Controlador de dominio + gpo

Proyecto Final

Bastionado de Redes y Sistemas

Eduardo Villacampa Escartín

# ÍNDICE

[0. ÍNDICE 1](#_Toc135075628)

[1. RESUMEN 2](#_Toc135075629)

[2. INTRODUCCIÓN 2](#_Toc135075630)

[3. CONCEPTO 2](#_Toc135075631)

[3.1. Definición de conceptos 2](#_Toc135075632)

[3.2. Características 3](#_Toc135075633)

[3.3. Aplicaciones y herramientas a utilizar 3](#_Toc135075634)

[4. PRÁCTICA 3](#_Toc135075635)

[4.1. Configuración de máquinas virtuales 3](#_Toc135075636)

[CONFIGURACIÓN IPFire 3](#_Toc135075637)

[CONFIGURACIÓN WINDOWS SERVER 2012R2 5](#_Toc135075638)

[CONFIGURACIÓN WINDOWS 7 7](#_Toc135075639)

[4.2. Promover Windows Server a controlador de dominio 8](#_Toc135075640)

[4.3. Unión del cliente (W7) al dominio 9](#_Toc135075641)

[4.4. Generación de usuarios, grupos y unidades organizativas 10](#_Toc135075642)

[CREACIÓN DE LOS ARCHIVOS CON LOS DATOS 10](#_Toc135075643)

[4.5. Creación de sistema de directorios compartidos 12](#_Toc135075644)

[4.6. Creación de Directivas de Grupo (GPOs) 14](#_Toc135075645)

[5. ANEXOS 16](#_Toc135075646)

[ANEXO I – Script para la creación de usuarios, grupos y unidades organizativas (genera\_AD\_Estructura.ps1) 16](#_Toc135075647)

[ANEXO II – Script para compartir directorios (Compartir.ps1) 17](#_Toc135075648)

# RESUMEN

El trabajo a realizar consiste en la implantación de un controlador de dominio con el objetivo de simular cómo se organiza el dominio de una organización. Para ello se va a trabajar con distintas máquinas virtuales, con el objetivo de simular lo que sería la red de la organización.

# INTRODUCCIÓN

En la actualidad, Internet se ha convertido en un pilar fundamental no solo para las organizaciones, sino para las personas en el desarrollo de su día a día.

(+)

# CONCEPTO

Para entender correctamente el proyecto que se va a realizar, es necesario aclarar una serie de conceptos que se van a nombrar y aplicar a lo largo del trabajo.

## Definición de conceptos

* **Active Directory (Directorio Activo):** Active Directory (AD) es un servicio de directorio para su uso en un entorno Windows Server. Se trata de una estructura de base de datos distribuida y jerárquica que comparte información de infraestructura para localizar, proteger, administrar y organizar los recursos del equipo y de la red, como archivos, usuarios, grupos, periféricos y dispositivos de red.
* **Controlador de dominio:** El controlador de dominio es el centro neurálgico de un dominio Windows. Los controladores de dominio tienen una serie de responsabilidades, y una de ellas es la autenticación que es el proceso de garantizar o denegar a un usuario el acceso a recursos compartidos o a otra máquina de la red, normalmente a través del uso de una contraseña. Esto permite validar a los usuarios de una red para ser partes de la plataforma de clientes que recibirán los servicios de información.
* **Dominio:** en el contexto del trabajo actual, un dominio se relaciona con una red que aloja distintos equipos informáticos (ordenadores, servidores, impresoras, etc).
* **Virtualización:** El concepto de virtualización hace referencia a una tecnología que permite la ejecución de varias máquinas virtuales sobre una máquina física con el objetivo de aprovechar al máximo los recursos de un sistema y que su rendimiento sea mayor.
* **GPOS:** Una GPO es un objeto que almacena uno o más valores de configuración que aplican a un usuario o equipo, pudiéndose aplicar sobre conjuntos de más de un usuario o más de un equipo.

## Características

## Aplicaciones y herramientas a utilizar

Como se ha explicado inicialmente, el objetivo de el proyecto es simular la gestión del directorio activo de una organización. Una organización cuenta con servidores, ordenadores de sobremesa, portátiles, dispositivos de red, impresoras, etc.

Como la utilización física de todos estos elementos es imposible a la hora de desarrollar este proyecto, se van a utilizar sistemas de virtualización con el objetivo de crear, a pequeña escala, lo que sería la red y el directorio activo de una organización.

