|  |  |
| --- | --- |
|  | **2019** |
|  |  |

|  |
| --- |
| **[Restricción de Aplicaciones con políticas de Grupo/Local]** |
| Manual explicativo con el procedimiento para bloquear ciertas características de ser necesario, con apoyo visual, los pantallazos corresponden a un servidor con Windows Server 2008 R2, puede que algunos pasos estén desactualizado, se pide investigar por parte del lector en caso que las versiones sean distintas y/o cambie el contenido del manual con lo que tiene el usuario en pantalla. |

# Introducción

La idea es enfocar un sistema con menor cantidad de herramientas, pero no eliminar aquellas necesarias para ciertos usuarios.

Si notamos muchos usuarios tienen facultados en los equipos los cuales no son necesarios para su actividad laboral, en estos casos, ocultar o restringir estas herramientas es el método más sencillo para evitar el mal uso o accidentes informáticos que pueden afectar la integridad de la compañía.

También debemos considerar que el enfoque de esta medida es para usuarios altamente dependientes de interfaces gráficas, puesto que con un acceso a PowerShell y los permisos necesarios basta con un par de líneas para obtener acceso o un script corto para colocar una tarea nueva.

Para aquello navegaremos por la herramienta de políticas de usuarios, sus diversas funciones y algunas configuraciones a modo de ejemplo para restringir algunas herramientas de interés.

A modo que el documento sea más legible se usara un anexo con las imágenes al final del documento en donde se podrán ver las imágenes, en caso de duda por parte del lector (tómese como referencia, no como un absoluto).

# Editando políticas de grupo

Para editar políticas de grupo debemos buscar el menú el cual nos da la opción, el cual puede ser *“Editar directivas de grupo”* o *“Edit group policy”* (véase imagen 1).

Este menú tiene dos universos, la máquina o conjunto local (estas afectan al pc como tal) y el conjunto de políticas del usuario (estas afectan al comportamiento del SO frente al usuario), estas últimas nos interesan más que las anteriores.

Dentro del menú del usuario tenemos tres carpetas (véase imagen 2) que contienen reglas predefinidas para su ejecución con rangos de alcance distintos, estas reglas cabe destacar se aplican independiente a cual computador el usuario este con la sesión iniciada, quiere decir están vinculadas al usuario no a la máquina.

* Configuraciones de Software (Software Settings)
  + Este nodo tiene un subnodo de instalación de software
* Configuraciones de Windows (Windows Settings)
  + Contiene cinco subnodos
    - Redirección de directories (Folder redirection)
    - Ajustes de seguridad (Security settings)
    - Scripts
    - Instalación remota de servicios (Remote installation services)
    - Mantenimiento de IE (Internet explorer maintenance)
* Plantillas administrativas (Administrative Templates)
  + Este nodo contiene todas las políticas basadas en los registro, ergo se similar a modificar regedit pero de una manera más segura

# Configuraciones de Windows

Como mencionamos anteriormente, este nodo dentro de las políticas de grupo se encarga sobre la configuración de políticas del SO, más que nada asuntos dependientes a la comunicación de puertos y seguridad en general (certificados) (véase imagen 3).

Scripts

Esta sección administra los accesos para la ejecución de scripts cuando el usuario inicia o cierra sesión en una máquina, scripts corriendo en el contexto del usuario están contemplados en esta configuración (véase imagen 4).

* Logon: Administra los scripts al inicio de la sesión, se pueden agregar tanto, scripts normales como scripts con PowerShell (véase imagen 5).
* Logoff: Administra los scripts al inicio de la sesión, se pueden agregar tanto, scripts normales como scripts con PowerShell (véase imagen 6).

Ajustes de Seguridad

Esta sección administra las políticas de las claves públicas, la cuales se pueden desactivar/activar en caso de ser necesario (véase imagen 7). Estos certificados son útiles para la renovación automática de los mismos sin intervención del usuario (autoenrollment certificate). O en otros casos permite mover datos de credenciales mientras se usan perfiles locales para los usuarios (credential roaming).

