

Prácticas de Infraestructura Informática

Bloque 2: Gestión de equipos mediante Directorio Activo

Sesión 2 - Gestión centralizada de equipos mediante directivas de grupo

Objetivos

Una de las razones fundamentales para adoptar el Directorio Activo es la de proporcionar el soporte básico para el uso de otra tecnología de gestión conocida como Directivas de Grupo (*Group Policy*). Esta tecnología permite aplicar todo tipo de configuraciones a los sistemas Windows, y cuando se combina con el Directorio Activo es la base para llevar a cabo la administración centralizada de los equipos de una organización.

En esta sesión se verán los conceptos básicos relativos a las Directivas de Grupo, así como las herramientas disponibles para gestionarlas.

Desarrollo

- **COMPROBACIÓN INICIAL:** en esta sesión no se necesita acceder a la red externa. Debido a ello, es conveniente detener el acceso a la red externa para evitar que los clientes Win11 se actualicen. En el sistema anfitrión, *Herramientas administrativas* -> *Enrutamiento y acceso remoto*. Entonces, comprueba que el servicio de enrutamiento está detenido. Si no es así, deténlo.

- **Creación de nuevas máquinas**

Para poder comprobar toda la potencia de administración proporcionada por las Directivas de Grupo, es necesario disponer de un mayor número de clientes. Debido a ello, la primera tarea que se llevará a cabo en esta práctica es poner en marcha dos nuevos clientes.

Creación de las máquinas virtuales para los nuevos clientes

- Creación de la primera máquina virtual
 - *Especificar el nombre y la ubicación:* elegir como nombre PLX-C-53 y dejar como ubicación la ruta por defecto.
 - *Generación:* 2
 - *Memoria:* 1024 MB
 - *Conexión de red:* No conectado
 - *Conectar disco duro virtual:* elegir *Exponer un disco duro virtual más adelante*
 - Finalizar la instalación
- Siguiendo las mismas pautas anteriores, crea también la máquina virtual PLX-C-54.

Creación de los discos virtuales para los clientes

- Creación del disco de diferenciación para la máquina PLX-C-53
 - *Panel Acciones* -> *Nuevo* -> *Disco duro*
 - *Elegir formato de disco:* se selecciona VHDX
 - *Elegir tipo de disco:* se selecciona *Diferenciación*
 - *Nombre:* PLX-C-53
 - *Ubicación (del disco duro primario):* Se selecciona la ruta de *Win11.vhdx*:
D:\ZZGrupoInfraestructuras\Recursos\Discos-Virtuales\Win11.vhdx
 - Finalizar

- Siguiendo las mismas pautas anteriores, crea el disco de diferenciación para la máquina PLX-C-54.

Configuración de los clientes

Se trata de arrancarlos y configurarlos de la forma apropiada.

- Abre la configuración de la máquina PLX-C-53 y realiza las siguientes actuaciones:
 - Conecta el disco PLX-C-53.vhdx a la *Controladora SCSI*.
 - En *Seguridad*, marca la casilla de verificación *Habilitar el módulo de plataforma segura*.
 - En *Procesador*, eleva *Número de procesadores virtuales* a 2.
 - En *Firmware*, establece la unidad de disco como primer dispositivo de arranque.
- Conecta una consola a la máquina y arráncala.
- Inicia sesión con la cuenta de *Alumno* (contraseña *MVclave00*).
- Cambia el nombre del equipo por el de la máquina virtual (PLX-C-53), y reinicia la máquina para que el cambio de nombre tenga efecto.
- Entra en sesión con el usuario *Alumno* y comprueba que el nombre del equipo ha cambiado según lo esperado.
- Establece la siguiente configuración de red:
 - *IP*: 192.168.0.53
 - *Máscara*: 255.255.255.0
 - *Puerta de enlace*: 192.168.0.100
 - *DNS*: 192.168.0.25
- Conecta la interfaz de red de la máquina a *Red virtual interna*.
- Para hacer las pruebas de conectividad de este cliente, en vez de crear la regla de entrada *Permitir ICMPv4*, simplemente desactivarás el firewall, ya que la regla *Permitir ICMPv4* será aplicada más adelante utilizando las Directivas de Grupo. Para desactivar el firewall, *Panel de control* -> *Sistemas y seguridad* -> *Firewall de Windows Defender* -> *Activar o desactivar el Firewall de Windows Defender*. Entonces, selecciona *Desactivar Firewall de Windows Defender*, tanto en la *Configuración de red privada* como en la *Configuración de red pública*.
- Para hacer las pruebas de conectividad, haz ping desde el sistema anfitrión a este cliente y viceversa. Recuerda que la dirección del anfitrión en la red interna es 192.168.0.100 (puerta de enlace).
- Configura el segundo cliente (PLX-C-54) de la misma forma. Ten en cuenta que la IP de este cliente debe ser 192.168.0.54.

• El registro de Windows

El registro es la base de datos de configuración de una plataforma Windows. Contiene toda la información de configuración del sistema operativo. En muchos casos, los programas instalados en el sistema también utilizan el registro para guardar sus configuraciones. Para ver y editar el registro se utiliza la herramienta *Regedit*.

- El ejercicio que se plantea a continuación sobre el registro se realizará en PLX-C-53. Pasa tu atención a esta máquina virtual.
- En PLX-C-53, abre la herramienta *Buscar* e introduce *Regedit*. Esta herramienta solo puede ejecutarse con privilegios elevados, y por eso se abre la ventana de *Control de cuentas de usuario*. Contesta *Sí* para que se ejecute.

El registro se organiza mediante dos elementos básicos: las *claves (keys)* y los *valores*. Las claves son contenedores que pueden contener, a su vez, otras claves y valores. Los valores son datos de configuración del sistema. Los elementos del registro se organizan siguiendo una estructura jerárquica. Los elementos que se encuentran en la cima de dicha estructura se conocen

como claves raíz (*root keys*). Observarás cinco claves raíz. A modo de ejemplo puede indicarse que la clave `HKEY_CURRENT_USER` contiene las configuraciones del usuario actual, y la clave `HKEY_LOCAL_MACHINE`, las configuraciones de la máquina.

(1) PREGUNTA. Además de `HKEY_CURRENT_USER` y `HKEY_LOCAL_MACHINE`, ¿cuáles son las otras tres claves raíz del registro?

El registro tiene unas dimensiones gigantescas, en lo que a número de claves se refiere, y su manejo es árido y complejo cuando se trabaja con él directamente. Debido a ello, las configuraciones suelen realizarse con otras herramientas más amigables proporcionadas por el sistema operativo. A modo de ejemplo, utilizarás el registro para modificar la configuración del servicio del sistema operativo *Cola de impresión*. Se trata del servicio que redirige los trabajos de impresión generados por los programas hacia las impresoras instaladas en el sistema. Si este servicio no está activo, las impresoras no están operativas.