Para ello, se van a utilizar las siguientes herramientas y/o aplicaciones:

* **VirtualBox:** Software de virtualización para arquitecturas x86/amd64. Mediante este software es posible instalar sistemas operativos adicionales, conocidos como ‘sistemas invitados’, dentro de otro sistema operativo ‘anfitrión’, cada uno con su propio ambiente virtual.
* **Windows Server 2012R2 (virtualizado):** Se creará una máquina virtual Windows Server 2012R2, que simulará el controlador de dominio de nuestra organización.
* **Windows 10 (anfitrión):** Equipo real desde el que configuraremos todos los sistemas virtualizados para simular la red de una organización.
* **Windows 7 (virtualizado):** Equipos virtuales que simularán los ordenadores de los trabajadores de la organización.
* **IPFire (virtualizado):** Distribución de Linux que funciona como un router y un firewall. Se va a utilizar para simular el router de la organización. Para ello se creará una red NAT.

# PRÁCTICA

En esta práctica se va a implantar un controlador de dominio en una red empresarial. Para ello va a ser necesario seguir los distintos pasos que se muestran a continuación:

## Configuración de máquinas virtuales

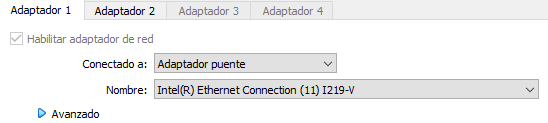
### CONFIGURACIÓN IPFire

Esta máquina va a actuar como el router de la organización. Para ello, se deben configurar las tarjetas de red de manera que una actúe como adaptador puente entre la máquina anfitrión e IpFire, y la otra para dar servicio al Windows Server y las maquinas Windows.

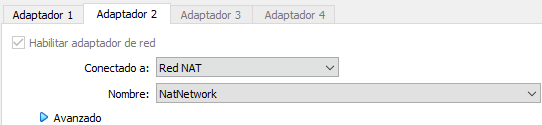
Para ello, la máquina se debe configurar de la siguiente manera:

1. Configuración de tarjetas de red

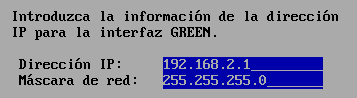
* Un adaptador de red deberá estar en Adaptador puente



* El otro en red NAT:



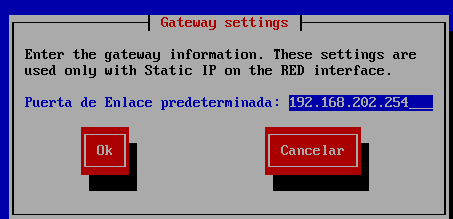
1. Una vez añadidas las tarjetas de red, debemos elegir el tipo de configuración de red para IPFire. Esto se hace desde la instalación, eligiendo la configuración **GREEN + RED.**
2. Posteriormente debemos asignar las tarjetas de red con la interfaz deseada, del siguiente modo:
   * GREEN: Adaptador 2, red local.
   * RED: Adaptador 1, adaptador puente.
3. Ahora hay que configurar las direcciones de red de cada interfaz:
   * Interfaz GREEN (Red local)



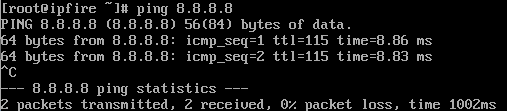
* + Interfaz RED (Adaptador puente)



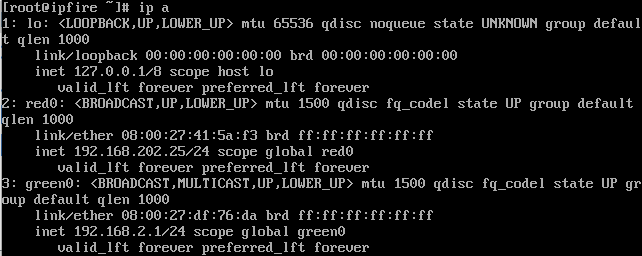
1. Establecemos la puerta de enlace:



1. Ahora debemos comprobar que tenemos conexión a Internet, ejecutando el comando **#ping**:



1. También podemos asegurarnos de que se ha aplicado la configuración de interfaces correctamente, mediante el comando **#ip a:**