Políticas basadas en Calidad de Servicio (QoS)

En esta sección podemos integrar reglas QoS, en donde podemos redirigir o dar más prioridad a tráfico especifico en caso de ser necesario (véase imagen 8).

# Plantillas Administrativas

Como ya recopilamos anteriormente, esta sección nos da acceso a reglas ya definidas las cuales restringen o conceden el acceso a ciertas acciones sobre programas, redes, etc. (cualquier cosa que tenga relación con configuraciones basadas en registros).

Panel de Control

Este nodo nos conecta con todas las reglas sobre la autorización a las diversas áreas del panel de control con el usuario, en donde podemos prohibir el acceso, ocultar opciones, prevenir cambios estéticos del sistema, no permitir la instalación de programas como su desinstalación. Prácticamente cada opción de configuración del panel de control está ubicada acá en donde se pueden ocultar o restringir su uso (véase imagen 9).

También están los nodos de escritorio y menú de inicio como barra de tareas las cuales mayoritariamente son restricciones a los cambios estéticos del sistema, como al uso de aero y activación/desactivación.

Redes

Este nodo tiene diversos ámbitos, desde prohibir el acceso a las conexiones o como el usuario tiene acceso a las funciones de los dispositivos de redes, como también a los archivos offline que se almacenan como intercambio con herramientas online (véase imagen 10).

Sistema

Acá hay una gran variedad de configuraciones correspondientes a los componentes del sistema (véase imagen 11), dentro de las reglas más notables:

* Opciones Crtl+Alt+Del: Opciones las cuales dan acceso al administrador de tareas, así como al cambio de contraseña (también en panel de control).
* Instalación de drivers: Cambia la configuración sobre la búsqueda de drivers y las localidades disponibles para su búsqueda, así como su firma digital.
* Manager de comunicación sobre internet: El cual tiene varias reglas interesantes como el poder desactivar la impresión mediante http
* Logon: Permite correr ciertos programas la inicio de computador
* Acceso a almacenamiento removible: Administra el acceso a CD, floppy drives y discos removibles, entre otros, tanto para escritura como lectura.

