Unidad 6

Gestión de recursos en una red

Sistemas Informáticos

Índice

6.1. Permisos
6.1.1. La acreditación de los usuarios
6.1.2. Permisos de red y permisos locales
6.1.3. Compartir archivos o carpetas
6.1.4. Herencia
6.1.5. ACL

6.2. Derechos de usuarios
6.2.1. Directivas de seguridad. Objetos y ámbito de directivas

6.3. Servidores
6.3.1. Servidor de ficheros
6.3.2. Servidor de impresión

6.4. Conexión remota. Herramientas

6.5. Herramientas de seguridad
6.5.1. Cifrado
6.5.2. Cortafuegos

Introducción

En esta unidad lo que vamos a ver, van a ser las condiciones de seguridad bajo las cuales los usuarios se conectan a un sistema en red.

Lo primero que veremos a lo largo de este tema serán los permisos y los derechos sobre Windows, y las ACL y en que se basan.

Para establecer estos permisos, también hay que saber como compartir los recursos en Windows.

El siguiente punto que trataremos son las directivas de seguridad, y en que se basan.

Por último, lo que tendremos que ver en la unidad son las herramientas de seguridad existentes en los sistemas como son las de administración remota, la criptografía, etc.

Al finalizar esta unidad

- Sabremos configurar el acceso a recursos locales y en red aplicando permisos locales y en red, herencia y listas de control de acceso.
- Seremos capaces de diferenciar los derechos de usuarios sobre los permisos sobre los recursos.
- Podremos establecer directivas de seguridad sobre usuarios y equipos.
- Conoceremos lo que son derechos de usuario u directivas de seguridad.
- Sabremos implementar y hacer uso de servidores de ficheros, servidores de impresión y servidores de aplicaciones.
- Seremos capaces de acceder a equipos en red o servidores utilizando técnicas de conexión remota.
- Podremos estudiar los requisitos de seguridad del sistema, usuarios y de los datos mediante la inst6alación y evaluación de utilidades de seguridad básicas.

6.1. Permisos

Los **derechos o privilegios** de los usuarios son atributos que afectan a una cuenta de usuario o a un grupo con la función de permitir realizar ciertas acciones sobre todo el sistema y no un solo recurso.

Por otra parte, los **permisos** son características propias de cada recurso en concreto (o conjuntos de recursos aglomerados en otro), en el que se dirá que usuarios o grupos pueden trabajar con estos recursos y que acciones pueden realizar sobre estos.

6.1.1. La acreditación de los usuarios

Cada vez que damos autorización a un usuario para que pueda conectarse a un sistema Windows, el propio sistema le construye una acreditación única que se llama **Security Access Token (SAT)**. Esta es la identificación que realmente el sistema usa para saber quién está generando cada proceso en cada momento y así poder saber si tiene permitido realizar dicho proceso sobre dicho recurso concreto.

Dentro del SAT encontramos los siguientes atributos de protección:

- El **SID** que se usa para que el usuario esté identificado de manera única.
- **La lista de los SID** de cada uno de los grupos en los que está el usuario incluido.
- **La lista de los derechos** que tiene el usuario al completo ya sea por sí mismo o por los grupos a los que pertenece.

6.1.2. Permisos de red y permisos locales

Los permisos que se establecen para un recurso compartido solo tienen validez para los usuarios que acceden a través de la red. En caso de que también se le quiera aportar seguridad de manera local habrá que establecer los permisos anteriormente dichos.

Como pasaba de manera local, los permisos de un recurso compartido tienen una cierta herencia y por lo tanto se aplican a todos los permisos que haya en la red, de manera que, cuando se tenga acceso a un recurso compartido, se tendrá además a las carpetas y archivos que se contienen.

Para controlar el acceso a los recursos compartidos en red, se usan principalmente tres métodos:

- Usar los permisos de recursos compartidos, estos son relativamente sencillos de aplicar y administrar.
- Usar los permisos NTFS que tienen algo más de control sobre los recursos compartidos.
- Usar una combinación de los dos, que suele ser la opción más recomendada.

Si por lo que sea, se usa una combinación de permisos de recursos y NTFS, siempre primará el permiso más restrictivo.

Los permisos NTFS estándar y especiales

En Windows distinguimos dos tipos de permisos NTFS:

- **Los permisos NTFS especiales.** Estos permisos controlan que acciones se pueden llevar a cabo sobre las carpetas y archivos.
- **Los permisos NTFS estándar.** Son combinaciones de permisos NTFS especiales que vienen predefinidos en el sistema.

Estos permisos predefinidos son necesarios para que cuando el administrador comience con la administración de nuestro sistema tenga más facilidad, pero por lo general después sufrirá cambios y se optará por los permisos NTFS especiales.

Cuando se cambian los permisos de las carpetas o archivos en Windows debemos de seguir en la medida de lo posible una serie de reglas:

- Debemos tener en cuenta que a veces, un único proceso puede que conlleve ejecutar acciones sobre distintas carpetas o archivos. Esto quiere decir, que, si ese proceso necesita de permisos específicos en esas carpetas o archivos, debe de tenerlos concedidos, en caso contrario tendremos un error de ejecución genérico por falta de permisos.
- Los permisos de Windows son acumulativos, es decir, un usuario puede ejecutar todos los permisos que tenga disponibles como cuenta de usuario, pero también todos los que tengan los grupos a los que pertenezca.
- No es necesario que haya una denegación de permisos (que también se puede hacer), porque su ausencia ya implica que no se pueden ejecutar esas acciones.
- Si sí que se han denegado permisos, pero a la vez también tenemos activados los mismos, estamos en la tesitura de un conflicto de permisos. En este caso siempre priman los permisos de denegación o negativos. Esto es parecido a lo que pasaba con los permisos explícitos y heredados.

6.1.3. Compartir archivos o carpetas

Para compartir un directorio tenemos dos maneras de cómo actuar:

- Compartir el directorio desde las propiedades de la carpeta.
- Compartir el directorio desde Administración de equipos.

Para compartir un directorio desde las propiedades de la carpeta debemos:

1. Lo primero que haremos será crear la carpeta en cuestión:

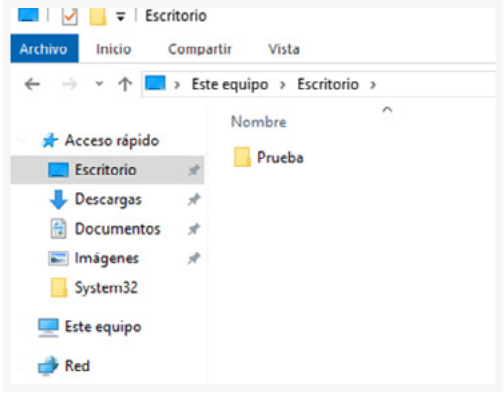

Imagen 1. Compartir directorios 1

2. Cuando esté creado, hacemos clic derecho sobre la carpeta y seleccionamos Propiedades.

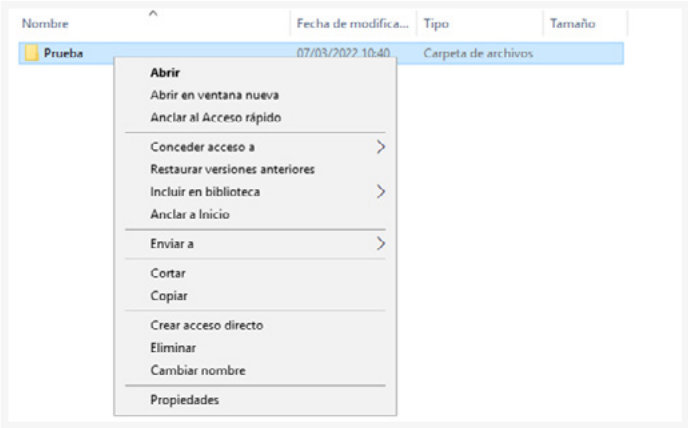

Imagen 2. Compartir directorios 2

3. Dentro de las propiedades, nos dirigimos a la pestaña Compartir.

4. Una vez aquí elegiremos la opción Uso compartido de carpetas y archivos de red → Compartir.

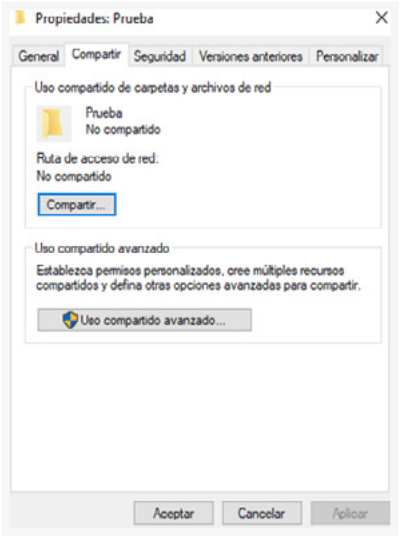

Imagen 3. Compartir directorios 3

5. Nos aparecerá entonces un cuadro de diálogo donde nos dirá que seleccionemos que usuarios tienen acceso a esta carpeta, en nuestro caso hemos seleccionado a Alumno1.
6. Una vez elegidos los usuarios, en la parte derecha se pueden editar los permisos del usuario.

