

IES Valle Inclán



FTP linux y windows

Carlos González Martín

Contenido

1.	Cambiamos el nombre a la maquina	3
2.	Instalamos paquetes	3
3.	Cambiamos la red	4
4.	Comprobación básica.....	5
5.	Securización.....	6
6.	Comprobaciones	7
7.	DNS	8
8.	Comprobaciones con dns en linux	9
9.	FTP windows server	10
10.	Comprobaciones windows	30
11.	Otros programas	32
12.	Conclusión.....	41

1. Cambiamos el nombre a la maquina

Para empezar, lo que haremos será cambiar el nombre a la máquina, para que sea más fácil identificar la máquina.

```
root@debian-12:~# hostnamectl set-hostname FTP
root@debian-12:~#
```

Cerramos sesión y al iniciar sesión nos saldrá el nombre de la máquina.

```
root@FTP:~#
root@FTP:~#
root@FTP:~#
root@FTP:~#
root@FTP:~#
root@FTP:~#
root@FTP:~#
root@FTP:~#
root@FTP:~#
```

Suelen haber problemas con el dns propio de la máquina virtual, por eso modificamos el archivo hosts.

```
GNU nano 7.2 /etc/hosts *
1 127.0.0.1    localhost
2 127.0.1.1    FTP      debian-12
3
4 # The following lines are desirable for IPv6 capable hosts
5 ::1          localhost ip6-localhost ip6-loopback
6 ff02::1      ip6-allnodes
7 ff02::2      ip6-allrouters
8
```

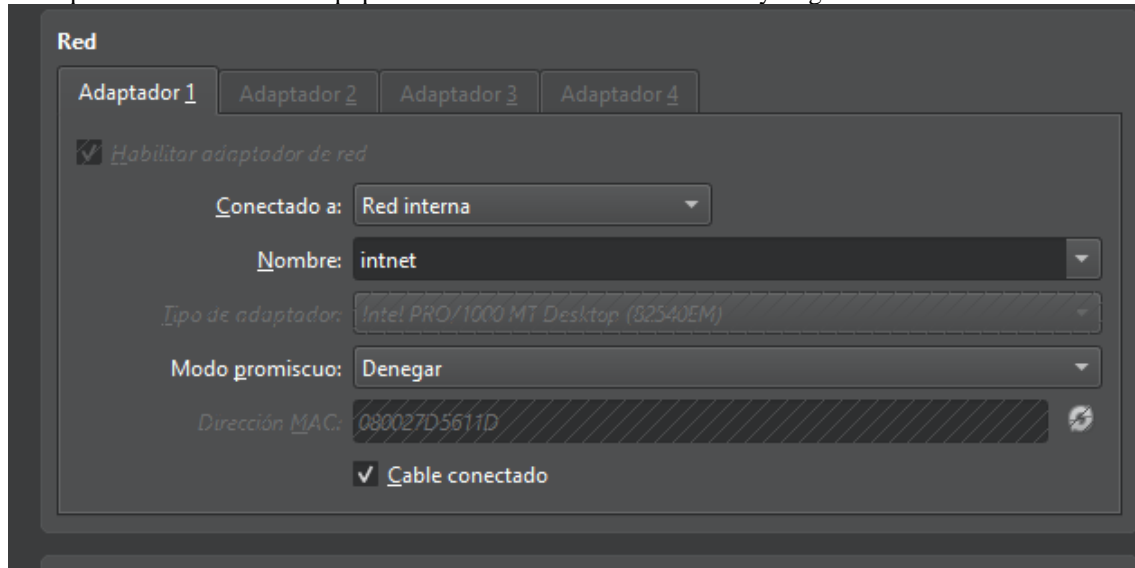
2. Instalamos paquetes

Ahora lo que haremos será instalar el paquete vsftpd.

```
root@FTP:~# apt update ; apt install vsftpd -y
Obj:1 http://security.debian.org/debian-security bookworm-security InRelease
Obj:2 http://deb.debian.org/debian bookworm InRelease
Obj:3 http://deb.debian.org/debian bookworm-updates InRelease
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se pueden actualizar 45 paquetes. Ejecute «apt list --upgradable» para verlos.
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
vsftpd ya está en su versión más reciente (3.0.3-13+b2).
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 45 no actualizados.
root@FTP:~# _
```

3. Cambiamos la red

Para que nos interfiera otros equipos de la red usaremos la red interna y asignaremos IPs.



Una vez que lo tenemos en red interna nos iremos al /etc/network/interfaces.

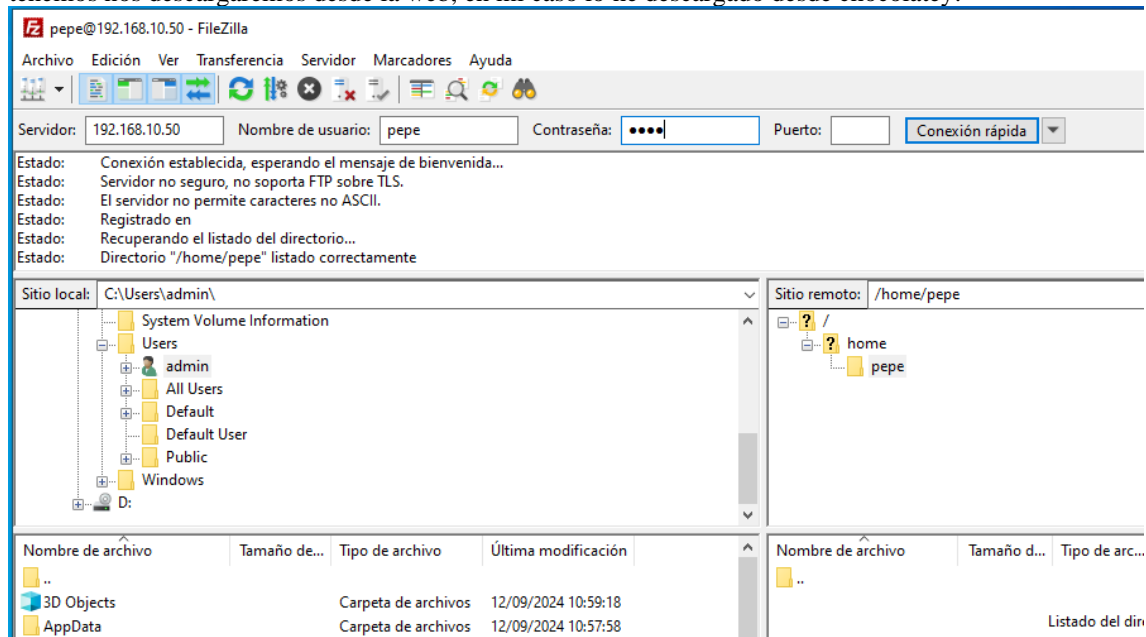
```
GNU nano 7.2 /etc/network/interfaces
1 # This file describes the network interfaces available on your system
2 # and how to activate them. For more information, see interfaces(5).
3
4 source /etc/network/interfaces.d/*
5
6 # The loopback network interface
7 auto lo
8 iface lo inet loopback
9
10 # The primary network interface
11 allow-hotplug enp0s3
12 #iface enp0s3 inet dhcp
13 iface enp0s3 inet static
14     address 192.168.10.50
15     netmask 255.255.255.0
16
```

4. Comprobación básica

Crearemos un usuario llamado pepe y probaremos si funciona la conexión, podemos usar otros usuarios del sistema, pero es mejor que creamos uno nuevo.

```
root@FTP:~# adduser pepe
Añadiendo el usuario 'pepe' ...
Añadiendo el nuevo grupo 'pepe' (1001) ...
Adding new user 'pepe' (1001) with group 'pepe (1001)' ...
Creando el directorio personal '/home/pepe' ...
Copiando los ficheros desde '/etc/skel' ...
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
passwd: contraseña actualizada correctamente
Cambiano la información de usuario para pepe
Introduzca el nuevo valor, o pulse INTRO para usar el valor predeterminado
Nombre completo []:
Número de habitación []:
Teléfono del trabajo []:
Teléfono de casa []:
Otro []:
¿Es correcta la información? [S/n] S
Adding new user 'pepe' to supplemental / extra groups 'users' ...
Añadiendo al usuario 'pepe' al grupo 'users' ...
root@FTP:~#
```

Ahora en un windows 10 en red interna con distinta IP, nos conectaremos mediante FileZilla, si no lo tenemos nos descargaremos desde la web, en mi caso lo he descargado desde chocolatey.



5. Securitización

Ahora vamos a habilitar la escritura y que solo un usuario pueda acceder al sistema, y evitar posibles hackeos.

Nos iremos a `/etc/vsftpd.conf` y escribiremos lo siguiente.

```
165 #####
166 #
167 #     PERSONAL CONFIG     #
168 #
169 #####
170 chroot_local_user=YES
171 allow_writeable_chroot=YES
172 anonymous_enable=NO
173 write_enable=YES
174 userlist_enable=YES
175 userlist_file=/etc/vsftpd.userlist
176 userlist_deny=NO
177
178
179
180
```

Le indicaremos que solo puede acceder el usuario pepe con el usuario userlist file.

```
GNU nano 7.2 /etc/vsftpd.userlist
1 pepe
2
```

Cambiamos el directorio de trabajo de pepe y crearemos una carpeta en la raíz.

```
dic 10 20:57:28 FTP systemd[1]: Starting vsftpd.service - vsftpd FTP server...
dic 10 20:57:28 FTP systemd[1]: Started vsftpd.service - vsftpd FTP server.
root@FTP:~# mkdir /pepe
root@FTP:~# nano /etc/passwd
```

Ahora nos iremos al `/etc/passwd` y cambiamos el directorio de trabajo de pepe.

```

GNU nano 7.2 /etc/passwd
1 root:x:0:0:root:/root:/bin/bash
2 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
3 bin:x:2:2:bin:/bin:/usr/sbin/nologin
4 sys:x:3:3:sys:/dev:/usr/sbin/nologin
5 sync:x:4:65534:sync:/bin:/bin/sync
6 games:x:5:60:games:/usr/games:/usr/sbin/nologin
7 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
8 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
9 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
10 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
11 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
12 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
13 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
14 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
15 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
16 irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
17 _apt:x:42:65534::/nonexistent:/usr/sbin/nologin
18 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
19 systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
20 usuario:x:1000:1000:usuario,,,:/home/usuario:/bin/bash
21 messagebus:x:100:107::/nonexistent:/usr/sbin/nologin
22 vboxadd:x:997:1::/var/run/vboxadd:/bin/false
23 ftp:x:101:109:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
24 pepe:x:1001:1001::,/pepe:/bin/bash
25

```

Ahora añadimos al usuario pepe y al grupo pepe en la carpeta raíz.

```

root@FTP:/# chown pepe:pepe /pepe
root@FTP:/#

```

6. Comprobaciones

Ahora vamos a comprobar que podemos subir archivos.

The screenshot shows the FileZilla interface with the following details:

- Server:** 192.168.10.50, **Username:** pepe, **Password:** [masked], **Port:** [empty], **Connection:** Conexión rápida.
- Status Log:**
 - Estado: Comenzando la subida de C:\Users\admin\Desktop\esto es una prueba de pepe.txt
 - Estado: Transferencia correcta, transferidos 0 bytes en 1 segundo
 - Estado: Recuperando el listado del directorio "/trabajos"...
 - Estado: Calculando compensación de la zona horaria del servidor...
 - Estado: Timezone offset of server is 0 seconds.
 - Estado: Directorio "/trabajos" listado correctamente
- Local Site:** C:\Users\admin\
 - ProgramData
 - Recovery
 - System Volume Information
 - Users
 - admin
 - All Users
 - Default
 - Default User
 - Public
 - Windows
- Remote Site:** /trabajos
 - trabajos
- File List:**

Nombre de archivo	Tamaño de...	Tipo de archivo	Última modificación
..		Carpeta de archivos	12/09/2024 10:59:18
3D Objects		Carpeta de archivos	12/09/2024 10:57:50
AppData		Carpeta de archivos	12/09/2024 10:57:50

Nombre de archivo	Tamaño d...	Tipo de arc...	Última modific...	Permis...
..				
esto es una prueba de pepe.txt	0	Document...	10/12/2024 22:...	-rw----

7. DNS

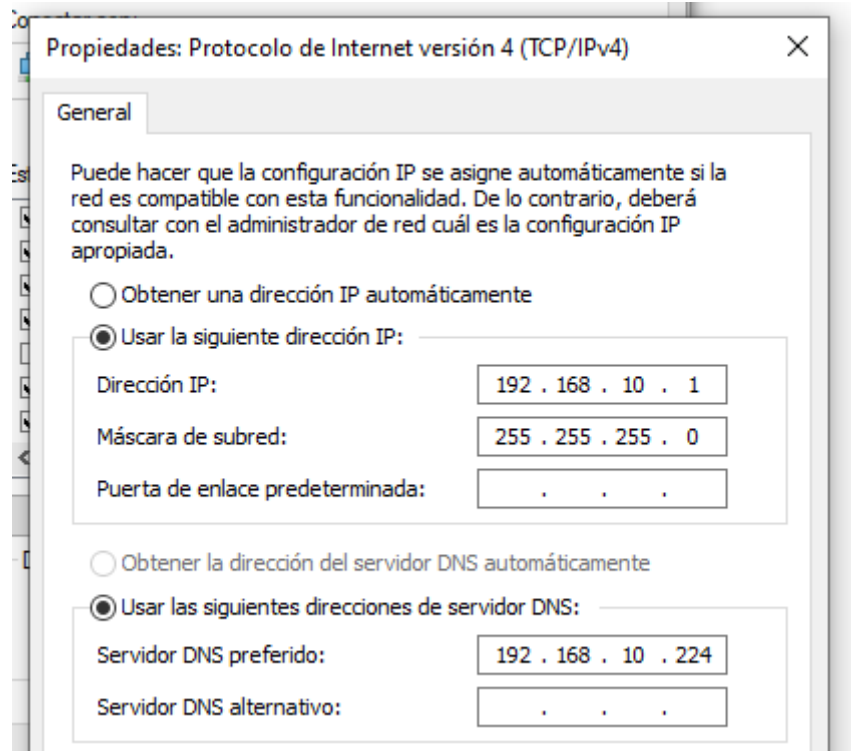
Ahora vamos a crear un DNS en linux, en la práctica anterior lo hicimos, asique voy a obviar las IPs de la maquina o algunos archivos de configuración, pero los archivos de los registros son los importantes.

```
GNU nano 7.2 db.asir.com
1 ;
2 ; BIND data file for local loopback interface
3 ;
4 $TTL 604800
5 @ IN SOA dns.asir.com. root.asir.com. (
6     2      ; Serial
7     60     ; Refresh
8     86     ; Retry
9     24     ; Expire
10    60 )   ; Negative Cache TTL
11 ;
12 @ IN NS  dns.asir.com.
13
14 dns IN A  192.168.10.224
15 ftp IN A  192.168.10.50
16 ftp2 IN A 192.168.10.60
17 cliente IN A 192.168.10.1
18
```

