

UD 9 C Directivas de Grupo GPO

Índice

Directivas de Grupo GPO

1. ¿Qué son las directivas de grupo?
 - 1.1. Valores de configuración de equipo y de usuario
 - 1.2. Directivas locales
 - 1.3. Ejemplo de directiva
 - 1.4. Herencia de permisos de GPO
 - 1.5. Conflictos en la GPO's
 - 1.6. Bloqueo de despliegue de GPO
 - 1.7. ¿Cómo configurar el "forzado" de las directivas?
 - 1.8. Filtrado del despliegue de GPO
 - a. Filtro de seguridad de GPO
 - b. Filtros WMI
 - c. Estado de GPO
2. Administración del entorno de usuario
 - 2.1. Habilitar y deshabilitar valores
 - 2.2. Editar un valor de una directiva
 - 2.3. Secuencias de comandos
 - a. Práctica. Crear una secuencia de comandos y asignarla a una cuenta de usuarios
Secuencias de comandos desde la ficha de usuario
Secuencias de comandos con directivas GPO
 - 2.4. Gpupdate
 - 2.5. Gpresult
 - 2.6. Referencia de las directivas
3. Elementos de las GPO
 - 3.1. Almacenamiento y replicación de las GPO
 - a. Replicación de GPO's
 - b. Carpeta USER
 - c. Carpeta Machine
 - d. Carpeta ADM
 - e. Archivos registry.pol
 - f. Archivo GPT.INI
 - 3.2. Definición de las directivas, componentes
 - 3.3. Plantillas administrativas de las directivas de grupo
 - 3.4. Visor de eventos
 - 3.5. Creación de una directiva de inicio
4. Implantar impresoras con directivas de grupo
 - 4.1. Implementación de conexiones de impresora

Directivas de Grupo GPO

Una de las tareas más importantes que debemos realizar con nuestros equipos en nuestra empresa es, por supuesto, controlarlos. Controlarlos significa poder definir cómo queremos que trabajen los usuarios. En el sentido de que tipo de configuración queremos que tengan en el equipo. Por ejemplo, hay un grupo de ordenadores que utilizan los operarios de fábrica que deben tener un fuerte control para que no ejecuten aplicaciones no permitidas. En este caso podremos eliminar todas las opciones del menú inicio o simplemente indicar que sólo puedan ejecutar ciertas aplicaciones. Otro caso, queremos realizar una instalación desatendida (automática) de un programa a todos los equipos de una unidad organizativa. No hay problema, todas estas cosas y muchas más las haremos con las GPO o las directivas de grupo, llamadas también políticas (por la traducción de "policy").

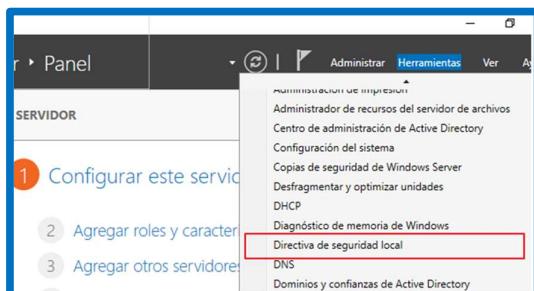
Las directivas ya existían allá por las primeras versiones de Windows NT, pero a partir de Windows 2000 se ampliaron hasta permitir realizar cualquier tipo de configuración de los equipos. La versión de las directivas de 2019 permite controlar además todas las opciones de los sistemas más modernos como todas las versiones de Windows 10.

Las directivas las aplicaremos sobre una organización entera, dominio, sitio o unidad organizativa. Otro ejemplo, podemos establecer una directiva global para establecer que a los tres intentos fallidos de inicio de sesión se bloquee la cuenta del usuario. O instalar una impresora determinada al departamento de "Calidad".

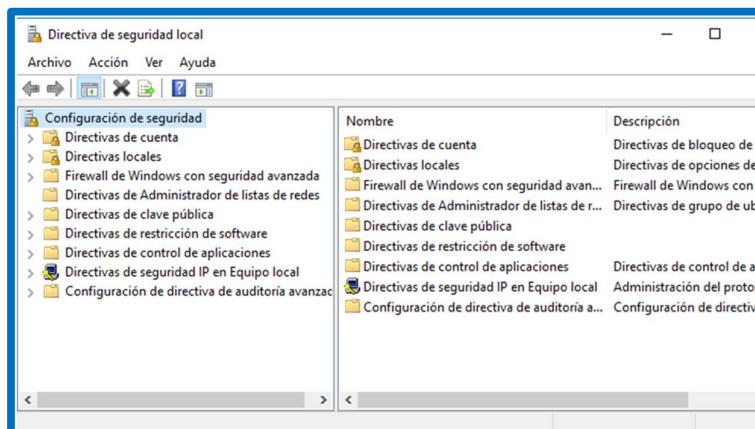
1. ¿Qué son las directivas de grupo?

Las directivas de grupo proporcionan el control de la administración sobre los usuarios y los equipos de nuestra red. Podremos definir el estado del ambiente de trabajo de los usuarios una sola vez, confiando que Windows Server hará cumplir continuamente esta configuración de directivas. La verdad es que no nos ha aclarado mucho de momento. Pero si decimos que las directivas van a configurar automáticamente los entornos Windows de todos los equipos de nuestra red eso parece más fácil de entender. Un ejemplo muy sencillo, podemos utilizar una directiva que ponga a todos los equipos de mi red el mismo fondo de escritorio, salvapantallas y además bloquear esta parte de la configuración de Windows para que los usuarios no puedan cambiarlo. Eso se acerca más al objetivo de las directivas.

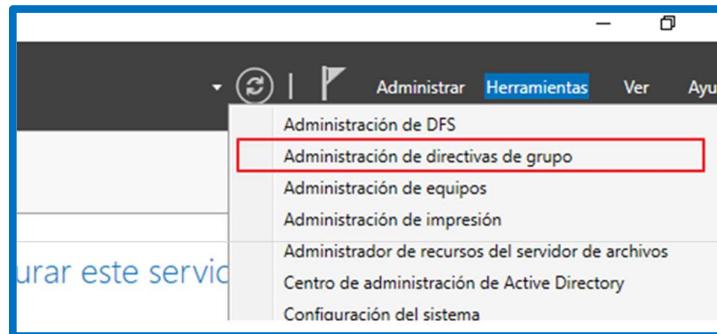
Hay dos ámbitos de las directivas, las locales y las del dominio. Las locales solo afectan al propio equipo, por ejemplo, las de nuestro servidor Windows Server las podemos encontrar aquí:



Si ejecutamos esta opción, veremos la lista de directivas:



Corresponde a todo lo que podemos configurar en el servidor en cuanto a acceso, seguridad, recursos, ... Pero las que nos interesan son las del dominio, que serán las que apliquemos a todos los equipos:



1.1. Valores de configuración de equipo y de usuario

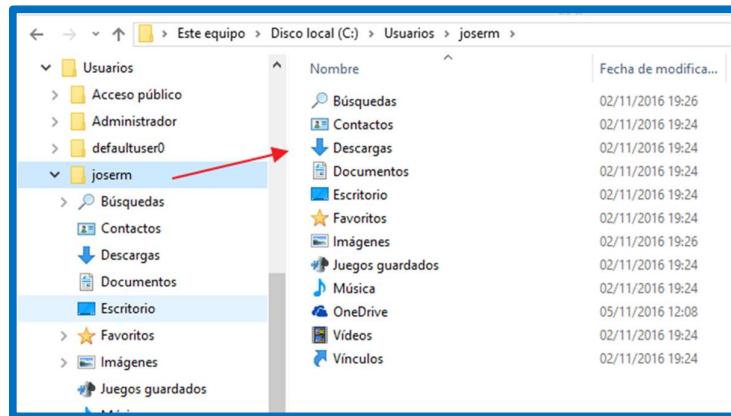
Segundo plano

Además de su ámbito (directivas locales o del dominio), existen dos tipos de directivas: las que se aplican a los equipos y las que se aplican a los usuarios. Las diferencias en principio no parecen muy claras, pero veamos varios ejemplos. Las directivas de equipo se activan cuando se enciende el ordenador afectando a toda la instalación de Windows. El ejemplo más claro es que creamos una directiva para que se instale una actualización de seguridad de Windows en los equipos. Cuando se enciendan estos equipos y, sin tener que iniciar la sesión, los equipos instalarán en segundo plano esa actualización de seguridad.

Instalación en segundo plano significa que es transparente para el usuario, no interviene en la instalación y no es consciente de que se está realizando.

Las directivas de usuarios se aplican a los perfiles de los usuarios

Cuando iniciamos una sesión en un equipo por primera vez, se crea un perfil de usuario con las carpetas comunes: mis documentos, favoritos, ... y otras de tipo temporal. Las carpetas que componen este perfil las podemos ver en la carpeta "document and settings" de los equipos, si es un Windows XP, o "Usuarios" en versiones posteriores:



Esta carpeta se crea para cada usuario que hace un inicio de sesión del equipo. De esta forma, el sistema mantiene la información de cada usuario en sitios independientes. Sólo los administradores y los propietarios de cada perfil tienen acceso a él. Las directivas de usuarios se aplican a cada usuario, aunque haga un inicio de sesión en distintos equipos. Por ejemplo, unas opciones de menú personalizadas según el departamento al que pertenezcan.

Ejemplo: quitar el acceso al panel de control.

Otro ejemplo: creamos una directiva para quitar el acceso al panel de control y así garantizarnos que los usuarios no hagan modificaciones del sistema. Si este usuario hace un inicio de sesión en el equipo, leerá estos cambios y Windows los aplicará en su perfil. Si este usuario inicia la sesión en otro equipo también se aplicará en el nuevo equipo. Asimismo, si hace un inicio de sesión un usuario que no tenga asignadas estas directivas de seguridad dispondrá de su entorno habitual. Esto es, se aplican siempre a los usuarios independientemente del equipo donde hayan iniciado la sesión.

Las directivas realmente realizan los cambios en el registro de Windows, que es donde reside toda la información de configuración del sistema y de los perfiles.

Detalles en las directivas de usuarios

1. Veamos algunos detalles que afectan a unas directivas y otras, en las directivas de usuarios:
 - Configuraciones específicas del sistema operativo. Configuraciones de escritorio.
 - Configuraciones de seguridad. Configuraciones de aplicaciones.
 - Opciones de redireccionamiento de carpetas.
 - Secuencias de comandos de inicio de sesión (logon scripts).
2. Para las directivas de equipos tenemos...
 - Valores de configuración de funcionamiento del sistema operativo.
 - Ambiente de los escritorios.
 - Configuraciones de seguridad del sistema operativo.
3. Dentro de la configuración de usuario también se encuentra:
 - La carpeta Software Settings: contiene configuraciones de software que se aplican a los usuarios sin importar en qué equipo inicien sesión.
 - La carpeta Windows Settings: contiene configuración Windows que se aplica a los usuarios sin importar en qué equipo inicien sesión. Esta carpeta también contiene los siguientes puntos: redirección de carpetas, valores de seguridad y secuencias de comandos.

Comportamiento del sistema operativo

Las directivas de equipo indican cómo se debe comportar el sistema operativo: escritorio, configuraciones de seguridad, inicios de sesión, opciones de aplicaciones asignadas al equipo y configuraciones de aplicaciones. Se aplican cuando el sistema operativo se inicia y durante un ciclo periódico de actualización. En general, las configuraciones de equipos sustituyen en caso de conflicto a las directivas de usuario.

Dentro de la configuración de equipo también se encuentra:

- La carpeta Software Settings: contiene las configuraciones de software que se aplican a todos los usuarios que inicien sesión en el equipo. Esta carpeta posee configuración de instalación de software.
- La carpeta Windows Settings: contiene configuraciones Windows que se aplican a todos los usuarios que inicien sesión en el equipo. Esta carpeta también contiene los siguientes puntos: valores de seguridad y secuencias de comandos.

Servicio NLA

El servicio NLA (Network Location Awareness) es un servicio de Windows utilizado para determinar cuándo se ha conectado un equipo a una infraestructura de directorio activo. La infraestructura de directivas de grupo utiliza este servicio para ver si necesita descargar y aplicar nuevas directivas de grupo.

1.2. Directivas locales

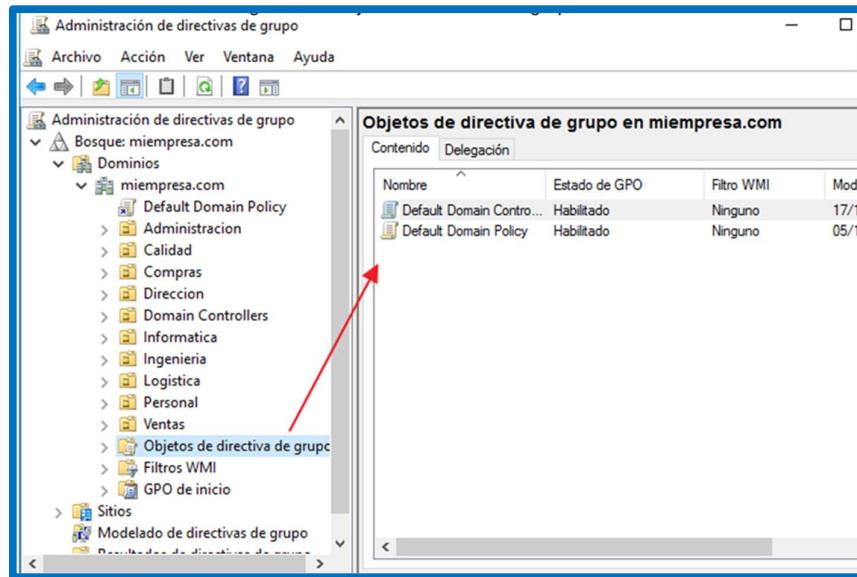
Como hemos comentado antes, tenemos dos tipos de directivas según su alcance: locales o de dominio. Las locales las tienen todos los equipos con Windows y las de dominio son las definidas para el bosque de nuestra organización (que en nuestros ejemplos se compone de un solo dominio "miempresa.com"). Obviamente las primeras solo afectan al equipo local y las segundas a los equipos del dominio o bosque que deseemos.

Como nuestro curso es con directorio activo y una organización mucho más controlada, estudiaremos las directivas de directorio o GPO.

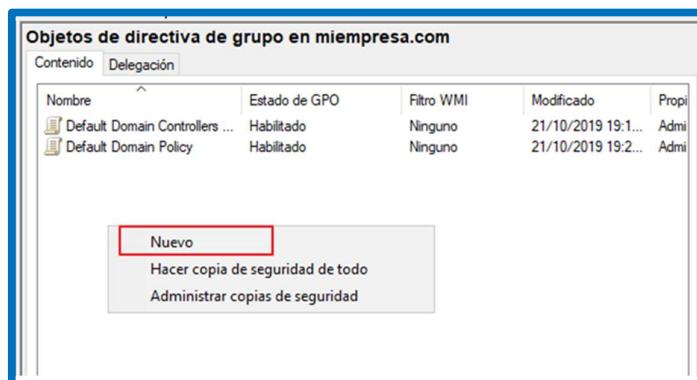
1.3. Ejemplo de directiva

1. Crear directiva

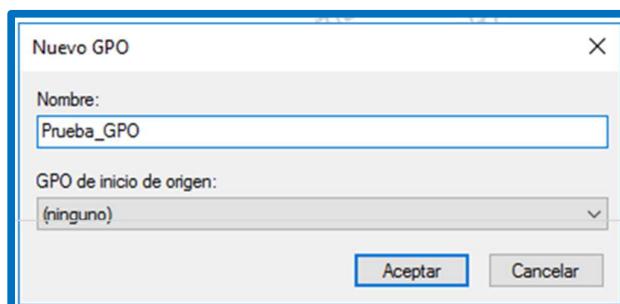
- Vamos a hacer una sencilla práctica para ver su funcionamiento. Dentro de las "Herramientas administrativas" abrimos el "Administrador de directivas de grupo". Luego lo veremos con más detalle, expandimos las ramas hasta llegar a los "Objetos de directiva de grupo":



- Esta carpeta es el contenedor de las directivas donde podemos ver que inicialmente tiene ya dos creadas. Pulsamos con el botón derecho para indicarle "Nuevo"



- Vamos a ponerle el nombre de "Prueba_GPO":



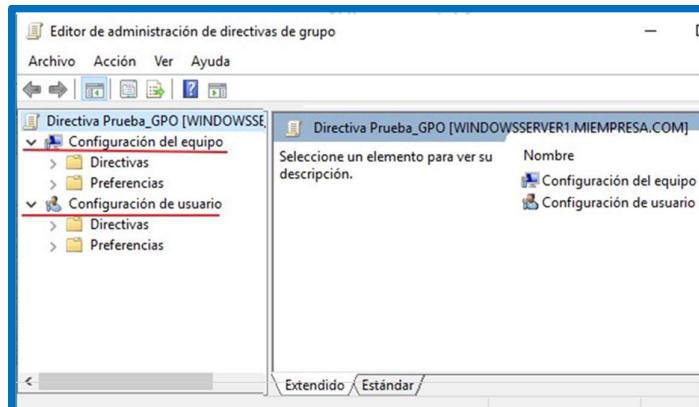
- Ya la tenemos creada, vacía todavía, pero creada:

Objetos de directiva de grupo en miempresa.com				
Nombre	Estado de GPO	Filtro WMI	Modificado	Propietario
Default Domain Controllers ...	Habilitado	Ninguno	21/10/2019 19:1...	Administrador
Default Domain Policy	Habilitado	Ninguno	21/10/2019 19:2...	Administrador
Prueba_GPO	Habilitado	Ninguno	01/11/2019 19:1...	Administrador

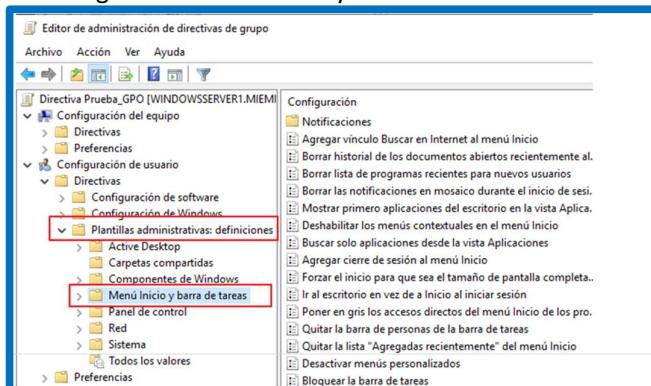
- Ahora pulsaremos con el botón derecho encima de ella para editarla:



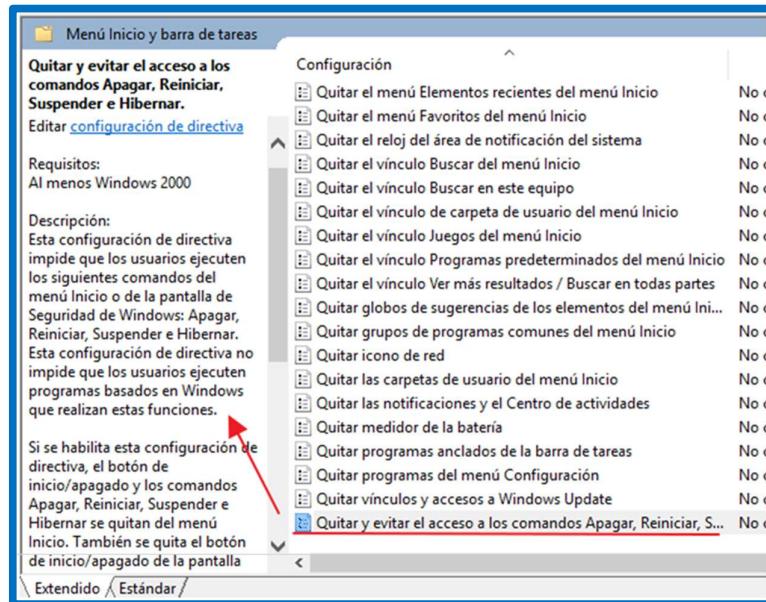
- Se abrirá el editor de directivas donde podremos modificar todas las opciones. Vemos que están los dos grandes grupos de directivas que hemos comentado antes: "Configuración del equipo" y "Configuración de usuario":