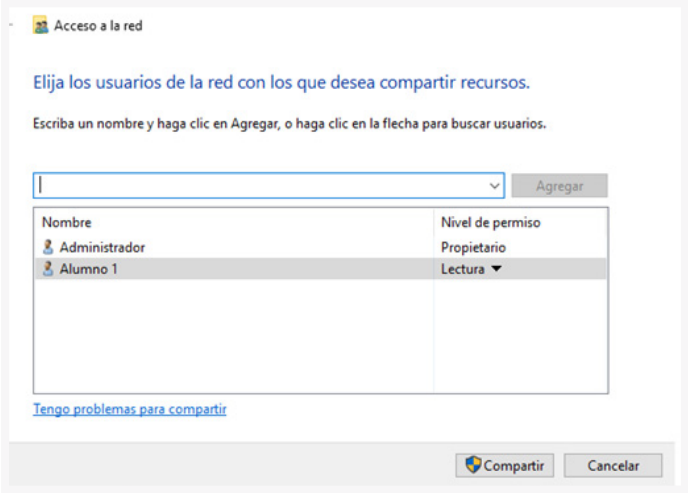

Imagen 4. Compartir directorios 4

7. Acto seguido el sistema nos avisará de que la carpeta ha sido creada y su nombre y ruta de acceso.
8. Si estamos de acuerdo seleccionamos Listo.

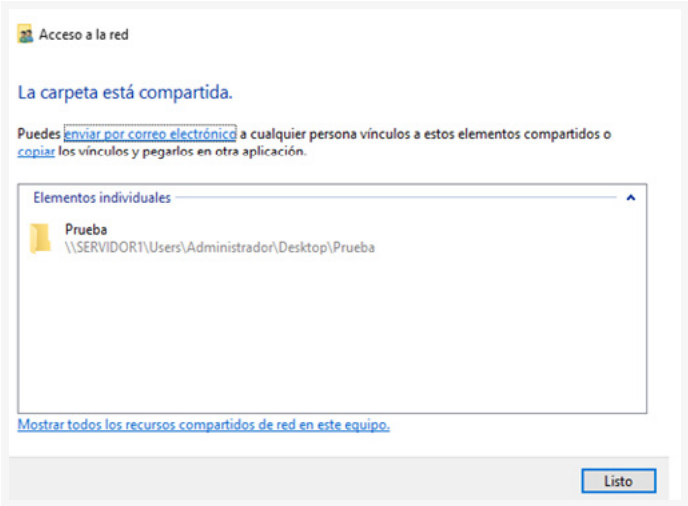

Imagen 5. Compartir directorios 5

9. Si volvemos ahora las propiedades, veremos que ya aparece la carpeta como compartida y su ruta de acceso.

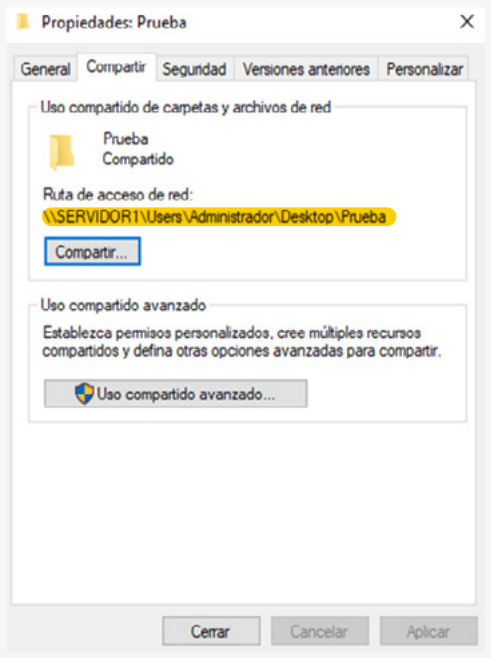

Imagen 6. Compartir directorios 6

10. Por último, si en vez de seleccionar la primera opción, hubiésemos seleccionado la segunda, nos saldría una ventana como la de más abajo, pero esta opción es parecida a la que vamos a hacer a continuación, por lo que no se va a hacer en este apartado.

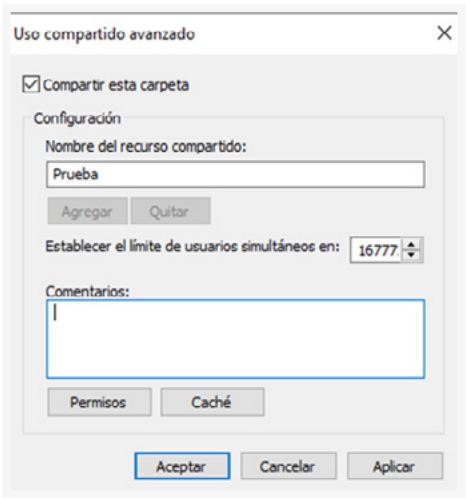

Imagen 7. Compartir directorios 7

11. Si nos dirigimos ahora a un equipo cliente y seleccionamos la pestaña Red del explorador de archivos, nos aparecerán las máquinas visibles, pero no el recurso compartido, por lo que habrá que buscarlo.

12. En la ruta de las carpetas escribimos nosotros:

```
\\SERVIDOR1
```

13. Se nos mostrarán los recursos que ya dijimos se compartían de manera automática.

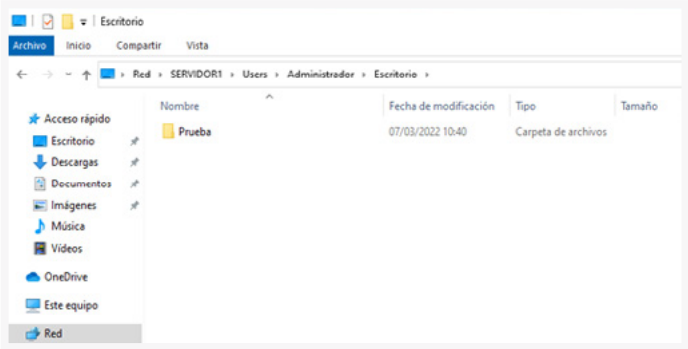

Imagen 8. Compartir directorios 8

14. Si ahora escribimos la ruta completa que se nos planteaba antes, vemos que se ha compartido correctamente dicho recurso.

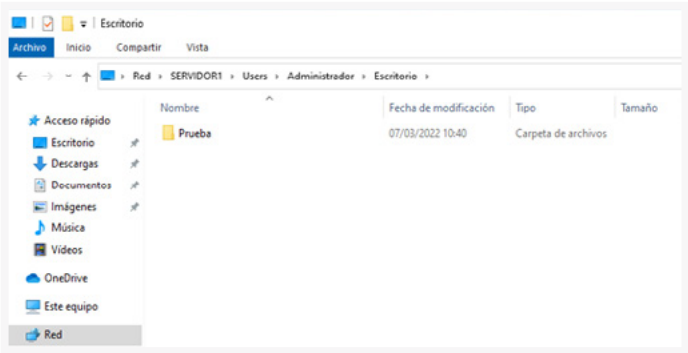

Imagen 9. Compartir directorios 9

PARA TENER EN CUENTA

Aunque no se hayan compartido los directorios padres del recurso creado, estos se crean de manera automática y se comparten para poder llegar hasta el recurso deseado.

PARA TENER EN CUENTA

Además, para poder realizar esta tarea es necesario que el usuario tenga el permiso requerido o sea administrador del sistema

Para realizar esta operación, desde el administrador de equipos, hacemos lo siguiente:

1. Creamos la carpeta que queremos compartir como recurso.
2. Abrimos Administración de equipos.
3. En Recursos compartidos, hacemos clic derecho y seleccionamos Recurso compartido nuevo...

