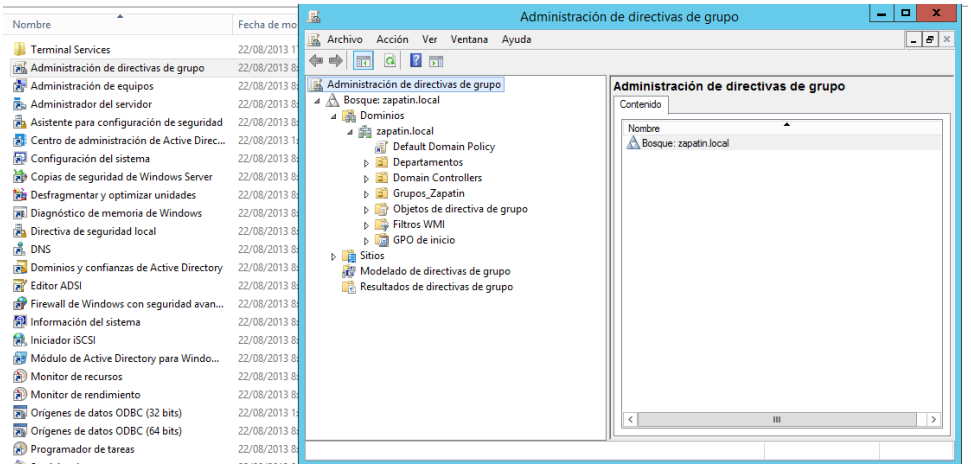
# RUBIO AVILA MARIO TAREA 9.1

## Contexto

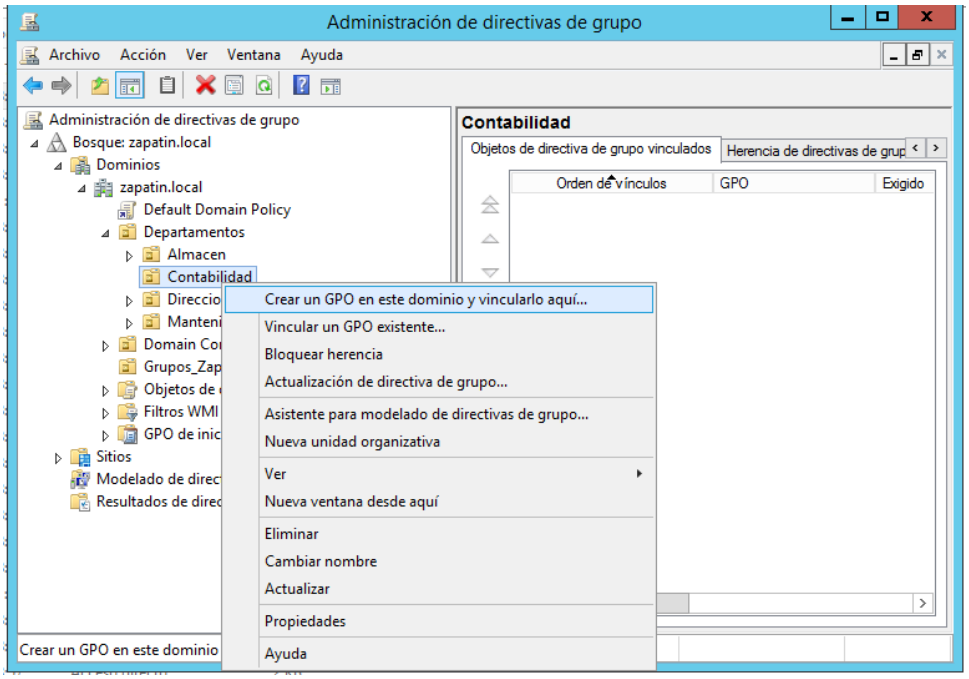
Continuando con la máquina virtual de la tarea 8.1.

## El grupo de contabilidad no puede acceder al panel de control.

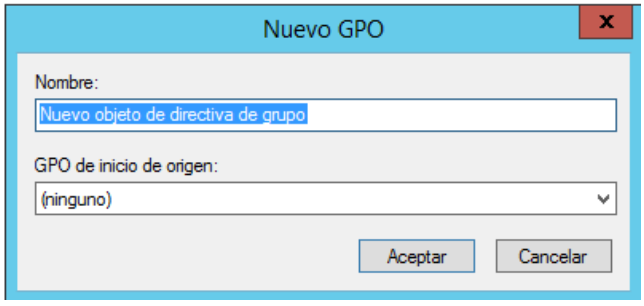
Lo primero a realizar es abrir el administrador de directivas de grupo.



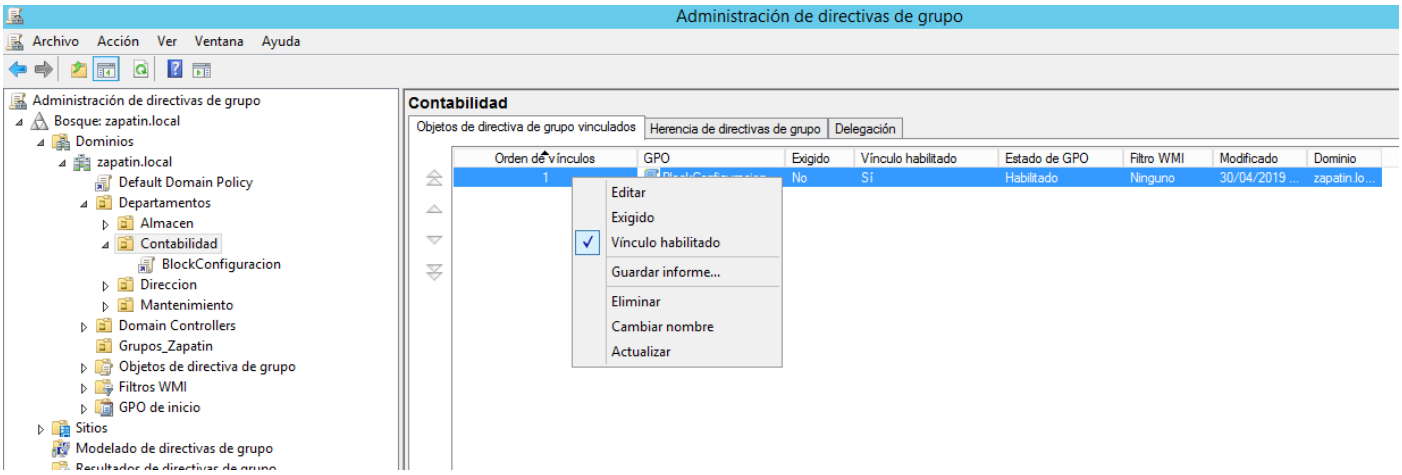

Ahora seleccionamos el departamento contabilidad y creamos una nueva gpo en este dominio



