

**ESCUELA POLITÉCNICA NACIONAL**

FACULTAD DE INGENIERÍA DE SISTEMAS

INGENIERÍA EN SISTEMAS INFORMÁTICOS Y DE COMPUTACIÓN

ADMINISTRACIÓN DE SISTEMAS OPERATIVOS

Y REDES

SEMESTRE 2017-B

TEORÍA Y PRÁCTICA DETALLADA

# FTP

21 DE DICIEMBRE DE 2017

REALIZADO POR:

TANIA MARICELA GUAMUSHIG AIMACAÑA

Contenido

[Servicios básicos FTP 0](#_Toc485223183)

[1. Objetivos 2](#_Toc485223184)

[2. Marco teórico 2](#_Toc485223185)

[FTP 2](#_Toc485223186)

[Transferencia de datos en FTP. 2](#_Toc485223187)

[El modelo FTP 3](#_Toc485223188)

[El cliente de FTP. 4](#_Toc485223189)

[El servidor de FTP. 4](#_Toc485223190)

[Servidores virtuales. 5](#_Toc485223191)

[Seguridad del servidor de FTP. 5](#_Toc485223192)

[3. Desarrollo de la práctica 7](#_Toc485223193)

[4. Análisis de resultados 17](#_Toc485223194)

[5. Conclusiones y recomendaciones 17](#_Toc485223195)

[6. Bibliografía 17](#_Toc485223196)

## **Objetivos**

• Conocer el funcionamiento de FTP cliente y servidor

• Configurar FTP en WINDOWS SERVER Y LINUX.

• Realizar la configuración de FTP en IPv4

• Definir rangos de funcionamiento de FTP

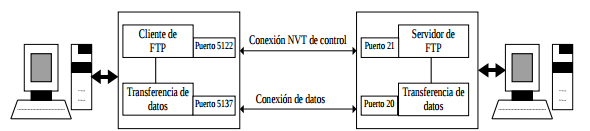
## **Marco teórico**

## FTP

El FTP es uno de los sistemas de almacenamiento y distribución de archivos más populares de Internet. La sencillez con la que se realizan el montaje y el acceso, permiten a cualquier usuario acceder a archivos y carpetas remotas, casi como si se tratara de su propio disco duro.

Para resolver estos problemas, se desarrolló el protocolo de transferencia de archivos (File Transfer Protocol). FTP es un programa muy básico para la transferencia de archivos entre ordenadores, pero a la vez es muy sencillo y fácil de usar, permitiendo ser utilizado de forma interactiva por un usuario, o bien, desde cualquier otra aplicación.

En FTP, un cliente de FTP establece una conexión con un servidor de FTP a través de lo que se conoce como conexión de control, siendo esta conexión de control una sencilla sesión de NVT1. El cliente envía los comandos al servidor a través de la conexión de control y el servidor envía respuestas al cliente a través de la misma.



## Transferencia de datos en FTP.

Además de los problemas del nombre de los archivos, etc., el principal problema existente en la transferencia de archivos entre ordenadores es el diferente formato que tienen los mismos datos en función del hardware y sistema operativo que se ejecute. Por tanto, en una transferencia de archivos entre dos ordenadores, ambos necesitan conocer el formato de los datos que van a transmitir y recibir.

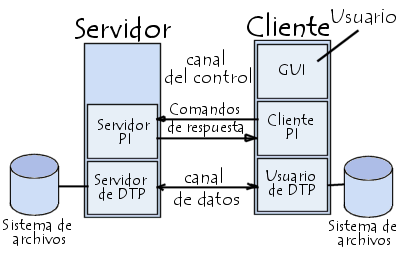
Para definir el formato de transferencia, FTP utiliza tres atributos: Tipo de los datos, estructura de los datos y modo de transmisión. El tipo de los datos que se van a transmitir se indica mediante el comando de control TYPE. Los tres tipos de datos más utilizados son texto ASCII, texto EBCDIC y datos binarios, siendo el tipo ASCII el establecido generalmente por defecto.

El envío de datos de tipo ASCII entre computadoras con distinto sistema operativo Linux/UNIX, Windows y MacOS, principalmente, posee el problema de la distinta codificación del final de línea, etc. Para evitar este problema, los archivos de texto son convertidos desde ASCII al formato de NVT en el emisor y de forma inversa en el receptor, con lo que el problema es subsanado. La transmisión de datos de texto EBCDIC se suele producir solo entre ordenadores IBM, de forma que en ellos no suceden los problemas que ocurren en los datos de tipo ASCII, por lo que los datos son enviados sin ser convertidos a NVT.