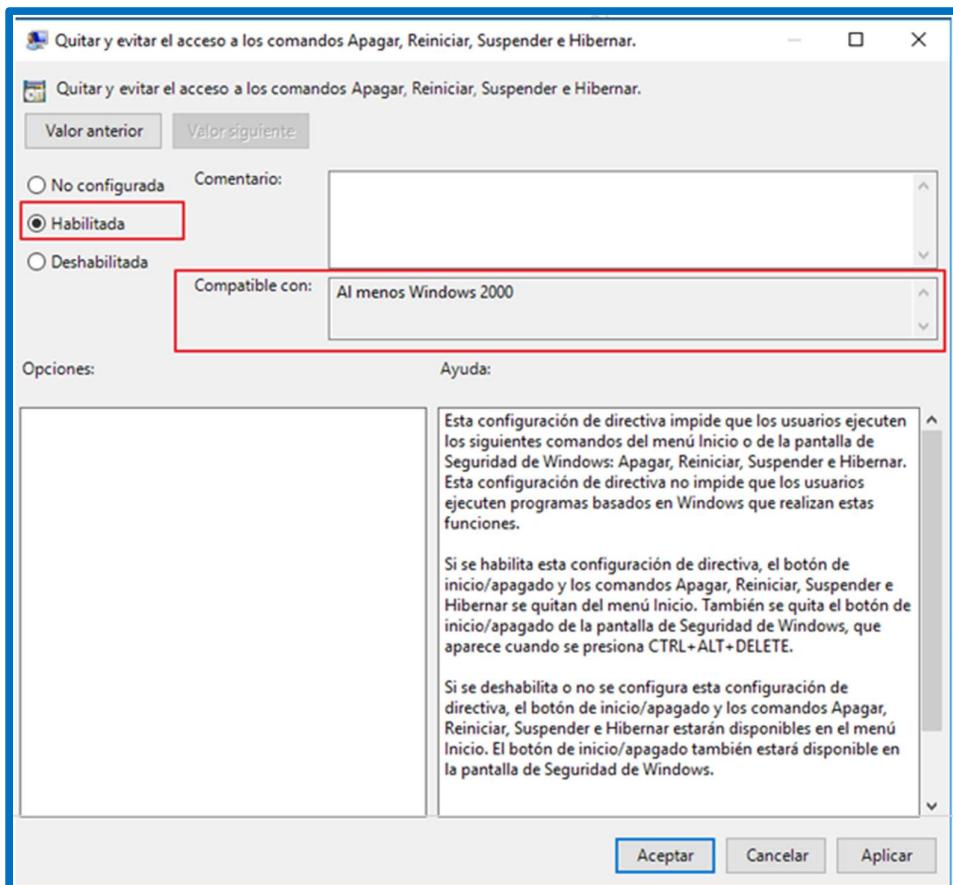
- La directiva que queremos implementar debe evitar que los usuarios apaguen su equipo con la opción de "apagar equipo". Es decir, modificaremos las opciones de su menú de inicio para quitar esta opción. Expandimos la sección "Configuración de usuario" y "Plantillas administrativas":



- Ahora seleccionamos la rama de la izquierda "Menú Inicio y barra de tareas" que nos mostrará una serie de directivas en la parte de la derecha:



- Si hacemos clic en "Configuración" se ordenarán de forma alfabética y corresponde justo con la última de ellas. Seleccionamos la directiva "Quitar y evitar el acceso a los comandos Apagar, Reiniciar, Suspender" y hacemos doble clic sobre ella:



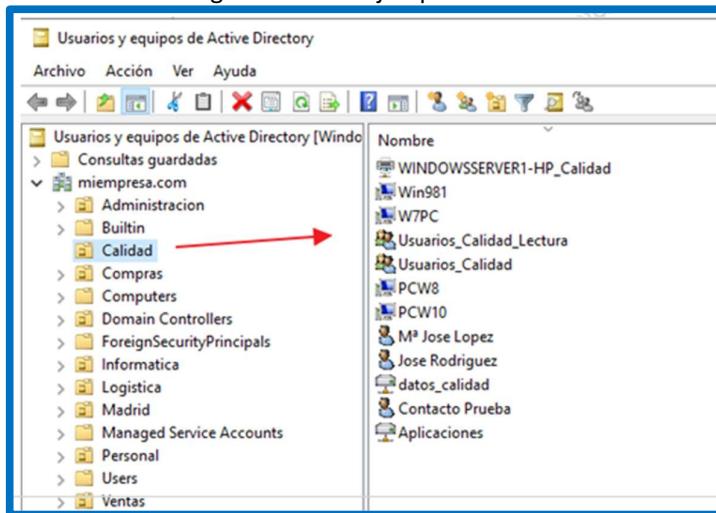
- Por defecto esta directiva está "no configurada", así que seleccionaremos la opción "Habilitada". Vemos que nos indica que debemos tener en los clientes al menos Windows 2000 como sistema operativo. En general deberemos tener en cuenta este mensaje para comprobar que se aplicará al sistema operativo que queramos.

Quitar medidor de la batería	No configurada
Quitar programas anclados de la barra de tareas	No configurada
Quitar programas del menú Configuración	No configurada
Quitar vínculos y accesos a Windows Update	No configurada
Quitar y evitar el acceso a los comandos Apagar, Reiniciar, S...	Habilitada

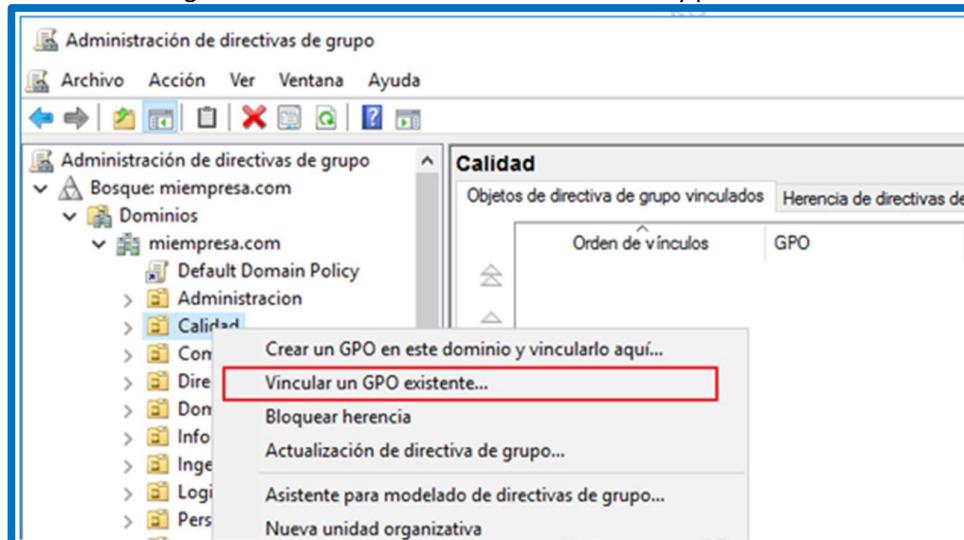
Si nos fijamos en la lista de directivas es la única que aparece como habilitada en esta sección. Las demás aparecen como "No configuradas".

2. Activar directiva.

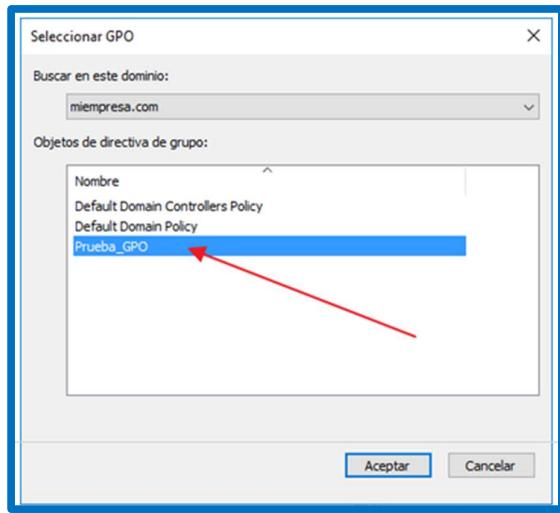
- Sigamos activando nuestra directiva. De momento la hemos creado en un contenedor, es decir, en una carpeta donde podemos ir definiendo distintas directivas que podremos ir asignando más adelante. Antes de aplicarla nos fijaremos en esta unidad organizativa de ejemplo:



- Vamos a aplicar la directiva sobre esta unidad organizativa. Como la directiva que hemos creado es de usuario, significa que se aplicará a los usuarios que estén dentro de esta unidad organizativa. Para vincularla, seleccionamos la unidad organizativa en el administrador de directivas y pulsamos con el botón derecho:



- Seleccionamos la opción de "Vincular una GPO existente":



- Indicamos ahora la directiva que hemos creado antes, quedando vinculada a la unidad organizativa "Calidad". Las sincronizaciones de las directivas se realizan cada cierto intervalo de tiempo, pero si queremos que se apliquen inmediatamente podemos forzarlo ejecutando el comando "gpupdate":

```

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Prueba la nueva tecnología PowerShell multiplataforma https://aka.ms/pscore6

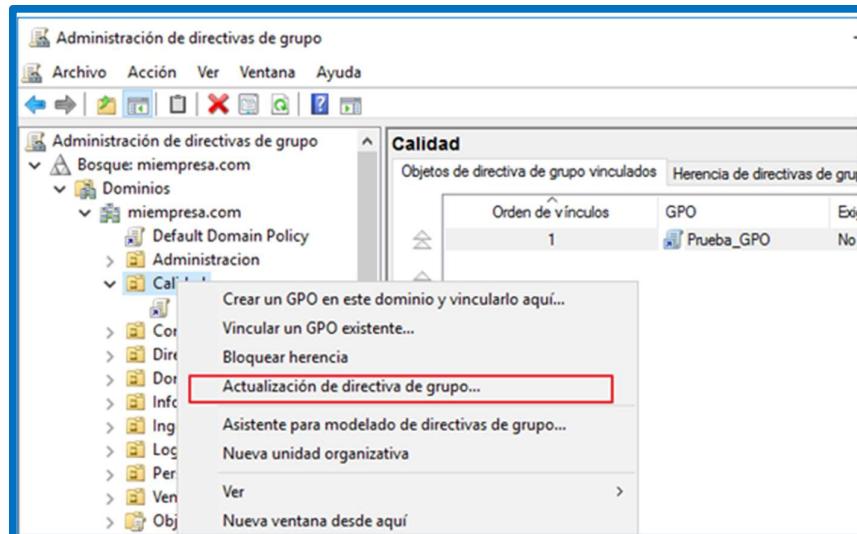
PS C:\Users\Administrador> gpupdate
Actualizando directiva...

La actualización de la directiva de equipo se completó correctamente.
Se completó correctamente la Actualización de directiva de usuario.

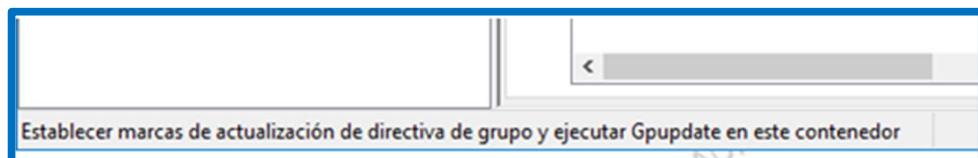
PS C:\Users\Administrador>

```

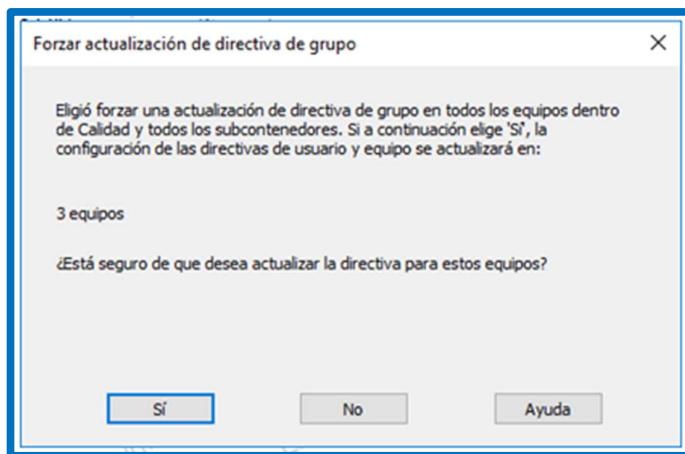
- Mejor dicho, esta era la forma que teníamos de hacer esta actualización hasta Windows 2012. Ahora disponemos de una opción en el menú para poder realizar esta operación de forzar que se aplique inmediatamente la directiva. Esta opción la tenemos en el menú contextual de las directivas:



- Si nos fijamos en la ayuda de la parte inferior nos avisa que ejecutará precisamente el comando que acabamos de comentar, Gpupdate:



- Al seleccionar esta opción nos avisará de a cuantos objetos se aplicará:



Puede que nos de error esta actualización debido a las reglas de cortafuegos, pero no pasa nada, se sincronizarán enseguida en los equipos. Si son directivas de usuario se actualizarán en el siguiente inicio de sesión y si son de equipo en el reinicio del equipo.

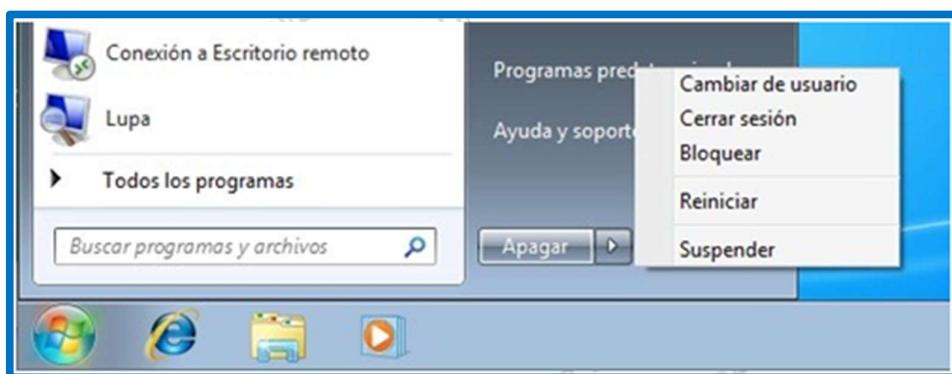
Importante: Probar con el usuario adecuado

Ojo, las directivas las hemos creado de usuario. Por tanto, debemos probarlas con usuarios que pertenezcan a la unidad organizativa en la que la hemos vinculado. Si iniciamos la sesión en los equipos con el usuario "administrador" no hará efecto, sin embargo, debería funcionar con el usuario "jrodriguez" que pertenece a esa OU.

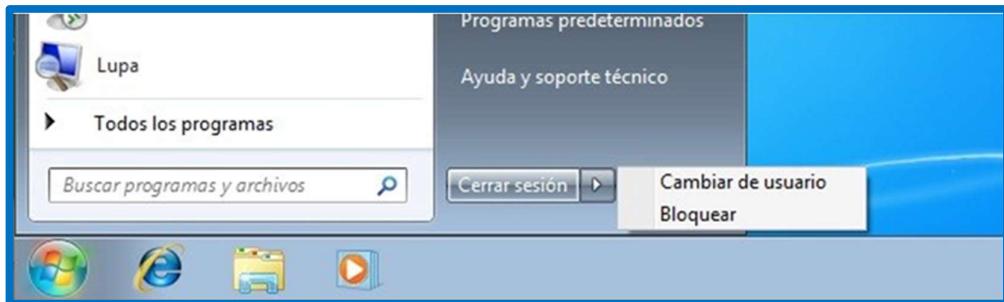
Si la directiva hubiera sido de equipo, habría afectado a todos los usuarios de ese equipo.

3. Probar el funcionamiento.

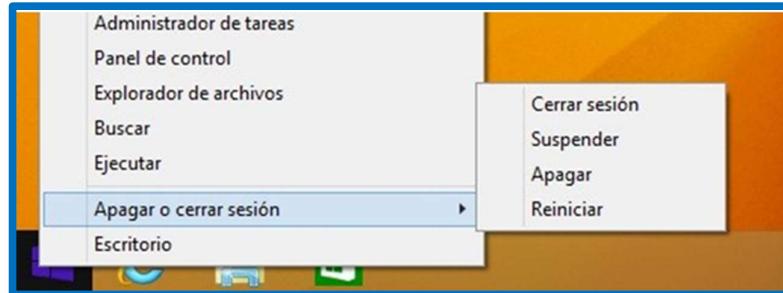
- Podemos probar ya si funciona. Vamos a fijarnos en el aspecto de los botones de Windows 7 antes de aplicar esta directiva:



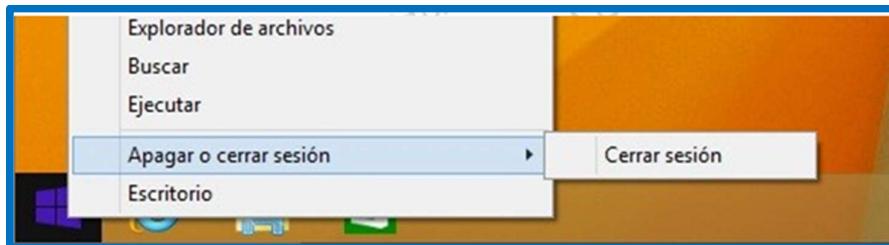
- Pero si aplicamos la directiva resulta que cambia a:



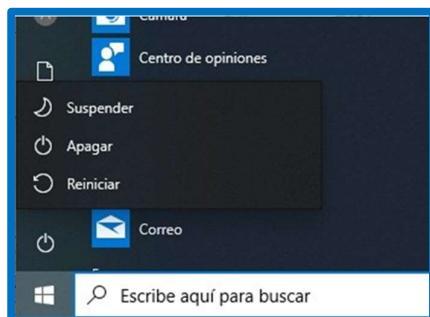
- Con Windows 8.1:



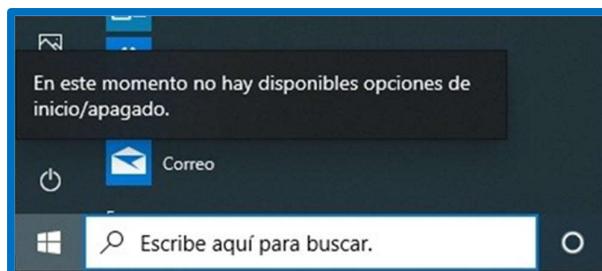
- Y después de la directiva:



- Con Windows 10:



- Al eliminarse las tres opciones ya no nos muestra ninguna:



- Han desaparecido las opciones de "Reiniciar, Suspender y Apagar" e incluso la opción predeterminada del botón es la de "Cerrar sesión" y no la de "Apagar", que la hemos suprimido con la directiva.