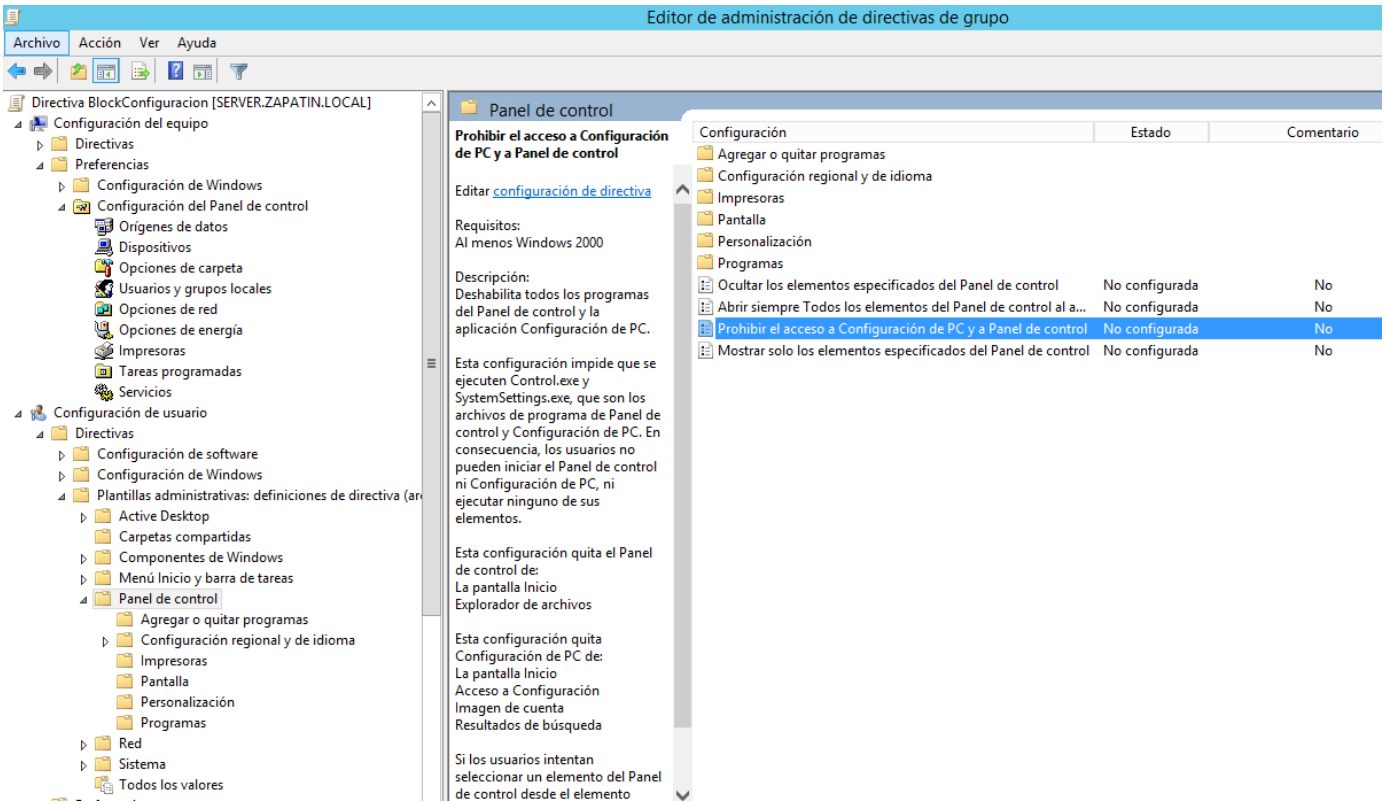

Le elegimos un nombre

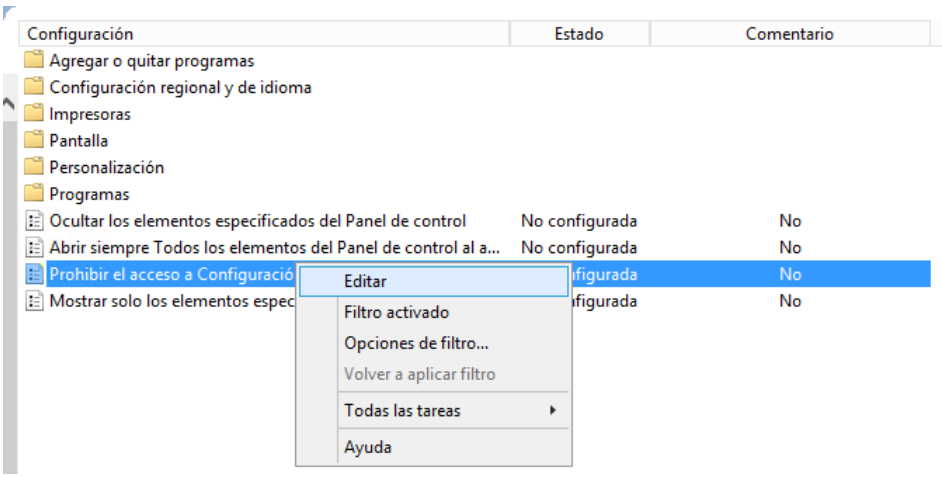



Ahora vamos a editar

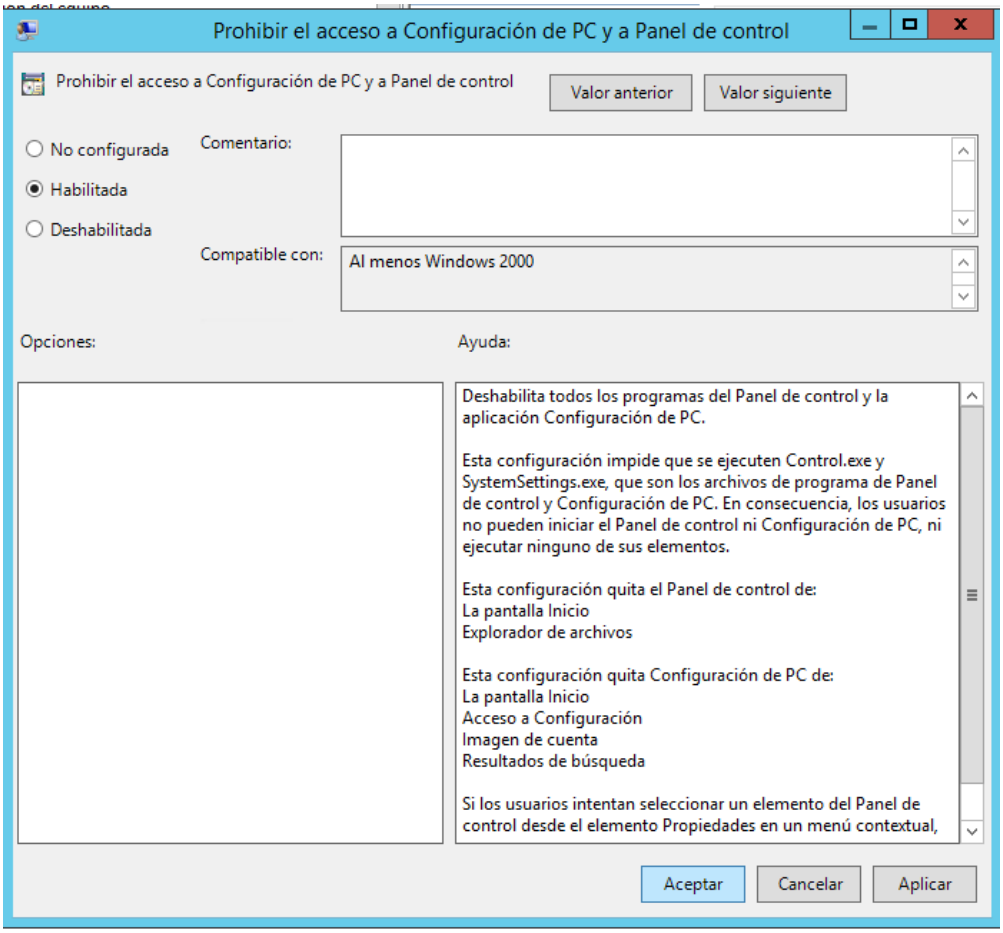



En el editor vamos a buscar una plantilla ya predefinida que nos ayudara a realizar esta tarea de manera rápida.



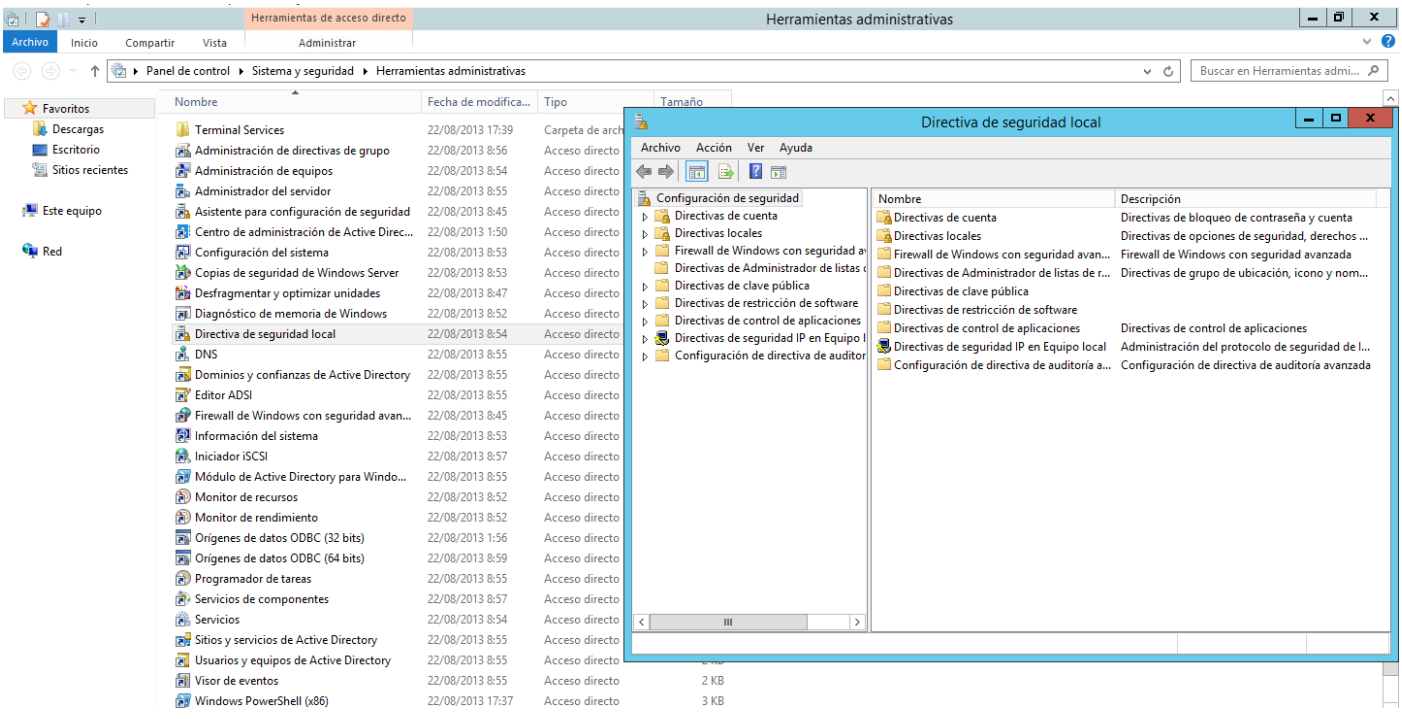

Ahora la habilitamos y le damos aceptar. Y ya podemos ir cerrando la directiva ya esta activada para el grupo contabilidad.



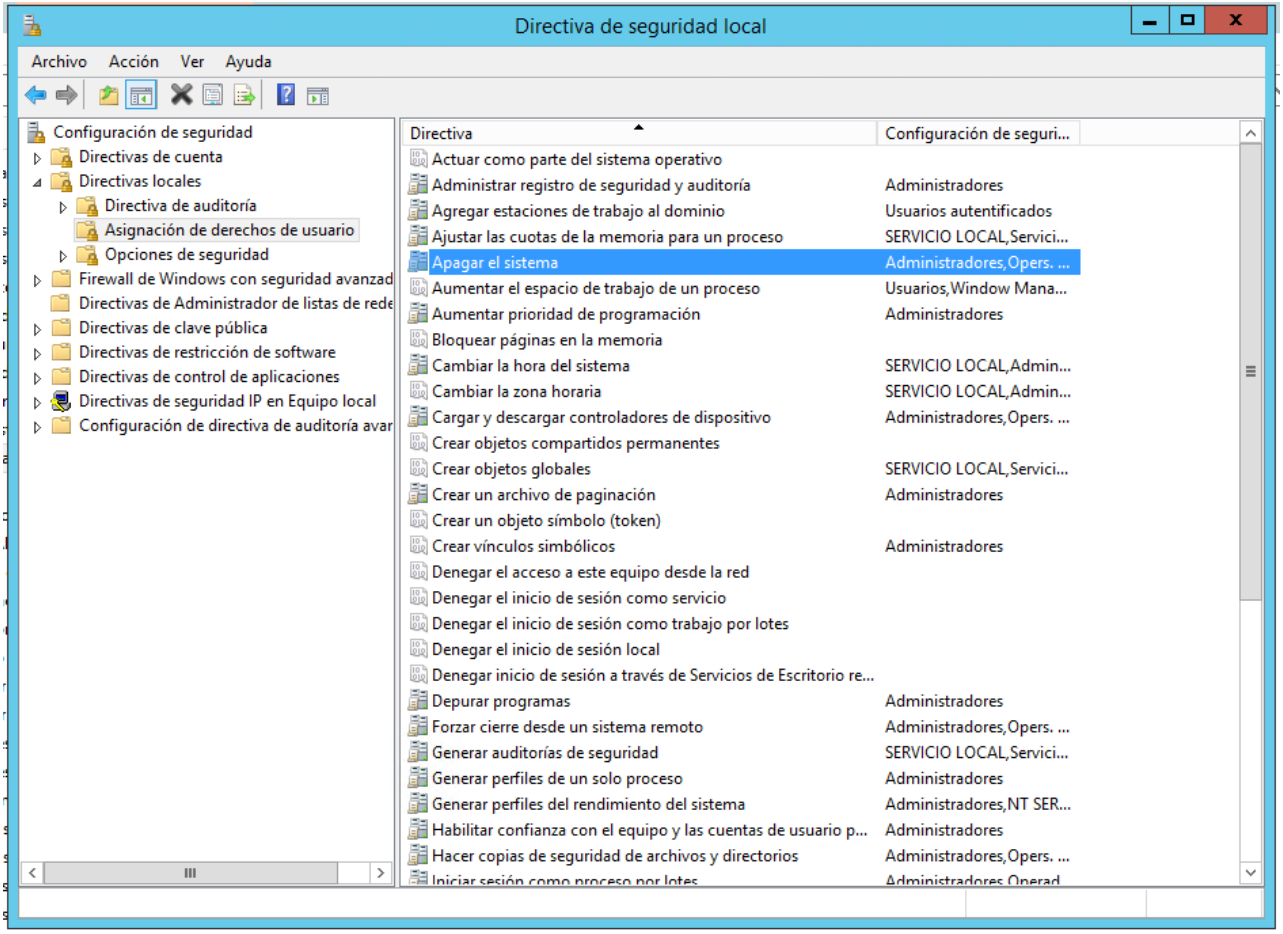

Cuando un usuario de la cuenta contabilidad intenta abrir el panel de control obtendrá el siguiente mensaje.

## Ningún usuario excepto los del grupo de dirección pueden apagar el equipo.

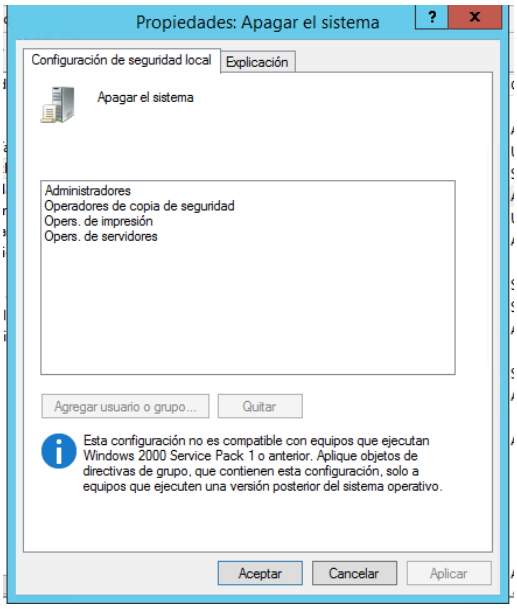
Ahora abrimos las directivas de seguridad local.



