.ko

3. Bloquear dispositivos USB con chmod en Linux

Otro método sencillo para lograr el bloqueo de los dispositivos USB en Linux, sabiendo que cada USB se monta en /media/ o si la distribución usa **systemd**, se montará en /run/media/, por ello, debemos editar los permisos de estas rutas para que solo el usuario root tenga el acceso y nadie más, para ello ejecutaremos lo siguiente:

```
sudo chmod 700 /media/
```

O en su caso:

```
sudo chmod 700 /run/media/
```

Con este método, la unidad si será montada, pero no será desplegada ninguna notificación al usuario, ni podrá acceder directamente al contenido de esta, solo el usuario root.

colvetic@Solvetic=Ubuntu:~\$ sud sudo] password for solvetic: colvetic@Solvetic=Ubuntu:~\$	lo chmod 700	/media/		

Fuente: https://www.solvetic.com/tutoriales/article/4801-bloquear-dispositivos-usb-con-comando-chmod-linux/

Deshabilitar ejecución automática (autorun):

Para sistema operativo Microsoft Windows

NOTA: Para realizar los siguientes pasos es necesario utilizar una cuenta con privilegios de administración.

Si desea detener la ejecución automática USB en Microsoft Windows 10 o simplemente desactivar AutoRun CD, seguir estos pasos:

A. Detener AutoRun en Windows 10 mediante el Editor del Registro:

- 1. En Buscar escribir regedit y abrir el comando Editor del Registro.
 - Ir a la siguiente tecla:









${\sf HKEY_CURRENT_USERS of tware Microsoft Windows Current Version Policies Exp}$



- 2. En el panel derecho de la ventana crear un nuevo valor DWORD **NoDriveTypeAutorun** y establecer su valor en algunos de los siguientes:
 - FF Desactivar AutoRun en todas las unidades.
 - 20 Desactivar AutoRun en unidades de CD-ROM.
 - 4 Desactivar AutoRun en unidades extraíbles.
 - 8 Desactivar AutoRun en unidades fijas.
 - 10 Desactivar AutoRun en unidades de red.
 - 40 Desactivar AutoRun en discos RAM.
 - 1 Desactivar AutoRun en unidades desconocidas.
- Para desactivar el AutoRun en una determinada combinación de unidades, tendrá que combinar sus valores. Por ejemplo, en CD-ROM y unidades extraíbles, establezca el valor de DWORD en 28.
- 4. Para devolver la funcionalidad AutoRun, se debe eliminar el valor **NoDriveTypeAutorun** DWORD.









B. Deshabilitar AutoRun usando la directiva de grupo:

Aquí están los pasos a seguir:

- 1. Ir a **Inicio**> escribir **gpedit.msc**> hacer doble clic en el primer resultado para iniciar la directiva de grupo.
- 2. Ir a Configuración del equipo> seleccionar Plantillas administrativas> ir a Componentes de Windows.



3. Seleccionar **Políticas de reproducción automática**> navegar hasta el panel de detalles:

Local Group Policy Editor			– 🗆 X
File Action View Help			
🗢 🔿 🙍 🗔 🗟 🖬 🛛 🌱			
Application Compatibility	AutoPlay Policies		
AutoPlay Policies Biometrics	Turn off Autoplay		Setting
BitLocker Drive Encryption	Edit policy setting	^	Turn off Autoplay
Cloud Content	Requirements:		Disallow Autoplay for non-volume devices
Connect	At least Windows 2000		Set the default behavior for AutoRun
Data Collection and Preview Bui Delivery Ontimization	This policy setting allows you to		
Desktop Gadgets	turn off the Autoplay feature.		
> Desktop Window Manager Device and Driver Compatibility	Autoplay begins reading from a drive as soon as you insert		
Device Registration	media in the drive. As a result, the setup file of programs and the		
Edge Ul	music on audio media start immediately.		

4. Hacer doble clic en **Desactivar** la reproducción automática para desactivar la función.









Para sistema operativo Linux

NOTA: Para realizar los siguientes pasos es necesario utilizar una cuenta con privilegios de administración.

