Vamos a proceder a realizar nuestra pequeña guía sobre MLGPO (Multiple Local Group Policy Objects) o lo que en español significa; Múltiples Directivas de Objetos de Grupo Local.

INTRODUCCIÓN

Recordemos que una "directiva" es diferente de un "permiso". La directiva es un atributo que afecta a un usuario o grupo y que le permite (o deniega) una acción en el sistema (y no a un objeto o recurso concreto, como es el caso de los permisos). Para determinar estos derechos el sistema construye para cada usuario y/o grupo el denominado SAT (Security Access Token) el cual contiene el SID tanto del usuario, como de los grupos a los que pertenece y su propiamente dicha, lista de derechos.

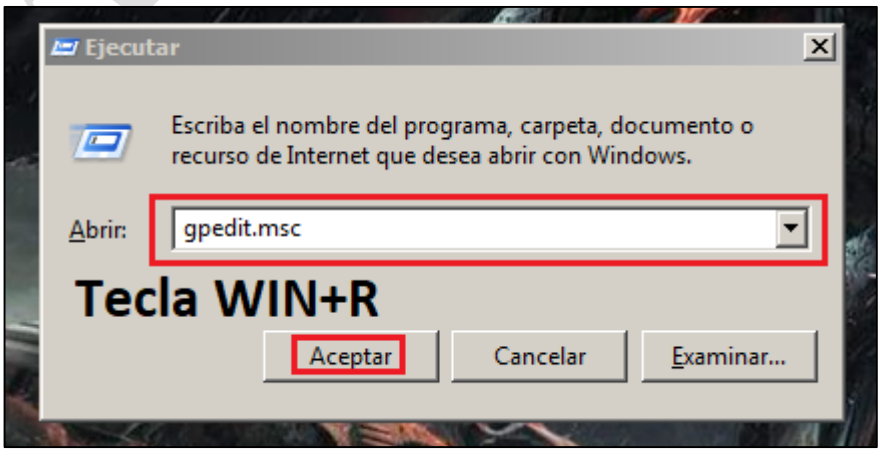
PASOS PREVIOS

Antes de realizar esta guía he preparado mi Windows 7 Profesional, es decir, le he instalado el Service Pack 1 para no tener problemas a la hora de instalación de software actual, así como su "activación con licencia" para quitarle todas las limitaciones de uso. Por otro lado, he creado un conjunto de usuarios, así como activar la cuenta de invitado, para posteriormente proceder a investigar una larga lista de directivas e ir trasteando en ellas (cambiando cosas) y comprobando su funcionamiento:

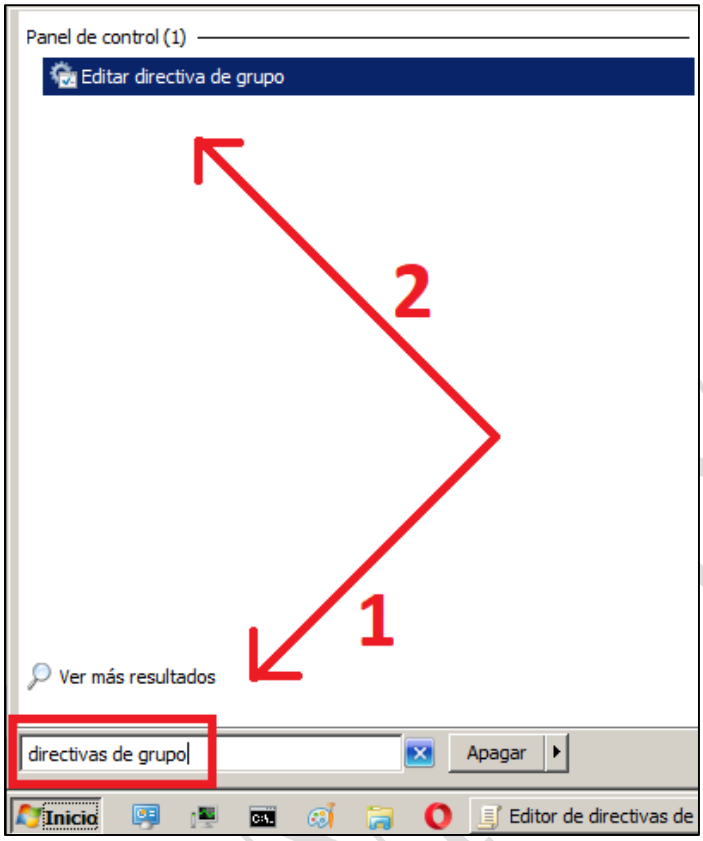
LGPO y MLGPO (Breve explicación)

Procedo a explicar 2 posibles maneras de entrar en el LGPO (general). Este es utilizado para aplicar **directivas sobre todos los usuarios y grupos locales**… **De ahí la diferencia entre uno y otro y la "M" de "Multiple" en el MLGPO**. Nosotros vamos a utilizar el 2º, para aplicar directivas a usuarios o grupos concretos y que así no afecten a todos por igual. Siendo así las formas para entrar a este primero (LGPO) es:

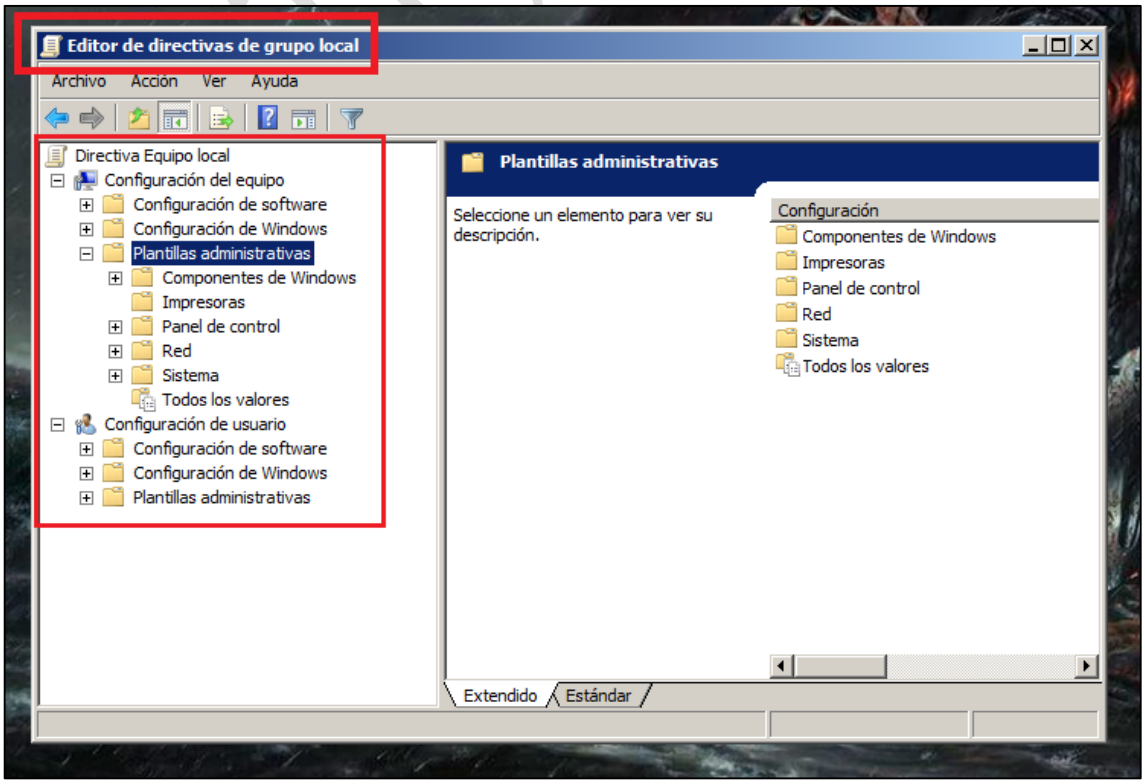
1. Pulsando la **tecla Windows+R** para iniciar la **consola "ejecutar" y aplicar "gpedit.msc"**:



2. Otra forma es directamente en el buscador del **botón inicio de Windows tecleando "directivas de grupo"** de la manera siguiente:



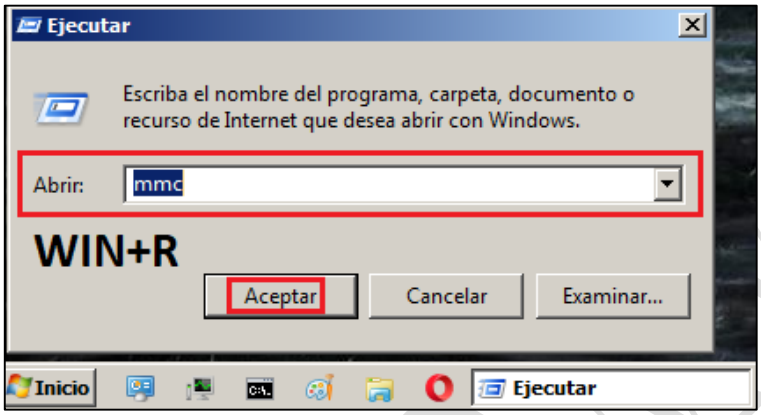
Una vez hecha 1 de estas 2 opciones estaremos en esta ventana, la consola de administración de directivas de grupo, para todos los usuarios y grupos locales:



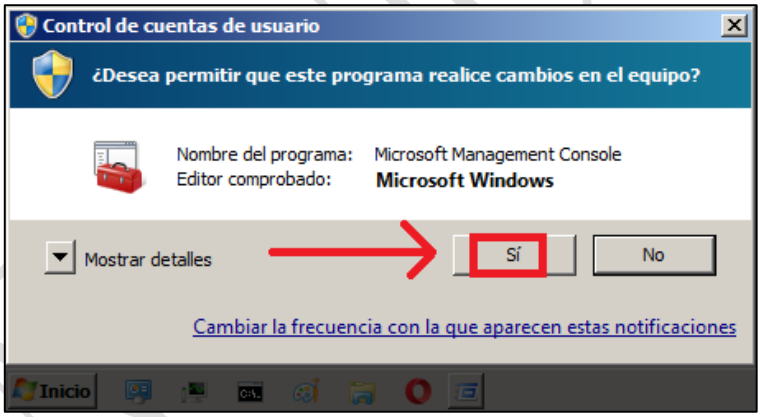
¡¡PERO ESTO NO ES LO QUE QUEREMOS!!

Como dijimos anteriormente nosotros vamos a editar el MULTIPLE Local Group Policy Objects ya que vamos a configurar directivas, algunas si, para todos los usuarios y grupos del equipo pero **OTRAS más concretas solamente para** el grupo de usuarios **No Administradores.**

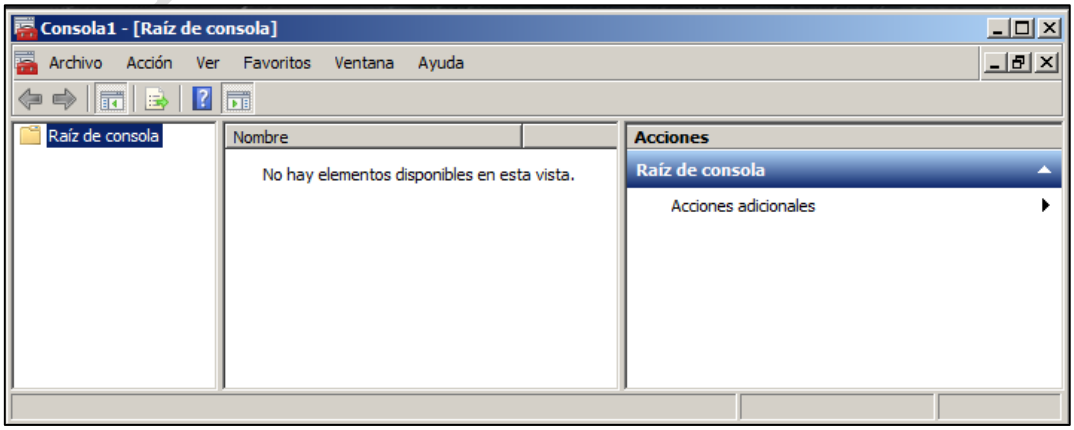
Y la forma de entrar en esta consola según nos ha explicado el profesor es tecleando **Windows+R** y una vez en dicha **consola "ejecutar" introducir "mmc"**:



Una vez hecho esto tendremos que conceder permiso para que dicha consola realice cambios en el equipo, evidentemente solo podremos hacerlo como Administrador, por tanto, pulsamos en SI:

