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?

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

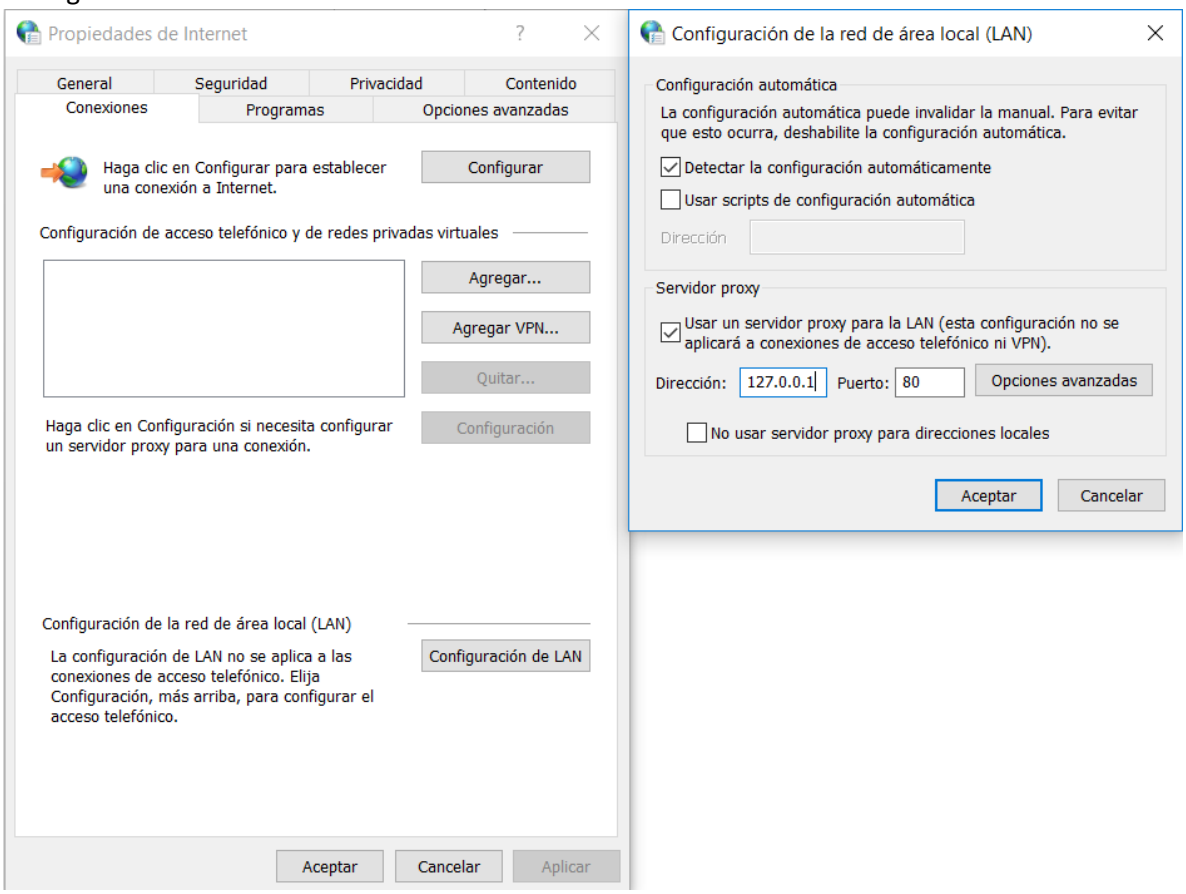
Mediante este protocolo se busca segurizar una PC que se encontrara en el sector de aula universitaria de una unidad de detención, debido a esto se realizara la mayor cantidad de restricciones posibles para su utilización en condiciones de encierro, lo cual implica:

- 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

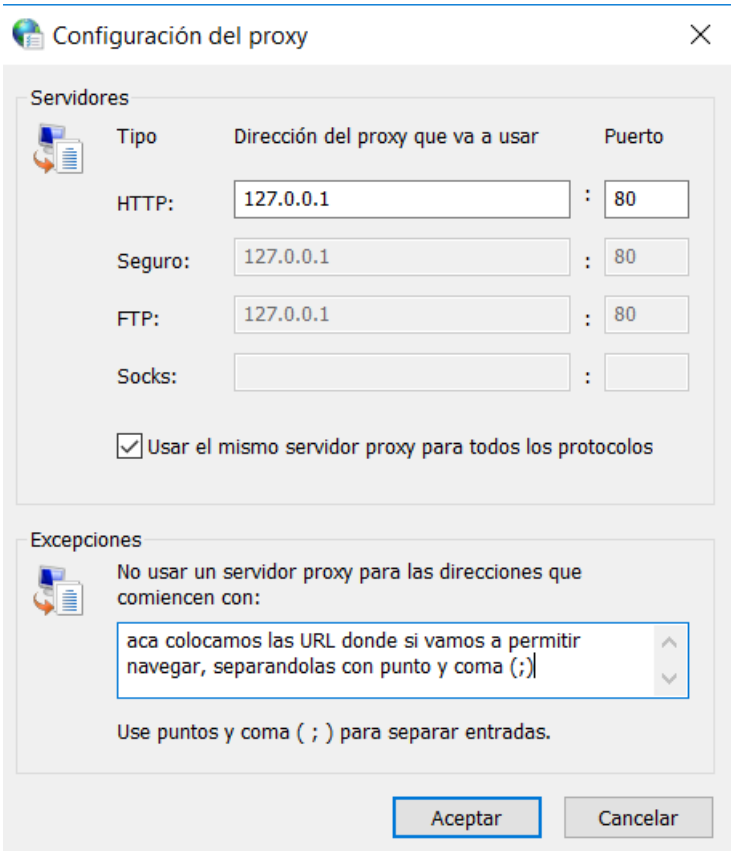
Para la restricción de navegación a través de internet, realizamos los siguientes pasos:

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



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

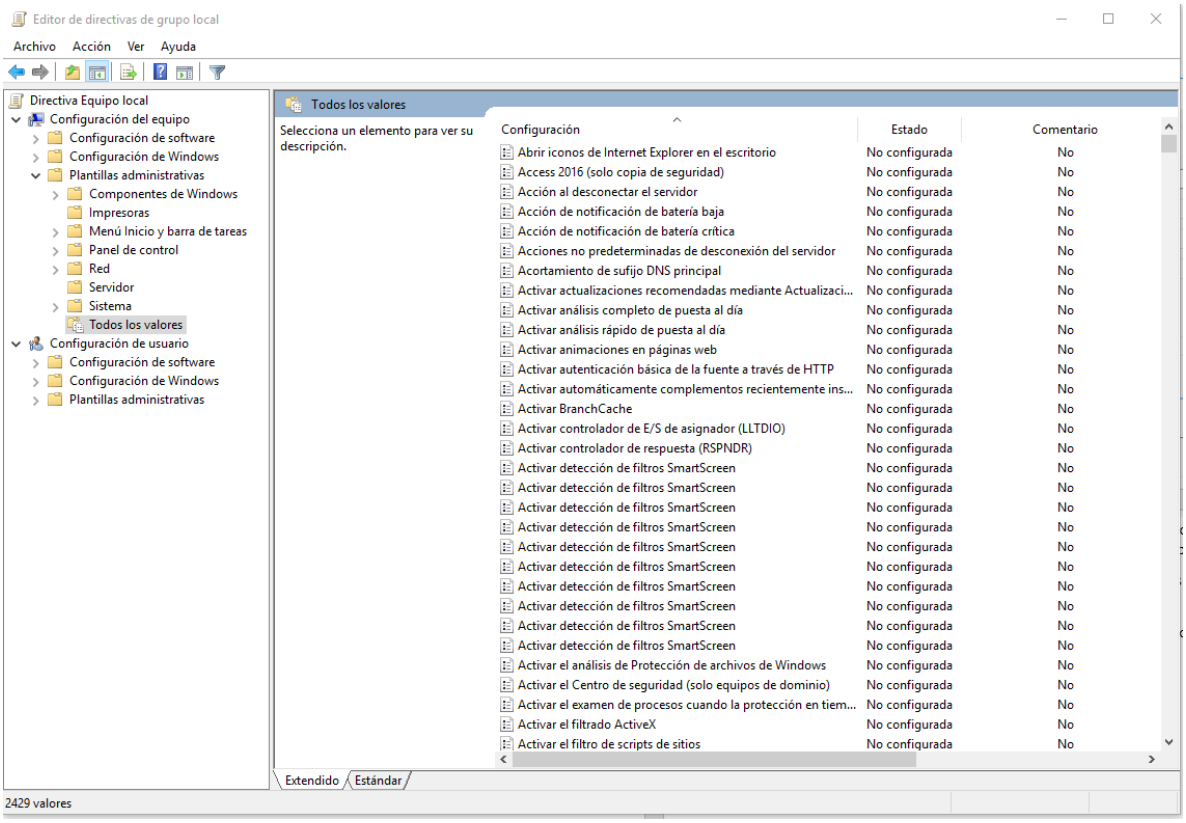
- Procedemos ingresando en “opciones avanzadas”.