Para deshabilitar la ejecución automática en Ubuntu Linux, siga estos pasos:

- 1. Ejecutar "gconf-editor" desde la terminal.
- 2. Abrir /aplicaciones/nautilus/preferencias.
- 3. Buscar "media_automount_open" y desmárquelo.
- 4. También puede marcar "media_autorun_never".
- 5. Cerrar gconf-editor.



Cifrado de dispositivos:

El cifrado ayuda a proteger los datos en tu dispositivo para que solo puedan acceder a ellos personas con autorización.

Para sistema operativo Windows

Si el cifrado no está disponible en tu dispositivo, probablemente puedas activar el cifrado de BitLocker estándar en su lugar. (Tenga en cuenta que BitLocker no está disponible en la edición de Windows 10 Home).









- Iniciar sesión en Windows con una cuenta de administrador (puede que deba cerrar sesión y volver a iniciarla para cambiar de cuenta). Para obtener más información, consulte Crear una cuenta local en Windows.
- 2) Seleccionar botón de Inicio, y seleccionar Configuración > Actualización y seguridad > Cifrado del dispositivo. Si Cifrado del dispositivo no aparece, entonces no está disponible. Probablemente podría utilizar el cifrado de BitLocker estándar en su lugar. Abrir Cifrado de dispositivo en Configuración.
- 3) Si el cifrado del dispositivo se encuentra desactivado, seleccionar Activar.
- 4) Activar el cifrado del dispositivo de BitLocker estándar.
- 5) Iniciar sesión en el dispositivo Windows con una cuenta de administrador.
- 6) En el cuadro de búsqueda de la barra de tareas, escribir Administrar BitLocker y después selecciónalo en la lista de resultados. O bien, seleccione el botón Inicio y, a continuación, en Sistema de Windows, seleccionar Panel de control. En Panel de control, seleccionar Sistema y seguridad, a continuación, en Cifrado de unidad BitLocker, seleccionar Administrar BitLocker.
- 7) Seleccionar Activar BitLocker y a continuación, seguir las instrucciones:



a) Tras seleccionar Activar BitLocker se iniciará un asistente que primero analizará la unidad para ver si es compatible, y acto seguido preguntará por el método de cifrado que se desee utilizar. En este caso lo más normal es utilizar una protección mediante contraseña, así que se deberá seleccionar esta opción e introducir la contraseña que dos veces.







🙀 Cifrado de unidad BitLocker	r (D:)
Elija cómo desea desblo	oquear la unidad
🗹 Usar una contraseña para de	esbloquear la unidad
Las contraseñas deben conte	ener mayúsculas y minúsculas, números, espacios y símbolos.
Escribir la contraseña	••••••
Vuelva a escribir la contrase	eña
🗌 Usar la tarjeta inteligente pa	ra desbloquear la unidad
Deberá insertar la tarjeta inte unidad.	eligente. El PIN de la tarjeta inteligente será necesario cuando desbloquee

 b) Tras pulsar en siguiente, preguntará como se desea realizar una copia de seguridad de la clave de recuperación. La recomendación es imprimirla y guardarla en un lugar seguro, pero también se puede guardar en la cuenta de Microsoft o en un archivo TXT. Tras hacer la opción deseada, pulsar siguiente para continuar.

	×
÷	🙀 Cifrado de unidad BitLocker (D:)
	¿Cómo desea realizar la copia de seguridad de la clave de recuperación?
	 Se guardó la clave de recuperación.
	Si olvida la contraseña o pierde la tarjeta inteligente, puede usar la clave de recuperación para acceder a la unidad.
	→ Guardar en la cuenta Microsoft
	ightarrow Guardar en un archivo
	→ Imprimir la clave de recuperación
	¿Cômo puedo encontrar después mi clave de recuperación?
	Siguiente Cancelar

c) El asistente preguntará la cantidad de la unidad que se desea cifrar, pudiendo escoger entre cifrar solo el espacio ocupado o cifrar la unidad entera. Cifrar solo el espacio ocupado es más rápido inicialmente, pero luego tardará más cuando se quiera hacer modificaciones a la unidad, es por eso por lo que, se recomienda cifrar la unidad entera.