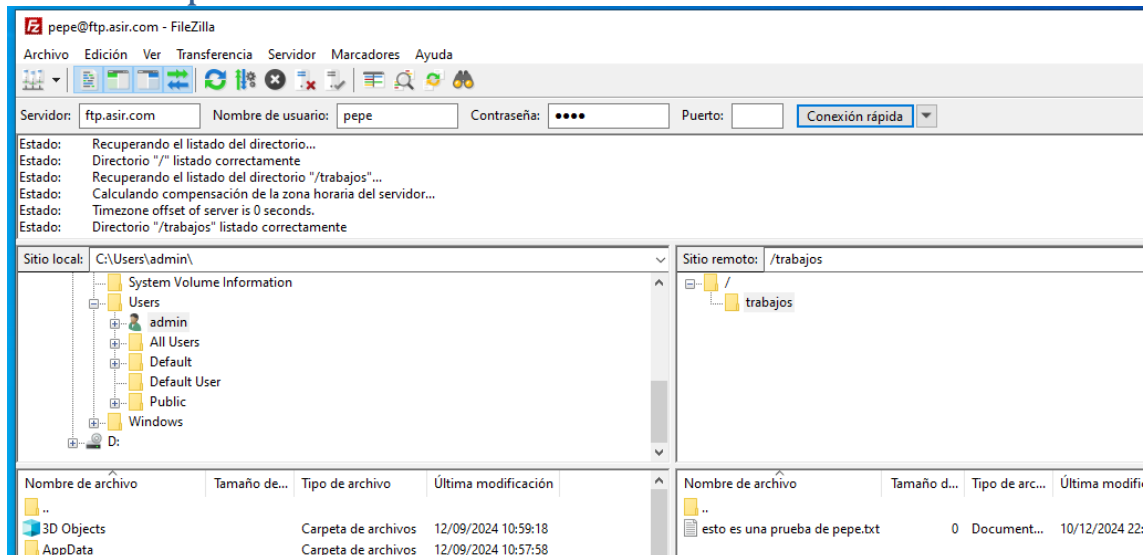
Ahora vamos a ver el archivo de zona inversa.

```
GNU nano 7.2 db.192.168.10
1 ;
2 ; BIND reverse data file for broadcast zone
3 ;
4 $TTL 604800
5 @ IN SOA dns.asir.com. root.asir.com. (
6     1      ; Serial
7     60     ; Refresh
8     86     ; Retry
9     24     ; Expire
10    60 )   ; Negative Cache TTL
11 ;
12 @ IN NS  dns.asir.com.
13
14 224 IN PTR dns.asir.com.
15 50  IN PTR ftp.asir.com.
16 60  IN PTR ftp2.asir.com.
17 1   IN PTR cliente.asir.com.
18
```


Ahora vamos a cambiar en las maquinas el dns preferido, ya que vamos a apuntar a una maquina distinta a la que normalmente es.



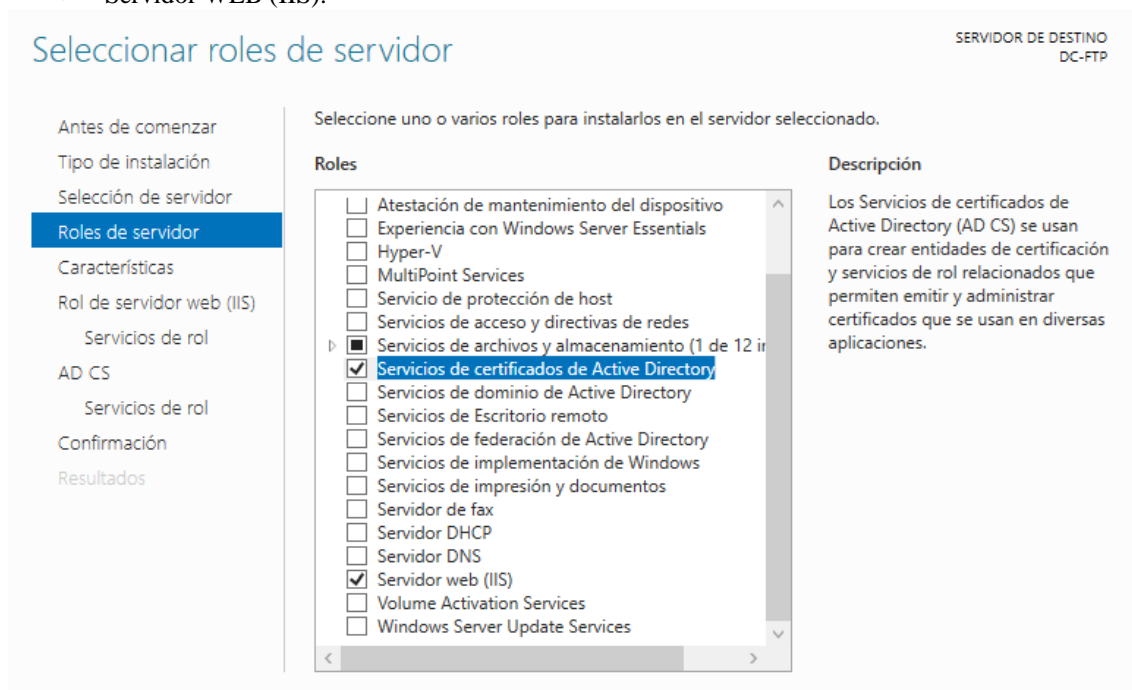
8. Comprobaciones con dns en linux



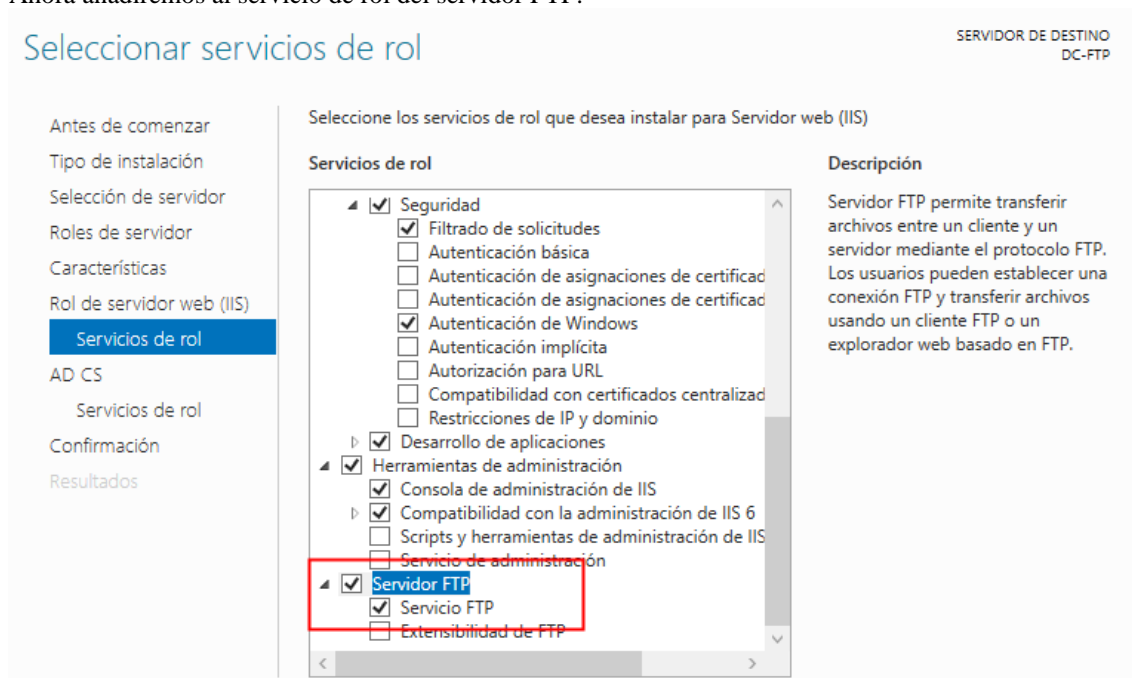
9. FTP windows server

Lo que haremos será seleccionar los siguientes roles.

- Servicio de certificados de active directory.
- Servidor WEB (IIS).



Ahora añadiremos al servicio de rol del servidor FTP.



Luego en servicio de certificados de active directory y le daremos a inscripción web de entidad de certificación.

Seleccionar servicios de rol

SERVIDOR DE DESTINO
DC-FTP

Antes de comenzar
Tipo de instalación
Selección de servidor
Roles de servidor
Características
Rol de servidor web (IIS)
Servicios de rol
AD CS
Servicios de rol
Confirmación
Resultados

Seleccione los servicios de rol que desea instalar para Servicios de certificados de Active Directory

Servicios de rol	Descripción
<input checked="" type="checkbox"/> Entidad de certificación	
<input checked="" type="checkbox"/> Inscripción web de entidad de certificación	Inscripción web de entidad de certificación proporciona una interfaz web sencilla que permite a los usuarios realizar tareas como solicitar y renovar certificados, recuperar listas de revocación de certificados (CRL) e inscribirse para certificados de tarjeta inteligente.
<input type="checkbox"/> Respondedor en línea	
<input type="checkbox"/> Servicio de inscripción de dispositivos de red	
<input type="checkbox"/> Servicio web de directiva de inscripción de certificado	
<input type="checkbox"/> Servicio web de inscripción de certificados	

Le daremos a instalar y cuando complete la instalación le daremos a “configurar servicios de certificados de Active directory en el servidor de destino”.

Progreso de la instalación

SERVIDOR DE DESTINO
DC-FTP

Antes de comenzar
Tipo de instalación
Selección de servidor
Roles de servidor
Características
Rol de servidor web (IIS)
Servicios de rol
AD CS
Servicios de rol
Confirmación
Resultados

Ver progreso de la instalación

Instalación de característica

Requiere configuración. Instalación correcta en DC-FTP.

Servicios de certificados de Active Directory
Se requieren pasos adicionales para configurar Servicios de certificados de Active Directory en el servidor de destino.

Configurar Servicios de certificados de Active Directory en el servidor de destino

Entidad de certificación
Inscripción web de entidad de certificación
Herramientas de administración remota del servidor
Herramientas de administración de roles
Herramientas de Servicios de certificados de Active Directory

Nos saldrá la siguiente ventana.

Credenciales

SERVIDOR DE DESTINO
DC-FTP

Credenciales
Servicios de rol
Confirmación
Progreso
Resultados

Especifique las credenciales para configurar servicios de rol

Para instalar los servicios de rol siguientes, debe pertenecer al grupo Administradores local:

- Entidad de certificación independiente
- Inscripción web de entidad de certificación
- Respondedor en línea

Para instalar los servicios de rol siguientes, debe pertenecer al grupo Administradores de organización:

- Entidad de certificación empresarial
- Servicio web de directiva de inscripción de certificados
- Servicio web de inscripción de certificados
- Servicio de inscripción de dispositivos de red

Credenciales:

Una vez que le demos a siguiente nos saldrá servicios de rol y seleccionaremos los servicios que se configuraran.

SERVIDOR DE DESTINO
DC-FTP

Servicios de rol

Credenciales

Servicios de rol

Tipo de instalación

Tipo de CA

Clave privada

Criptografía

Nombre de CA

Período de validez

Base de datos de certifica...

Seleccionar los servicios de rol que se configurarán

- ☒ Entidad de certificación
- ☒ Inscripción web de entidad de certificación
- ☐ Respondedor en línea
- ☐ Servicio de inscripción de dispositivos de red
- ☐ Servicio web de inscripción de certificados
- ☐ Servicio web de directiva de inscripción de certificados

Le daremos a siguiente y nos preguntara el tipo de instalación de la entidad de certificación.

SERVIDOR DE DESTINO
DC-FTP

Tipo de instalación

Credenciales

Servicios de rol

Tipo de instalación

Tipo de CA

Clave privada

Criptografía

Nombre de CA

Período de validez

Base de datos de certifica...

Confirmación

Progreso

Especifique el tipo de instalación de la CA

Las entidades de certificación (CA) empresariales pueden usar Servicios de dominio de Active Directory (AD DS) para simplificar la administración de los certificados. Las CA independientes no usan AD DS para emitir ni administrar certificados.

- ☐ CA empresarial
Las CA empresariales deben pertenecer al dominio y normalmente están en línea para emitir certificados o directivas de certificados.
- ☒ CA independiente
Las CA independientes pueden pertenecer a un grupo de trabajo o a un dominio. No requieren AD DS y se pueden usar sin conexión a la red (sin conexión).

Luego nos indicara el tipo de certificación.

SERVIDOR DE DESTINO
DC-FTP

Tipo de CA

Credenciales

Servicios de rol

Tipo de instalación

Tipo de CA

Clave privada

Criptografía

Nombre de CA

Período de validez

Base de datos de certifica...

Confirmación

Especifique el tipo de CA

Al instalar Servicios de certificados de Active Directory (AD CS), crea o amplía una jerarquía de infraestructura de clave pública (PKI). Se sitúa una CA raíz en la parte superior de la jerarquía de PKI, que emite su propio certificado autofirmado. Una CA subordinada recibe un certificado de la CA inmediatamente superior en la jerarquía de PKI.

- ☒ CA raíz
Las CA raíz son las primeras y puede que las únicas configuradas en una jerarquía de PKI.
- ☐ CA subordinada
Las CA subordinadas requieren una jerarquía de PKI establecida y están autorizadas a emitir certificados de la CA inmediatamente superior en la jerarquía.

Ahora le indicaremos si queremos usar una clave privada o la crearemos.

Clave privada

Credenciales

Servicios de rol

Tipo de instalación

Tipo de CA

Clave privada

Criptografía

Nombre de CA

Período de validez

Base de datos de certifica...

Confirmación

Progreso

Resultados

Especifique el tipo de la clave privada

Para generar y emitir certificados a clientes, una entidad de certificación (CA) debe disponer de una clave privada.

☒ Crear una clave privada nueva

Use esta opción si no dispone de una clave privada o desea crear una clave privada nueva.

☐ Usar clave privada existente

Use esta opción para asegurar la continuidad con los certificados emitidos previamente al reinstalar una CA.

☐ Seleccionar un certificado y usar su clave privada asociada

Seleccione esta opción si tiene un certificado en este equipo o si desea importar un certificado y usar su clave privada asociada.

☐ Seleccionar una clave privada existente en este equipo

Seleccione esta opción si conserva las claves privadas de una instalación anterior o si desea usar una clave privada de otra procedencia.

Una vez que le demos a siguiente le indicaremos el tipo de claves criptográficas.

Criptografía para la CA

Credenciales

Servicios de rol

Tipo de instalación

Tipo de CA

Clave privada

Criptografía

Nombre de CA

Período de validez

Base de datos de certifica...

Confirmación

Progreso

Especifique las opciones criptográficas

Seleccionar un proveedor de servicios criptográficos:

Longitud de la clave:

RSA#Microsoft Software Key Storage Provider

2048

Seleccione el algoritmo hash para firmar los certificados emitidos por esta CA:

SHA256

SHA384

SHA512

SHA1

MD5

☐ Permitir interacción del administrador cuando la CA obtiene acceso a la clave privada.

Luego le indicaremos el nombre para identificar la entidad de certificación.

Nombre de CA

SERVIDOR DE DESTINO
DC-FTP

- Credenciales
- Servicios de rol
- Tipo de instalación
- Tipo de CA
- Clave privada
- Criptografía
- Nombre de CA**
- Período de validez
- Base de datos de certifica...
- Confirmación
- Progreso
- Resultados

Especifique el nombre de la CA

Escriba un nombre común para identificar esta entidad de certificación (CA). Este nombre se agrega a todos los certificados emitidos por la CA. Los valores de sufijo de nombre distintivo se generan automáticamente, pero se pueden modificar.