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

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

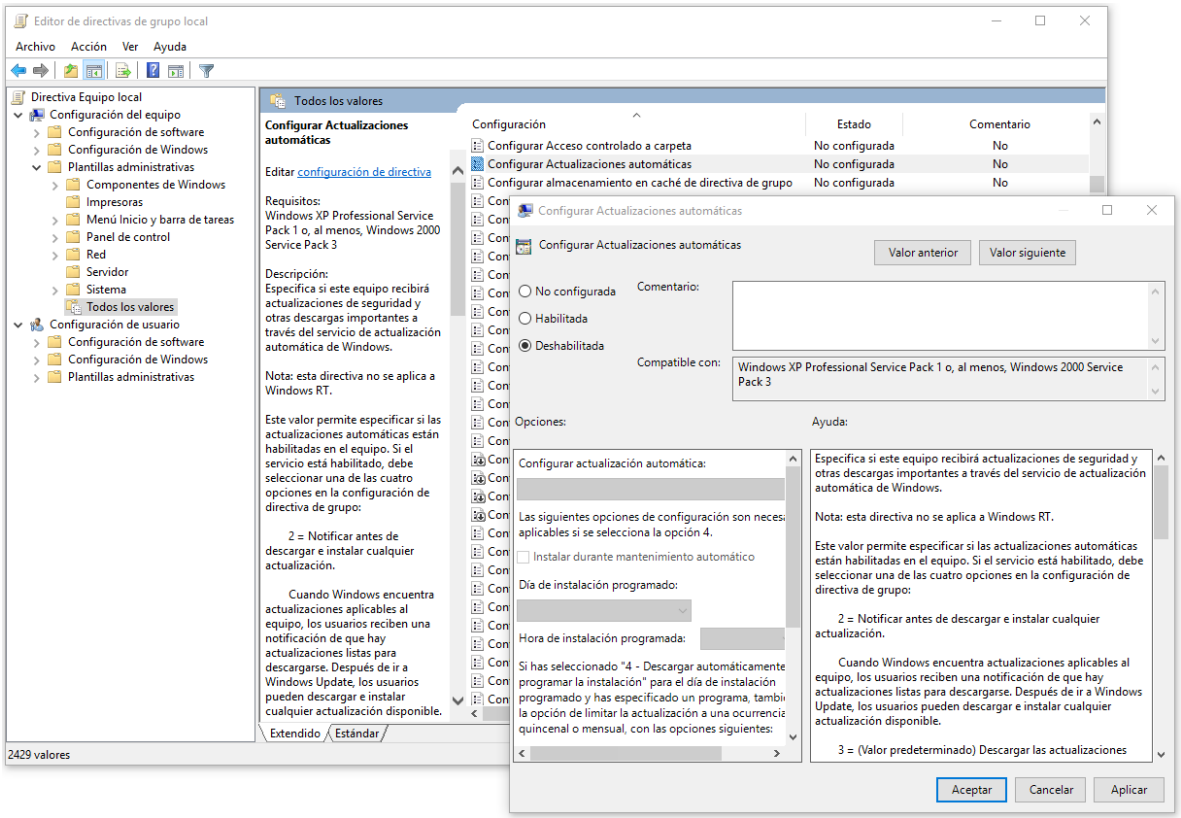
- Ingresamos a “Ejecutar” tecla Windows + R > y ejecutamos el comando gpedit.msc. Una vez dentro iniciamos las restricciones en Configuración *del equipo* > Plantillas administrativas > Todos los valores.