Componentes de Windows

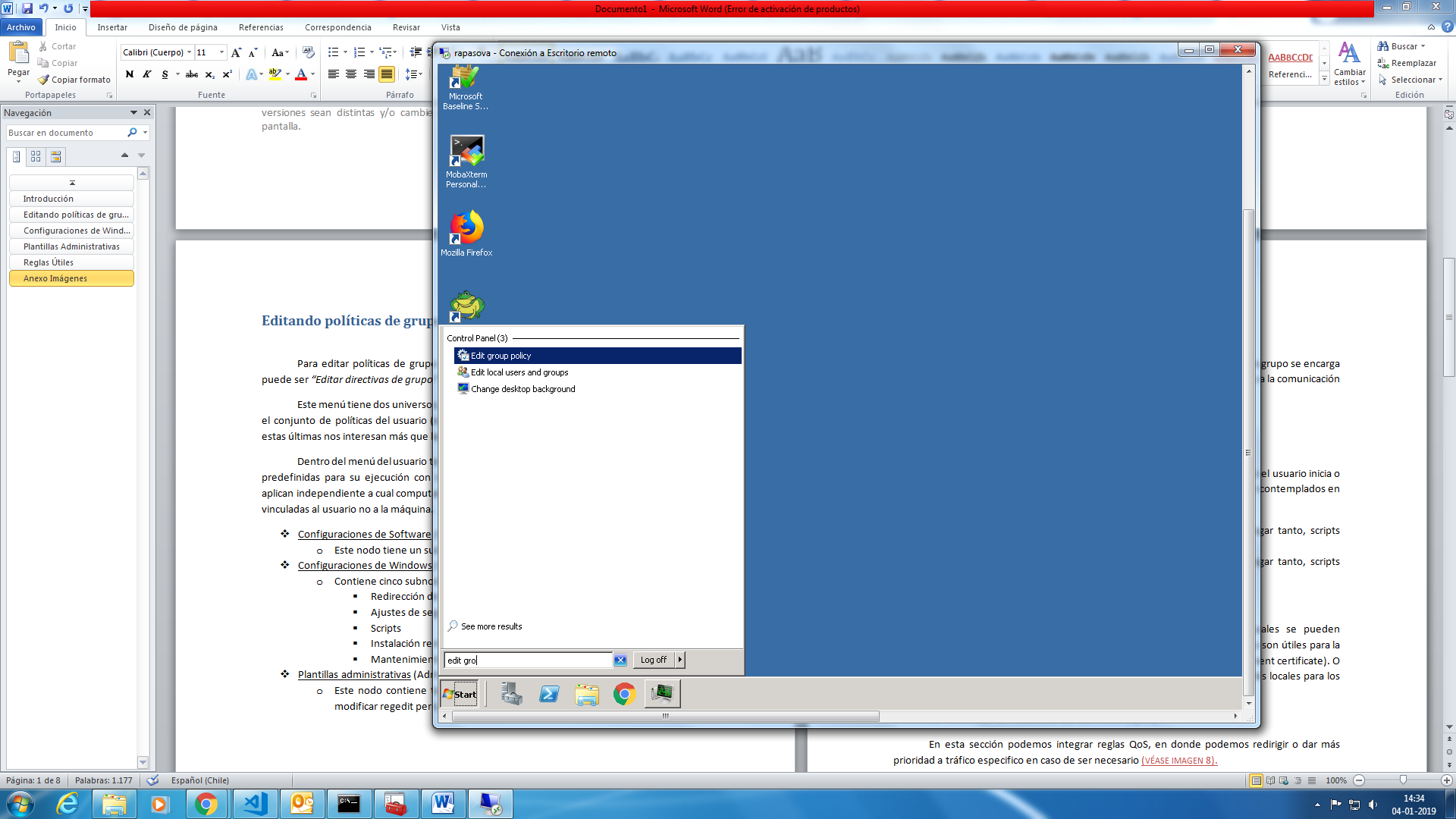
Este nodo trae reglas para cada herramienta, una que puede tomar nuestro interés es revocar permisos para correr scripts en PowerShell (véase imagen 12).