Nombre común para esta entidad de certificación:

Sufijo de nombre distintivo:

Vista previa de nombre distintivo:

Ahora le indicaremos el periodo de validez.

Período de validez

SERVIDOR DE DESTINO
DC-FTP

- Credenciales
- Servicios de rol
- Tipo de instalación
- Tipo de CA
- Clave privada
- Criptografía
- Nombre de CA
- Período de validez**
- Base de datos de certifica...
- Confirmación
- Progreso
- Resultados

Especifique el período de validez

Seleccione el período de validez para el certificado generado para esta entidad de certificación (CA):

Años

Fecha de expiración de CA: 10/12/2029 21:52:00

El período de validez configurado para este certificado de CA debe superar el período de validez de los certificados que emitirá.

Ahora le indicaremos donde se encontrará la base de datos.

Base de datos de CA

SERVIDOR DE DESTINO
DC-FTP

Credenciales
Servicios de rol
Tipo de instalación
Tipo de CA
Clave privada
Criptografía
Nombre de CA
Período de validez
Base de datos de certifica...
Confirmación
Progreso
Resultados

Especifique las ubicaciones de las bases de datos

Ubicación de la base de datos de certificados:
C:\Windows\system32\CertLog

Ubicación del registro de la base de datos de certificados:
C:\Windows\system32\CertLog

Luego le daremos a confirmar y nos saldrá lo siguiente.

Resultados

SERVIDOR DE DESTINO
DC-FTP

Credenciales
Servicios de rol
Tipo de instalación
Tipo de CA
Clave privada
Criptografía
Nombre de CA
Período de validez
Base de datos de certifica...
Confirmación
Progreso
Resultados

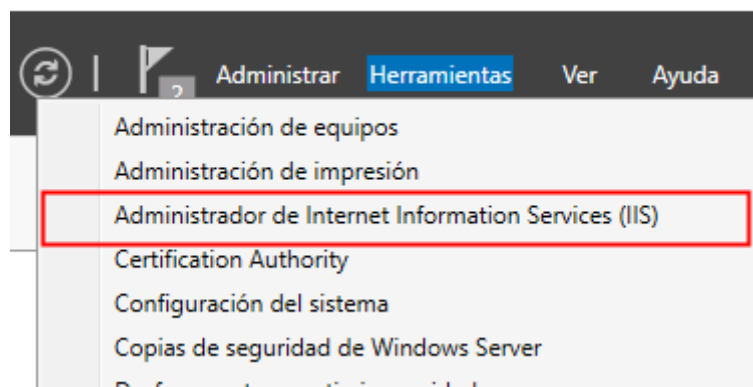
Se configuraron los roles, servicios de rol o características siguientes:

Servicios de certificados de Active Directory

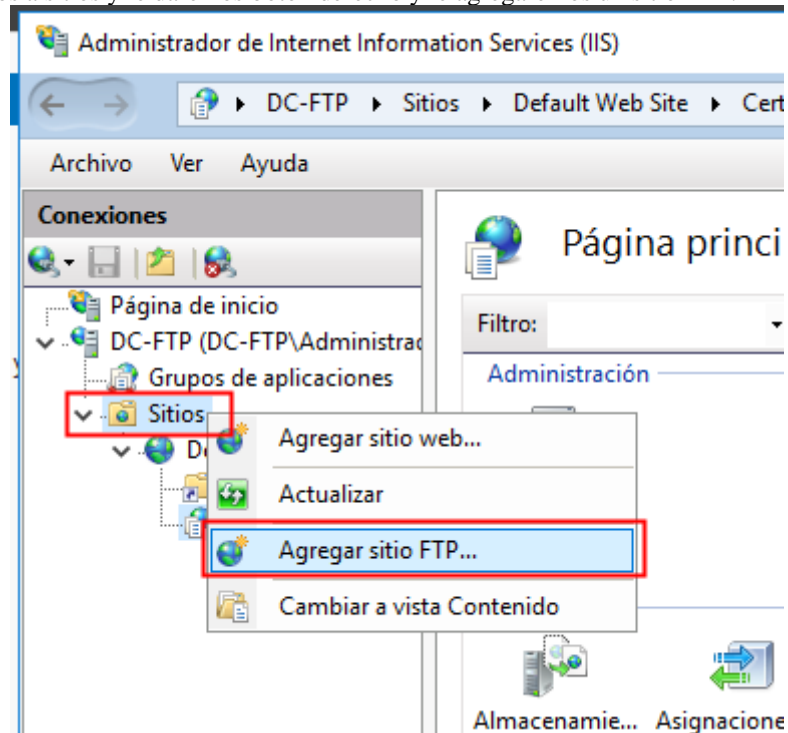
Entidad de certificación **✓ Configuración realizada correctamente**
[Más información acerca de la configuración de CA](#)

Inscripción web de entidad de certificación **✓ Configuración realizada correctamente**
[Más información acerca de la configuración de inscripción web](#)

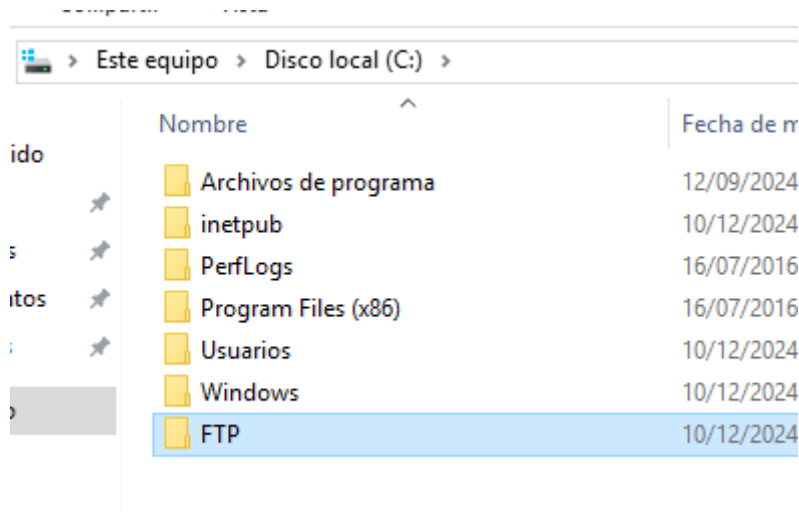
Ahora nos iremos a la administración de internet information services (IIS).



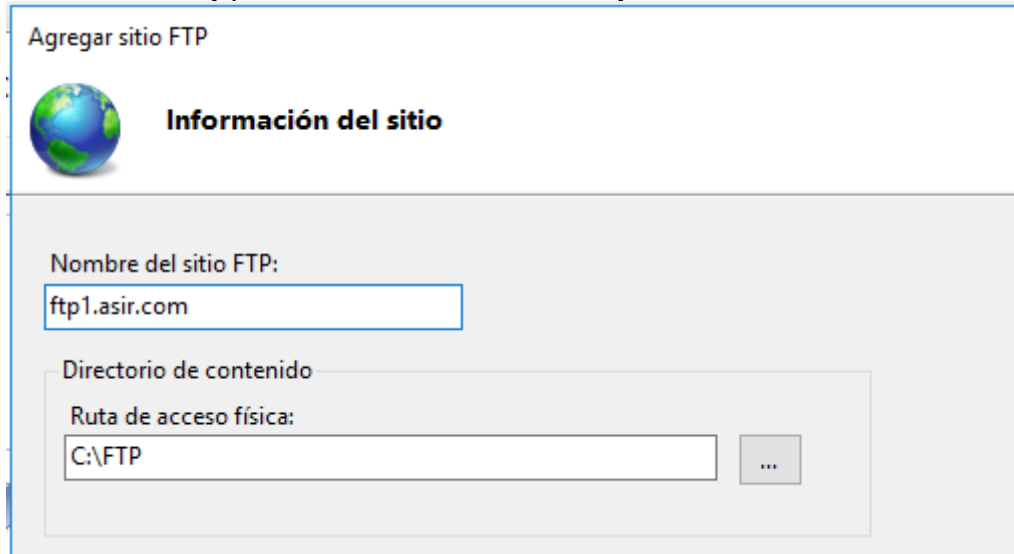
Ahora nos iremos a sitios y le daremos botón derecho y le agregaremos un sitio FTP.



Crearemos una carpeta en C:\ y es donde se guardará todos archivos que subiremos al servidor.



Ahora nos iremos al IIS y pondremos el nombre del sitio FTP y la ruta de acceso.



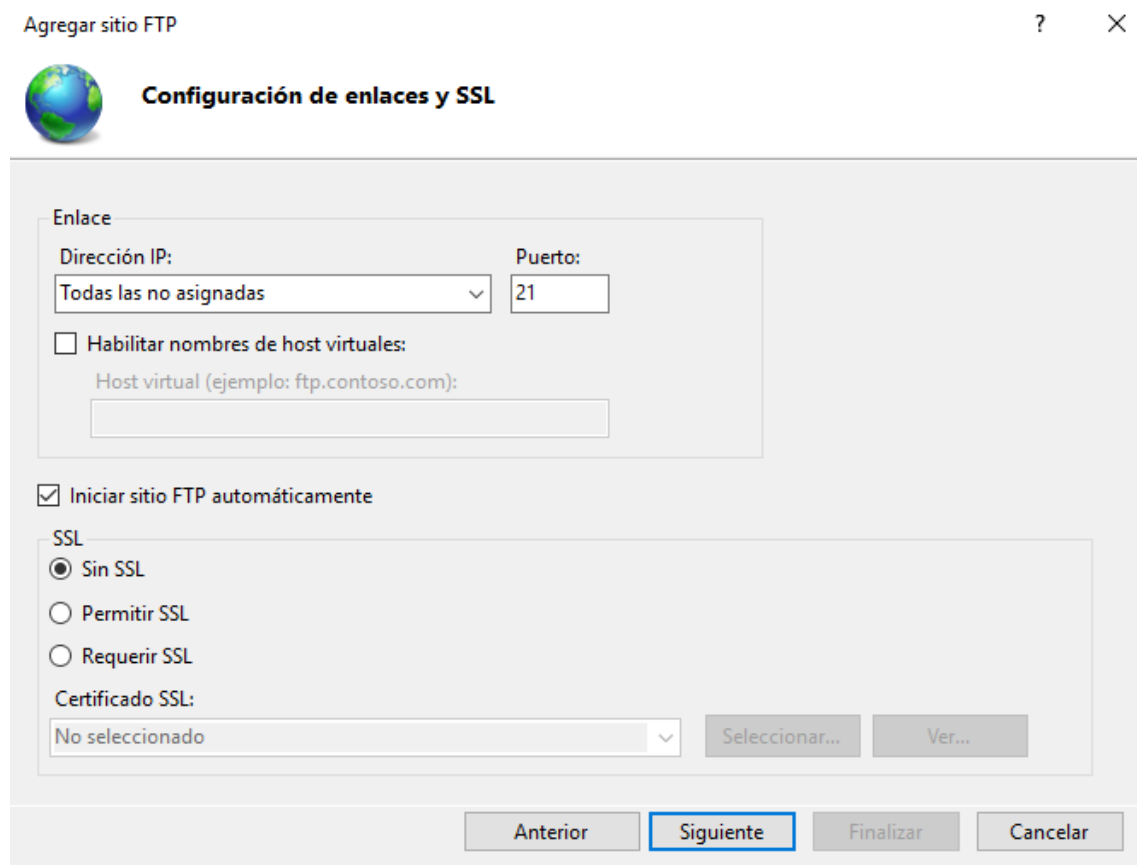
Agregar sitio FTP

Información del sitio

Nombre del sitio FTP:
ftp1.asir.com

Directorio de contenido
Ruta de acceso física:
C:\FTP

Le daremos a siguiente y le indicaremos el tipo de enlace y luego el certificado SSL, por ahora no hace falta, pero más adelante lo habilitaremos ya que vamos a crear nuestro certificado.



Agregar sitio FTP

Configuración de enlaces y SSL

Enlace

Dirección IP: Todas las no asignadas Puerto: 21

☐ Habilitar nombres de host virtuales:
Host virtual (ejemplo: ftp.contoso.com):

☒ Iniciar sitio FTP automáticamente

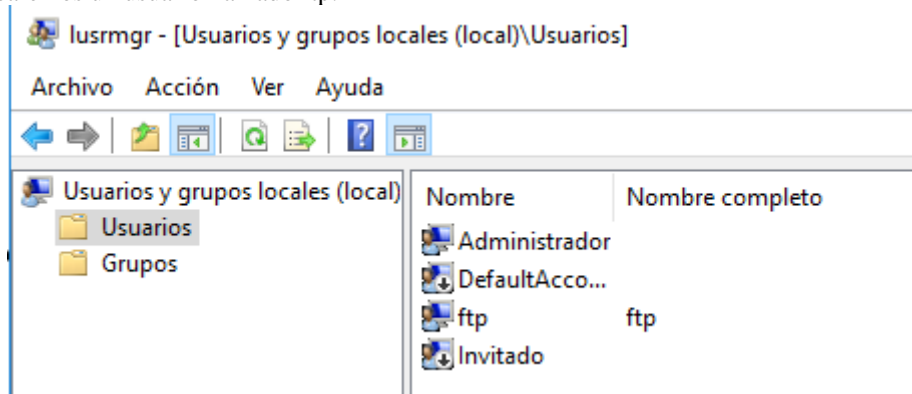
SSL

☒ Sin SSL
☐ Permitir SSL
☐ Requerir SSL

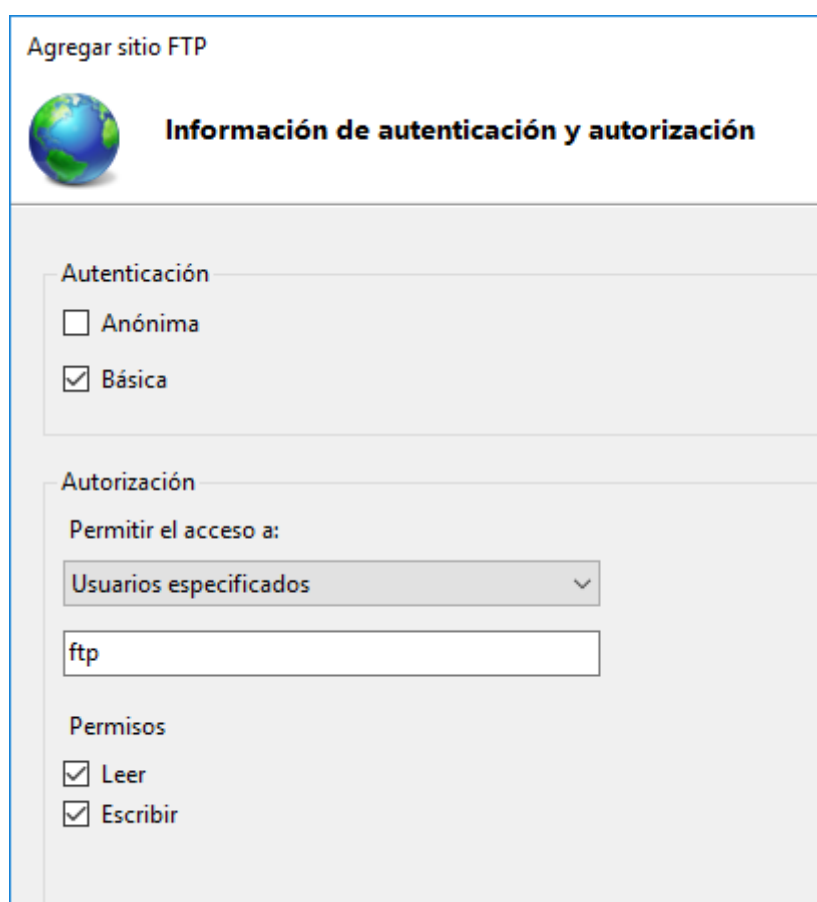
Certificado SSL:
No seleccionado Selecccionar... Ver...