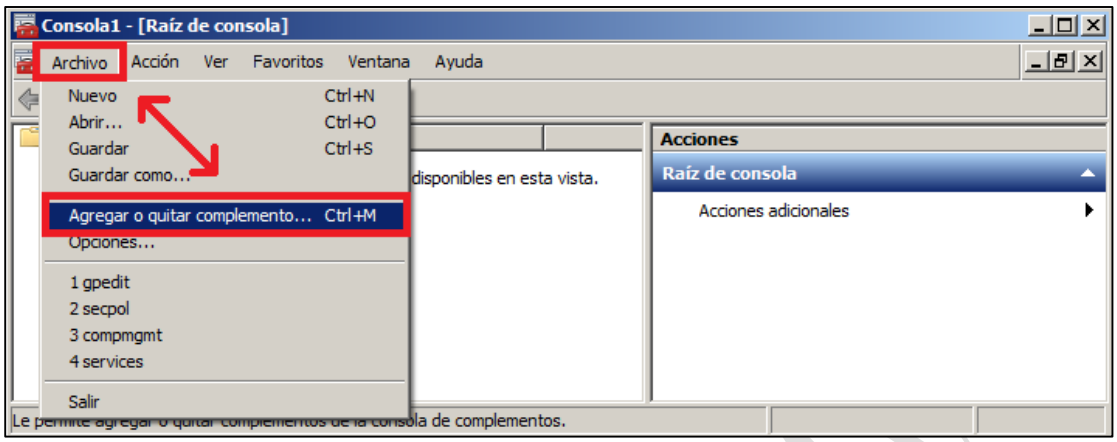


Podremos observar esta ventana (consola de MMC). En lo que respecta a esta consola podemos decir que: Microsoft Management Console (MMC) es utilizada para crear, guardar y abrir herramientas administrativas, denominadas consolas, que administran el hardware, el software y los componentes de red del Sistema Operativo – Referencia [Docs.Microsoft]:

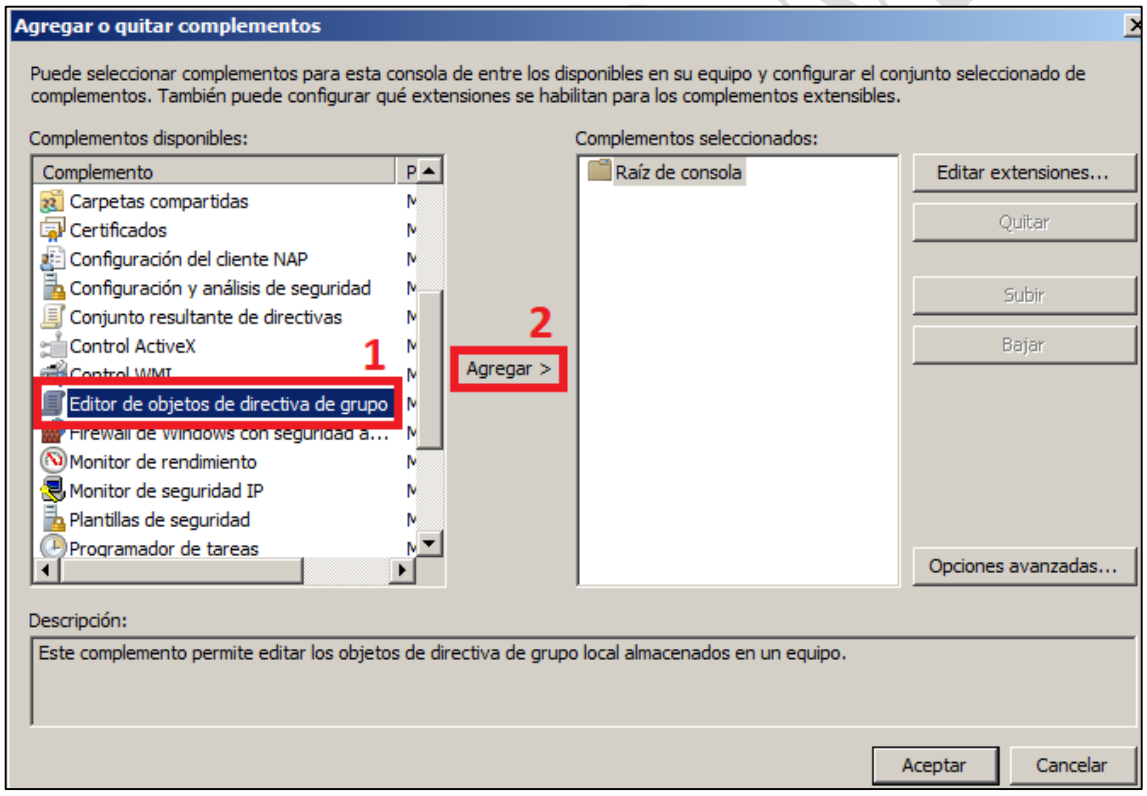


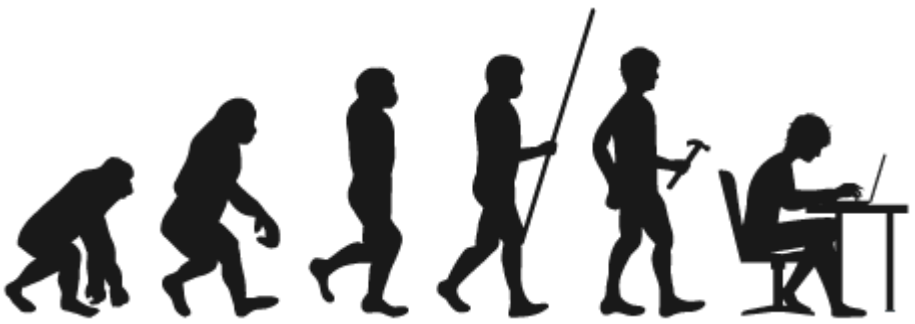
PRIMEROS PASOS A REALIZAR EN DICHA CONSOLA

1. Debemos agregar los complementos necesarios a la consola, para esto:

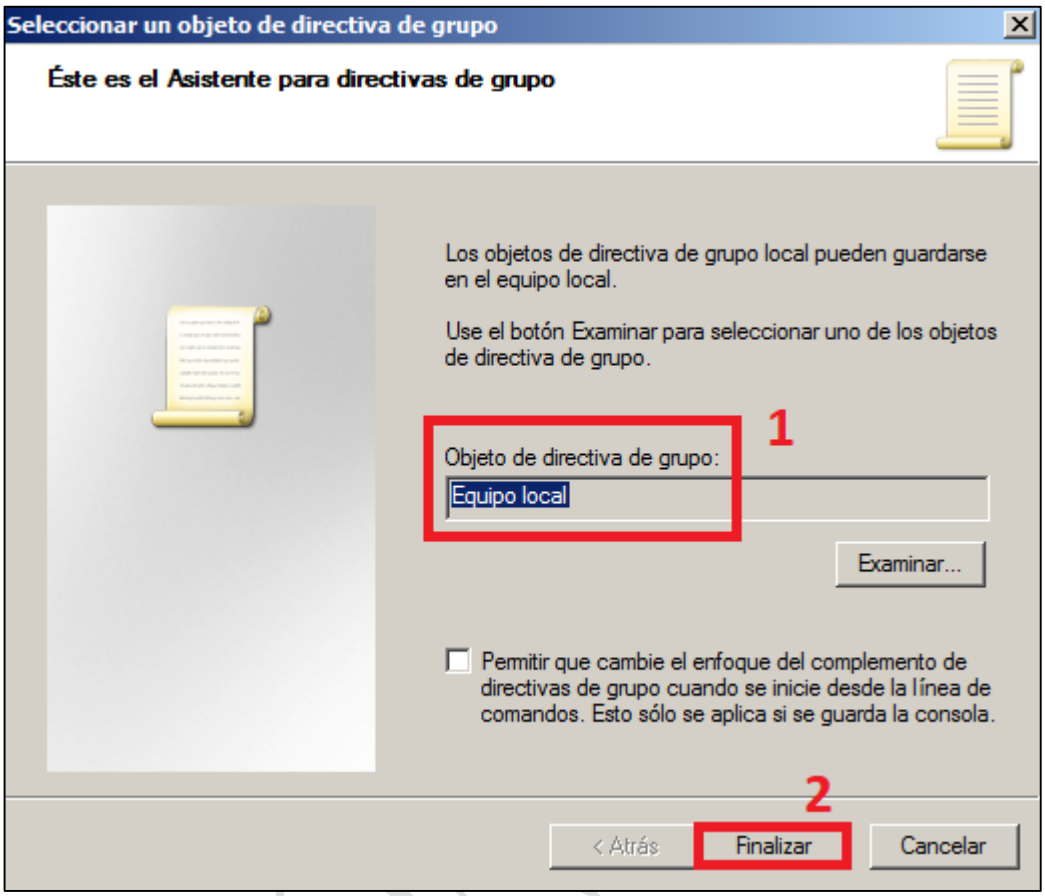


2. Seleccionamos el complemento "Editor de objetos de directiva de grupo"(1) y pulsamos en agregar(2):

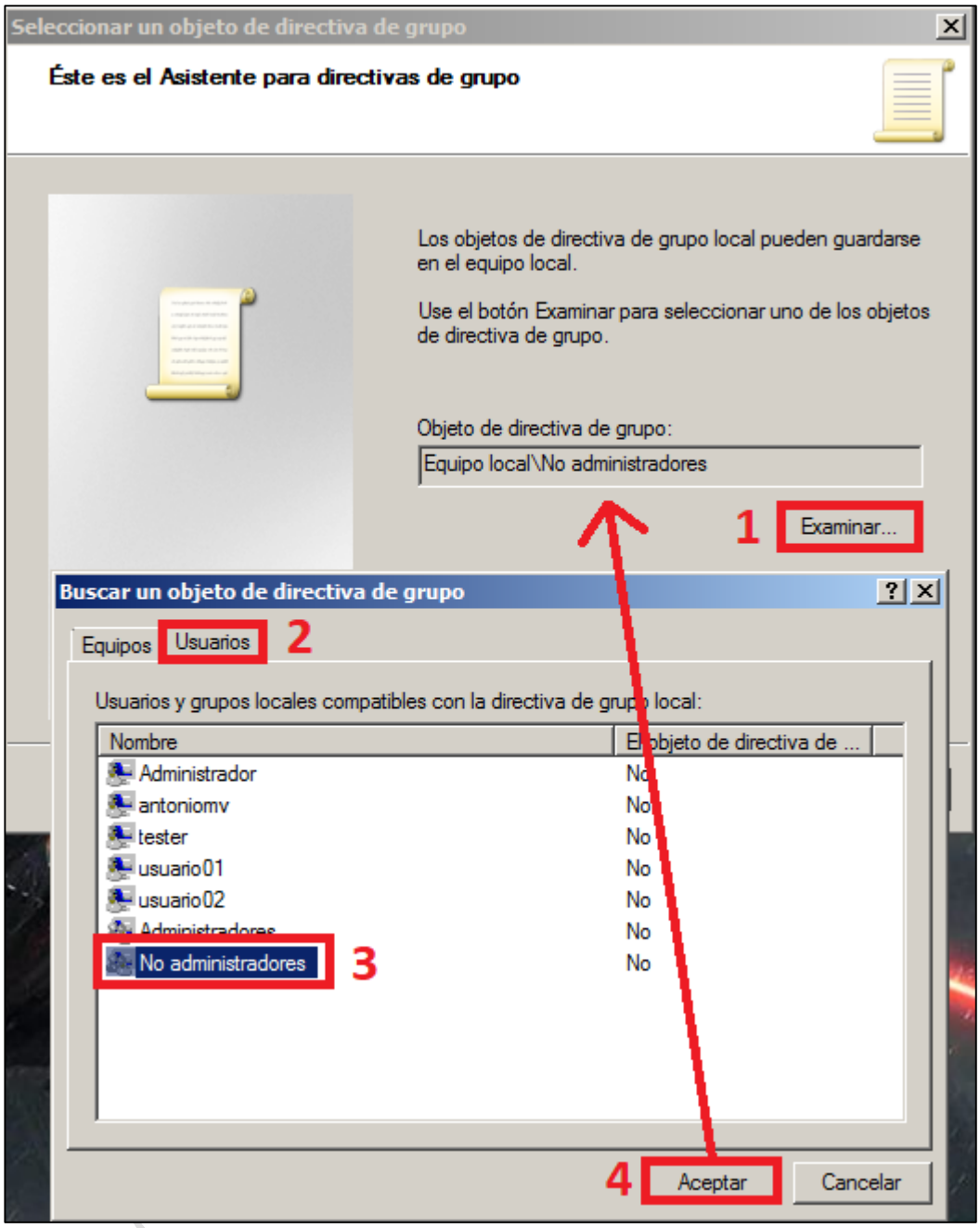




3. En la ventana que se muestra, por defecto nos aparece “Equipo local” (1) el cual nos pide la guía, por tanto, sencillamente pulsamos en finalizar (2):

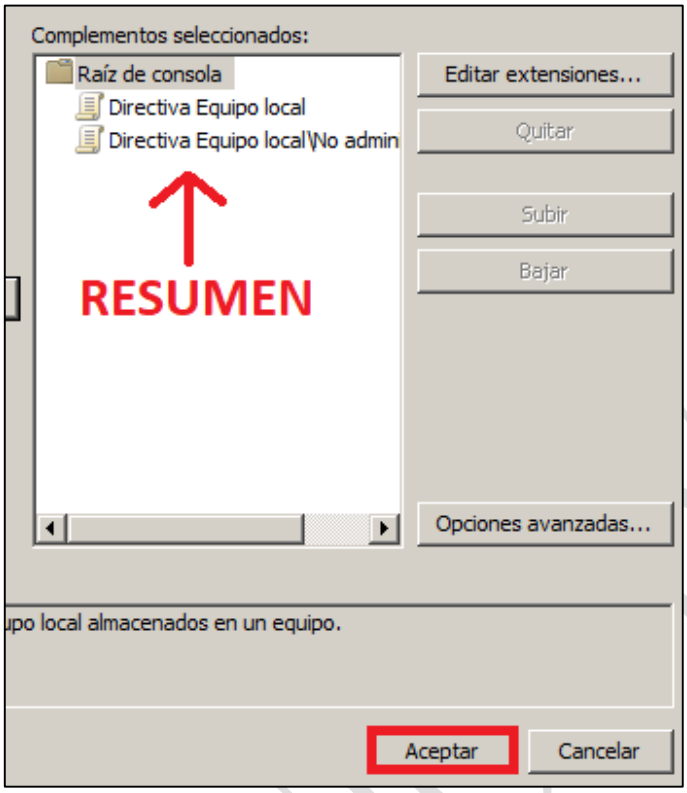


4. **Para agregar a los Usuarios no administradores** que nos pide el ejercicio realizamos la misma **operación del paso 2 pero después** efectuamos la imagen siguiente:

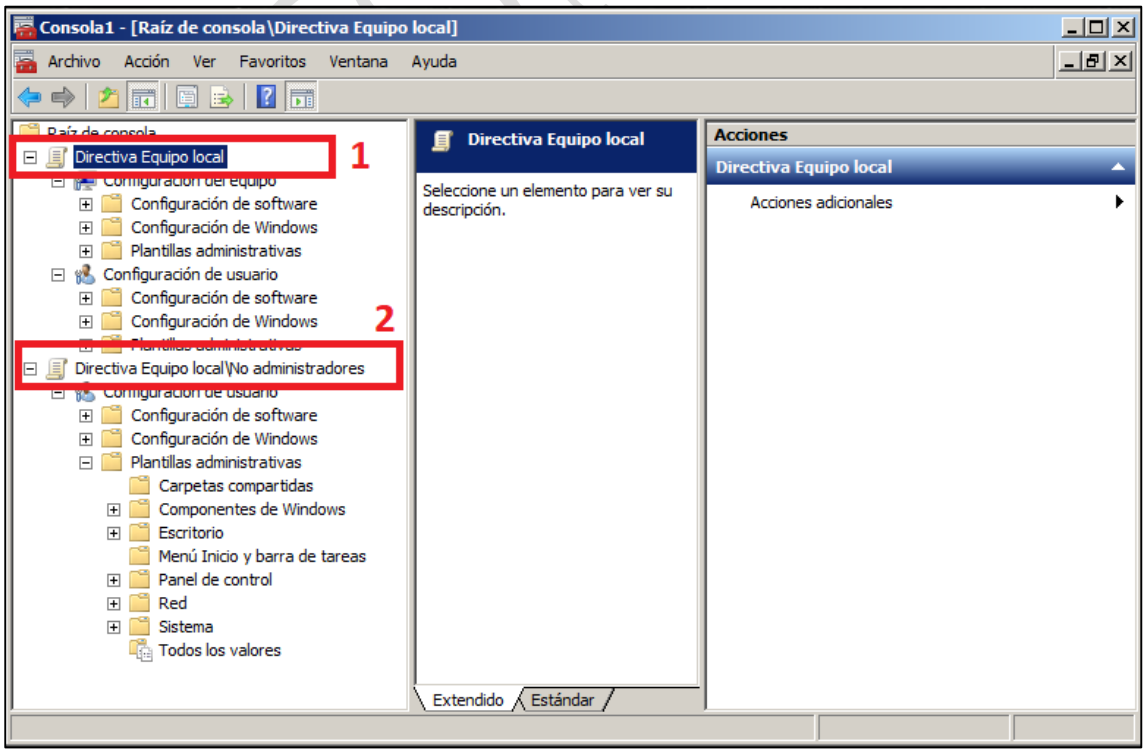


Es decir, en dicha pantalla donde antes aparecía "Equipo local" ahora debemos pulsar primero en "examinar" (1), seleccionar la pestaña "Usuarios" (2) y por consiguiente los "No administradores" (3). Seguidamente pulsamos en "aceptar" (4) para tener el resultado en el Objeto de directiva de grupo.

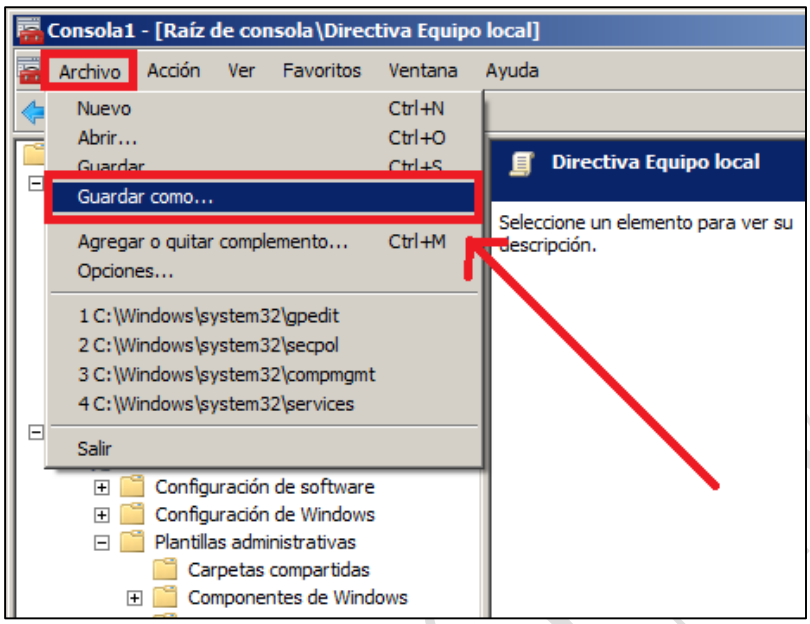
5. Una vez hecho todo esto tendremos que ver algo así en dicha consola:



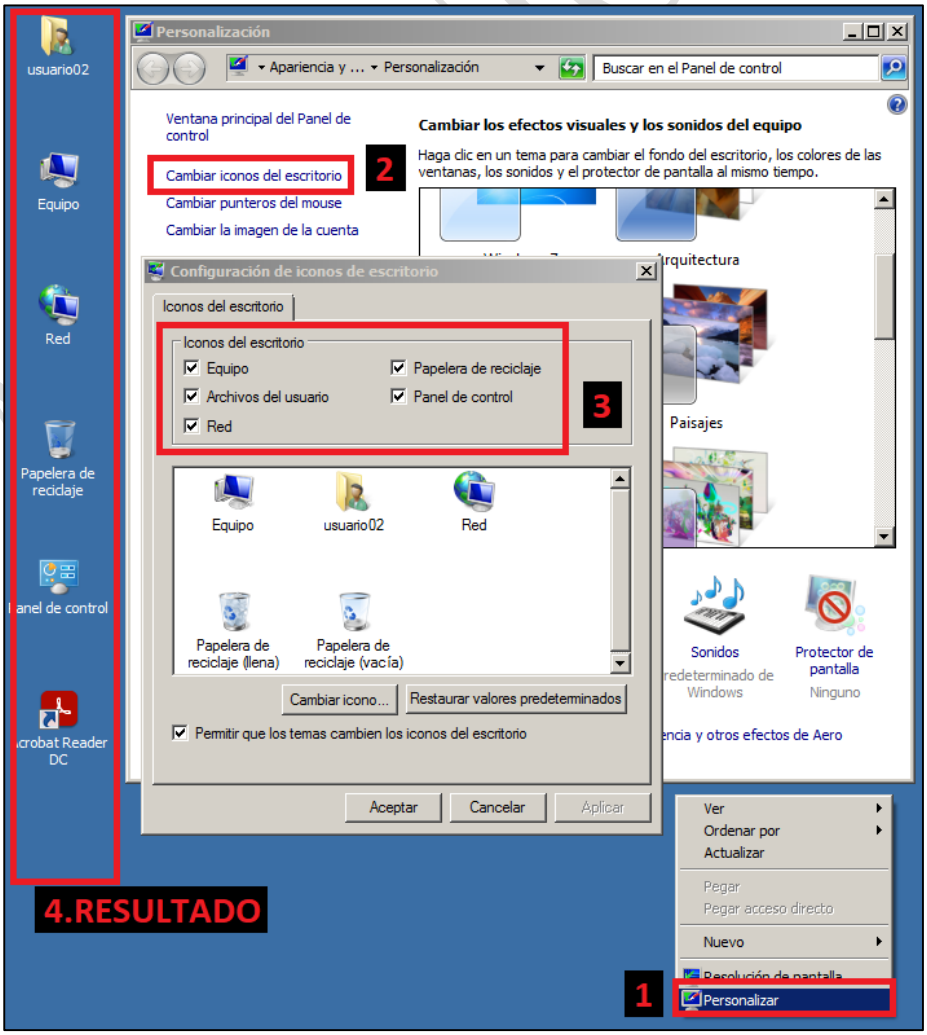
6. Siendo así pulsamos en **"Aceptar"** y por consiguiente debemos ver la consola con dichos complementos de esta manera, donde apreciamos las 2 raíces principales, es decir, Directiva Equipo local (1) y Directiva Equipo local\No administradores (2):



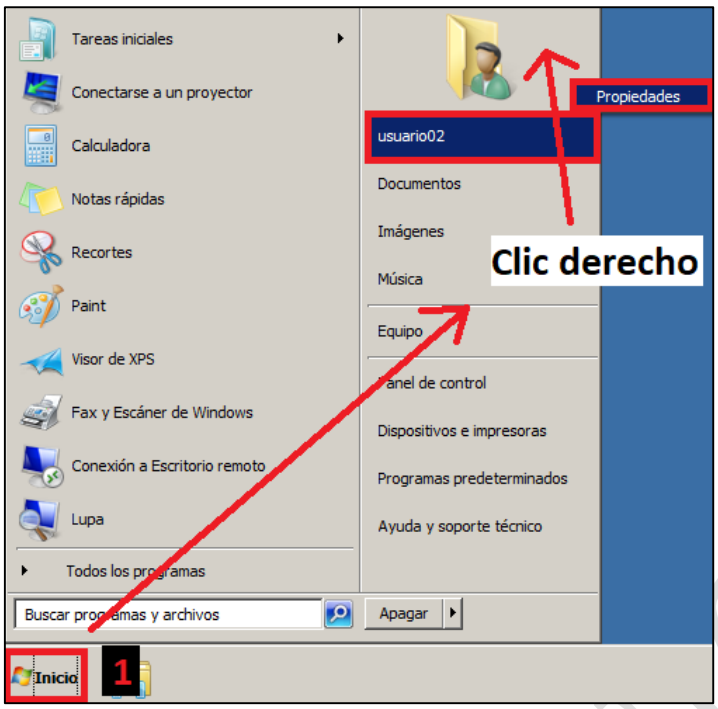
7. Llegados a este paso es **FUNDAMENTAL que NO SE NOS OLVIDE GUARDAR** dicha consola en un sitio de fácil acceso, tanto ahora como conforme vayamos haciendo cambios en ella e implantando nuevas directivas. Para ello:

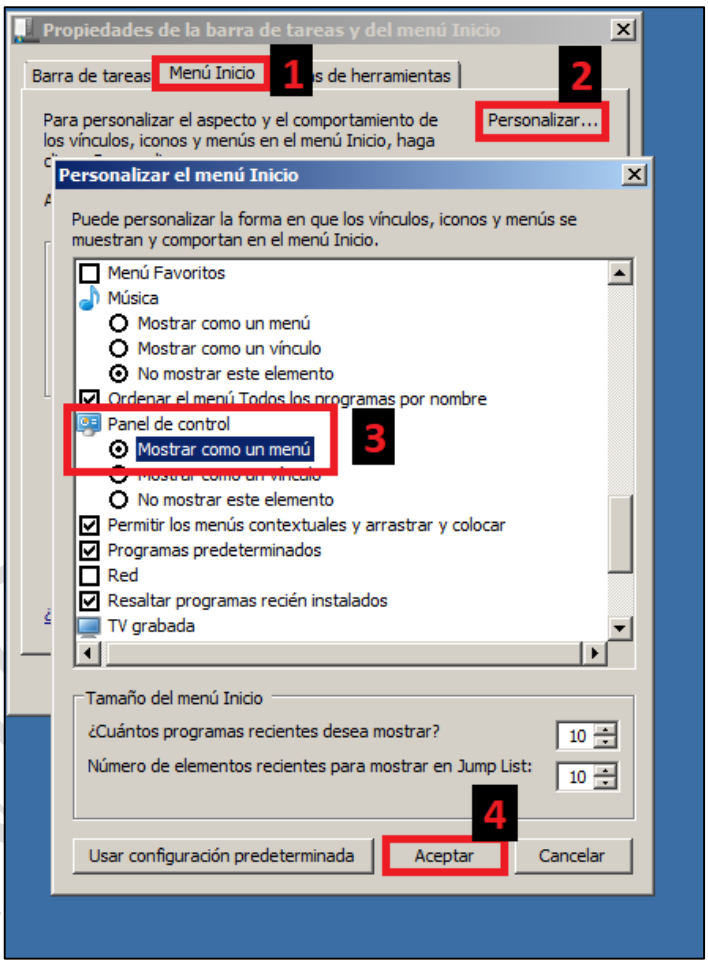


PASOS A REALIZAR EN USUARIO NO ADMINISTRADOR ANTES DE REALIZAR CAMBIOS EN LAS DIRECTIVAS (PARA PODER VISUALIZAR DICHOS CAMBIOS DESPUÉS). BREVE RESUMEN:



De esta manera según la imagen anterior veremos **que ocurre cuando cambiemos las directivas para ocultar la papelera de reciclaje u otros elementos como el panel de control** a usuarios no administradores y de igual forma en el Menú Inicio con las siguientes 2 imágenes…



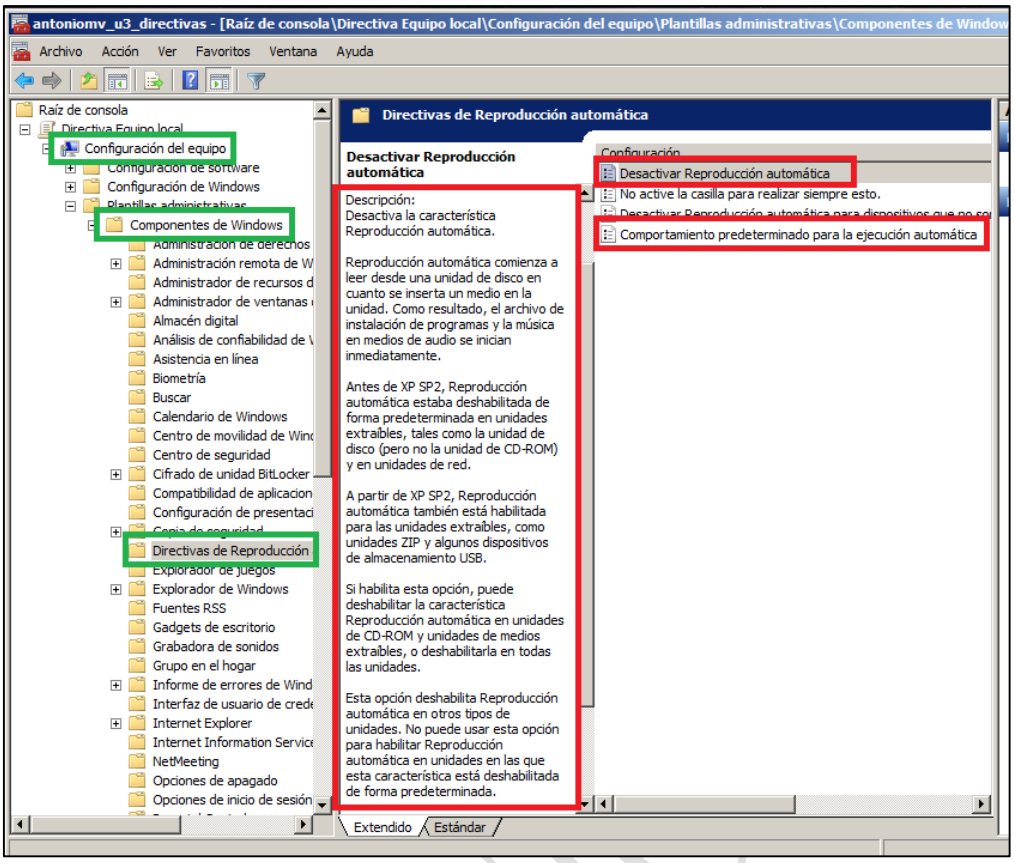


… Configurando de esta manera el Menú Inicio para mostrar, por ejemplo, **la consola "ejecutar"** o para que el Panel de Control se muestre como un menú en vez de un vínculo hacia él.

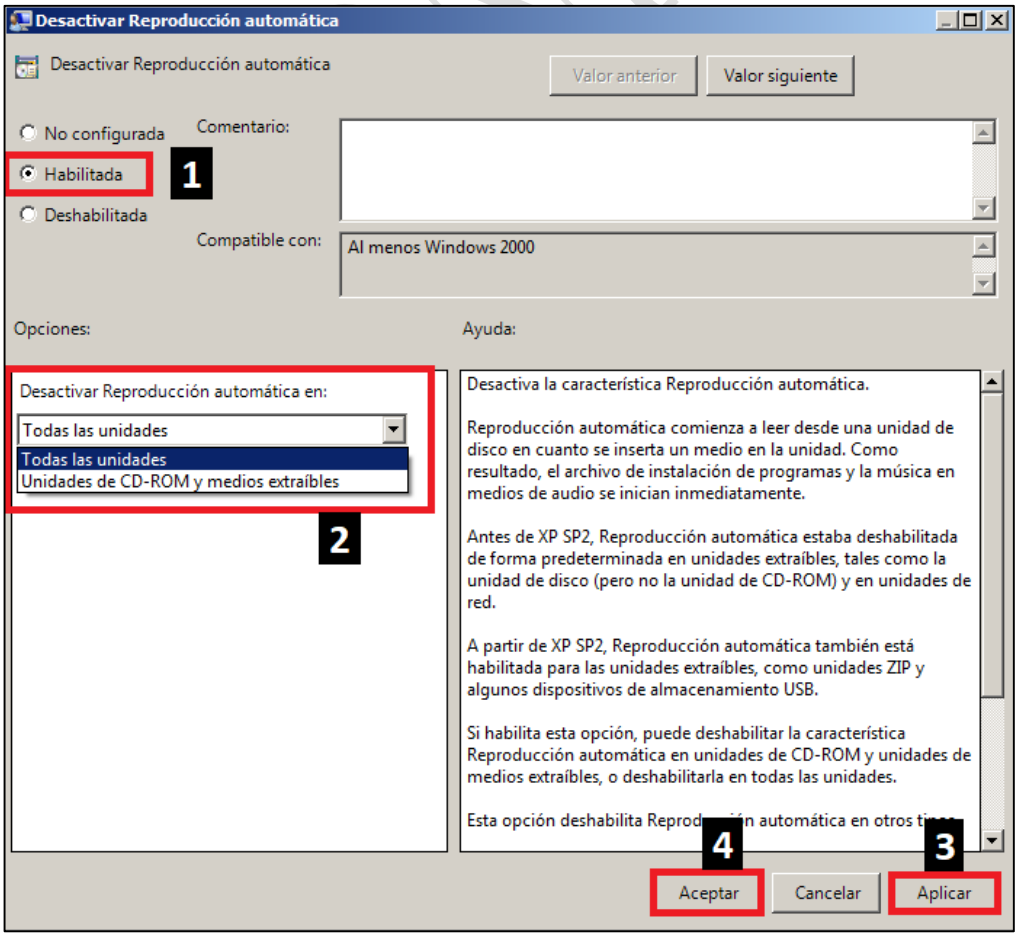
EXPLORACIÓN Y CONFIGURACIÓN DE DIRECTIVAS DE EQUIPO LOCAL Y/O DIRECTIVAS DE EQUIPO LOCAL PARA USUARIOS NO ADMINISTRADORES

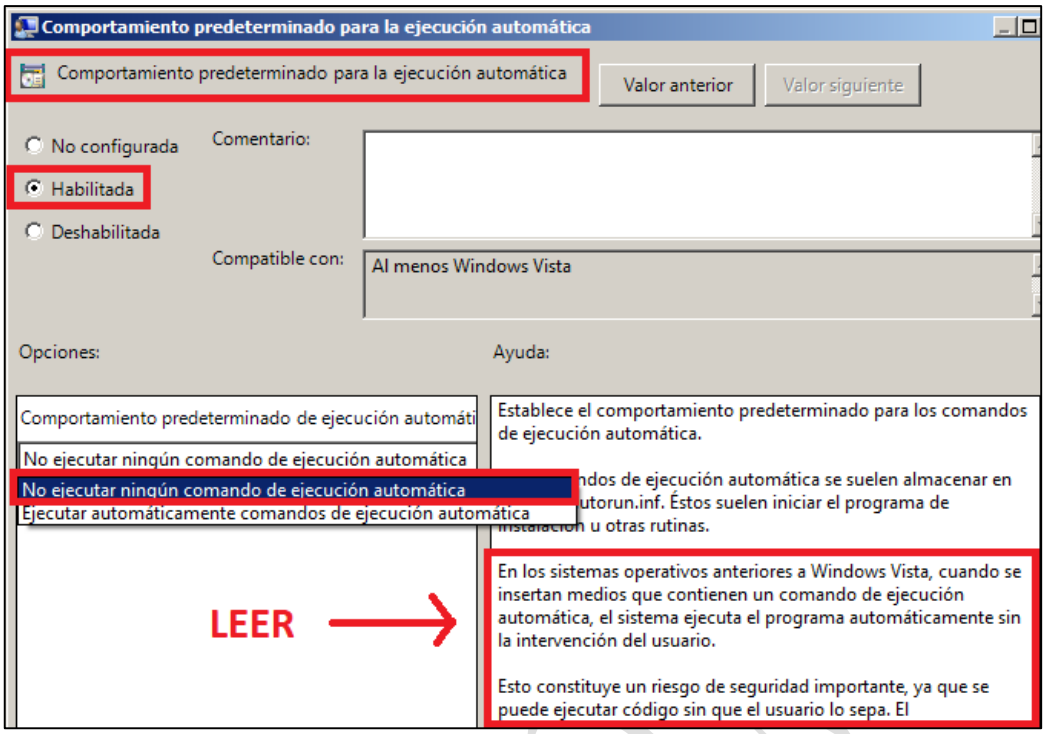
1. **Directiva de equipo Local/Configuración del equipo/Componentes de Windows/Directivas de reproducción automática:** Un administrador, a pesar de tener responsabilidad como administrador, no deja de ser una persona común. Es por esto que para esta directiva hemos decidido cambiarla en **Directiva de equipo Local/Configuración del equipo** de manera que afectará a TODOS los usuarios ya sean locales o remotos, incluyendo administradores y no administradores. ¿¿Por qué?? En la siguiente imagen podréis apreciar la descripción de dicha directiva y lo hemos decidido así porque como dije antes, un administrador no deja de ser una persona común a la que pueden chantajear o hacer extorsión para que en un supuesto caso, introduzca una unidad de PENDRIVE o CD-ROM/DVD en el equipo, lo cual puede provocar un holocausto (Véase la serie Mr. Robot con su protagonista Elliot Anderson, donde ocurre esta situación).

   Siendo así procedemos a desactivar esta y otra más relevante a lo comentado aquí. El procedimiento para estas y todas las demás será el mismo, pudiendo cambiar algún detalle:

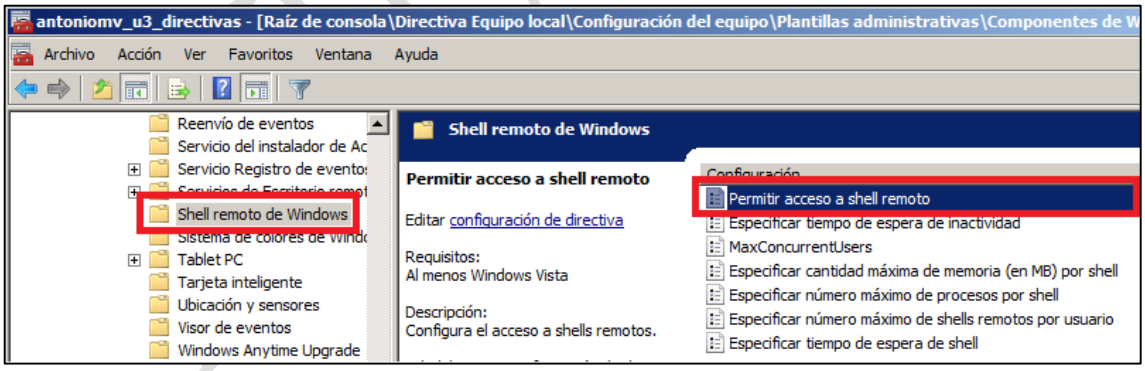


2.