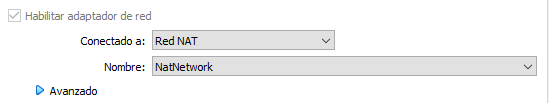
****

### CONFIGURACIÓN WINDOWS SERVER 2012R2

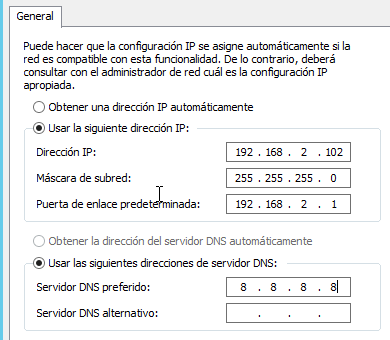
Contraseña: Proyectogpo45

Una vez tengamos nuestro Windows Server instalado, lo tenemos que configurar para meterlo en la red NAT que hemos creado con IPFire. Para ello, debemos seguir los siguientes pasos:

1. Desde la configuración de Virtualbox, configuramos la tarjeta de red como red NAT:

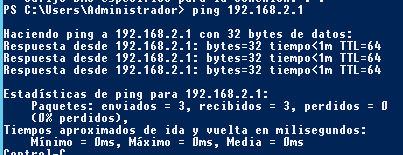


1. Abrimos el Panel de Control 🡪 Redes e Internet 🡪 Centro de redes y recursos compartidos 🡪 Cambiar la configuración del adaptador 🡪 Ethernet 🡪 Propiedades 🡪 IPv4 y aplicar la siguiente configuración:

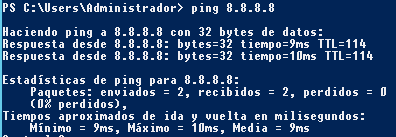


1. Guardamos y reiniciamos la máquina. Comprobamos que la configuración se ha aplicado correctamente y funciona como queremos mediante el comando **#ping:**

* Ping al router (IPFire)



* Ping al servidor DNS:

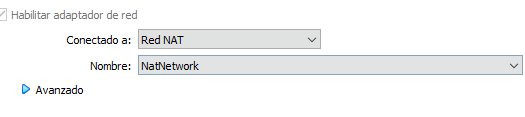


### CONFIGURACIÓN WINDOWS 7

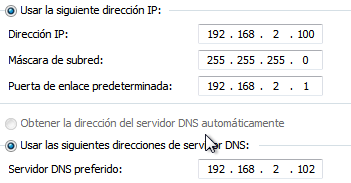
Una vez instalada nuestra máquina Windows 7, la debemos incluir en la red NAT creada con IPFire. Esta máquina simulará los ordenadores de los empleados de la organización.

Para incluirlo en la red NAT creada, debemos seguir los siguientes pasos:

1. Configuración de tarjeta de red en modo red NAT, desde el menú de Virtualbox:



1. Abrimos el Panel de Control 🡪 Redes e Internet 🡪 Centro de redes y recursos compartidos 🡪 Cambiar la configuración del adaptador 🡪 Conexión de área local 🡪 Propiedades 🡪 IPv4 y aplicar la siguiente configuración:



1. Comprobamos que funciona correctamente mediante el comando **#ping:**

* Ping al router (IPFire):



* Ping al servidor DNS (Windows Server): el ping desde el Windows 7 al Windows Server no funciona, debido a que aún no se ha configurado el servidor para que funcione como servidor DNS.

`

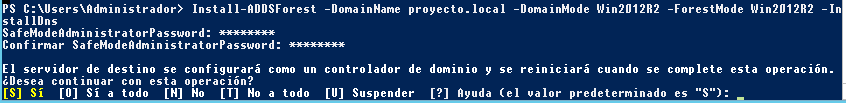
## Promover Windows Server a controlador de dominio

Una vez configuradas todas las máquinas y creada la red NAT, vamos a configurar el Windows Server para que actúe como controlador de dominio.