Anterior Siguiente Finalizar Cancelar

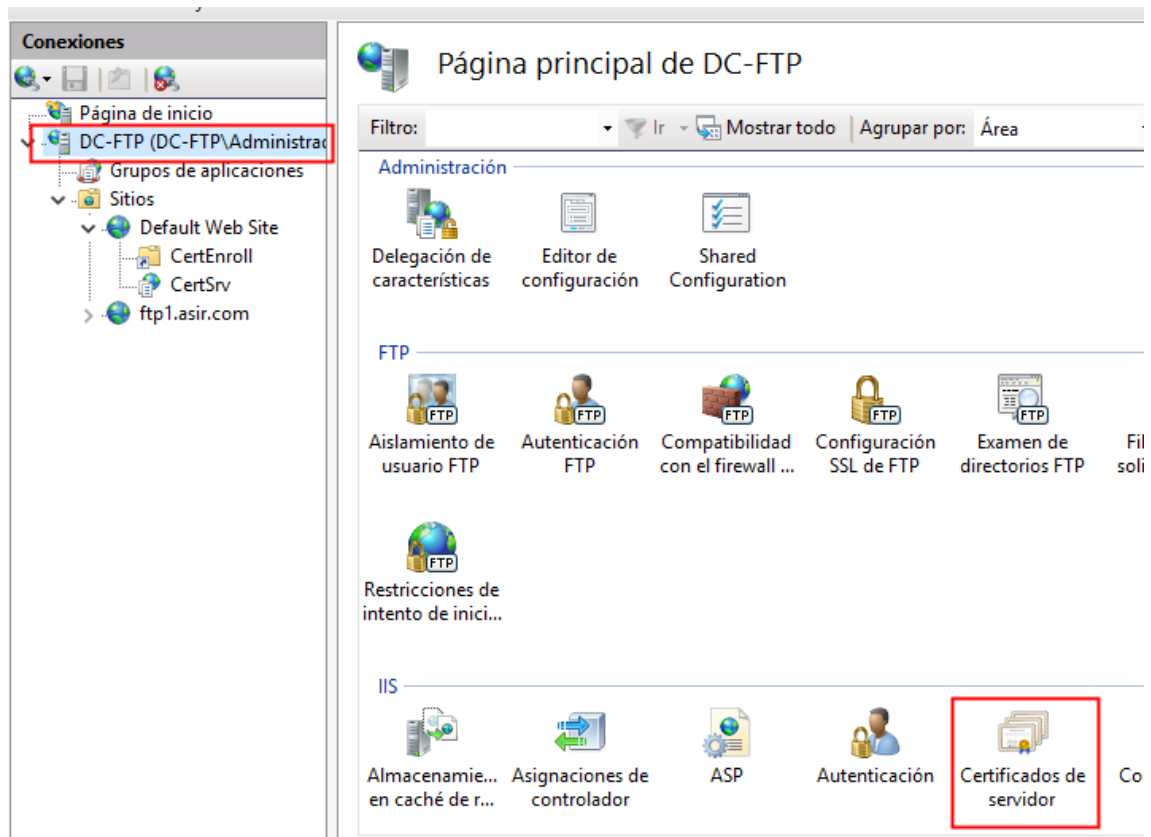
Ahora crearemos un usuario llamado ftp.



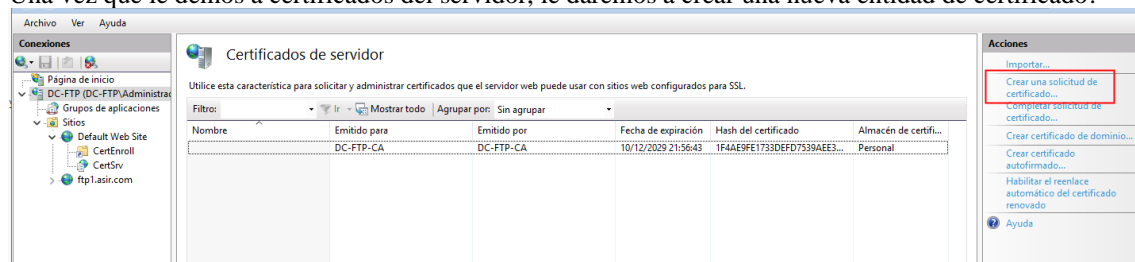
Una vez que antes le demos a siguiente le permitiremos el acceso al usuario FTP.



Una vez que hemos terminado crearemos los certificados.




Una vez que le demos a certificados del servidor, le daremos a crear una nueva entidad de certificado.



Y escribiremos el nombre de la entidad requerida para el certificado.

Solicitar certificado ? X

 **Propiedades de nombre distintivo**

Especifique la información requerida para el certificado. Estado o provincia y Ciudad o localidad deben ser nombres oficiales y no deben contener abreviaturas.

Nombre común: ftp1.asir.com

Organización: IES

Unidad organizativa: VALLE

Ciudad o localidad: MADRID

Estado o provincia: ESPAÑA

País o región: ES

Una vez que hemos dado a siguiente nos dirá el proveedor de servicios criptográficos y la longitud de bits del certificado.

Solicitar certificado



Propiedades de proveedor de servicios criptográficos

Seleccione un proveedor de servicios criptográficos y una longitud en bits. La longitud en bits de cifrado determina la seguridad de cifrado del certificado. Cuanto mayor sea la longitud en bits, más segura será la comunicación. Sin embargo, una longitud en bits grande puede mermar el rendimiento.

Proveedor de servicios criptográficos:

Microsoft RSA SChannel Cryptographic Provider

Longitud en bits:

1024

Ahora nos dirá el nombre y donde lo va a guardar.

Solicitar certificado



Nombre de archivo

Especifique un nombre para la solicitud de certificado. Esta información se puede enviar a una entidad de certificación para que la firme.

Especificar un nombre de archivo para la solicitud de certificado:



Y le daremos a finalizar.

Abriremos el certificado a ver como es.



CERTIFICADO: Bloc de notas

Archivo Edición Formato Ver Ayuda

```

|-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDSzCCArQCAQAwZjELMAkGA1UEBhMCRVVxEDAOBgNVBAGMB0VTUEHDkUExDzAN
BgNVBACMBk1BRFJJRDEMMAoGA1UECgwDSUVTMQ4wDAYDVQQQLDAVWQUxMRTEWMBQG
A1UEAwwNZnRwMS5hc2lyLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA
t1BABPhv5DwwH6eMMGOomEomCM1t/UE4b2nipSPLGeFBb00zX432QKcm/DJb9WVw
wHXn7CfzmtscGj3T3ZDwmajqcGidRsw8wWoICJmCisWfNYxZu82Ayr3kXMGknVW
jG8DGRkcfeRwgwjMSAUVtuXik8mgoacq2ioEppyqq2sCAwEAAaCCAAMwHAYKKwYB
BAGCNw0CAzEOfgwxMC4wLjE0MzkzLjIwPQYJKwYBBAGCNxUUMTAwLgIBBQwGREMt
R1RQDBREQy1GVFBcQWRtaW5pc3RyYWVvcgwLSW51dE1nci5leGUwcgYKKwYBBAGC
Nw0CAjFkMGICAQEeWgBNAGkAYwByAG8AcwBvAGYAdAAgAFIAUwBBACAAUwBDAGGA
YQBuAG4AZQBzACAAQwByAHkAcAB0AG8AZwByAGEAcABoAGkAYwAgAFAAcgBvAHYA
aQBkAGUAcgMBADCBzwYJKoZIhvcNAQkOMYHBMIG+MA4GA1UdDwEB/wQEAwIE8DAT
BgNVHSUEDDAKBggrBgEFBQcDATB4BgkqhkiG9w0BCQ8EazBpMA4GCCqGSIb3DQMC
AgIAgDAOBggqhkiG9w0DBAICAIAwCwYJYIZIAWUDBAEFMAcGBSsOAwIHMAoGCCqGSIb3DQMHMB0G
Bg1ghkgBZQMEAQIwCwYJYIZIAWUDBAEFMAcGBSsOAwIHMAoGCCqGSIb3DQMHMB0G
A1UdDgQWBBTAqev6aFJxAFczvh1ACzWSdcZqZzANBgkqhkiG9w0BAQUFAAOBgQAF
+eTJzIvWyk9I0/A1GfKp2CjG57G5oaAIR4yDPISdkaez1Bv5JZVTxP2ebiPtFe18
zJ7mSjSpzK8iXdgYBXhGCIntKVHmHSVWHk9ZZpGskiqS+E4nPAw+S4rZKy1Yt0VY
2Bg9f8z0GEa0RuZrp9JKN4BRYfdTkLF3M7m3WI1zdW==
-----END NEW CERTIFICATE REQUEST-----

```

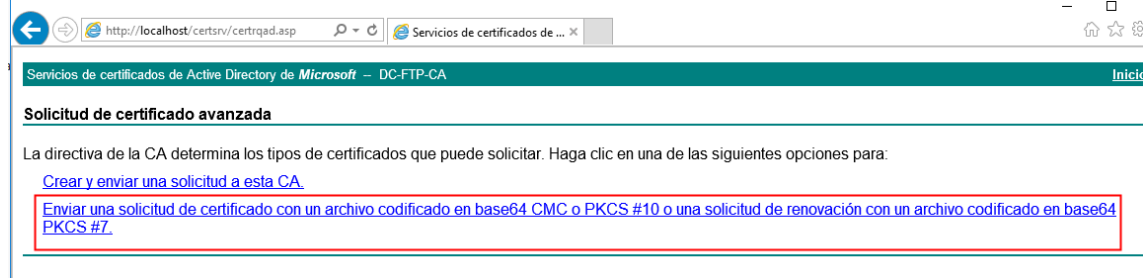
Ahora nos iremos a internet, en mi caso es internet Explorer, ya que es windows server 2016 y escribiremos lo siguiente en el buscador, una vez que nos salga la siguiente pantalla le daremos a solicitar un certificado.



Una vez que le demos a solicitar un certificado nos saldrá la siguiente ventana y le daremos a solicitud avanzada de certificado.



Una vez que nos salga la siguiente le daremos a enviar el certificado que hemos creado anteriormente.

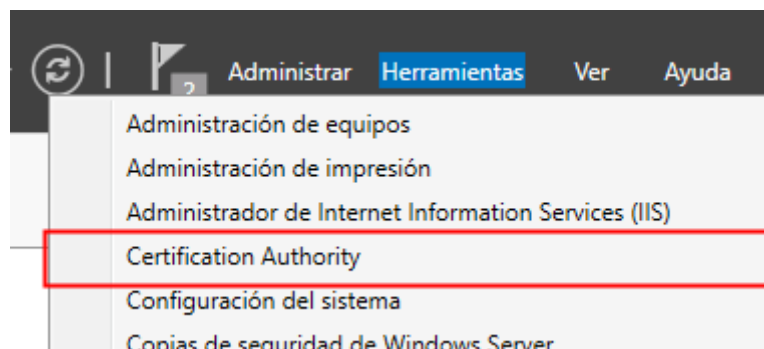


Copiamos el certificado en el navegador y le daremos a enviar.

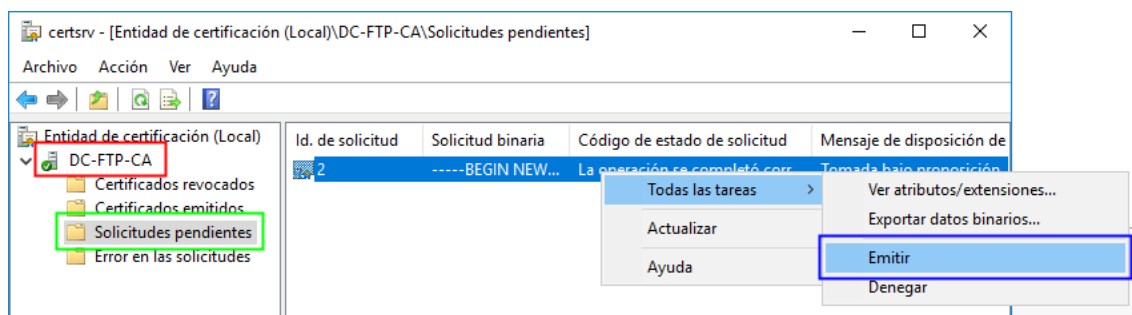
[illegible]

Una vez que le demos a enviar nos saldrá la siguiente pantalla.

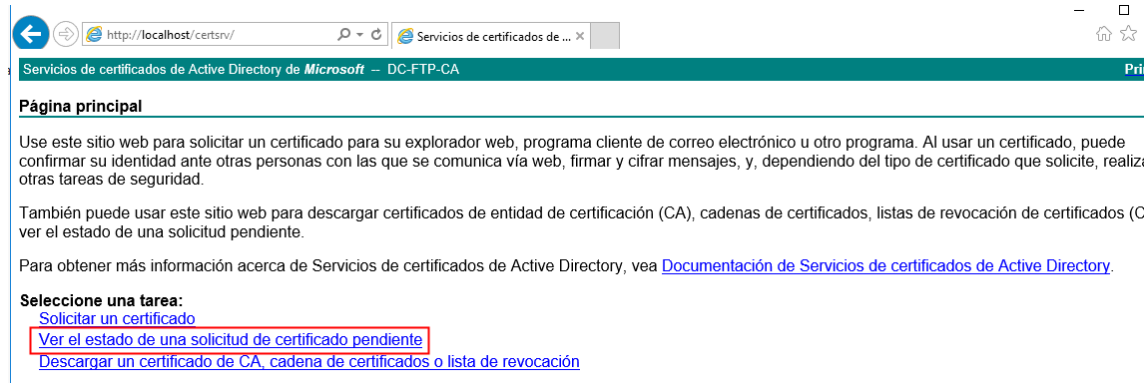
Ahora tenemos un certificado pendiente, tenemos que irnos al servidor para validar el certificado.



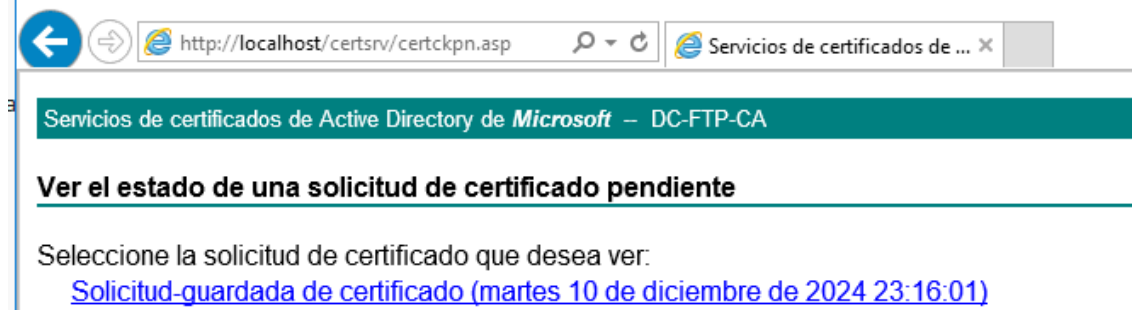
Y nos saldrá la siguiente pantalla, donde le daremos al nombre del servidor y luego en solicitudes pendientes, veremos la solicitud que hemos enviado hace un momento y le daremos a emitir.