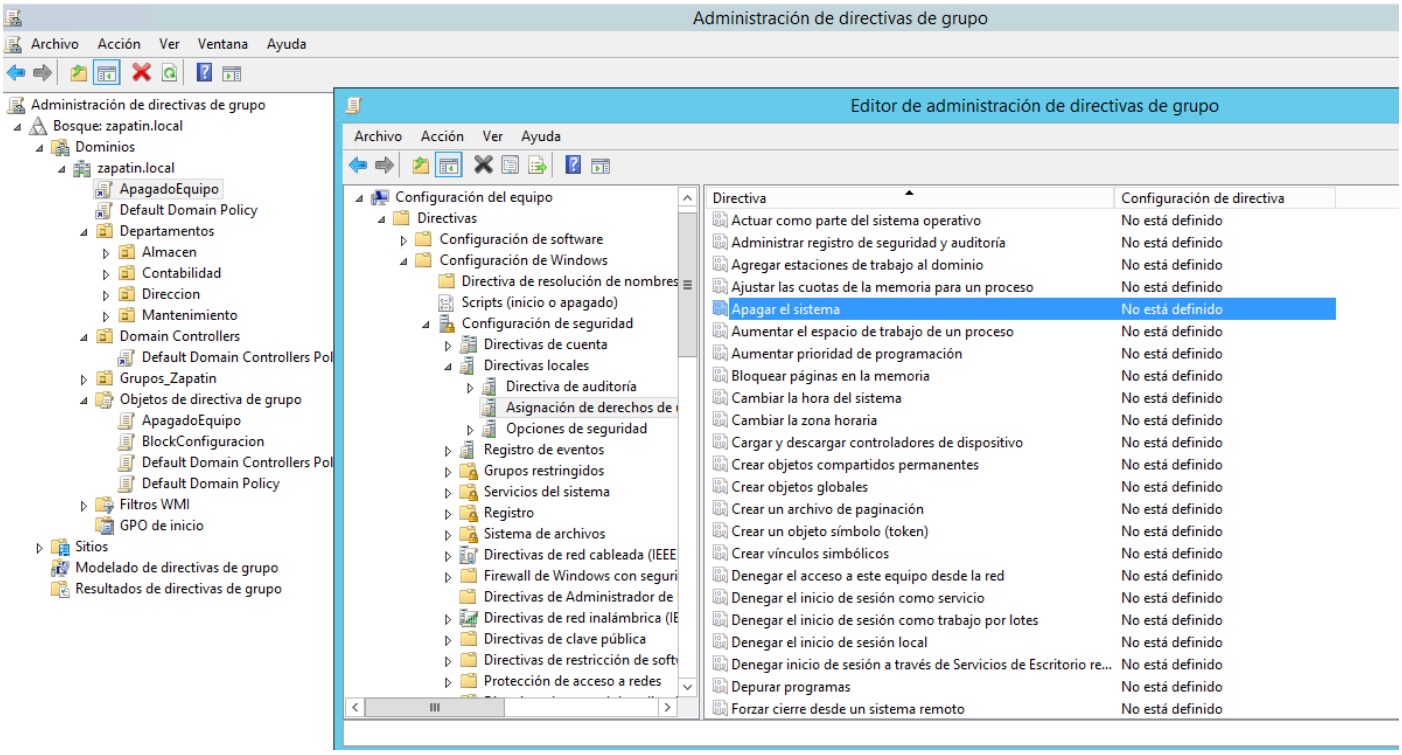

Aquí iremos a directivas locales y a la asignación de derechos de usuarios y buscaremos la de apagar el sistema, damos botón derecho y elegimos propiedades



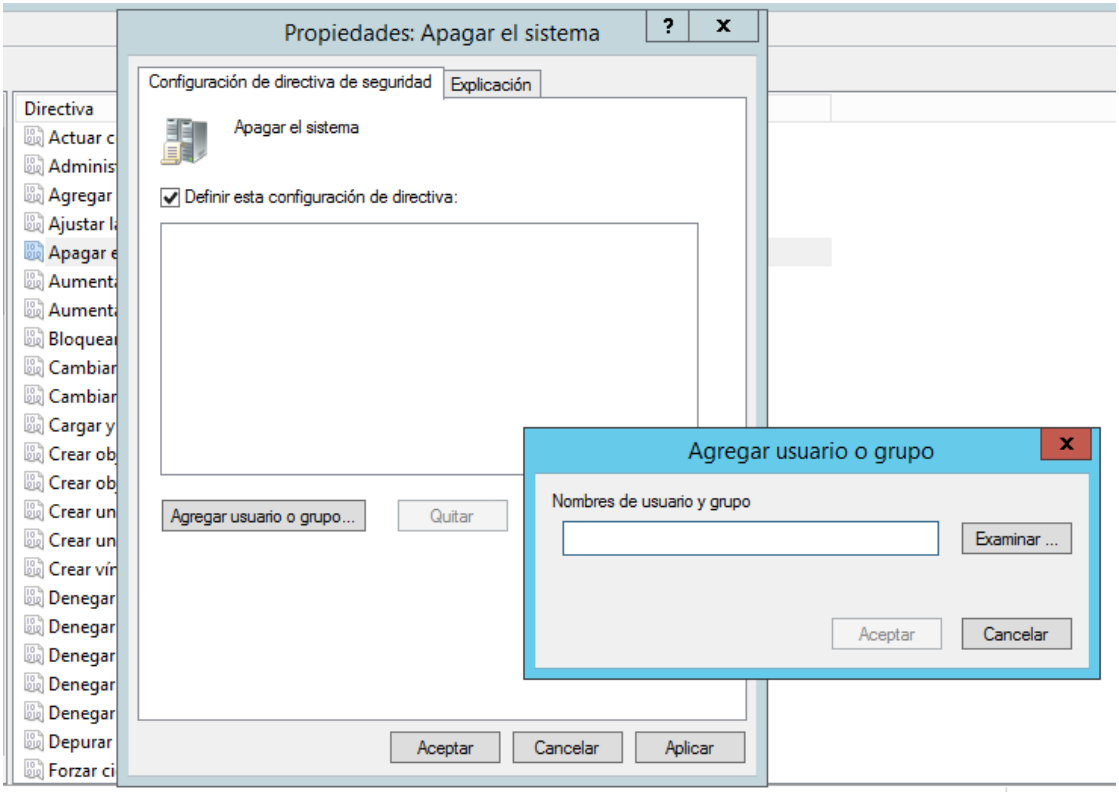

Y vemos que algo pasa no nos permite desde aquí las modificaciones. Tras analizar en Windows server 2012 hubo un cambio y esto ahora vine impuesta por la GPO Default Domain Policy si estas unido a un dominio que es nuestro caso, es decir que tendremos que tocar esa configuración en la GPO del dominio.



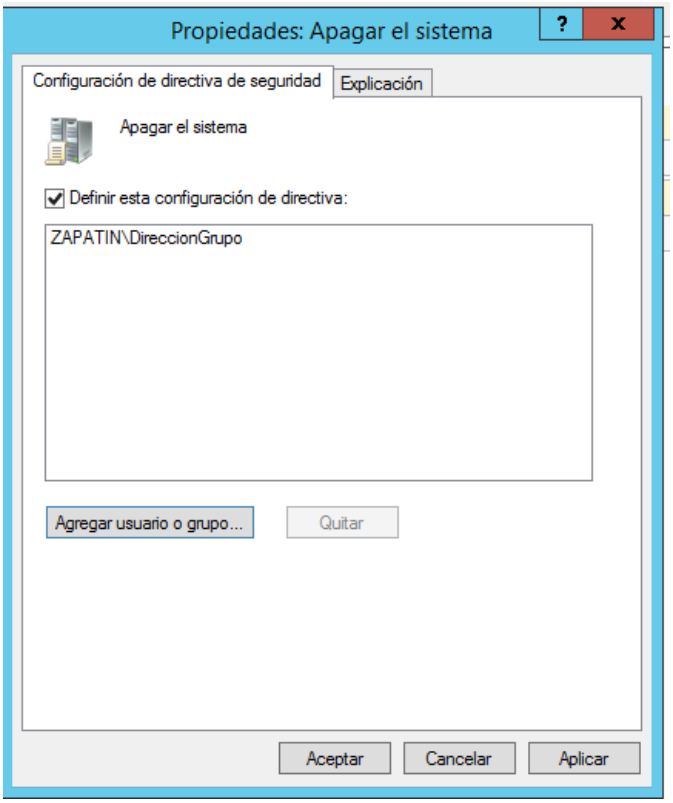

Por lo que volvemos al administrador de directivas de grupo. Creamos un nuevo gpo que abarque al dominio y en el editor vamos a configuración de Windows/configuración de seguridad/directivas locales/asignación de derechos de usuarios y buscamos apagar