Importante: Usuario no afectado por la directiva

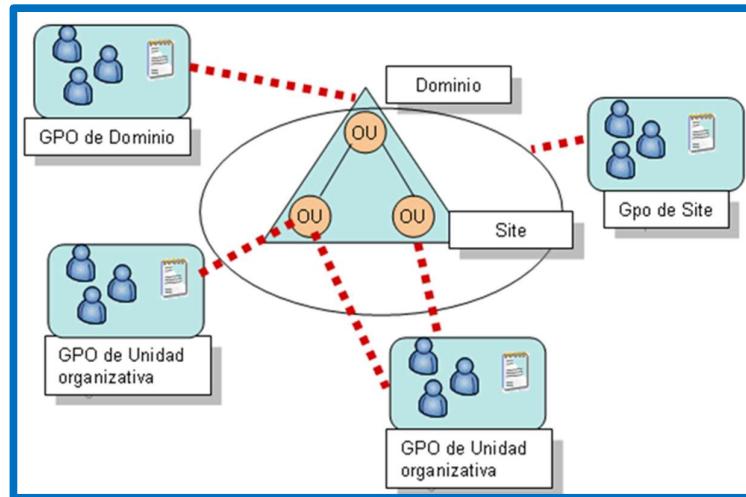
Si volvemos a hacer inicio de sesión con el usuario de administración "administrador@miempresa.com" todo volverá a la normalidad. Este usuario de administración no está en la unidad organizativa de "Calidad" y por tanto no le afecta esta directiva.

Ha sido una operación muy sencilla. Si nos hemos fijado un poco, habremos visto la cantidad de opciones que podemos modificar sólo en esta parte de menús... las posibilidades son realmente ilimitadas. Las directivas son una herramienta absolutamente imprescindible para tener controlada nuestra red.

Podemos, por ejemplo, crear una directiva que impida el acceso al panel de control: al aplicarse automáticamente a todos los equipos conseguimos que los usuarios no puedan modificar ningún parámetro del panel de control poniéndonos a salvo de los usuarios que les gusta modificar las configuraciones. Es algo imprescindible y, si bien al principio no las tendremos mucho en cuenta, con el tiempo veremos que es una herramienta fundamental para configurar nuestros equipos y usuarios. Todo esto redundará en una mejora de la administración al centralizar operaciones y evitar que los usuarios hagan operaciones no permitidas.

4. Vínculos de GPO

Todas las GPOs se almacenan en un contenedor del directorio activo llamado "Objetos de directivas de grupo". Cuando utilizamos una GPO en un sitio (site), dominio o unidad organizativa lo que hacemos es enlazar (link) una GPO con el contenedor de objetos de directivas de grupo. Automáticamente se crean todas en un directorio, esto es perfecto para tener siempre todas las directivas centralizadas. Esto va a facilitar mucho la sincronización con otros controladores de dominio del bosque, ya que, si están todas en una misma carpeta, aunque técnicamente se llama contenedor de objetos, es mucho más fácil de enviarlas a los otros servidores.



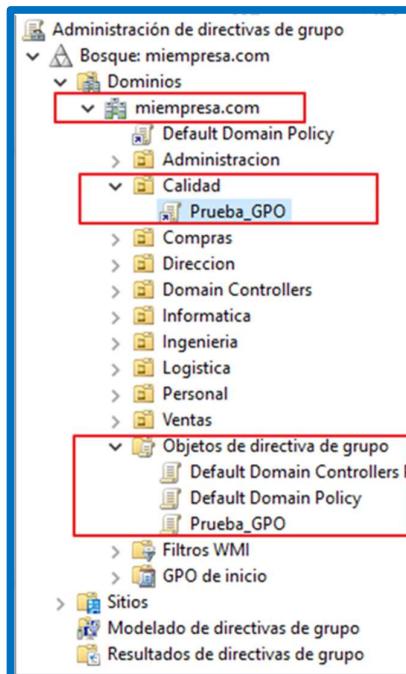
Cuando creamos un enlace a una GPO podemos hacer los dos pasos de una vez: crearla y enlazarla. En cuanto a permisos, solamente los miembros de los grupos "Administradores" y "Administradores del dominio" tienen los permisos necesarios para enlazar GPOs a dominios y unidades organizativas. Sólo los miembros del grupo "Enterprise Admins" tienen los permisos para enlazar GPOs a sitios.

Cuando creamos una GPO en el contenedor de directivas, la GPO no se aplica a ningún usuario o equipo hasta que se crea el enlace. Es decir, podemos crear directivas, pero si no las enlazamos no se activarán. Esto es importante porque podemos crear directivas y dejarlas almacenadas, pero sin vincular.

1.4. Herencia de permisos de GPO

1. Directivas a distintos niveles

Podemos establecer directivas a distintos niveles: sitios, dominios o unidades organizativas simplemente seleccionando el nivel en el que queremos vincularla. Hemos visto antes que había dos directivas ya creadas, vamos a fijarnos otra vez en el árbol:



2. Directivas vinculadas

Vemos que en el contenedor hay creadas tres directivas que pueden estar vinculadas o no. Ahora nos fijamos en el dominio "miempresa.com" donde podemos ver que a ese nivel está vinculada la directiva "Default Domain Policy". Debajo, en la unidad organizativa "Calidad", está vinculada la que hemos creado antes "prueba_GPO". Aquí vemos claramente que podemos vincular directivas a distintos niveles: bosques, dominios o unidades organizativas. En nuestro ejemplo sólo tenemos un nivel de unidades organizativas, pero es habitual tener varios niveles. Por ejemplo, dentro de informática dos unidades más que sean "sistemas" y "desarrollo" para agrupar a los usuarios de estos dos tipos de funciones.

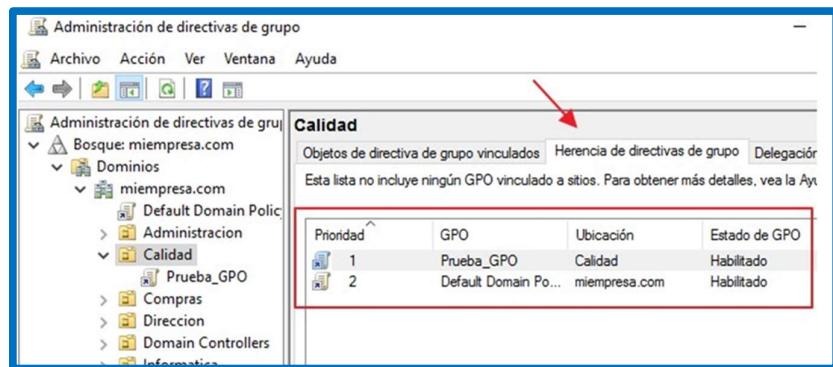
3. Orden

Cuando tenemos varios niveles ¿qué directiva se aplica primero? En este caso por defecto se "heredan" siempre las de los niveles superiores.

El orden en el que Windows Server aplica las GPOs depende del contenedor del Directorio Activo al que está enlazada o vinculada la GPO. Las GPOs se aplican primero al sitio, después a los dominios y por último a las unidades organizativas de los dominios.

4. Herencia

Un contenedor hijo hereda GPO's del contenedor padre. Esto significa que un contenedor hijo puede tener muchas GPO's aplicadas a sus usuarios y equipos sin tener una GPO enlazada directamente a él. Hacemos clic en la unidad organizativa de Calidad y nos fijamos en la derecha:



Vemos dos directivas:

- Prueba. Vinculada directamente en la unidad organizativa.
- "Default Domain Policy". Heredada de la raíz del dominio "miempresa.com". Al estar a un nivel superior, automáticamente y si no lo impedimos, se aplican a las unidades organizativas de nivel inferior.

Las GPO's son acumulativas, es decir, se van heredando. La herencia de las directivas de grupo es el orden en el cual Windows Server aplica las GPO's. Este orden y la herencia determinan que configuraciones afectan a usuarios y equipos. Si hay varias GPO's que definen un mismo valor tendrá preferencia la última GPO que se aplicó.

1.5. Conflictos en la GPO's

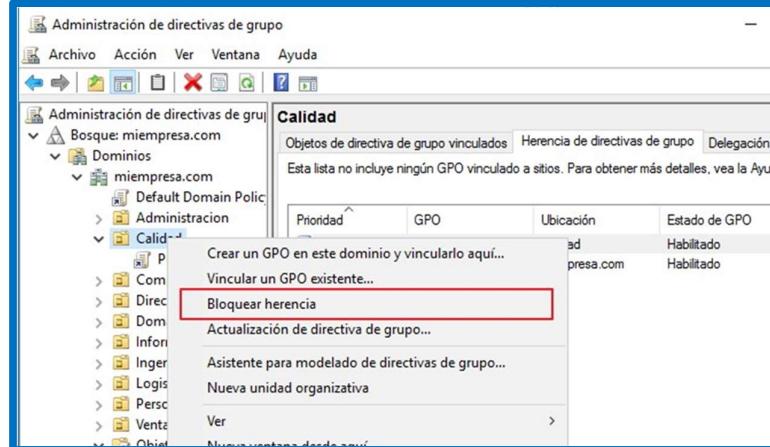
Las combinaciones complejas de GPOs pueden crear conflictos y, consecuentemente, requerir modificar el comportamiento de la herencia por defecto. Cuando una configuración de Group Policy se configura para una unidad organizativa padre (que tiene otras debajo) y la misma configuración de la GPO no se configura para la unidad organizativa hija, los objetos de esta última heredan la configuración de Group Policy de la unidad organizativa padre.

Cuando se configura una GPO para ambas (unidades organizativas padre e hija) se aplican las dos configuraciones. Si las configuraciones son incompatibles, la unidad organizativa hija conserva su propia configuración de GPO. Debemos estar atentos a esto último: en caso de conflicto de directivas va a prevalecer la que tenga la OU hija.

1. Modificar las reglas de herencia para GPOs específicas.

Si el orden de herencia por defecto no resuelve las necesidades de nuestra organización, podemos modificar las reglas de herencia para GPOs específicas. Disponemos de dos opciones para cambiar el orden de herencia por defecto:

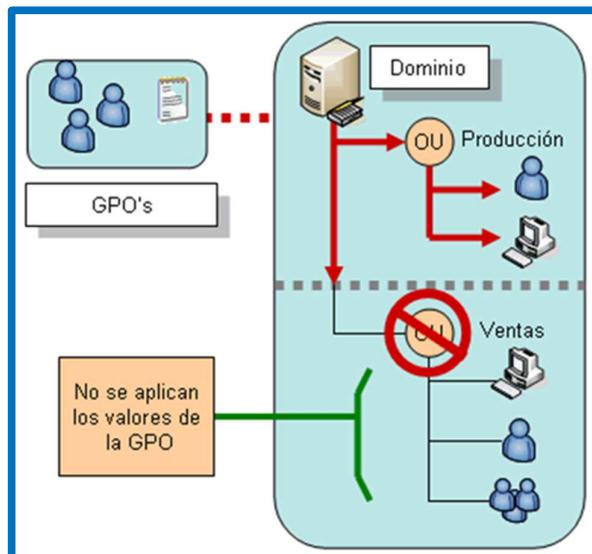
- **No reemplazar:** Esta opción se utiliza para prevenir que contenedores hijo eliminan una GPO con prioridad más alta de configuración. Esta alternativa es útil para hacer cumplir GPOs que representen reglas de negocio de la organización. La opción "No reemplazar" se fija sobre una base individual de GPO. Podemos fijar esta opción en una o más GPOs según lo requiera. Cuando se fija más de una GPO en "No reemplazar", la GPO más alta en la jerarquía fijada en "No reemplazar", tomará precedencia.
- **Bloquear herencia:** Esta opción se utiliza en contenedores hijo para bloquear herencia de todos los contenedores padres. Es útil cuando una unidad organizativa requiere una única configuración de GPO. "Bloquear herencia" se fija basándose en el contenedor. En caso de conflicto, la opción "No reemplazar" toma siempre precedencia sobre la opción "Bloquear herencia".



Tiene cierta similitud con los permisos de los ficheros. Automáticamente los ficheros adquieren los permisos de las carpetas padre. En este caso, sino lo impedimos, las unidades organizativas heredan los permisos de sus contenedores.

1.6. Bloqueo de despliegue de GPO.

Podemos prevenir en un contenedor hijo la herencia de cualquier GPO de los contenedores padre habilitando la opción "bloquear herencia" en el contenedor hijo. De esta manera, evitamos que el contenedor herede todas las configuraciones de las GPO. Esto es útil cuando un contenedor de directorio activo requiere GPO's únicas y deseamos asegurarnos que las configuraciones no se hereden.



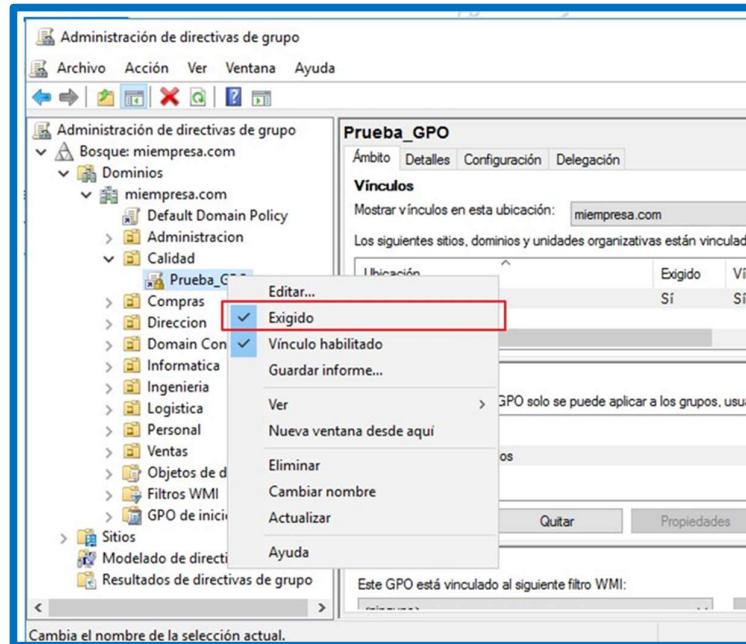
Al usar esta opción de bloquear la herencia debemos considerar lo siguiente:

- No se puede elegir selectivamente qué GPOs bloquea. Este bloqueo afecta a todas las GPOs de todos los contenedores padre, excepto las GPOs configuradas con la opción "Forzado".
- Bloquear herencia no bloquea la herencia de una GPO vinculada a un contenedor padre, si el enlace o vínculo se configura con la opción No reemplazar.

1.7. ¿Cómo configurar el "forzado" de las directivas?

Puede parecer complejo, pero al final todo es más sencillo de lo que parece. Es importante que tengamos claro el tema de las herencias de directivas y qué sucede en los conflictos.

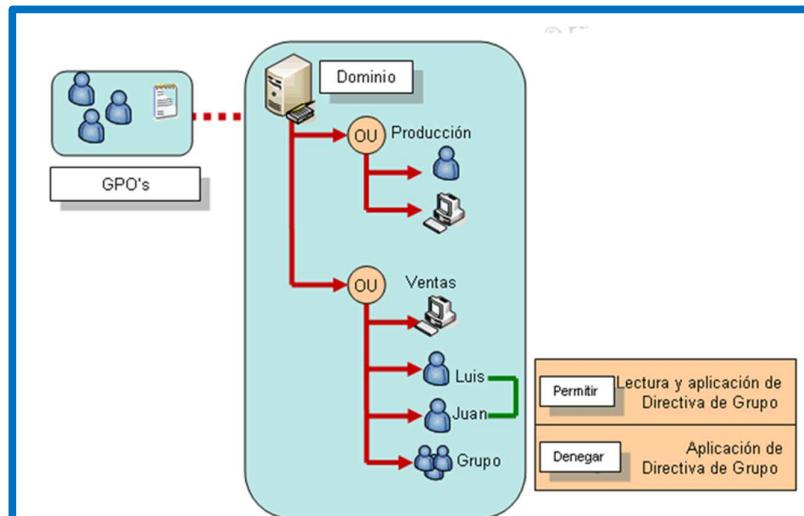
Veamos ahora como forzar un enlace de una GPO. Para hacer esto debemos seleccionar la GPO en el nivel que queremos: sitio, dominio o unidad organizativa. Luego con el botón derecho seleccionaremos "Exigido":



1.8. Filtrado del despliegue de GPO

Por defecto, todos los valores contenidos en las GPOs se aplican a todos los usuarios y equipos de ese contenedor. Esto puede producir efectos no deseados porque quisiéramos limitar o filtrar su aplicación. Esta opción se utiliza muy poco y te recomiendo un buen diseño de las unidades organizativas y GPO's para no utilizar este filtrado. Con estas características de filtrado podemos determinar qué configuraciones se aplican a los usuarios y a los equipos en el contenedor específico.

Lo mejor es que se apliquen a todo el contenedor que indiquemos y no tener que hacer un filtrado de unos si y otros no, pero bueno como existe esta posibilidad, la comentamos...



Podemos filtrar el despliegue de la GPO fijando permisos en el enlace o vínculo de la GPO para conceder el acceso de lectura o negar el permiso en la GPO. Para que se apliquen a una cuenta de usuario o de equipo, la cuenta debe tener por lo menos el permiso de lectura para una GPO. Los permisos por defecto para una GPO nueva tienen la siguiente entrada en el control de acceso (ACEs):

- Usuarios autenticados. Tiene permiso de lectura y aplicar GPO.
- Administradores del dominio (y similares). Tiene permiso de lectura, escritura, crear objetos hijo, eliminar GPO's.

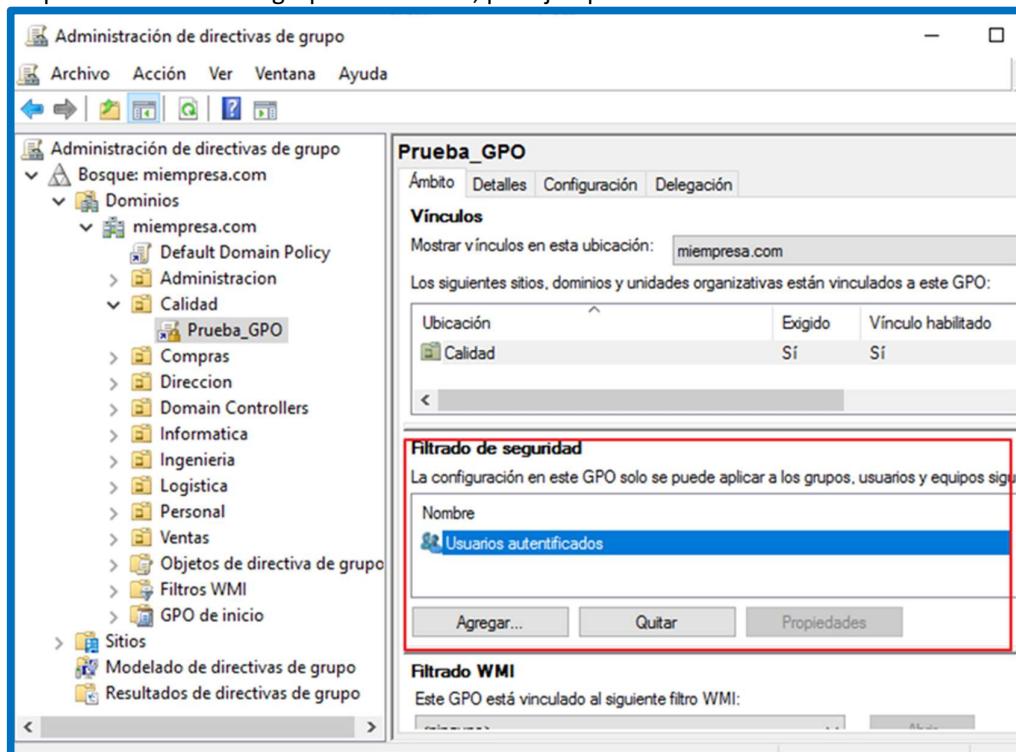
Utilizaremos los siguientes métodos de filtrado:

- Denegación explícita. Este método se utiliza al negar el acceso a la Group Policy. Por ejemplo, podríamos negar explícitamente el permiso al grupo de seguridad de los administradores, lo cual prevendría a los administradores en la unidad organizativa de la recepción de valores GPO.
- Remove "usuarios autenticados". Podemos omitir a los administradores de la unidad organizativa del grupo de seguridad, que significa que no tienen ningún permiso explícito para la GPO.