Floring work associated also be considered also as alterna
Elegir que cantidad de la unidad desea cirrar
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)

d) Preguntará por el modo de cifrado. El modo de cifrado nuevo requiere cierta versión de Windows (es XTS-AES), la misma es recomendable en caso de un posible uso de ese pendrive USB en ese ordenador, es recomendable utilizar el modo compatible, en caso de reutilizar/llevar el pendrive USB en cualquier parte.

	×
Reference Cifrado de unidad BitLocker (D:)	
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 151 o versiones posteriores, elige el nuevo modo de cifrado.	1)
⊖ 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)	
Siguiente Cancela	
	 Cifrado de unidad BitLocker (D:) 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 es trata de una unidad extrable 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)

e) Tras pulsar sobre **Iniciar cifrado**, comenzará el proceso, que llevará unos minutos dependiendo de la capacidad de la unidad.











Una vez concluido el proceso, cada vez que el pendrive es introducido a un PC, éste pedirá la contraseña para acceder a él. En caso de querer desactivar Bitlocker para dejar la unidad sin proteger, se deberá pulsar nuevamente sobre Bitlocker en el menú del principio, seleccionar «Administrar BitLocker» y luego «Descifrar unidad».

Para sistema operativo Linux

NOTA: Para realizar los siguientes pasos es necesario utilizar una cuenta con privilegios de administración.

Los pasos a tener en cuenta para realizar esta tarea son:

1. Instalar Gnome Disks y herramientas de cifrados

La aplicación Gnome Disks hace que el bloqueo de una unidad USB externa sea más sencillo. Si se utiliza un entorno de escritorio Linux basado en Gnome, es muy probable que deba ser instalado la aplicación Gnome Disks. Sin embargo, muy posiblemente debe configurarlo antes de usarlo.

• Abrir una ventana de terminal para instalar Gnome.











2. Cifrar unidad USB

Iniciar la aplicación Gnome Disks en el ordenador Linux. Posteriormente, conectar la unidad USB que se desea cifrar. Una vez conectado al sistema, localizarlo en la barra lateral de la izquierda y hacer clic en él.

	15	GB Thumb Drive /dev/sdb	Ċ	≡	•	• 6
1.0 TB Hard Disk HGST HTS541010A9E680 15 GB Thumb Drive Kingston DataTraveler 3.0	Model Size Partitioning Serial Number	Kingston DataTraveler 3.0 (0001) 15 GB (15,47,20,47,104 bytes) Master Boot Record				
	Volumes	000000000000000000000000000000000000000				
		USB Partition 1 15 GB MP				
		P				
	Size	15 GB — 15 GB free (0.1% full)				
	Device	/dev/sdb1 CECD-8EB9				
	Partition Type	W95 FAT32 (LBA) (Bootable)				
	Contents	FAT (32-bit version) — Mounted	at /media/root	<u>/USB</u>		

Fuente https://esgeeks.com/proteger-cifrar-usb-linux/

- Una vez cargado la unidad USB en discos Gnome, proceder a formatear el dispositivo en un sistema de archivos Linux (ext3, ext4). Para formatear, hacer clic en el botón de menú. Luego, en el menú, seleccionar la opción "Format Disk".
- Al hacer clic en "Format Disk" aparecerá un menú. En este menú, hay dos opciones. Estas opciones son "Erase" y "y". Establezca la primera opción en "Quick" y la segunda opción en "MBR / DOS".







	Forma	t Disk	0
Erase	Don't overwrite existing o	lata (Quick)	•
Partitioning	Compatible with all syste	ms and devices (MBR / [DOS) -
		Cancel	Format

Fuente https://esgeeks.com/proteger-cifrar-usb-linux/

• Permitir que la unidad formatee y borre todos los datos.