- Mediante la herramienta *Buscar*, localiza y abre la consola *Impresoras y escáneres*. En esta consola se muestran todos los dispositivos de este tipo instalados en el sistema.

(2) PREGUNTA. Indica los equipos mostrados por la consola *Impresoras y escáneres*.

- 1)
- 2)
- 3)

- Se trata de dispositivos de impresión virtuales. No obstante, desde el punto de vista del sistema operativo se tratan como si fueran dispositivos físicos.
- En este momento el servicio *Cola de impresión* está operativo, y, debido a ello, estos dispositivos de impresión virtuales están accesibles. Si se para el servicio *Cola de impresión*, dejarán de estar accesibles.
- De forma habitual, los servicios se manejan con la consola *Servicios*. Esta consola es accesible desde *Herramientas de Windows*. Abre la consola *Servicios*. Busca el servicio *Cola de impresión*. Observa que el estado del servicio es *En ejecución* y el tipo de inicio, *Automático*. Pulsa sobre el servicio para abrir su ventana de propiedades. Entre otros datos, puedes observar el nombre real del servicio, que es *Spooler*, ya que *Cola de impresión* es lo que se conoce como *Nombre para mostrar*. Cierra la ventana de propiedades.
- Vas a cambiar el tipo de inicio, pero editando el registro directamente, en vez de utilizar la consola *Servicios*. Para ello, es necesario conocer en qué parte del registro se guarda la información relativa a los servicios instalados en el sistema. Esta información se almacena en la clave que se indica a continuación:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services`

- Utilizando la herramienta *Regedit*, navega hasta la clave anterior. La clave *Services* almacena una clave por cada servicio disponible en el sistema. Busca la clave *Spooler*. Dentro de esta clave hay un conjunto de valores que representan la información de configuración del servicio. En concreto, el valor *Start* determina el tipo de inicio del servicio. En este momento, este valor debe ser un 2, que significa *Automático*. Vas a cambiar el valor 2 por 3, que significa *Manual*. Para cambiar el valor, pulsa sobre él y en la ventana que se abre, haz el cambio.
- Una vez realizado el cambio, vuelve a la consola *Servicios*. Entonces menú *Acción -> Actualizar*. Debes observar que el tipo de inicio del servicio ha cambiado a *Manual*.
- Para ver el efecto, reinicia la máquina virtual.
- Abre *Impresoras y escáneres* y observa que los dispositivos de impresión se encuentra en el estado *No conectado*. Esto es debido a que *Spooler* no ha arrancado.

Ahora vas a operar a la inversa que antes. Harás un cambio en la configuración de *Spooler* usando la consola *Servicios* y observarás el efecto mediante el editor del registro.

- Abre *Regedit* y ubícate en la clave *Spooler*. Observa que el valor *Start* es 3.
- Abre la consola *Servicios* y observa el servicio *Cola de impresión*. El servicio no está en ejecución y su tipo de inicio es *Manual*. Pulsa sobre el servicio y cambia su tipo de inicio a *Automático*.
- En el editor del registro en el menú *Ver*, pulsa en *Actualizar* y observa que *Start* ha pasado al valor 2.
- Reinicia la máquina virtual para que todo quede como estaba.
- Abre *Impresoras y escáneres* y observa que los dispositivos *Fax*, *Microsoft Print to PDF* y *Microsoft XPS Document Writer* vuelven a estar disponibles.

• Introducción a las directivas de grupo

Un gran número de configuraciones de la plataforma Windows puede ser llevado a cabo utilizando una infraestructura de gestión conocida como *Directivas de grupo*. Esta infraestructura proporciona un conjunto de herramientas para llevar a cabo las configuraciones de una forma cómoda y productiva. Las *Directivas de grupo* interactúan con el registro para establecer las configuraciones, proporcionando un mecanismo mucho más amigable que la manipulación directa del registro para la gestión de las mismas.

La gran importancia de las *Directivas de grupo* es que pueden aplicarse desde los controladores de dominio a los equipos gestionados por dichos controladores, proporcionando de esta forma un mecanismo centralizado de gestión de equipos. No obstante, si bien las *Directivas de grupo* han sido esencialmente diseñadas para aplicarse en el contexto de un directorio activo, también están disponibles para ser utilizadas localmente en cada equipo. En este caso reciben el nombre de *Directivas de grupo local*.

Las configuraciones y posibles ficheros asociados a las directivas de grupo se contienen en unos objetos denominados GPO (Group Policy Objects). En el equipo local habrá un único objeto GPO, conteniendo las directivas de grupo local. En los controladores de dominio se pueden definir y almacenar tantos objetos GPO como se requiera, en función de la complejidad administrativa del dominio en cuestión.


A continuación, se empieza por analizar el uso de esta infraestructura en un equipo local (*Directivas de grupo local*), para después pasar a ver cómo se utilizan en la gestión de los equipos de un dominio.

• Directivas de grupo local

Almacenamiento del GPO local

El objeto GPO local, al igual que los que se definen en el dominio, se almacena en dos partes. Una parte del GPO se conoce como GPC (Group Policy Configuration). Esta parte contiene los datos de configuración del GPO y se almacena en el registro. La otra parte del GPO recibe el nombre de GPT (Group Policy Template) y está orientada a almacenar los ficheros necesarios para la aplicación del GPO, como por ejemplo, un script de inicio de sesión, o un ejecutable de instalación. El GPT se almacena en una carpeta del sistema.

En un sistema recién instalado el GPO local no existe. Éste se crea la primera vez que se ejecuta la herramienta *gpedit.msc*, que es la que se utiliza para gestionar el GPO local.

- En este momento vas a observar las ubicaciones en las que se generará el GPO local, para comprobar que todavía no ha sido creado.
- La parte GPT del GPO se almacena en la carpeta *C:\Windows\System32\GroupPolicy*. Abre esta carpeta y observa que se encuentra vacía.
- Al crear el objeto GPO, esta carpeta se volverá oculta. Para poder verla, hay que configurar el *Explorador de archivos* para que muestre carpetas ocultas. Para ello, en una ventana del *Explorador de archivos*, botón  -> *Opciones* -> pestaña *Ver*. Entonces seleccionar la opción *Mostrar archivos, carpetas y unidades ocultos*.