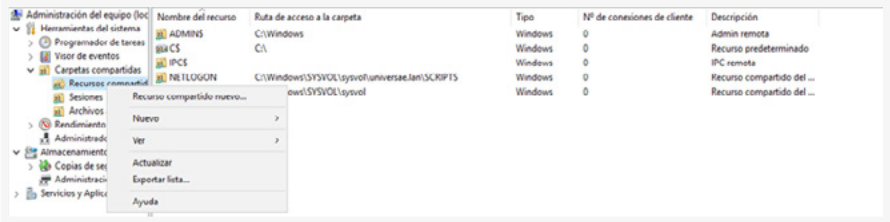

Imagen 10. Compartir directorios v2 1

4. En el cuadro que se nos abre, nos pide la ruta de la carpeta que se quiere compartir, ya sea poniéndola nosotros o buscando en el equipo.

5. Seleccionamos, por lo general, la opción Examinar y hacemos la búsqueda de la carpeta moviéndonos entre directorios.

6. Seleccionamos la carpeta y damos al siguiente paso.

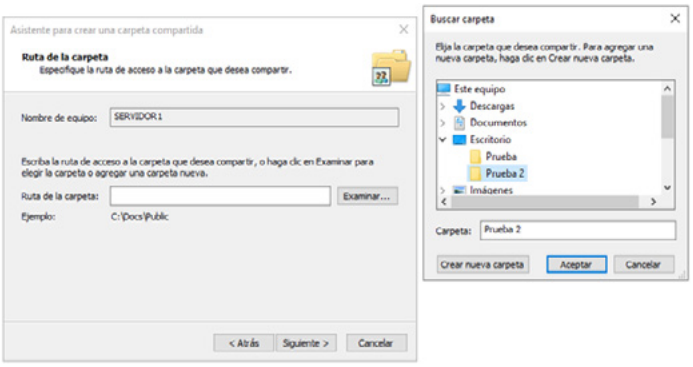

Imagen 11. Compartir directorios v2 2

7. Una vez que se ha seleccionado la carpeta, nos aparecerá un cuadro en el que pide varios datos que se pueden modificar, nosotros los dejamos por defecto.

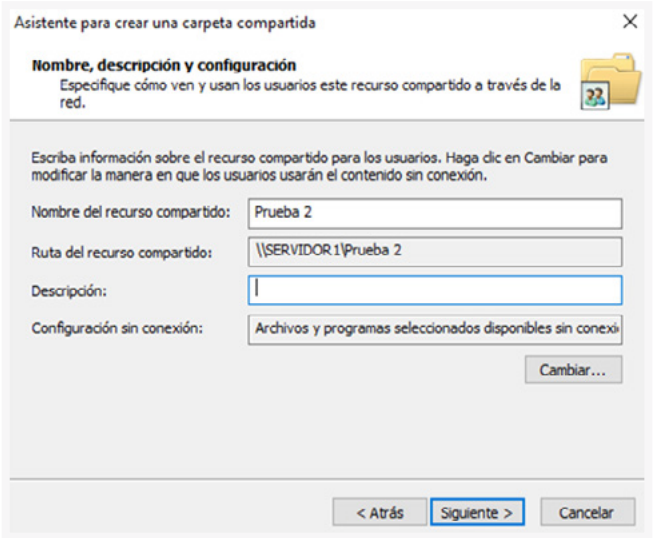

Imagen 12. Compartir directorios v2 3

8. Nos piden ahora que definamos cuales son en principio los permisos que tendrá este recurso, nosotros lo dejamos solo para administradores.

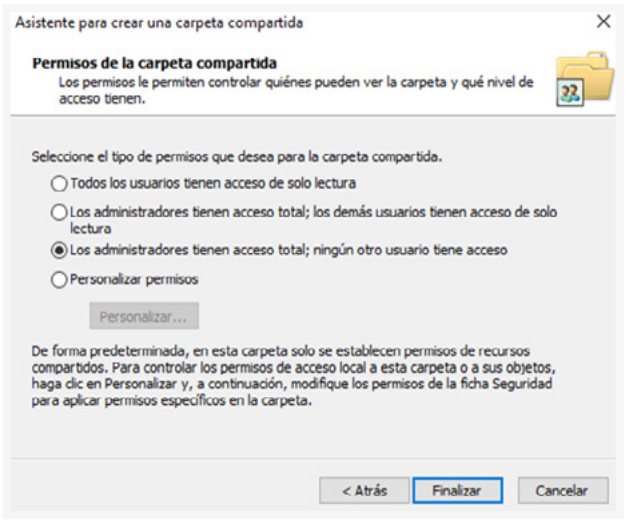

Imagen 13. Compartir directorios v2 4

9. Una vez que se ha creado el recurso, podemos ver que aparece en la lista de recursos compartidos,

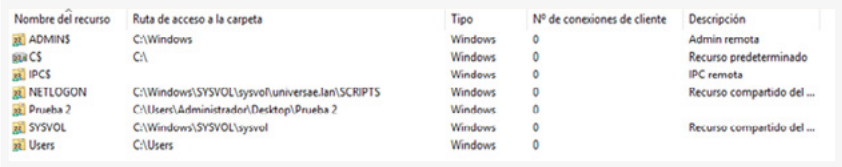

Imagen 14. Compartir directorios v2 5

Las capturas o imágenes que no se muestran, pero cuando realicemos el proceso se verán, se dejan por defecto

6.1.4. Herencia

Al principio del tema ya hicimos una pequeña introducción sobre lo que eran los permisos NTFS en sistemas Windows, pero ahora vamos a verlos en más profundidad.

Como recordaremos, estos permisos se basaban en la herencia de permisos para aplicar los mismos a todos los archivos y directorios que comprendiese el editado. Para realizar cambios en los permisos heredados, tenemos tres modos:

- Realizar cambios en la carpeta principal para que se cambien los heredados,
- Seleccionar la denegación de los permisos heredados en los archivos que así deseemos.
- Usar permisos explícitos que se contrapongan a los heredados.
- Deshabilitar la herencia. Para eso debemos de hacer lo siguiente:

1. Lo primero es abrir de nuevo las propiedades del recurso.
2. Ahora en la pestaña Seguridad, seleccionamos Opciones avanzadas.

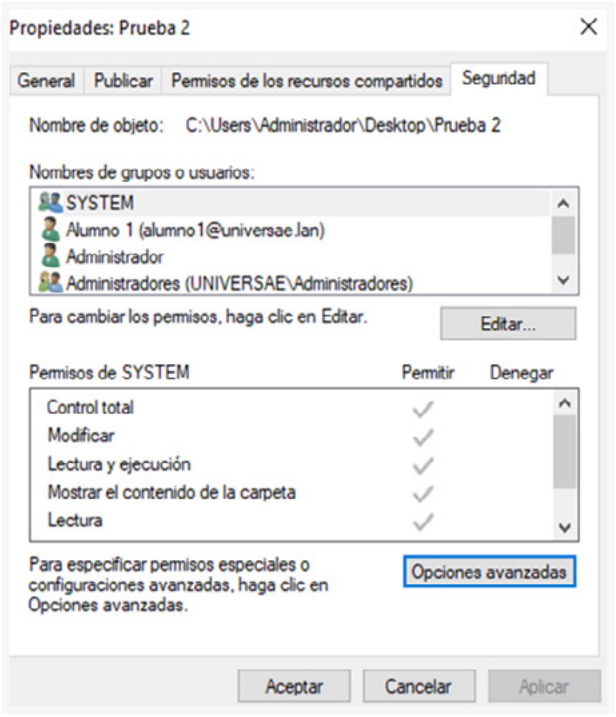

Imagen 15. Propiedades de seguridad

3. Una vez que lo hemos seleccionado, nos aparecerá una ventana para editar de manera más avanzada ciertos permisos.
4. Seleccionamos la opción Deshabilitar herencia y se nos dirá que queremos que hagamos con los permisos. Elegiremos opción dependiendo de cual nos interesa más.
5. Aplicamos y registramos los cambios.

