

10 DE JULIO DE 2018

PROTOCOLO HARDENING

DESTINADO A AULA UNIVERSITARIA - UNIDADES DE DETENCIÓN







Protocolo de Hardening

Windows 10 PC - Unidades de Detención

Contenido

¿Qué es el Hardening?	2
Gpedit.msc	2
Objetivos	2
Procedimiento	3
Restricción de navegación a través de internet	3
Habilitar, deshabilitar y restringir funciones del SO Windows	5
Restringir el acceso mediante contraseña al BIOS / UEFI de la PC	7
Precintar gabinete con precintos numerados	7





¿Qué es el Hardening?

Hardening (palabra en inglés que significa endurecimiento) en seguridad informática es el proceso de asegurar un sistema mediante la reducción de vulnerabilidades en el mismo, esto se logra eliminando software, servicios, usuarios, etc, innecesarios en el sistema; así como cerrando puertos que tampoco estén en uso además de muchas otros métodos y técnicas.

Gpedit.msc

Editor de directivas de grupo local

A los efectos de este protocolo, Gpedit será una de las herramientas principales para su correcta concreción.

El editor de políticas de grupo de Windows es una potente herramienta con la cual puedes modificar opciones semiocultas del sistema operativo Windows.

Objetivos

Mediante este protocolo se busca segurizar una PC que se encontrara en el sector de aula universitaria de una unidad de detención, debido a esto se realizara la mayor cantidad de restricciones posibles para su utilización en condiciones de encierro, lo cual implica:

- Habilitar, deshabilitar y restringir funciones del SO Windows mediante el editor de directivas de grupo local Gpedit.msc
- Aplicar restricciones a la navegación por internet mediante configuración de las propiedades de internet del SO.
- Restringir el acceso mediante contraseña al BIOS / UEFI de la PC.







Procedimiento

Para la restricción de navegación a través de internet, realizamos los siguientes pasos:

 Ingresamos a Panel de control > Opciones de internet > Solapa Conexiones > Configuración LAN.

🔮 Propiedades de Internet	? X Configuración de la red de área local (LAN) X
General Seguridad Privacidad Conexiones Programas Opciones Image: Program and the second	Contenido anzadas Configuración automática La configuración automática puede invalidar la manual. Para evitar que esto ocurra, deshabilite la configuración automática. y Detectar la configuración automáticamente Usar scripts de configuración automática Dirección gar r VPN ar Usar un servidor proxy para la LAN (esta configuración no se aplicará a conexiones de acceso telefónico ni VPN). Dirección: 127.0.0.1 Puerto: 80 Opciones avanzadas No usar servidor proxy para direcciones locales Aceptar Cancelar
Configuración de la red de área local (LAN) La configuración de LAN no se aplica a las conexiones de acceso telefónico. Elija Configuración, más arriba, para configurar el acceso telefónico.	ión de LAN

Debemos tildar "usar un servidor proxy para LAN..." donde colocaremos en dirección ip local de la maquina (127.0.0.1) con puerto 80.





 FIOLEGENIOS INGLESATIOU ET OPCIONES avanzagas 	adas	avanzada	pciones	en	ngresando	s ing	demos	Proced	•
---	------	----------	---------	----	-----------	-------	-------	--------	---

	Tipo Dirección del proxy que va a usar Puerto				
	HTTP:	127.0.0.1]:	80	
	Seguro:	127.0.0.1	:	80	
	FTP:	127.0.0.1	:	80	
	Socks:		:		
	✓ Usar e	l mismo servidor proxy para todos los p	rote	ocolos	
cepci	Usar e ones No usar u	l mismo servidor proxy para todos los p n servidor proxy para las direcciones qu	iroto	ocolos	
cepci	Usar e ones No usar u comiencer	l mismo servidor proxy para todos los p n servidor proxy para las direcciones qu n con:	iroto	ocolos	
cepci	Usar e ones No usar u comiencer aca coloc navegar,	l mismo servidor proxy para todos los p n servidor proxy para las direcciones qu n con: camos las URL donde si vamos a permit separandolas con punto y coma (;)	irote ie	ocolos	

En esta ventana debemos completar las "Excepciones" donde colocaremos las URL donde si vamos a permitir navegar, separándolas con punto y coma (;).