Veamos otra vez con detenimiento el gráfico anterior. Incluso con el mejor diseño posible de las unidades organizativas de nuestra empresa o de la infraestructura del directorio activo se nos puede dar el caso de que no queremos aplicar una GPO a ese grupo de equipos o usuarios. Para facilitar la selección de los usuarios o equipos tenemos la capacidad de filtrar a quienes queremos que se aplique. Veamos las formas en las que podemos realizar este filtrado:

a. Filtro de seguridad de GPO

Las directivas se aplican al grupo de seguridad "Usuarios autenticados", es decir, a los usuarios y equipos del dominio. Podemos modificar este ámbito para que, a pesar de que queremos aplicar la GPO a una unidad organizativa, le queremos indicar un grupo de usuarios, por ejemplo:



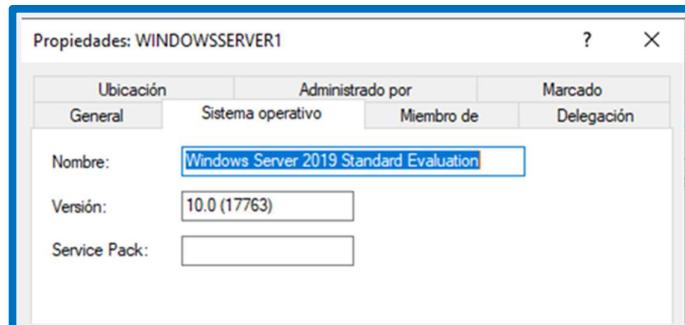
Podemos eliminar el grupo predeterminado y definir un grupo con los usuarios o equipos que queremos que se aplique. Obviamente, para que se aplique a esta unidad organizativa, los usuarios deben pertenecer además al grupo de seguridad que hemos definido.

b. Filtros WMI

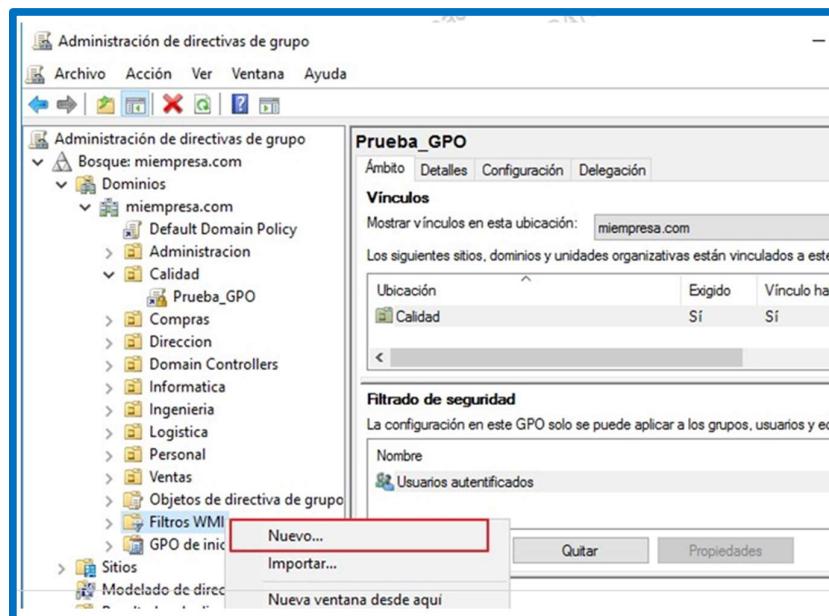
Un filtro WMI es una consulta que ejecuta el servidor y se utiliza para incluir o excluir determinados objetos. Es decir, en lugar de indicar un grupo de seguridad como antes, podemos definir una consulta al directorio activo para que se aplique o se excluya la directiva a los equipos/usuarios seleccionados.

1. Un ejemplo muy sencillo: podemos crear una consulta en las que se obtengan los equipos que tengan una determinada versión de sistema operativo, así se aplicaría esa directiva solo a esos equipos.

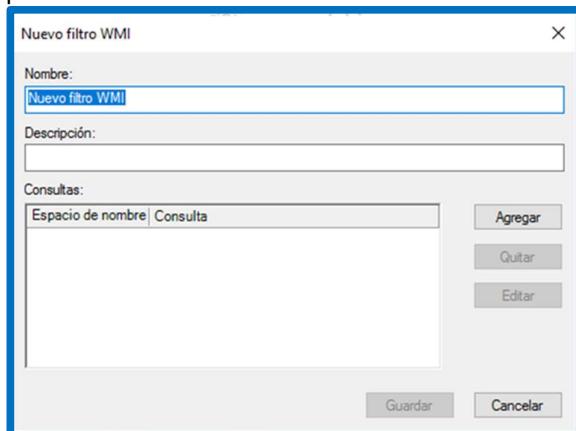
Windows 7 y Windows 2008 R2 corresponden a la versión 6.1 de Windows, Windows 8 y Windows 2012 son la versión 6.2 y Windows 10 y Server 2016/2019 la versión 10.0.



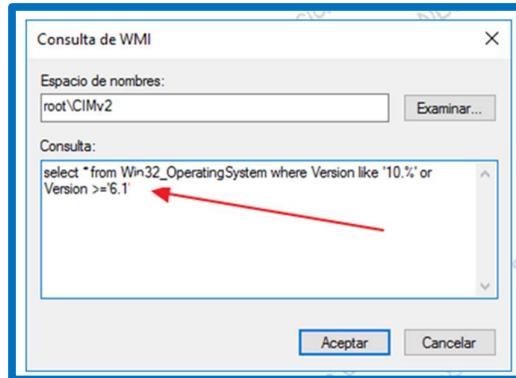
2. Vamos a crear un ejemplo. Nos vamos a la sección de filtros WMI y seleccionamos un nuevo filtro:



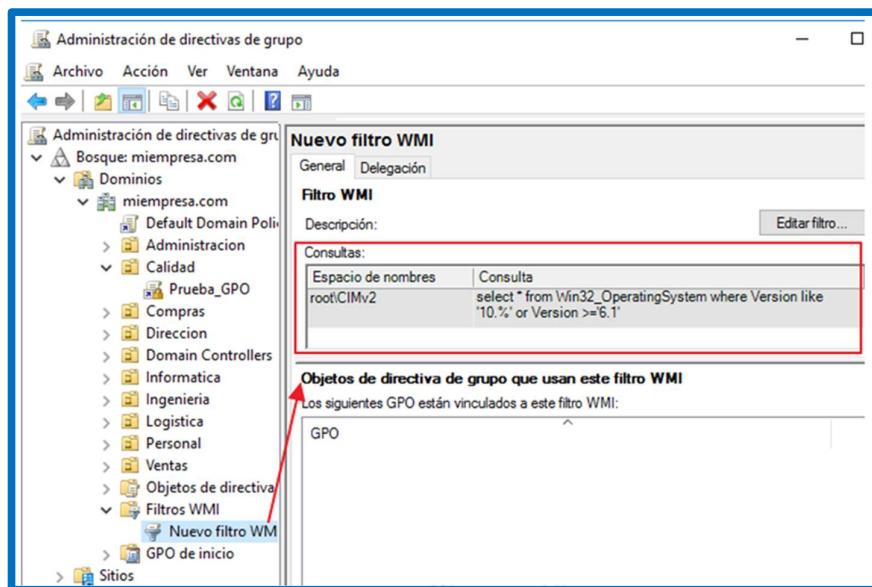
3. Nos mostrará una pantalla para introducir los datos identificativos:



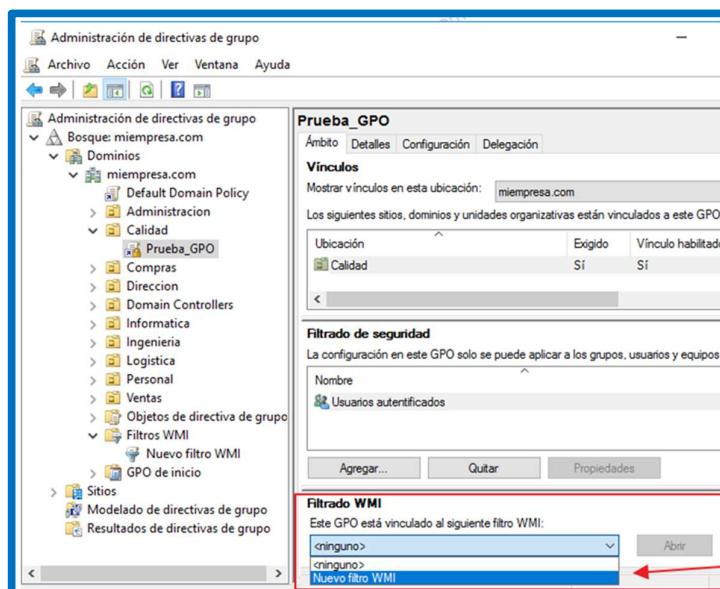
4. En "Aregar" pondremos la consulta que queremos ejecutar. En este ejemplo haremos una consulta SQL para que nos extraiga los equipos que ejecutan "Windows 8.1 o Windows 10", de esta forma:



5. Pulsaremos en aceptar y ya tendremos una consulta WMI lista para ejecutarse.



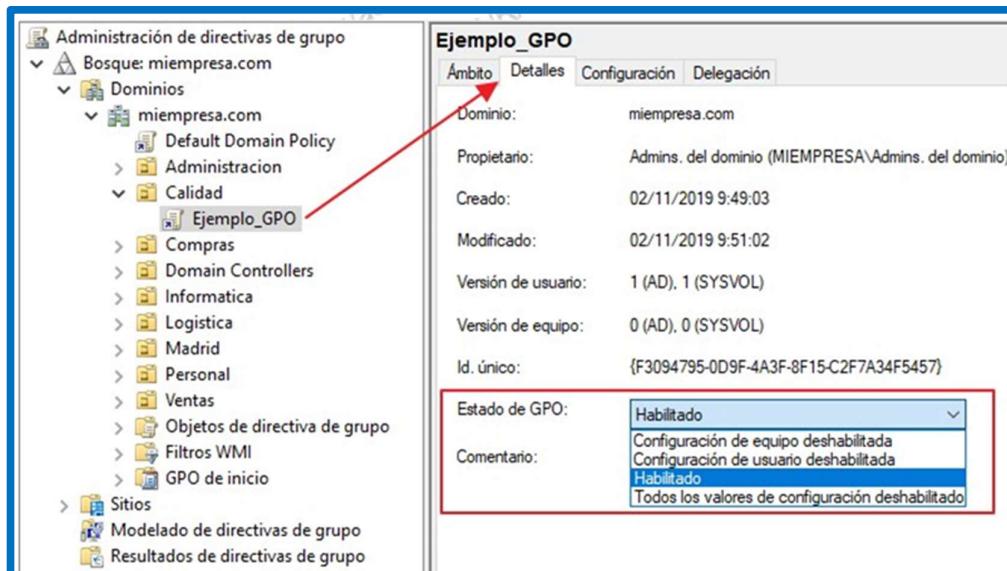
6. La ejecución no se hace desde esta pantalla, sino que enlazaremos GPO's para que seleccionen lo que hemos definido en esta consulta. Seleccionamos una GPO y miramos en la parte de abajo:



Asociaremos en la pantalla inferior de la GPO el filtro WMI definido. Cuando se aplique la directiva sólo se realizará sobre los usuarios o equipos que cumplan esa condición. Esto hace que sea muy versátil porque al ser dinámica la ejecución en el momento que alguien cumpla con estos criterios aplicará los valores definidos en la directiva.

c. Estado de GPO

Tenemos una opción donde vemos el estado de la directiva:



Lo habitual es que esté habilitada, pero podemos, desde aquí, deshabilitarla completamente o sólo las secciones de usuario o equipo.

2. Administración del entorno de usuario

La administración del entorno de usuario implica controlar lo que éstos pueden hacer cuando inician la sesión en la red. Esto se hace a través de las directivas de grupo controlando los escritorios, conexiones de red y las interfaces de usuario. Controlaremos el entorno de los usuarios para asegurarnos que tengan lo necesario para realizar sus trabajos. De esta manera, no podrán modificar o eliminar sus configuraciones y entorno.

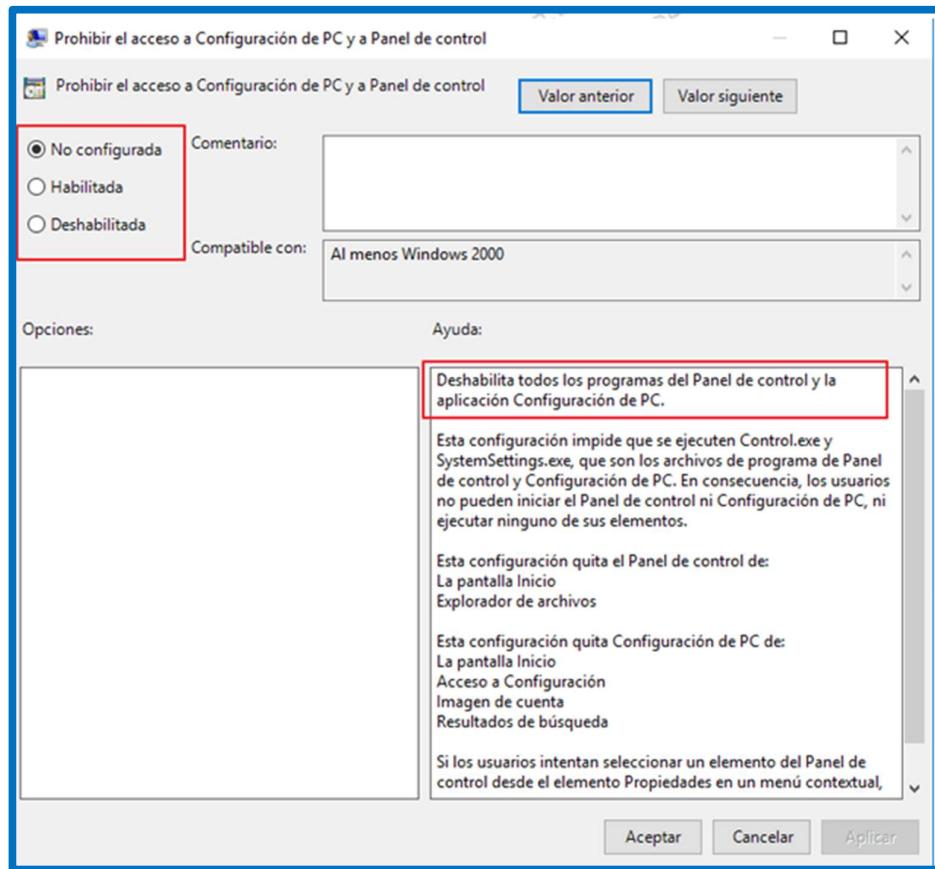
Cuando configuramos este entorno de forma centralizada podemos realizar:

- **Controlar los equipos y usuarios** Esto es posible configurando el escritorio del usuario con directivas basadas en entradas del registro. Así nos aseguramos que los usuarios tengan los mismos entornos, incluso como ya hemos comentado, si inician la sesión en equipos distintos. Además, podemos controlar cómo nuestro Server maneja los perfiles de usuario. Con la redirección de carpetas de usuario podemos también definir una ubicación central en un servidor, así podemos asegurar que los datos del usuario estén disponibles siempre sin importar el equipo desde el cual inicien sesión.
- **Despliegue de programas** Por despliegue entendemos a la instalación desatendida de programas. El software se instala en los equipos o en los usuarios. Con esta instalación podemos asegurarnos que los usuarios tengan sus programas, "service packs", y parches.

2.1. Habilitar y deshabilitar valores

Las directivas pueden tener distintos valores. Habitualmente las opciones son: "No configurada" que quiere decir que todavía no se ha establecido, "Habilitada" que está activada y "Deshabilitada" que estamos inhabilitando la opción (no la directiva). Hay que fijarse bien en el enunciado de la directiva. Por ejemplo, para el caso de una directiva que diga "Impedir al usuario que acceda al panel de control". Si está habilitada significa que no tendrá acceso y si está deshabilitada si tendrá acceso. Como por defecto está habilitado para los usuarios, si dejamos como "no configurada" causará el mismo efecto ya que tendrán acceso a él.

Ejemplo



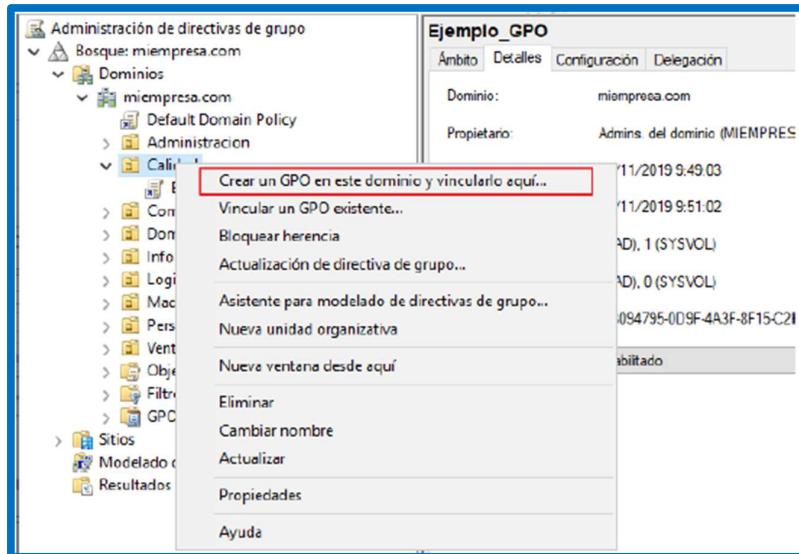
Cuando permitimos un valor estamos consintiendo la acción. Por ejemplo, para no permitir el acceso al panel de control podemos activar "Prohibir el acceso al panel de control". Por tanto, quedaría "habilitada" la prohibición del acceso al panel de control y los usuarios que tengan aplicada esta directiva no tendrán acceso a él.

Una GPO modifica los valores de registro en los usuarios y equipos en los que se aplica. La configuración por defecto de los valores de las directivas es "No configurada". Si queremos restablecer el valor de una directiva al valor que tenía predeterminado debemos seleccionarla y volveríamos a dejarla como "No configurada".