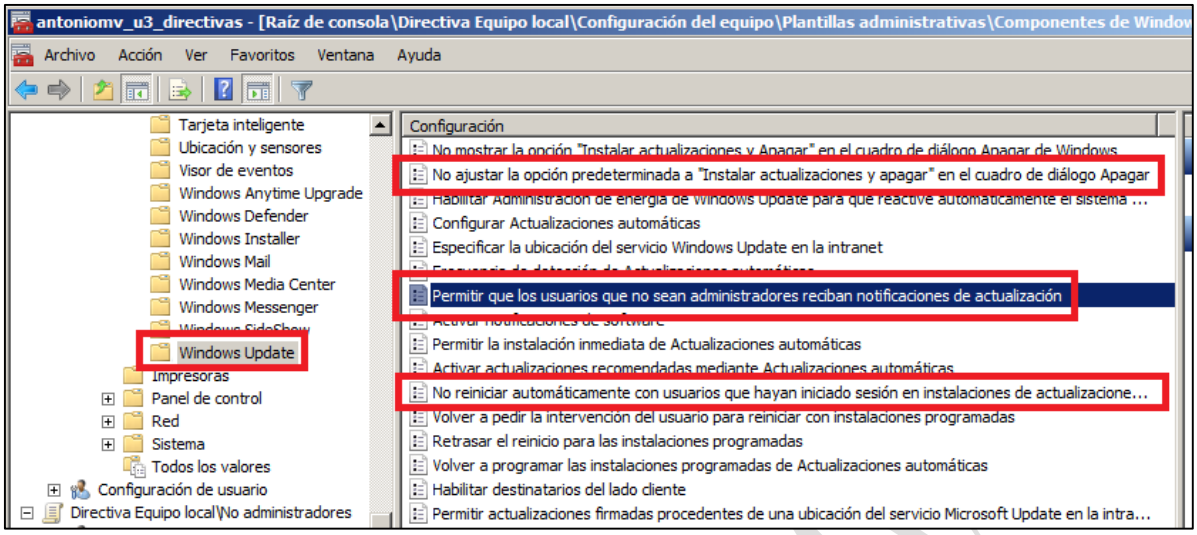




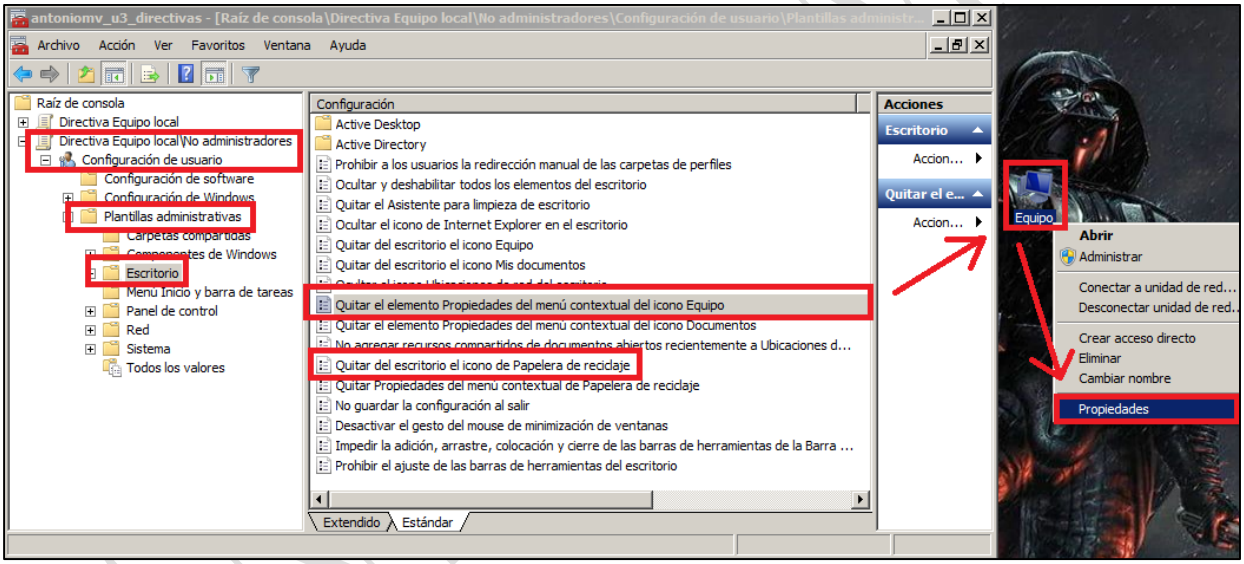
2. **Directiva de equipo Local/Configuración del equipo/Componentes de Windows/Shell Remoto de Windows:** comentando con el profesor hablamos que un usuario explicito con malas intenciones y que pudiera tener las credenciales de un usuario administrador, puede destrozar totalmente un sistema con el termina Power Shell de Windows. Es por esto que voy a deshabilitar esta directiva para todo el equipo y asegurar un posible problema menos que resolver:



3. **Directiva de equipo Local/Configuración del equipo/Componentes de Windows/Windows Update:** En este apartado voy a deshabilitar y configurar algunas directivas de actualizaciones de Windows ya que muchas de estas pueden causar problemas en el equipo (es bueno informarse antes de instalarlas cuando las publican, ya que podrían causarnos un problema). De hecho, se dice que una actualización o cambio debe probarse siempre 1º en un entorno de prueba antes de sacarlo al mercado. Con Windows 10 esto no ocurre, digamos que todos los usuarios somos beta tester de sus actualizaciones (y a muchísima gente esto le ha provocado muchos quebraderos de cabeza con objetos que desaparecen, etc…) Es por esto que vamos a deshabilitar las actualizaciones para usuarios no administradores.



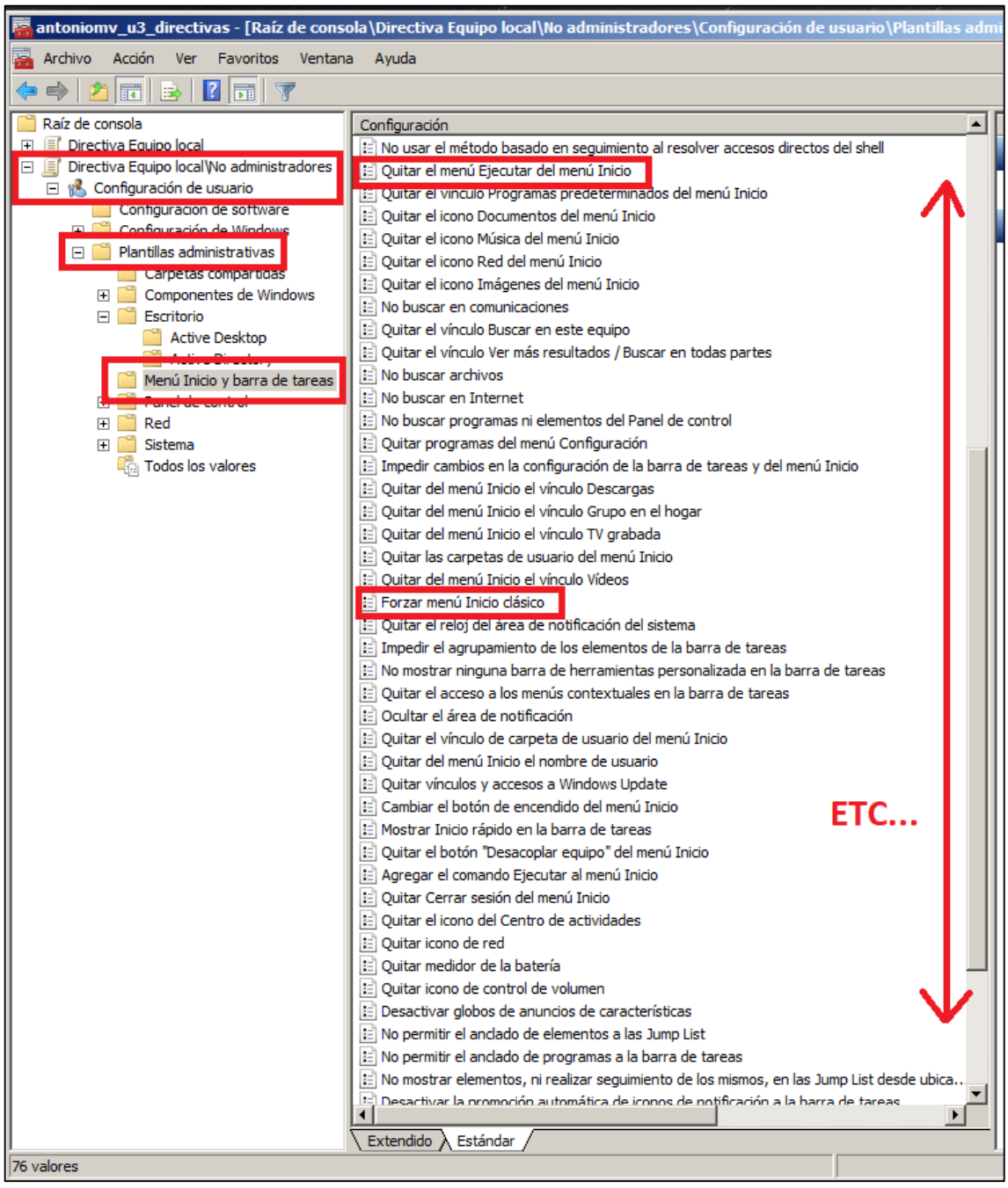
A partir de aquí desde: Raíz de consola\Directiva de equipo Local\No Administradores\Configuración de usuario\Plantillas administrativas



Configuración de directivas de escritorio para usuarios no administradores: en dicha imagen voy a deshabilitar 2 directivas. Una es la de mostrar propiedades en el menú contextual del icono "equipo" y la otra es "ocultar papelera de reciclaje". De esta manera un usuario que elimine archivos no podrá borrarlos definitivamente al no tener acceso a la papelera de reciclaje pero por tanto, tampoco podrá restaurarlos así que necesitará la ayuda de un usuario administrador. Respecto a las propiedades del icono "equipo" es por temas de seguridad, ya que dicha opción te puede llevar a opciones más complejas de configuración del equipo.

<u>Configuración de directivas de Menú Inicio y barra de tareas</u> para usuarios no administradores:
Procedo a deshabilitar opciones como:

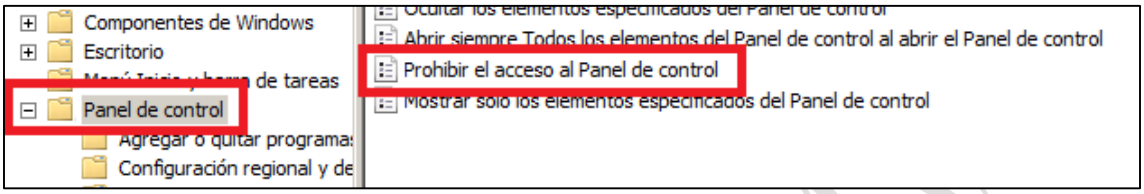
- Quitar el vínculo Juegos del menú inicio.
- Quitar el comando Ejecutar del menú inicio.
- Forzar Menú Inicio Clásico (para optimizar el rendimiento)
- Quitar vínculos y accesos a Windows Update.
- Desactivar vistas en miniatura de la barra de tareas (para optimizar el rendimiento)
- Y algunas más…

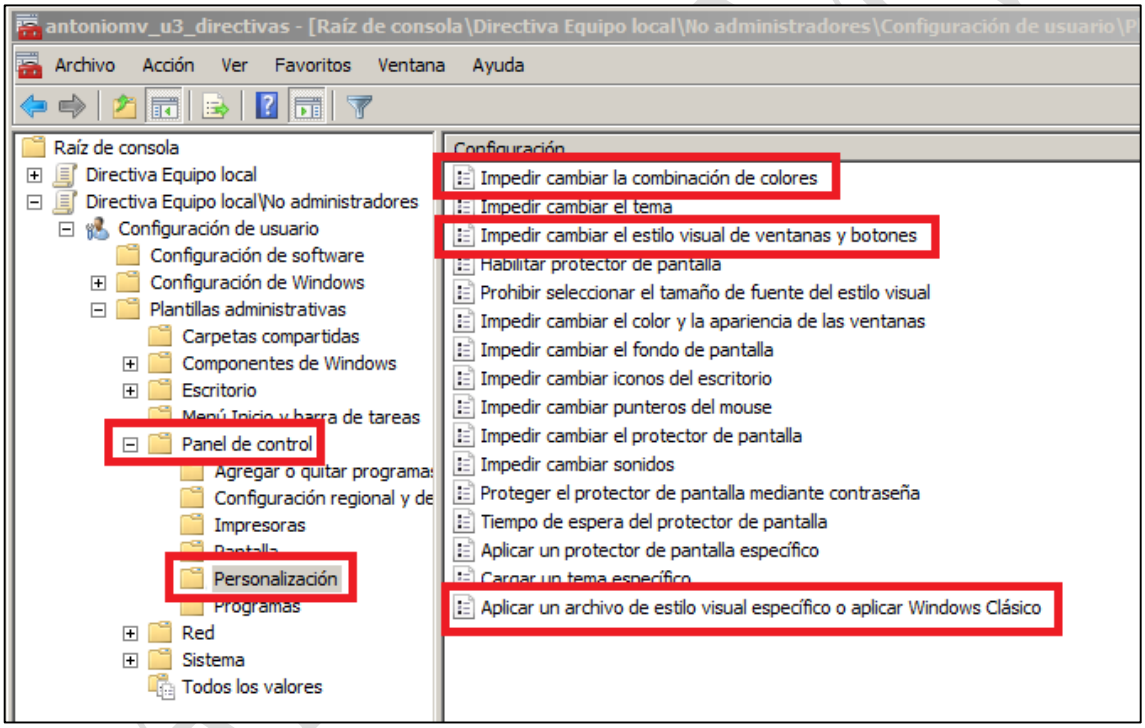


<u>Configuración de directivas de Panel de Control</u> para usuarios no administradores:

Procedo a deshabilitar algunas directivas como:

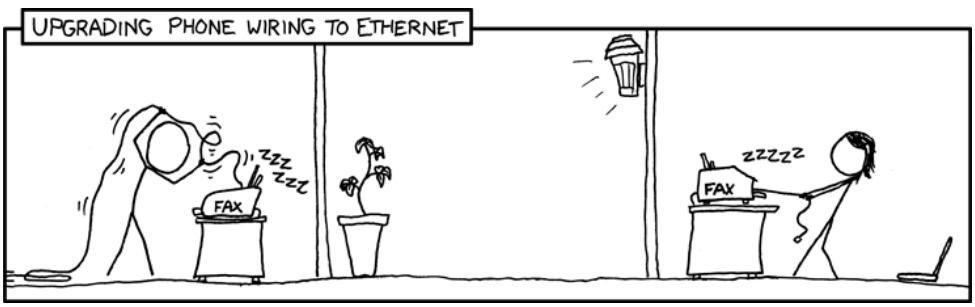
- Prohibir el acceso al Panel de control.
- En Personalización: impedir cambiar la combinación de colores.
- En Personalización: impedir cambiar el estilo visual de ventanas y botones.
- En Personalización: aplicar un archivo de estilo visual especifico o aplicar Windows Clásico (por optimización ya que estamos trabajando con una máquina virtual).
- En Programas: ocultar "Características de Windows".