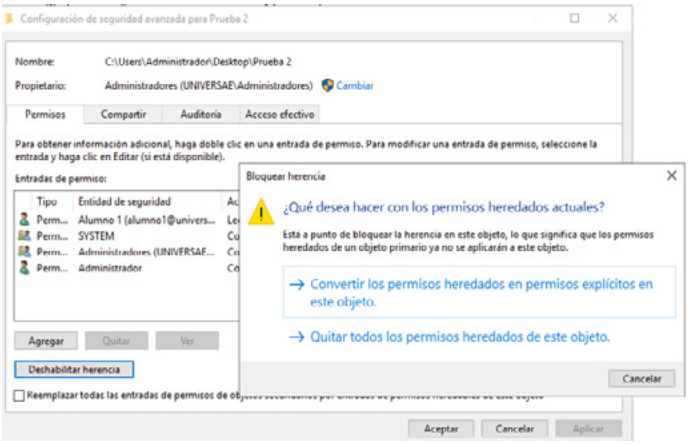

Imagen 16. Deshabilitar la herencia

6.1.5. ACL

En todos los sistemas Windows con archivos NTFS, cada uno de los archivos o directorios que tenemos posee los siguientes atributos de protección:

- El **SID del propietario:** se trata el usuario que en primera instancia creó el archivo o carpeta, pero puede que se haya modificado esto en algún momento.
- La **lista de control de acceso de protección (ACL):** aquí incluiremos los permisos que se usan para regular que usuarios pueden acceder o no a los recursos del sistema y que acciones pueden hacer sobre estos. No hay un número definido de entradas en esta lista. Esta a su vez se divide en dos listas de manera real que se llaman:
  - Lista de Control de Acceso Discrecional (DACL). Cada uno de sus elementos se llaman Entrada de control de Acceso (ACE) y se usa para unir un SID de una cuenta con la adjudicación de una serie de permisos.
  - Un archivo tiene dos DACL en vez de una debido a que en los sistemas Windows existe la herencia de permisos, es decir, permisos que se han concedido en carpetas superiores y que por defecto se aplican a todo lo que cuelgue de estas. Entonces, en una DACL tendremos los permisos heredados y en otra los permisos explícitos del archivo.
- **La lista de control de acceso de seguridad (SACL):** aquí se nos indicarán que acciones debe de auditar o registrar el sistema en caso de se hagan. (sobre el archivo o carpeta).

6.2. Derechos de usuarios

Como hemos mencionado anteriormente, los **derechos o privilegios** indican que acciones pueden o no realizar los usuarios que se encuentren iniciados en el sistema. Esta lista de derechos viene dada en el SAT, como se vio en el punto anterior.

En Windows existen principalmente dos tipos de derechos:

- **Derechos de conexión**, mediante los que se establecen las diferentes formas en las que un usuario puede acceder a un sistema. Destacan:
  - Denegar el acceso desde la red a este equipo. Si no está activo se permitirá que el usuario se pueda conectar con un equipo remoto a otro a través de la red.
  - Permitir el inicio de sesión local. Nos permite que se inicie sesión físicamente en el equipo en cuestión.
- Los **privilegios** (estos solo se pueden llamar así, no derechos también) mediante los cuales definimos el resto de las acciones que el usuario puede realizar dentro del sistema. Destacan (por ejemplo);
  - Añadir equipos a un dominio.
  - Realizar copias de seguridad del sistema de directorios.
  - Restaurar dichas copias de seguridad.
  - Cambiar la configuración del sistema.
  - Impedir la instalación de controladores de dispositivos.
  - Apagar el sistema.

Los derechos tienen prioridad sobre los permisos, es decir, si hay un conflicto, siempre se tendrán en cuenta los primeros.

6.2.1. Directivas de seguridad. Objetos y ámbito de directivas

Las **directivas de seguridad** en Windows son una serie de normas donde se refleja el comportamiento que debe de tener el equipo en lo referente a la seguridad.

Existen dos tipos principales:

- **Directivas de seguridad local**. Son las usadas cuando lo que tenemos es un equipo con sistema operativo Windows, pero no tienen un Directorio Activo instalado (Windows 10 o Windows Server sin AD). Los nodos de configuración son menores que en otros casos. Si queremos configurarlas, debemos de hacer lo siguiente:
  - Menú de Inicio → Herramientas administrativas → Directivas de seguridad local

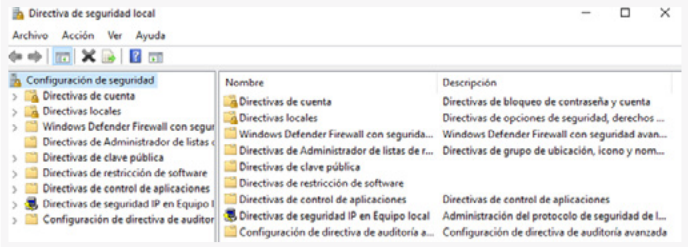

Imagen 17. Directivas de seguridad local

- **Directiva de seguridad de dominio.** Son las directivas que tenemos en un sistema Windows Server que tiene un Active Directory instalado, es decir, querer modificar la configuración de seguridad para los equipos dentro del dominio. Si queremos configurar estas directivas, debemos de hacer lo siguiente:
  - Inicio → Herramientas administrativas → Administración de directivas de grupo

Imagen 18. Administración de directivas de grupo

Dentro de estas últimas, además, tenemos las **directivas de seguridad del controlador de dominio**. Funcionan como las últimas en todo, pero en este caso, la configuración que se modifica es para otros controladores de dominio.

También albergan aquí directivas de seguridad para objetos del AD, como pueden ser las Unidades organizativas.

6.3. Servidores

Para poder realizar la compartición de recursos dentro de un sistema, estos deben lógicamente de alojarse en servidores dedicados expresamente a esta tarea. Lógicamente, estos servidores deben de contar con suficientes recursos como para poder funcionar fluidamente con todas las peticiones de acceso que van a recibir por parte de clientes.

Todo servidor debe de cumplir con los siguientes tres aspectos:

1. **Disponibilidad.** El servidor debe de estar encendido y accesible todo el tiempo prácticamente, pudiendo ser parado únicamente para tareas de mantenimiento preventivo.
2. **Escalabilidad.** El sistema debe de estar posibilitado a su crecimiento si aumenta la carga de trabajo.
3. **Mantenimiento.** Como mencionamos en el primer punto, es necesario llevar un mantenimiento preventivo del sistema para que no acarreen futuros problemas.

Dependiendo del tipo de recurso que se ofrece al cliente, el servidor a montar será de un tipo u otro. Hay multitud de tipos de servidores, pero nosotros nos vamos a basar en estos tres:

- Servidor de ficheros
- Servidor de impresión
- Servidor de aplicaciones

6.3.1. Servidor de ficheros

Un servidor de ficheros se instala con la intención de almacenar de manera segura y controlada los ficheros que se van a compartir con varios usuarios de un mismo sistema en red. Este tipo de servidor nos ayuda a tener centralizada la gestión de los permisos, de las copias de seguridad y de las demás propiedades de los ficheros almacenados.

El protocolo que se usa en estos servidores para la compartición de los ficheros es FTP, File Transfer Protocol de manera principal. También existen FTPS y SFTP que añaden una mayor seguridad al intercambio de datos.

Configuración de un servidor FTP en Windows

Si queremos habilitar un servicio de FTP en Microsoft Windows Server, debemos de realizar los siguientes pasos:

1. Lo primero que debemos es coger un servidor con un directorio activo previamente montado y funcionando.
2. Ahora, abrimos el centro de administración del servidor desde Herramientas administrativas en el Inicio.
3. Dentro del Administrador del servidor, en la esquina superior derecha, seleccionamos la opción Administrar.
4. Ahora hacemos clic sobre la primera opción, Agregar roles y características.