All data on the disk will be lost recovery services	but may still be recoverable by data
Tip: If you are planning to recy or disk, you should use a more information from falling into the	cle, sell or give away your old computer thorough erase type to keep your private e wrong hands
Affected Devices	
15 GB Thumb Drive — King	gston DataTraveler 3.0 [0001] (/dev/sdb)

Fuente https://esgeeks.com/proteger-cifrar-usb-linux/

 Al finalizar el formateo, hacer clic en el botón "+", configurar la opción "Type" en "Encrypted, compatible with Linux systems" o "".









revious	Format Volume	Next
Volume Name	EsGeeks	
	For example: "Angela's Files" or "Backup".	
Erase	∞−	
	Overwrites existing data, but takes longer.	
Туре	Internal disk for use with Linux systems only (Ext ²	1)
	Password protect volume (LUKS)	
	O For use with Windows (NTFS)	
	O For use with all systems and devices (FAT)	
	Other	

Fuente https://esgeeks.com/proteger-cifrar-usb-linux/

 Utilizando el menú del sistema de archivos, configurar la unidad USB con un código de acceso (cifrado por contraseña). Luego, hacer clic en el botón "Create" para finalizar el proceso de cifrado.

Previous	Set Password Cre		
Data stored in Be careful not	the volume will only be accessible with the correct pas to forget it.	sword.	
Passwor	desgeeks		
	Mix uppercase and lowercase and try to use a number or t	Veak two.	
Confirm	n esgeeks		
	Show Password		
	E Show Fassword		









	15 GB Thumb Drive	Ċ	=	0	Θ	0
10 TB Hard Disk HGST HTS541010A9E680 15 GB Thumb Drive Kingstan DataTraveler 3.0	Model Kingston DataTraveler 3.0 (0001) Size 15 GB (15,47,20,47,104 bytes) Partitioning Master Boot Record Serial Number 60A44C42539CF280571C6586 Volumes					
	Parties 1 15-06 LINS					
	EsGeeks 33 GB Ext4					
	Size 15 GB (15.47.06.90.304 bytes)					
	Device /dev/sdc1 UUID 1115e273-ce5c-420e-9c3b-1a1a87e	a310e				
	Partition Type Oxe8 Contents LUKS Encryption (version 1) — Unloc	ked				

USB cifrado mediante Gnome Disk

Fuente https://esgeeks.com/proteger-cifrar-usb-linux/

3. Comprobar USB cifrado

• Una vez cifrada, acceder a la unidad USB. Si se desea colocar archivos en él, primero se deberá montar en el sistema. Para montar la unidad, conectarlo al puerto USB e iniciar el administrador de archivos.



Fuente https://esgeeks.com/proteger-cifrar-usb-linux/









• En el administrador de archivos, buscar la unidad en la lista de dispositivos del lado izquierdo. Hacer doble clic en la unidad e ingresar la contraseña para acceder a la unidad USB cifrada.

< > I C EsGeeks	
습 Home	
🖀 Desktop	
Descargas	
Documentos	
🖆 Imágenes	
🎵 Música	
E Vídeos	Folder is Empty
🗑 Trash	
🔇 EsGeeks 🛛 🛆	
+ Other Locations	

Fuente https://esgeeks.com/proteger-cifrar-usb-linux/

Una vez que se haya obtenido el acceso a la unidad USB cifrada, esta funcionará como cualquier otro dispositivo en Linux. Para poner archivos en él, simplemente se podrá arrastrar a la carpeta.

Implementar una protección de antivirus:

Instalar y mantener actualizado un software antivirus. La instalación de software antivirus de un proveedor de confianza es un paso importante para prevenir y detectar infecciones.

A continuación, citamos una lista de los antivirus gratuitos (versión free) más usados y conocidos del mercado:

- Total AV
- Panda
- PcProtect
- Avira
- McAfee
- Norton
- ScanGuard
- BullGuard
- Kaspersky
- Avast









- Bitdefender
- AVG

A continuación, citamos una lista de los antivirus corporativos más usados y conocidos del mercado:

- Kaspersky
- Avast Business
- Intego
- Panda Endpoint Protection Plus
- BullGuard Premium Protection
- ESET Endpoint Antivirus
- AVG Business
- Bitdefender GravityZone Business Security
- Norton Small Business
- McAfee Security for Business
- Windows Defender (Azure)
- Avira Protection Cloud
- Acronis Cyber Protect
- Malwarebytes for Teams
- Vipre Core Defense

Escenario 2 - Una organización mediana con un nivel de

madurez medio, que cuenta con controlador de dominio y

un antivirus centralizado.