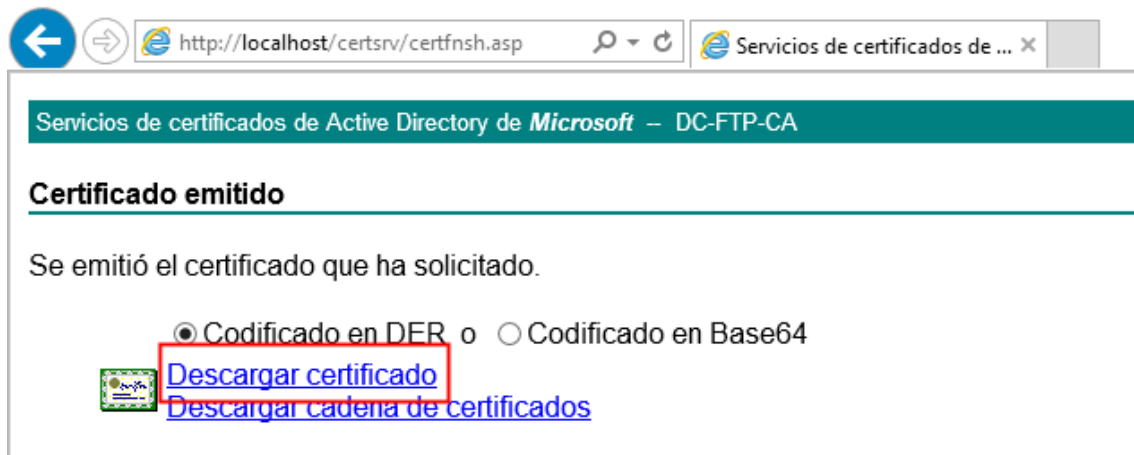
Una vez que lo hemos emitido, nos iremos a la página web donde estábamos antes y le daremos a ver el estado de la solicitud.



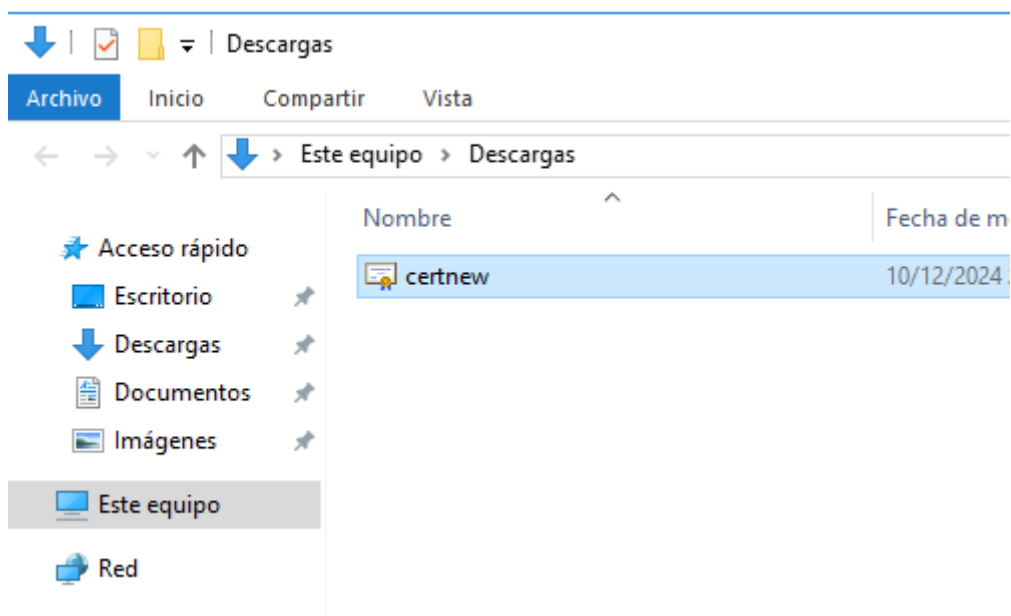
Una vez que le demos a ver el estado de la solicitud, veremos que hay una solicitud guardada.



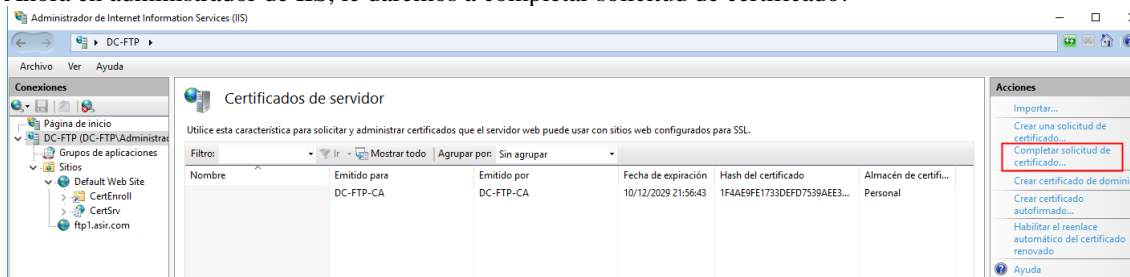
Una vez que le demos a ver la solicitud, le daremos a descargar certificado.



Una vez descargado el certificado lo guardaremos, en mi caso es en descargas.



Ahora en administrador de IIS, le daremos a completar solicitud de certificado.



Una vez que le demos a completar solicitud de certificado nos saldrá lo siguiente, escribiremos el nombre del certificado que hemos creado antes y un nombre.

Completar solicitud de certificado



Especificar respuesta de entidad de certificación

Complete una solicitud de certificado creada previamente recuperando el archivo que contiene la respuesta de la entidad de certificación.

Nombre del archivo que contiene la respuesta de la entidad de certificación:

C:\Users\Administrador\Downloads\certnew.cer

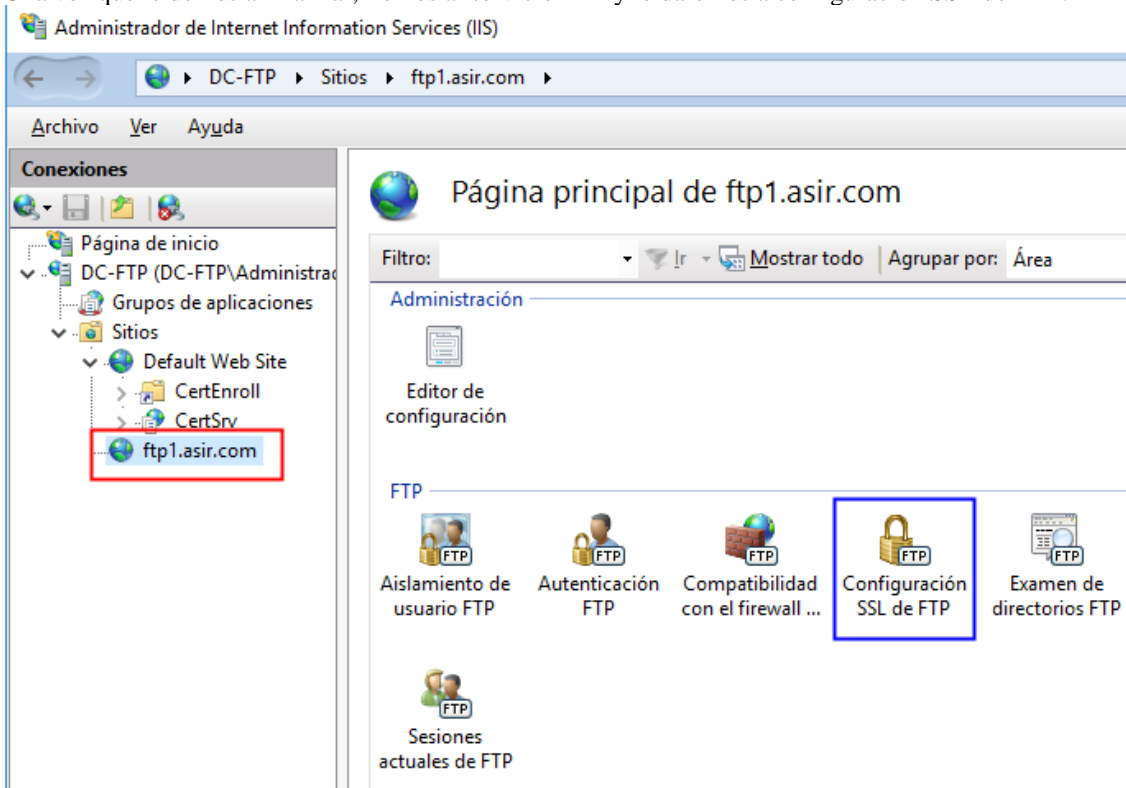
Nombre descriptivo:

ftp1

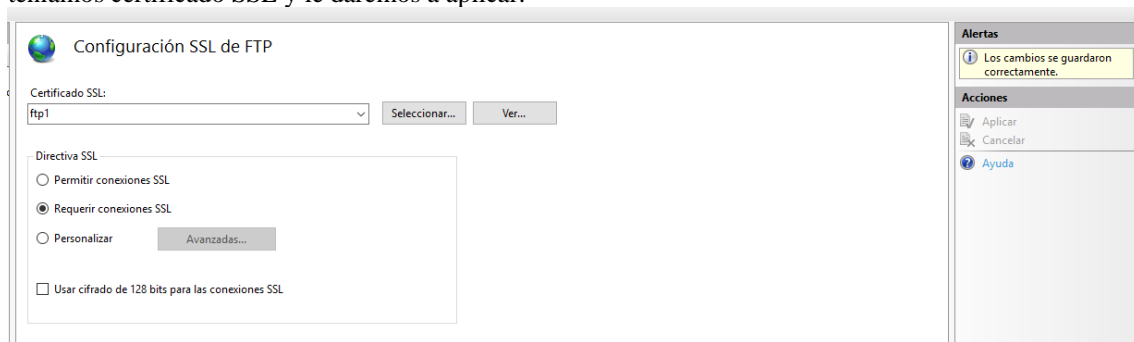
Seleccione un almacén de certificados para el nuevo certificado:

Personal

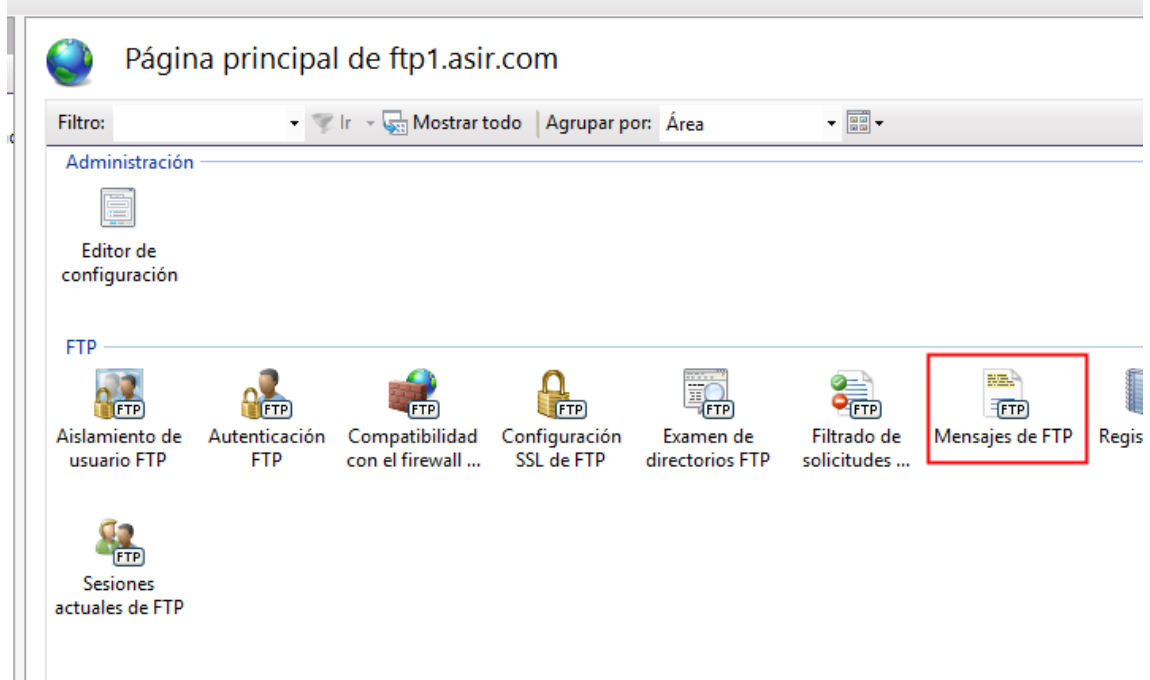
Una vez que le demos a finalizar, iremos al servicio FTP y le daremos a configuración SSL de FTP.




Y nos saldrá la siguiente ventana, donde antes hemos dicho que no queríamos conexiones SSL, ya que no teníamos certificado SSL y le daremos a aplicar.



Ahora nos iremos a mensajes de FTP y pondremos un mensaje de bienvenida y uno de despedida.



Ahora pondremos un mensaje personalizado.



