

ACTIVIDADES BÁSICAS 1.

A continuación, seguiremos una serie de pautas básicas de configuración y mantenimiento de nuestros sistemas Windows que permitan optimizar mejor su rendimiento y de paso subir un escalón en la mejora de la seguridad de los mismos.

- Ver ficheros, carpetas y unidades ocultas, del sistema y no ocultar las extensiones de ficheros conocidos (virus Kournikova).
 - o Comandos **assoc** y **ftype**
- Nombre NetBIOS y Work Group (red P2P).
- Protección SSD (gestión de temporales, descargas, indización, hiberfil.sys, pagefile.sys).
 - o Comando **powercfg /? ----- powercfg -h off**
 - o Documento **“Cambiar la ubicación de un perfil.pdf”**.
 - o Carpetas SoftwareDistribution, WinSxS.
- Msconfig.
- Gestión de los Servicios.
Comandos **services.msc --- sc.exe**
Práctica de servicios innecesarios para deshabilitar.
- Software de terceros básico (nos descargamos el fichero **“Software básico.zip”**):
AutoRuns64. **Script para autorunsc (CLI)**.
CCleaner.
ClamAV.
Revo Uninstaller.
TCPView64.
Suite de Nirsoft y de Sysinternals.
Software **“Seguridad del Entorno Windows.zip”**.
- Introducción a las GPOs y directivas del sistema:

Secpol.msc: Inicio -- Panel de control -- Sistema y Seguridad -- Herramientas administrativas -
- Directiva de seguridad local. O bien **secpol.msc**
Directivas de cuenta: Directiva de contraseñas y Directiva de bloqueo de cuenta.
Directivas locales: Directiva de auditoría, Asignación de derechos de usuario y Opciones de seguridad.

Gpedit.msc: Configuración del usuario (estas directivas se aplican cuando el usuario se autentifica en el equipo).
Configuración del equipo (estas directivas se aplican cuando se inicia el equipo).
De las tres opciones que dispone, la más interesante es la tercera (Plantillas administrativas).
Dentro de la opción segunda (Configuración de Windows), la opción Configuración de seguridad corresponde íntegramente a **secpol.msc** o Directiva de seguridad local.

Ejemplo:

Hay una directiva muy interesante con respecto a la Red que la vamos a cambiar aquí. Es la siguiente: Configuración del equipo, Plantillas administrativas, Red, Programador de paquetes QoS, Limitar ancho de banda reservable. Habilitar esta opción y poner el ancho de banda a 0%.

NOTA: En documentos posteriores, ampliaremos conocimientos y prácticas sobre GPOs.