1. Cambiamos el nombre del servidor



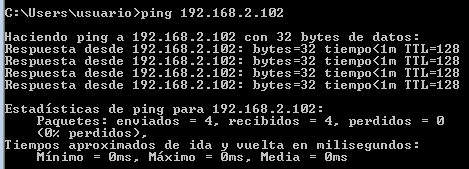
1. Reiniciar el servidor
2. Instalamos el servicio de controlador de dominio
3. Configuramos el nivel funcional de bosque y del dominio



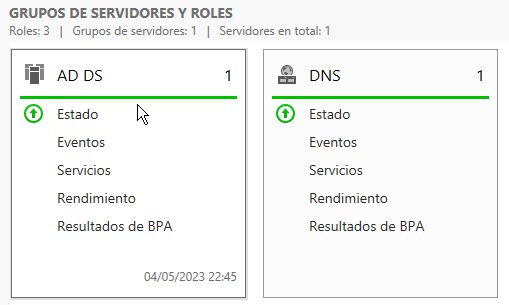
1. Ahora el equipo se reinicia automáticamente. Al ingresar de nuevo, podemos ver como entramos con el administrador de dominio:



1. Ahora, si que funciona el ping entre la máquina Windows 7 y el Windows Server:

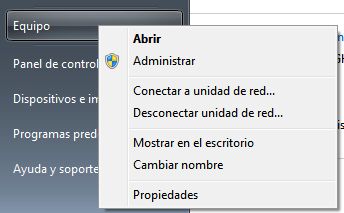


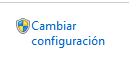
1. Finalmente, podemos comprobar la correcta instalación y configuración del dominio y su DNS:



## Unión del cliente (W7) al dominio

Una vez configurado nuestro dominio, el siguiente paso es añadir nuestra máquina virtual W7 al dominio. Para ello, hay que seguir los siguientes pasos:

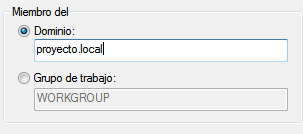
1. En nuestro Windows 7, abrimos el menú de inicio, y hacemos clic derecho en equipo 🡪 Propiedades:
2. Clicamos en cambiar configuración:



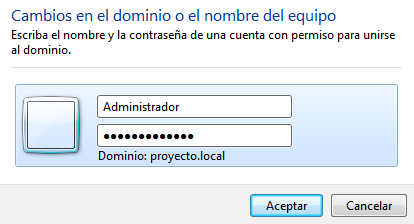
1. Clicamos en cambiar:



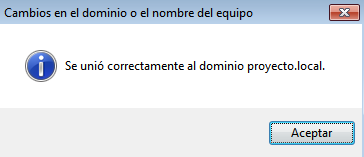
1. Habilitamos la casilla ‘Miembro del dominio’ y la rellenamos con el nombre del dominio al que nos queremos unir, en nuestro caso, ‘**proyecto.local’**:



1. Nos solicitará las credenciales del administrador del dominio. Las ingresamos y pulsamos aceptar:



1. Nos muestra el diálogo de que nos hemos unido correctamente al dominio:



1. Reiniciamos el equipo.
2. Ahora ingresaremos con un usuario del dominio, no del equipo local:



En el caso de una organización, se debería repetir este proceso en todos los ordenadores que quieran vincularse al dominio. En nuestro caso, vamos a utilizar sólo una máquina virtual Windows 7 que simulará todos los ordenadores de la organización vinculados al dominio, ya que ahora crearemos los distintos usuarios de la organización a los que accederemos desde esta máquina.

## Generación de usuarios, grupos y unidades organizativas

Una vez creado el dominio y vinculada la máquina virtual Windows 7 (simulará todos los ordenadores de la organización) el siguiente paso será crear los usuarios desde los que se accederá al dominio.

### CREACIÓN DE LOS ARCHIVOS CON LOS DATOS

1. En primer lugar, instalaremos las ‘Guest Additions’ de Virtualbox en nuestro servidor. Para ello, acceder a este equipo y pulsar sobre la siguiente unidad:



1. Pulsaremos sobre el siguiente ejecutable:



1. Lo instalamos y reiniciamos el equipo. Esto nos permitirá compartir archivos con la máquina anfitrión con mayor facilidad.
2. Ahora crearemos los archivos .csv en los que introduciremos los datos de los usuarios que queremos crear. Se crearán dos archivos. Uno con la información de los usuarios (usuarios.csv) y otro con la información de los departamentos (departamentos.csv).

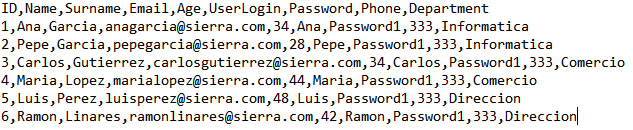
Podemos crear los archivos mediante el bloc de notas de Windows, siempre y cuando a la hora de guardarlo lo guardemos con la extensión .csv.