Y seleccionamos los usuarios que podrán apagar el equipo

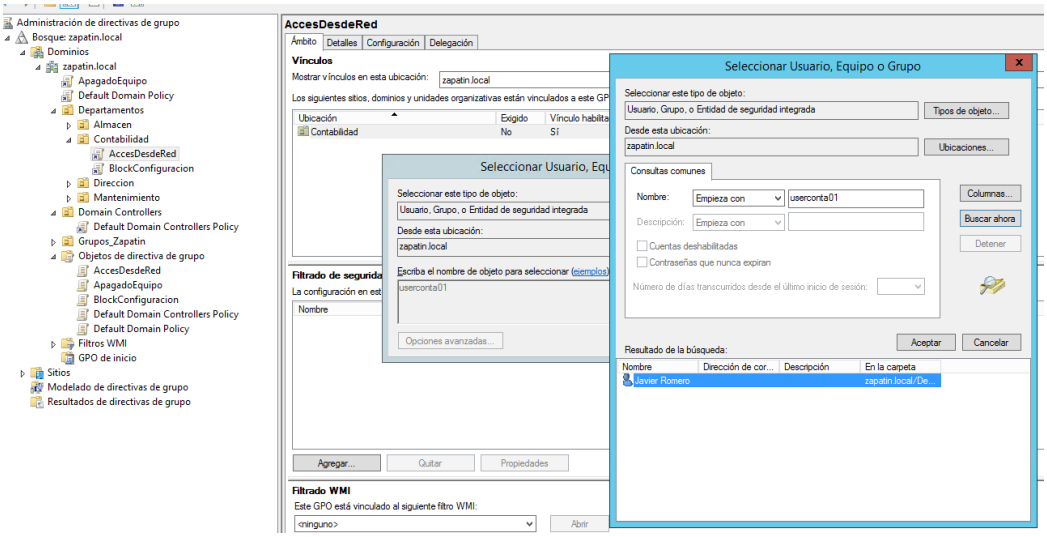


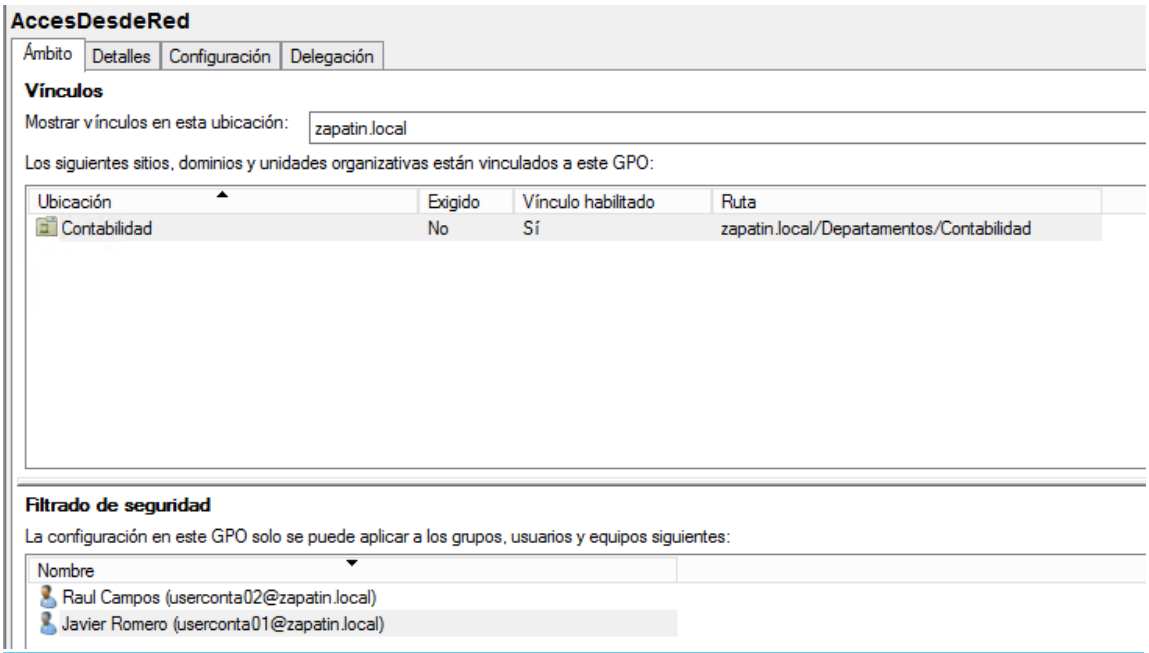

Que en nuestro caso va a ser un grupo

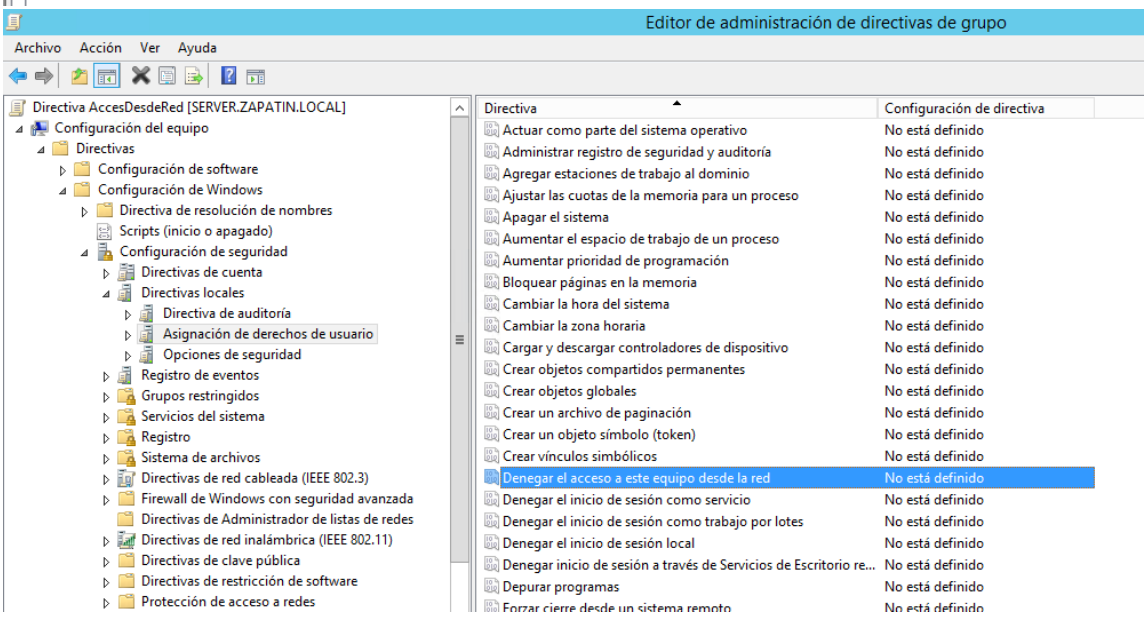


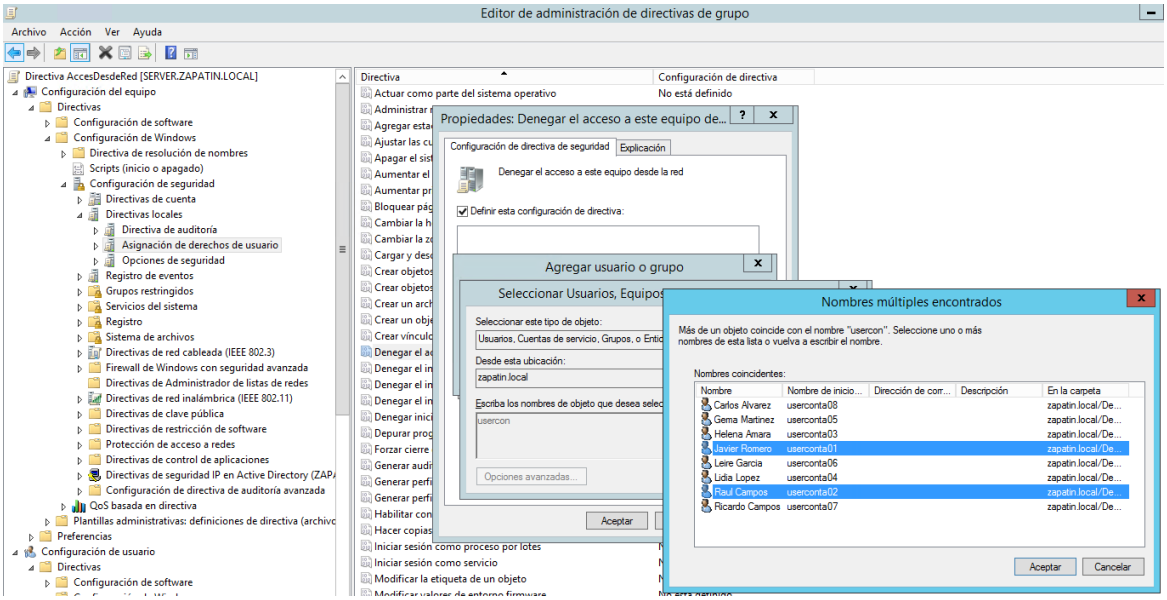

## Denegar el acceso a este equipo desde la red para los usuarios userconta01 y userconta02.

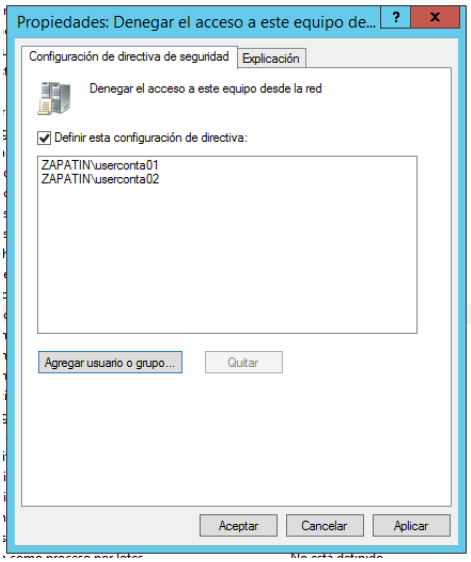
Creamos la nueva directiva y añadimos los dos usuarios, como se muestra acontinuacion.



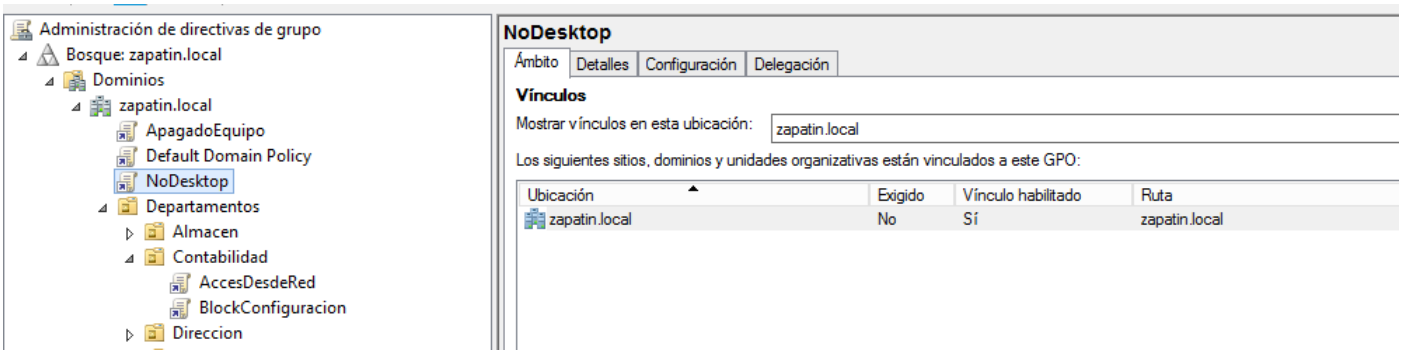

AccesDesdeRed
Ámbito
Detalles
Configuración
Delegación
Vínculos
Mostrar vínculos en esta ubicación:
zapatin.local
Los siguientes sitios, dominios y unidades organizativas están vinculados a este GPO:
Ubicación
Exigido
Vínculo habilitado
Ruta
Contabilidad
No
Sí
zapatin.local/Departamentos/Contabilidad
Filtrado de seguridad
La configuración en este GPO solo se puede aplicar a los grupos, usuarios y equipos siguientes:
Nombre
Raul Campos (userconta02@zapatin.local)
Javier Romero (userconta01@zapatin.local)