- La parte GPC del GPO se almacena en el registro en la clave siguiente:
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Group Policy Objects
Abre el editor del registro. Navega hasta la clave *CurrentVersion* y observa que si bien puedes ver la clave *Goup Policy*, aún no existe la clave *Group Policy Objects*.
- Las directivas de grupo local se gestionan con una herramienta llamada *Editor de directivas de grupo local*, si bien, en Windows 11, para acceder a esta herramienta se utiliza un enlace llamado *Editar directiva de grupo*, que es el que muestra la herramienta *Buscar*. Al ejecutar esta herramienta por primera vez se genera el GPO local, aunque sin configuración alguna. Usando la herramienta *Buscar*, localiza y ejecuta *Editar directiva de grupo*. Entonces observa que en *C:\Windows\System32\GroupPolicy* se ha creado el fichero *gpt.ini* y las carpetas *Machine* y *User*. Se trata de la estructura de información requerida para almacenar la parte GPT del GPO local.
- Abre el editor del registro, actualiza la información (menú *Ver -> Actualizar*), si es necesario, y observa que se ha creado la clave *Group Policy Objects*, y dentro de ésta, otras dos claves nombradas mediante identificadores GUID (Global Unique Identifier). Estas dos claves almacenan la parte GPC del GPO local.

Editor de directivas de grupo local

Esta herramienta está orientada a gestionar el GPO local. Recuerda que a esta herramienta se accede mediante el enlace *Editar directiva de grupo*.

- Si en este momento *Editor de directivas de grupo local* no estuviera en ejecución, ejecútalo.
Los diferentes aspectos de configuración a gestionar por las *Directivas de grupo* se denominan, a su vez, *directivas*. Éstas se organizan en dos grupos, las que se aplican al equipo y las que se aplican a los usuarios.
- En el *Editor de directivas de grupo local* observa las ramas *Configuración del equipo* y *Configuración de usuario*. Bajo estas ramas hay, a su vez, otras ramas orientadas a organizar las directivas. La rama *Configuración de Windows* engloba, fundamentalmente, aspectos relativos a la configuración de seguridad del sistema, mientras que la rama *Plantillas administrativas* permite gestionar el resto de la configuración. La gran mayoría de las directivas se encuentran bajo la rama *Plantillas administrativas*.
- Para ver la interacción entre el *Editor de directivas de grupo local* y el registro, vas a configurar una directiva cualquiera, por ejemplo, la directiva que impide a los usuarios cambiar el tema. Éste determina las combinaciones de colores utilizadas por el sistema para presentar la información en el escritorio. Se desea que la directiva se aplique a los usuarios locales, por lo que hay que buscar esta directiva en la rama *Configuración del usuario*. Para acceder a esta directiva utiliza la siguiente ruta:
Configuración del usuario -> Plantillas administrativas -> Panel de control -> Personalización -> Impedir cambiar el tema.
Haz doble clic sobre la directiva para abrir el asistente que permite cambiar su configuración. Observa que el estado actual de la directiva es *No configurada*. Esto significa que se aplica el comportamiento por defecto, que en este caso es permitir al usuario cambiar el tema.
- Antes de aplicar la directiva, vas a comprobar que el usuario puede cambiar el tema. Botón derecho sobre el *Escritorio -> Personalizar*. Busca el apartado *Tema* y ábrelo. Comprueba que puedes elegir cualquiera de los temas. Sin embargo, para no modificar el entorno de trabajo, no lo cambies. Simplemente, has comprobado que puedes realizar el cambio. Cierra la pantalla de personalización.
- Vuelve al *Editor de directivas de grupo local*, abre la directiva *Impedir cambiar el tema*, elige la configuración *Habilitada* y aplícala. En la columna *Estado* del *Editor de directivas de grupo local* se muestra el estado *Habilitada*.
- Abre de nuevo la pantalla de personalización y ubícate en el apartado *Tema*. Entonces comprueba que ya no puedes cambiar el tema. Justo encima del apartado *Tema actual*, se

muestra un mensaje relacionado con las restricciones a la configuración impuestas por la directiva que acabas de aplicar.

(3) PREGUNTA. ¿Qué indica dicho mensaje?

- La idea es que la directiva aplicada limita la capacidad de los usuarios de modificar la configuración del sistema. Muchas directivas se utilizan precisamente para esto, otras se usan para otros cometidos.
- Ahora vas a observar el efecto de la aplicación de esta directiva en el registro del sistema. Abre el editor del registro. En el menú *Ver*, pulsa en *Actualizar*. Bajo la clave *Group Policy Objects*, puedes observar las dos claves nombradas mediante identificador GUID. Una de estas claves termina con la palabra *Machine* y la otra con *User*. La que termina con *Machine* almacena las configuraciones relativas al equipo, y la que termina con *User*, las correspondientes a los usuarios. Observa que en la clave *User* se han generado un conjunto de claves hasta *Explorer*, en la que se ha creado el valor *NoThemsTab*.

(4) PREGUNTA. ¿Qué número se almacena en dicho valor?

- El valor indicado en la pregunta anterior significa que esta directiva está habilitada.
- En el *Editor de directivas de grupo local*, vuelve a dejar la directiva *Impedir cambiar el tema* en el estado *No configurada*, que es su configuración por defecto.
- Si la ventana *Personalizar* estaba abierta, ciérrala y vuelve a abrirla. Ubícate en el apartado *Tema* y comprueba que, de nuevo, puedes cambiar el tema. No obstante, no realices ningún cambio. Cierra la ventana *Personalizar*.
- Vuelve al editor del registro. En el menú *Ver*, pulsa en *Actualizar*. Comprueba que *NoThemsTab* ha sido eliminado.

• Directivas de grupo

Cuando se utiliza el término *Directivas de grupo* “a secas”, sin el calificativo “local”, se hace referencia a directivas aplicadas en el contexto de una infraestructura de directorio activo. En dicho contexto, las directivas pueden aplicarse en tres ámbitos diferentes: en un dominio, en una unidad organizativa, o bien en un sitio (concepto no visto en estas prácticas). En cualquiera de estos ámbitos las directivas se aplican mediante objetos GPO.

Pasos iniciales

Antes de empezar a analizar y probar las directivas de grupo se agregará PLX-C-53 al dominio *practicas.local*, con objeto de tener mayor variedad de clientes para pruebas.

- Arranca el controlador de dominio (PLX-S-DC), e inicia sesión con el usuario *Administrador*.
- Agrega PLX-C-53 al dominio. Reinicia la máquina con objeto de que la agregación sea efectiva. Inicia sesión con el usuario local *Alumno*. Comprueba que la máquina se ha agregado correctamente al dominio mirando el nombre del equipo.
- En el controlador de dominio, comprueba que se ha creado una cuenta para este equipo en el contenedor *Computers*.