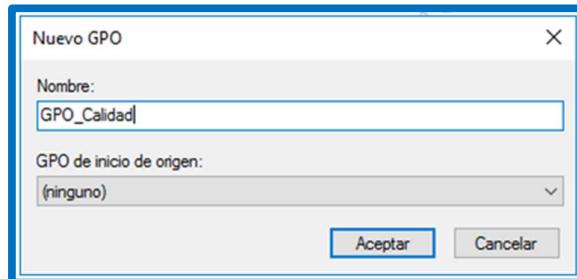
2.2. Editar un valor de una directiva

Crear una GPO

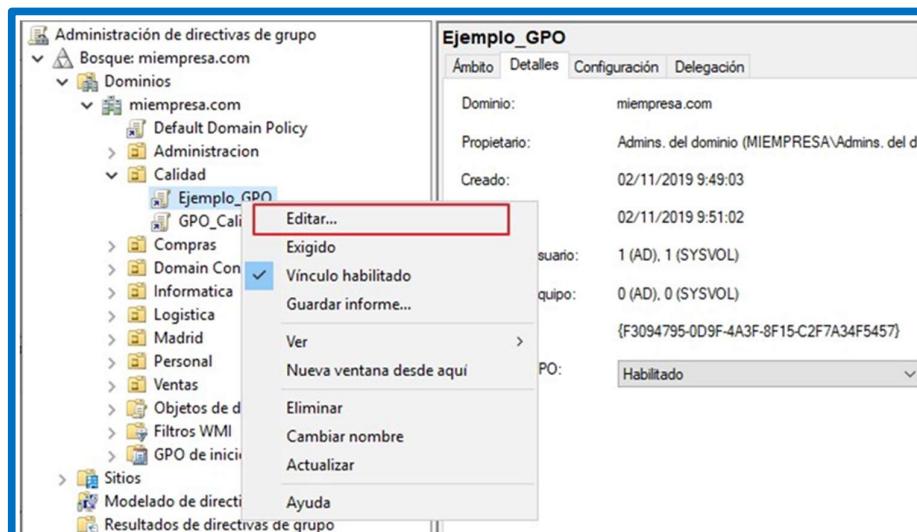
- Veamos todo el proceso completo. Hacemos clic en una unidad organizativa y seleccionamos "Crear una GPO en este dominio y vincularlo aquí":



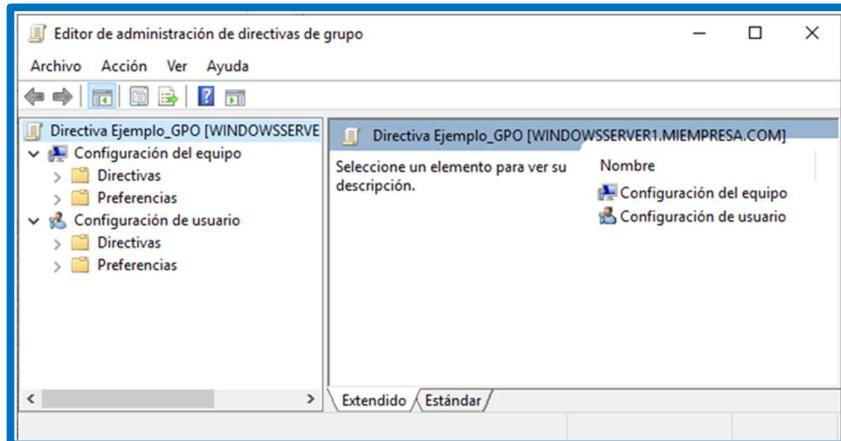
- Ponemos un nombre, por ejemplo "GPO_Calidad".



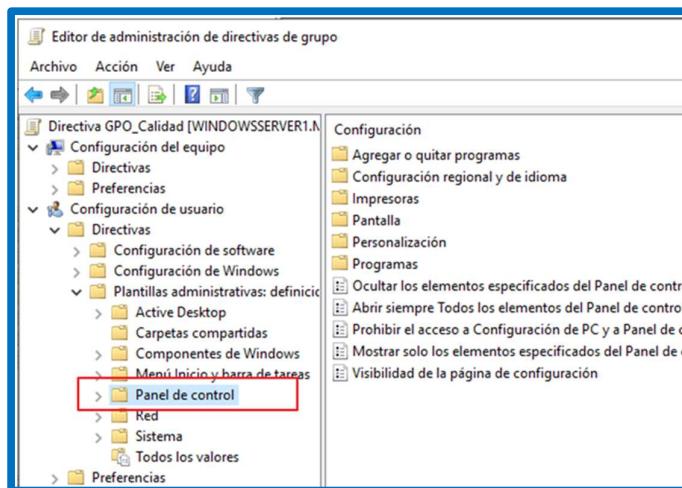
- Ahora pulsa con el botón derecho en la directiva y seleccionamos "Editar":



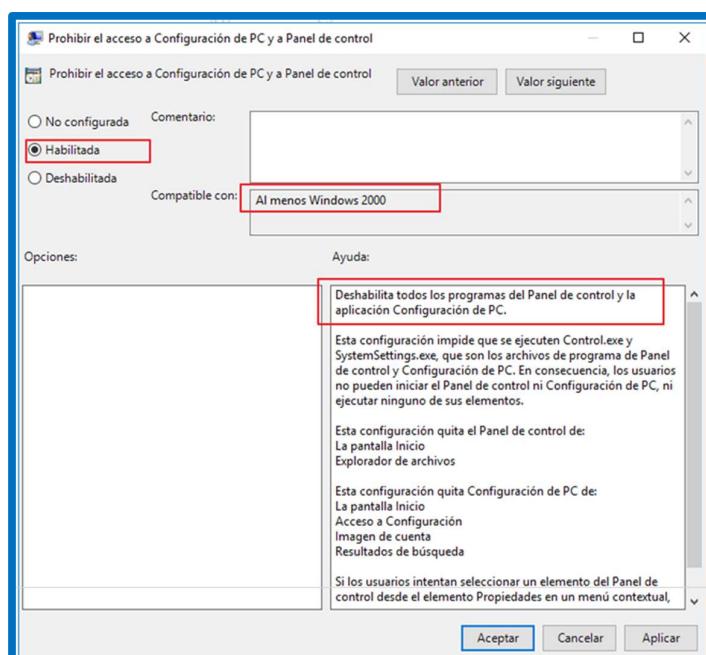
4. Ahora podemos modificar los valores que queremos de la directiva:



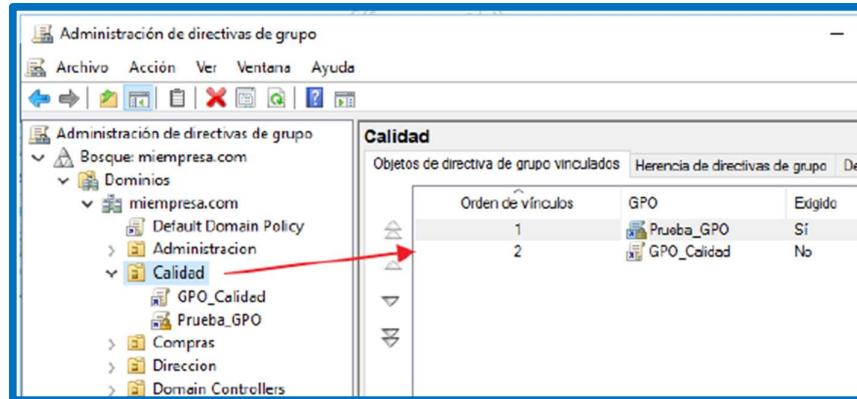
5. Por ejemplo, abrimos dentro de "Configuración de usuario" abrimos "Plantillas administrativas" y luego "Panel de control":



6. Aquí podemos definir varios valores para personalizar el funcionamiento del panel de control. Por ejemplo, hacemos clic en "Prohibir el acceso al Configuración de PC y Panel de control":



7. Activamos esta prohibición habilitando la directiva. Finalmente cerramos la ventana del "Editor de objetos de grupo" y volvemos a nuestra consola administrativa donde vemos a la derecha:



8. Corresponde a la directiva que acabamos de crear. Como vemos no está "exigida" porque no hemos utilizado esa opción, pero si está el vínculo habilitado porque la hemos "creado y vinculado". En la segunda solapa:

Prioridad	GPO	Ubicación	Estado de GPO
1 (exigido)	Prueba_GPO	Calidad	Habilitado
2	GPO_Calidad	Calidad	Habilitado
3	Default Domain Po...	miempresa.com	Habilitado

Vemos las directivas activas en este contenedor que es la unidad organizativa "Calidad". En este caso tiene la que acabamos de crear y las dos que estaban a nivel del dominio y OU Calidad.

Detalles de esta directiva

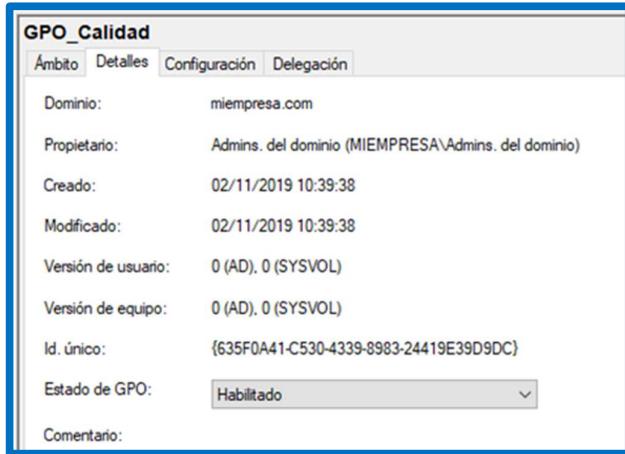
1. Ahora veremos más detalles de esta directiva: expandimos el árbol de la unidad organizativa donde hemos creado esta directiva y veremos qué aparece debajo de ella. Hacemos clic para ver más detalles a la derecha:

Filtrado de seguridad

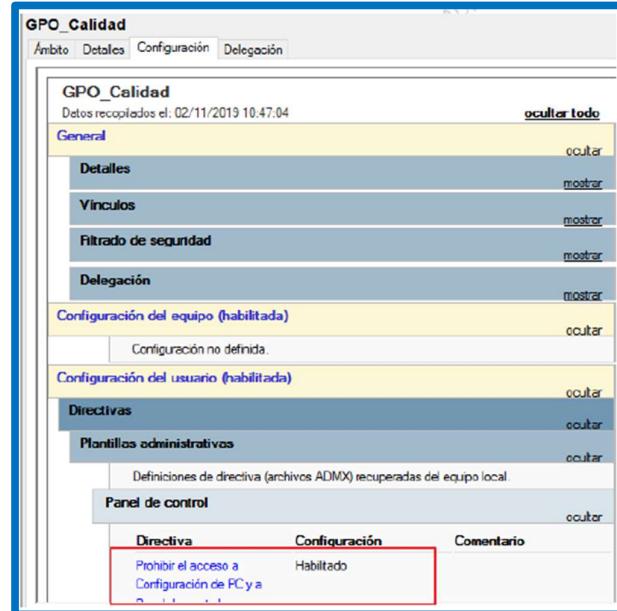
La configuración en este GPO solo se puede aplicar a los grupos, usuarios y unidades organizativas que cumplen con las siguientes condiciones:

- Nombre: Usuarios autenticados

2. A la izquierda aparecen la lista de las directivas aplicadas a esa unidad organizativa y a la derecha todos los detalles importantes. Para empezar en la primera solapa "Ámbito" vemos donde está vinculada "Informática" y debajo a quien se ha aplicado "Usuarios autenticados". Hasta ahora, estamos repasando todas las opciones que hemos visto antes. Aquí podríamos restringir esta directiva a sólo un grupo de usuarios en lugar de a todos los autenticados que son todos los de nuestro dominio. En la segunda pestaña: repasando todas las opciones que hemos visto antes. Aquí podríamos restringir esta directiva a sólo un grupo de usuarios en lugar de a todos los autenticados que son todos los de nuestro dominio. En la segunda pestaña:



3. Vemos los detalles completos de esta directiva y además en la parte de abajo podríamos deshabilitarla. En la tercera solapa:



4. Tenemos un informe con todos los valores que va a aplicar esta directiva. Esta pantalla es imprescindible para ver que valores se ha establecido. Inicialmente se muestra como un árbol donde si vamos haciendo clic en "Mostrar" se van expandiendo las opciones hasta llegar a "Texto de la barra de título", que es el valor de que hemos puesto antes en la directiva. Finalmente: haciendo clic en "Mostrar" se van expandiendo las opciones hasta llegar a "Texto de la barra de título", que es el valor de que hemos puesto antes en la directiva. Finalmente:

The screenshot shows the 'Configuración' tab of the 'GPO Calidad' properties window. It displays a table of permissions for groups and users:

Nombre	Permisos válidos	Heredado
Administradores de empresa...	Editar configuración, eliminar, modific...	No
Admins. del dominio (MIEMP...)	Editar configuración, eliminar, modific...	No
ENTERPRISE DOMAIN CO...	Lectura	No
SYSTEM	Editar configuración, eliminar, modific...	No
Usuarios autenticados	Lectura (de Filtrado de seguridad)	No

Nos muestra todos los permisos: administradores para editar la configuración y usuarios autenticados como "lectura" o receptores de la directiva.

2.3. Secuencias de comandos

Las secuencias de comando permiten ejecutar una serie de comandos para automatizar algunas tareas. Podemos utilizar secuencias de comandos o "scripts" para configurar secuencias centralizadas que se ejecutarán cuando se inicie y apague el equipo o cuando los usuarios inicien la sesión. Podemos especificar cualquier tipo de secuencias de comandos incluyendo los antiguos archivos por lotes (o batch), programas ejecutables y secuencias de comandos escritas con Windows Script Host (WSH).

Un ejemplo típico es crear una secuencia que ejecute un programa de bienvenida a la red y unos comandos para que nos asigne automáticamente las unidades de red de los servidores. Para ayudar a manejar y configurar los escritorios y entornos de los usuarios podemos:

- Ejecutar secuencias de comandos que realicen tareas que no se pueden hacer con directivas, por ejemplo, configurar impresoras, accesos directos, conexiones de red, ...
- Limpiar escritorios cuando los usuarios cierren la sesión.
- Ejecutar antiguos comandos Ms-DOS para compatibilidad con antiguas aplicaciones, ...

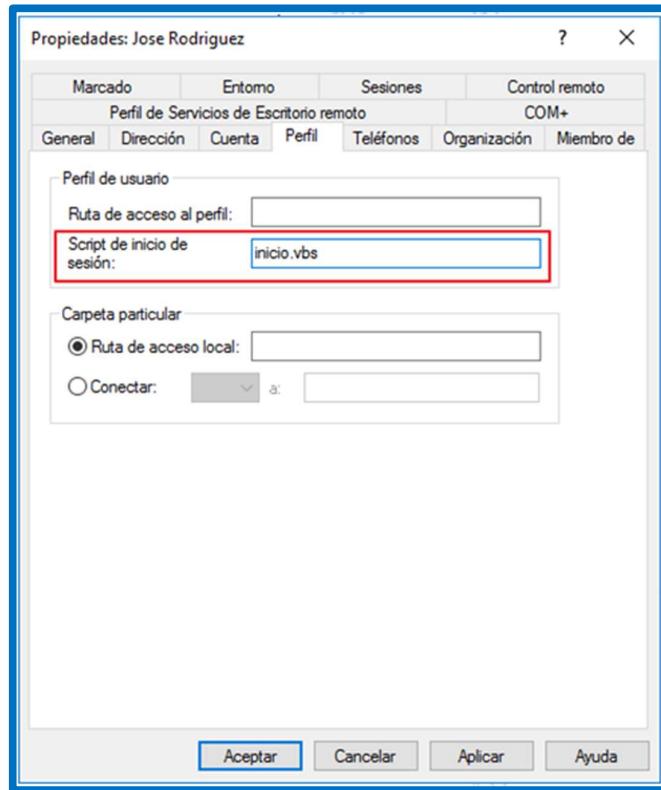
Podemos asignar estas secuencias desde la pantalla de la ficha de usuarios para que cada usuario tenga una secuencia distinta. Pero las directivas de grupo son la mejor forma para ejecutar estas secuencias de comandos.

¿Por qué no utilizamos PowerShell para esta programación? Muy sencillo, los clientes por defecto no tienen PowerShell instalado. Se trata de un módulo orientado a los servidores y puede que los clientes no lo tengan habilitado o instalado.

Práctica. Crear una secuencia de comandos y asignarla a una cuenta de usuarios

- Secuencias de comandos desde la ficha de usuario

1. Tenemos dos formas de asignar estas directivas. La primera forma es indicando en la ficha de usuario el fichero de la secuencia de comandos. En este caso nos iríamos a la consola "Usuarios y equipos" y en la ficha del usuario, indicarle el nombre de los archivos de comandos dentro de la solapa "Perfil":



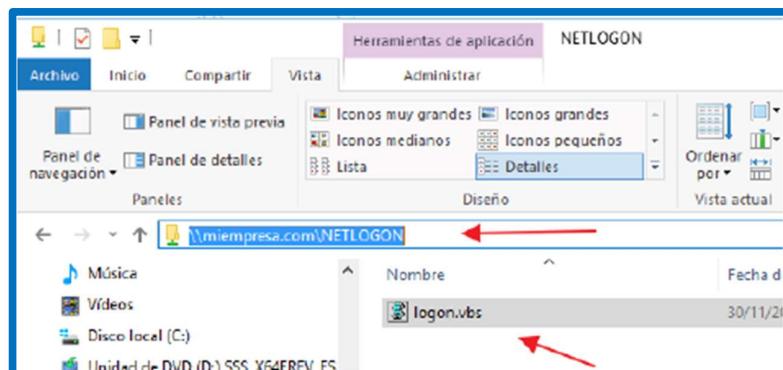
2. En el segundo cuadro de texto le indicamos el nombre del fichero de secuencia de comandos que queremos ejecutar. Los ficheros de WSH (secuencias de comandos) tienen de extensión .vbs. Un ejemplo de este fichero sería:

The screenshot shows a 'Bloc de notas' (Notepad) window titled 'logon.vbs: Bloc de notas'. The window contains the following VBScript code:
set wshShell = CreateObject ("WScript.Shell")
wshShell.run ("%logonserver%\netlogon\inicio.exe") (1)

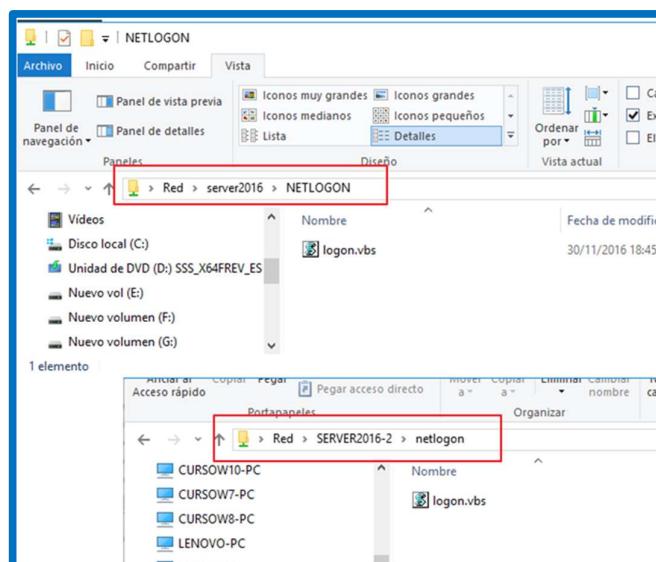
Set WshNetwork=Wscript.CreateObject ("WScript.Network") (2)
WshNetwork.MapNetworkDrive "F:", "\\\Server2016\datos"
The code consists of two numbered sections: (1) runs a local executable and (2) maps a network drive.

Este lenguaje necesita algo de aprendizaje, pero al estar basado en "visual basic" es sencillo de escribir. En el ejemplo primero ejecuta un programa (1) y luego hacer un mapeo de la unidad de red (2). El programa del punto 1 sólo es una pantalla de bienvenida que le mostramos al usuario.