## El modelo FTP

El protocolo FTP está incluido dentro del modelo cliente-servidor, es decir, un equipo envía órdenes (el cliente) y el otro espera solicitudes para llevar a cabo acciones (el servidor).

Durante una conexión FTP, se encuentran abiertos dos canales de transmisión: un canal de comandos (canal de control) y un canal de datos:



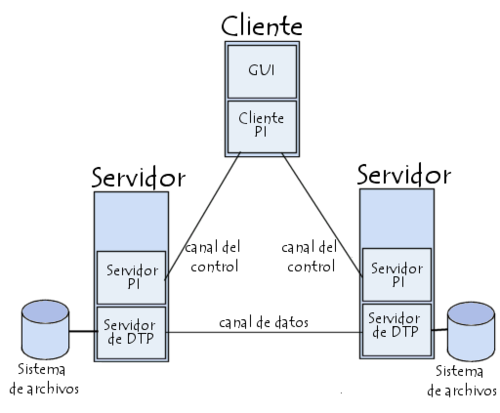
Por lo tanto, el cliente y el servidor cuentan con dos procesos que permiten la administración de estos dos tipos de información:

**DTP** (proceso de transferencia de datos) es el proceso encargado de establecer la conexión y de administrar el canal de datos. El DTP del lado del servidor se denomina SERVIDOR DE DTP y el DTP del lado del cliente se denomina USUARIO DE DTP.

**PI** (intérprete de protocolo) interpreta el protocolo y permite que el DTP pueda ser controlado mediante los comandos recibidos a través del canal de control. Esto es diferente en el cliente y el servidor. El SERVIDOR PI es responsable de escuchar los comandos que provienen de un USUARIO PI a través del canal de control en un puerto de datos, de establecer la conexión para el canal de control, de recibir los comandos FTP del USUARIO PI a través de este, de responderles y de ejecutar el SERVIDOR DE DTP. El USUARIO PI es responsable de establecer la conexión con el servidor FTP, de enviar los comandos FTP, de recibir respuestas del SERVIDOR PI y de controlar al USUARIO DE DTP, si fuera necesario.

Cuando un cliente FTP se conecta con un servidor FTP, el USUARIO PI inicia la conexión con el servidor de acuerdo con el protocolo Telnet. El cliente envía comandos FTP al servidor, el servidor los interpreta, ejecuta su DTP y después envía una respuesta estándar. Una vez que se establece la conexión, el servidor PI proporciona el puerto por el cual se enviarán los datos al Cliente DTP. El cliente DTP escucha el puerto especificado para los datos provenientes del servidor.

Es importante tener en cuenta que, debido a que los puertos de control y de datos son canales separados, es posible enviar comandos desde un equipo y recibir datos en otro. Entonces, por ejemplo, es posible transferir datos entre dos servidores FTP mediante el paso indirecto por un cliente para enviar instrucciones de control y la transferencia de información entre dos procesos del servidor conectados en el puerto correcto.



En esta configuración, el protocolo indica que los canales de control deben permanecer abiertos durante la transferencia de datos. De este modo, un servidor puede detener una transmisión si el canal de control es interrumpido durante la transmisión.

## El cliente de FTP.

En este punto nos limitaremos a exponer el uso interactivo del cliente de FTP por parte de un usuario. Una explicación de cómo usar el cliente FTP desde un programa de aplicación puede obtenerse mediante una consulta a las páginas de manual5 . Las funciones esenciales de transferencia de archivos permiten a los usuarios copiar archivos de un sistema a otro, ver listados de directorios y realizar tareas normales, como cambiar de directorio y cambiar el nombre o borrar un archivo.

El cliente de FTP se encuentra en /usr/bin/ftp.

## El servidor de FTP.

El servidor de FTP es el programa que se encarga de recibir las peticiones de los clientes y procesarlas. En la actualidad, existen, solo en Linux, varios servidores diferentes de FTP. Nosotros describiremos el Very Secure FTPD, que es un servidor con características añadidas que mejoran su seguridad.

El Very Secure FTP se encuentra en /usr/sbin/vsftpd, siendo, de forma clásica, ejecutado en el arranque del sistema y permaneciendo a la escucha del puerto 21 TCP. El servidor se encuentra configurado con unas opciones de funcionamiento por defecto, que pueden modificarse mediante los ficheros de configuración que se encuentren en el directorio /etc/vsftpd/. Generalmente, en dicho directorio solo existe un fichero, de nombre vsftpd.conf, que permite configurar el funcionamiento básico del servidor así como sus opciones de seguridad6 .