(5) PREGUNTA. Indica el nombre de la herramienta que tienes que utilizar para realizar dicha comprobación.

- En el caso de que PLX-C-54 no se encuentre arrancado, arráncalo. De momento, este equipo permanecerá fuera del dominio *practicas.local*. Se usará para comparar ciertos aspectos de

comportamiento entre equipos que se encuentran agregados a un dominio, y equipos que no lo están.

Consola *Administración de directivas de grupo*

La herramienta para gestionar las directivas de grupo se conoce como Group Policy Management Console (*Administración de directivas de grupo*) y es instalada por defecto en los controladores de dominio.

- En el controlador de dominio, para abrir esta consola, *Herramientas administrativas -> Administración de directivas de grupo*.
- Observa que el elemento raíz de la consola es el bosque, *practicass.local* (recuerda que el bosque toma el nombre del dominio raíz).
- Bajo el bosque hay dominios y sitios. En el caso de estas prácticas, los sitios no son aplicables, ya que no se han creado sitios en la infraestructura de directorio activo. En la rama dominios, observarás el dominio *practicass.local*, que por ser un dominio raíz tiene el mismo nombre que el bosque. Bajo este dominio puedes observar todas las unidades organizativas que hay creadas en él, ya que las directivas de grupo son aplicables a ellas.
- Bajo el dominio *practicass.local*, también debes observar el contenedor *Objetos de directiva de grupo*. Se trata de un contenedor virtual cuyo objetivo es presentar al usuario todos los objetos GPO creados en el dominio. Cuando se instala un controlador de dominio se crean dos objetos GPO por defecto, que son el *Default Domain Controllers Policy* y el *Default Domain Policy*. El primero contiene directivas que se aplican a todos los controladores del dominio, y el segundo, directivas aplicables a todos los equipos del dominio. Microsoft recomienda NO modificar estos objetos GPO creados por defecto.
- Vas a analizar alguna de las directivas aplicadas por el GPO *Default Domain Policy*. En el contenedor *Objetos de directiva de grupo*, haz doble clic en el objeto *Default Domain Policy*. En el caso de que se muestre el mensaje “Los permisos para este GPO en la carpeta SYSVOL no son coherentes con los de Active Directory...” Pulsa *Aceptar*. Entonces elige la pestaña *Configuración*. Esto genera automáticamente un informe de la configuración de la directiva de grupo. En el caso de este GPO, solo se definen directivas de equipo, relativas a diversos aspectos de seguridad. Para ver las directivas establecidas, en el apartado *Configuración de seguridad* pulsa en el enlace *mostrar*.
- En este punto, te centrarás en analizar el primer bloque de directivas. Se trata de *Directivas de cuenta/Directiva de contraseña*. Esta sección aglutina un conjunto de directivas que obligan a los usuarios a utilizar unas determinadas políticas en la creación de sus contraseñas. Pulsa en *mostrar*. Entonces fíjate en las dos directivas siguientes:
 - *Las contraseñas deben cumplir los requisitos de complejidad*. Uno de estos requisitos impone que la contraseña debe contener caracteres de al menos tres grupos de entre cuatro. Estos grupos son las letras mayúsculas, las letras minúsculas, los dígitos numéricos (del ‘0’ al ‘9’) y los caracteres no alfabéticos (como por ejemplo, ‘\$’, ‘#’, ‘%’, etc.). Observa que esta directiva se encuentra en el estado *Habilitado*.
 - *Longitud mínima de la contraseña*.

(6) PREGUNTA. ¿En qué valor se encuentra establecida esta directiva?

-
- Ahora comprobarás cómo las directivas anteriores son impuestas a PLX-C-53, por encontrarse este equipo integrado en el dominio. En este equipo abre la consola *Administración de equipos*. Entonces abre *Usuarios y grupos locales -> Usuarios*. Crea un nuevo usuario llamado *Pruebas*. Introduce como contraseña **123** y comprueba que no puedes crear el usuario. El problema es que la contraseña no cumple los requisitos de complejidad. Ahora prueba con **Aa1234**. Tampoco se puede crear el usuario. En este caso el problema es que la contraseña no cumple la longitud mínima. Finalmente prueba con **Aa12345**. Esta contraseña sí cumple todos los requisitos

establecidos por las directivas, y por lo tanto el usuario se creará. Una vez creado el usuario, elimínalo, ya que no será necesario utilizarlo posteriormente.

- Ahora pasarás a trabajar en PLX-C-54, que no está integrado en el dominio, por lo que no estará afectado por las directivas de contraseña del dominio. En este equipo, crea el usuario *Pruebas*. Introduce como contraseña **123**. Comprueba que el usuario se crea sin problemas. Finalmente, elimina el usuario *Pruebas*.

Almacenamiento de objetos GPO

Los objetos GPO generados en el dominio se almacenan siguiendo un esquema similar al utilizado para almacenar el GPO local. Al igual que éste, los GPO del dominio se organizan en dos partes, la GPC (Group Policy Configuration) y la GPT (Group Policy Template). En el caso del dominio, la parte GPC se almacena en la base de datos del dominio, y la parte GPT, en una carpeta del controlador de dominio.

- Vas a observar la parte GPT de los dos GPO creados por defecto en el controlador de dominio. Estos objetos se almacenan en la siguiente ruta:
C:\Windows\SYSTEM32\sysvol\practicas.local\Policies\
 - En el controlador de dominio, observa que en esta ruta hay creadas dos carpetas nombradas mediante nombres de tipo GUID. Si entras en cualquiera de ellas, podrás observar que tienen la misma estructura que la correspondiente al GPT local.
 - Vuelve a la consola de *Administración de directivas de grupo*. Selecciona el GPO *Default Domain Controllers Policy*. Elige la ficha *Detalles* y observa el identificador de este GPO (campo *Id. único*). Comprueba que este identificador se corresponde con una de las carpetas ubicadas en C:\Windows\SYSTEM32\sysvol\practicas.local\Policies\. Selecciona ahora el GPO *Default Domain Policy* y observa que su identificador (campo *Id. único*) se corresponde con la otra carpeta ubicada en la ruta anterior.