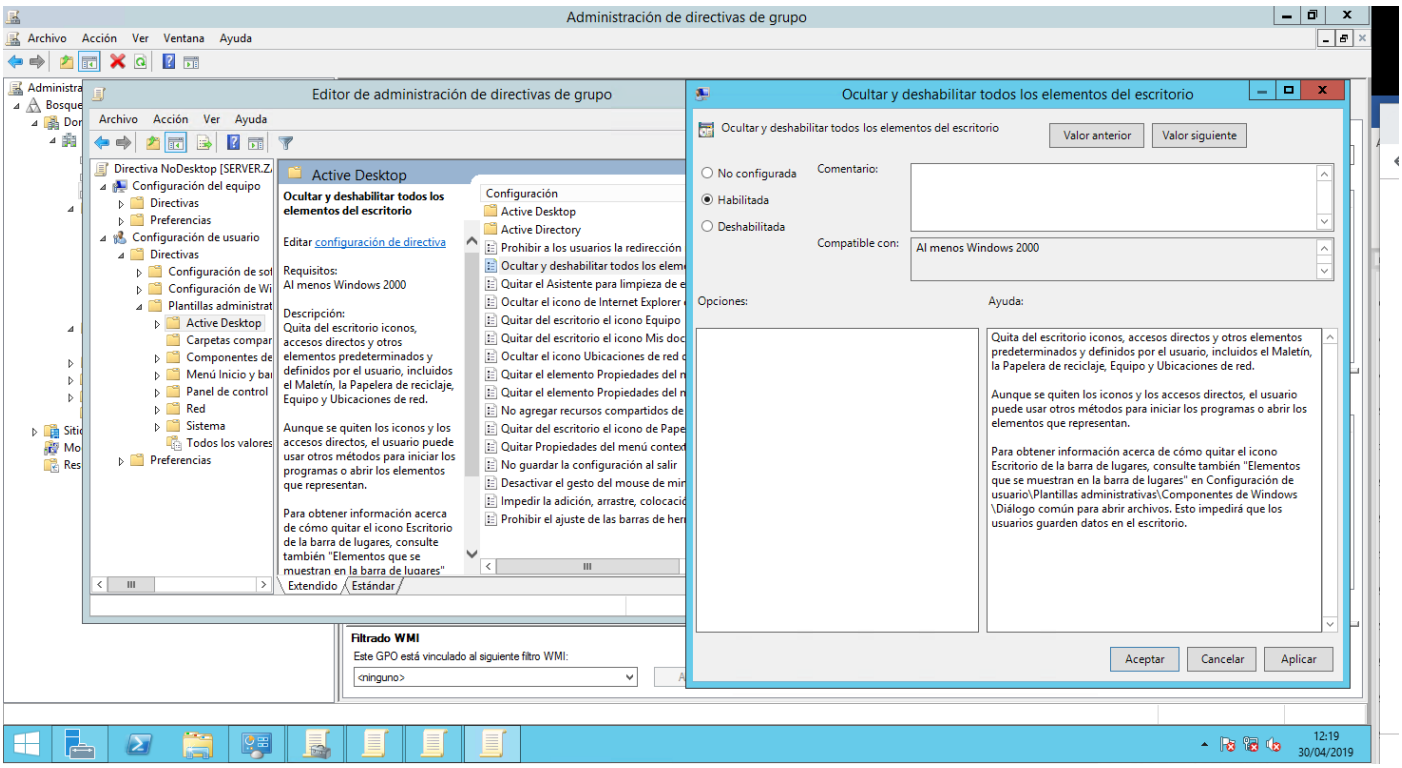

Editor de administración de directivas de grupo
Archivo
Acción
Ver
Ayuda
Directiva AccesDesdeRed [SERVER.ZAPATIN.LOCAL]
Configuración del equipo
Directivas
Configuración de software
Configuración de Windows
Directiva de resolución de nombres
Scripts (inicio o apagado)
Configuración de seguridad
Directivas de cuenta
Directivas locales
Directiva de auditoría
Asignación de derechos de usuario
Opciones de seguridad
Registro de eventos
Grupos restringidos
Servicios del sistema
Registro
Sistema de archivos
Directivas de red cableada (IEEE 802.3)
Firewall de Windows con seguridad avanzada
Directivas de Administrador de listas de redes
Directivas de red inalámbrica (IEEE 802.11)
Directivas de clave pública
Directivas de restricción de software
Protección de acceso a redes
Directiva
Configuración de directiva
Actuar como parte del sistema operativo
No está definido
Administrar registro de seguridad y auditoría
Agregar estaciones de trabajo al dominio
Ajustar las cuotas de la memoria para un proceso
Apagar el sistema
Aumentar el espacio de trabajo de un proceso
Aumentar prioridad de programación
Bloquear páginas en la memoria
Cambiar la hora del sistema
Cambiar la zona horaria
Cargar y descargar controladores de dispositivo
Crear objetos compartidos permanentes
Crear objetos globales
Crear un archivo de paginación
Crear un objeto símbolo (token)
Crear vínculos simbólicos
Denegar el acceso a este equipo desde la red
Denegar el inicio de sesión como servicio
Denegar el inicio de sesión como trabajo por lotes
Denegar el inicio de sesión local
Denegar inicio de sesión a través de Servicios de Escritorio re...
Depurar programas
Forzar cierre desde un sistema remoto


Editor de administración de directivas de grupo
Archivo
Acción
Ver
Ayuda
Propiedades: Denegar el acceso a este equipo de...
Configuración de directiva de seguridad
Explicación
Denegar el acceso a este equipo desde la red
Definir esta configuración de directiva:
Agregar usuario o grupo
Seleccionar Usuarios, Equipos
Seleccionar este tipo de objeto:
Usuarios, Cuentas de servicio, Grupos, o Entid
Desde esta ubicación:
zapatin.local
Escriba los nombres de objeto que desea selec
usercon
Opciones avanzadas...
Aceptar
Nombres múltiples encontrados
Más de un objeto coincide con el nombre "usercon". Seleccione uno o más nombres de esta lista o vuelva a escribir el nombre.
Nombres coincidentes:
Nombre
Nombre de inicio...
Dirección de corr...
Descripción
En la carpeta
Carlos Alvarez
userconta08
zapatin.local/De...
Gema Martinez
userconta05
Helena Amara
userconta03
Javier Romero
userconta01
Leire Garcia
userconta06
Lidia Lopez
userconta04
Raul Campos
userconta02
Ricardo Campos
userconta07
Aceptar
Cancelar



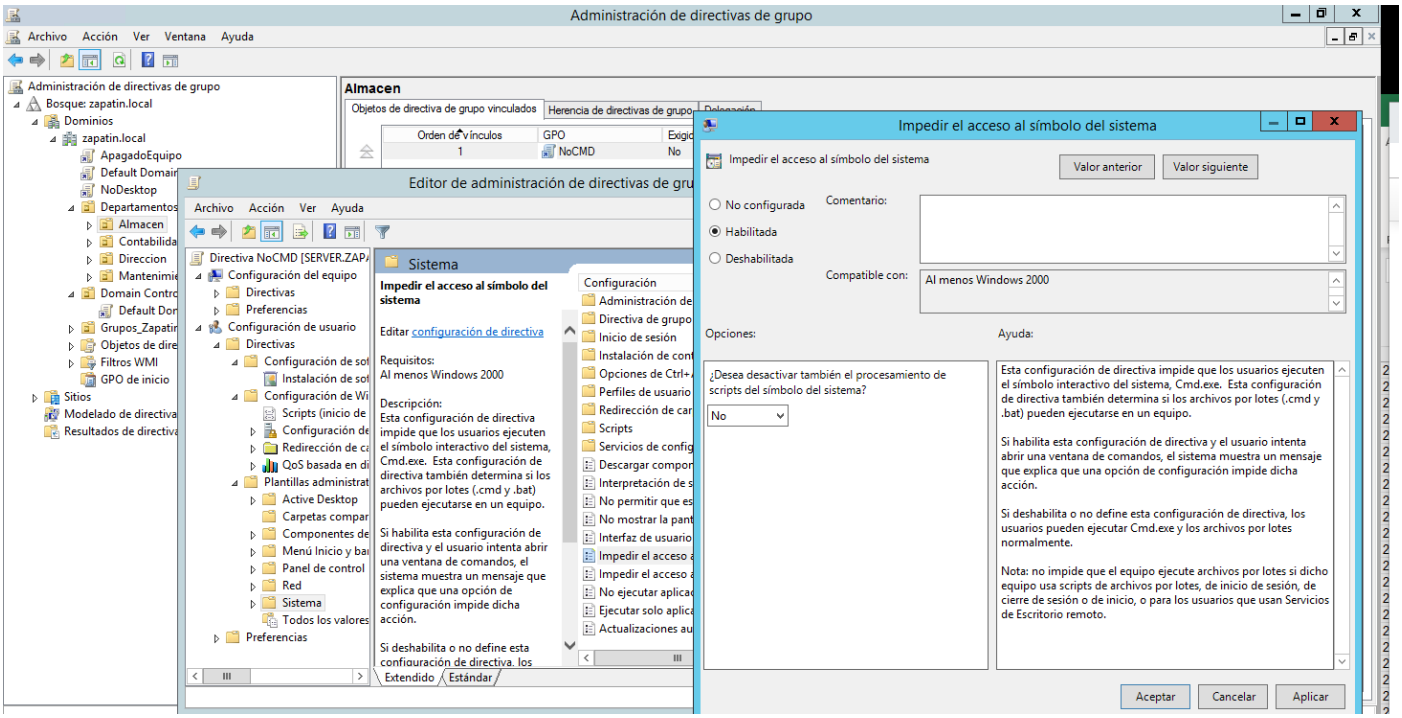

## Ocultar todos los elementos del escritorio para todos los usuarios.



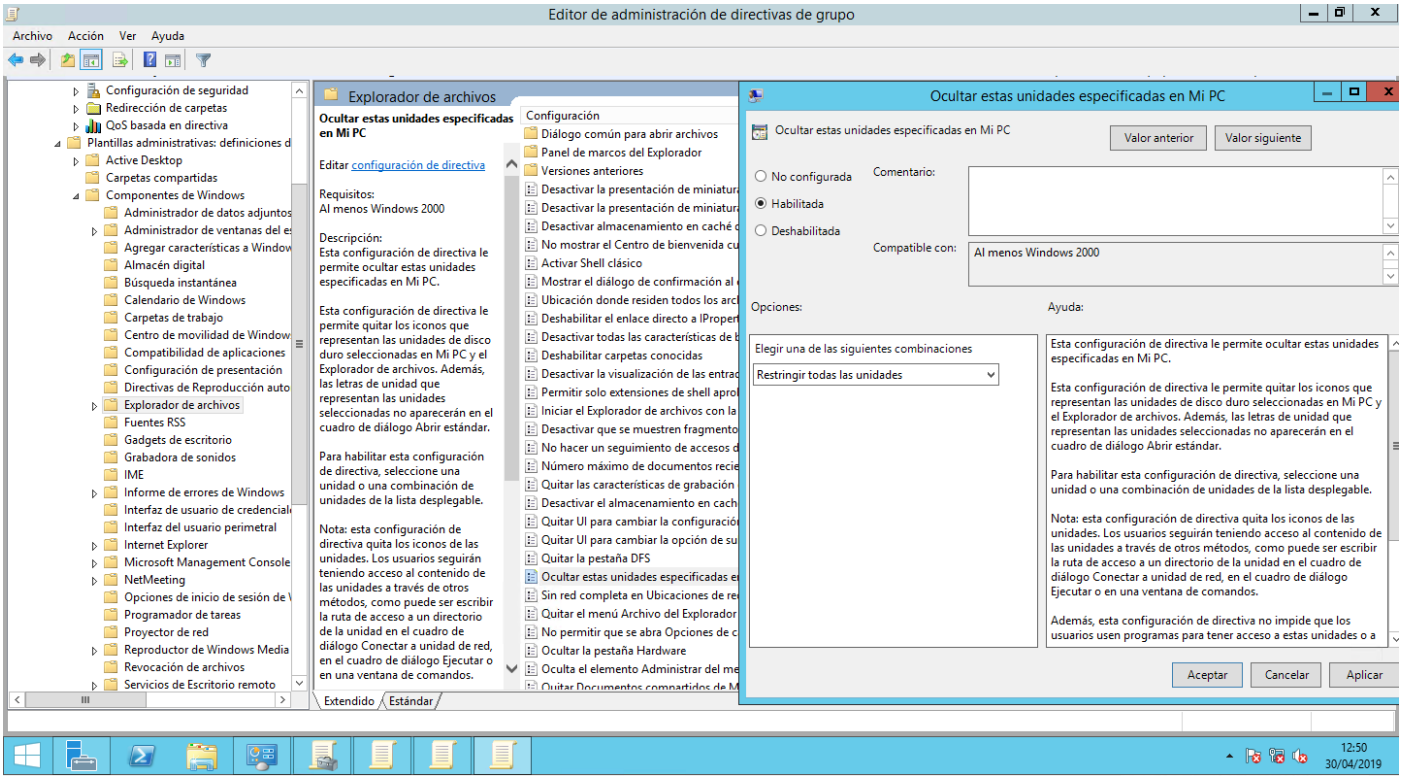

## Impedir el acceso al símbolo del sistema al grupo Almacén.

Viene siendo lo mismo que en casos anteriores. Crear una nueva política que bloque la posibliladad de abrir la línea de comandos.



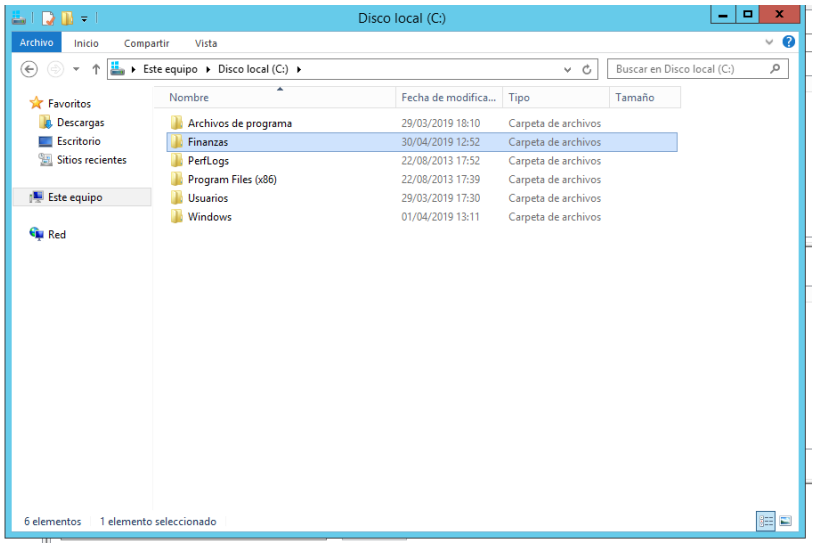

## Impedir el acceso a las unidades desde "mi pc".

Como no se especifica pondo a todo el mundo que es lo mas restrictivo y desde el punto de seguridad es lo mas correcto