3. Y un detalle, estos ficheros de secuencias de comandos deben almacenarse en un sitio especial que, al igual que en las directivas, va a permitir centralizar la ubicación de todos estos ficheros WSH. Esta ruta es la raíz del DFS "miempresa.com" donde hay una carpeta compartida para estos ficheros de secuencias de comandos:

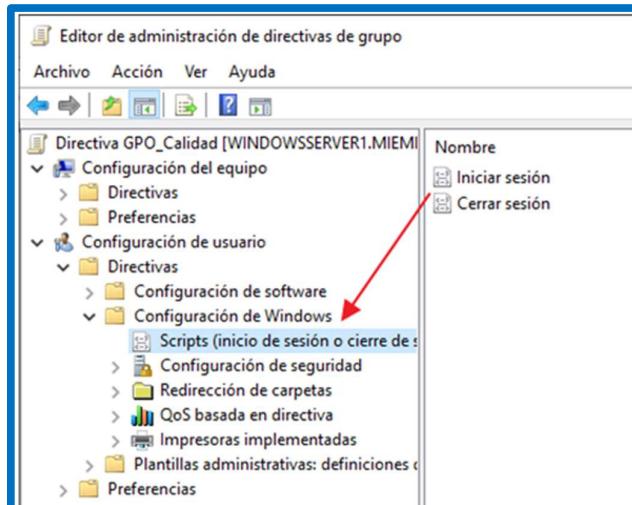


4. Al estar definido en el DFS se replicará en todos los controladores de dominio. Veamos nuestros dos servidores y las rutas físicas de los recursos compartidos:

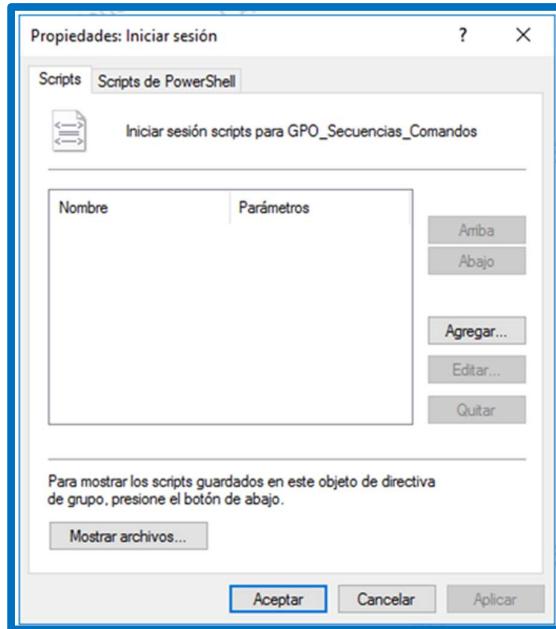


• Secuencias de comandos con directivas GPO

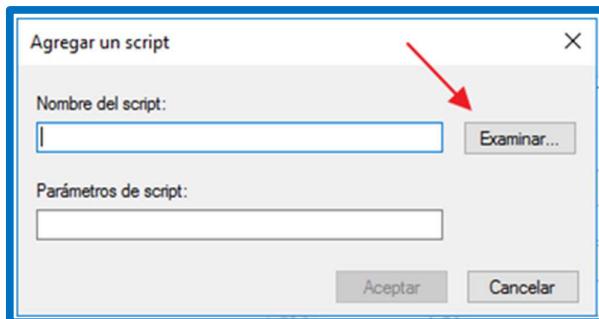
1. La otra forma de asignar estos scripts es mediante una directiva de grupo. Creamos una directiva o editamos una y vamos a la opción "Secuencias de comandos" dentro de la "Configuración de Windows" en la sección "Configuración de usuario":



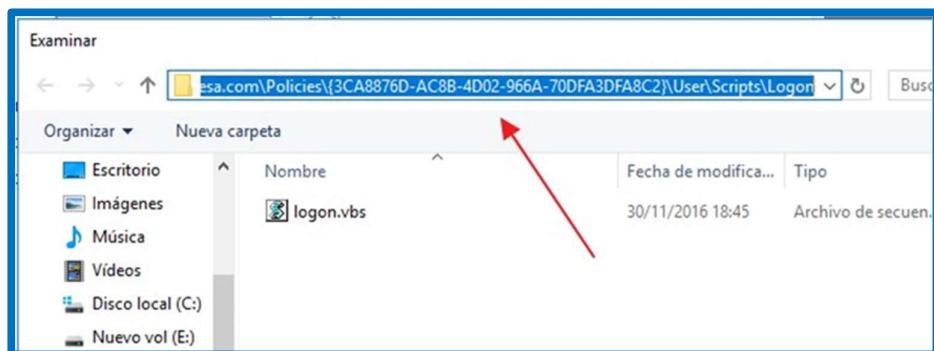
2. Vemos a la derecha las dos acciones en las que se pueden ejecutar estos comandos. Si hacemos doble clic:



3. En este cuadro podemos añadir una secuencia de comandos pulsando en "Añadir...":

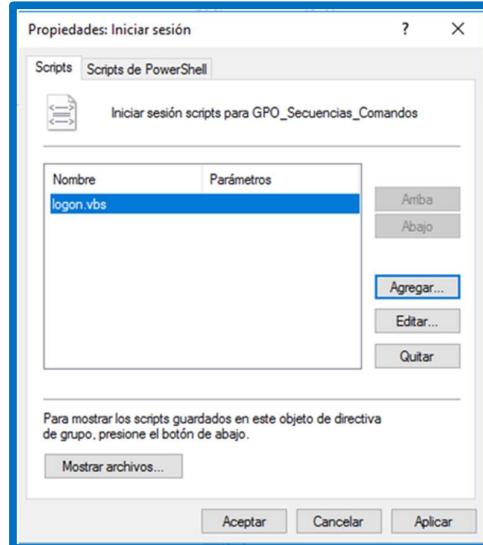


4. En el nombre escribiremos el nombre del fichero o pulsamos en "Examinar" que nos muestra la carpeta especial donde se almacenan estos ficheros.



La ruta incluye un identificador de la directiva "{3CA88... }\User\Scripts\Logon". Los parámetros del script corresponderían a opciones especiales para la ejecución de la secuencia de comandos.

5. Una vez metido en la lista podemos dar prioridad a unos ficheros u otros, modificarlos, eliminarlos:



Al ejecutar esa secuencia de comandos se ejecuta el programa que hemos creado y se "mapea" automáticamente la unidad de red así que garantizamos que está accediendo al servidor por si utilizase aplicaciones o datos remotos. Por ejemplo, al iniciarse Windows el usuario recibiría una pantalla de bienvenida.

2.4. Gpupdate

- Herramienta de línea de comandos**

Gpupdate es una herramienta de línea de comandos que actualiza los valores de las directivas de grupo. En ocasiones, y debido a las sincronizaciones que realizan los dominios, puede que estas directivas no se apliquen inmediatamente. Para forzar que se activen inmediatamente podemos abrir una consola y ejecutar el comando GPupdate. De esta forma, cuando estemos haciendo pruebas sabemos que se están aplicando, otra cosa es que funcione lo que hemos puesto. Por defecto, las configuraciones de seguridad se actualizan cada 90 minutos en un puesto de trabajo o un servidor, y cada cinco minutos en un controlador de dominio.

```
PS C:\Users\Administrador> gpupdate /?
Descripción: actualiza varias opciones de directiva de grupo.

Sintaxis: Gpupdate [/Target:{Computer | User}] [/Force] [/Wait:<valor>]
          [/Logoff] [/Boot] [/Sync]

Parámetros:

Valor           Descripción
/Target:{Computer | User} Especifica que solo se actualizan las directivas
                           del usuario o del equipo. De forma predeterminada,
                           se actualizan las directivas de ambos, usuario
                           y equipo.

/Force          Vuelve a aplicar toda la configuración de
               directivas. De forma predeterminada solo se
               aplicarán las directivas que cambiaron.

/Wait:{valor}   Establece el número de segundos de espera
               del final del proceso. El valor predeterminado
               es de 600 segundos. El valor "0" indica no
               esperar. El valor "-1" indica esperar de forma
               indefinida. Cuando se sobrepasa el tiempo
               límite, la línea de comandos se vuelve a mostrar
               pero se siguen procesando las directivas.

/Logoff         Produce un cierre de sesión luego de que se
               ha actualizado la configuración de directivas
               de grupo. Esto se requiere para las extensiones
               de directivas de grupo de cliente que no
```

Ejemplo:

- C:\gpupdate
- C:\gpupdate /target:equipo
- C:\gpupdate /force /wait:100
- C:\gpupdate /boot

- **Parámetros**

Gpupdate tiene los siguientes parámetros.

- **/Target:{equipo | usuario}**. Especifica la actualización solamente para un usuario o equipo. Por defecto se actualizan las dos.
- **/Force**. Vuelve a aplicar todas las directivas creadas. Por defecto solamente se aplican las que se hayan cambiado.
- **/Wait:{Value}**. Fija el número de segundos para esperar el procesamiento de la directiva. Por defecto, es de 600 segundos. El valor ' 0 ' significa no esperar. El valor ' -1 ' significa esperar indefinidamente.
- **/Logoff**. Causa un cierre de sesión después de actualizar la configuración.
- **/Boot**. Provoca que el equipo se reinicie después de la actualización.
- **/Sync**. Provoca que la próxima configuración se aplique sincrónicamente.

2.5. Gpresult

Puede que en ocasiones se apliquen muchas directivas distintas y queremos generar un informe de las que se han aplicado a un equipo o usuario.

El comando gpresult muestra los valores de las directivas de grupo de un usuario o equipo. Así que utilizaremos "gpresult" para ver qué configuraciones de las GPOs son efectivas y localizar problemas en la aplicación.

```
PS C:\Users\Administrador> gpresult /?
GPRESULT [/S sistema [/U usuario [/P [contraseña]]]] [[/SCOPE ámbito]
[/USER usuarioDestino] [/R| /V| /z] [/C/X| /H] <archivo> [/F]

Descripción:
Esta herramienta de línea de comandos muestra información del conjunto
resultante de directivas (RSOP) para un usuario y equipo de destino.

Ejemplos:
GPRESULT /R
GPRESULT /H GPReport.html
GPRESULT /USER usuario_destino /V
GPRESULT /S sistema /USER usuario_destino /SCOPE COMPUTER /Z
GPRESULT /S sistema /U usuario /P contraseña /SCOPE USER /V
    no se puede usar con /A, /H.
```

Ejemplos:

Los ejemplos siguientes muestran cómo se puede utilizar el comando gpresult:

- C:\gpresult /user targetusername /scope computer
- C:\gpresult /s srvmain /u maindom/hiropln /p p@ssW23 /user targetusername /scope USER
- C:\gpresult /s srvmain /u maindom/hiropln /p p@ssW23 /user targetusername /z >policy.txt
- C:\gpresult /s srvmain /u maindom/hiropln /p p@ssW23

- **Parámetros**

Gpresult tiene los siguientes parámetros.

- **/s equipo**. Especifica el nombre o dirección IP de un equipo remoto. Por defecto es el equipo local.
- **/u Domain/User**. El comando funciona con los permisos de la cuenta del usuario que se especifica User o Domain/User. Por defecto son los permisos del usuario que se encuentre autenticado en el equipo que ejecuta el comando.
- **/p Password**. Especifica la contraseña de la cuenta del usuario que se especifica en el parámetro **/u**.
- **/user TargetUserName**. Especifica el nombre del usuario del que se exhiben los datos RSOP.
- **/scope {user|computer}**. Muestra los valores del usuario o equipo. Los valores válidos para el parámetro **/scope** son user o computer. Si se omite el parámetro **/scope**, gpresult exhibe ambos, usuario y equipo.
- **/v**. Muestra información con más detalle.
- **/z**. Muestra toda la información disponible sobre la directiva. Dado que este parámetro produce más información que el parámetro **/v**, se debe redirigir la salida a un archivo de texto cuando se utilice este parámetro (por ejemplo, se puede escribir **gpresult /z >directiva.txt**).
- **/?**. Muestra la ayuda en la ventana de comandos.

- **Consulta en ejecución para el usuario "administrador"**

Veamos esta consulta en ejecución. Vamos a comprobar la directiva que se está aplicando para el usuario "administrador" y para el usuario "jrodriguez". Como éste último está en la unidad organizativa de "Calidad", le afectará la directiva de la restricción de acceso al panel de control y de los botones de apagar:

```
CONFIGURACIÓN DE USUARIO
-----
CN=Administrador,CN=Users,DC=miempresa,DC=com
Última vez que se aplicó la Directiva de grupo: 02/11/2019 a las 11:14:06
Directivas de grupo aplicadas desdeWindowsServer1.miempresa.com
Umbral del vínculo de baja velocidad de las Directivas de grupo:500 kbps
Nombre de dominio: MIEMPRESA
Tipo de dominio: Windows 2008 o posterior

Objetos de directiva de grupo aplicados
-----
n/a

Los objetos GPO siguientes no se aplicaron porque fueron filtrados
-----
Directiva de grupo local
    Filtrar: No aplicado (vacío)

El usuario es parte de los siguientes Grupos de seguridad
-----
Usuarios del dominio
Todos
Usuarios
Administradores
NT AUTHORITY\INTERACTIVE
INICIO DE SESIÓN EN LA CONSOLA
Usuarios autenticados
Esta compañía
```

- **Consulta en ejecución para el usuario "jrodriguez"**

Y para el usuario "jrodriguez":

```
CONFIGURACIÓN DE USUARIO
-----
CN=Jose Rodriguez,OU=Calidad,DC=miempresa,DC=com
Última vez que se aplicó la Directiva de grupo: 02/11/2019 a las 10:23:47
Directivas de grupo aplicadas desdeWindowsServer1.miempresa.com
Umbral del vínculo de baja velocidad de las Directivas de grupo:500 kbps
Nombre de dominio: MIEMPRESA
Tipo de dominio: Windows 2008 o posterior

Objetos de directiva de grupo aplicados
-----
Ejemplo_GPO

Los objetos GPO siguientes no se aplicaron porque fueron filtrados
-----
Directiva de grupo local
    Filtrar: No aplicado (vacío)

El usuario es parte de los siguientes Grupos de seguridad
-----
Usuarios del dominio
Todos
Usuarios
Administradores
NT AUTHORITY\INTERACTIVE
INICIO DE SESIÓN EN LA CONSOLA
Usuarios autenticados
Esta compañía
LOCAL
```

Es una buena herramienta para saber si a determinado usuario y/o equipo se le está aplicando la directiva. Ya hemos visto un poco de las directivas y dada su gran importancia para configurar o mantener una configuración homogénea en nuestra red veremos más cosas en la siguiente unidad...

3. Elementos de las GPO

Veamos ahora más técnicamente los elementos de las GPO, así comprenderemos mejor su funcionamiento.

Recuerda: Objetos GPO

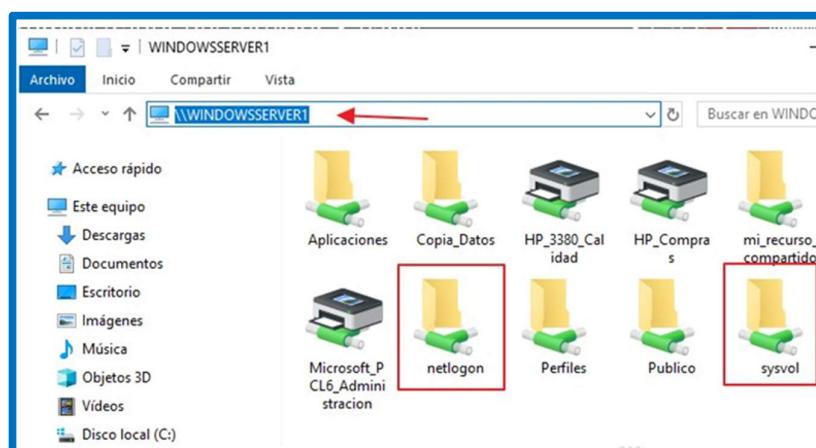
Las GPO, como ya sabemos, son una serie de valores que se aplican en los usuarios o equipos del directorio activo. Estos valores se configuran con las plantillas que se obtienen con el editor pudiéndose ampliar para configurar otros valores. Esto es interesante, porque podremos ampliar las directivas con nuevos elementos. Por ejemplo, se publica un nuevo Service Pack para Windows 10 en el que se ofrece un nuevo cortafuegos mucho más avanzado, por ejemplo. Con la consola de Windows 2008 no podríamos configurar ese cortafuegos porque no tendríamos las directivas adecuadas. Sin embargo, existe la posibilidad de ampliar las directivas para recoger las funcionalidades de nuevos programas y así poder configurarlos.

3.1. Almacenamiento y replicación de las GPO

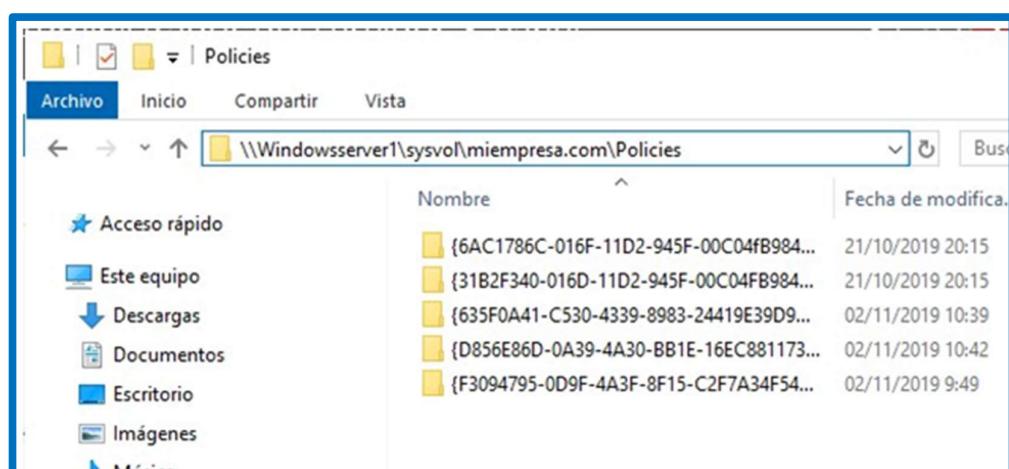
Las GPO se almacenan en el sistema de ficheros y en la base de datos del directorio activo. Cada dominio del bosque del directorio activo almacena una copia completa de las GPO's de su dominio.

Dentro del directorio activo, los enlaces e información de versión se almacenan en la base de datos de la partición de contexto de nombres de dominio. Como esta partición solo se replica dentro del propio dominio el proceso de GPO's a través de otros dominios puede ser muy complejo y costoso en tiempo.