# Reglas Útiles

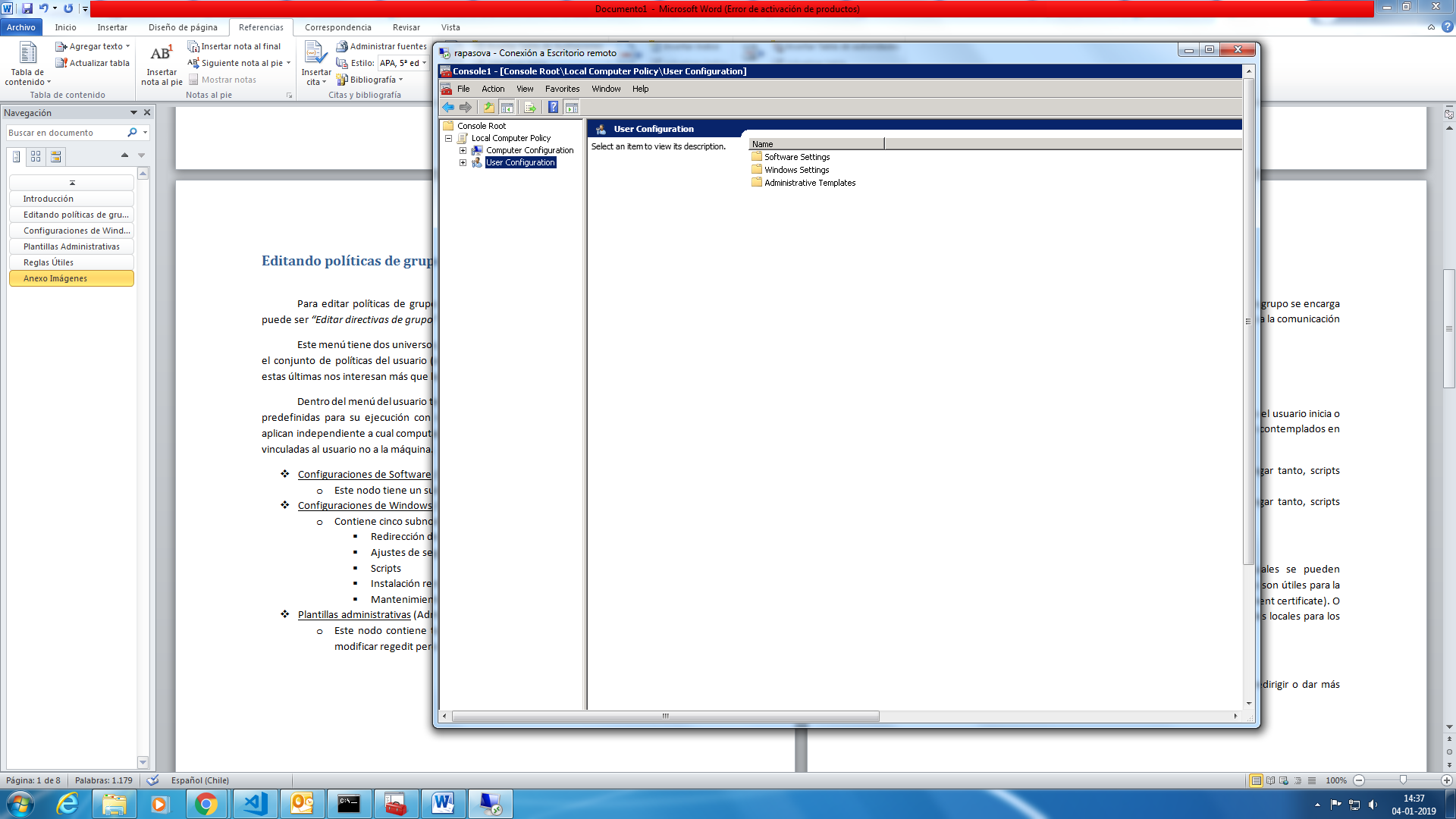
Dentro del funcionamiento pueden surgir eventos en los cuales necesitemos restringir el acceso a algunas características, muchas de estas no son tan simples de lograr o requieren más de una regla para que funcionen.

* Restringir PowerShell: Para restringir esta herramienta se deben cumplir dos condiciones, primero que PowerShell no pueda ser abierto por el usuario, pero además que la línea de comando no pueda ser accedida puesto que PowerShell es accesible fácilmente por esa herramienta (véase imagen 13).
* Restringir programador de tareas: Esta herramienta es un servicio de Microsoft, por lo tanto no es un ejecutable, el ejecutable que lo llama es *mmc.exe* el cual es la consola de administración de Windows. Esta consola puede ser restringida igual que PowerShell, pero también puede ser accedida por ella, el hecho de bloquearla soló hace más difícil su uso si el perpetrador se enfoca en interfaces gráficas y no en líneas de comando, ya que no es recomendable quitar el acceso a PowerShell como a *mmc.exe*.