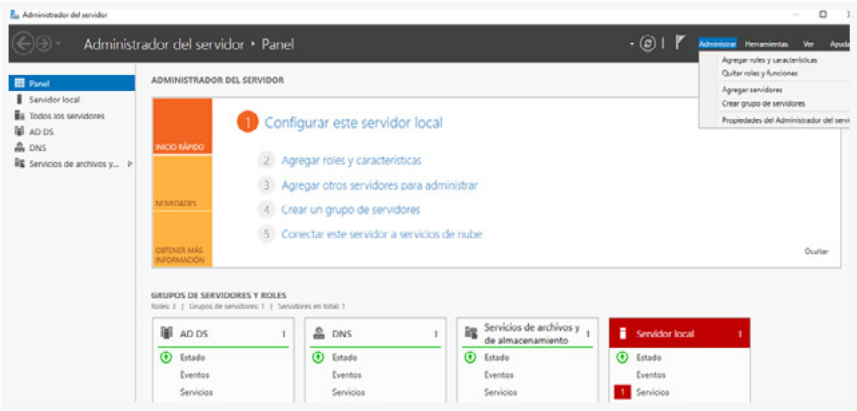

Imagen 19. FTP en Windows 1

5. Se nos abre el asistente de instalación de roles y características.

6. Damos a siguiente en la primera pantalla, y después seleccionamos la primera de las opciones de instalación.

Imagen 20. FTP en Windows 2

7. Una vez que se ha pasado de ventana, nos toca elegir servidor, y tendremos que hacerlo como en la imagen siguiente:

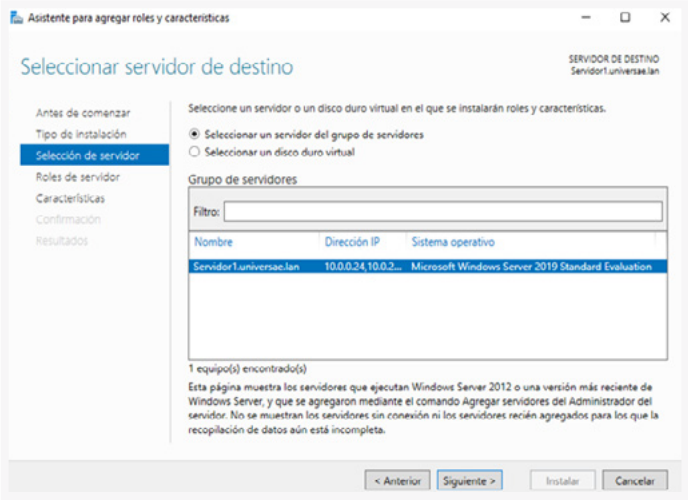

Imagen 21. FTP en Windows 3

8. Vamos ahora la pantalla de selección de roles, aquí seleccionamos Servidor web (IIS) como rol a instalar.

9. Se nos abre una ventana que nos indica si deseamos agregar las características asociadas al rol, decimos que sí.

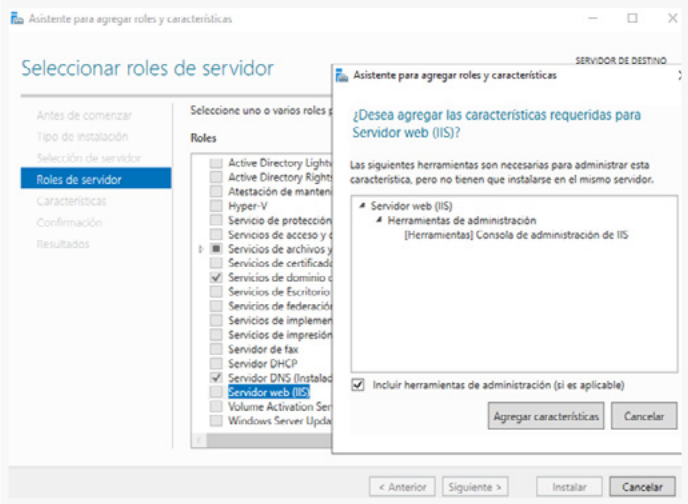

Imagen 22. FTP en Windows 4

10. Dejamos por defecto las demás opciones hasta que lleguemos a la pestaña Servicios de rol.

11. Aquí, seleccionamos el servicio Servidor FTP, con su subopción primera marcada también, para instalar el servicio.

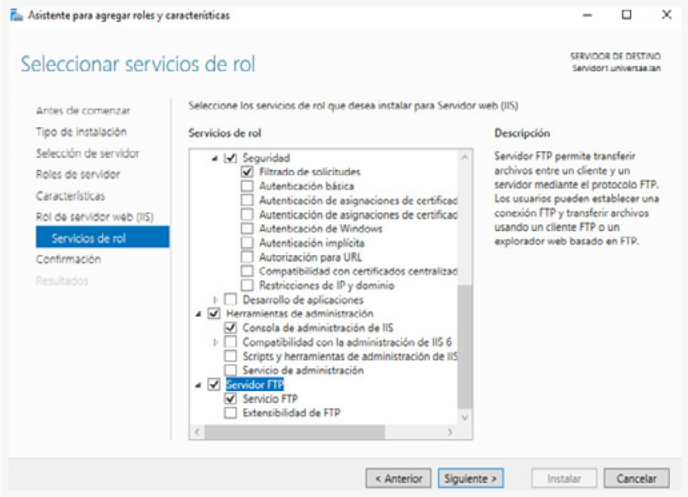

Imagen 23. FTP en Windows 5

12. Por último, lo que hacemos es confirmar la instalación y esperar a que termine.

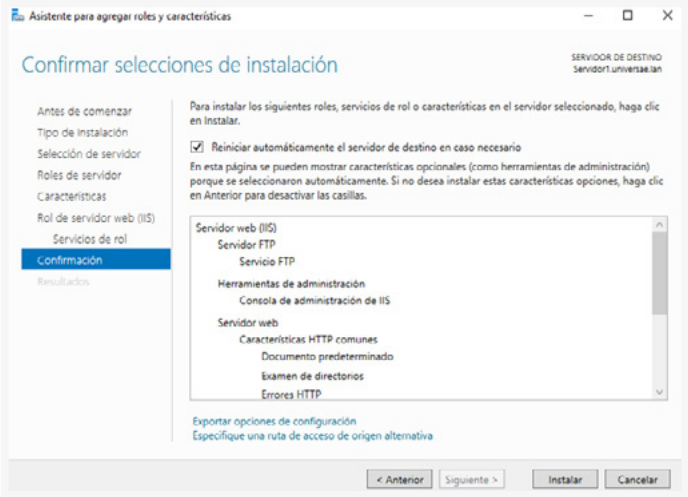

Imagen 24. FTP en Windows 6

13. Ahora vamos a crear un grupo para que los usuarios accedan al servidor de FTP.

14. Nos vamos a Herramientas y seleccionamos Centro de administración de Active Directory.

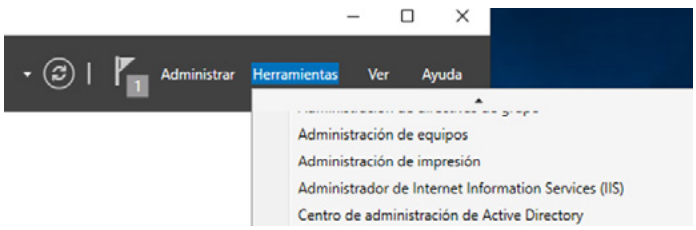

Imagen 25. FTP en Windows 7

15. En nuestro dominio, hacemos clic derecho y seguimos la siguiente selección:

    a. Nuevo

    b. Grupo

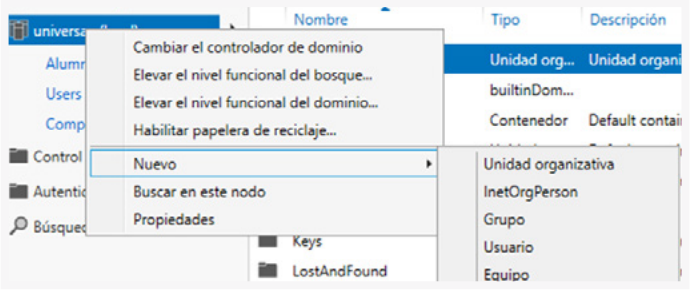

Imagen 26. FTP en Windows 8

16. Creamos un grupo para el acceso a los recursos de FTP.

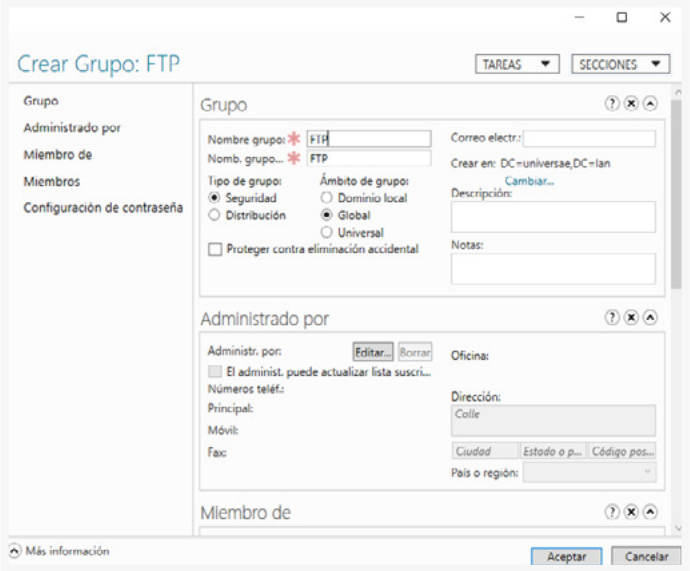

Imagen 27. FTP en Windows 9

17. Creamos ahora el directorio donde queremos que accedan.

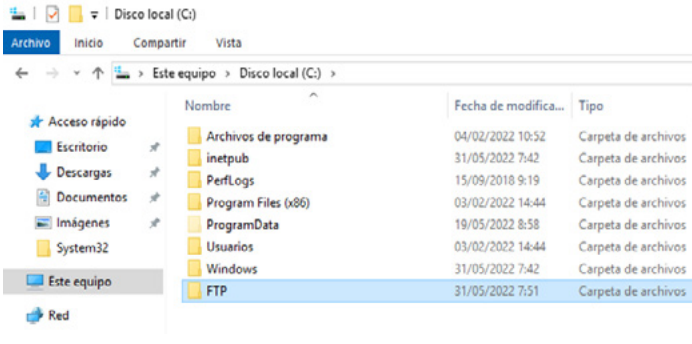

Imagen 28. FTP en Windows 10

18. De nuevo en el administrador del servidor, vamos a herramientas y seleccionamos Administrador de Internet Information Services (IIS), para configurar nuestro FTP.