**departamentos.csv:**





**usuarios.csv**

****



Como se puede observar, se han creado tres departamentos (informática, comercio, dirección) y 6 usuarios, dos por cada departamento.

El siguiente paso es crear el script que ejecutaremos para crear los usuarios. Este script lo crearemos mediante PowerShell. Para obtener el código, véase [Anexo I - Script para la creación de usuarios, grupos y unidades organizativas (genera\_AD\_Estructura.ps1).](#_ANEXO_I_–)

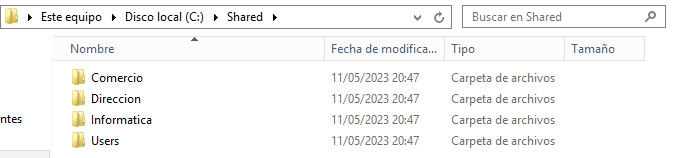
1. Una vez tengamos nuestros tres archivos en el equipo anfitrión, los arrastramos a nuestro servidor. En caso de no funcionar, podemos crear una carpeta compartida.
2. Una vez tengamos los archivos en el servidor, ejecutaremos el script creado.
3. Comprobamos que los usuarios y grupos se han creado correctamente desde el Windows 7, accediendo con los usuarios creados:



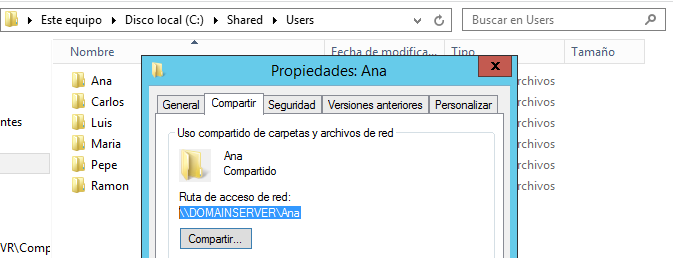
## Creación de sistema de directorios compartidos

Ahora que hemos creado todos los usuarios, vamos a crear un sistema de directorios compartidos en red. Para ello, hay que seguir los siguientes pasos:

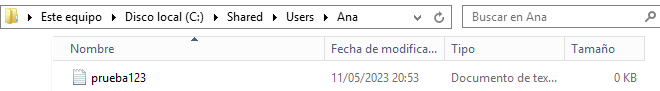
1. Creación del script en PowerShell para la creación de los directorios compartidos. Véase [Anexo II - Script para compartir directorios (Compartir.ps1)](#_ANEXO_II_–).
2. Una vez creado el script, lo ejecutamos en nuestro servidor.
3. Una vez ejecutado, comprobamos desde el servidor que se ha ejecutado correctamente:



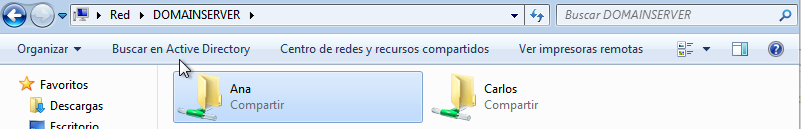
1. También lo comprobamos desde el Windows 7. Para ello, en primer lugar, debemos mirar la ruta de compartición en el Windows Server:



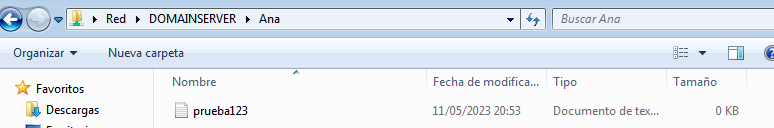
1. Creamos un documento desde el Windows Server en una de las carpetas de cualquier usuario para hacer la prueba:



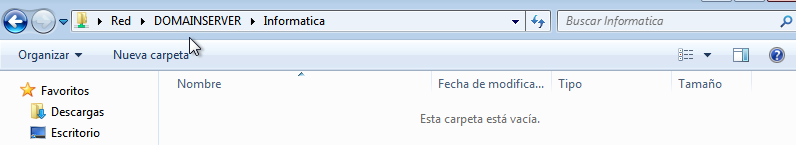
1. Accedemos a la ruta de la carpeta compartida desde el Windows 7:



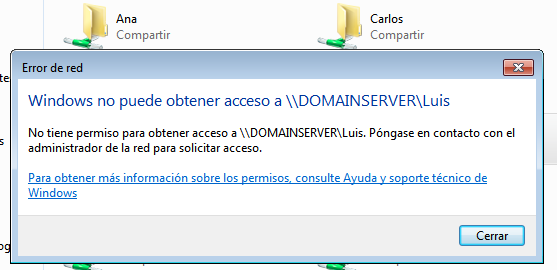
1. Comprobamos que se encuentra el archivo creado desde el Windows Server:



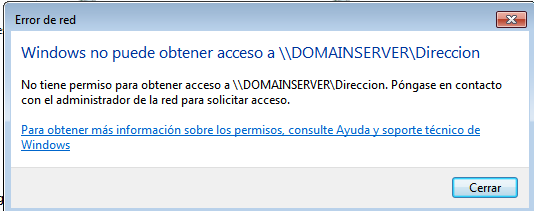
1. A su vez, comprobamos que este usuario tiene acceso a la carpeta ‘Informática’, ya que hemos añadido el usuario ‘Ana’ al grupo:



1. En el caso de querer acceder desde el usuario ‘Ana’ a la carpeta de otro usuario, por ejemplo ‘Luis’, no nos lo permitirá debido a que no tiene permisos de acceso a otras carpetas:



1. Lo mismo ocurriría si intentamos acceder a las carpetas ‘Comercio’ o ‘Dirección’:



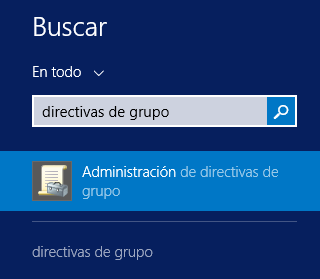
1. En resumen, desde cada usuario sólo se podrá acceder a la carpeta personal y a la carpeta del departamento en el que cada usuario haya sido dado de alta.

## Creación de Directivas de Grupo (GPOs)

Como se ha explicado anteriormente, las Directivas de Grupo (GPOs, *Group Policy Objects,)* son objetos que almacenan uno o más valores de configuración que aplican a un usuario o equipo, pudiéndose aplicar sobre conjuntos de más de un usuario o más de un equipo.

Resumiendo, son el conjunto de reglas que se aplicarán a los equipos o grupos creados anteriormente, con el objetivo de gestionar la configuración de los mismos, en cuanto al acceso que tienen a algunas aplicaciones, configuración de interfaces, etc.

Para comenzar a configurar las Directivas de Grupo, debemos acceder a nuestro Windows Server, y en la pestaña de inicio pulsar en la lupa de la esquina superior derecha, donde buscaremos ‘Administración de Directivas de Grupo’



Otra opción para acceder a la administración de las directivas de grupo, es ejecutar el siguiente comando desde PowerShell:



A continuación, se mostrarán las Directivas de Grupo que se van a configurar, simulando la gestión de los equipos de una organización empresarial.

**ICONOS DEL MENÚ Y LA BARRA DE TAREAS**

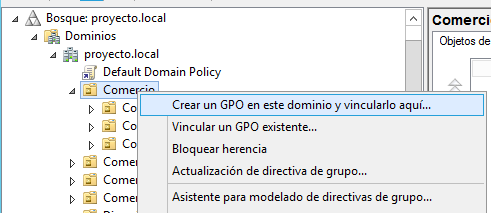
El objetivo de esta política de grupo es establecer que iconos aparecerán en el menú y en la barra de tareas en los equipos Windows 7.

En la siguiente imagen se muestran los iconos que aparecen en el menú y la barra de tareas de los equipos W7 por defecto:

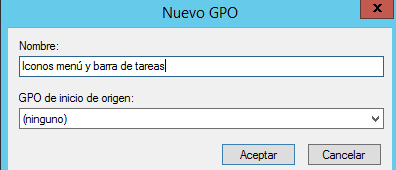


Ahora, comenzaremos con la configuración de la política de grupo para los usuarios pertenecientes al grupo ‘Comercio’.