DEPARTAMENTO INFORMÁTICA AREA TIC'S Y PROGRAMACIÓN





Para habilitar, deshabilitar y restringir funciones del SO Windows mediante el editor de directivas de grupo local Gpedit.msc, realizamos los siguientes pasos:

 Ingresamos a "Ejecutar" tecla Windows + R > y ejecutamos el comando gpedit.msc. Una vez dentro iniciamos las restricciones en Configuración <u>del equipo</u> > Plantillas administrativas > Todos los valores.

Editor de directivas de grupo local				- 0	\times
Archivo Acción Ver Ayuda					
J Directiva Equipo local	Todos los valores				
 Configuración del equipo Configuración de coffuero 	Selecciona un elemento para ver su	Configuración	Estado	Comentario	^
Configuración de Windows	descripción.	E Abrir iconos de Internet Explorer en el escritorio	No configurada	No	
Plantillas administrativas		Access 2016 (solo copia de seguridad)	No configurada	No	
> Componentes de Windows		Acción al desconectar el servidor	No configurada	No	
Impresoras		Acción de notificación de batería baja	No configurada	No	
> Menú Inicio y barra de tareas		Acción de notificación de batería crítica	No configurada	No	
> 🧮 Panel de control		Acciones no predeterminadas de desconexión del servidor	No configurada	No	
> 🚞 Red		E Acortamiento de sufijo DNS principal	No configurada	No	
Servidor		E Activar actualizaciones recomendadas mediante Actualizaci	No configurada	No	
> 🧾 Sistema		Activar análisis completo de puesta al día	No configurada	No	
Todos los valores		📰 Activar análisis rápido de puesta al día	No configurada	No	
V 🐔 Configuración de usuario		Activar animaciones en páginas web	No configurada	No	
Configuración de software		Activar autenticación básica de la fuente a través de HTTP	No configurada	No	
> Configuración de Windows		Activar automáticamente complementos recientemente ins	No configurada	No	
> Plantillas aurimistrativas		🗈 Activar BranchCache	No configurada	No	
		E Activar controlador de E/S de asignador (LLTDIO)	No configurada	No	
		Activar controlador de respuesta (RSPNDR)	No configurada	No	
		Activar detección de filtros SmartScreen	No configurada	No	
		Activar detección de filtros SmartScreen	No configurada	No	
		Activar detección de filtros SmartScreen	No configurada	No	
		Activar detección de filtros SmartScreen	No configurada	No	
		Activar detección de filtros SmartScreen	No configurada	No	
		Activar detección de filtros SmartScreen	No configurada	No	
		Activar detección de filtros SmartScreen	No configurada	No	
		Activar detección de filtros SmartScreen	No configurada	No	
		Activar detección de filtros SmartScreen	No configurada	No	
		Activar detección de filtros SmartScreen	No configurada	No	
		Activar el análisis de Protección de archivos de Windows	No configurada	No	
		📰 Activar el Centro de seguridad (solo equipos de dominio)	No configurada	No	
		Activar el examen de procesos cuando la protección en tiem	No configurada	No	
		E Activar el filtrado ActiveX	No configurada	No	
		E Activar el filtro de scripts de sitios	No configurada	No	× *
	Estandida (Estándas /	s			7
2429 valores					

Una vez allí buscaremos cada una de las siguientes configuraciones y quedaran en el estado indicado.