El formato del fichero vsftpd.conf es muy simple. Cada línea que comienza por el símbolo # es un comentario, mientras que el resto de líneas son directivas que configuran el funcionamiento del servidor. Las líneas de directivas tienen el formato: opcion=valor Donde es muy importante destacar que no debe ponerse ningún espacio entre la opción, el signo “=” y el valor. Las opciones que posee el servidor para su configuración pueden dividirse, para su estudio, en tres grandes grupos, opciones booleanas, opciones numéricas y opciones de cadena.

## Servidores virtuales.

Si un ordenador posee varios interfaces de red, es posible ejecutar varias instancias del servidor vsftpd de forma que cada una de ellas atienda las peticiones de un interfaz de red, especificando en el fichero de configuración de cada uno de los servidores las direcciones IP que escucha, los directorios que utiliza, etc. Por ejemplo, supongamos que tenemos un ordenador con dos interfaces de red, un interfaz con una dirección IP pública, por ejemplo 147.156.222.65, y el otro interfaz con una dirección privada, por ejemplo 192.168.1.1, de forma que queremos que el interfaz público atienda las peticiones de la red Internet, mientras que el interfaz privado atienda las peticiones de nuestra Intranet.

La configuración de estos dos servidores virtuales es tan sencilla como crear, dentro del directorio /etc/vsftpd dos ficheros, que llamaremos publico.conf y privado.conf10, donde especificaremos las opciones de cada uno de ellos, especialmente la dirección IP en la que permanecen a la escucha mediante la opción listen\_address que vimos con anterioridad.

## Seguridad del servidor de FTP.

Como hemos visto en las opciones de configuración, el servidor posee dos modos de funcionamiento, modo activo y modo pasivo. En la especificación original de FTP, el funcionamiento del servidor era en modo activo. Para ello, se definía el comando PORT como el método por defecto para establecer una conexión de datos, de forma que el servidor, desde su puerto TCP 20, intentaba establecer una conexión con la dirección IP y el puerto TCP del cliente que le había sido indicado por la conexión de control.

Este funcionamiento, que es seguro para el servidor, tiene un inconveniente, y es la presencia de un cortafuegos en el cliente, pues de forma general, muchas redes configuran sus cortafuegos de forma que no permiten el establecimiento de una conexión TCP a sus ordenadores, impidiendo el funcionamiento en modo activo del servidor.

**Acceso anónimo**

Los servidores FTP anónimos ofrecen sus servicios libremente a todos los usuarios, permitiendo acceder a sus archivos sin necesidad de disponer de ningún identificador. De esta forma todo el mundo tendrá acceso al servicio, pudiendo acceder a la información sin ningún tipo de restricción. Este usuario, por lo general, tiene privilegios limitados, ya que por lo general sólo podrá leer y copiar los archivos existentes, pero no podrá modificarlos ni crear otros nuevos.

**Acceso de usuario**

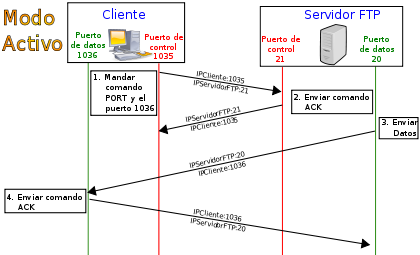
Este es el tipo de acceso más común dentro de los servicios de alojamiento que nos podemos encontrar. Con este tipo de usuarios, se dispondrá de un usuario y una clave para poder acceder al contenido, pudiendo así subir y bajar información. Es la forma más segura de utilizar este servicio, ya que en todo momento podremos sabe quién se ha conectado.

**Acceso de invitado**

Esta forma de conectarse vía FTP se trata de permitir que cada usuario conecte a la máquina mediante su login y su password, pero evitando que tenga acceso a partes del sistema de archivos que no necesita para realizar su trabajo, de esta forma accederá a un entorno restringido, algo muy similar a lo que sucede en los accesos anónimos, pero con más privilegios.

**Puerto de funcionamiento**

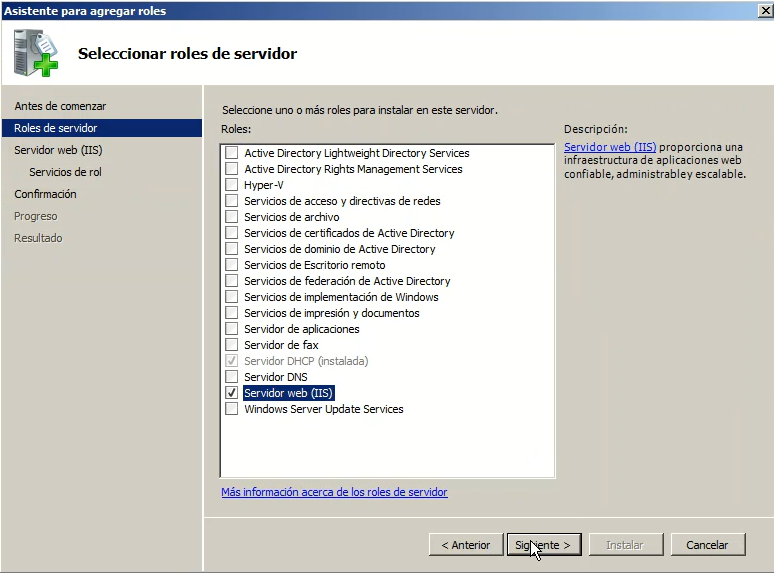
El servicio FTP es ofrecido por la capa de aplicación del modelo de capas de red TCP/IP al usuario, utilizando normalmente el puerto de red 20 y el 21.