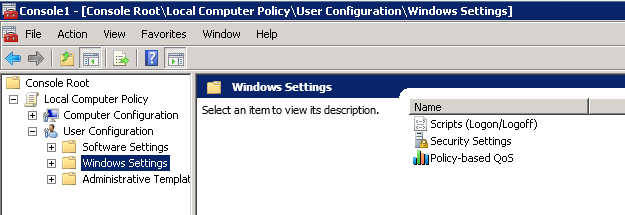
# Anexo Imágenes



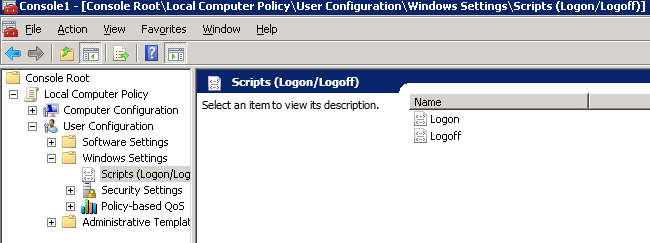
Imagen



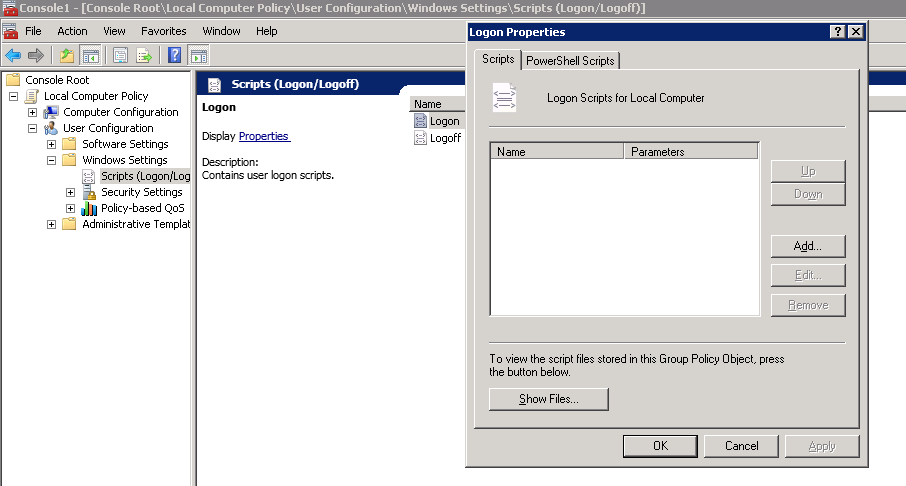
Imagen



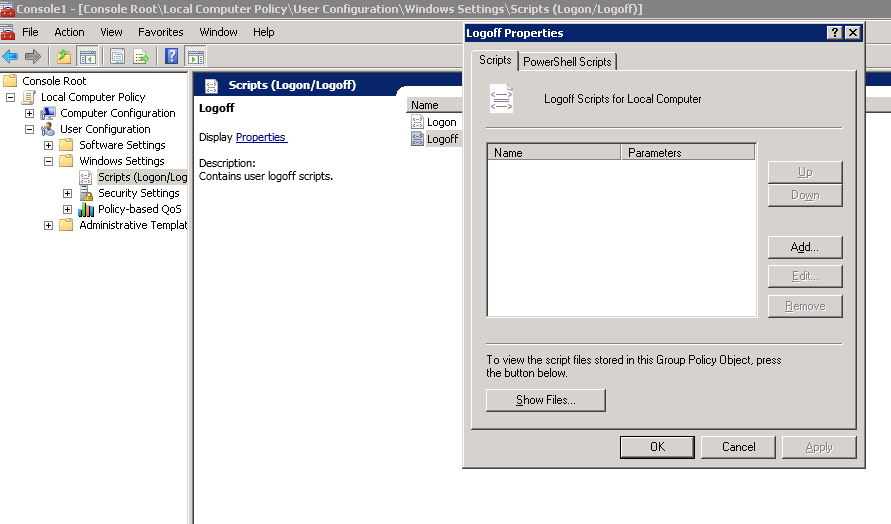
Imagen