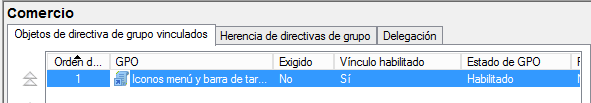
1. Para ello, en nuestro Windows Server, una vez dentro de la administración de directivas de grupo, accederemos a Bosque 🡪 Dominio 🡪 Comercio, y sobre ‘Comercio’ haremos clic derecho y pulsaremos ‘Crear un GPO en este dominio y vincularlo aquí…’:



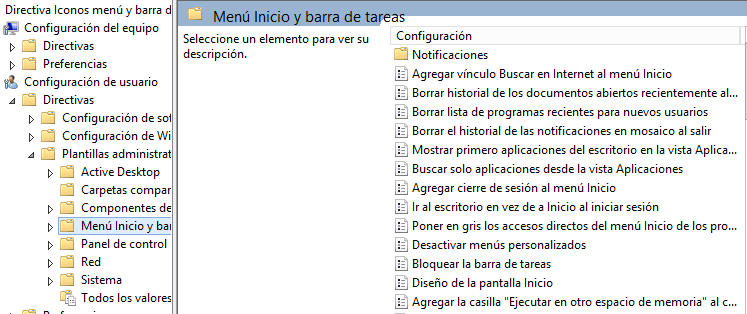
1. Nos solicitará un nombre:



1. Ahora nos aparecerá la GPO en el apartado ‘Comercio’:



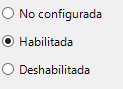
1. Haremos clic derecho y pulsaremos ‘Editar’.
2. En la ventana que nos aparece, accederemos a Configuración del usuario 🡪 Directivas 🡪 Plantillas Administrativas 🡪 Menú inicio y barra de tareas:



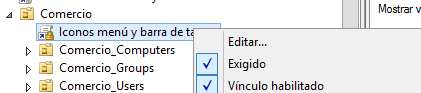
1. Aquí podemos ver todo lo que se puede quitar o habilitar y las políticas que se aplicarán a todos. Ahora queremos quitar el icono de red en los equipos W7 de Comercio. Para ello, buscaremos ‘Quitar icono de red’:



1. Haremos doble clic y la habilitaremos:

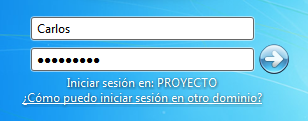


1. Pulsaremos Aplicar 🡪 Aceptar.
2. Ahora cerraremos la ventana de políticas y volveremos a la de administración de directivas de grupo.
3. Accedemos a Comercio 🡪 hacemos clic derecho 🡪 Iconos del menú y barra de tareas 🡪 Exigido:



De esta manera, exigimos el cumplimiento de esta política para los usuarios pertenecientes a Comercio.

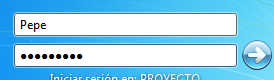
1. Ahora, para comprobar que se ha aplicado correctamente, reiniciaremos el Windows 7 y accederemos con un usuario perteneciente a comercio, por ejemplo ‘Carlos’:



1. Como podemos observar, ahora no aparece el icono de red en la esquina inferior derecha:



1. Ahora comprobaremos que esta política no ha afectado a los usuarios de otros grupos. Para ello, iniciaremos sesión con un usuario perteneciente al grupo Informática, por ejemplo ‘Pepe’:



1. Como podemos observar, la política no ha afectado a este usuario, ya que no pertenece al grupo Comercio:
2. Ahora añadiremos más políticas sobre los iconos de menú y barra de tareas. El proceso es el mismo, sólo que hay que elegir las directivas que deseemos. Las directivas a aplicar serán las siguientes:

**Quitar el vínculo Juegos del menú de inicio**

****

**Bloquear la barra de tareas**

****

# ANEXOS

### ANEXO I – Script para la creación de usuarios, grupos y unidades organizativas (genera\_AD\_Estructura.ps1)

$usersfile= Import-Csv -Path "C:\Usuarios\Administrador\Documentos\usuarios.csv"

$departmentsfile = Import-Csv -Path "C:\Usuarios\Administrador\Documentos\departamentos.csv"

foreach ($dept in $departmentsfile){

#crear un grupo para cada departamento

New-ADGroup -Name $dept.DepartName -GroupScope Global

#crear un OU para cada departamento

New-ADOrganizationalUnit -Name $dept.DepartName -ProtectedFromAccidentalDeletion $false

$departmentName=$dept.DepartName

$DNOUDept = Get-ADOrganizationalUnit -Filter 'Name -eq $departmentName' | Select-Object -ExpandProperty DistinguishedName

#crear tres OUs dentro de cada UODepartamento (Usuarios, Equipos, Grupos) y moverlos dentro del OU con el nombre del departamento