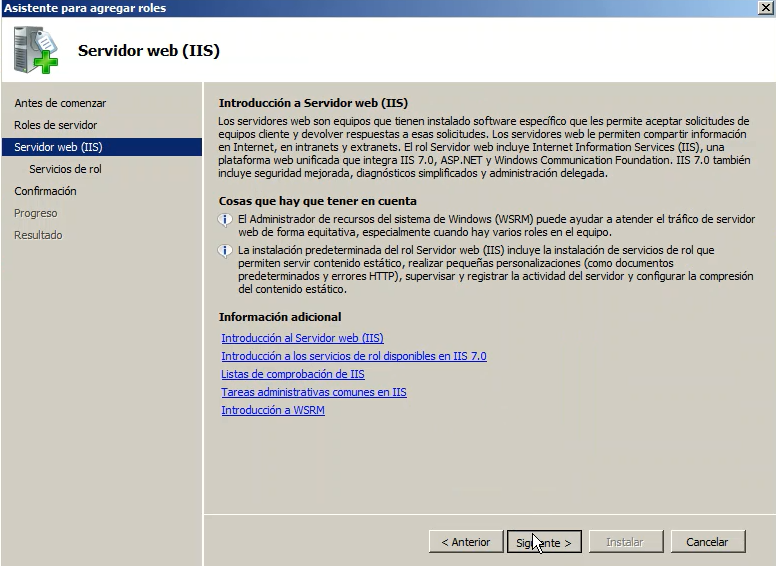
## **Desarrollo de la práctica**

**Configuración FTP en Windows Server**

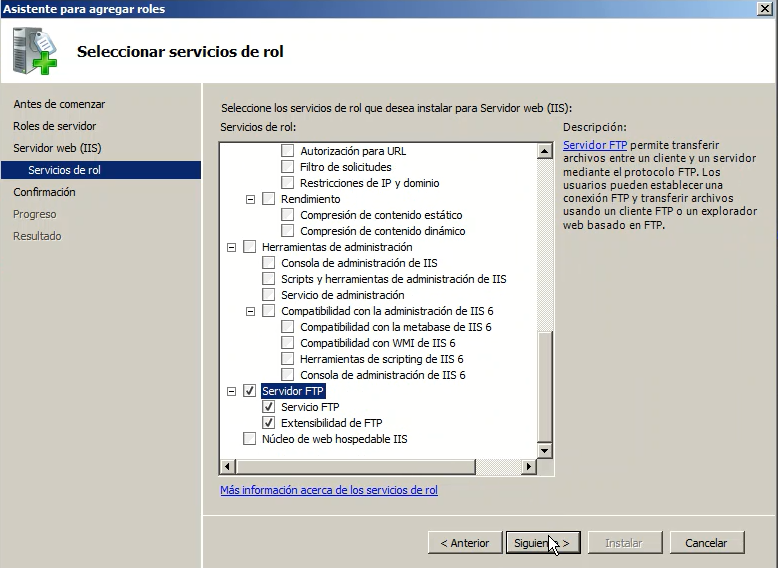
Se selecciona los roles de servidor en asistente para agregar roles.



