

SISTEMAS INFORMÁTICOS

Gestión de permisos de red

ÍNDICE

/ 1. Introducción y contextualización práctica	3
/ 2. Directorio activo	4
2.1. Estructura de directorio activo	4
2.2. Crear dominio e instalar Active Directory	5
/ 3. Permisos y derechos	6
3.1. Derechos	6
3.2. Permisos	6
3.3. Asignación de permisos	7
3.4. Conexión remota	7
3.5. Herencia de permisos	8
/ 4. Control de acceso a los recursos	9
4.1. Listas de control de acceso	9
4.2. Auditoría de objetos	10
/ 5. Directiva de seguridad	11
5.1. Crear un GPO en Windows Server	12
/ 6. Caso práctico 1: “Bloquear equipos”	13
/ 7. Caso práctico 2: “Compartir impresoras en red”	14
/ 8. Resumen y resolución del caso práctico	15

SÓLO DIRECTOS

Diferenciar permisos y derechos en entornos de red.

Conocer Directorio Activo de Windows y su funcionamiento.

Facilitar el acceso a recursos por medio de permisos.

Conocer y aplicar directivas de seguridad

/ 1. Introducción y contextualización práctica

Una vez instalado Windows Server y configuradas las opciones locales del sistema, es el momento empezar a configurar el servidor para gestionar los dispositivos clientes de la red.

Durante este tema, veremos cómo administra Windows Server los objetos de la red, y como configurar algunas de sus funcionalidades, como son, la asignación de permisos o aplicar medidas de seguridad.

A continuación, vamos a plantear un caso práctico a través del cual podremos aproximarnos de forma práctica a la teoría de este tema.



Fig. 1. La red es compartida y requiere permisos

/ 2. Directorio activo

El **Directorio Activo**, también conocido como **Active Directory** o **AD**, es el servicio de directorio de Windows Sever que mediante una base de datos, almacena toda la información sobre los objetos de una red, facilitando su organización, gestión y búsqueda por parte de los usuarios y administradores. En un servidor con Directorio Activo se almacenan datos con información acerca de los objetos de la red, como pueden ser archivos, servidores, impresoras, cuentas de usuario y resto de equipos de la red.

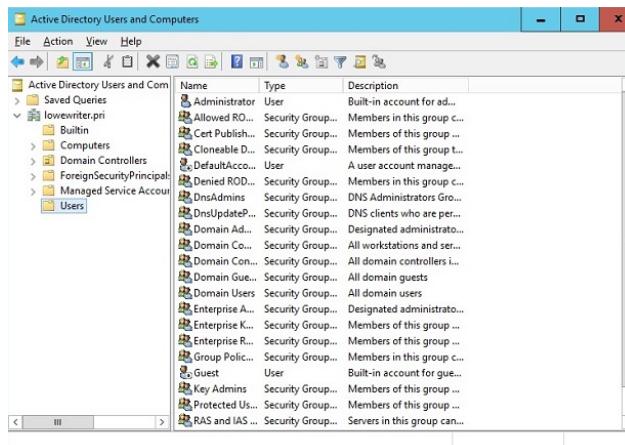


Fig. 2. Directorio Activo en Windows Server

Directorio Activo está principalmente orientado para entornos corporativos o entidades con gran cantidad de recursos informáticos en los que es necesario administrar dichos elementos de forma centralizada, sin necesidad de actuar ordenador por ordenador.

Las principales características de Directorio Activo son:

- **Centraliza la administración de los recursos de la red.** Facilita accesos o los deniega en función de los permisos asignados a los usuarios y equipos de la red.
- **Los usuarios pueden utilizar cualquier recurso y aplicación de la red** siempre y cuando estén habilitados para ello.
- **La administración está fundamentada en directivas.** Las directivas permiten implementar medidas y políticas de seguridad a todos los objetos de la red.
- **Alta escalabilidad.** Permite la integración de multitud de objetos, e incluso establecer relaciones de confianza entre diferentes dominios.
- **Distribución jerárquica.** La información esta almacenada de forma similar a un árbol de directorios.

2.1. Estructura de directorio activo

Su estructura está basada principalmente en los siguientes conceptos y elementos:

- **Dominio.** Es la estructura fundamental, ya que agrupa todos los objetos de forma ordenada y jerárquica. Los dominios son identificados por un nombre de dominio DNS, el cual, a su vez, es el sufijo que se asigna a todos los equipos miembros. Un ejemplo de dominio es radio.es. Un ordenador que pertenezca a dicho dominio y tenga el nombre PC01, su nombre completo sería PC01.radio.es.

En organizaciones de grandes dimensiones, se suelen crear diferentes dominios para que cada una de sus partes sea administrada independientemente, pero integradas en un árbol con nombres comunes.

- **Árbol.** Conjunto de uno o más dominios que comparten el mismo espacio de nombres, y un nombre raíz.
- **Bosque.** Conjunto de uno o más árboles que mantienen la misma estructura de nombres independientes y están conectados entre los dominios.
- **Unidad Organizativa (OU).** Se trata de los contenedores en los que se organizan los objetos del dominio. Se pueden encontrar en su interior grupos, usuarios o equipos.