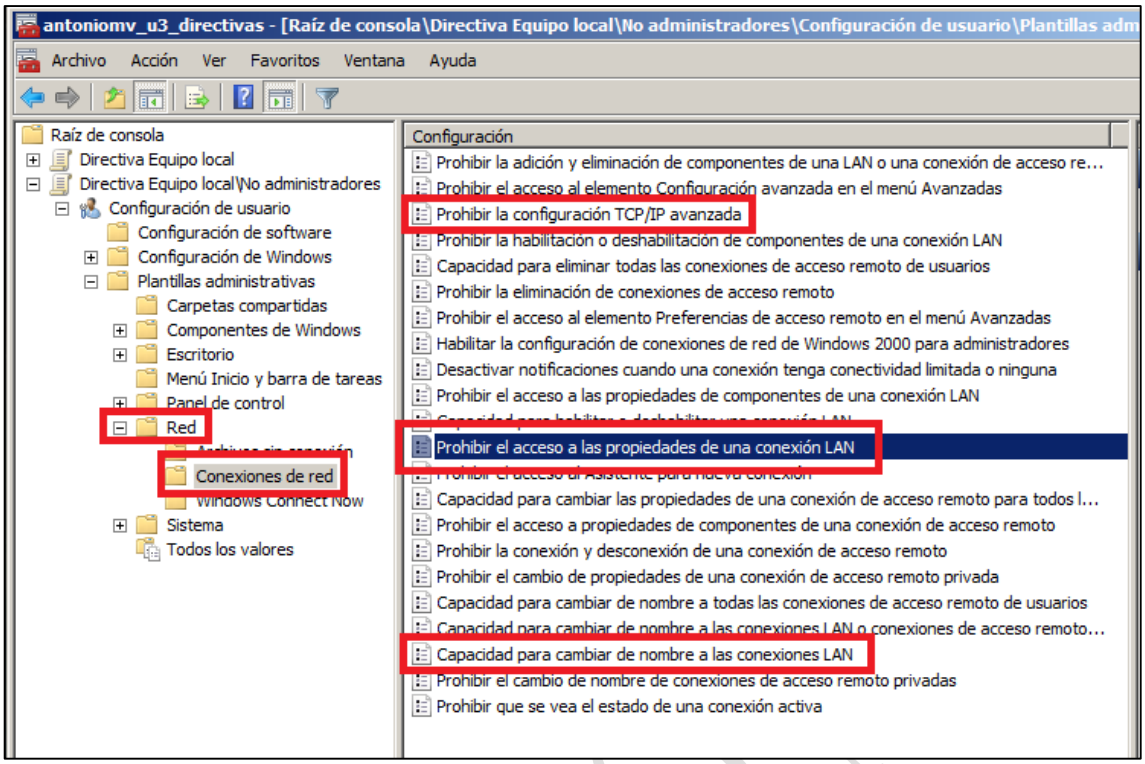




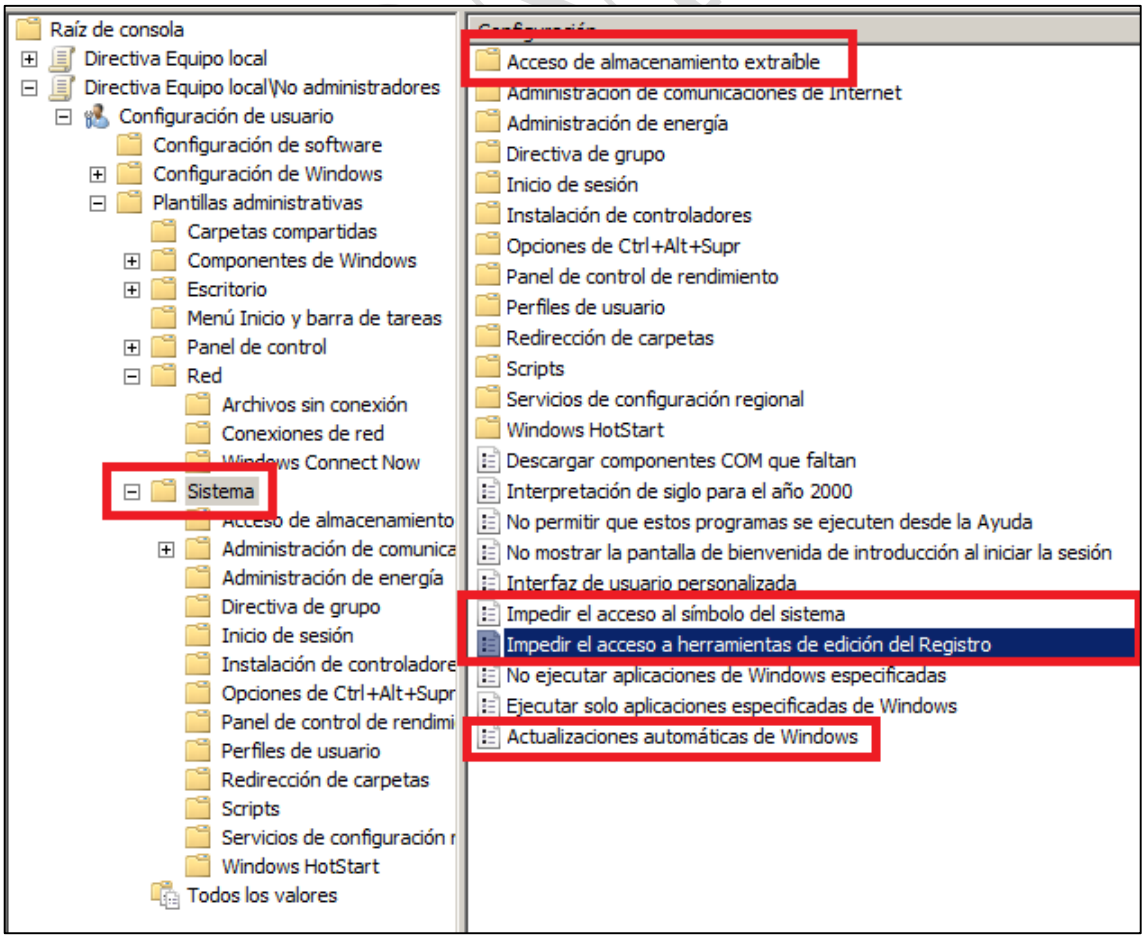
<u>Configuración de directivas de Red</u> para usuarios no administradores:

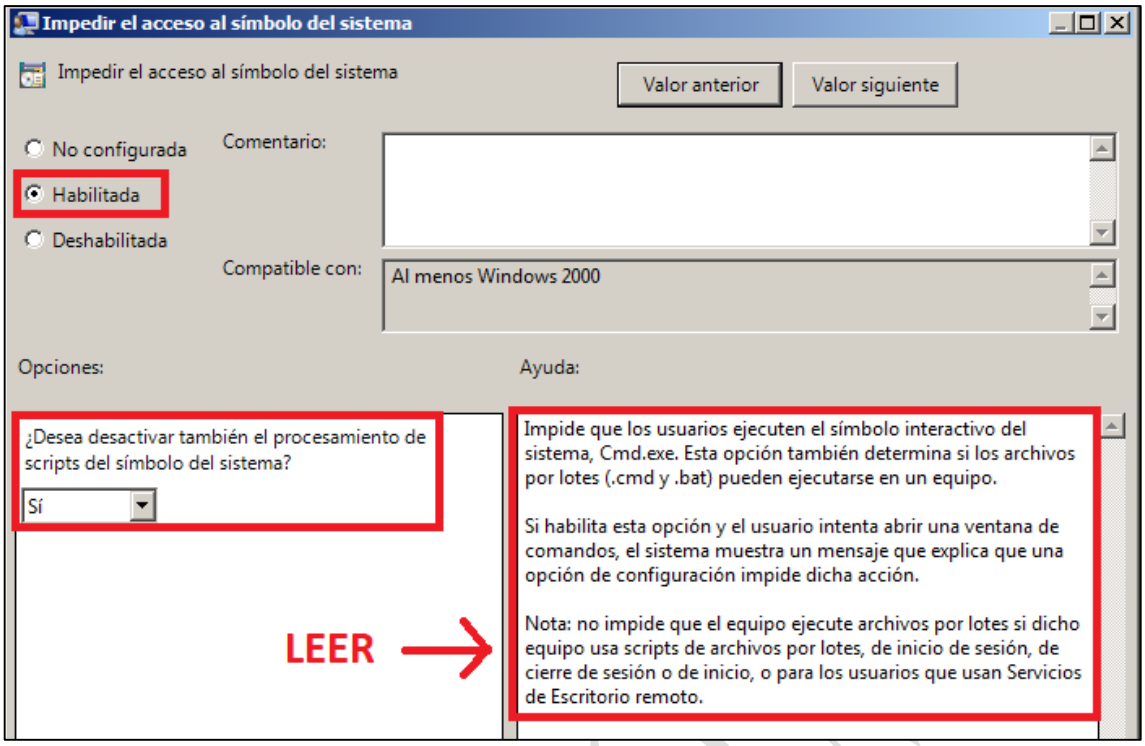
Procedo a deshabilitar ciertas características de Red para que usuarios no administradores no puedan modificar conexiones LAN ya que para un administrador es un trabajo bastante laborioso el configurar todos los equipos de una red, como para permitir que usuarios sin el debido conocimiento toquen estos parámetros:





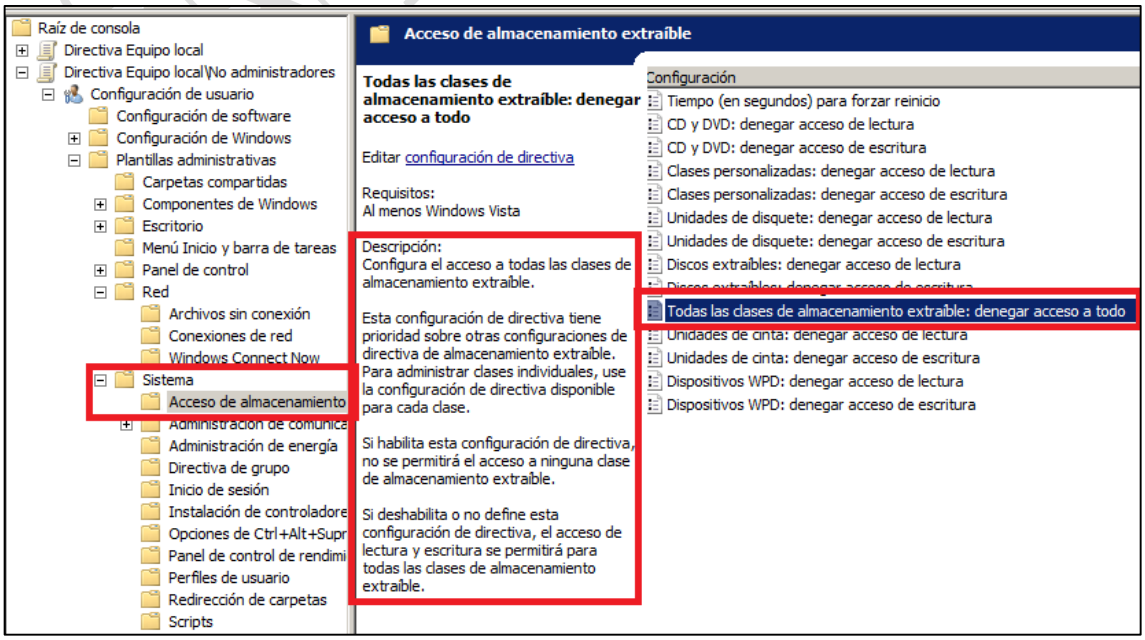
<u>Configuración de directivas de Sistema</u> para usuarios no administradores (IMÁGENES Y BREVE EXPLICACIÓN)



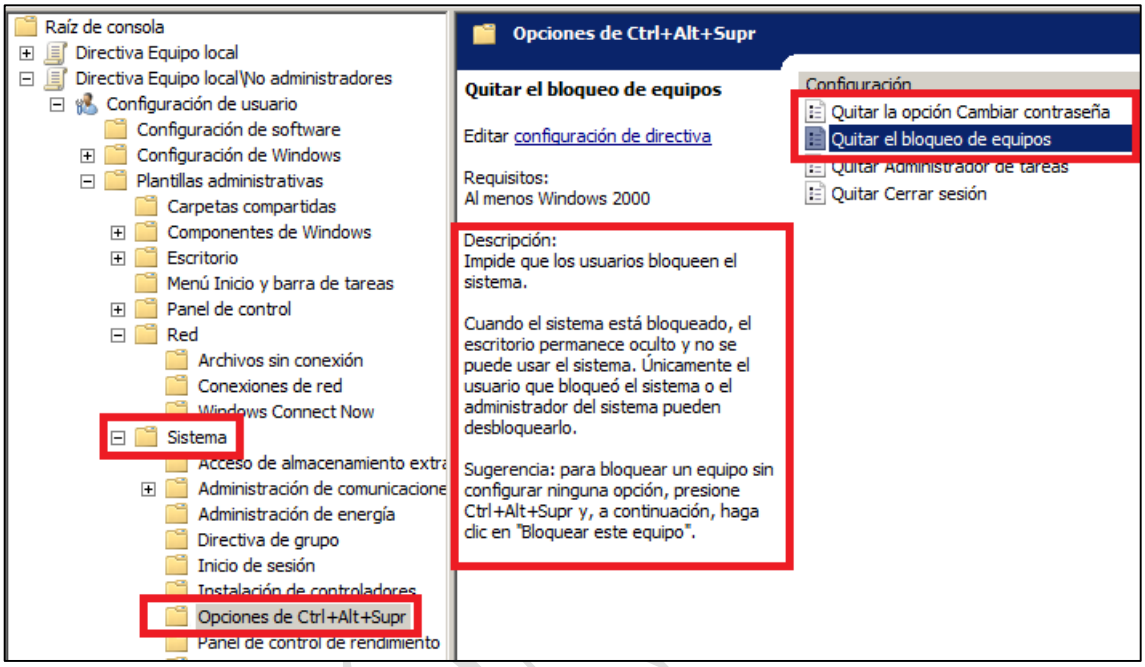


En las 2 imágenes anteriores podemos ver que he deshabilitado ciertas opciones como:

- **Impedir el acceso al símbolo del sistema:** El CMD es una herramienta delicada si no se trabaja con los conocimientos adecuados así que he prohibido su utilización en el sistema para usuarios no administradores.
- **Impedir el acceso a herramientas de edición del Registro:** como la anterior, el Registro de Windows es todavía más peligroso. Por este motivo también he prohibido su acceso a usuarios básicos.
- **Actualizaciones automáticas de Windows:** como ya dijimos anteriormente en la página 11 de este documento, una mala actualización puede provocar errores graves en el sistema así que he limitado esta opción solamente a los usuarios administradores.