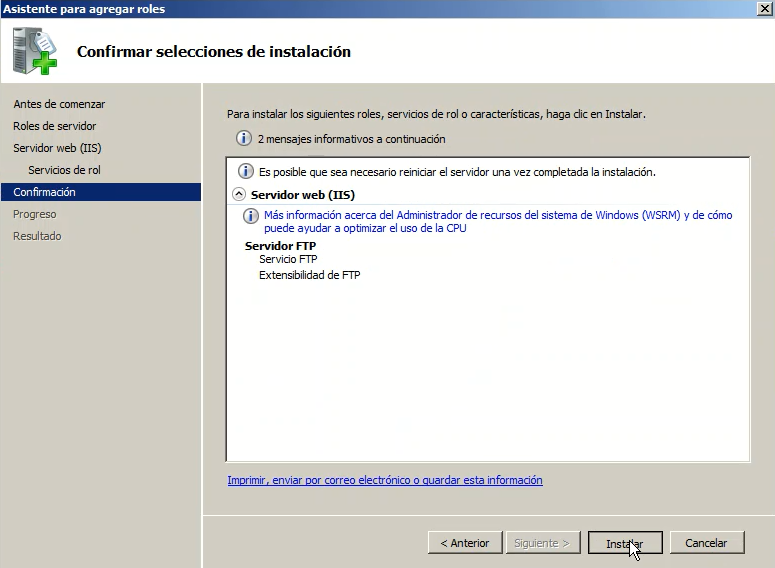
Se da clic en siguiente



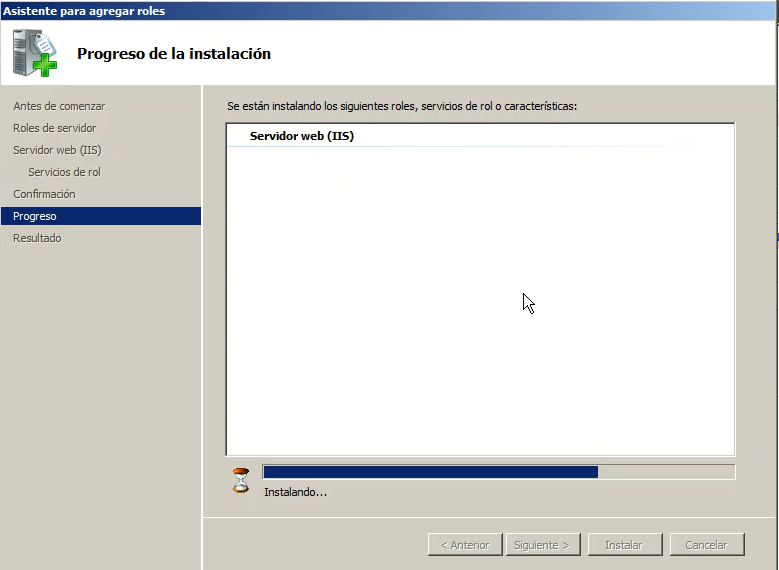
Se elige el servidor FTP y se da clic en siguiente.



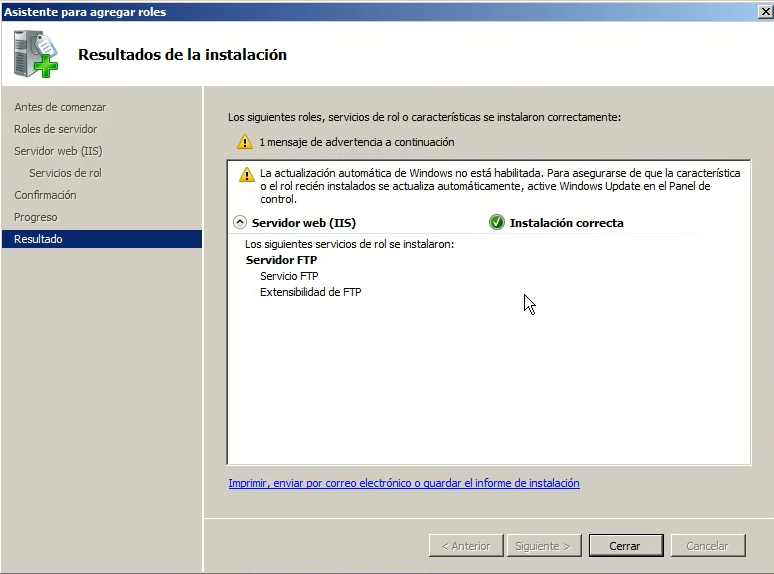
En configuración se confirma la instalación y se da clic en instalar.