Mensajes de FTP

Comportamiento del mensaje

- ☐ Suprimir titular predeterminado
- ☐ Admitir variables de usuario en los mensajes
- ☒ Mostrar mensajes detallados para las solicitudes locales

Texto del mensaje

Titular:

Bienvenida:

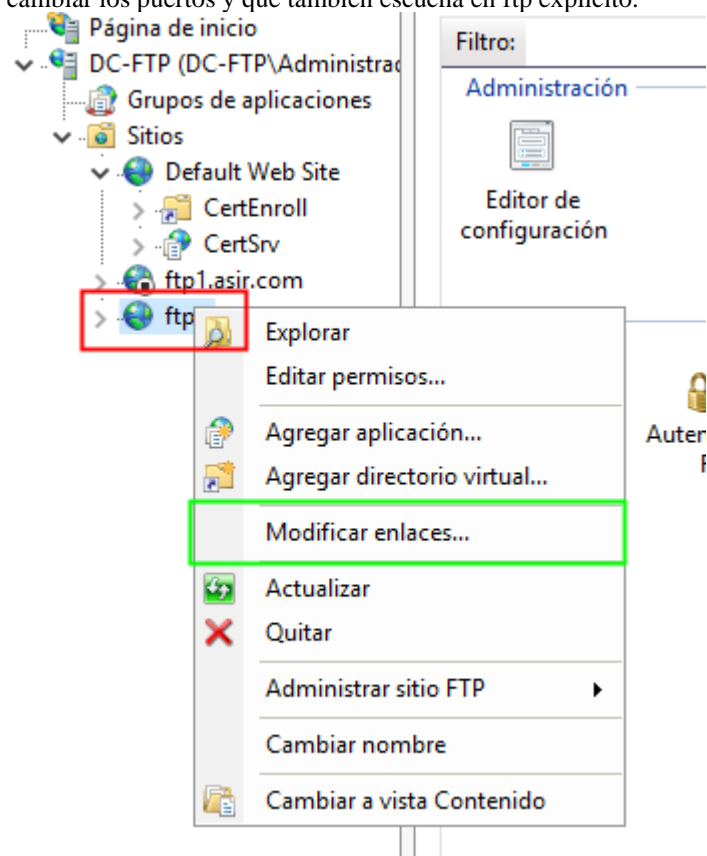
bienvenido al FTP en windows server

Salida:

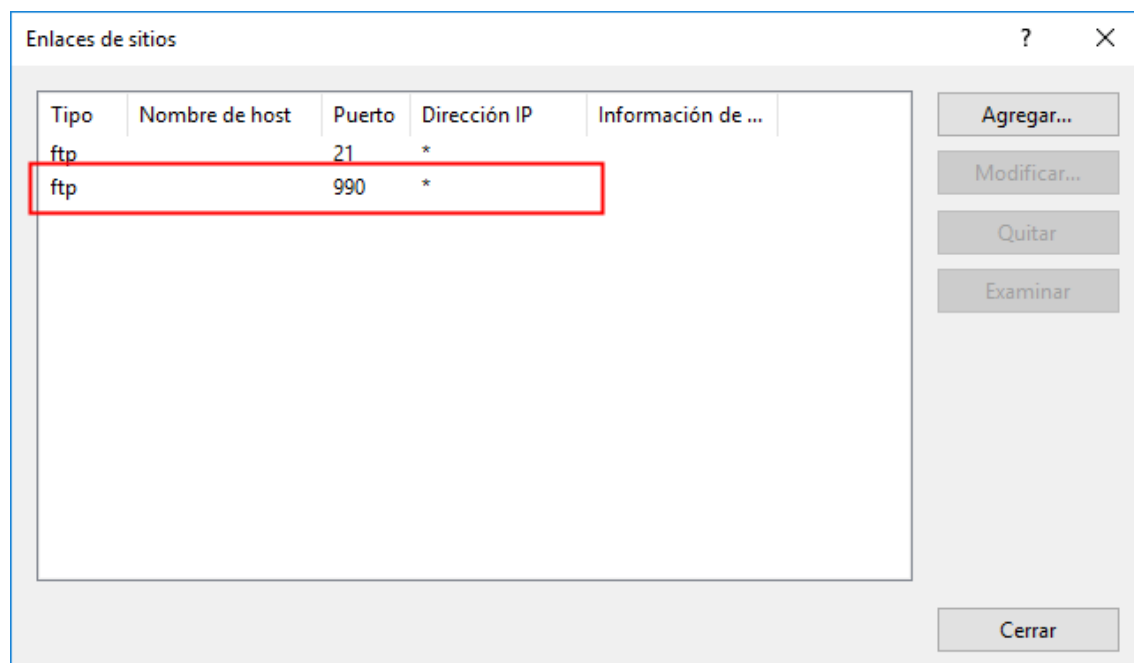
¡hasta luego!

Nº máximo de conexiones:

Ahora nos iremos a cambiar los puertos y que también escucha en ftp explícito.

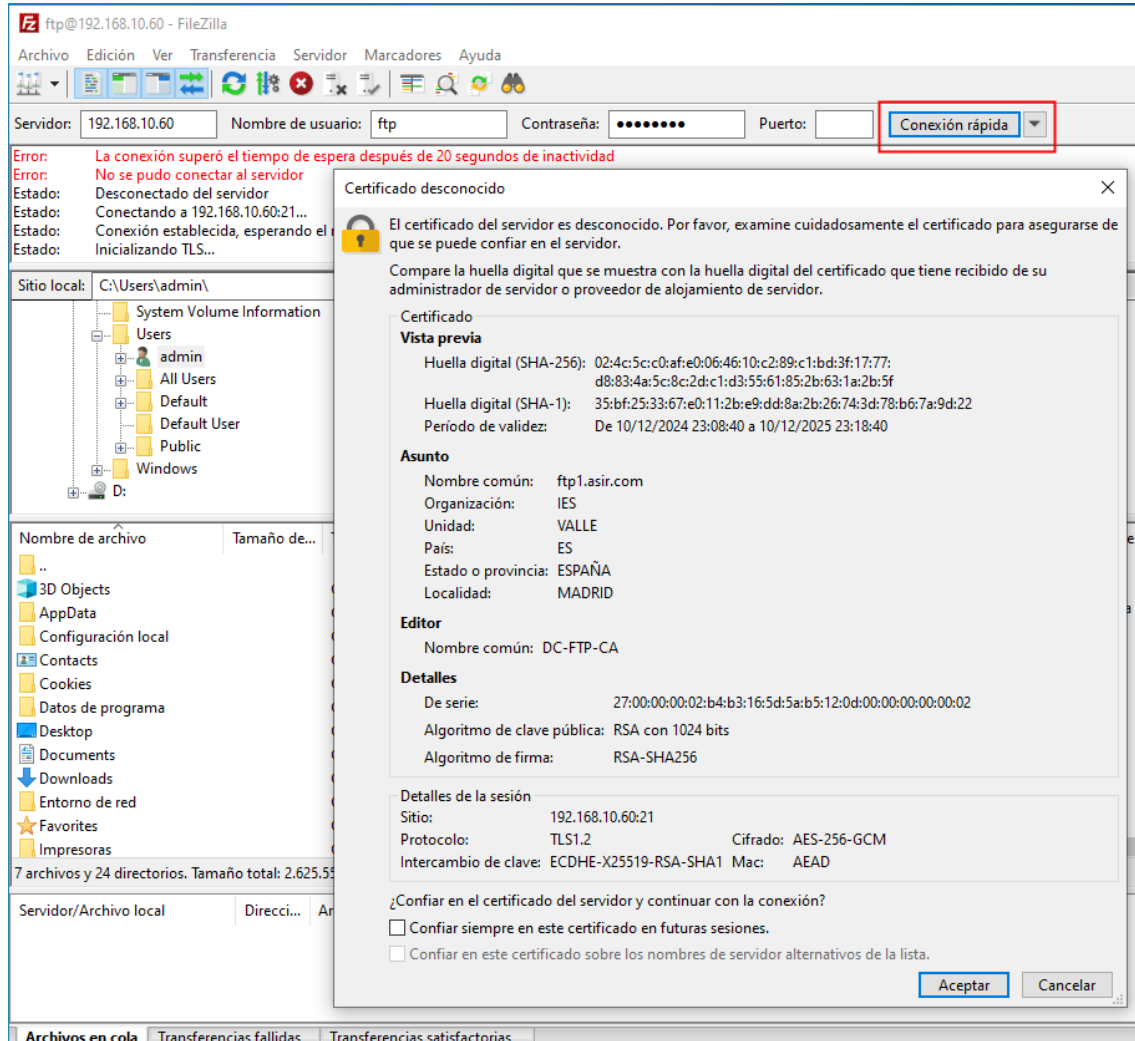


Una vez que le demos a agregar escribiremos el puerto y le daremos a aceptar.

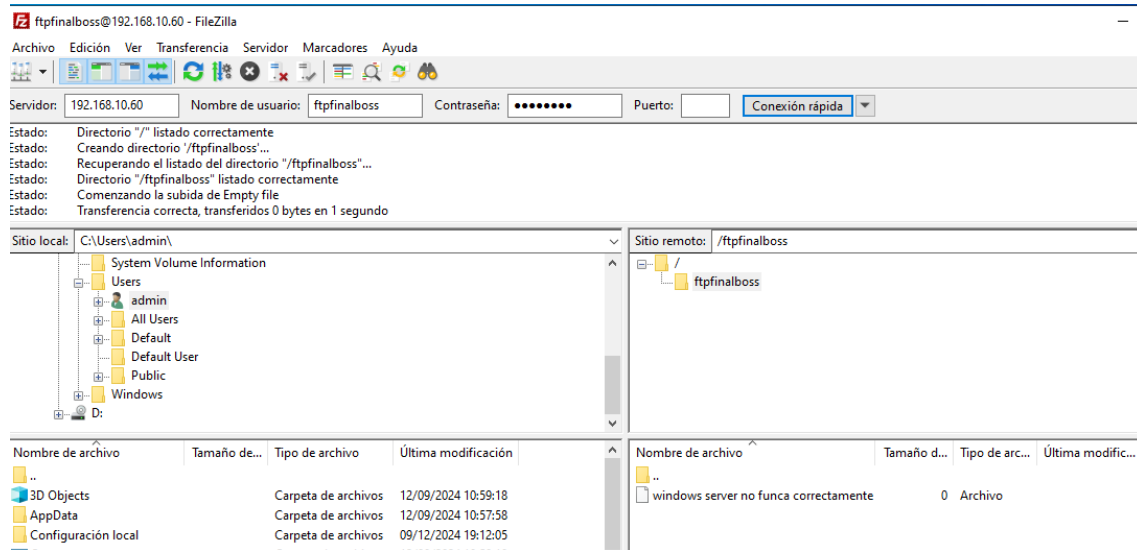


10. Comprobaciones windows

Ahora iniciamos sesión en el cliente y abrimos una conexión con FTP y veremos que nos sale el certificado.



Debido a problemitas ocasionado el usuario ftp, hemos tenido que crear otro usuario, como también hemos tenido que hacer un servidor ftp de 0, pero ahora con el usuario ftpfinalboss si funciona.

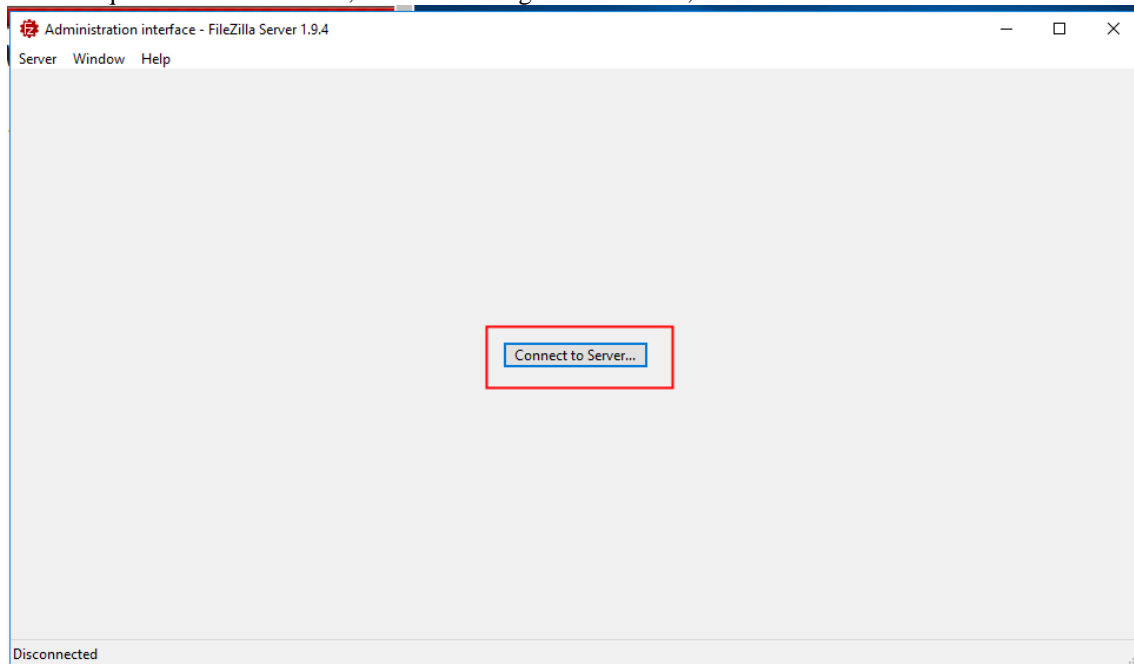


Hemos hecho un usuario y también hemos hecho una subida por ftp.

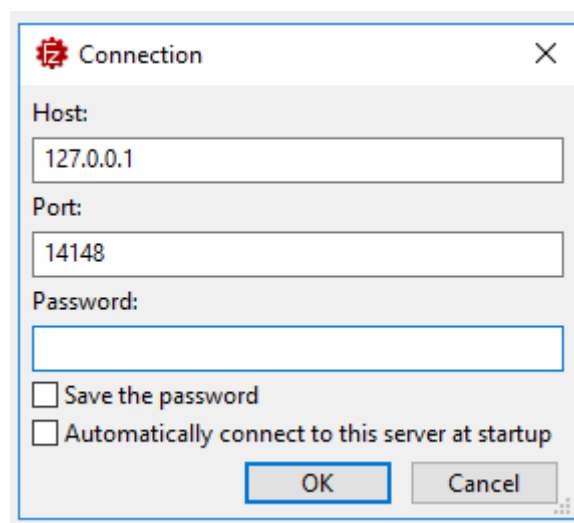
11. Otros programas

Ahora vamos a usar otros programas gratuitos y probar que podemos hacer un servidor ftp en windows. Vamos a usar FileZilla server.

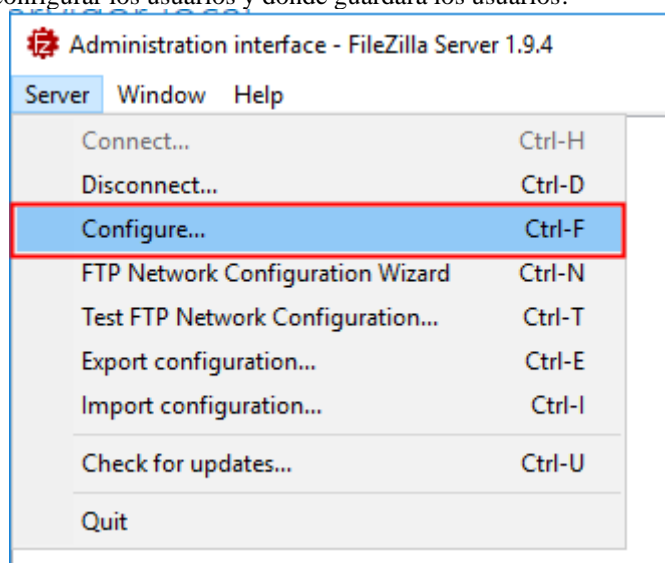
Una vez que lo hemos instalado, nos saldrá la siguiente ventana, le daremos a connect to server.



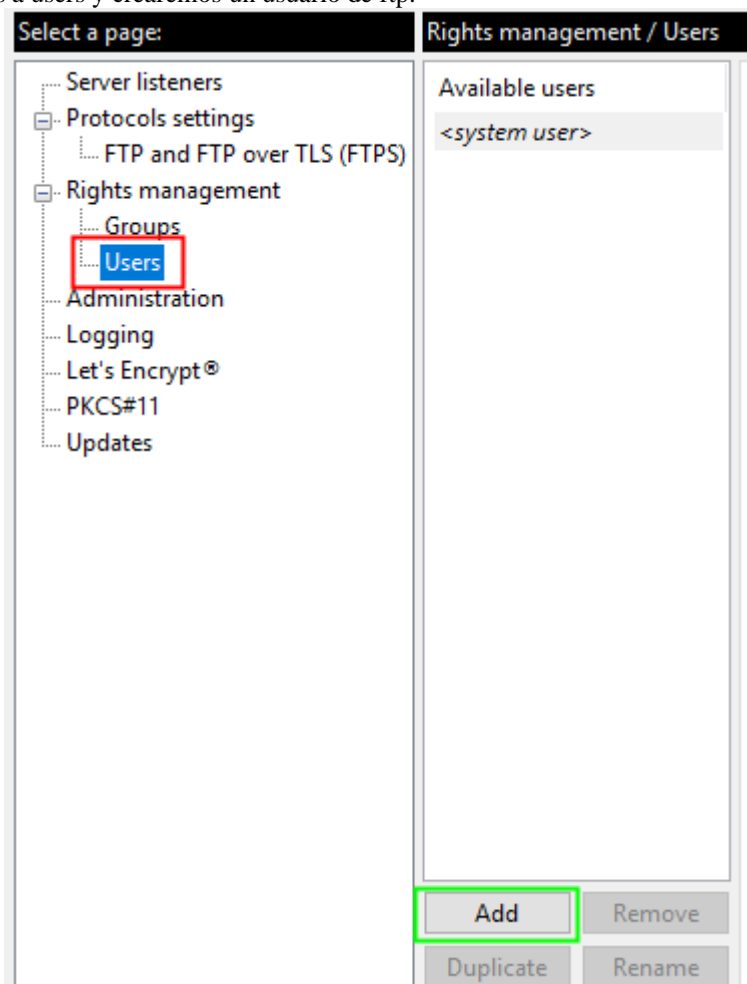
Lo dejaremos por defecto, ya que en la instalación no hemos puesto contraseña de administrador.