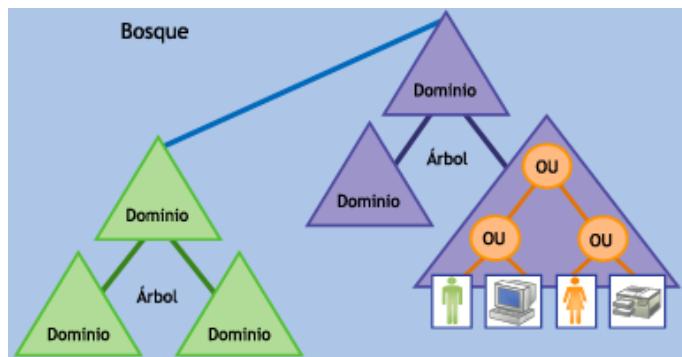


Fig. 3. Diferentes objetos de un servicio de Directorio Activo

- **Grupos de dominio.** Se emplean para asignar permisos a los diferentes recursos del dominio. Siempre que se quiera asignar un permiso a un recurso, debemos asignárselo a un grupo del dominio. A diferencia de los grupos locales, solo se asignan permisos a los objetos y usuarios del equipo en que se crean.
- **Objetos.** Son los recursos de la red: Usuarios, equipos impresores, etc.

2.2. Crear dominio e instalar Active Directory

Antes de comenzar el proceso de creación del dominio e instalación de directorio activo, se recomienda configurar el direccionamiento IP y el nombre del servidor, ya que, si después se realizan cambios, puede haber problemas de configuración o comunicación con el resto de objetos del dominio.

Para crear un dominio en Windows Server, en primer lugar debemos instalar los servicios de Active Directory. En Windows Server las funciones se agregan a través de la herramienta *Administrador del servidor*, a la que se puede acceder mediante el botón *Inicio* de Windows.

Una vez abierta la herramienta, tenemos que hacer clic en *Agregar roles y características*, y seguir el asistente hasta confirmar la instalación.



Fig. 4. Administrador del servidor en Windows Server.

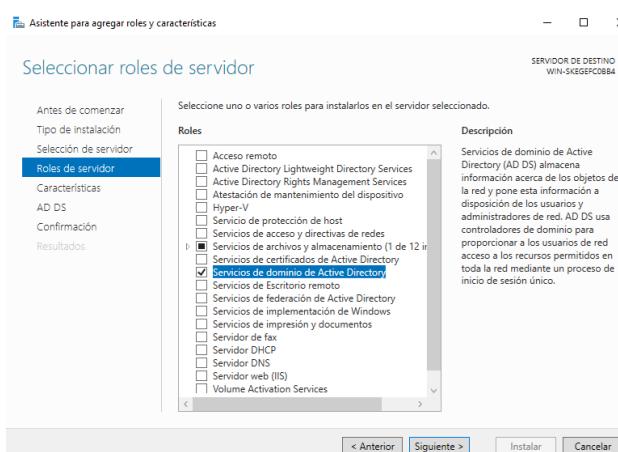


Fig. 5. Agregar rol Servicios de dominio de Active Directory

Instalado Active Directory, el siguiente paso es crear el controlador de dominio. Para ello, desde Administrador del servidor seleccionamos la opción Promover este servidor a controlador de dominio.

/ 3. Permisos y derechos

Windows se basa principalmente en dos conceptos para llevar a cabo el control de acceso de cada usuario y grupo: **los derechos y permisos**.

3.1. Derechos

Los **derechos** son atributos que permiten a los usuarios o grupos realizar determinadas acciones. Los administradores son los encargados de asignar los derechos específicos a usuarios o grupos de usuarios. Entre ellos se pueden encontrar:

- **Derechos de conexión.** Son las distintas maneras que tiene un usuario para acceder al sistema. Por ejemplo, acceder a un equipo a través de la red o de forma local.
- **Privilegios.** Se refieren a la acciones concretas y predefinidas que un usuario puede realizar una vez está conectado al equipo. Algunos privilegios son instalar aplicaciones, crear usuarios, agregar equipos al dominio o cambiar la hora del sistema.

3.2. Permisos

Los **permisos** permiten o deniegan el acceso a los usuarios o grupos de usuarios a los diferentes recursos del sistema o dominio.

Los permisos básicos en los archivos de sistemas Windows son:

- **Lectura.** Solo se puede visualizar el contenido y atributos.
- **Escritura.** Se pueden sobrescribir archivos y modificar los atributos.
- **Lectura y ejecución.** Solo para archivos ejecutables. Permite su lectura y ejecución.
- **Modificar.** Se puede modificar y borrar el archivo.
- **Control total.** Permite cualquier acción sobre el archivo, incluso modificar los permisos o propietarios.

Para cambiar los permisos, haga clic en Editar.		
Permisos de Usuarios	Permitir	Denegar
Control total		
Modificar		
Lectura y ejecución	✓	
Lectura	✓	
Escritura		
Permisos especiales		

Fig. 6. Diferentes permisos que se pueden aplicar

3.3. Asignación de permisos

Una de las funcionalidades básicas y esenciales de Windows Server es compartir archivos entre los usuarios y grupos del sistema o dominio.

Se recomienda asignar los permisos en grupos. Principalmente en entornos con gran cantidad de usuarios se agiliza el trabajo y se tiene un mayor control sobre el acceso de cada usuario. Cada vez que se necesite aplicar, modificar o denegar permisos a carpetas o ficheros, con solo detallar el grupo al que afecta, se aplican dichos permisos a todos los usuarios que formen parte de dicho grupo.