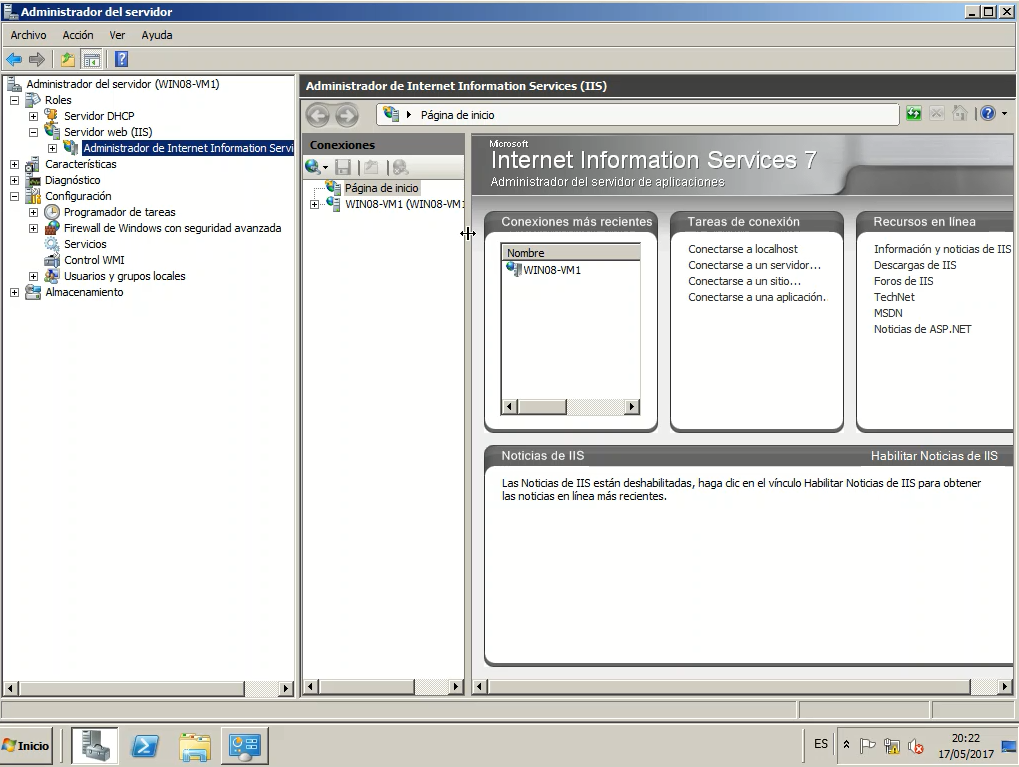
Luego se revisa el progreso de la instalación.



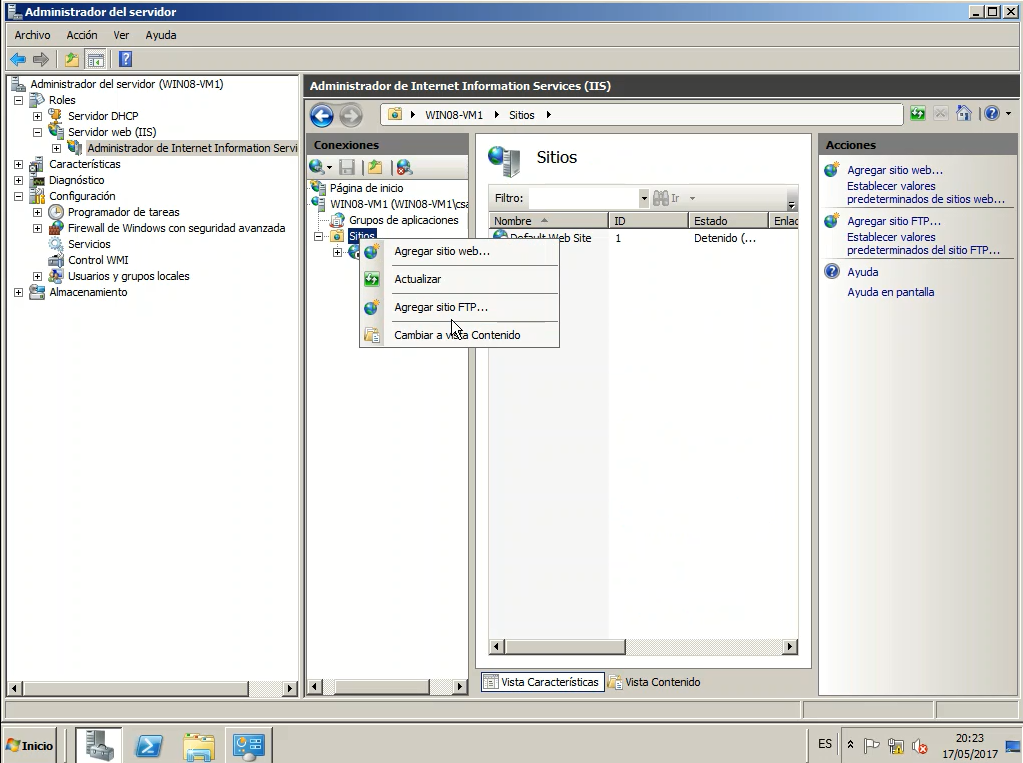
A continuación, se puede ver los datos de la instalación y se procede a dar clic en cerrar.