$OUNameUsers=$dept.DepartName+"\_Users"

New-ADOrganizationalUnit -Name $OUNameUsers -ProtectedFromAccidentalDeletion $false

$DNOUUsers = Get-ADOrganizationalUnit -Filter 'Name -eq $OUNameUsers' | Select-Object -ExpandProperty DistinguishedName

Move-ADObject -Identity $DNOUUsers -TargetPath $DNOUDept

$OUNameComputers=$dept.DepartName+"\_Computers"

New-ADOrganizationalUnit -Name $OUNameComputers -ProtectedFromAccidentalDeletion $false

$DNOUComputer = Get-ADOrganizationalUnit -Filter 'Name -eq $OUNameComputers' | Select-Object -ExpandProperty DistinguishedName

Move-ADObject -Identity $DNOUComputer -TargetPath $DNOUDept

$OUNameGroups=$dept.DepartName+"\_Groups"

New-ADOrganizationalUnit -Name $OUNameGroups -ProtectedFromAccidentalDeletion $false

$DNOUGroup = Get-ADOrganizationalUnit -Filter 'Name -eq $OUNameGroups' | Select-Object -ExpandProperty DistinguishedName

Move-ADObject -Identity $DNOUGroup -TargetPath $DNOUDept

#añadir el grupo del OUDeptGroup

$departName = $dept.DepartName

$DNGroup=Get-ADGroup -Filter {name -eq $departmentName} | Select-Object -ExpandProperty DistinguishedName

#como hemos movido el UODepartmentGroup, revisamos el DN (ha cambiado)

$DNOUGroup=Get-ADOrganizationalUnit -Filter 'Name -eq $OUNameGroups' | Select-Object -ExpandProperty DistinguishedName

Move-ADObject -Identity $DNGroup -TargetPath $DNOUGroup

}

foreach($user in $usersfile){

#crear AD Usuario

New-ADUser -Name $user.UserLogin -GivenName $user.Name -Surname $user.Surname -EmailAddress $user.Email -MobilePhone $user.Phone -AccountPassword (ConvertTo-SecureString $user.Password -AsPlainText -Force) -Enabled $true

#añadir el AD Usuario al AD Grupo

Add-ADGroupMember $user.Department -Members $user.UserLogin

#mover el usuario al correcto OU departamento

$OUNameUsers = $user.Department+"\_Users"

$DNOUUsers=Get-ADOrganizationalUnit -Filter 'Name -eq $OUNameUsers' | Select-Object -ExpandProperty DistinguishedName

$userlogin=$user.UserLogin

$DNUser=Get-ADUser -Filter {samaccountname -eq $userlogin} | Select-Object -ExpandProperty DistinguishedName

Move-ADObject -Identity $DNUser -TargetPath $DNOUUsers

}

### ANEXO II – Script para compartir directorios (Compartir.ps1)

$userfile=Import-Csv -Path "C:\Users\Administrador\Documents\usuarios.csv"

$departmentsfiles=Import-Csv -Path "C:\Users\Administrador\Documents\departamentos.csv"

foreach($dept in $departmentsfiles){

#Crear el directorio compartido para cada departamento

New-Item -ItemType Directory -Path ("C:\Shared\"+$dept.DepartName)

#Crear la compartición en SMB

New-SmbShare -Name $dept.DepartName -Path ("C:\Shared\"+$dept.DepartName)

#Dar permisos de modificación al grupo con el mismo nombre que el departamento

Grant-SmbShareAccess -Name $dept.DepartName -AccountName $dept.DepartName -AccessRight Change -Force

#Quitar el permiso de acceso al grupo TODOS

Revoke-SmbShareAccess -Name $dept.DepartName -AccountName "Todos" -Force

}

foreach($user in $userfile){

#Crear un directorio personal para cada usuario

New-Item -ItemType Directory -Path ("C:\Shared\Users\"+$user.UserLogin)

#Crear la compartición en SMB

New-SmbShare -Name $user.UserLogin -Path ("C:\Shared\Users\"+$user.UserLogin)

#Dar permisos de acceso total al usuario de dicha carpeta personal

Grant-SmbShareAccess -Name $user.UserLogin -AccountName $user.UserLogin -AccessRight Full -Force

#Quitar el permiso de acceso al grupo TODOS

Revoke-SmbShareAccess -Name $user.UserLogin -AccountName "Todos" -Force

}