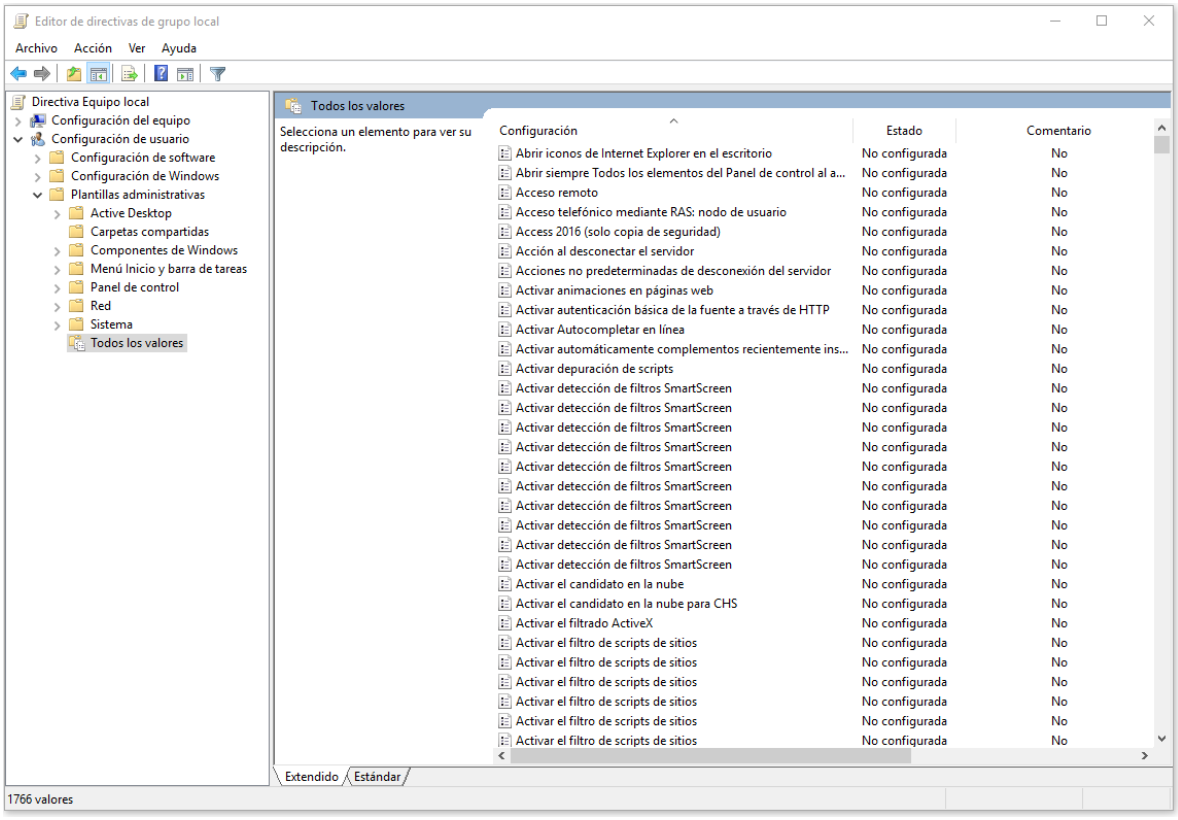
Una vez allí buscaremos cada una de las siguientes configuraciones y quedaran en el estado indicado.

CONFIGURACIÓN DE EQUIPOS > PLANTILLAS ADMINISTRATIVAS > TODOS LOS VALORES	
• **Configurar Actualizaciones automáticas.**	Deshabilitada
• **Deshabilitar la página Opciones avanzadas.**	Habilitada
• **Discos extraíbles: 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”.



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



Una vez allí aplicamos la siguiente tabla de valores.

CONFIGURACION 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.