→Sistema\Acceso de almacenamiento extraíble: como vemos en la imagen anterior y siendo algo comentado con el profesor en clase, un usuario que meta un pendrive con archivos personales, música, etc… ¡¡PUEDE LIARLA PARDA!! Y contagiar toda la red con un virus, troyano u otro tipo de ataque. Anteriormente mencionamos en otro apartado una situación parecida en una conocida famosa serie de Televisión donde ocurre exactamente eso con un CD-ROM y un empleado extorsionado (Véase la serie Mr. Robot con su protagonista Elliot Anderson, donde ocurre esta situación). Por este motivo he bloqueado el acceso a todas las unidades de almacenamiento extraíbles.

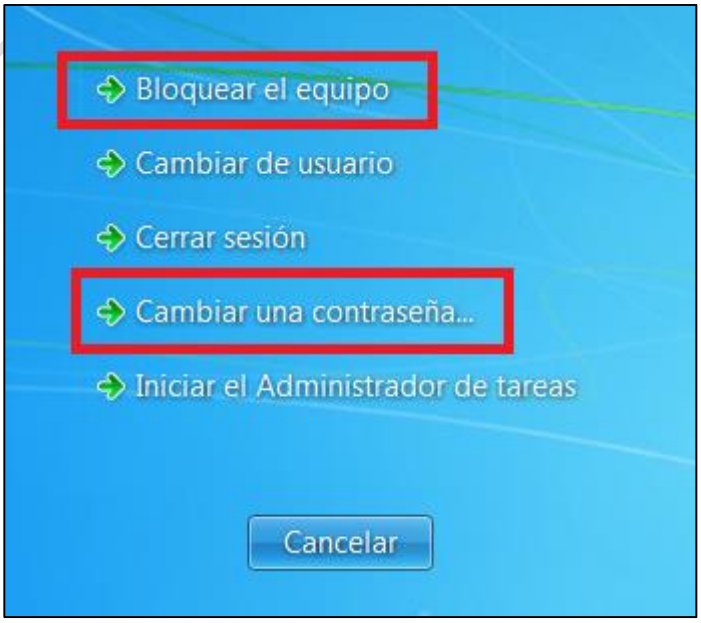


↑↑ Sistema\Acceso de almacenamiento extraíble ↑↑ : Otra opción interesante en Sistema es la de las opciones que aparecen cuando se pulsa Ctrl+Alt+Supr y me ha parecido curioso poder desactivar las opciones de "cambiar contraseña" y "quitar el bloqueo de equipo":

De esta manera cuando veamos todos los cambios realizados en un usuario no administrador, al pulsar dichas teclas no aparecerán estas 2 opciones aquí a la derecha

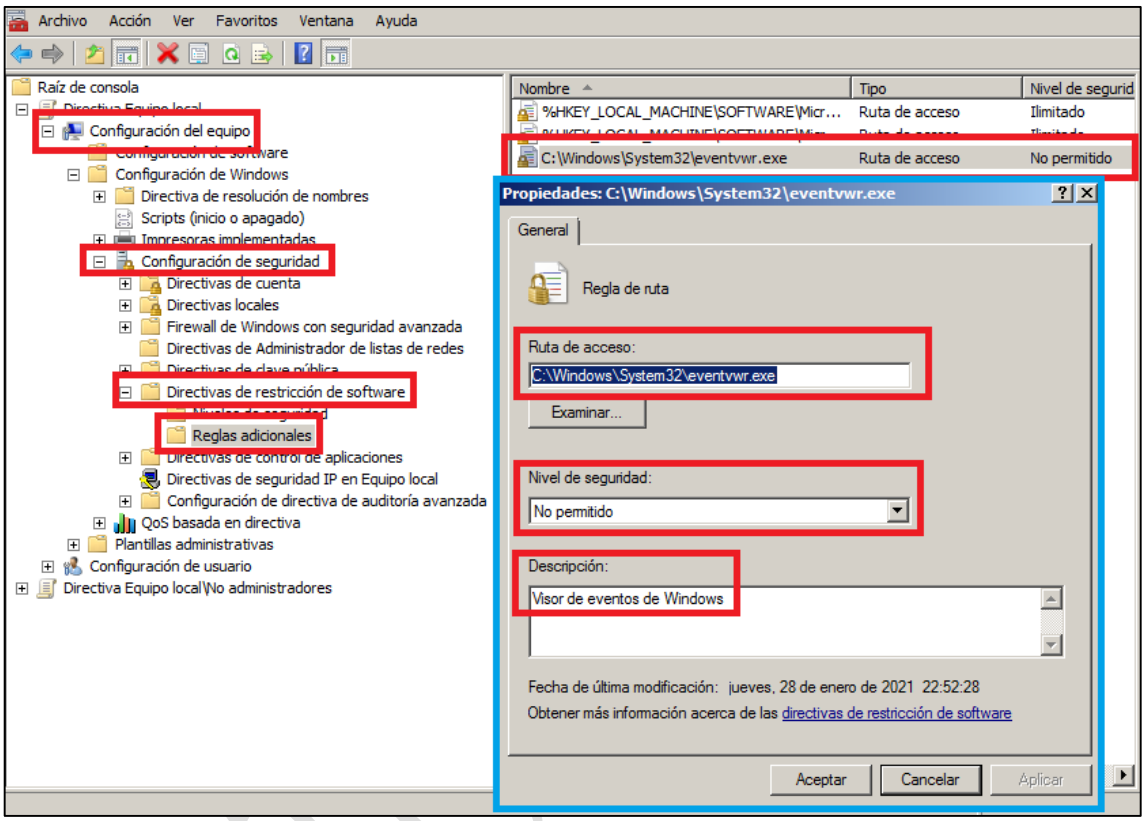
→→

Además de otras opciones como ver la papelera de reciclaje en el escritorio, tener acceso al panel de control y diversas opciones más que hemos restringido para dichos usuarios.



Por último la última directiva que vamos a cambiar para este proyecto (entre tantísimas otras, ya que las directivas de Windows son un mundo inmenso por explorar) será una restricción de software (aplicación), en este caso, el visor de eventos de Windows, para que un usuario no administrador no pueda usarla. Para ello, nos hemos ido de nuevo a...

Directiva de equipo Local\Configuración del equipo\Configuración de seguridad\Directivas de restricción de software\Clic secundario → Nueva\Reglas adicionales\Nueva ruta de acceso:



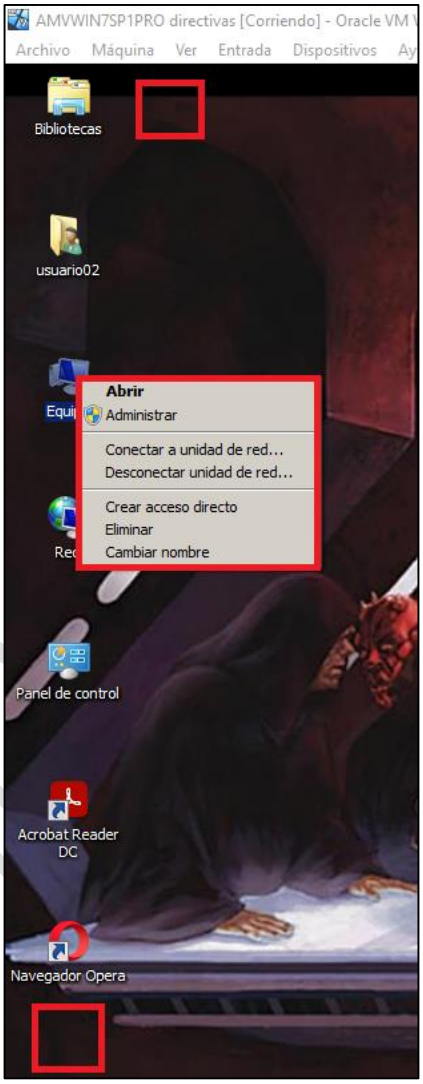
Como tal, hemos puesto la ruta de acceso a dicha aplicación y en nivel de seguridad que por defecto esta puesta para "usuario básico" es decir, no administrador, hemos seleccionado "NO PERMITIDO". En la descripción podemos ver la aplicación seleccionada.

DE AQUÍ EN ADELANTE, VAMOS A LOGUEARNOS CON USUARIO02, EL CUAL NO ES ADMINISTRADOR Y VAMOS A COMPROBAR TODOS LOS CAMBIOS REALIZADOS:

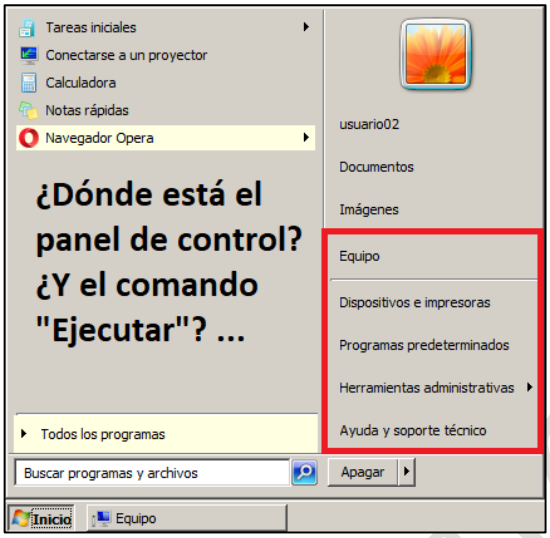
- Papelera de reciclaje oculta.
- Ocultar las propiedades en el menú contextual del icono Equipo
- Acceso al panel de control no permitido.
- Acceso a CMD y Registro de Windows prohibido.
- Denegación de ejecución automática de dispositivos extraíbles como CD-ROM's o imágenes ISO.
- Denegación de acceso a dispositivos extraíbles como unidades de PENDRIVE.
- Ocultar el comando Ejecutar del menú inicio.
- Prohibir la configuración de redes LAN.
- Prohibir la ejecución del visor de eventos (ESTE NO FUNCIONA, NO LO HICE BIEN ☹)
- Etc… etc… etc…

INTERFAZ DE USUARIO DE USUARIO02 CON LOS CAMBIOS REALIZADOS

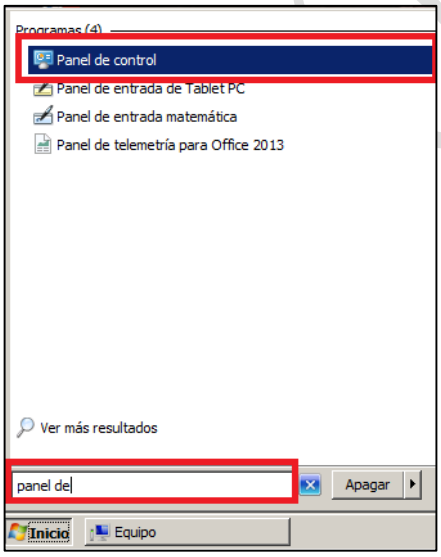
De momento en el escritorio de usuario02 podemos apreciar que ha desaparecido la papelera de reciclaje.