3.4. Conexión remota

Los sistemas Windows permiten conectarse de forma remota al equipo, pero para ello hay que cumplir dos requisitos:

- Habilitar la característica de escritorio remoto en el equipo. Para ello hay que ir a *Este equipo, Configuración del Acceso remoto* y activar *Permitir las conexiones remotas a este equipo*

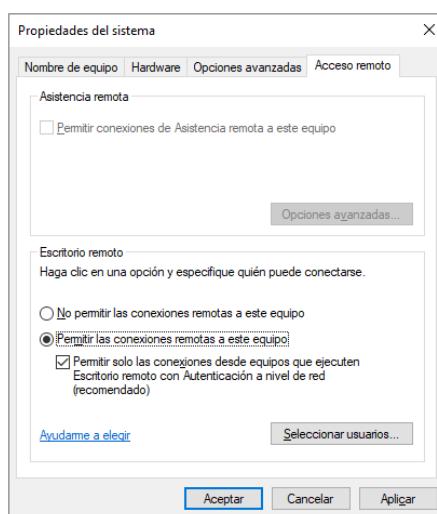


Fig. 7. Activar escritorio remoto

- En la misma ventana, añadir los usuarios que tendrán permitido conectarse de forma remota

3.5. Herencia de permisos

La herencia es una característica para que los objetos de una unidad organizativa o contenedor hereden automáticamente todos los permisos de dicho contenedor. Los administradores pueden asignar o administrar los permisos de herencia fácilmente.

Por ejemplo, en una carpeta a la que tiene acceso, y permiso de escritura el grupo del departamento de Finanzas, sobre los archivos que sean creados en su interior, tendrían los mismos permisos.

Para habilitar o deshabilitar la característica herencia, hay que ir a *Propiedades* de una carpeta, ir a la pestaña *Seguridad* y hacer clic en *Opciones avanzadas*.

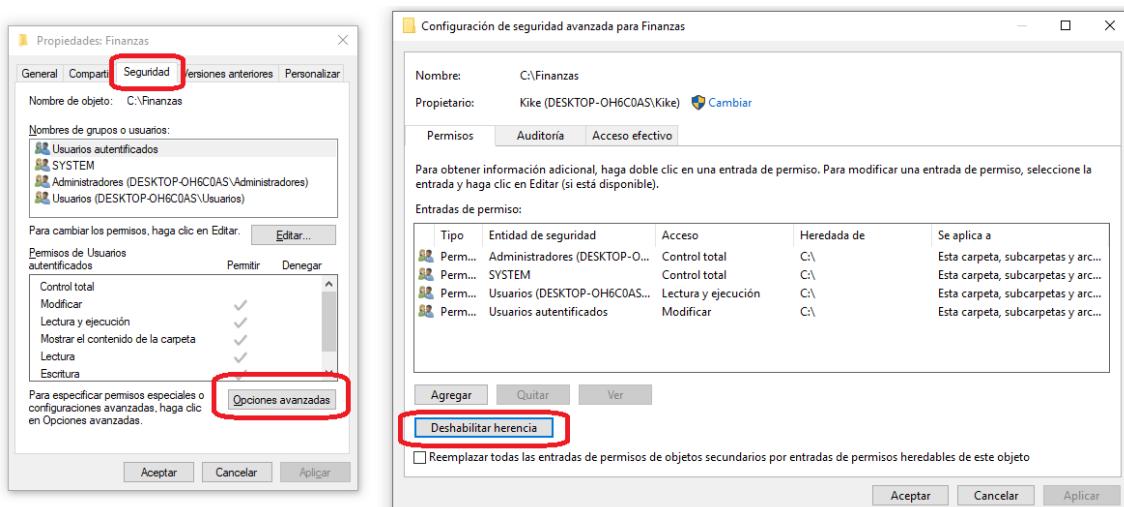


Fig. 8. Ejemplo de deshabilitar herencia en una carpeta

Para bloquear la herencia de todos los objetos del dominio de red, hay que abrir la herramienta *Administración de directivas de grupo*, que se encuentra en las *Herramientas administrativas* de Panel de control.

Dentro de la herramienta, desplegar el bosque hasta llegar al dominio concreto en el que se desea realizar la acción, hacer clic con el botón derecho y seleccionar Bloquear herencia.