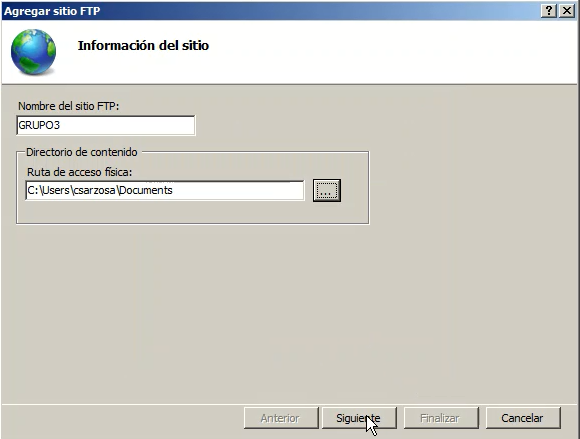
Se verifica en administrador del servidor la página web de inicio.



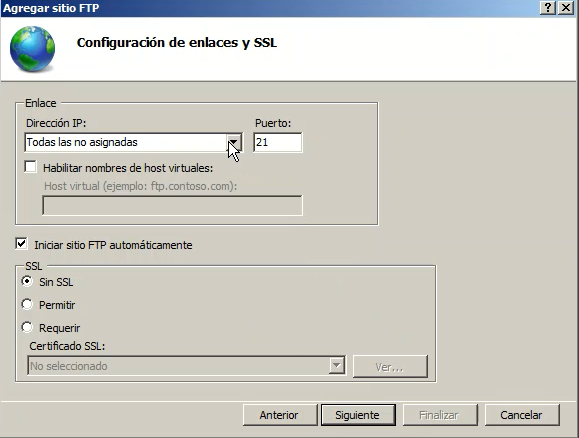
Se agrega un sitio FTP



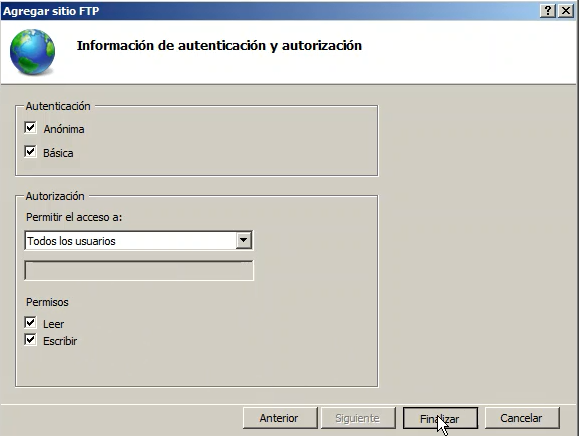
Se procede a escribir la información del sitio web.



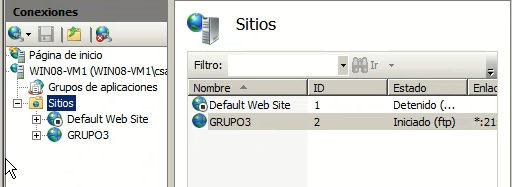
Se procede a ingresar la configuración SSL



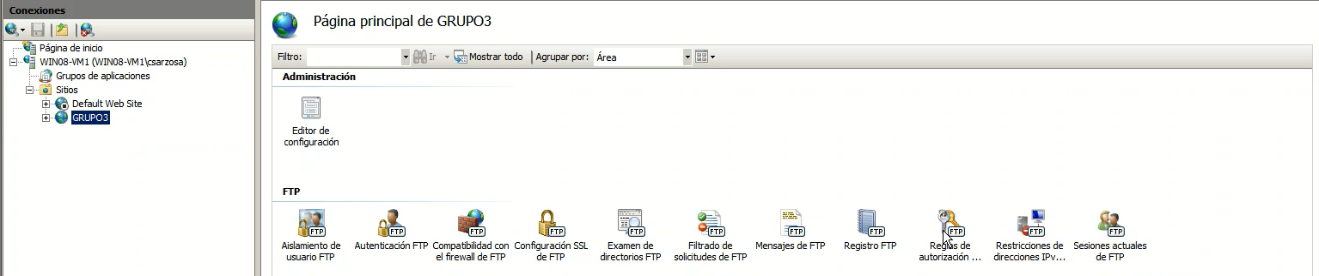
Se procede a marcar la información de autenticación y autorización.



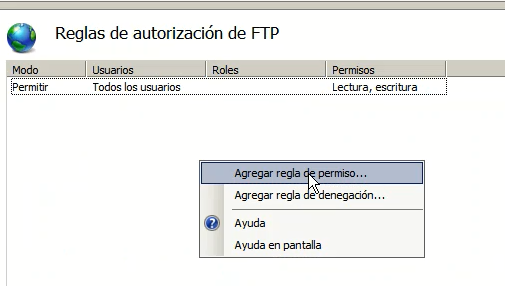
Se configura los sitios.