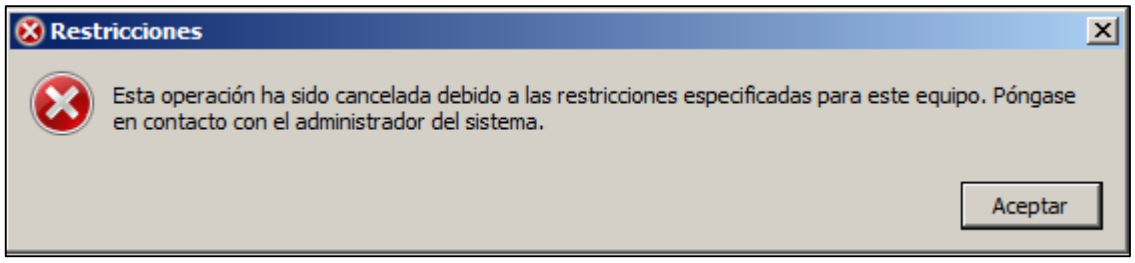
Observamos también que si hacemos clic derecho en el icono Equipo, en su menú contextual también ha desaparecido la selección “Propiedades”.



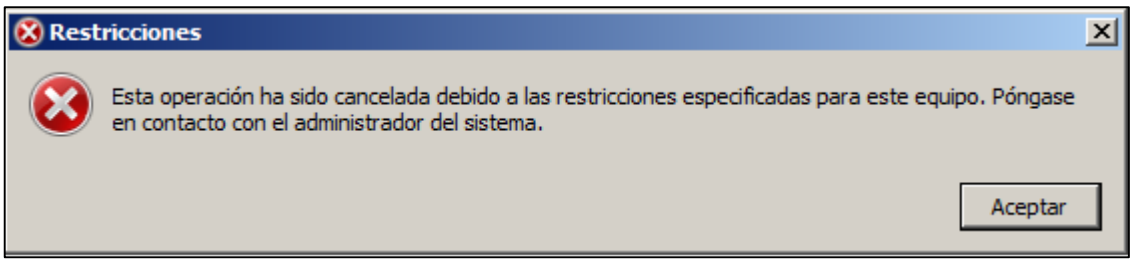
Efectivamente no aparece ni el panel de control ni el comando “Ejecutar”. No obstante si lo buscamos en “buscar programas y archivos”…



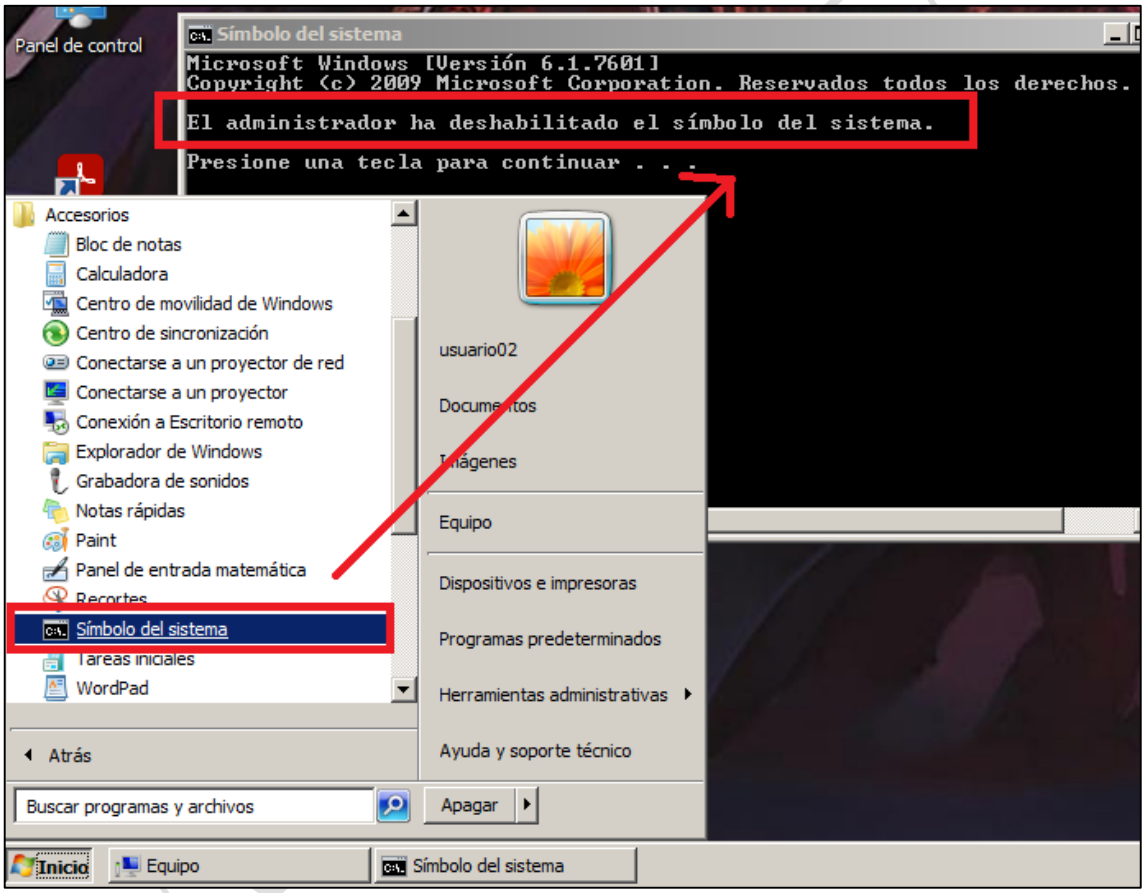
Podremos intentar acceder a dicho panel de control. Pero el resultado de ello, será la siguiente y última imagen de esta página.



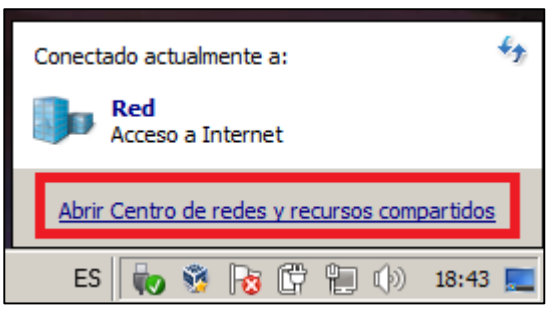
También hemos intentado acceder al símbolo del sistema (CMD) y a su vez al propio registro de Windows sin conseguirlo. Si lo hacemos con el comando "Ejecutar" anteriormente mencionado, al cual hemos intentado acceder pulsando el atajo de teclado Windows + R…



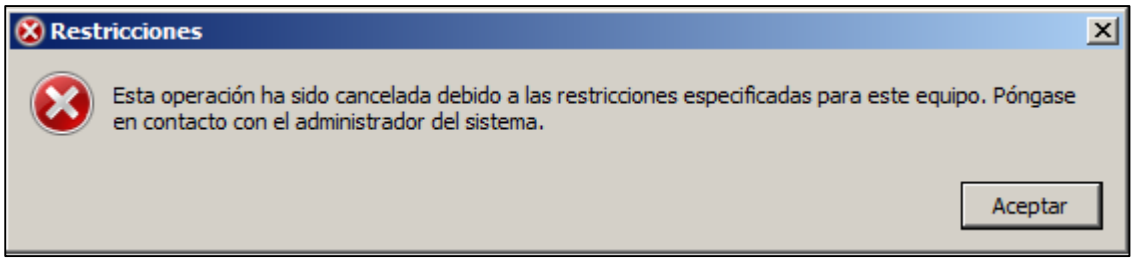
Y si lo intentamos a través de la interfaz gráfica…



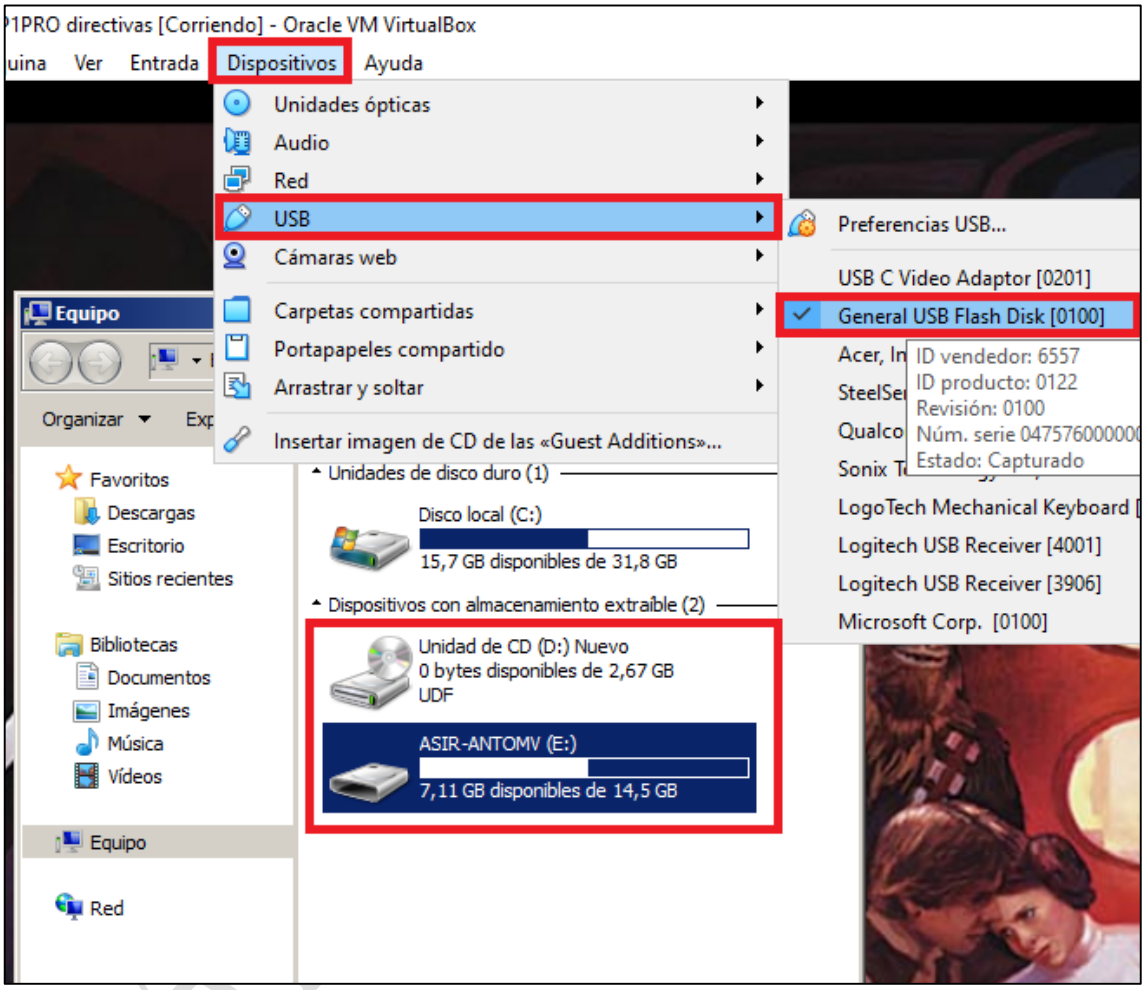
Dijimos también que íbamos a prohibir el acceso al control de redes y recursos compartidos para que un usuario no administrador no pueda trastear la configuración, por si la estropeaba…



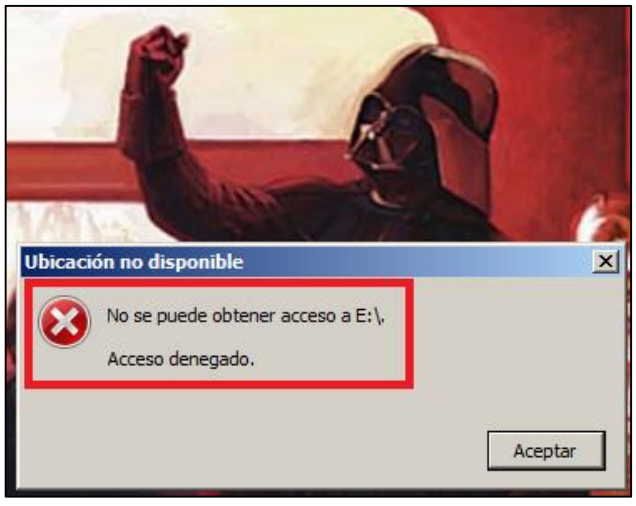
Y efectivamente volvemos a obtener el mismo resultado de antes. Una ventana que avisa de las restricciones del equipo…



MEDIOS EXTRAIBLES (CD-ROM's, PENDRIVES, ETC…)



Como resultado de haber bloqueado el acceso a todo tipo de medios extraíbles, la respuesta del equipo al intentar acceder a dichos medios extraíbles será esta con dicha ventana emergente:



BREVE RESUMEN PARA TERMINAR

El mundo de las directivas es totalmente inmenso. Un buen administrador que domine este campo a la hora de administrar una empresa, tiene mucho a su favor y seguro que es un empleado muy cotizado pero como tal, todo requiere experiencia y conocimiento o lo que es igual… TIEMPO. Se podría dedicar una cuarta parte de nuestra vida solamente a esta temática y seguiría faltando porque ya se sabe, el mundo tecnológico, se actualiza día tras día.

Este ha sido mi trabajo de 3-4 días sin descanso para realizar dicha guía MLGPO sobre las Múltiples Directivas de Objetos de Grupo Local, en inglés: MULTIPLE Local Group Policy Objects.

Espero que les haya gustado. Un saludo cordial.
Atentamente:

Antonio Martínez Vela
Alumno de FPGS º1 de ASIR