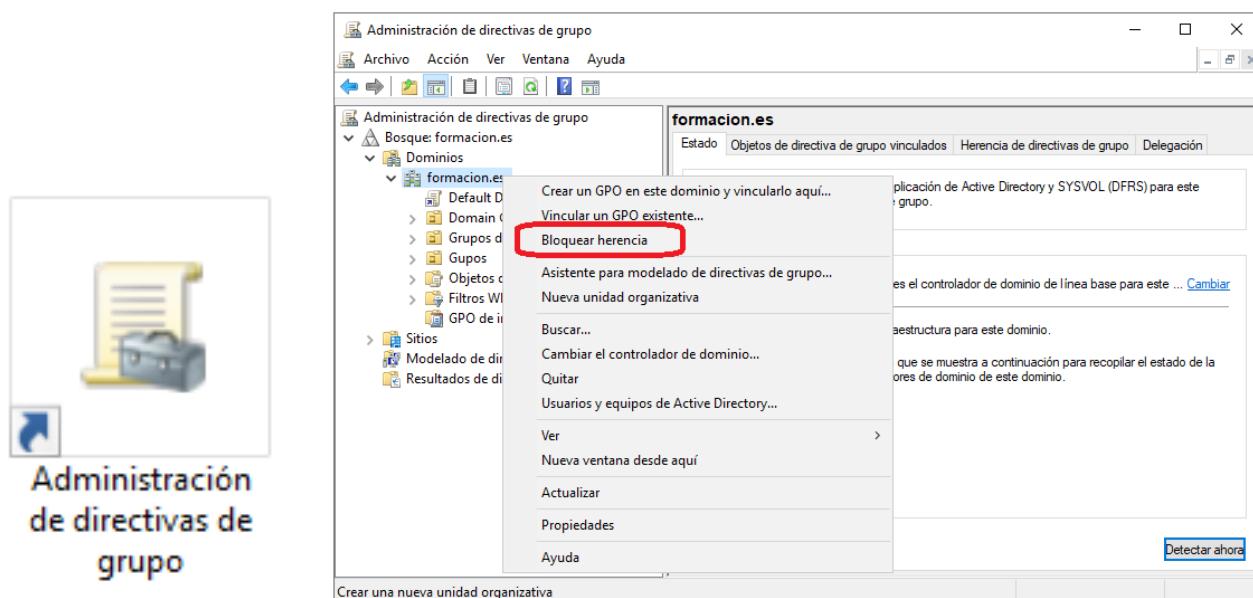


Fig. 9. Administración de directivas de grupo en Panel de control.

Fig. 10. Bloquear herencia en un dominio de red

/ 4. Control de acceso a los recursos

4.1. Listas de control de acceso

Las listas de control de acceso o ACL (del inglés, *Access Control List*), son utilizadas para administrar el tráfico de datos y flujo, por medio de un router o cortafuegos.

Algunas de las tareas de una ACL son:

- Limitar el tráfico para aumentar el rendimiento.
- Filtrar el tráfico, solo permitiendo los tipos de datos admitidos.
- Securizar todos los elementos de la red.
- Permitir o denegar a los equipos de la red el acceso a los diferentes servicios de red.

En Windows Server se incluye por defecto un cortafuegos o firewall. Éste permite definir ciertos valores y parámetros entre el servidor y el resto de equipos de la red. En la parte izquierda del panel de administración del cortafuegos, se pueden crear y modificar tres tipos de reglas:

- **Reglas de entrada.** Son las correspondientes a todo el tráfico que pretende entrar al servidor.
- **Reglas de salida.** Se refiere a las conexiones del servidor hacia la red externa.
- **Reglas de seguridad de conexión.** Aplica reglas especiales para asegurar una mayor protección entre dos dispositivos.

Para crear una nueva regla, hay que hacer clic con el botón derecho sobre la regla de cualquiera de los tipos de reglas, y seleccionar *Nueva regla*.

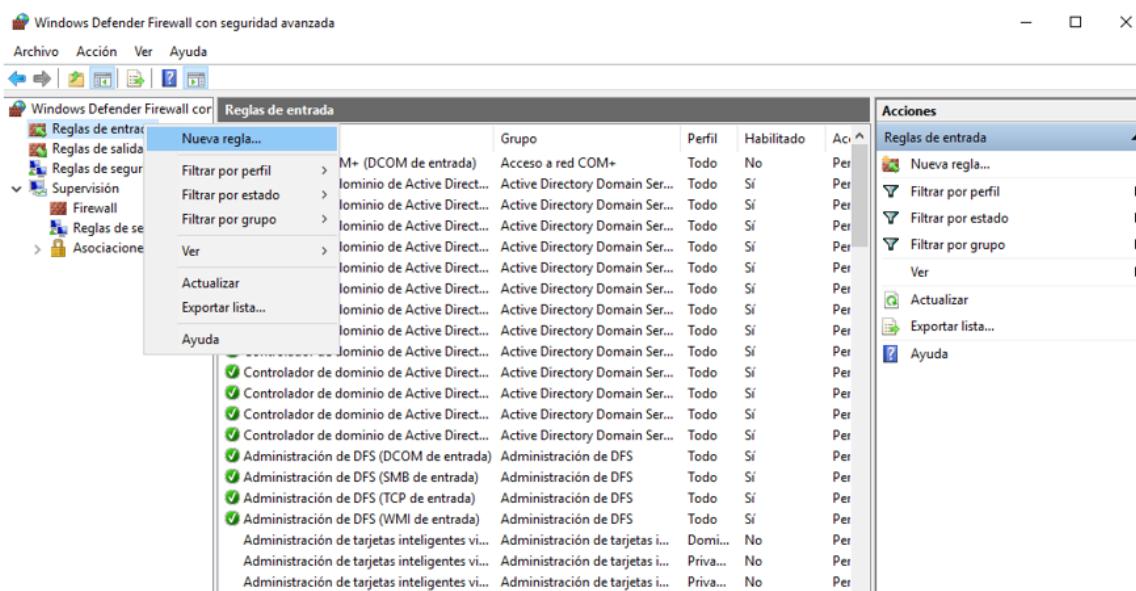


Fig. 11. Windows Defender. Firewall de Windows Server

4.2. Auditoría de objetos

Los administradores también pueden auditar el acceso o intentos de acceso a los objetos por parte de los usuarios.

La auditoría de acceso a los objetos locales se activa desde la herramienta *Directiva de seguridad local*, y a continuación en *Directiva de auditoría, Auditar el acceso a objetos*.