Algunas buenas prácticas que pueden ejecutarse para este escenario son:

- Deshabilitar USB a través de política de GPO.
- Deshabilitar ejecución automática por GPO.
- Deshabilitar escritura en USB extraíble.

Deshabilitar USB a través de política de GPO:

Para sistema operativo Windows

NOTA: Para realizar los siguientes pasos es necesario utilizar una cuenta con privilegios de administración dentro del dominio Microsoft Windows de la organización.









Crear una nueva unidad organizativa en nuestro árbol de Active Directory.

 Mover todos aquellos equipos cliente a los debemos bloquear la posibilidad de poder usar dispositivos de disco USB.



- 2. Abrir una nueva ventana del **Administrador** de directivas de Grupo, allí se localizará un acceso directo dentro de las **Herramientas Administrativas**.
- 3. Acceder al menú **Inicio de Windows** y, seguidamente, en el cuadro de texto llamado Ejecutar escribir gpmc.msc. Después, hacer clic en botón **Aceptar**.
- 4. Abrir una nueva ventana del Administrador de directivas de Grupo. En el árbol lateral izquierdo de la consola, desplegar la rama llamada **Objetos de directiva de grupo**.
- 5. Seleccionar con el botón derecho del ratón la rama **Objetos de directiva de grupo** y, en el menú desplegable, seleccionar la opción llamada Nuevo.
- 6. Aparecerá una nueva ventana emergente llamada Nuevo GPO, en ella, asignar un nombre descriptivo a la nueva GPO y dejar la selección GPO inicio de origen en ninguno, luego **Aceptar**.







	Admin	istración de directivas de grup	00		- a X
🚊 Archive Acción Ver Vertana Ayuda					- 0
++ 2 m 0 8 0 m					
Administración de directivas de grupo a Á Bosque: DOMLOCAL	Objetos de directiva de Contenido Delegación	grupo en DOM.LOCAL			
Contract Contract CAL Contract CA	Indexes Control Donain Failing Graduit Donain Failing Graduit H05 preva preva	Estado de GPO Hobilitado Hobilitado Hobilitado Hobilitado Hobilitado	Films WMI Ninguns Ninguns Ninguns Ninguns Ninguns	Modificado 10/54/2017 11:80-60 10/54/2017 11:40-40 10/54/2017 11:20-56 11/54/2017 12:20-56 11/54/2017 12:20-50	Propietailo Admas del domino (DOM - Admas del domino (DOM - Admas del domino (DOM - Admas del domino (DOM - Admas del domino (DOM -
	Administrar copies Administrar copies Ver Nuero vertiana desde aquí Actualizar	3	Nuevo GPO	×	
Resultados de directivas de grupo	1	CPO-BLOQUED-USB	4		
h and separation of suscission in factors		GPD de ance de orgen: (avejuro)	5 Acaptar	Genosia	
Muestra la Ayuda para la valención actual.					1

- 7. Una vez creada la nueva GPO, seleccionarla y, en la división derecha de la ventana del Administrador de directivas de Grupo, seleccionar la sección llamada Configuración.
- 8. Comprobar las configuraciones, para ello, se deberá situar el cursor en la parte blanca de la división derecha de la ventana y con el botón derecho del ratón y desplegar el menú para finalmente seleccionar la opción llamada **Edición**.
- Aparecerá una nueva ventana emergente llamada Editor de Administración de directivas de Grupo, en el árbol lateral izquierdo de esta nueva ventana se desplegará la rama:

Configuración del equipo\Directivas\Plantillas Administrativas: definiciones de directiva\Sistema\Acceso de almacenamiento extraíble

- 10. Dentro de la rama llamada Acceso de almacenamiento extraíble se debe buscar la plantilla administrativa llamada Todas las clases de almacenamiento extraible: **denegar acceso a Todo**.
- 11. Editarla y habilitarla. Hecho esto, guardar los cambios realizados sobre la plantilla.