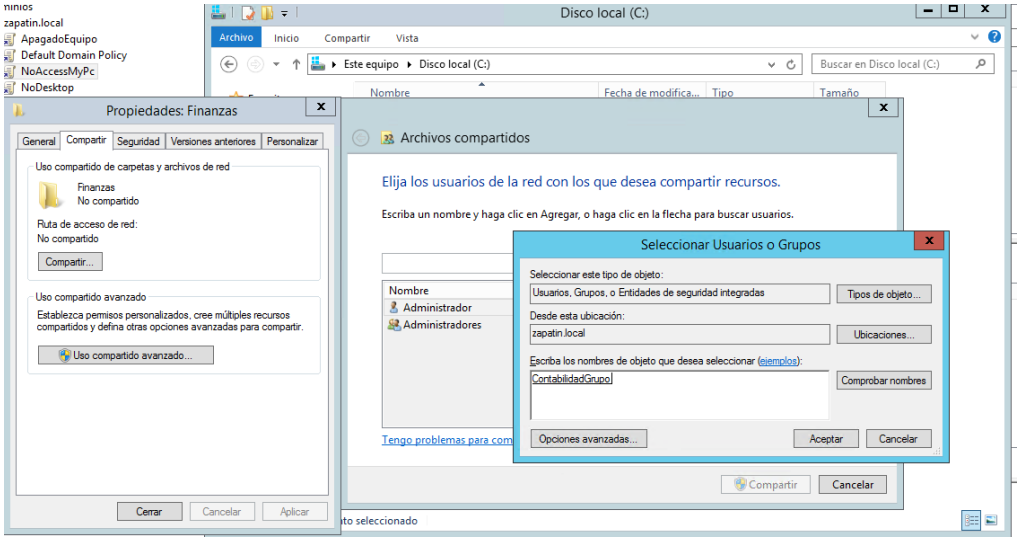


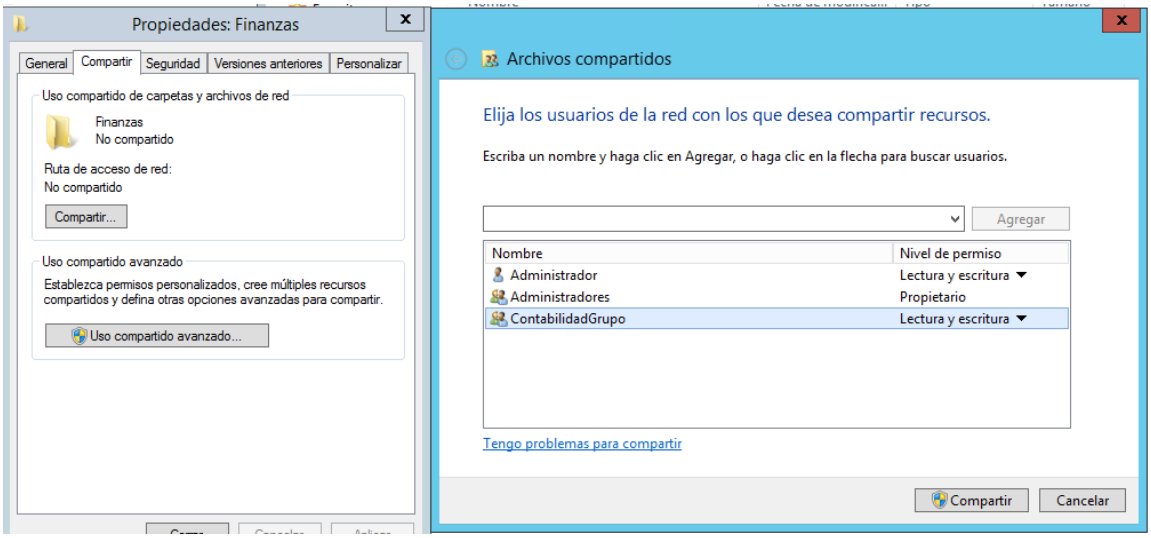

## Auditar el acceso de los accesos de los usuarios contabilidad a una carpeta compartida Finanzas que deberás crear en el Windows2012.

Lo primero a realizar es la carpeta que nos solita.

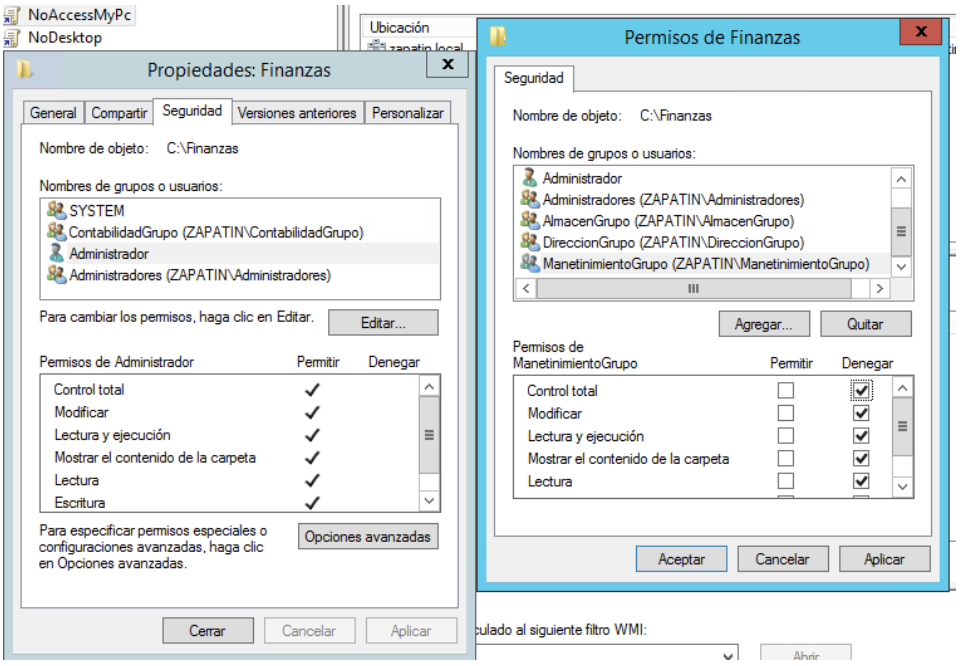



Una vez la tenemos creada la tenemos que compartir y crear los permisos correspondientes.

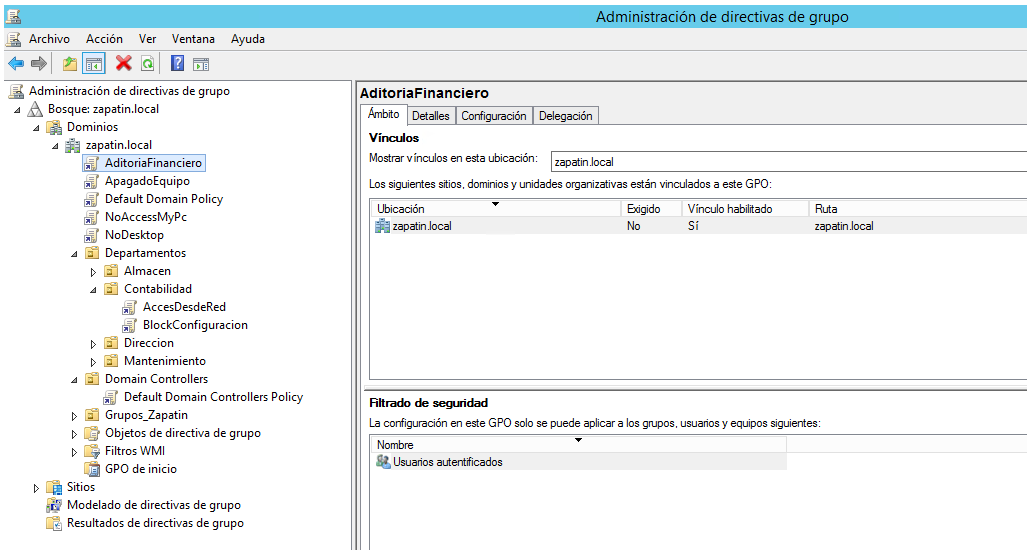


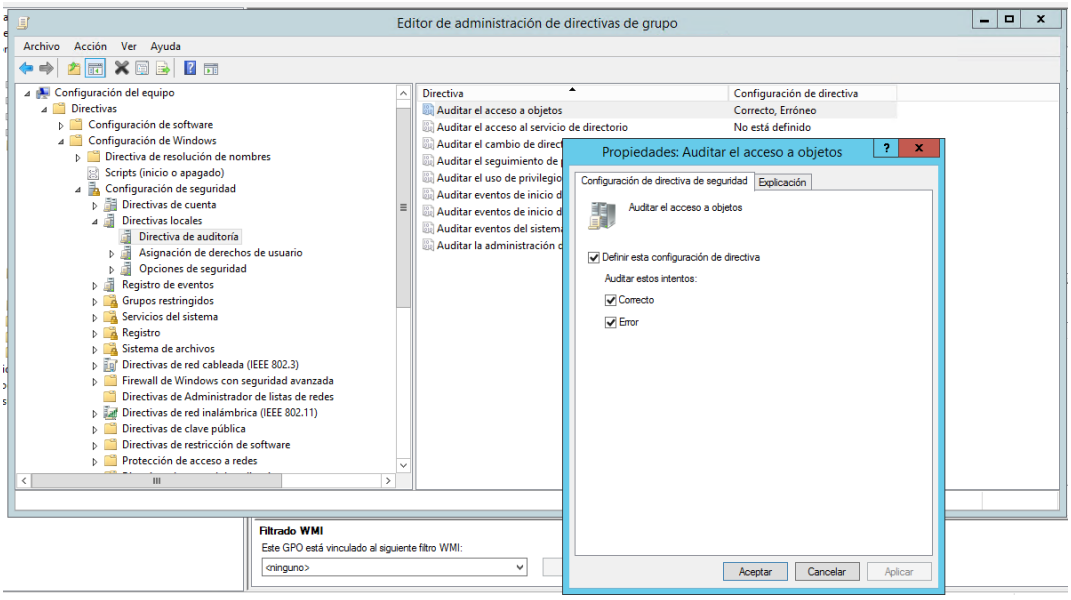

Tras tenerla configurada para el grupo vamos a indicar que los otros grupos no tienen autorizado el acceso. Voy a permitir el acceso a los administradores, pero por ser una practica esto en un proyecto para un cliente deberia ser eliminado por seguridad.




Una vez realizado lo anterior ya creamos la directiva para la auditoria del objeto para todo el dominio ya que me interasa saber auditar si alguien de otro grupo intenta hacer algo no muy etico.