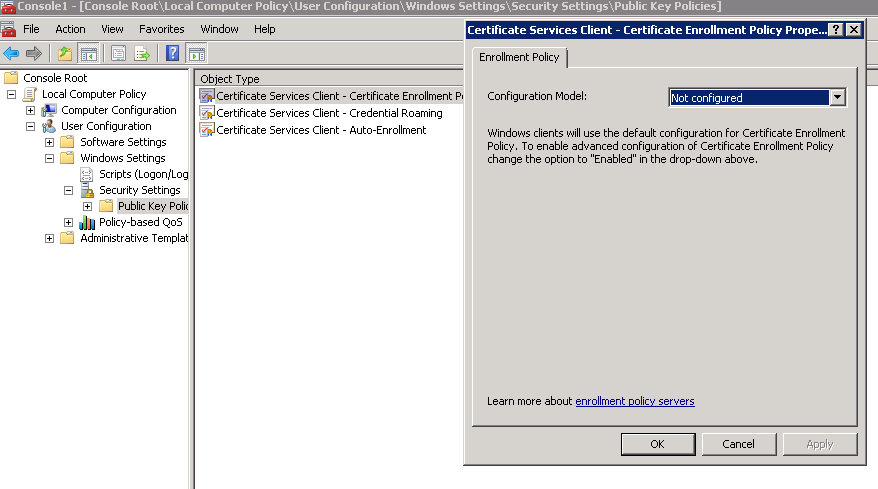
Imagen



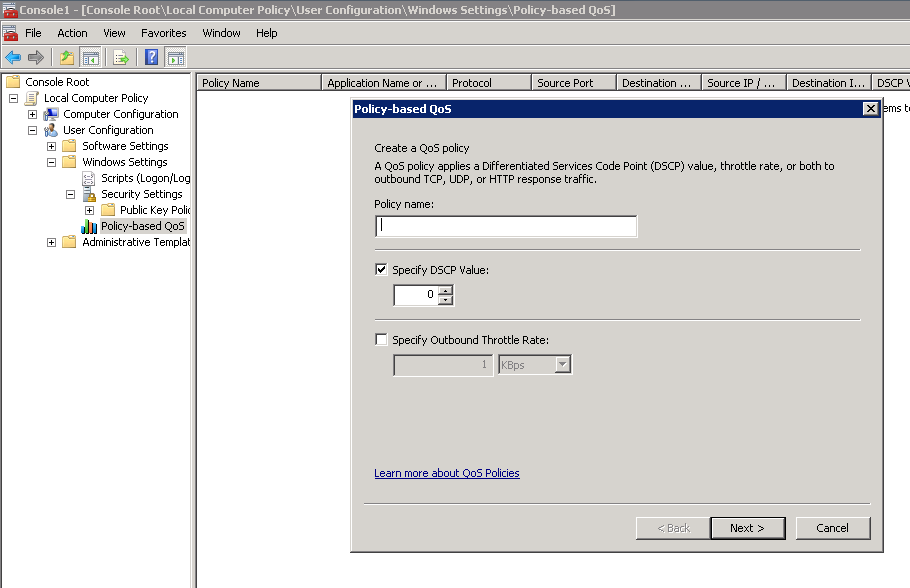
Imagen



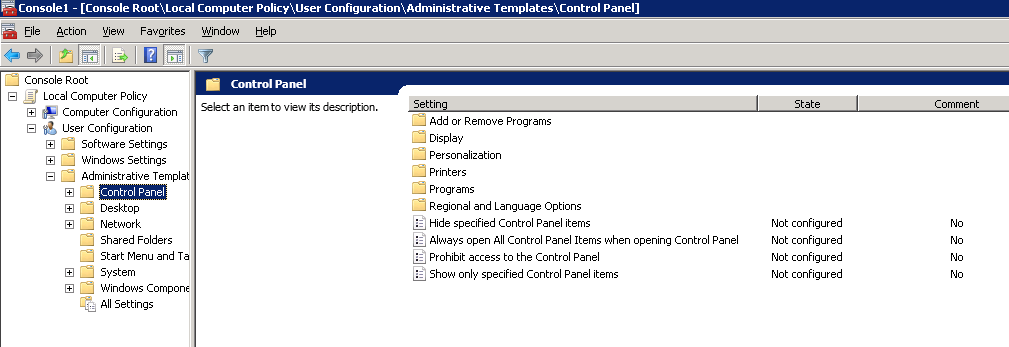
Imagen



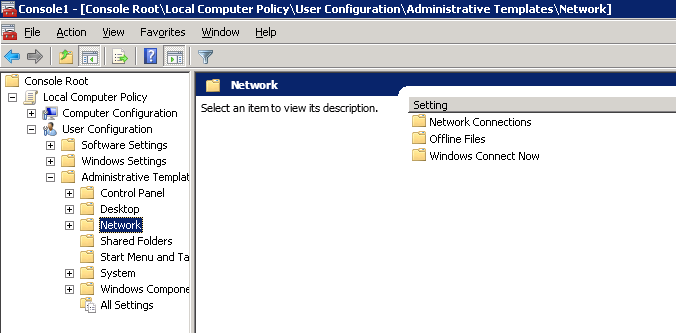
Imagen