- 12. Vincular la nueva GPO a la unidad organizativa creado en los primeros pasos.
- 13. En lateral izquierdo de la consola del Administrador de directivas de Grupo desplegar la rama del dominio. Con el botón derecho del ratón, seleccionarla unidad organizativa para desplegar el menú, para luego, seleccionar la opción del nuevo menú **Ilamada Vincular un GPO existente**.
- 14. Aparecerá una pequeña ventana llamada **Seleccionar GPO**, en el menú seleccionar la GPO de bloqueo de dispositivos USB y guardar los cambios.







<u>a</u>			Administración d	le directivas d	le grupo		
Archivo Acción Ver Ve	entana Ayuda						1.16
🕈 🏟 🙇 📷 🛍 🕷							
Administración de desctives de grupe		GPO-BLOQUE	O-USB				
A Bosque: DOMIDCAL		Anbtu Detalies	Configuración Delega	ción Estado			
A DOMLOCAL		GPO-BLO	QUEO-USB				
Default Domai	n Policy	Datios recepted	us el. 27/05/2017 17:27	12			mostrar todo
) Domain Col	Crear un GPO en este dom	inio y vincularlo aquí					and a
) 🏩 Servidores-	Yincular un GPO existente.		strativas				roles.
Default	Bloquear herencia		nes de directiva (a	ethives ADMO(res	ouperadas del equipo local		
Default	Actualización de delectiva	de grupo	como de almaco	numiento estra	ible		state
GPO-BL	Asistente para modelado d	le directivas de grupo.			Configuración	Consertario	
_ hears	Nurva Unidad organizativa		1	enamiento ostralibi	r hubiltado		
i si no?	Charles Ventaria desde aqui						and the
GPD de inic	Cambia: nombre		poinno defesda				COSE
i Stice	Actualizar						
p 10 Resultados de direct	Propiedades				Selections	(20) X	
	Ayuda						
12				Buscar en e	este dominio (
A sector in Association in anti-				DOM	ALOCAL	*	
миела и луши рака и хессой	t actual.			Citrartos de	directiva da grupo:		
				Non	rtse *		
				Def	ault Domain Controllers Policy ault Domain Policy		
					HLOQUIO-LISI	4	
				GPC	SHB-U-RDS		
				10	ař:		
				100			
						5 Aceptar Carcelar	

15. La nueva directiva impedirá que los usuarios tengan acceso a los dispositivos de disco que conecten a sus conexiones USB locales.

** * 2 m × a 8 m		1.1.1.1
Administratica de direction de grupo Administratica de direction de grupo BOMLOCA DOMLOCA DOMLOCA	BPO-IIL COULID-USB Anton:	
	Apropr. Dutor freesendor Februado WMI Ente GPC unit versited al againers life WMI emigranco	×

Deshabilitar ejecución automática por GPO:

1. Abrir la herramienta de administración de políticas de grupo.









2. Crear una nueva política de grupo.



3. Ingresar un nombre para la nueva política de grupo.

	New GPO	x
<u>N</u> ame:		
MY-GP0		
Source Starter GPO:		
-anormonas		_









4. En la pantalla Administración de directivas de grupo, expandir la carpeta denominada Objetos de directiva de grupo. Hacer clic con el botón derecho en su nuevo objeto de política de grupo y seleccionar la opción **Editar**.



5. Editar de directivas de grupo, expandir la carpeta Configuración del equipo y localizar el siguiente elemento.

Computer Configuration > Administrative Templates > Windows Components > Autoplay Policies

6. Acceder a la carpeta de configuración de políticas de reproducción automática.











- 7. Acceder y habilitar la opción llamada Desactivar reproducción automática.
- 8. Seleccionar la opción para desactivar la reproducción automática en todas las unidades.



- 9. Acceder y habilitar la opción llamada **Establecer el comportamiento predeterminado** para la ejecución automática.
- 10. Seleccionar la opción para no ejecutar ningún comando de ejecución automática.











11. Cerrar el editor de políticas de grupo.

Deshabilitar escritura en USB extraíble:

 Haga clic en el menú Inicio, busque y abra la herramienta Administración de políticas de grupo. En la pantalla Administración de políticas de grupo, busque la carpeta denominada Objetos de directiva de grupo.