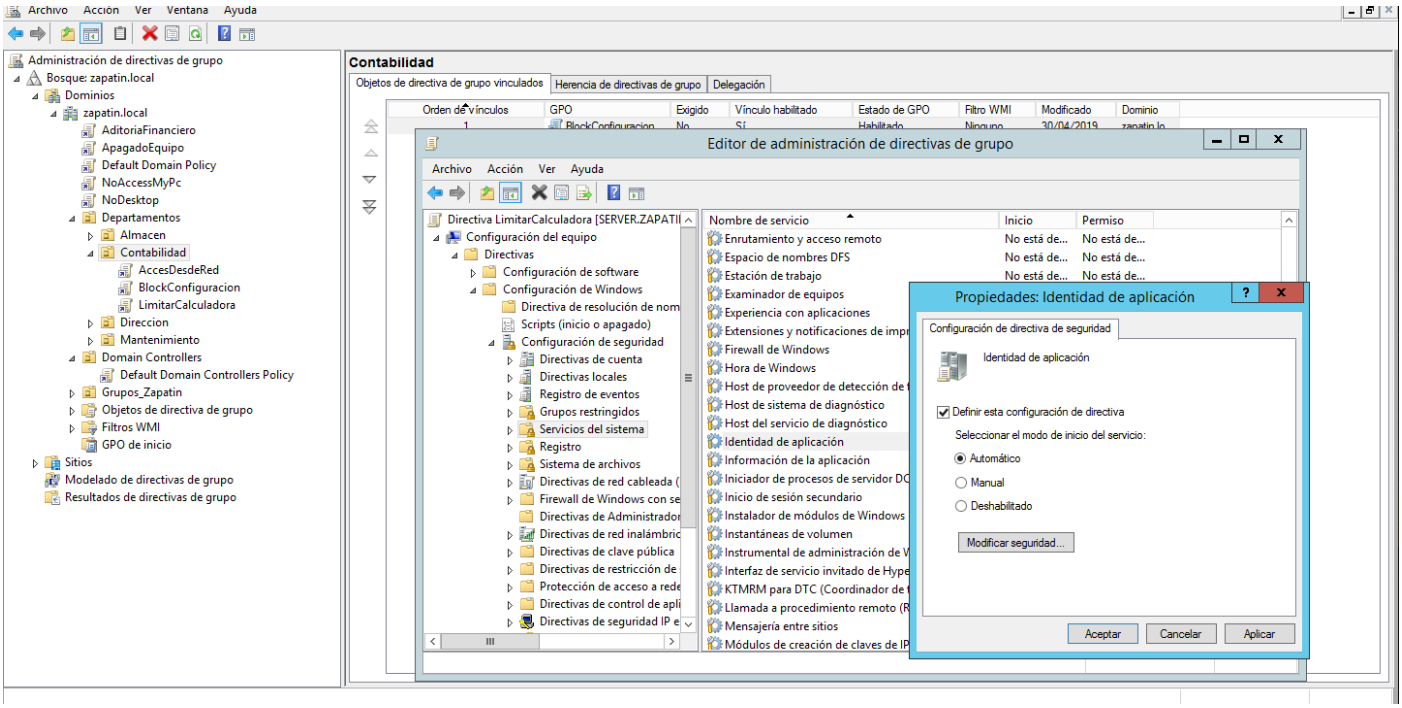



Auditamos tanto si acceden como si fallan en el acceso

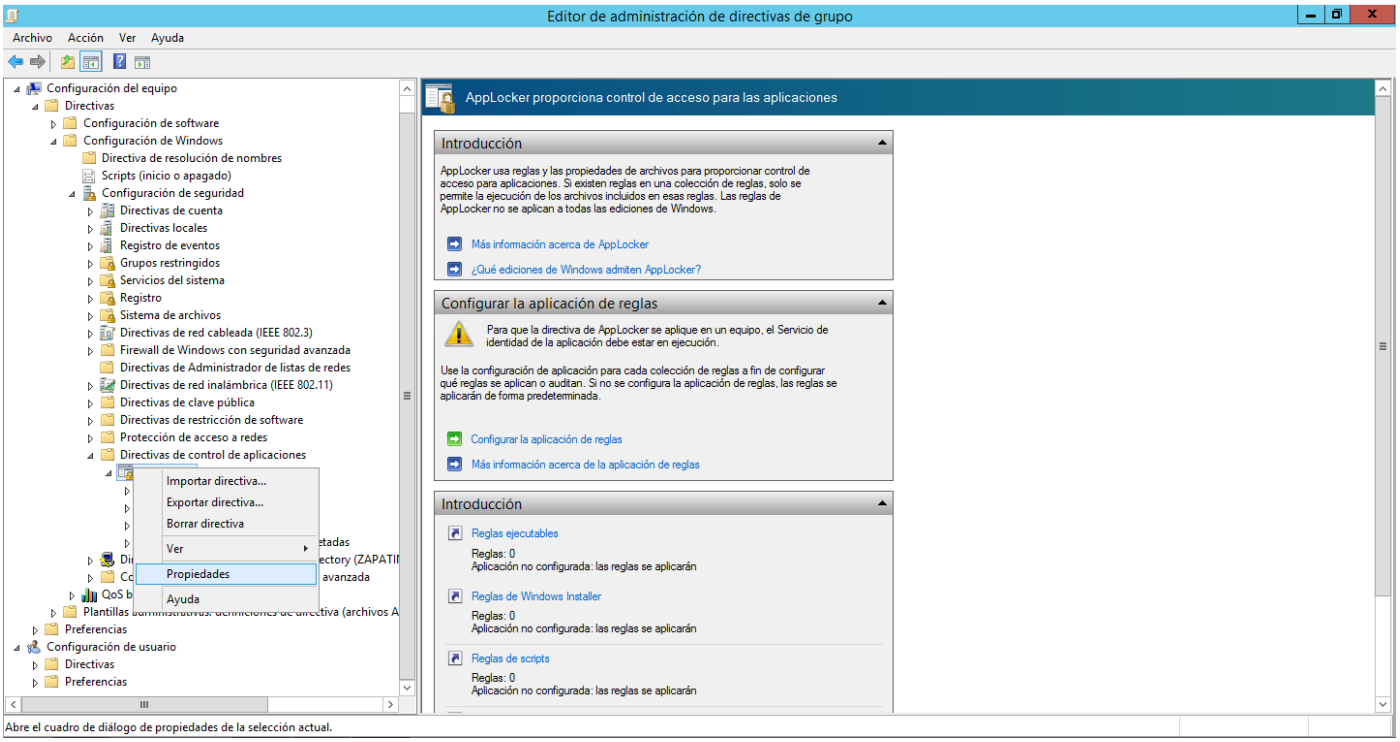


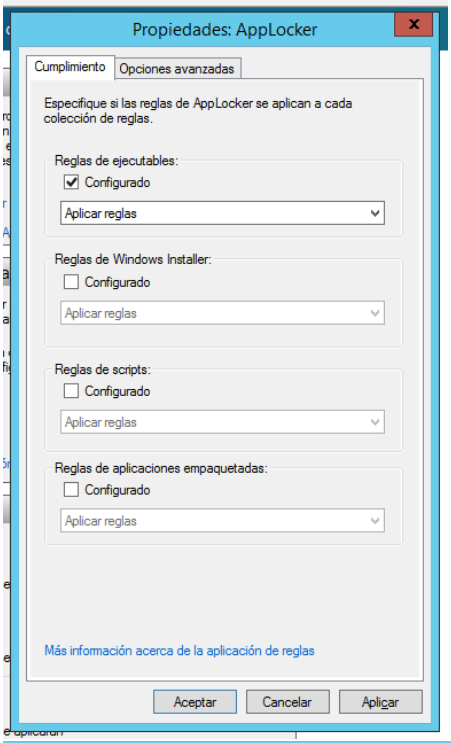
## El usuario userconta02 no podrá arrancar la calculadora en el WindowsServer2012 mediante escritorio remoto.

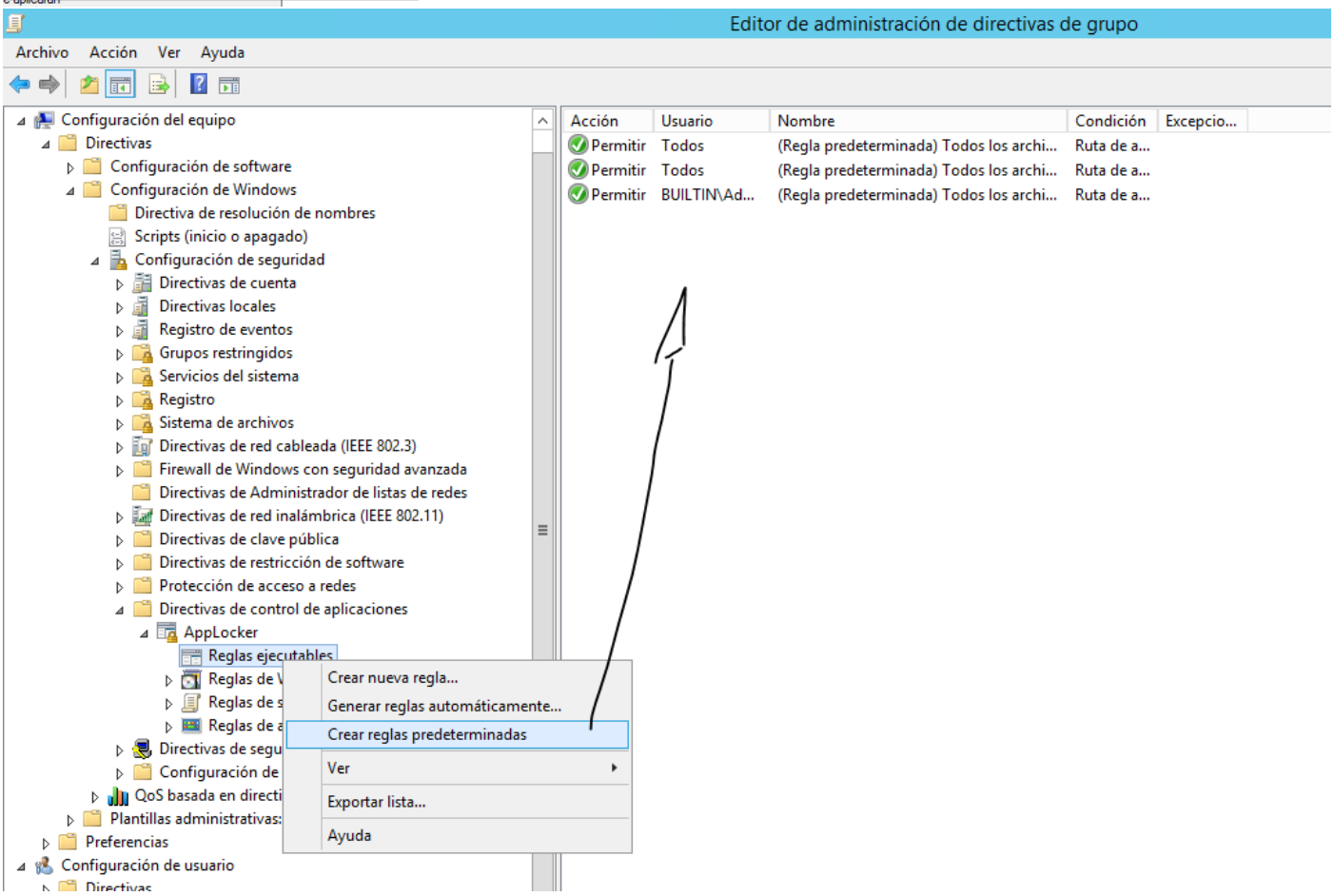
Lo primero será arrancar la identificación del la aplicación.

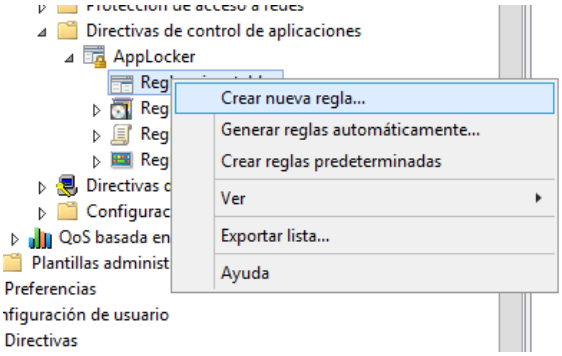


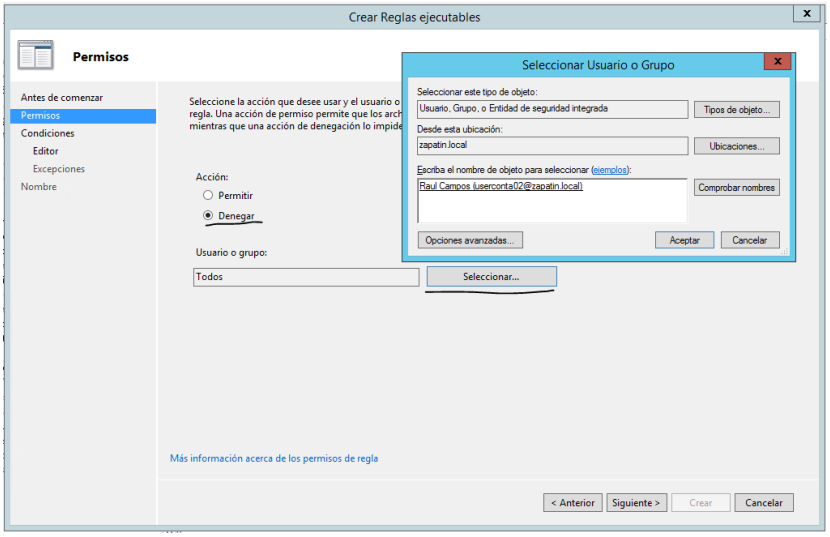

Ahora ya podemos a la configuración de la aplicación para eso seguimos los pasos detallados acontinuacion.