Creación y vinculación de objetos GPO

- Para crear un GPO, en la consola de *Administración de directivas de grupo*, selecciona *Objetos de directiva de grupo*. Entonces botón derecho -> *Nuevo*. Introduce un nombre para el GPO, por ejemplo, *Directiva-de-Prueba* y *Acepta*. Se crea el objeto GPO. Selecciona el objeto GPO que acabas de crear, y en la pestaña *Configuración*, observa la configuración del objeto. En este momento no hay ninguna configuración definida (nada en *Configuración del equipo* y nada en *Configuración del usuario*).
- En la ficha *Detalles*, observa el *Id. único* del GPO. Comprueba que se ha creado una carpeta para este objeto GPO en C:\Windows\SYSTEM32\sysvol\practicas.local\Policies\.

La creación de un objeto GPO no implica que éste empiece a aplicarse. Para ello, el objeto debe vincularse con una ubicación (sitio, dominio o unidad organizativa). Una vez que el GPO se ha vinculado a una ubicación, comenzará a aplicarse a todos los objetos de esa ubicación, ya sean estos, equipos o usuarios.

- De momento, vas a enlazar el objeto GPO al dominio, ya que en este caso se aplicará a todos los equipos y usuarios del dominio. Para hacer la vinculación, selecciona el dominio (*practicas.local*), entonces botón derecho -> *Vincular un GPO existente*. Selecciona el GPO *Directiva-de-Prueba* y acepta. Observarás que se crea el vínculo correspondiente debajo de *practicas.local*.

De momento, el GPO no tiene ningún efecto, ya que en él no se ha establecido ninguna configuración.

Edición de objetos GPO

La edición de objetos GPO se lleva a cabo mediante una herramienta conocida como *Editor de administración de directivas de grupo*. Esta herramienta se lanza directamente desde la consola de *Administración de directivas de grupo*.

- Selecciona *Directiva-de-Prueba*. Botón derecho -> *Editar*. Esto abre el *Editor de administración de directivas de grupo*. Esta herramienta es equivalente a la herramienta *Editor de directivas de grupo local*, que es la que se utiliza para editar el GPO local, y que ha sido vista anteriormente. No obstante, hay algunas diferencias, que se verán más adelante.
- Ahora vas a probar a configurar una directiva. A modo de ejemplo utilizarás una directiva que sirve para impedir a los usuarios utilizar la consola de comandos.
- En PLX-C-53, inicia sesión con el usuario del dominio *Alu1*. Abre la consola de comandos. Observa que en este momento, el usuario *Alu1* no tiene ninguna restricción de acceso a esta consola.
- En el controlador dominio, en el *Editor de administración de directivas de grupo*, abre *Configuración de usuario* -> *Directivas* -> *Plantillas administrativas* -> *Sistema*. Entonces busca la directiva *Impedir el acceso al símbolo del sistema*. En este momento, el estado de esta directiva es *No configurado*. Abre la directiva y habilítala. Cierra el *Editor de administración de directivas de grupo*.
- Pasa tu atención a la herramienta *Administración de directivas de grupo*. Para ver un informe de las directivas que has configurado en el GPO *Directiva-de-Prueba*, con el GPO seleccionado, elige la pestaña *Configuración*. En el caso de que sea necesario, menú *Acción* -> *Actualizar*. En la pestaña *Configuración* el sistema genera un informe de todas las directivas configuradas en el GPO. En la sección *Configuración del usuario*, puedes observar los apartados *Directivas* y *Plantillas administrativas*. Pulsa en el enlace *mostrar*. Ahora observarás el apartado *Sistema*. De nuevo, pulsa *mostrar*, y podrás ver la directiva que acabas de configurar (*Impedir el acceso al símbolo del sistema*). Observa que su configuración es *Habilitado*.

Las directivas aplicadas a usuarios tienen efecto durante los inicios de sesión. La idea es que cuando éstos ocurren, el equipo en el que se inicia sesión consulta al servidor de dominio si debe aplicar alguna directiva de usuario. Si es así, el servidor de dominio le proporciona la directiva al equipo y éste la aplica.

- En PLX-C-53, cierra sesión e inicia sesión de nuevo con el usuario del dominio *Alu1*. Abre la consola de comandos (*Símbolo del sistema*). Debes observar que no puedes utilizarlo.

(7) PREGUNTA. ¿Qué mensaje se indica en la consola de comandos?

- En el controlador de dominio, en el *Editor de administración de directivas de grupo*, cambia el estado de la directiva *Impedir el acceso al símbolo del sistema* a *No configurada*. En *Administración de directivas de grupo*, selecciona la pestaña *Configuración* y comprueba que el informe generado indica que no hay ninguna directiva configurada (NOTA: recuerda *Actualizar*, si es necesario).
- En PLX-C-53, si tienes alguna sesión iniciada, ciérrala. Entonces inicia sesión con el usuario del dominio *Alu1*. Abre la consola de comandos y comprueba que puedes utilizarla sin ninguna restricción.

Ámbito de aplicación de los objetos GPO

Los objetos GPO se pueden aplicar en tres ámbitos diferentes: *Dominios*, *Unidades Organizativas* y *Sitios*. Las directivas configuradas en un objeto GPO se aplicarán a todos los equipos y usuarios que se encuentran en el mismo ámbito que el objeto GPO. Debe tenerse en cuenta que los dominios son jerárquicamente superiores a los sitios y a las unidades organizativas. Por consiguiente, cuando un GPO se aplica a un dominio, se aplicará también a todos los sitios y unidades organizativas contenidas en él.

- Para probar el ámbito de aplicación de los objetos GPO vas a trabajar con dos objetos de este tipo: uno ya ha sido creado y vinculado al dominio *practicas.local*, se trata de *Directiva-de-Prueba*; el otro, que se llamará *Directiva-de-Prueba-2*, lo crearás a continuación y lo vincularás a la unidad organizativa *Alumnos*. Entonces comprobarás que a los usuarios

alumnos se les aplicará las configuraciones de los dos objetos GPO, pero a los usuarios que no son alumnos solo se les aplicará la configuración del objeto GPO vinculado al dominio.