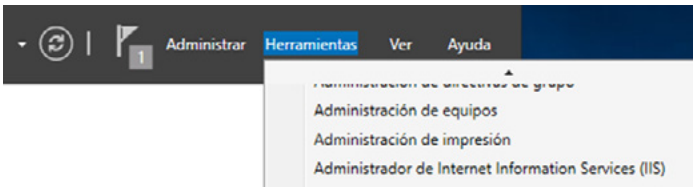

Imagen 29. FTP en Windows 11

19. Se abrirá una consola de configuración del servidor web.

20. En la parte izquierda, vemos un panel con el servidor, lo desplegamos.

21. Ahora tenemos una carpeta que pone Sitios, hacemos clic derecho sobre ella y seleccionamos Agregar sitio FTP...

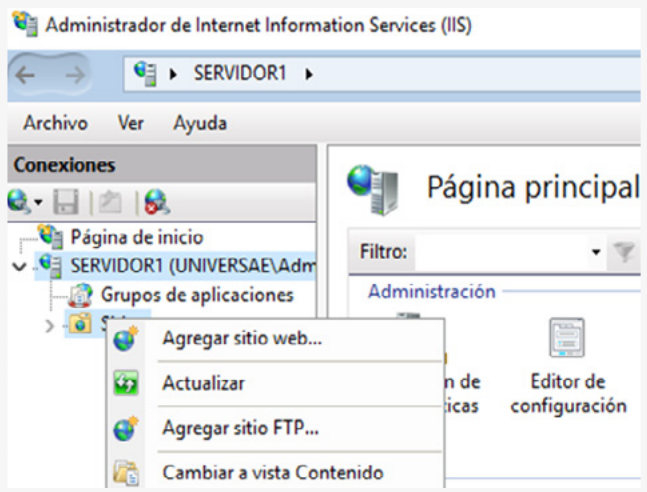

Imagen 30. FTP en Windows 12

22. En el asistente de agregación del sitio, debemos de indicar el nombre de sitio y la ruta del directorio al que queremos que se conecten los clientes del servicio, como en la siguiente imagen:

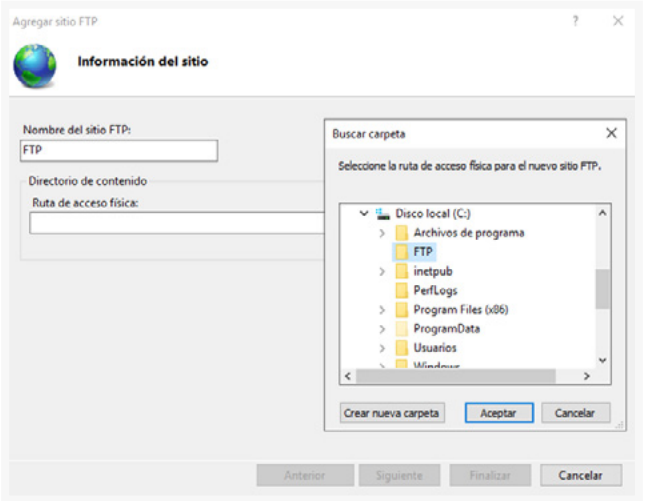

Imagen 31. FTP en Windows 13

23. Después, debemos de indicar que dirección queremos que tenga el servidor y el puerto de conexión, además de si la conexión va a ser mediante certificado SSL o no. Esto último es recomendable, pero en nuestro caso vamos a marcar que no debido a que no tenemos certificados instalados.

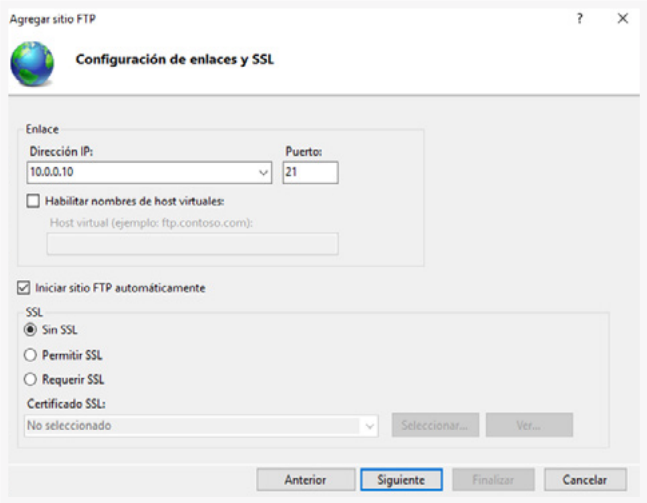

Imagen 32. FTP en Windows 14

24. Por último, debemos de indicar al servidor, que tipo de autenticación vamos a requerir, que suele ser Básica, que usuarios se pueden conectar, y que pueden realizar, si leer o modificar.

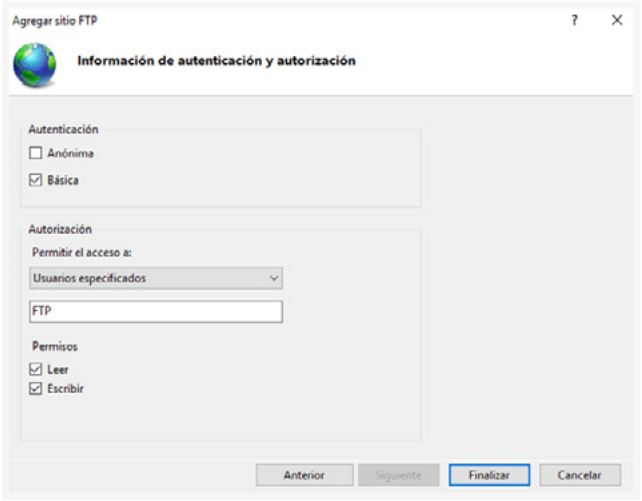

Imagen 33. FTP en Windows 15

Cliente FTP

Hay varios clientes de FTP, pero el más famoso es Filezilla.

Para poder conectarnos a un equipo remoto, debemos de activar en el Firewall de Windows el tráfico permitido para conexiones FTP por el puerto 21, pero esto no lo vamos a ver debido a que no es necesario en este punto.

Por último, saber que desde el mismo explorador de archivos podríamos conectarnos al servidor usando `ftp://Dirección_IP`.

6.3.2. Servidor de impresión

Normalmente, en una empresa, una impresora es uno de los servicios más demandados y usados, y es para esto para lo que se usan los servidores de impresión, para gestionar estas peticiones.

En estos servidores se alojan todas las conexiones con las impresoras y se distribuyen las cargas de trabajo entre las distintas impresoras, siempre que el usuario lo permita, claro está.

El modo de funcionamiento siempre es con las impresoras conectadas por red, igual que los clientes con el servidor. Dependiendo de la localización del servidor, tenemos dos tipos distintos:

- **Servidor externo:** el servidor se encuentra alojado fuera de las impresoras, conectándose por puertos a todas ellas.
- **Servidor interno:** algunas impresoras llevan incorporado un servidor de impresión

Hay servidores de impresión hardware propios que ya vienen montados solos y que llevan una guía de instalación, pero los sistemas Microsoft Windows Server pueden implementar el servicio de impresión.

Los pasos para dicha implementación son los siguientes:

1. Abrimos el administrador del servidor.
2. Seleccionamos la opción para agregar roles y características.
3. Damos a siguiente a todo hasta llegar a Roles de servidor.
4. Aquí, seleccionamos Servicios de impresión y documentos y agregamos sus características.