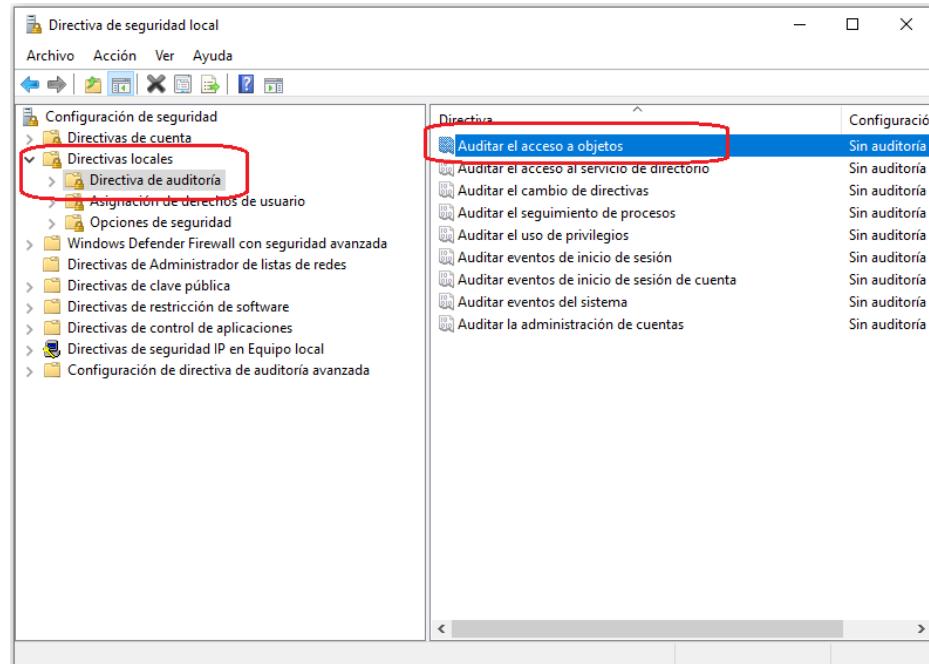


Fig. 12. Auditoría de todos los objetos locales

Para auditar una carpeta o archivo en concreto hay que ir a *Propiedades, Seguridad, Opciones avanzadas y Auditoria*.

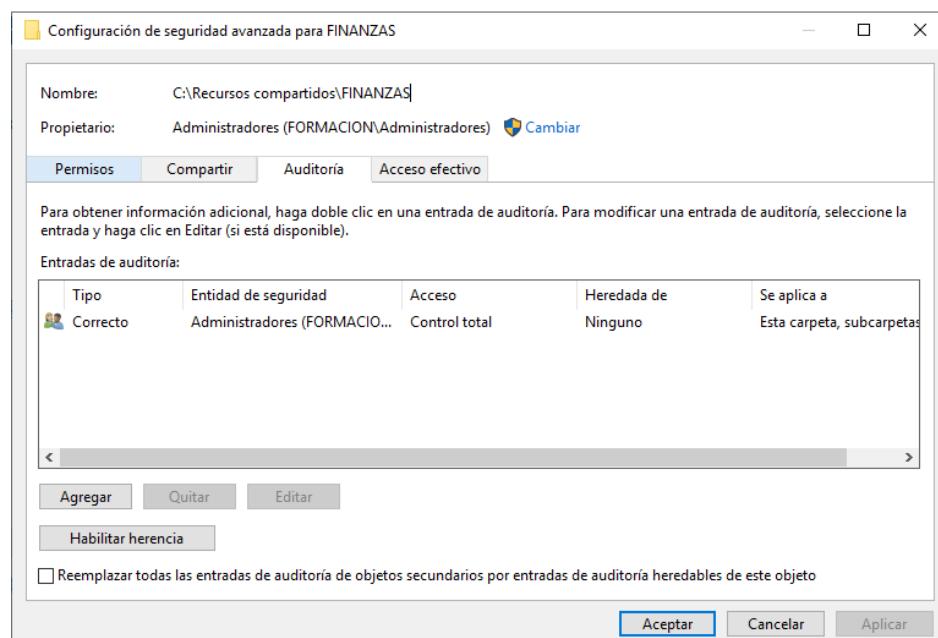


Fig. 13. Auditar una carpeta

Después de activar la auditoria de acceso a un determinado recurso, para ver el registro de acceso hay que acceder a Seguridad en el Visor de eventos.

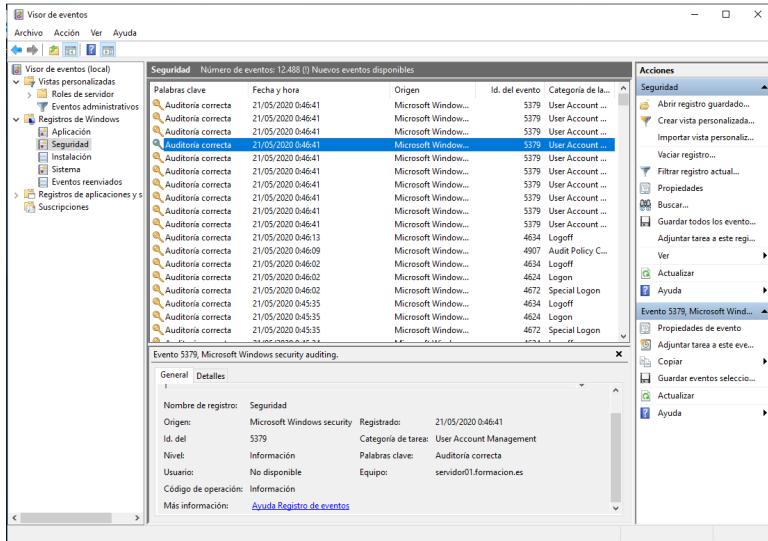


Fig. 14. Visor de eventos en Windows Server

/ 5. Directiva de seguridad

Las directivas de seguridad permiten implementar configuraciones específicas para los usuarios y/o equipos que forman parte del dominio. Dichas directivas se conocen comúnmente como GPO, *Group Policy Object*.