- Crea el objeto GPO *Directiva-de-Prueba-2* y vincúlalo a la unidad organizativa *Alumnos*. Despliega *Alumnos* para comprobar la vinculación del GPO.
- Mediante este GPO vas a establecer una fuerte restricción de seguridad para los usuarios *Alumnos*. Se trata de evitar que tengan acceso al panel de control del equipo. Para ello, selecciona *Directiva-de-Prueba-2* -> *Editar* para abrir el *Editor de administración de directivas de grupo* para esta nueva directiva. Entonces, selecciona *Configuración de usuario* -> *Directivas* -> *Plantillas administrativas* -> *Panel del control*. Busca la directiva *Prohibir el acceso a Configuración de PC y panel de control* y habilítala. En la consola *Administración de directiva de grupo*, genera el informe del GPO para corroborar que la directiva se ha configurado según lo esperado.
- Ahora selecciona el GPO *Directiva-de-Prueba*. Genera un informe del mismo y comprueba que en él no hay ninguna directiva configurada. Configura en este GPO la directiva que impide el acceso al símbolo del sistema. Después, genera el informe del GPO para corroborar la configuración aplicada.
- En PLX-C-53, inicia sesión con el usuario *Prof1*. Debes comprobar que a este usuario se le ha aplicado la directiva *Impedir el acceso al símbolo del sistema*, ya que esta directiva está en un GPO aplicado al dominio, y que, por consiguiente, se aplicará a todos los usuarios del dominio. Asimismo, comprueba que este usuario no tiene restricción de acceso al *Panel de Control*.
- Cierra la sesión abierta con *Prof1* y abre una nueva sesión con *Alu1*. Comprueba que para este usuario, ambas directivas han sido aplicadas, por lo que ni puede utilizar el panel de control, ni el símbolo del sistema.

(8) PREGUNTA. Si iniciases sesión con el usuario local *Alumno*, ¿se le aplicarían las directivas configuradas en alguno de los GPO anteriores (*Directiva-de-Prueba* y *Directiva-de-Prueba-2*)? Razona tu respuesta.

- Inicia sesión con el usuario local *Alumno* y confirma tu respuesta anterior.

Directivas de usuario frente a directivas de equipo

Las directivas configuradas en los objetos GPO pueden ir orientadas a usuarios o equipos. Las directivas orientadas a usuarios se aplicarán a todos los usuarios que se encuentren en el ámbito de aplicación de su GPO. Asimismo, las directivas de equipo se aplicarán a todos los equipos ubicados en el ámbito del GPO. Ambos tipos de directivas se pueden combinar en el mismo GPO, no obstante, las buenas prácticas de uso de objetos GPO recomiendan mantenerlas en GPO separados.

- Con objeto de indicar apropiadamente la orientación funcional de los GPO creados en el dominio, renómbralos según se indica a continuación:
 - *Directiva-de-Prueba* cambia a *Directiva-de-Usuarios*
 - *Directiva-de-Prueba-2* cambia a *Directiva-de-Usuarios-2*

Las directivas de equipo se aplican “teóricamente” al arrancar el equipo. Sin embargo, esto falla muy a menudo, debido a que cuando el cliente intenta contactar con el controlador de dominio para que éste le informe de las directivas a aplicar, todavía no se ha establecido una comunicación válida. Entonces la aplicación de estas directivas se fía al mecanismo de refresco en segundo plano. El tiempo de aplicación por defecto de este mecanismo es cada 90 minutos más un desplazamiento aleatorio de otros 30 minutos.

(9) PREGUNTA. ¿Cuál crees que será el cometido de este desplazamiento aleatorio? Si tienes dudas, pregúntale a tu profesor.

El tiempo de refresco por defecto es perfectamente adecuado para un entorno de producción, pero en el caso de estas prácticas, la comprobación de la aplicación de las directivas resultaría muy tediosa. Con objeto de superar este inconveniente, se utilizará una herramienta disponible en todo equipo Windows, cuyo objetivo es actualizar sus directivas. Se trata de la herramienta *gpupdate*. Todas las directivas de equipo las aplicarás utilizando esta herramienta, con objeto de observar su efecto con inmediatez.

- Crea un GPO denominado *Directiva-de-Equipos* y vincúlalo al dominio *practicass.local*.
- En este GPO vas a configurar una directiva de equipo. Se trata de la directiva que establece si en la pantalla de inicio de sesión se muestra o no el último usuario que inició sesión. El comportamiento por defecto es que dicho usuario se muestra. Sin embargo, en los entornos de trabajo donde los equipos son utilizados por múltiples usuarios, como las aulas de prácticas de la EPI, no es recomendable mostrar el último inicio de sesión, ya que es más seguro mantener la privacidad de los identificadores de usuario.
- En PLX-C-53, si tienes una sesión abierta, mira el usuario que tiene abierta la sesión. Cierra sesión y solicita iniciar una nueva. Observa que la ventana de inicio de sesión muestra el usuario que tenía la sesión abierta. Éste es el comportamiento que se desea cambiar. Sea cual fuere el usuario anterior, inicia sesión con el usuario local *Alumno*.
- En el controlador de dominio, selecciona el GPO *Directiva-de-Equipos* y éditalo para abrir el *Editor de administración de directivas de grupo*. Observa que hay dos ramas principales: *Configuración del equipo* y *Configuración de usuario*. La primera rama contiene todas las directivas que se aplicarán al equipo, y la segunda rama, las que se aplicarán a los usuarios. Según se indicó anteriormente, vas a aplicar la directiva que establece si en la pantalla de inicio de sesión se muestra o no al último usuario que inició sesión, que es una directiva de equipo. Para acceder a esta directiva, *Configuración del equipo -> Directivas -> Configuración de Windows -> Configuración de seguridad -> Directivas locales -> Opciones de seguridad*. Entonces busca la directiva *Inicio de sesión interactivo: No mostrar último inicio de sesión*. Habilita esta directiva.
- En la consola de *Administración de directivas de grupo*, en la pestaña *Configuración*, asegúrate de que la directiva ha sido habilitada.
- En PLX-C-53 (donde tienes sesión iniciada con el usuario *Alumno*), abre una consola de comandos y ejecuta el comando `gpupdate /force`. Según se indicó anteriormente, este comando fuerza la aplicación de las directivas, tanto las correspondientes al GPO local, como las correspondientes a los GPO ubicados en el dominio y aplicables al equipo.
- Cierra la sesión abierta con el usuario *Alumno*.
- Solicita iniciar una nueva sesión. Observa que la pantalla de inicio de sesión ya no muestra el último usuario que inició sesión. O sea, el comportamiento de la pantalla de inicio de sesión ha cambiado, en respuesta a la directiva que acabas de aplicar.
- Inicia sesión con el usuario local *Alumno*.
- Ahora dejarás la directiva *Inicio de sesión interactivo: No mostrar último inicio de sesión* en su estado original. En el controlador de dominio, cambia el estado de la directiva a NO ESTÁ DEFINIDO.
- En PLX-C-53 ejecuta de nuevo `gpupdate /force`. Cierra sesión. Entonces comprueba que la pantalla de inicio de sesión, de nuevo, vuelve a mostrar el último usuario que inició sesión, *Alumno*, en este caso.