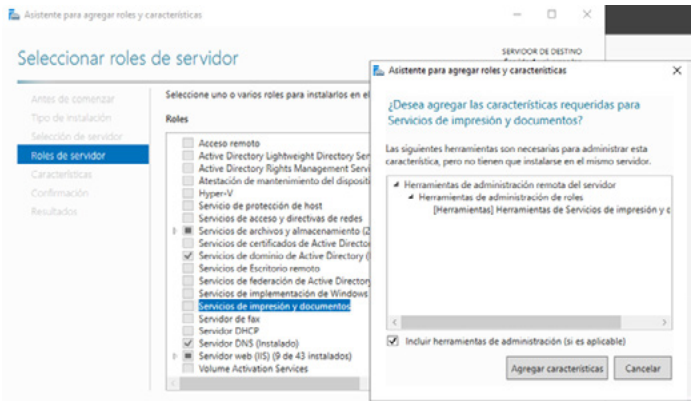

Imagen 34. Servidor de impresión en Windows 1

5. Todo lo demás se deja por defecto hasta que termine el asistente de instalación.
6. Ahora, en Herramientas, seleccionamos Administración de impresión.

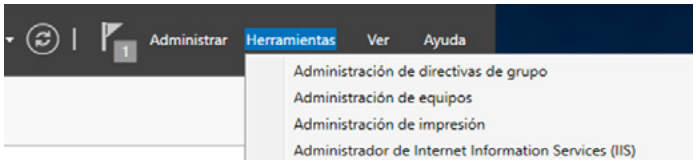

Imagen 35. Servidor de impresión en Windows 2

7. Se nos abre un cuadro de configuración con diversas opciones relacionadas con la impresión.
8. En el lateral izquierdo tenemos todas las opciones, pero nos interesa la siguiente concatenación:

   Administración de impresión → Servidores de impresión → Nuestro_servidor → Impresoras
9. En impresoras hacemos clic derecho, y elegimos Agregar impresora…
10. Aquí agregaríamos la impresora por el medio que deseemos, luego seleccionaríamos los controladores y ya estaría funcionando.

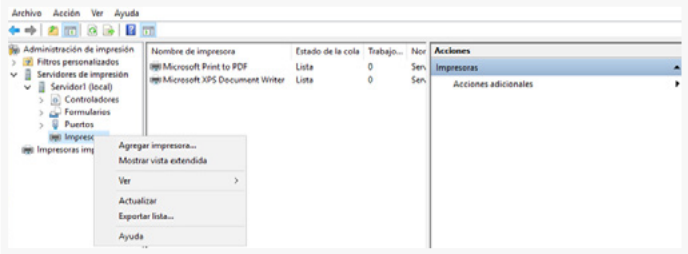

Imagen 36. Servidor de impresión en Windows 3

Clientes de impresión

Da igual de que tipo sea el servidor de impresión, la configuración desde el cliente siempre va a ser la misma en Microsoft Windows, y es la siguiente:

1. Abrimos el panel de control
2. Seleccionamos Hardware y sonido → Ver dispositivos e impresoras

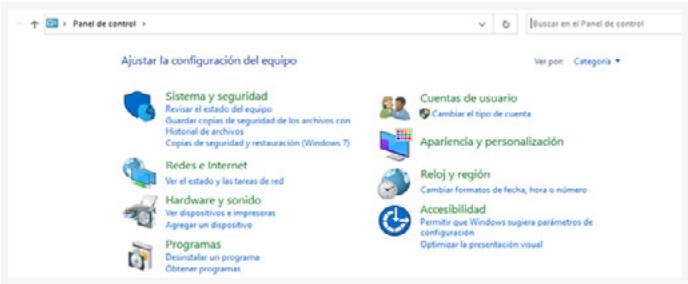

Imagen 37. Panel de control

3. Elegimos la opción Agregar una impresora

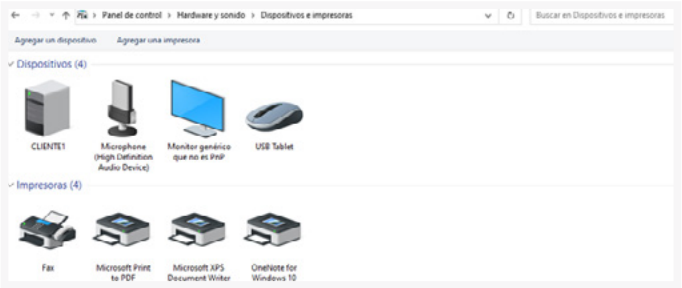

Imagen 38. Dispositivos e impresoras

4. En este punto hay dos vertientes, vamos a verlas:

   a. Si la impresora nos aparece de primeras, la seleccionamos, instalamos los controladores en caso de que no los lleve, y a funcionar.

   b. Si la impresora no nos aparece de primeras:

      + Seleccionamos la opción de más abajo que pone La impresora que quiero no está en la lista.

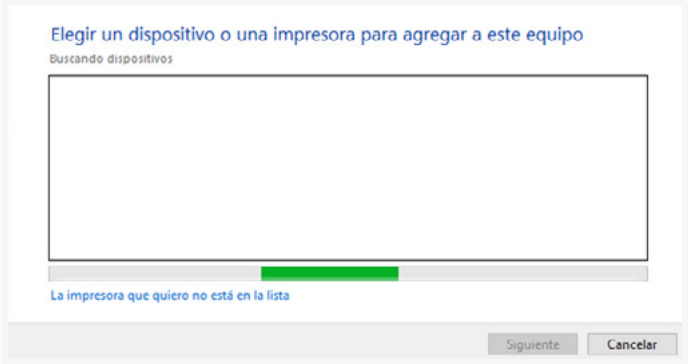

Imagen 39. Agregar impresoras en Windows 1

      + De nuevo, tenemos dos vertientes:

         › La primera es por nombre, donde, como podemos ver en la siguiente imagen, seleccionamos el nombre de la impresora usando el servidor también y después el mismo proceso que antes.

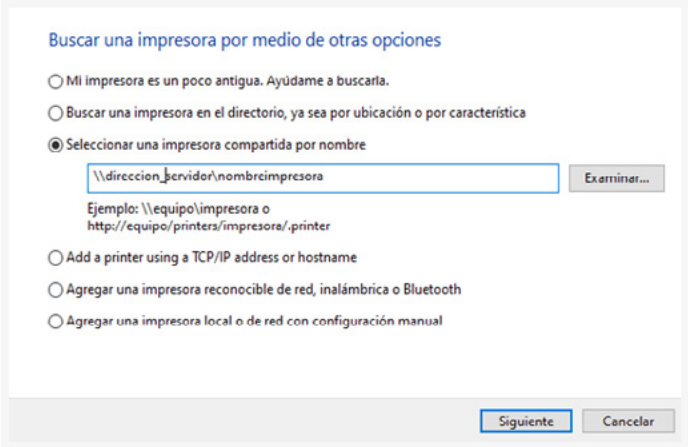

Imagen 40. Agregar impresoras en Windows 2

         › La otra opción es seleccionar agregar la impresora por dirección IP, la cual ponemos, y seguimos el mismo asistente de instalación de la impresora hasta que esta se encuentre funcionando.

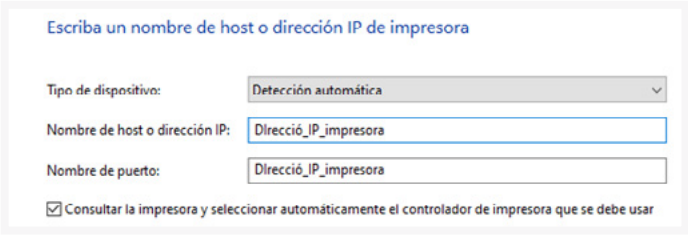

Imagen 41. Agregar impresoras en Windows 3

6.4. Conexión remota. Herramientas

El termino **administración remota** se dirige a la realización de acciones desde un equipo que nosotros manejamos, pero realmente se ejecutan en otro equipo al que no tenemos acceso físicamente.

Existen una gran variedad de programas para la administración remota, TeamViewer, Anydesk, VNC, etc. Con respecto a resto, Windows Server incorpora algunas herramientas nativas o utilidades que permiten las conexiones remotas. Son las tres siguientes:

- Servicios de escritorio remoto. Estos servicios permiten que lo usuarios se puedan conectar al servidor que se encuentra con este servicio activado de manera totalmente normal.
- Escritorios remotos. Es el cliente que se usa para la conexión a los servidores con los servicios de escritorio remoto activo. Hace falta un usuario y una contraseña real del servidor para poder conectarnos a este. Todo lo que hagamos se ejecutará en el servidor remoto, pues en nuestro equipo solo se ejecutará el asistente de conexión.
- Asistencia remota. Se ve el escritorio de los usuarios que estén conectados a un equipo en tiempo real con la intención de solventar los problemas que hayan podido suceder.