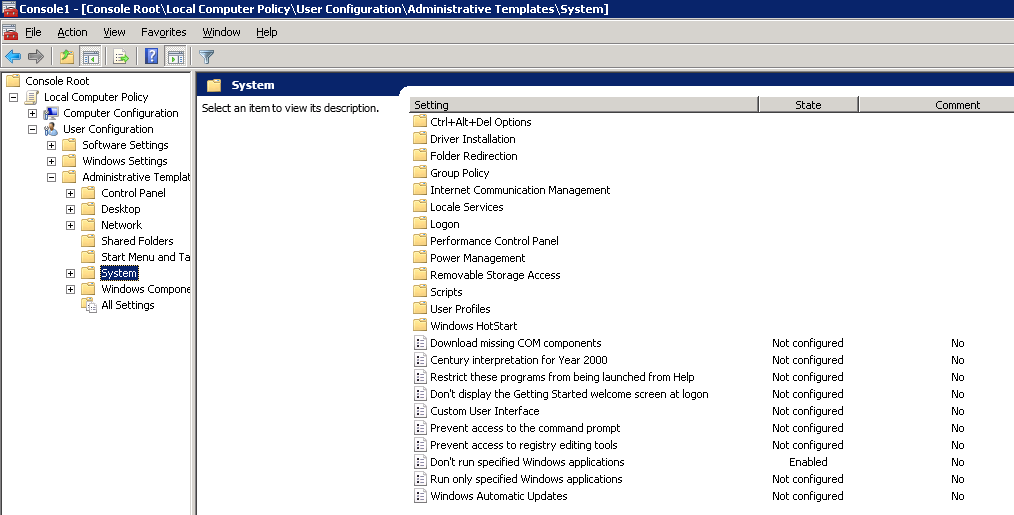
Imagen



Imagen



Imagen



Imagen

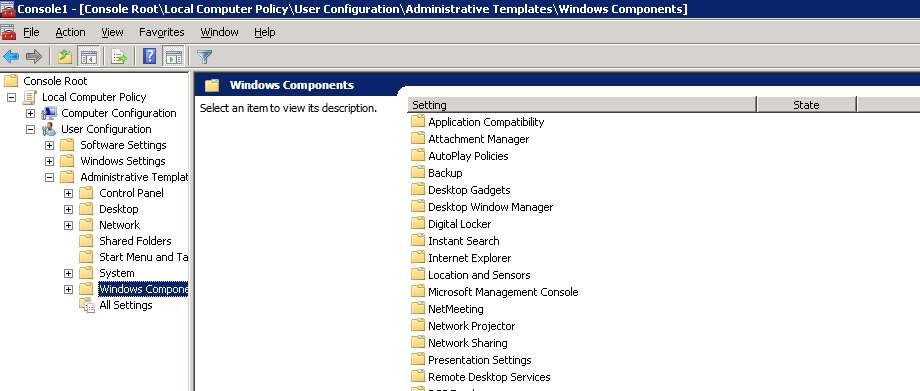
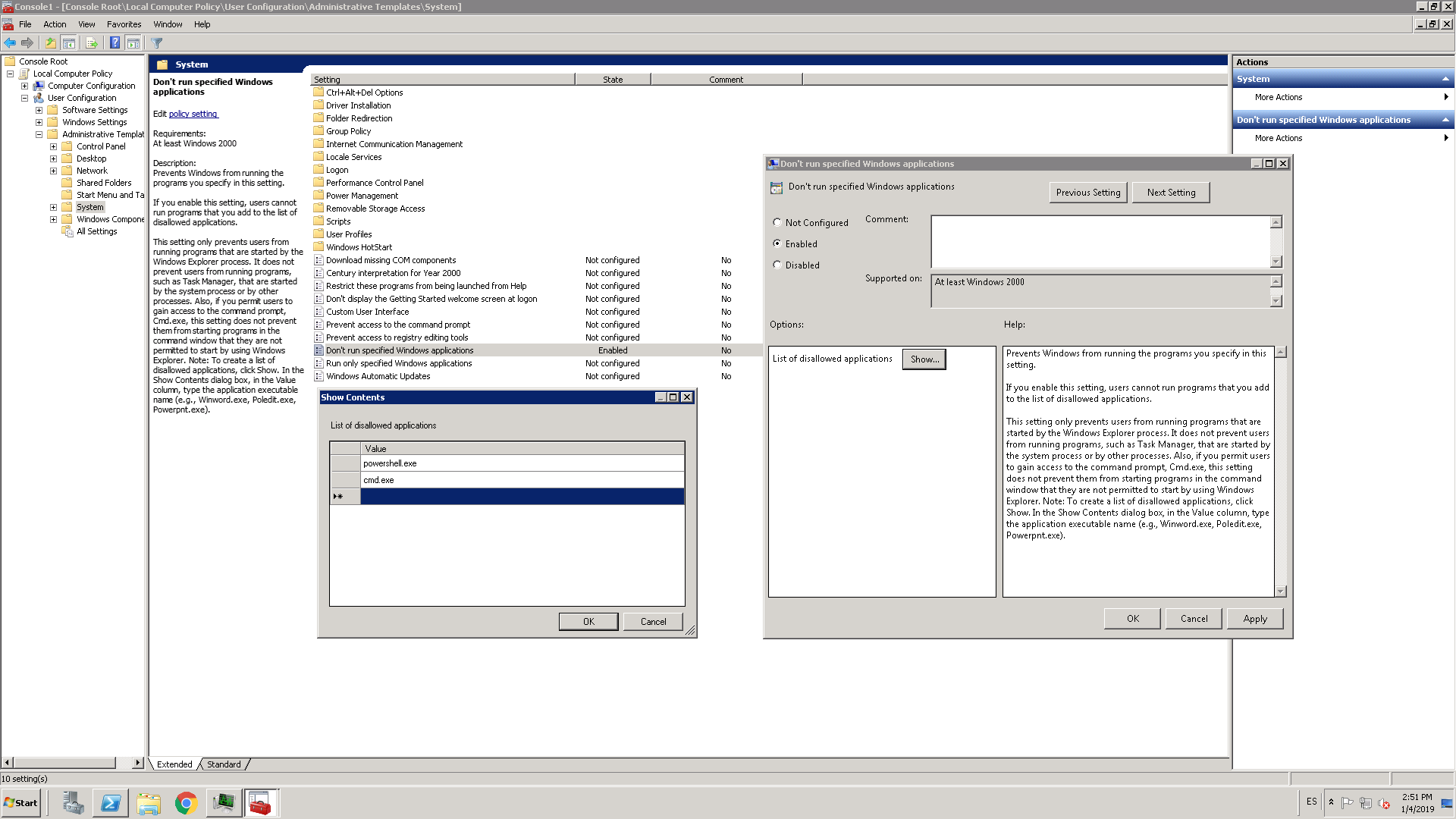


Imagen 

Imagen

Contenido

[Introducción 1](#_Toc534376935)

[Editando políticas de grupo 2](#_Toc534376936)

[Configuraciones de Windows 3](#_Toc534376937)

[Plantillas Administrativas 4](#_Toc534376938)

[Reglas Útiles 6](#_Toc534376939)

[Anexo Imágenes 7](#_Toc534376940)