• Preferencias

Las preferencias están orientadas a configurar lo que habitualmente se conoce como experiencia de escritorio del usuario. Entre las operaciones que se pueden llevar a cabo con las preferencias se encuentran la creación de accesos directos, el mapeo de unidades de almacenamiento y de impresoras de red, la creación de carpetas y el despliegue de archivos, aunque éstos son solo algunos ejemplos de sus posibilidades. No obstante, sí debe reseñarse una diferencia esencial entre las preferencias y las directivas. Estas últimas son de obligado cumplimiento, es decir, el usuario no tiene la posibilidad de modificar el comportamiento establecido por una directiva. Sin embargo, en el caso de las preferencias, las configuraciones establecidas por ellas sí pueden ser modificadas por el usuario, si éste lo desea.

- Como ejemplo de preferencia se creará un enlace directo a un programa en el escritorio de los usuarios del grupo *Alumnos*. Esto podría ser útil para hacer visible un programa que hubiera sido distribuido mediante algún mecanismo automatizado. En este caso, a modo de ejemplo, se plantea un ejemplo más simple: se establecerá un enlace directo al bloc de notas.
- Para establecer la preferencia indicada, crea un nuevo objeto GPO denominado *Preferencias-de-Alumnos* y vincúlalo a la unidad organizativa *Alumnos*. Edita el GPO. Se abre el *Editor de administración de directivas de grupo*. Las preferencias se configuran en la rama *Preferencias*, que está disponible tanto para equipos como para usuarios.
- Para establecer la preferencia indicada anteriormente, navega hasta *Configuración de usuario -> preferencias -> Configuración de Windows -> Accesos directos*. Entonces *Botón derecho -> Nuevo -> Acceso directo*. Se abre la ventana de propiedades del acceso directo. En el campo *Acción*, elige *Crear*. Esto significa que cada vez que un usuario afectado por este GPO inicie sesión, se creará el acceso directo. En el campo *Nombre*, se indica el nombre que se desea dar al acceso directo. Llámalo *Notepad*. En el campo *Tipo de destino*, se elige *Objeto del sistema de archivos*, ya que el acceso directo va a hacer referencia a un fichero ejecutable ubicado en el sistema. En el campo *Ubicación*, debe indicarse el lugar en el que se creará el acceso directo. Elige *Escritorio*. En el campo *Ruta de destino*, debe indicarse la ruta completa del fichero al que hace referencia el acceso directo. La ruta del bloc de notas es la siguiente:

`%windir%\system32\notepad.exe`

`%windir%` es una variable de entorno que indica el directorio de instalación de Windows.

Introduce la ruta indicada en el campo *Ruta de destino*. En este caso, no es necesario configurar más campos del acceso directo. *Acepta* para salvarlo. Observa en el panel *Accesos directos* que se ha creado el acceso directo *Notepad*.

En *Administración de directivas de grupo*, selecciona la fincha *Configuración -> menú Acción -> Actualizar*. Comprueba de esta forma que la preferencia ha sido configurada.

- A continuación, vas a comprobar la aplicación del acceso directo configurado. En PLX-C-53, cierra sesión. Ahora inicia una nueva sesión con el usuario *Alu1*. Observa que se ha creado en el escritorio el acceso directo *Notepad*. Haz doble clic sobre el acceso directo para comprobar su correcto funcionamiento. Intenta borrar el acceso directo. ¿Puedes hacerlo? La respuesta debe ser **SÍ**. Recuerda que las preferencias establecen configuraciones que sí pueden ser modificadas por el usuario. Cierra sesión y vuelve a iniciar sesión de nuevo con el mismo usuario (*Alu1*). Observa que aunque has borrado el acceso directo al bloc de notas, ahora dicho acceso vuelve a estar disponible en el escritorio. Esto es debido a que la preferencia se ha vuelto a aplicar al iniciar sesión.
- Cierra sesión e inicia una nueva con el usuario *Prof1*. Comprueba que el acceso directo al bloc de notas no se mapea para este usuario. Esto es debido a que *Prof1* está fuera del ámbito de actuación del GPO *Preferencias-de-Alumnos*.

(10) PREGUNTA. Además de *Alu1*, ¿para qué otro usuario del dominio se establecerá el enlace al bloc de notas en su escritorio? Razona tu respuesta.

- Comprueba tu respuesta iniciando sesión con dicho usuario.

• Ejecución de scripts mediante directivas de grupo

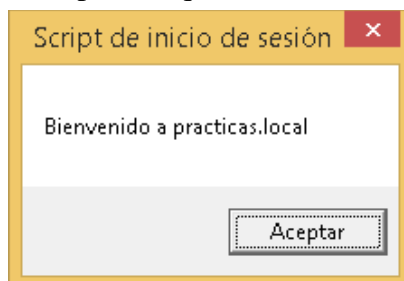
Las directivas y las preferencias permiten aplicar un variadísimo espectro de configuraciones a los equipos de un dominio. Sin embargo, cuando la complejidad de las configuraciones a realizar rebasa las capacidades ofrecidas por directivas y preferencias, entonces es necesario realizar programas que lleven a cabo estas configuraciones. Habitualmente, estos programas se implementan utilizando lenguajes de scripting, que serán tratados más adelante en la asignatura. En este punto, el objetivo es mostrar las capacidades ofrecidas por las directivas de grupo para la ejecución de scripts.

En la plataforma Windows se utilizan fundamentalmente tres tipos de scripts: los ficheros de comandos, los scripts escritos en Visual Basic, y los scripts escritos en PowerShell.

- Empezarás escribiendo un script muy simple, que envía un mensaje a la pantalla, quedando a la espera de que el usuario pulse el botón *Aceptar*. Utilizarás el lenguaje Visual Basic, que te permitirá construir este script con una sola línea de código.
- Antes de comenzar, vas a comprobar el estado de la opción de carpeta que controla la visualización o no de las extensiones de archivos. Cuando se manejan scripts, es recomendable que las extensiones de los archivos estén visibles.
- En el controlador de dominio, *Panel de control -> Apariencia y personalización -> Opciones del Explorador de archivos -> pestaña Ver*, entonces busca la opción *Ocultar las extensiones de archivo para tipos de archivo conocidos*, y asegúrate de que está desactivada.
- En el escritorio, crea un fichero de texto llamado *Script-Inicio.txt*. Después, cambia la extensión *txt* por *vbs*, que es la que corresponde a los scripts de Visual Basic. Observa que cambia el icono del fichero.
- Para editar el script con el bloc de notas, *Botón derecho -> Editar*.
- El script a escribir es muy simple. Utiliza una sentencia de asignación en la que se asigna a una variable el valor retornado por la función *MsgBox()*. Esta función envía un mensaje a la pantalla y espera a que el usuario pulse un botón. La estructura de la línea que tienes que escribir en el script es la siguiente:

```
X=MsgBox(prompt, button, title)
```

- La ventana que debe generar el script es la que se muestra a continuación



- Para buscar información sobre la función *MsgBox()*, en el navegador del sistema anfitrión, teclea *MsgBox vba*. Esto te lleva a una página de Microsoft donde se documenta esta función.