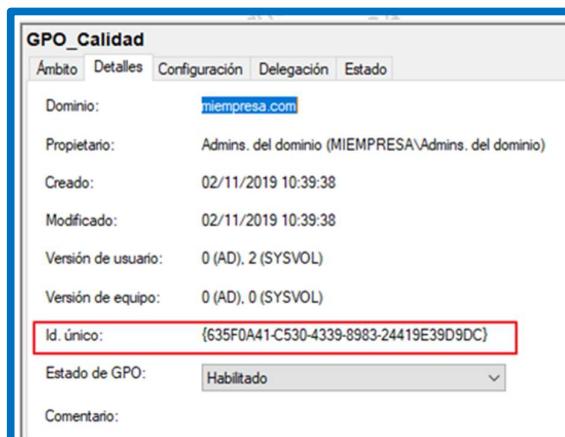
1. Los valores de las GPO's se almacenan en el sistema de ficheros de todos los controladores de dominio dentro de la carpeta "SYSVOL". Esta carpeta está compartida en todos los controladores de dominio:



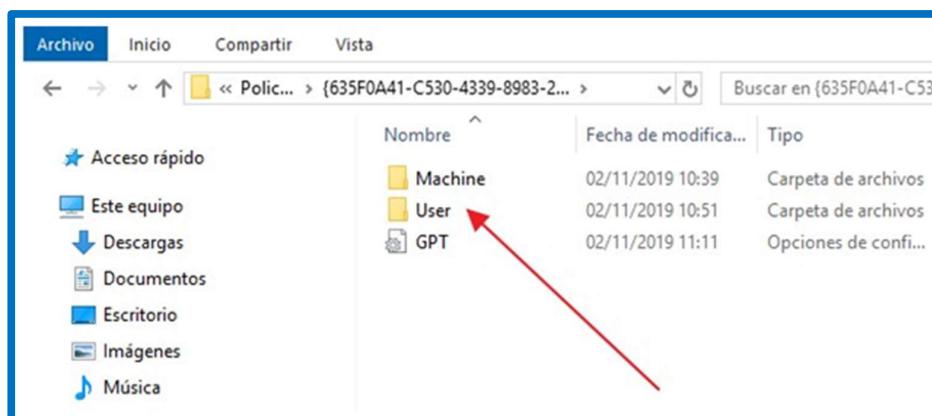
2. Cada GPO de dominio tiene su propia carpeta dentro de la subcarpeta "sysvol\miempresa.com\policies":



3. El nombre de la carpeta de la GPO es un identificador global único (GUID) asignado cuando se crea la directiva. El GUID de una GPO lo podemos ver en las propiedades de una directiva de dominio desde la consola:



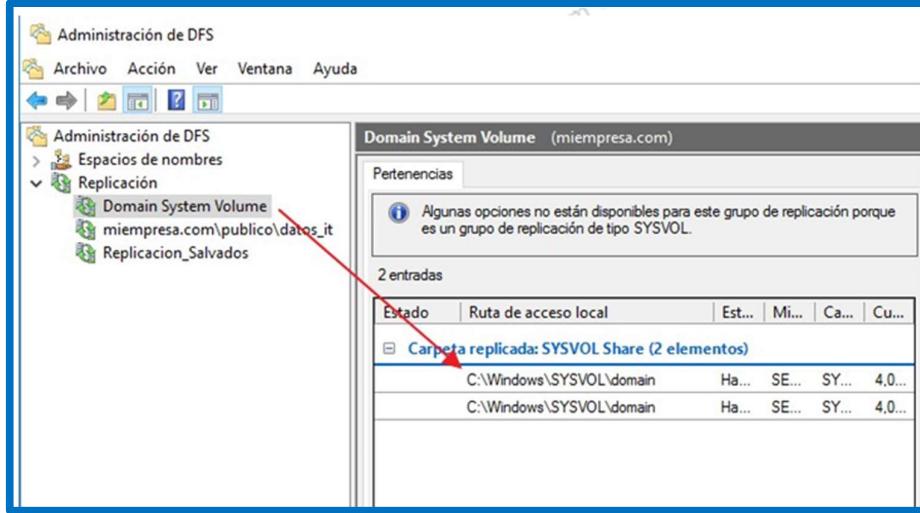
4. Dentro de la carpeta de la GPO se encuentran dos carpetas "User" y "Machine", opcionalmente la carpeta "ADM" y un fichero gpt.ini:



• Replicación de GPO's

Ya sabemos que se encuentra en la base de datos de un controlador de dominio, así que su replicación se realizará a todos los demás controladores de dominio. El sistema de ficheros que compone las GPO se replica con el recurso compartido SYSVOL utilizando el sistema de replicación distribuida de ficheros DFSR que vimos hace unas unidades.

El tiempo de replicación a los demás controladores de dominio es el planificado en el DFSR que por defecto utiliza los mismos parámetros que la replicación del directorio activo, es decir, cada 5 minutos. Primero se realiza dentro del propio sitio y luego a los demás controladores de los otros sitios. Recordemos lo que vimos de las réplicas con los demás sitios (sites).



Esta pantalla la vimos en una unidad anterior donde podíamos ver que, efectivamente, ya hay una replicación de SYSVOL preparada y programada en el servicio DFS. También podemos el servidor principal para la réplica de directivas en la solapa:

• Carpeta USER

Una de las carpetas que hay dentro de las directivas es la carpeta "User". Contiene los ficheros y carpetas necesarios para almacenar los programas, scripts y otros valores de configuración de directivas específicos para el usuario. Recordemos que había dos tipos de directivas: de usuario y de equipo.

• Carpeta Machine

Lo mismo que en el caso anterior, pero para los valores del equipo.

• Carpeta ADM

Los archivos de plantilla utilizados por un GPO se almacenan en una carpeta de "ADM". Por ejemplo, si el GUID (identificador único global) asociado con la "Directiva predeterminada de dominio" objeto de directiva de grupo es {016 31B2F340 D-11 D 2-945F-00C04FB984F9}, la ruta local a la carpeta ADM asociada con este objeto de directiva de grupo podría ser la ruta de acceso siguiente, donde SYSVOL Location es la ubicación de la carpeta SYSVOL:

- SYSVOL Location\ nombre de dominio \Policies
- \{31B2F340-016D-11D2-945F-00C04FB984F9\}\Adm

No existe la carpeta ADM dentro de la carpeta objeto de directiva de grupo asociada hasta que se ha abierto el objeto de directiva de grupo por primera vez, y hacemos clic en el equipo o usuario nodo de configuración.

Cuando se crea un objeto de directiva de grupo y seleccionamos un usuario o equipo, los archivos se copian desde la carpeta %SystemRoot%\Inf del equipo cliente a la carpeta ADM adecuada para el GPO en SYSVOL. Cuando un administrador agrega una plantilla ADM a un objeto de directiva de grupo que existe en Active Directory, el archivo ADM se copia de la ubicación del usuario especificado en la carpeta ADM del objeto asociado de directiva de grupo en SYSVOL.

En ambos casos, cuando el servicio de replicación de archivos (FRS) descubre el archivo modificado (en este caso un archivo nuevo), replica ese archivo en otros controladores de dominio en el mismo dominio. Cuando otro administrador abre el objeto de directiva de grupo, el archivo ADM está presente para cargarse junto con el objeto de directiva grupo que permite a las opciones disponibles que se mostrará en la herramienta de directiva de grupo.

- **Archivos registry.pol**

Dentro de una directiva, los valores están segmentados en varias secciones. Muchos de estos valores son claves y valores de registro. El estado del valor de estas configuraciones se almacena en estos ficheros "registry.pol" en las carpetas "User" o "Machine".

- **Archivo GPT.INI**

Cuando creamos una GPO se crea una carpeta en SYSVOL con su identificador único, como ya hemos visto anteriormente. En la raíz de esa carpeta nos encontramos con un archivo GPT.INI:

Nombre	Fecha de modifica...	Tipo
Machine	02/11/2019 10:39	Carpetas de archivos
User	02/11/2019 10:51	Carpetas de archivos
GPT	02/11/2019 11:11	Opciones de configuración

Este fichero tiene el número de revisión de la GPO. Cuando se procesa por primera vez el número de revisión se almacena en el sistema y cuando se realizan nuevos procesos se compara el número de referencia del fichero con el valor almacenado en la caché del sistema. Si no ha cambiado el número, no se procesan determinadas partes de la GPO. Las que si se procesan son las secuencias de comandos o "scripts".

Cada vez que cambia la GPO se incrementa ese número de revisión.

3.2. Definición de las directivas, componentes

Plantillas administrativas de las directivas de grupo

Las plantillas administrativas GPO son un conjunto de valores escritos en XML que definen la secciones con sus valores. Proporcionan una forma sencilla de acceder a los valores de configuración de usuario y equipo. Cuando se crea una GPO, se importa un conjunto de plantillas administrativas que proporcionan las configuraciones que hemos visto antes. Además, y como ya hemos comentado, podemos importar nuevas plantillas para ampliar las configuraciones de los usuarios y equipos.

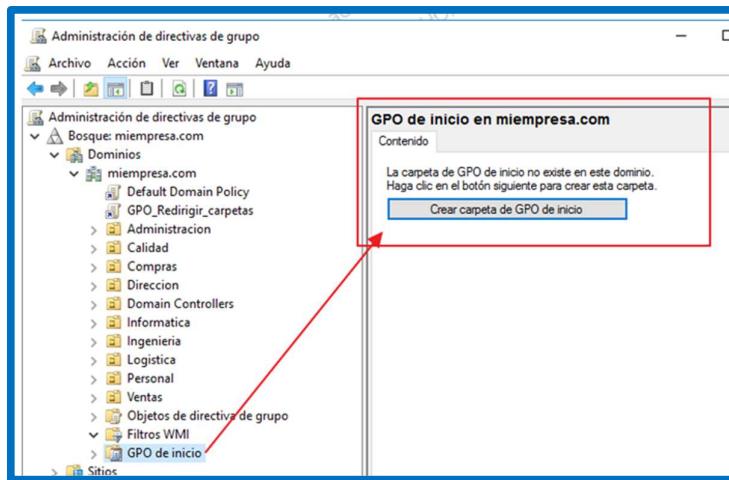
Almacén central de Windows Server

Desde Windows 2008, cambia la forma de almacenamiento de las directivas. Desde esta versión, las nuevas GPO's solo almacenan las carpetas y ficheros necesarios para almacenar los valores de configuración, secuencias de comandos (scripts), fichero registry.pol y otros ficheros relacionados. Cuando abrimos una directiva con estos dos sistemas operativos se hace una referencia a una copia de las plantillas administrativas.

Tenemos una nueva opción para crear un único almacén central de información dentro de la carpeta SYSVOL. Este almacén central puede contener todas las plantillas administrativas. De esta forma cuando se crea un GPO y se abre para su edición, el sistema primero comprueba si existe este depósito central y solo utilizará en ese caso las plantillas de este almacén central.

GPO's de inicio:

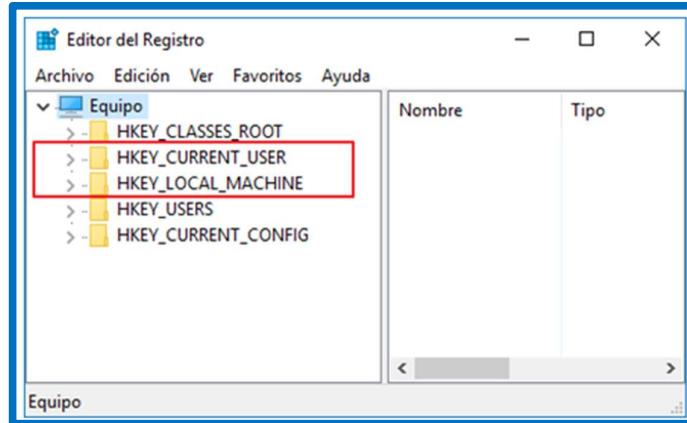
Las herramientas de administración de GPO's de Windows proporcionan una característica llamada GPO de Inicio, que apareció por primera vez en Windows 2008:



Son similares al resto de directivas, pero solo contienen valores disponibles de plantillas administrativas. Los objetos de directiva de grupo (GPO) de inicio proceden de un objeto de directiva de grupo y proporcionan la capacidad de almacenar una colección de valores de la directiva "Plantilla administrativa" en un solo objeto. Podemos importar y exportar GPO de inicio facilitando su distribución a otros entornos. Al crear un objeto de directiva de grupo a partir de un GPO de inicio, el nuevo objeto tiene todos los valores de configuración de directiva de las plantillas administrativas y sus valores definidos en el GPO de inicio.

Plantillas administrativas de las directivas de grupo

Las plantillas administrativas son el núcleo de la GPO. La mayoría de los valores que administramos con las plantillas administrativas corresponder con valores del registro para el equipo o la cuenta del usuario.



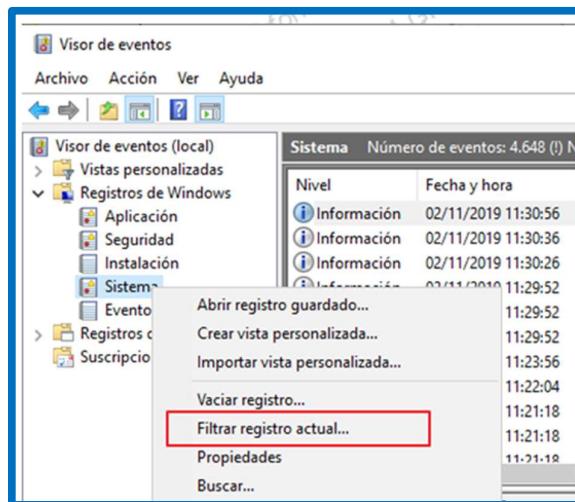
Corresponden con las claves de registro "HKEY_CURRENT_USER" y "HKEY_LOCAL_MACHINE" que vemos en la pantalla anterior en la edición del registro. Otros valores son secuencias de comandos o "scripts" y en otras ocasiones y como veremos más adelante, para instalar software en equipos o usuarios. Estas plantillas administrativas se dividen en tres tipos:

- Ficheros ADM de Windows 2000 cliente y servidor, Windows XP y Windows 2003.
- Ficheros ADMLX y ADML a partir de Windows Vista (7, 2008, 2008 R2, 8, 2012, 10, 2016 y 2019).
- Ficheros ADM, ADMX y AMDL personalizados para ampliar las funcionalidades de las GPO más allá de las proporcionadas por las plantillas.

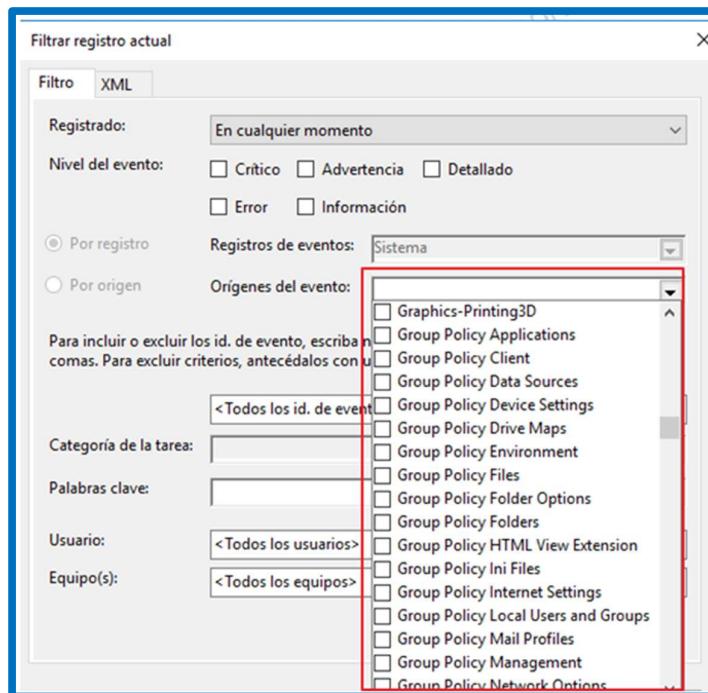
3.3. Visor de eventos

El visor de eventos no es un elemento de las GPO, pero lo comentamos aquí porque nos será muy útil para revisar y monitorizar el estado de las GPO.

- Los eventos administrativos incluyen el estado de las GPO procesadas en un equipo y usuario concreto, incluyendo información de alto nivel detallando si la GPO se ha podido aplicar o no. Como tenemos muchos eventos y no será fácil encontrar los relacionados con las GPO, tendremos que filtrarlos. Para aplicar un filtro seleccionaremos:

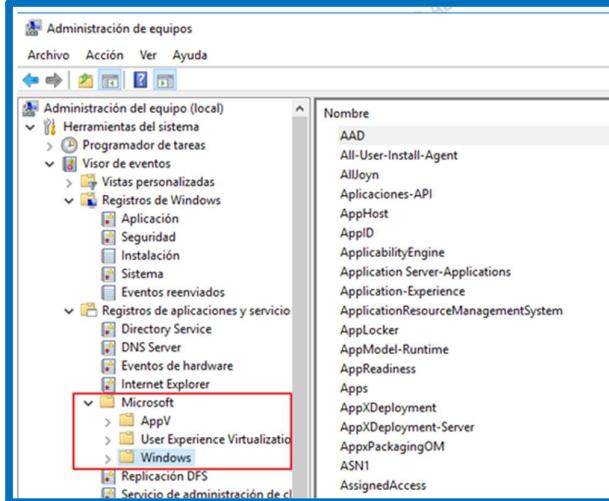


- Seleccionaremos solo lo que queremos ver:

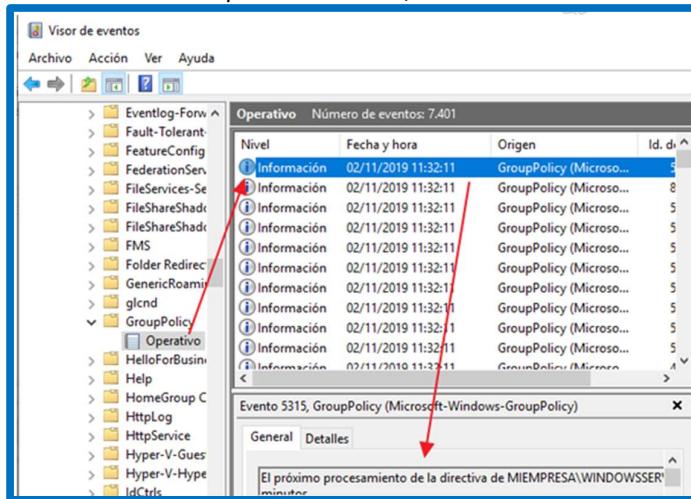


Seleccionaremos las relativas a las directivas de grupo que queramos filtrar. Nos muestra sólo los eventos que nos interesan sobre la aplicación correcta o fallida de las directivas y otros datos importantes.

3. También podemos ver los eventos de operaciones. Cuando se procesa una GPO, se crean los eventos de operaciones en cada tarea realizada. Esto reduce enormemente el tipo de resolución de problemas porque tenemos aquí un detalle exhaustivo de todo lo realizado. Para verlo, nos iremos al visor de eventos:



4. En este caso veremos los eventos de la sección "Registro de aplicaciones y servicios", expandimos las ramas de "Microsoft" y "Windows". De los elementos que nos muestra, seleccionaremos:

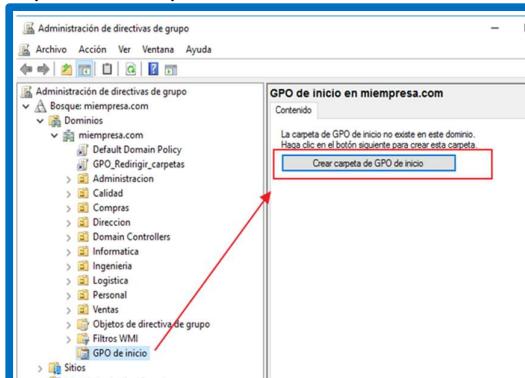


Con lo que tendremos un registro completo de las operaciones (no de los eventos como antes) realizadas.

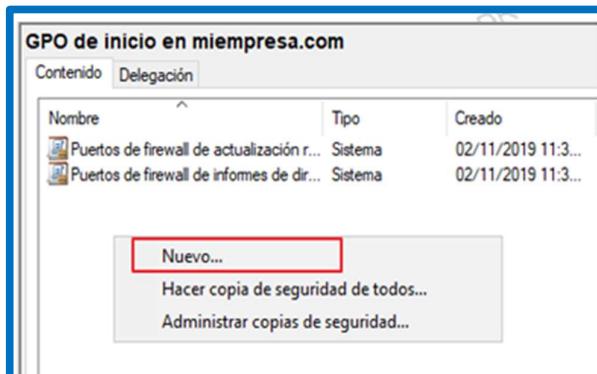
3.4. Creación de una directiva de inicio

Hemos comentado antes que existe lo que se llama "directiva de inicio". Permite a los administradores crear o cargar GPO's básicas con valores de plantillas administrativas preconfiguradas para poder utilizarse en las plantillas. Si existe ya una directiva de inicio, cuando creamos una nueva nos preguntará si queremos utilizar estos valores preconfigurados.