2. Hacer clic con el botón derecho en la carpeta Objetos de directiva de grupo y seleccione la opción Nueva.











3. Ingresar un nombre para nueva política.

	New GPO X
Name:	
DENY USB WRITE	
Source Starter GPO:	
(none)	¥
	OK Cancel

En nuestro ejemplo, el GPO se llamó: DENY USB WRITE.

En la pantalla Administración de política de grupo, expanda la carpeta denominada Objetos de directiva de grupo.

4. Hacer clic con el botón derecho en su nuevo Objeto de directiva de grupo y seleccione la opción **Editar**.

Group Policy Management		
A Forest: TECH.LOCAL		
⊿ 🚰 Domains		
⊿ TECH.LOCAL		
Default Domain Policy		
Domain Controllers		
⊿ i Group Policy Objects		
📑 Default Domain Co	ontrollers Policy	
🗾 Default Domain Po	licy	
DENY USB WRITE		
	Edit	
	GPO Status	•
	Back Up	

En la pantalla del editor de políticas de grupo, se le presentará a **Configuraciones de usuario** y Configuraciones de computadora. Cambiar solo las configuraciones de la Computadora. No se necesita cambiar ninguna configuración de usuario.









- 5. En la pantalla del editor de políticas de grupo, expanda la carpeta de configuración de la computadora y ubique el siguiente elemento.
 - Configuración del equipo> Plantillas administrativas> Sistema> Acceso de almacenamiento extraíble



• A la derecha, se presentará la lista de opciones de configuración disponibles.

Setting	State	Comment
E Set time (in seconds) to force reboot	Not configured	No
E CD and DVD: Deny execute access	Not configured	No
E CD and DVD: Deny read access	Not configured	No
E CD and DVD: Deny write access	Not configured	No
E Custom Classes: Deny read access	Not configured	No
Custom Classes: Deny write access	Not configured	No
Floppy Drives: Deny execute access	Not configured	No
Floppy Drives: Deny read access	Not configured	No
Floppy Drives: Deny write access	Not configured	No
Removable Disks: Deny execute access	Not configured	No
Removable Disks: Deny read access	Not configured	No
Removable Disks: Deny write access	Not configured	No
All Removable Storage classes: Deny all access	Not configured	No
All Removable Storage: Allow direct access in remote sessions	Not configured	No
Tape Drives: Deny execute access	Not configured	No
Tape Drives: Deny read access	Not configured	No
Tape Drives: Deny write access	Not configured	No
WPD Devices: Deny read access	Not configured	No
WPD Devices: Deny write access	Not configured	No









- Primero, deshabilitar el acceso de escritura a los dispositivos de almacenamiento USB.
- Hacer doble clic en el elemento de configuración denominado Discos extraíbles: Denegar acceso de escritura.

En la pantalla del elemento de configuración, debe seleccionar la opción Habilitar.

Removable Disks: Deny Not <u>C</u> onfigured Cor Enabled Disabled Sup Options:	y write access mment: pported on: At le	Brevious Setting Mext Setting ast Windows Vista 0
Not <u>Configured</u> Cor Enabled Disabled Sup Options:	pported on: At l	ast Windows Vista
Enabled Disabled Sup Options:	pported on: At l	ast Windows Vista
O Disabled Sup Options:	pported on: At le	ast Windows Vista
Sup Options:	pported on: At le	ast Windows Vista
Options:		~
Options:		
		Help:
		This policy setting, white access to removable disks. If you enable this policy setting, white access is denied to this removable storage class. If you disable or do not configure this policy setting, write access is allowed to this removable storage class. Note to require that users write data to Bilacker-protected storage, enable the policy setting "Deny write access to drives not protected by Bilacker," which is located in "Computer Configuration/Administrative Templates/Windows Components/BitLocker Drive Encryption/Removable Data Drives,"

Si se desea deshabilitar el acceso de escritura a CD y DVD.

7. Hacer doble clic en el elemento de configuración denominado CD y DVD: Denegar acceso de escritura.

En la pantalla del elemento de configuración, debe seleccionar la opción Habilitar.