Debes analizar cómo utilizar la función para generar la ventana indicada antes. Ten en cuenta que el botón *OK* de la versión inglesa de VBS se traduce por *Aceptar* en la versión española. Ten en cuenta también que las cadenas de caracteres se escriben delimitadas mediante el carácter comillas dobles (").

(11) PREGUNTA. Escribe en el recuadro siguiente el contenido de tu script.

- Ejecuta el script comprobando su correcto funcionamiento.
- Se trata ahora de aplicar este script mediante directivas de grupo a todos los alumnos de la organización. Para ello se utilizará una directiva disponible en los objetos GPO.

(12) PREGUNTA. Teniendo en cuenta los GPO que has creado en el dominio hasta este momento, así como sus vinculaciones actuales, el GPO más apropiado para desplegar el script sería *Directiva-de-Usuarios-2*. ¿Qué razones crees que apoyan esta elección?

- Ahora vas a realizar las operaciones de configuración necesarias para desplegar *Script-Inicio.vbs* mediante *Directiva-de-Usuarios-2*.
- Lo primero es ubicar el script en un recurso que sea accesible para los ordenadores objetivos. Un recurso accesible a través de la red es una carpeta compartida.

Recurso de distribución de archivos

- En el controlador de dominio, crea la carpeta *C:\ZZRD*. RD quiere decir Recurso de Distribución. Se utilizará esta carpeta como el “recurso de distribución de ficheros de la infraestructura del directorio activo” para los ordenadores del dominio. Siempre que se requiera distribuir un fichero al dominio, se ubicará en esta carpeta.
- Botón derecho sobre *ZZRD* -> *Propiedades* -> ficha *Compartir* -> botón *Compartir*. En este punto hay que elegir los usuarios que estarán autorizados para acceder a este recurso. Selecciona *Buscar personas* -> botón *Opciones avanzadas* -> botón *Buscar ahora*. Entonces busca el grupo *Usuarios autenticados y Acepta*. Este grupo proporciona autorización de acceso al recurso a todos los usuarios que hayan iniciado sesión en el dominio. Por defecto, se proporciona acceso de lectura a este grupo. Esto está bien así, ya que los usuarios solo necesitan poder leer del recurso de distribución. Pulsa el botón *Compartir*, para completar esta operación.
- Mueve *Script-Inicio.vbs* a *C:\ZZRD*.
- En PLX-C-53, si tienes sesión abierta con algún usuario, ciérrala. Entonces, inicia sesión con *Alu1*.
- En PLX-C-53, utilizando la dirección IP del servidor de dominio, comprueba que puedes alcanzar el recurso compartido *ZZRD*. Si tienes dudas sobre esto, pregúntale a tu profesor.

(13) PREGUNTA. Escribe el identificador UNC que has utilizado para acceder al recurso de distribución.

- Haz doble clic sobre el script, comprobando que puedes ejecutarlo.
- En este punto, queda comprobado que PLX-C-53 tiene acceso a *Script-Inicio.vbs*.

Configuración de la directiva para la distribución de scripts

- Edita *Directiva-de-Usuarios-2*. Entonces navega hasta *Configuración de usuario* -> *Directivas* -> *Configuración de Windows* -> *Scripts (inicio de sesión o cierre de sesión)*. Entonces pulsa sobre *Iniciar sesión*. Se abre el asistente *Propiedades: Iniciar sesión*.
- Pulsa en el botón *Agregar*. En el campo *Nombre del script*, debes introducir la ruta que tendrán que utilizar los equipos del dominio para alcanzar el script. Dicha ruta es la siguiente:

\\192.168.0.25\ZZRD\Script-Inicio.vbs

- Escribe la ruta cuidadosamente (cualquier error hará que el script no se ejecute) y *Aceptar*.
- En el asistente *Propiedades: Iniciar sesión* -> *Aplicar* y *Aceptar*.
- En *Administración de directivas de grupo*, pestaña *Configuración*, menú *Acción* -> *Actualizar*. Entonces comprueba que la directiva se ha configurado de la forma esperada.

Pruebas

- En PLX-C-53, cierra la sesión que tienes abierta e inicia una nueva sesión con el usuario *Alu1*. Debes comprobar que el script se ejecuta según lo esperado.
- En PLX-C-53, cierra sesión e inicia una nueva con el usuario *Prof1*.

(14) PREGUNTA. ¿Se ha ejecutado ahora el script de inicio de sesión? ¿Por qué?

(15) PREGUNTA. Si inicias sesión con *Alu1* en PLX-C-51, ¿se ejecutará el script? ¿Por qué?

- Haz la prueba pertinente para verificar tu respuesta anterior.

(16) PREGUNTA. Sin crear ningún nuevo GPO y sin modificar las directivas configuradas en ninguno de ellos, ¿qué podrías hacer para que *Script-Inicio.vbs* se aplicase a cualquier usuario del dominio que iniciase sesión en cualquier equipo?

- Prueba tu respuesta. En PLX-C-53, cierra la sesión abierta. Entonces, inicia sesión con el usuario *Prof1* y comprueba que el script se ejecuta.

• Tareas finales

- Apaga todas las máquinas virtuales, salvo el controlador de dominio.
- En esta sesión has creado los siguientes objetos GPO:
 - *Directiva-de-Equipos*
 - *Directiva-de-Usuarios*
 - *Directiva-de-Usuarios-2*
 - *Preferencias-de-Alumnos*
- Estos GPO afectan al comportamiento de los equipos y usuarios del dominio, pero ya no son necesarios. Debido a ello, es aconsejable eliminarlos.
- En el controlador de dominio, abre *Administración de directivas de grupo*. En la rama *Objetos de directiva de grupo*, localiza los GPO indicados. Para eliminarlos, botón derecho -> *Eliminar*. **¡Atención! Los GPO *Default Domain Controller Policy* y *Default Domain Policy* no debes tocarlos.**
- Menú *Inicio* -> *Windows powershell*. Con objeto de resetear las directivas que se hayan aplicado al controlador de dominio, ejecuta el comando `gpupdate /force`. (NOTA: debido a una de las directivas aplicadas anteriormente, la consola de comandos no está accesible en este momento. Debido a ello, se utiliza la consola de powershell para ejecutar *gpupdate*.)