CONFIGURACIÓN DE EQUIPOS > PLANTILLAS ADMINISTRATIVAS > TODOS LOS VALORES				
Configura	ar Actualizaciones automáticas.	Deshabilitada		
• Deshabili	itar la página Opciones avanzadas.	Habilitada		
• Discos ex	traíbles: denegar acceso de ejecución.	Habilitada		





A modo de ejemplo, buscamos "Configurar Actualizaciones automáticas" e ingresamos haciendo doble clic > una vez dentro seleccionamos la opción "Deshabilitada".

Editor de directivas de grupo local		X	
Directiva Equipo local	Todos los valores		
	Configurar Actualizaciones automáticas Editar <u>configuración de directiva</u> Requisitos: Windows XP Professional Service	Configuración Estado Comentario El Configura Acceso controlado a carpeta No configurada No Il Configura Actualizaciones automáticas No configurada No El Configurar Actualizaciones automáticas No configurada No	×
 Panel de control Red Servidor Sistema Todos los valores Configuración de usuario Configuración de software Configuración de software Plantillas administrativas 	Pack 10, al menos, Windows 2000 Service Pack 3 Descripción: Especifica si este equipo recibirá actualizaciones de seguridad y otras descargas importantes a través del servicio de actualización automática de Windows. Notas esta directiva no se aplica a Michaeumo III.	Con Configurar Actualizaciones automáticas Valor anterior Valor siguiente Con Con Configurada Comentario: Con O No configurada Comentario: Con O Habilitada Con Con Con Con Compatible con: Vindows XP Professional Service Pack 1 o, al menos, Windows 2000 Service Pack 3	~
	Este valor permite especificar si las actualizaciones automáticas están habilitadas en el equipo. Si el servicio está habilitado, debe seleccionar una de las cuatro opciones en la configuración de directiva de grupo:	El Con Con El Con Con Opciones: Ayuda: Con El Con Configurar actualización automática: Bà Con Las siguientes opciones de configuración son neces.	d y ción
	2 = Notificar antes de descargar e instalar cualquier actualización. Cuando Windows encuentra actualizaciones aplicables al equipo, los usuarios reciben una notificación de que hay actualizaciones listas para deseamente Deravió de la b	Con aplicables si se selecciona la opción 4. Con Instalar durante mantenimiento automático Con Con Con Con Con Con Hora de instalación programado: Con Hora de instalación programada: Con Stave relaccionado 14. Descaper utamáticamente Con Stave relaccionado 14. Descaper utamáticamente	al
2429 valores	Vindows Update, los suvarios pueden descargare instalar cualquier actualización disponible. Extendido / Estándar/	Con programa la instalación ² y a Dexargia a duba entratación entre quipo, los usuarios reciben una notificación de que hay actualizaciónen sitas para descargares. Después de ir a Windo Update, los usuarios veden descargar e instalar cualquier actualización disponible.	s

 A posterior continuando con las restricciones dentro de gpedit iniciamos las restricciones en Configuración de <u>usuarios</u> > plantillas administrativas > todos los valores.