En Windows Server se utiliza la herramienta *Administración de directivas de grupo*, que se encuentra entre las *Herramientas administrativas*. También se puede abrir por medio del comando `gpmc.msc`.

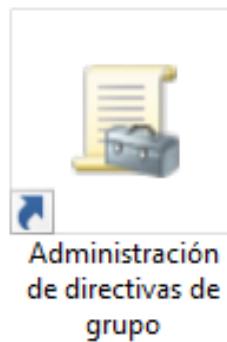


Fig. 15. Administración de directivas de grupo en Panel de control.

Existen diferentes directivas en función del objeto al que se aplican:

- **Equipo local.** Afectan únicamente al equipo local. Es independiente de las que sean aplicadas al dominio al que pertenezca
- **Sitio.** Afectan a todos los equipos y usuarios de un sitio, con indiferencia del dominio al que pertenezcan.
- **Dominio.** Se aplican a todos los usuarios y equipos de un dominio.
- **Unidad Organizativa.** Se aplican exclusivamente a los equipos y usuarios que se encuentren en una determinada Unidad Organizativa.

Dentro de la configuración de las directivas, se tiene acceso tanto a la Configuración de equipo, como a la Configuración de usuario.

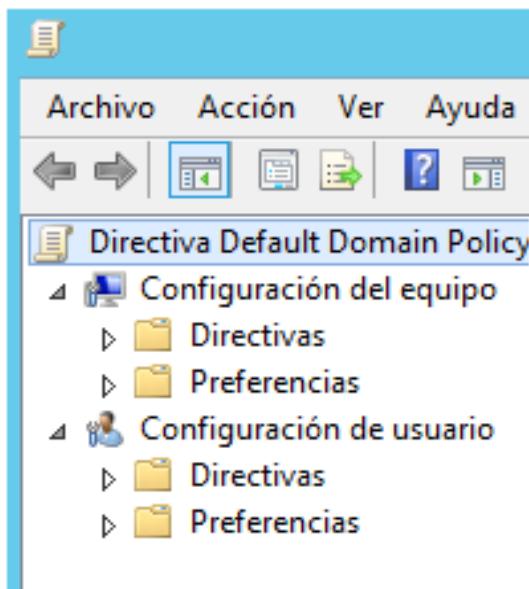


Fig. 16. Aplicar GPO a equipos y/o usuarios.

5.1. Crear un GPO en Windows Server

Para crear una GPO hay hacer clic sobre alguno de los objetos, seleccionar *Crear un GPO...* y definir un nombre para dicha GPO.

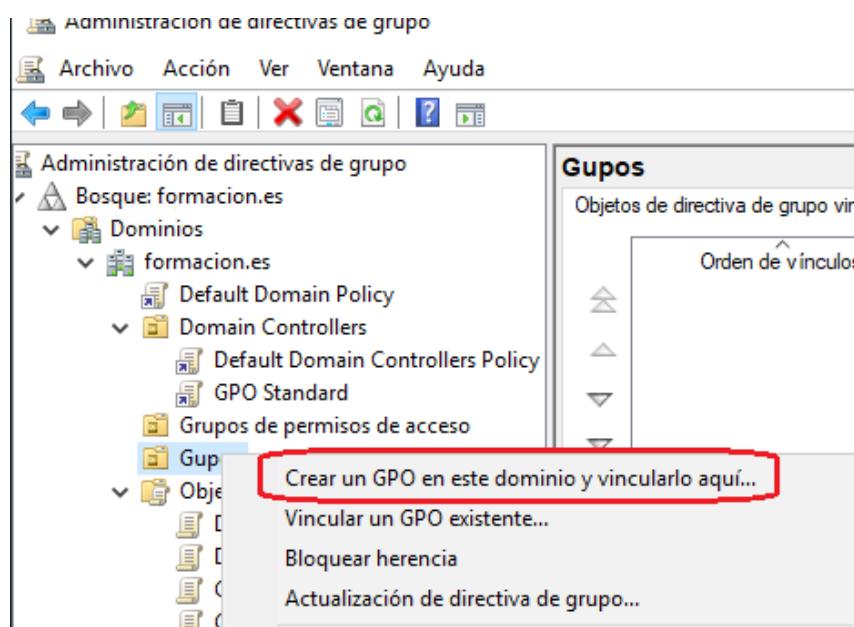


Fig. 17. Crear GPO para un dominio

Después, hacer clic en Editar sobre la GPO creada .

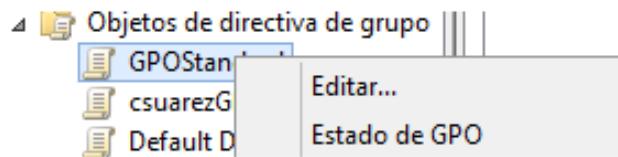


Fig. 18. Editar GPO.