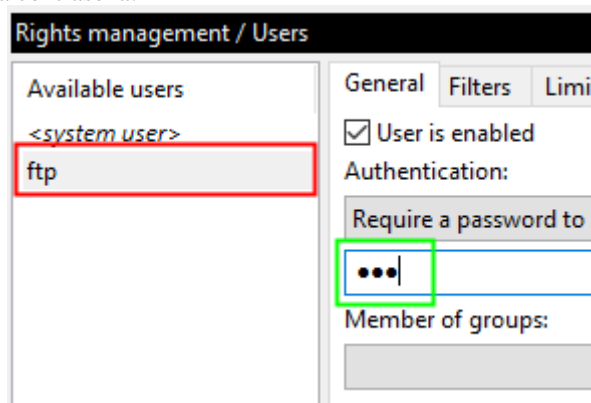
Ahora nos iremos a configurar los usuarios y donde guardara los usuarios.



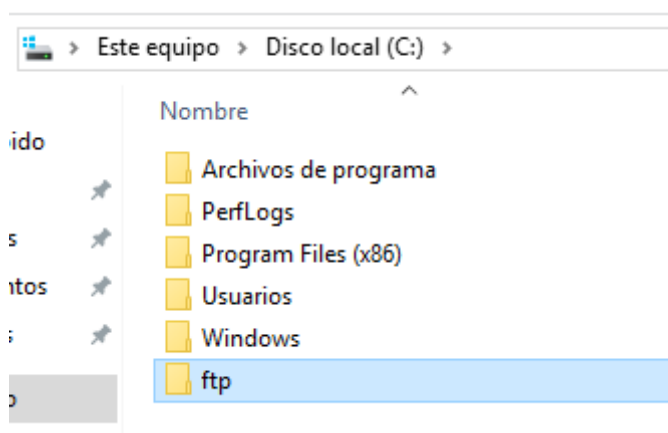
Ahora nos iremos a users y crearemos un usuario de ftp.



Creamos el usuario con la contraseña.



Ahora vamos a cambiar el directorio de trabajo, vamos a crear una carpeta en C:\ para guardar todos los archivos.



Ahora le indicamos el directorio que hemos creado antes.

Rights management / Users

Available users
 <system user>
 ftp

General Filters Limits

☒ User is enabled

Authentication:

Require a password to log in

Leave empty to keep existing password

Member of groups:

Mount points:

Virtual path	Native path
/	C:\ftp

Mount options

Access mode:
 Read + Write

☒ Apply permissions to subdirect
☒ Writable directory structure
☐ Create native directory if it doe

Add Remove [You can use placeholders in native p](#)

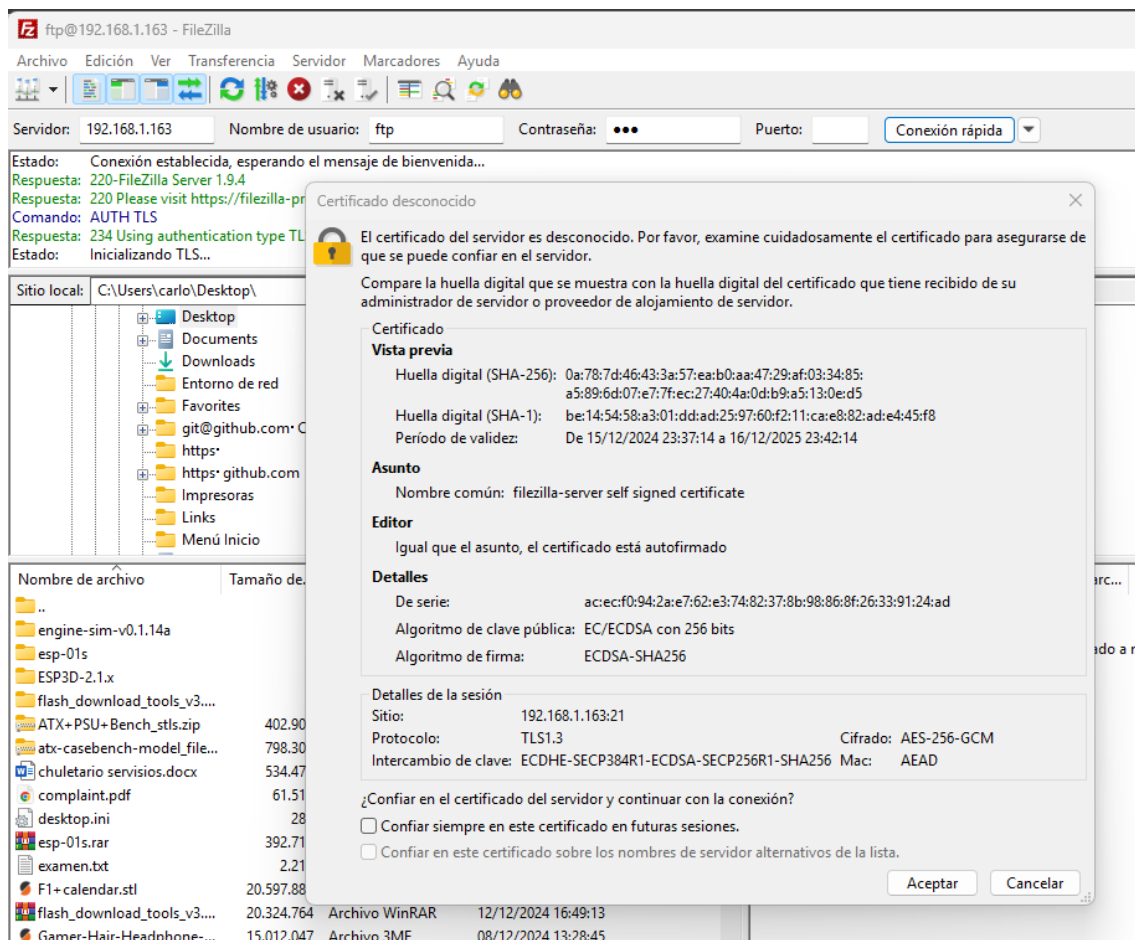
Description:

Una vez que le demos a aplicar y luego a aceptar, veremos en los logs de FileZilla que ha guardado todos los cambios.

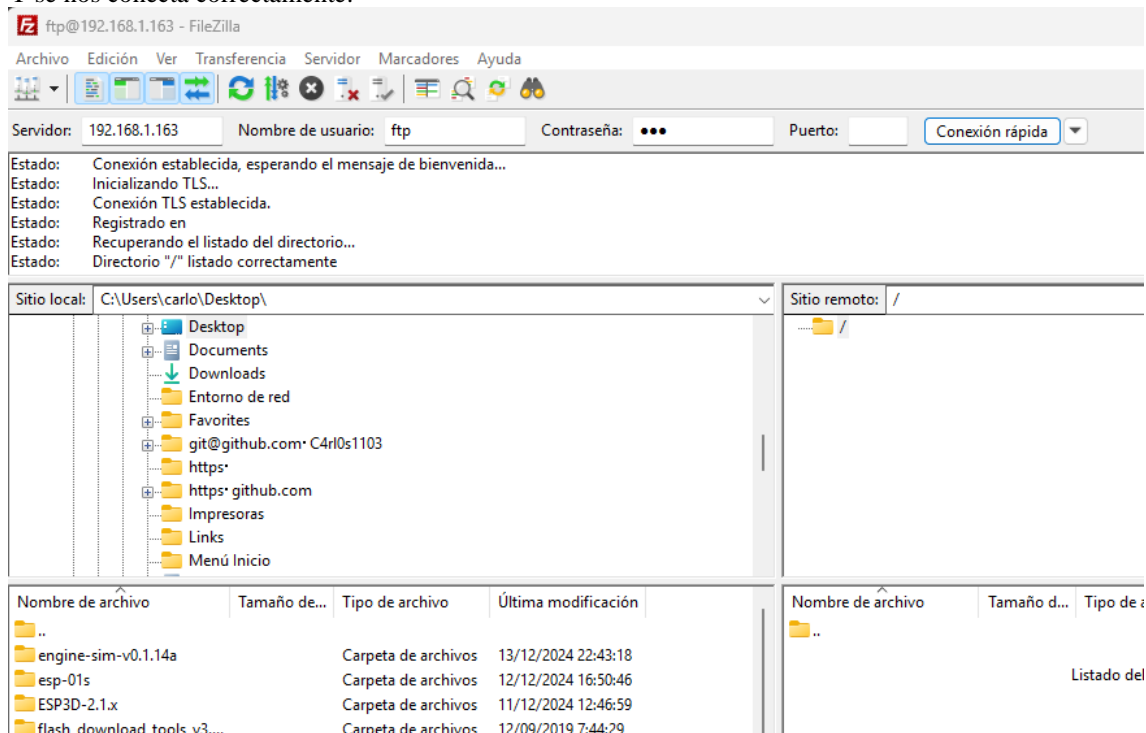
16/12/2024 9:03:30	Admin UI	Status	Getting certificate info...
16/12/2024 9:03:30		Status	Settings written to C:\ProgramData\filezilla-server\groups.xml.
16/12/2024 9:03:30		Status	Settings written to C:\ProgramData\filezilla-server\users.xml.
16/12/2024 9:03:30		Status	Settings written to C:\ProgramData\filezilla-server\disallowed_ips.xml.
16/12/2024 9:03:30		Status	Settings written to C:\ProgramData\filezilla-server\settings.xml.
16/12/2024 9:03:30		Status	Settings written to C:\ProgramData\filezilla-server\allowed_ips.xml.

MUY IMPORTANTE, QUITAR EL FIREWALL.

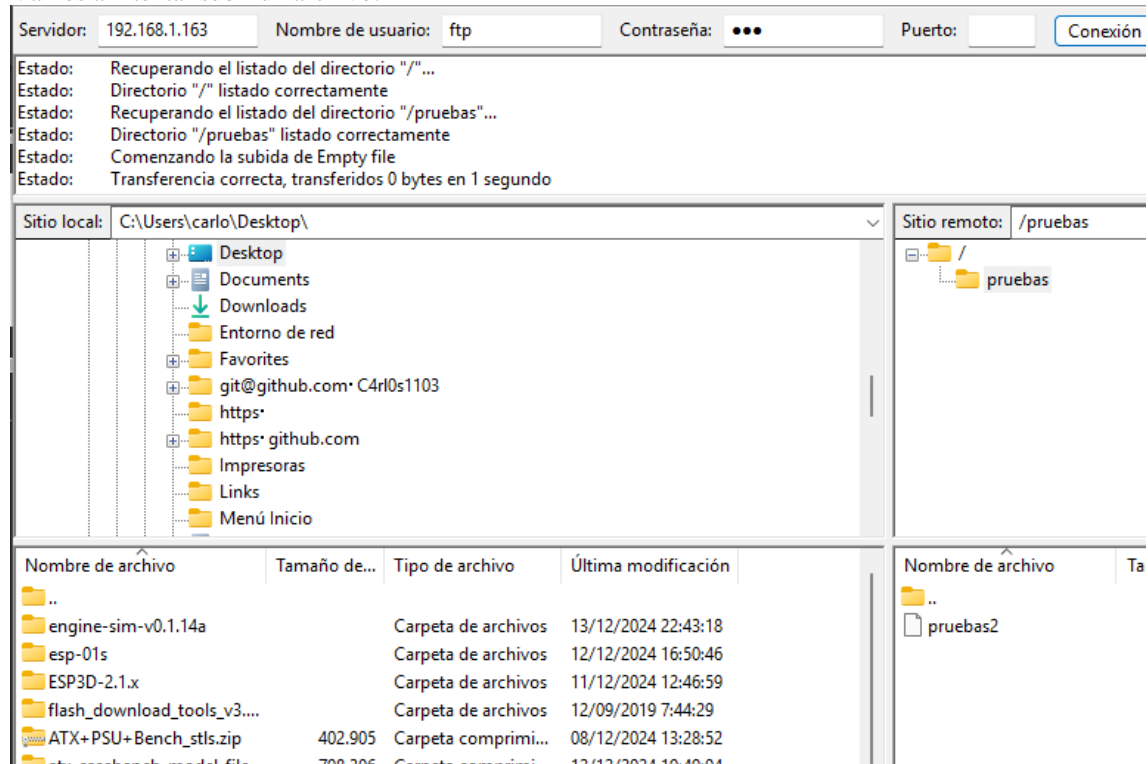
Ahora con un cliente, en mi caso la maquina real haremos la conexión.



Vemos que tiene un certificado propio de FileZilla.
Y se nos conecta correctamente.



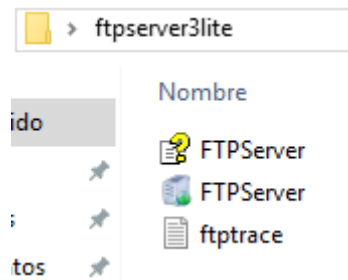
Vamos a intentar subir un archivo.



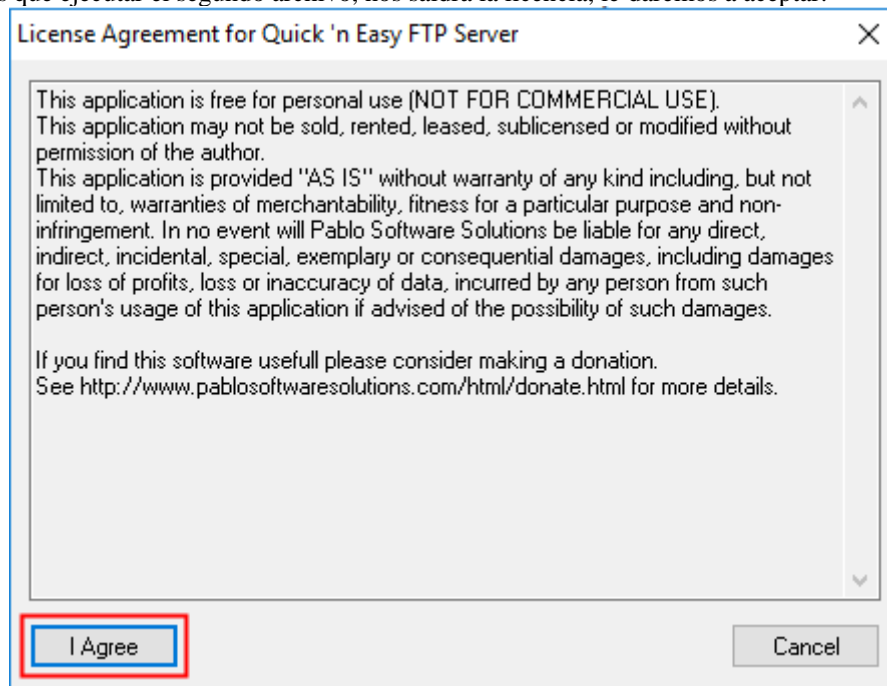
Y vemos que funciona correctamente.