1. Para crear una directiva de inicio pulsaremos primero en el botón:



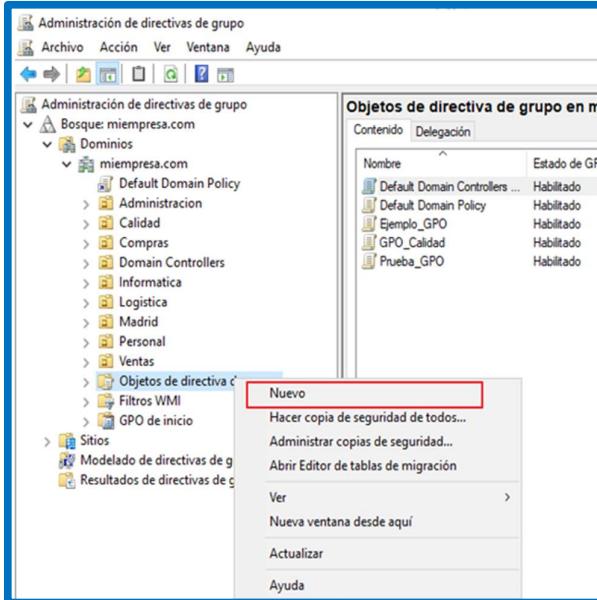
2. Una vez creada la carpeta podemos ahora crear la directiva, proceso que podemos hacer de varias formas. Podemos crearla desde cero con una plantilla en blanco, restaurarla de una copia de seguridad o importarla desde un archivo comprimido ".cab". En el caso más sencillo, es decir creándola desde cero, haremos lo siguiente: pulsamos en la parte derecha y diremos que queremos crear una nueva:



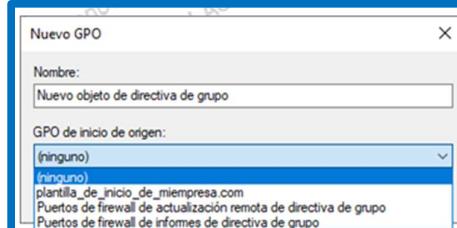
3. Vemos una serie de plantillas ya existentes de varios sistemas operativos, y debajo la opción de "Cargar archivo .CAB". En este caso la estamos creando nueva. Le ponemos un nombre y luego la editaremos para poner los valores que queramos.



4. A partir de ahora, cuando creamos una directiva, podremos basarnos en esta para que incorpore ya los valores que acabamos de fijar. Veamos si es cierto, nos vamos al contenedor de directivas para crear una normal y pulsamos con el botón derecho para crear una nueva:



5. No hemos hecho nada nuevo todavía, pero cuando nos pregunta el nuevo nombre:



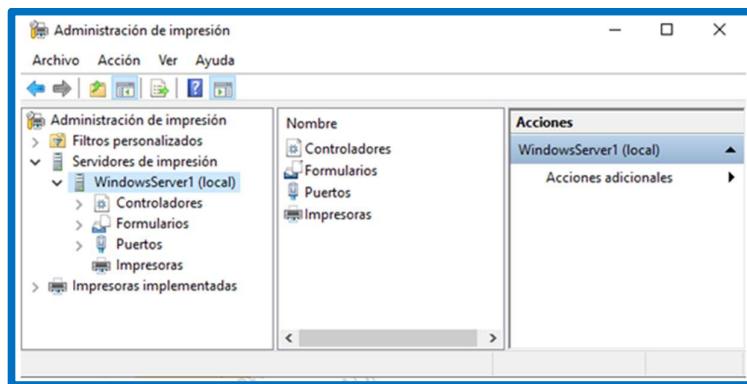
Vemos que nos deja indicar debajo una GPO de origen, con lo que la nueva tendrá ya los valores estándar que acabamos de definir en la directiva de inicio.

4. Implantar impresoras con directivas de grupo

1. Servicio de impresión que podemos instalar impresoras con directivas de grupo. Imaginemos la ventaja que supone esto: compramos un equipo y lo metemos en el dominio, una vez allí lo metemos en una unidad organizativa que tiene aplicada una directiva que le permite instalar determinadas impresoras. Cada departamento tiene sus propias directivas de impresoras, así si ese equipo lo movemos a otra unidad organizativa automáticamente dispondrá de las impresoras de ese nuevo departamento.

Otro ejemplo más interesante. Adquirimos una fotocopiadora multifunción con escáner de red y FAX. Deberíamos ir equipo por equipo a instalar los drivers y configurar todo. Sin embargo, podemos crear una directiva de grupo para que despliegue de forma automática este nuevo dispositivo en todos los equipos de nuestra red.

2. Utilizaremos el administrador de impresión para configurar estas directivas, vamos a recordar su entorno:



3. Podemos desplegar impresoras a equipos o usuarios y, además, si quitamos una impresora de una directiva desplegada, también se eliminará del usuario o equipo en el siguiente inicio de sesión. El despliegue lo podemos realizar desde la consola administrativa de las directivas o directamente desde la pantalla anterior del gestor de impresión. Por sencillez se recomienda utilizar esta última herramienta.

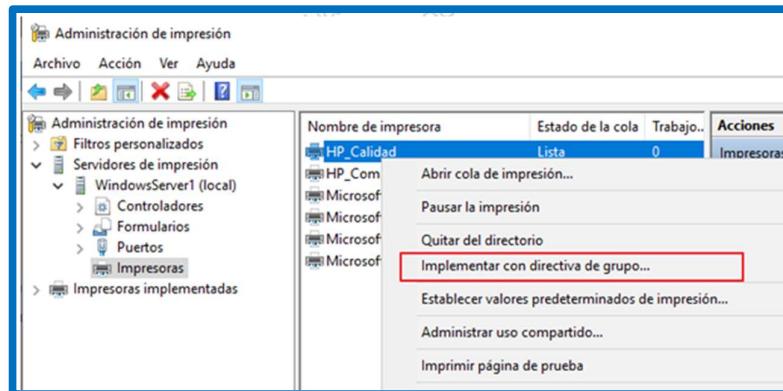
Este método de instalación de una impresora resulta útil en lugares como laboratorios, clases u oficinas sucursales, donde la mayoría de los equipos o usuarios necesitan obtener acceso a las mismas impresoras. También es un método útil para la implementación de controladores de impresoras para usuarios que no son miembros del grupo local Administradores y ejecutan Windows Vista, Windows 8 o 10.

Toda esta configuración funciona de forma automática a partir de Windows XP. Si el cliente es éste o anterior debemos usar la herramienta PushPrinterConnections.exe en un script de inicio (en conexiones por equipo) o en un script de inicio de sesión (en conexiones por usuario). Es una utilidad que permitirá esta automatización de instalación de impresoras que ya incorpora las demás versiones de Windows.

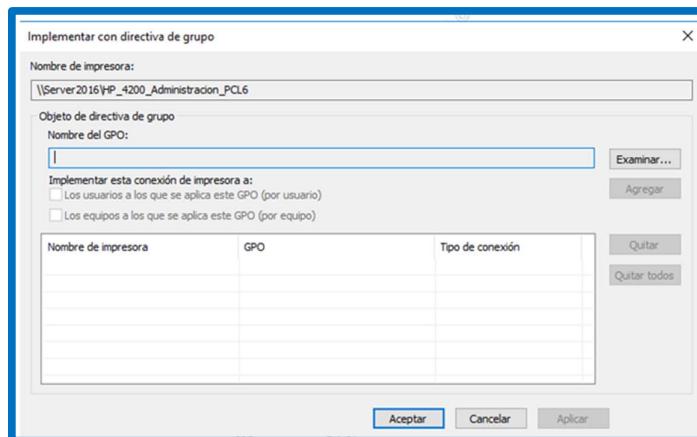
4.1. Implementación de conexiones de impresora

Para implementar conexiones de impresora para usuarios y equipos mediante directivas de grupo, utilizaremos el cuadro de diálogo "Implementar con directiva de grupo" de la consola "Administración de impresión". Con esto, conseguiremos añadir conexiones de impresora a un objeto de directiva de grupo (GPO).

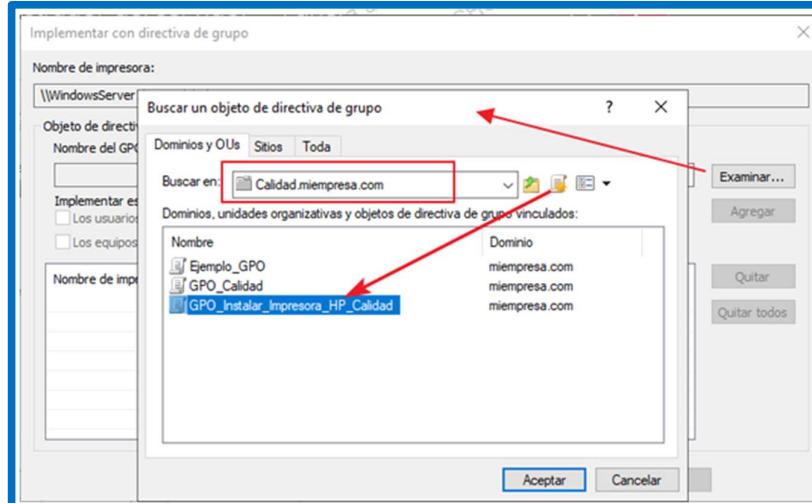
1. En el árbol Administración de impresión, en el servidor de impresión hacemos clic en impresoras y pulsamos con el botón derecho en la que queremos compartir mediante la GPO:



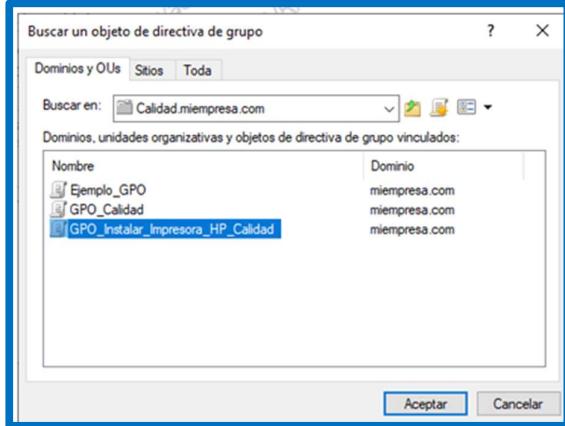
2. Nos mostrará un cuadro así:



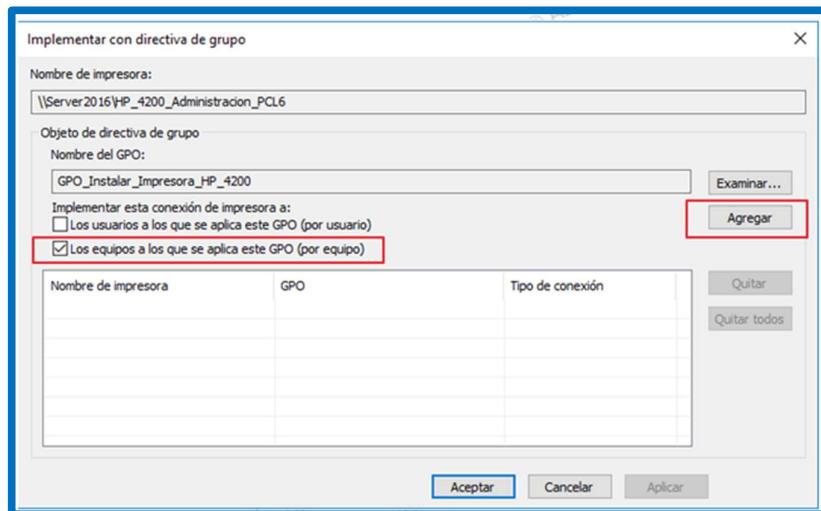
3. La impresora que quiero implementar es para el departamento de Calidad ya que se haya ubicada en ese departamento (ya pusimos de nombre a la impresora "HP_4200_Administracion_PCL6"). Pulsamos en "Examinar":



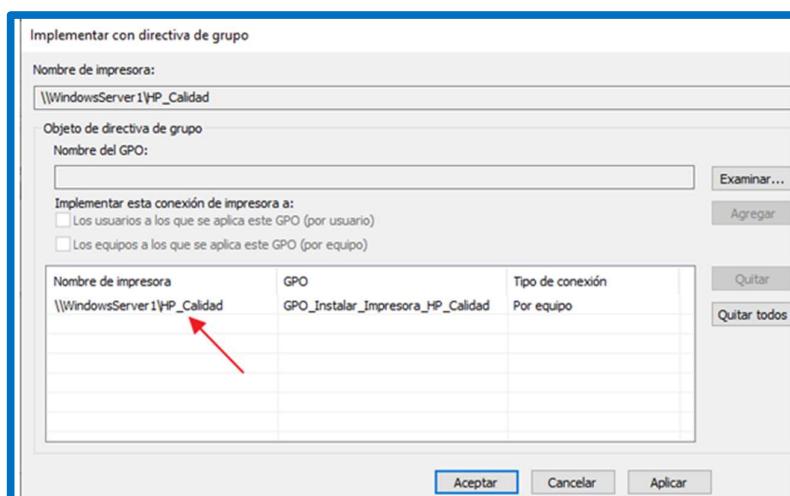
4. Podemos seleccionar en que directiva de grupo queremos implementar estas impresoras. En este caso teníamos una unidad organizativa llamada "Calidad", donde al hacer doble clic vemos las dos directivas que tiene de las prácticas que hemos hecho antes. Como no queremos mezclar las cosas, crearemos una directiva para la implementación de las impresoras, así será más fácil de administrar más adelante. Hacemos clic sobre el icono de "crear nueva directiva" que vemos marcado en la pantalla anterior. Creamos una que se llame como la unidad organizativa y la función que va a realizar:



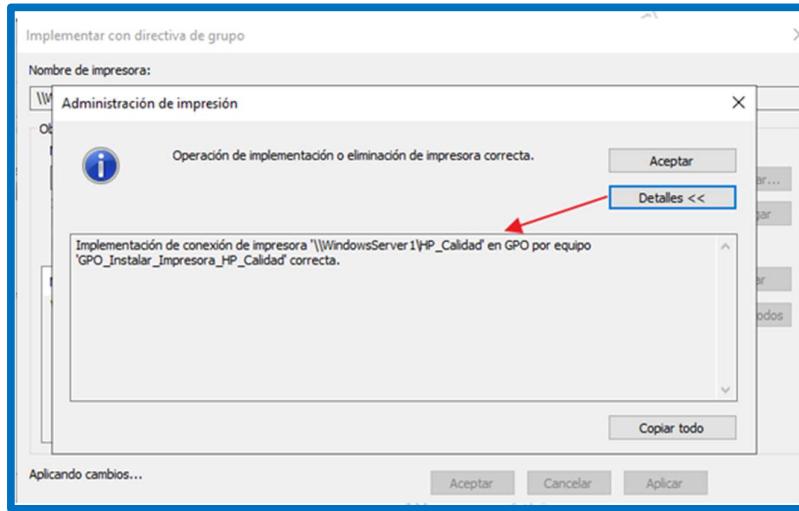
5. Con lo que nos queda:



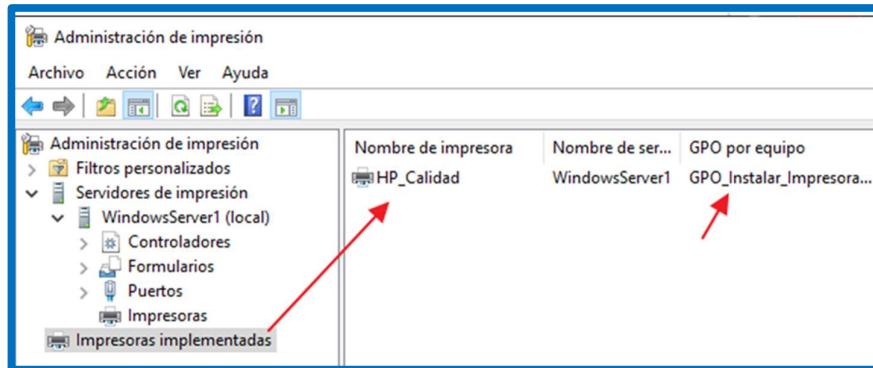
6. Hemos marcado que la aplique a los equipos para que sea independiente del usuario que entre en el equipo. Queremos que al colocar el equipo en la unidad organizativa, le instale las impresoras de forma automática. Pulsamos en "Agregar" para que aparezca en la lista:



7. Pulsamos en Aceptar y si todo va bien:



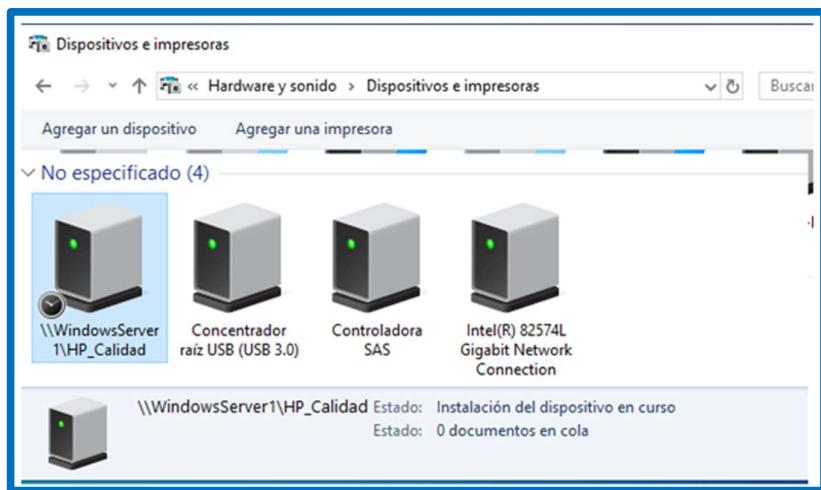
8. Ya está creada la directiva, veamos ahora en la consola administrativa:



9. Tenemos en "Impresoras implementadas" la que queríamos instalar automáticamente en los equipos de la unidad organizativa "Calidad". Vamos a comprobar la directiva que hemos creado desde el administrador de directivas. Abrimos y veamos los detalles de la que acabamos de crear:

The screenshot shows the 'Administración de directivas de grupo' (Group Policy Management) console. On the left, the tree view shows 'Bosque: miempresa.com' and 'Dominios' with 'miempresa.com' selected. Under 'miempresa.com', 'Calidad' is expanded, and 'GPO_Instalar_Impresora_HP_Calidad' is selected. On the right, the details pane for 'GPO_Instalar_Impresora_HP_Calidad' is shown. The 'General' tab displays 'Datos recopilados el: 02/11/2019 11:51:16'. The 'Configuración del equipo (habilitada)' (Enabled computer configuration) section is highlighted with a red border and contains the 'Directivas' (Policies) and 'Configuración de Windows' (Windows Configuration) sections. The 'Ruta' (Path) field shows '\\WindowsServer1\HP_Calidad'. A red arrow points from the 'GPO_Instalar_Impresora_HP_Calidad' entry in the tree view to the 'General' tab in the details pane.

10. Al ver la directiva y su contenido a la derecha, vemos lo sencilla que es y lo coherente con la asignación de recursos. Si entramos en uno de los equipos de la unidad organizativa de "Calidad", veremos que se ha aplicado la directiva y le ha instalado la impresora:



11. Solo con mover los equipos a las unidades organizativas se instalarán automáticamente las impresoras que tengamos configuradas en las directivas. Esto es un ahorro de tiempo enorme. Imaginemos además que tenemos unos equipos multifunción que utilizan decenas de personas. Sólo con vincular la directiva, habremos instalado la impresora a todos.

En las conexiones por equipo, Windows añade las conexiones de impresora cuando el usuario inicia sesión (o cuando el equipo se reinicia si se usa la utilidad PushPrinterConnections.exe). En las conexiones por usuario, Windows añade las conexiones de impresora durante la actualización de la directiva en segundo plano (o cuando el usuario inicia sesión si se usa la utilidad PushPrinterConnections.exe). Si quitamos la configuración de conexión de impresora desde el GPO, Windows quita las impresoras correspondientes del equipo cliente durante la siguiente actualización de directiva en segundo plano o en el inicio de sesión del usuario (o en el siguiente reinicio o inicio de sesión si se usa la utilidad PushPrinterConnections.exe).