Dentro de la GPO, hay numerosas opciones para aplicar directivas: sobre sistema, software, usuarios, scripts de inicio, impresoras, reglas, etc.

Por ejemplo, para asignar una unidad de red a los usuarios que inicien sesión, hay que ir a *Configuración del usuario, Preferencias, Configuración de Windows, Asignación de unidades*.

A continuación, seleccionar *Nueva, Unidad asignada*. Y tan solo queda introducir los datos de la unidad a compartir.

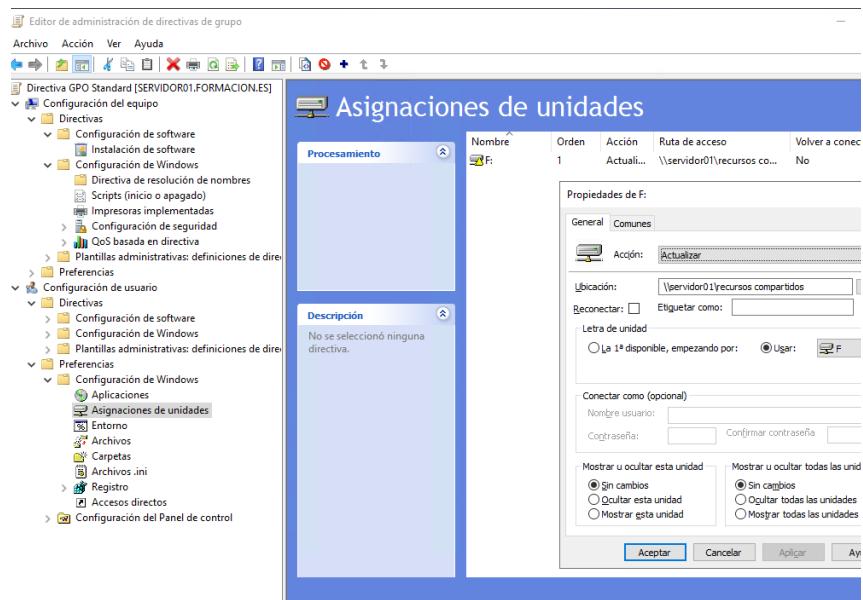


Fig. 19. Asignar unidad de red a todos los usuarios del dominio por GPO

/ 6. Caso práctico 1: “Bloquear equipos”

Planteamiento: Miriam trabaja en el departamento de informática de una empresa en la que hay unos 35 ordenadores y un servidor con Windows Server. Por seguridad, hay una circular en la empresa en la que se informa que todo trabajador debe bloquear su equipo cuando abandone su puesto de trabajo.

Esto no se está cumpliendo como se debiera y por tanto se está poniendo en riesgo la seguridad de la información.

Nudo: ¿Cómo puede Miriam activar que cuando pasen 3 minutos sin actividad en el equipo, la sesión de los usuarios sea bloqueada automáticamente?

Desenlace: Deberá crear una GPO desde el Administrador de directivas de grupo.

La puede llamar por ejemplo Bloqueo por inactividad.

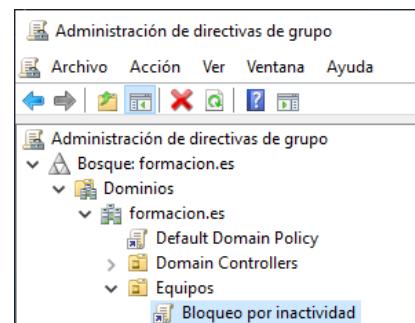


Fig. 20. GPO creada como Bloqueo por inactividad

Posteriormente, basta con hacer clic en *Editar*, y navegar hasta *Configuración de usuario, Directivas, Plantillas administrativas, Panel de control, Personalización*.

Tendría que habilitar las tres siguientes características:

- Habilitar protector de pantalla
- Proteger el protector de pantalla mediante contraseña
- Tiempo de espera del protector de pantalla: Al tratarse de 3 minutos, tiene que indicar 180 segundos

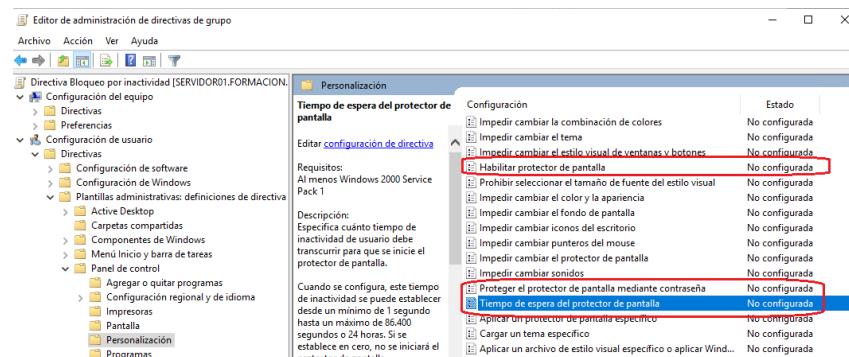


Fig. 21. Editor de GPO

Para que se sincronicen inmediatamente las nuevas directivas en los equipos cliente, se puede forzar la ejecución del comando

`gpupdate /force.`

/ 7. Caso práctico 2: “Compartir impresoras en red”

Planteamiento: Siguiendo con el caso de Miriam, en su empresa, además de los 35 ordenadores y el servidor con Windows Server, han adquirido 4 impresoras para compartir entre todos los usuarios.