Ahora vamos a usar otro programa llamado Quick'n Easy FTP Server Lite, de Pablo Software Solutions.

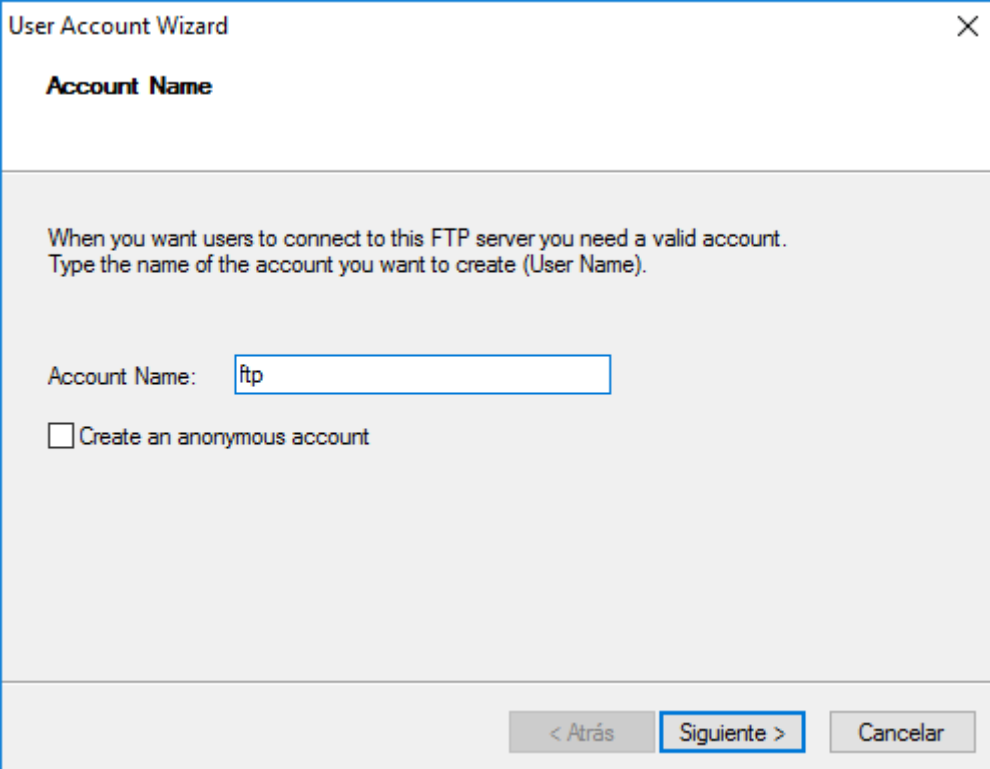
Una vez que hemos descargado y descomprimido, nos saldrá los siguientes archivos.



Y tenemos que ejecutar el segundo archivo, nos saldrá la licencia, le daremos a aceptar.



Ahora le indicamos el usuario que va a usar par ftp.



User Account Wizard

Account Name

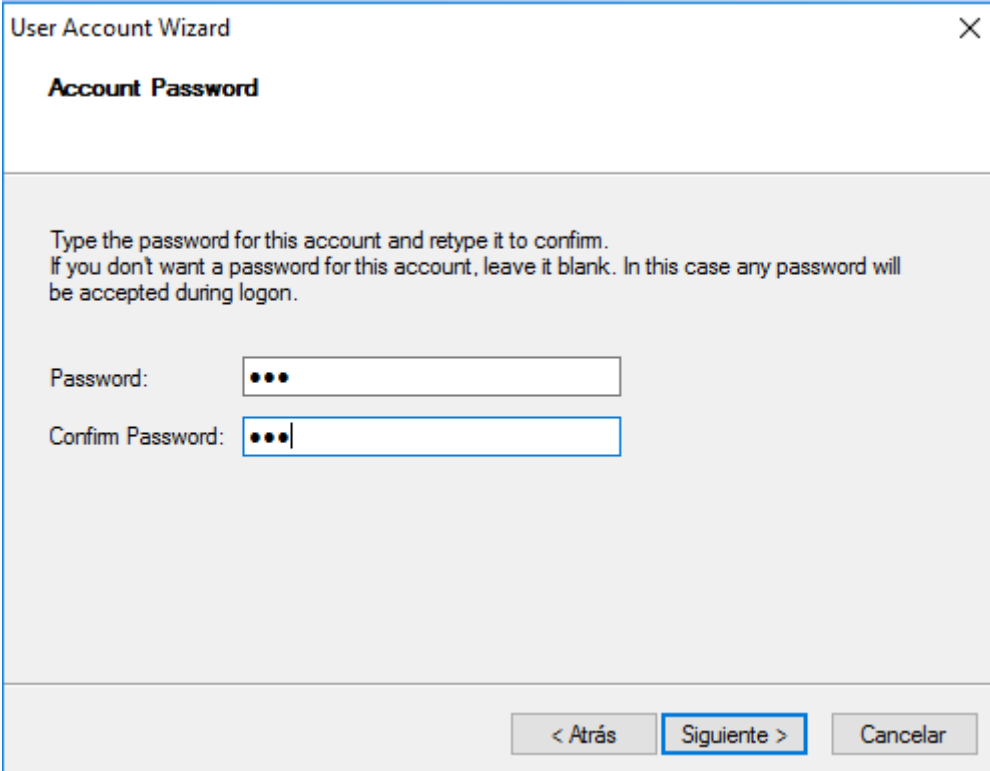
When you want users to connect to this FTP server you need a valid account.
Type the name of the account you want to create (User Name).

Account Name:

☐ Create an anonymous account

< Atrás **Siguiente >** Cancelar

Ahora le daremos a siguiente y escribiremos la nueva contraseña.



User Account Wizard

Account Password

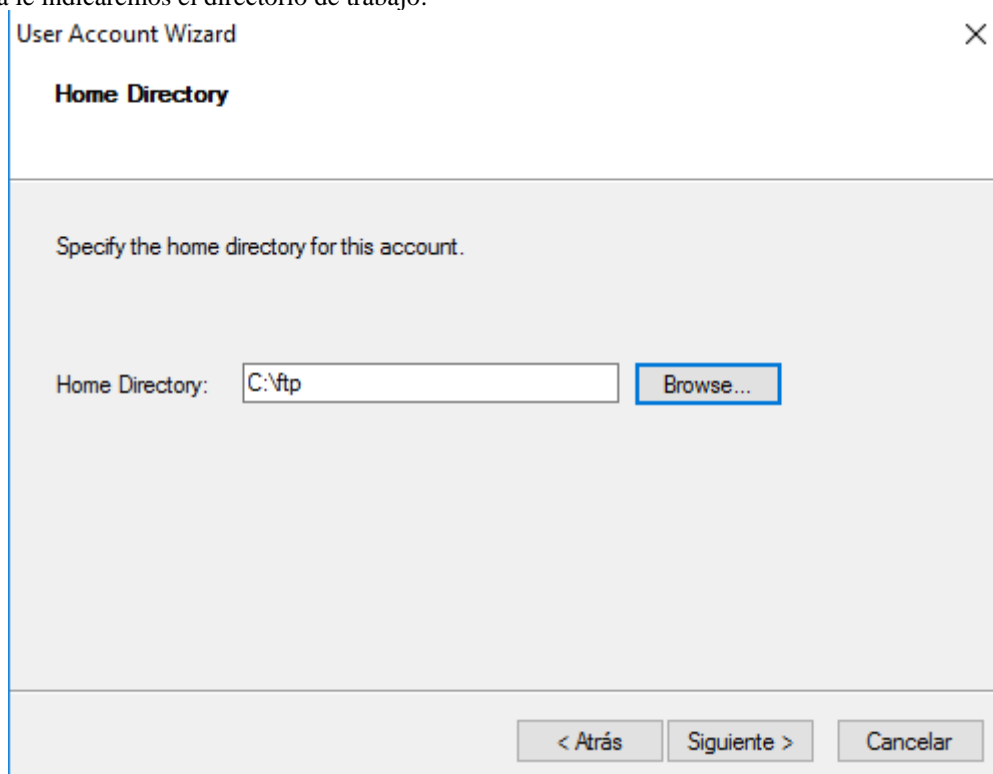
Type the password for this account and retype it to confirm.
If you don't want a password for this account, leave it blank. In this case any password will be accepted during login.

Password:

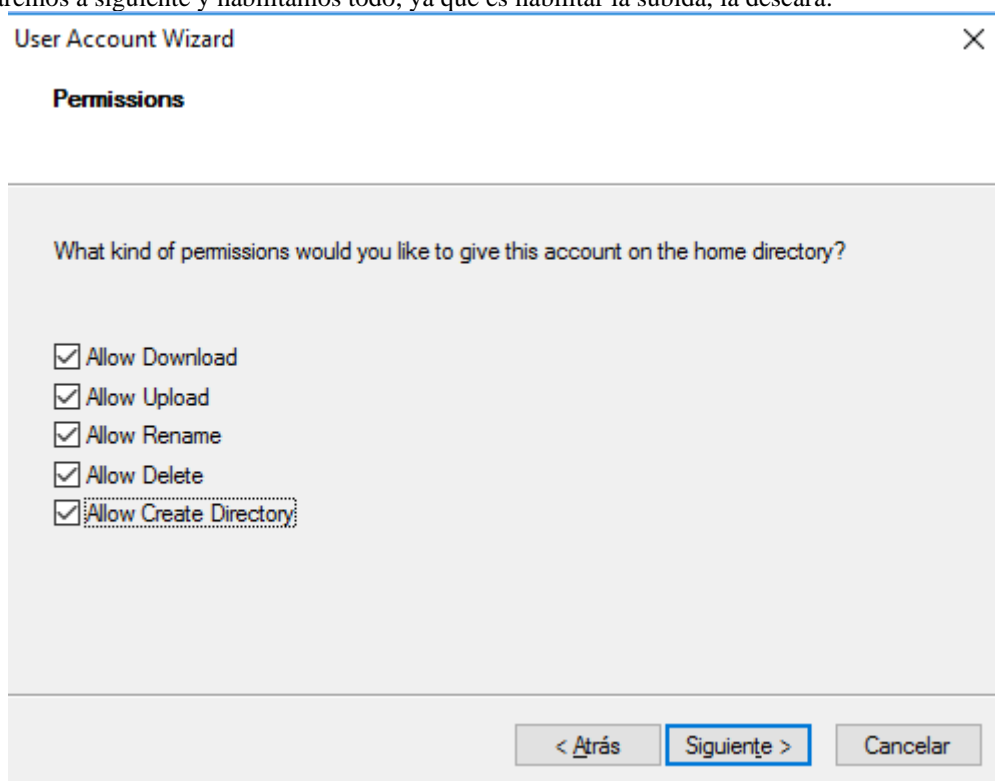
Confirm Password:

< Atrás **Siguiente >** Cancelar

Ahora le indicaremos el directorio de trabajo.

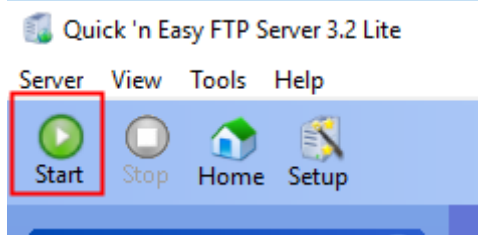


Le daremos a siguiente y habilitamos todo, ya que es habilitar la subida, la descara.

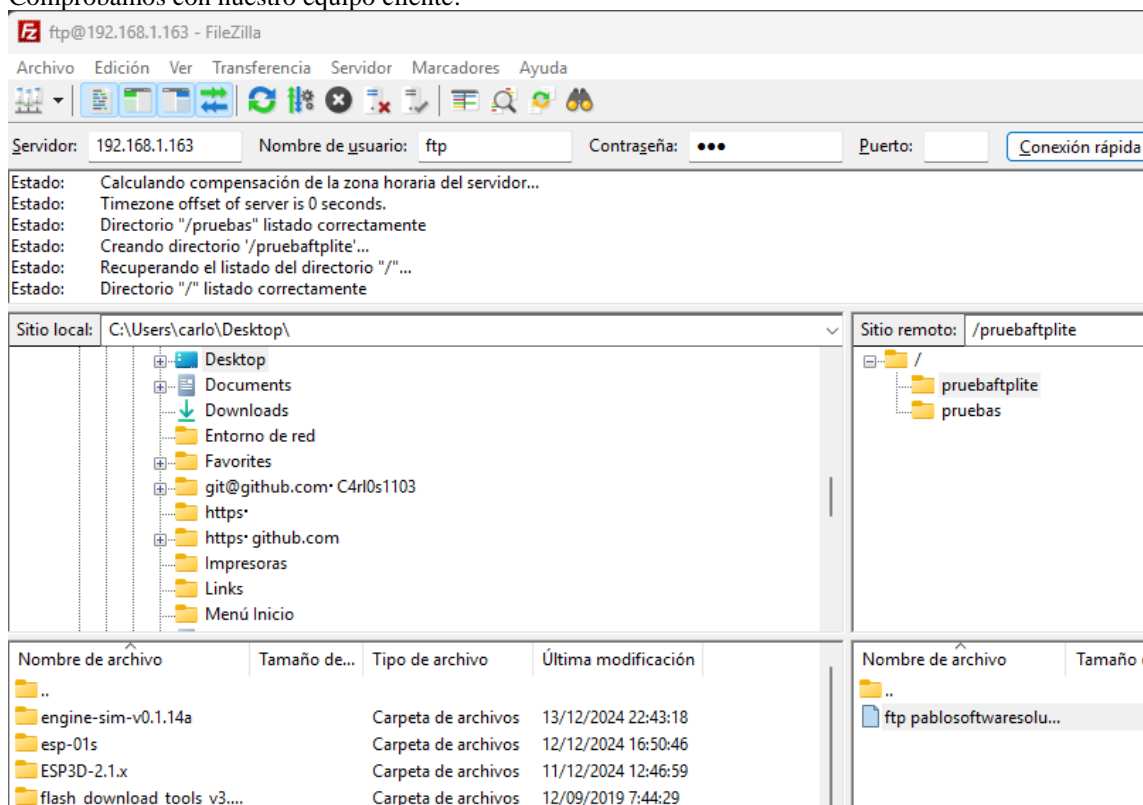


Y le daremos a finalizar.

Ahora iniciaremos el servicio.



Comprobamos con nuestro equipo cliente.



Y vemos que funciona correctamente.

12. Conclusión

La práctica permitió comprobar la eficacia del protocolo FTP para la transferencia de archivos tanto en Windows como en Linux, destacando sus diferencias técnicas. En Windows, las interfaces gráficas facilitan la configuración y el uso, mientras que en Linux, herramientas como vsftpd y comandos en terminal ofrecen mayor personalización y control. En ambos casos, es crucial implementar FTPS o SFTP y gestionar permisos correctamente para asegurar la protección de los datos. Esto asegura un funcionamiento adecuado adaptado a las necesidades de cada entorno.