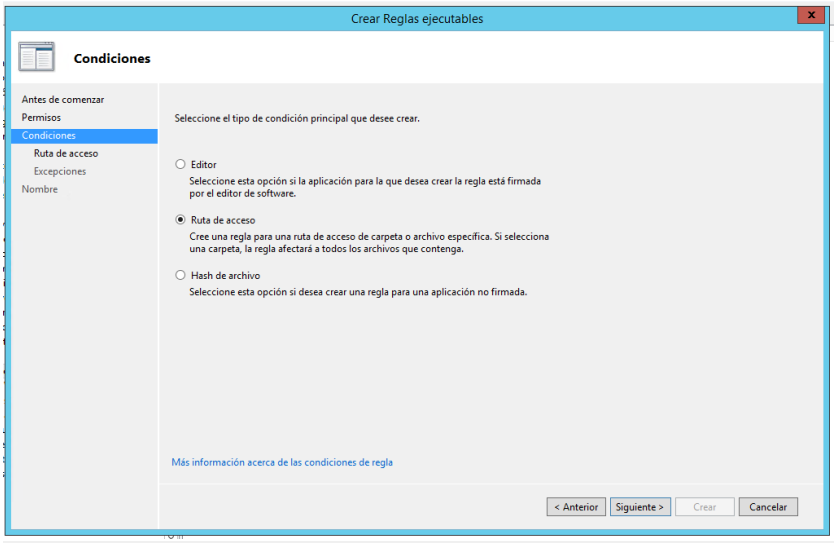


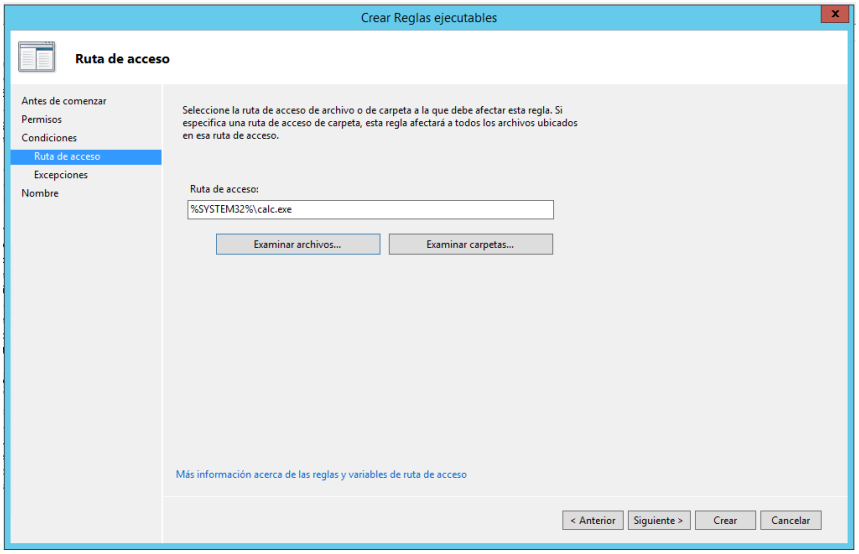

Propiedades: AppLocker
Cumplimiento
Opciones avanzadas
Especifique si las reglas de AppLocker se aplican a cada colección de reglas.
Reglas de ejecutables:
Configurado
Aplicar reglas
Reglas de Windows Installer:
Configurado
Aplicar reglas
Reglas de scripts:
Configurado
Aplicar reglas
Reglas de aplicaciones empaquetadas:
Configurado
Aplicar reglas
Más información acerca de la aplicación de reglas
Aceptar
Cancelar
Aplicar

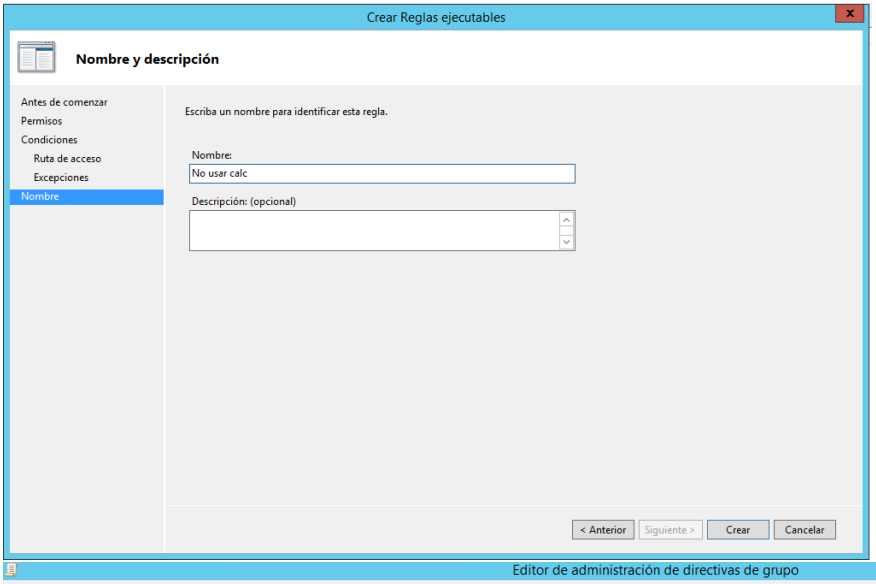

Editor de administración de directivas de grupo
Archivo
Acción
Ver
Ayuda
Configuración del equipo
Directivas
Configuración de software
Configuración de Windows
Directiva de resolución de nombres
Scripts (inicio o apagado)
Configuración de seguridad
Directivas de cuenta
Directivas locales
Registro de eventos
Grupos restringidos
Servicios del sistema
Registro
Sistema de archivos
Directivas de red cableada (IEEE 802.3)
Firewall de Windows con seguridad avanzada
Directivas de Administrador de listas de redes
Directivas de red inalámbrica (IEEE 802.11)
Directivas de clave pública
Directivas de restricción de software
Protección de acceso a redes
Directivas de control de aplicaciones
AppLocker
Reglas ejecutables
Crear nueva regla...
Generar reglas automáticamente...
Crear reglas predeterminadas
Ver
Exportar lista...
Ayuda
Preferencias
Configuración de usuario
Acción
Usuario
Nombre
Condición
Excepcio...
Permitir Todos (Regla predeterminada) Todos los archi... Ruta de a...
Permitir Todos (Regla predeterminada) Todos los archi... Ruta de a...
Permitir BUILTIN\Ad... (Regla predeterminada) Todos los archi... Ruta de a...

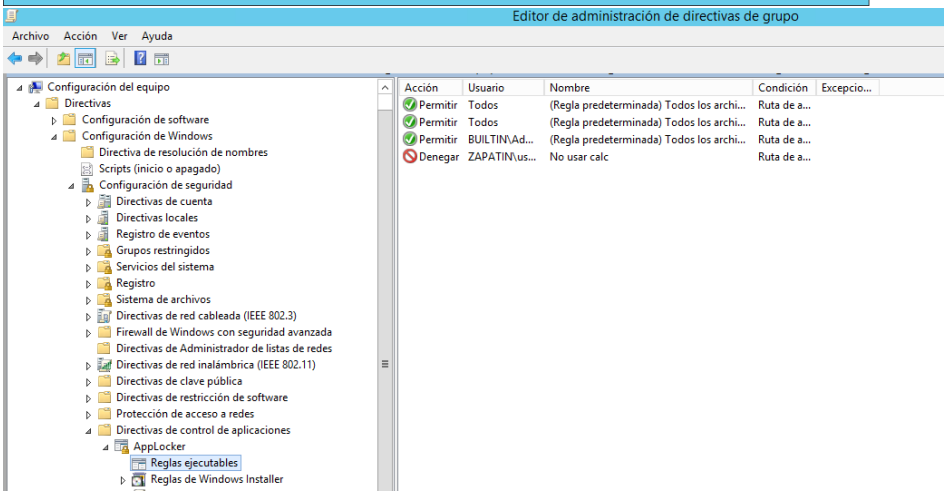

Directivas de control de aplicaciones
AppLocker
Crear nueva regla...
Generar reglas automáticamente...
Crear reglas predeterminadas
Ver
Exportar lista...
Ayuda
Preferencias
Directivas


Crear Reglas ejecutables
Permisos
Antes de comenzar
Permisos
Condiciones
Editor
Excepciones
Nombre
Acción:
Permitir
Denegar
Usuario o grupo:
Todos
Seleccionar...
Seleccionar Usuario o Grupo
Seleccionar este tipo de objeto:
Usuario, Grupo, o Entidad de seguridad integrada
Tipos de objeto...
Desde esta ubicación:
zapatin.local
Ubicaciones...
Escriba el nombre de objeto para seleccionar (ejemplos):
Raul Campos (userconta02@zapatin.local)
Comprobar nombres
Opciones avanzadas...
Aceptar
Cancelar
Más información acerca de los permisos de regla
< Anterior
Siguiente >
Crear
Cancelar


Crear Reglas ejecutables
Condiciones
Antes de comenzar
Permisos
Condiciones
Ruta de acceso
Excepciones
Nombre
Seleccione el tipo de condición principal que desee crear.
Editor
Seleccione esta opción si la aplicación para la que desea crear la regla está firmada por el editor de software.
Ruta de acceso
Cree una regla para una ruta de acceso de carpeta o archivo específica. Si selecciona una carpeta, la regla afectará a todos los archivos que contenga.
Hash de archivo
Seleccione esta opción si desea crear una regla para una aplicación no firmada.
Más información acerca de las condiciones de regla
< Anterior
Siguiente >
Crear
Cancelar


Crear Reglas ejecutables
Ruta de acceso
Antes de comenzar
Permisos
Condiciones
Ruta de acceso
Excepciones
Nombre
Seleccione la ruta de acceso de archivo o de carpeta a la que debe afectar esta regla. Si especifica una ruta de acceso de carpeta, esta regla afectará a todos los archivos ubicados en esa ruta de acceso.
Ruta de acceso:
%SYSTEM32%\calc.exe
Examinar archivos...
Examinar carpetas...
Más información acerca de las reglas y variables de ruta de acceso
< Anterior
Siguiente >
Crear
Cancelar


Crear Reglas ejecutables
Nombre y descripción
Antes de comenzar
Permisos
Condiciones
Ruta de acceso
Excepciones
Nombre
Escriba un nombre para identificar esta regla.
Nombre:
No usar calc
Descripción: (opcional)
< Anterior
Siguiente >
Crear
Cancelar


Editor de administración de directivas de grupo
Archivo
Acción
Ver
Ayuda
Configuración del equipo
Directivas
Configuración de software
Configuración de Windows
Directiva de resolución de nombres
Scripts (inicio o apagado)
Configuración de seguridad
Directivas de cuenta
Directivas locales
Registro de eventos
Grupos restringidos
Servicios del sistema
Registro
Sistema de archivos
Directivas de red cableada (IEEE 802.3)
Firewall de Windows con seguridad avanzada
Directivas de Administrador de listas de redes
Directivas de red inalámbrica (IEEE 802.11)
Directivas de clave pública
Directivas de restricción de software
Protección de acceso a redes
Directivas de control de aplicaciones
AppLocker
Reglas ejecutables
Reglas de Windows Installer
Acción
Usuario
Nombre
Condición
Excepcio...
Permitir Todos (Regla predeterminada) Todos los archi... Ruta de a...
Permitir Todos (Regla predeterminada) Todos los archi... Ruta de a...
Permitir BUILTIN\Ad... (Regla predeterminada) Todos los archi... Ruta de a...
Denegar ZAPATIN\us... No usar calc Ruta de a...