Nudo: ¿Cómo puede Miriam compartir las impresoras en red?

Desenlace: Miriam debe instalar cada impresora en el servidor de Windows Server con la aplicación Dispositivos e Impresoras en Panel de control.

En la última ventana del asistente de instalación debe activar la opción Compartir esta impresora para que otros usuarios de la red puedan buscarla y usarla.

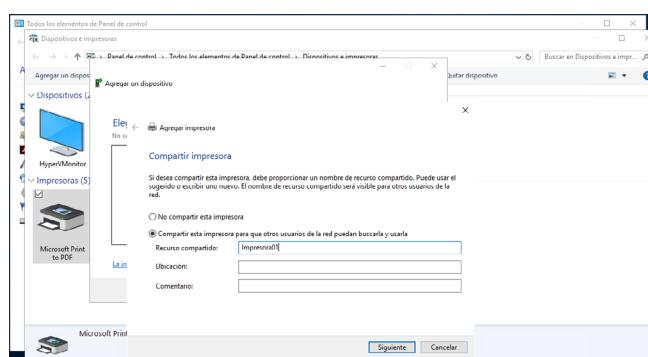


Fig. 22. Compartir impresora en red

En los equipos cliente, se puede usar la ruta \\nombredelservidor para acceder a los recursos compartidos como es la impresora instalada, y compartida por el servidor. Por ejemplo, si el servidor esta nombrado como servidor01, introduciendo \\servidor01 en el Explorador de archivos o en Ejecutar aparecerán los recursos compartidos como las impresoras, archivos o carpetas compartidas.

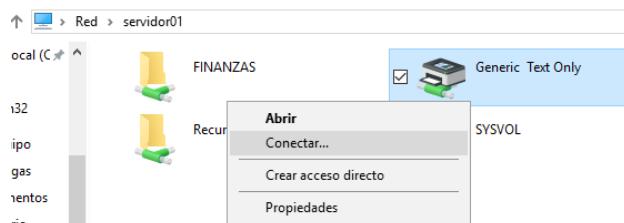


Fig. 23. Acceso a recursos compartidos en red

Haciendo clic en **Conectar**, la impresora quedará instalada en el equipo cliente.

/ 8. Resumen y resolución del caso práctico

Hemos empezado el tema con **el Directorio Activo**, también conocido como Active Directory o AD, siendo el servicio de directorio de Windows Server, que por medio de una base de datos almacena toda la información sobre los objetos de una red y facilita su organización, gestión y búsqueda por parte de los usuarios y administradores.

Hemos aprendido también, que Windows se basa principalmente en dos conceptos para llevar a cabo el control de acceso de cada usuario y grupo: **los derechos y permisos**.

Los derechos son atributos que permiten a los usuarios o grupos realizar determinadas acciones. Los permisos permiten o deniegan a los usuarios o grupos de usuarios, el acceso a los diferentes recursos del sistema o dominio.

Además, se ha estudiado que la **herencia** es una característica para que los objetos de una unidad organizativa o contenedor hereden automáticamente todos los permisos de dicho contenedor. Finalmente, hemos visto que las **directivas de seguridad** permiten implementar configuraciones específicas para los usuarios y/o equipos que forman parte del dominio.

Resolución del caso práctico inicial

Para limitar el acceso a la carpeta 'Apps Diseño' en la empresa de Jose, en primer lugar, éste debe crear un grupo en Active Directory en el que se incluya sólo a los diseñadores gráficos de la empresa.

A continuación, la solución es tan simple como aplicar permisos a la carpeta, exclusivamente para el nuevo grupo de diseñadores gráficos, y quitar el resto de grupos o usuario.

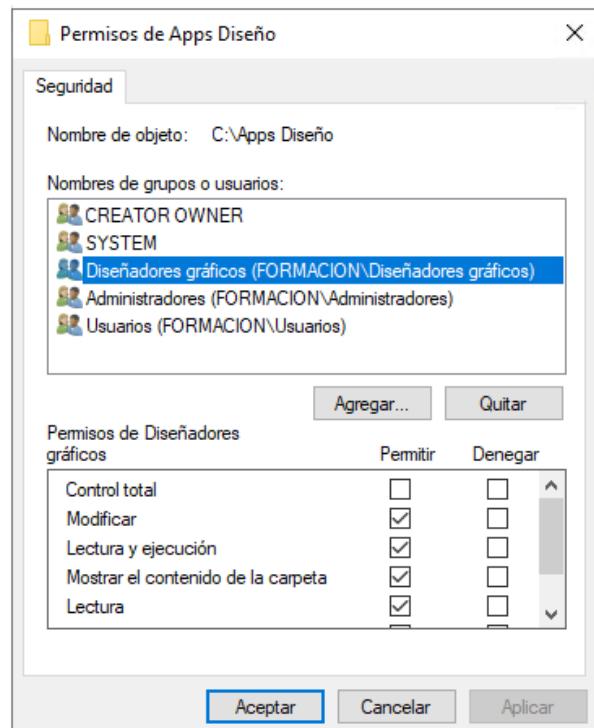


Fig. 24. Permisos para el grupo Diseñadores gráficos a la carpeta Apps Diseño