6.5. Herramientas de seguridad

6.5.1. Cifrado

Algoritmos simétricos o de clave privada

Reciben ese nombre porque utilizan la misma clave tanto para el cifrado como el descifrado del mismo.

Ambos receptor y emisor deben conocer la clave con el fin de poder tanto descifrarlo como cifrar el mensaje. Motivo por el cual conocemos este tipo de clave como clave privada.

Este algoritmo cuenta con la ventaja de la rapidez de su cálculo ya que cualquier ordenador actual cuenta con la capacidad de convertir el mensaje cifrado con mucha rapidez. El único inconveniente que presenta es la poca seguridad, porque es necesario transmitir la clave a través de la red, haciendo que esta sea vulnerable de manera casi instantánea.

Algoritmos asimétricos o de clave pública

Este tipo de algoritmos utilizan dos pares de claves (cuatro en total). Tanto el emisor como el receptor disponen de dos tipos de claves, una pública y otra privada. En este caso, solo comparten la clave pública.

En este caso, el cifrado es más seguro ya que para esto, se necesita la clave privada del emisor y la clave pública del receptor, y para descifrar el mensaje, es necesaria la clave privada del receptor y la clave pública del emisor.

El funcionamiento de este algoritmo sería de la siguiente manera:

- La pareja de claves (pública + privada) se genera a través de unas complicadas fórmulas matemáticas basadas en números primos. Aunque las dos claves tengan relación entre sí, es imposible averiguar la clave privada partiendo de la clave pública. Cuanto mayor sean esos números, mayor seguridad.
- Emisor y receptor deben intercambiar sus claves públicas. En este caso, con la tranquilidad de que alguien pueda interceptar la clave gracias a lo comentando anteriormente.
- El emisor combina el mensaje que desea enviar con su clave privada y la clave pública del receptor. Por el contrario, el receptor utiliza la otra pareja de claves para descifrar.

Es el algoritmo más adecuado para las transmisiones de datos por internet, aunque presenta un inconveniente: el cifrado asimétrico es lento.

Principales algoritmos de cifrado

La robustez o fortaleza de estos algoritmos ya sean simétricos o asimétricos, se basa en la longitud (expresada en bits) de la clave. Entre los que se encuentran los siguientes.

SIMÉTRICOS:

- **DES.** Clave de 52 bits. Es vulnerable y se puede romper la clave en un plazo de 24 horas.
- **TDES.** 192 bits. Equivale a aplicar 3 veces el algoritmo anterior.
- **RC2.** Varía entre 62 y 128 bits. Hasta 3 veces más rápido que DES y mucho más seguro
- **ICE.** Su longitud se basa en un múltiplo de 64.
- **IDEA.** Clave de 128 bits. Considerado como uno de los algoritmos más seguros actualmente.
- **AES.** Contempla claves de 128, 192 o 256 bits. Es el más utilizado actualmente.
- **Blowfish.** Claves entre 32 y 448 bits. Muy seguro, aunque lento.

ASIMÉTRICOS:

- **RSA.** Clave de 128, 256, 1024 o 2048. Ampliamente utilizado
- **DSA.** Claves entre 1024 y 3072 bits. Creado para el uso de firmas digitales, aunque está en constante desarrollo para mejorar su nivel de protección.
- **ECC.** Ofreciendo el mismo rendimiento que los anteriores con claves equivalentes, pero más cortas.

Cifrado híbrido

Consiste en utilizar un algoritmo asimétrico para intercambiar una clave de cifrado simétrico. En este caso, si algún usuario intercepta el mensaje, solamente le serviría para descifrar ese mensaje en concreto ya que el resto de los mensajes utiliza otra clave (en este caso aleatoria).

6.5.2. Cortafuegos

Es una de las medidas de seguridad más importantes a la hora de configurar una red LAN conectada a internet. Analiza todos los paquetes de datos que entran y salen por sus interfaces y, apoyándose en un conjunto de reglas, determinan de qué manera actuar con cada uno de ellos, es decir, aceptando o rechazando el mensaje.

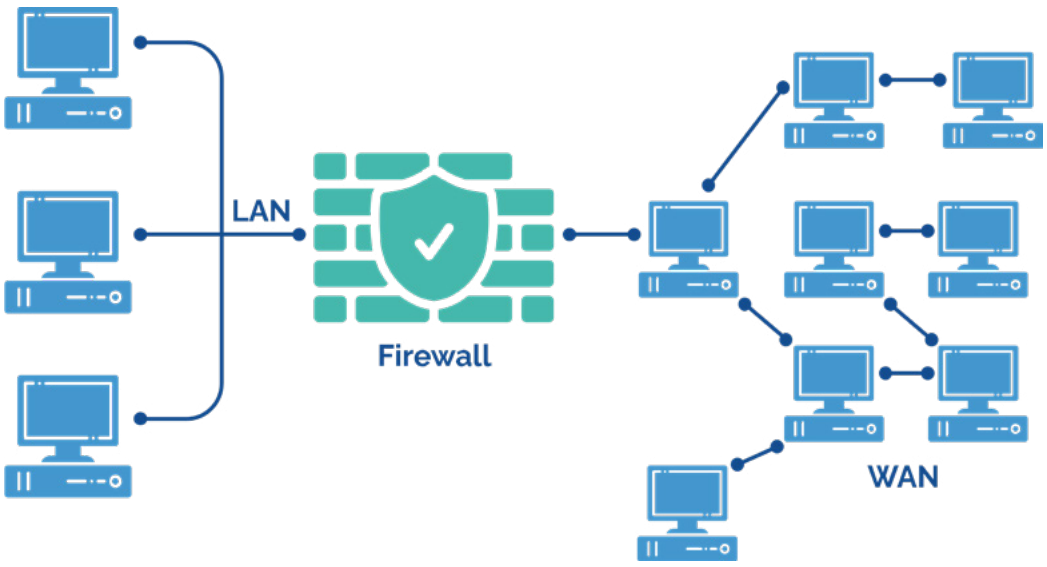

Imagen 42 Reglas presentes en una red LAN. El firewall suele representar como un símbolo de un muro

Los routers contienen un cortafuegos en su interior, por lo que podrían considerase como cortafuegos hardware. La diferencia entre uno y otro reside en que el software necesario (firmware), permita al administrador a crear un conjunto de reglas de filtrado.

Por ejemplo, los routers domésticos proporcionan un conjunto de reglas muy reducido preestablecido por el cortafuegos, aparte de la redirección de puertos.

Los cortafuegos en este tipo de dispositivos deben preocuparse únicamente de los paquetes de datos que reciben (INPUT), y los que generan ellos mismos (OUTPUT), y los más importantes, los que pasan a través de ellos (FORWARD).

Así mismo, todos los sistemas operativos incorporan su propio cortafuegos software, el cual controla las conexiones entrantes y salientes. Desde la versión 8 de Windows, se permite definir reglas según puerto, aplicaciones que van a recibir las conexiones, etc. Los sistemas Linux, en cambio, incorporan un cortafuegos orientado únicamente a los paquetes que entran y salen por las interfaces de red. Es muy potente, pero difícil de configurar, ya que se debe hacer mediante líneas de comandos.

En el caso de los cortafuegos hardware, se pone a disposición del usuario un sistema operativo interno para poder instalarlo en equipos PC, brindando la posibilidad de crear un cortafuegos software. Como es el caso de Mikrotik. Al igual que este, existen también cortafuegos open source basados en Linux/UNIX, como pfSense.

Un cortafuegos sirve para detener conexiones de red no deseadas. No se debe pensar que un cortafuegos protege contra todas las amenazas que hemos descrito anteriormente por varios motivos:

Si se abre un puerto específico, ya hay un canal por el cual recibir ataques. Esto implica que se deben tomar medidas adicionales para proteger los ataques destinados a ese puerto en concreto.

Contiene un número limitado de reglas que protegen ante cierto número de atacantes, dicho de otra manera, estará indefenso ante otros tipos de ataques no contemplados en esas reglas. Por eso, la administración es la encargada de actualizar dichas reglas.

Algunos ataques, como el conocido DoS (denegación de servicio) es imposible de evitar, aunque según las medidas de seguridad incorporadas, ayudan a mitigar sus efectos.

Para terminar, podemos decir que un cortafuegos es una medida de protección más, aunque podemos afirmar que estamos ante una de las medidas más importantes porque reduce la superficie de ataque de la red local.

www.universae.com