Editor de directivas de grupo local				- 0	\times
Archivo Acción Ver Ayuda					
Direction Family Land					
Directiva Equipo local	Todos los valores				_
Configuración de usuario	Selecciona un elemento para ver su	Configuración	Estado	Comentario	^
Configuración de software	descripción.	E Abrir iconos de Internet Explorer en el escritorio	No configurada	No	
Configuración de Windows		E Abrir siempre Todos los elementos del Panel de control al a	No configurada	No	
Plantillas administrativas		E Acceso remoto	No configurada	No	
> Active Desktop		Acceso telefónico mediante RAS: nodo de usuario	No configurada	No	
Carpetas compartidas		Access 2016 (solo copia de seguridad)	No configurada	No	
> Componentes de Windows		Acción al desconectar el servidor	No configurada	No	
> Menú Inicio y barra de tareas		Acciones no predeterminadas de desconexión del servidor	No configurada	No	
> Panel de control		Activar animaciones en páginas web	No configurada	No	
> 🔛 Red		Activar autenticación básica de la fuente a través de HTTP	No configurada	No	
> 🧮 Sistema		🗈 Activar Autocompletar en línea	No configurada	No	
Todos los valores		E Activar automáticamente complementos recientemente ins	No configurada	No	
		Activar depuración de scripts	No configurada	No	
		Activar detección de filtros SmartScreen	No configurada	No	
		E Activar detección de filtros SmartScreen	No configurada	No	
		Activar detección de filtros SmartScreen	No configurada	No	
		E Activar detección de filtros SmartScreen	No configurada	No	
		E Activar detección de filtros SmartScreen	No configurada	No	
		Activar detección de filtros SmartScreen	No configurada	No	
		E Activar detección de filtros SmartScreen	No configurada	No	
		Activar detección de filtros SmartScreen	No configurada	No	
		E Activar detección de filtros SmartScreen	No configurada	No	
		E Activar detección de filtros SmartScreen	No configurada	No	
		🗈 Activar el candidato en la nube	No configurada	No	
		📰 Activar el candidato en la nube para CHS	No configurada	No	
		E Activar el filtrado ActiveX	No configurada	No	
		E Activar el filtro de scripts de sitios	No configurada	No	
		Activar el filtro de scripts de sitios	No configurada	No	
		E Activar el filtro de scripts de sitios	No configurada	No	
		E Activar el filtro de scripts de sitios	No configurada	No	
		E Activar el filtro de scripts de sitios	No configurada	No	
		E Activar el filtro de scripts de sitios	No configurada	No	~
		<			>
	Extendido Estándar				

1766 valores





Una vez allí aplicamos la siguiente tabla de valores.

CONF	IGURACION DE USUARIO > PLANTILLAS ADMINISTRATIVAS > TODOS	LOS VALORES
•	Actualizaciones automáticas de Windows.	Habilitada
•	Administración de discos	Deshabilitada
•	Administración de equipos.	Deshabilitada
•	Desactivar la aplicación Tienda	Habilitada
•	Desactivar la oferta para actualizar a la versión de Windows más reciente.	Habilitada
•	Desactivar Reproducción automática	Habilitada
•	Deshabilitar el cambio de configuración de conexión.	Habilitada
•	Deshabilitar la configuración de la página Opciones avanzadas	Habilitada
•	Impedir acceso a las unidades desde Mi PC.	Habilitada
•	Impedir el acceso a herramientas de edición del Registro.	Habilitada
•	Impedir el acceso al símbolo del sistema.	Habilitada
•	Impedir que los usuarios personalicen su pantalla Inicio.	Habilitada
•	Impedir que los usuarios reemplacen el símbolo del sistema con Windows Powershell	Habilitada
•	Ocultar la página Agregar nuevos programas	Habilitada
•	Ocultar la página Cambiar o quitar programas	Habilitada
•	Ocultar la pestaña Configuración	Habilitada
•	Prohibir el acceso a Configuración de PC y a Panel de control	Habilitada
•	Prohibir el acceso a propiedades de componentes de una conexión de acceso remoto	Habilitada
•	Prohibir la configuración TCP/IP avanzada.	Habilitada
•	Quitar Agregar o quitar programas	Habilitada
•	Quitar el menú Archivo del Explorador de Archivos	Habilitada
•	Quitar el menú Ejecutar del menú Inicio.	Habilitada
•	Sin "Equipos próximos" en Ubicaciones de red.	Habilitada

Restringir el acceso mediante contraseña al BIOS / UEFI de la PC, esta configuración varía dependiendo del modelo y marca de la placa madre.

Precintar gabinete con precintos numerados para controlar el caso de un acceso indebido al interior del mismo y así evitar la manipulación de los componentes internos o el posible reset de BIOS / UEFI.



DEPARTAMENTO INFORMÁTICA AREA TIC'S Y PROGRAMACIÓN