		CD and DVD: Deny write access
CD and DVD: Der	y write access	Previous Setting Next Setting
 Not <u>C</u>onfigured <u>E</u>nabled 	Comment:	<u>^</u>
O <u>D</u> isabled	Supported on:	At least Windows Vista
Options:		Help:
		This policy setting denies write access to the CD and DVD removable storage class. If you enable this policy setting, write access is denied to this removable storage class. If you disable or do not configure this policy setting, write access is allowed to this removable storage class.
		OK Cancel Apply









Para finalizar la creación de políticas de grupo, debe cerrar la ventana del Editor de políticas de grupo. Solo cuando cierre la ventana de política de grupo, el sistema guardará su configuración.

Ha finalizado la creación del GPO de restricción de red. Sin embargo, aún necesita habilitar el uso de su nueva Política de grupo.

 En la pantalla Administración de políticas grupales, debe hacer clic con el botón derecho en la Unidad organizativa deseada y seleccionar la opción para vincular un GPO existente.

Group Policy Management Group Policy Management Group Forest: TECH.LOCAL Group Domains Group TECH.LOCAL	
Default Do	Create a GPO in this domain, and Link it here
þ 🗐 Domain C	Link an Existing GPO
D 🧊 Group Pol	Block Inheritance

En el ejemplo, se vinculará la política de grupo llamada **DENY USB WRITE** a la raíz de nuestro dominio llamado **TECH.LOCAL**.

	Select GPO
<u>L</u> ook	in this domain:
	TECH.LOCAL V
Group	p Policy objects:
	Name
	Default Domain Controllers Policy
	Default Domain Policy
	DENY USB WRITE
	SOFTWARE POLICY
	OK Cancel

NOTA: Después de aplicar el GPO, debe esperar 10 o 20 minutos (de acuerdo al periodo de sincronización de GPOs establecido por su organización). Durante este tiempo, el GPO se replicará en otros controladores de dominio que pueda tener. Después de esperar 20 minutos, debe reiniciar la computadora de un usuario. Durante el arranque, la computadora obtendrá y aplicará una copia de la nueva política de grupo, o forzar manualmente la actualización de









las políticas con el comando de cmd o powershell gpupdate /force (ejecutar el comando con privilegios administrativos)

Para probar la configuración, debe conectar una unidad de almacenamiento USB a la computadora e intentar guardar un archivo. Su computadora debe denegar automáticamente el acceso de escritura al dispositivo de almacenamiento USB.

En caso de aplicarse dichas configuraciones debe tener en cuenta los siguientes puntos:

- Verificar que la replicación entre controladores de dominio se encuentre funcionando correctamente.
- La GPO debe aplicarse sobre el grupo de computadores en específico a bloquear el puerto USB.
- La computadora al ser bloqueada debe estar vinculada al dominio Microsoft Windows de su organización.
- Verifique que la computadora tenga conexión de red con el controlador de dominio en el cual está implementando la GPO.

Referencias

- <u>https://www.techtarget.com/searchsecurity/tip/Your-USB-port-management-options</u>
- <u>https://esgeeks.com/proteger-cifrar-usb-linux/</u>
- <u>https://www.manageengine.com/data-security/best-practices/usb-drive-best-practices.html</u>
- <u>https://www.solvetic.com/tutoriales/article/4801-bloquear-dispositivos-usb-concomando-chmod-linux/</u>
- <u>https://support.microsoft.com/es-es/windows/activar-el-cifrado-de-dispositivo-</u> 0c453637-bc88-5f74-5105-741561aae838#ID0EBD=Windows_10
- https://hardzone.es/tutoriales/mantenimiento/cifrar-pendrive-usb-windows/
- <u>https://blog.ragasys.es/controlador-de-dominio-active-directory-sobre-linux-ubuntu</u>
- https://mundowin.com/como-desactivar-la-funcion-autorun-en-windows-10/
- <u>http://www.usbduplicatornow.com/disable-autorun-autoplay.html</u>
- https://www.pantallazos.es/2017/08/gpo-bloquear-unidades-disco-usb.html
- <u>https://techexpert.tips/windows/gpo-disable-autorun-autoplay/</u>