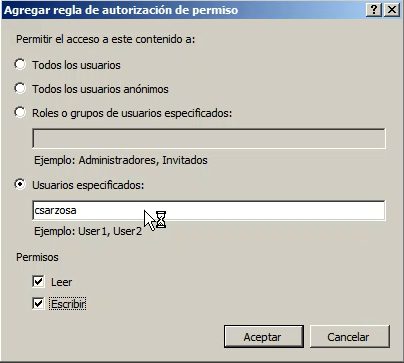
Se procede a editar a la configuración de los sitios.

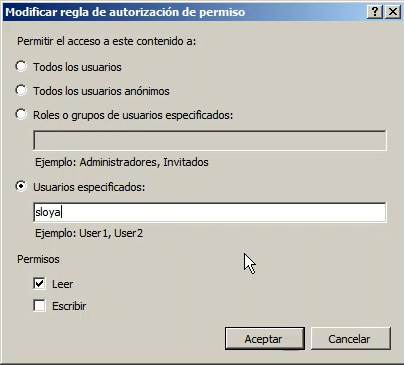


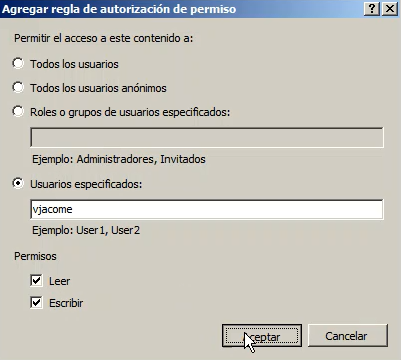
En las reglas de autorización se agrega una regla de permiso.



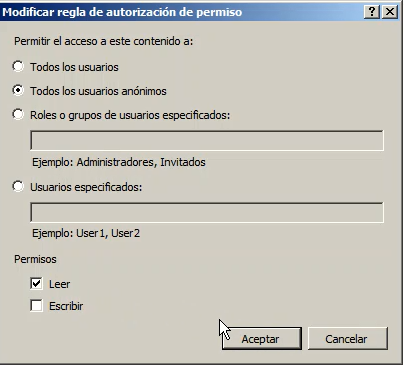
Se marcan los permisos que se van a otorgar a cada usuario.



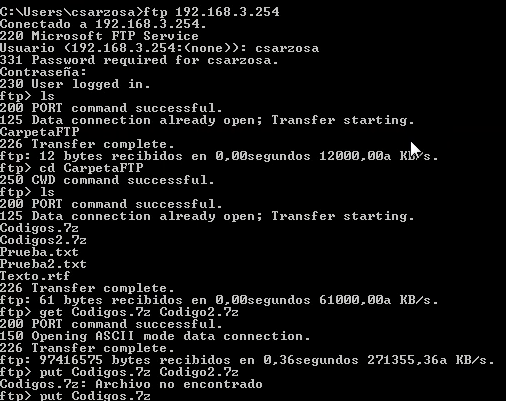


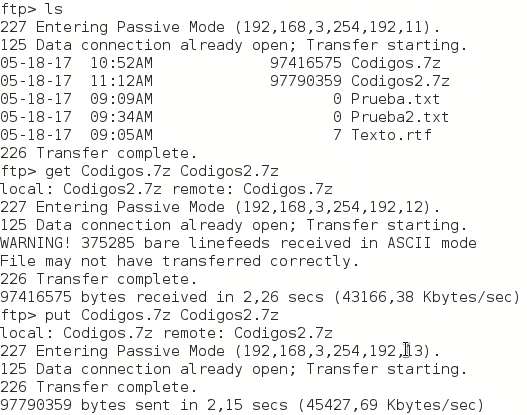


Se permite el acceso a todos los usuarios anónimos.

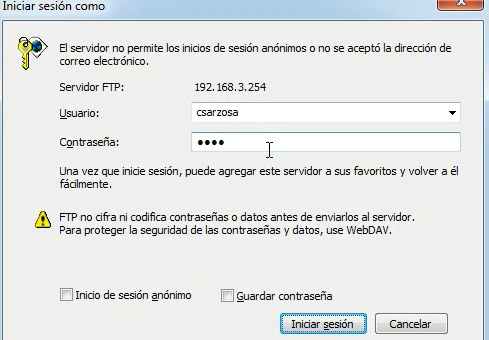


**Prueba FTP en Linux Server**

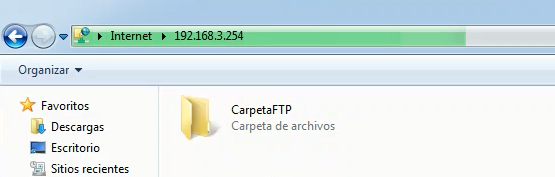




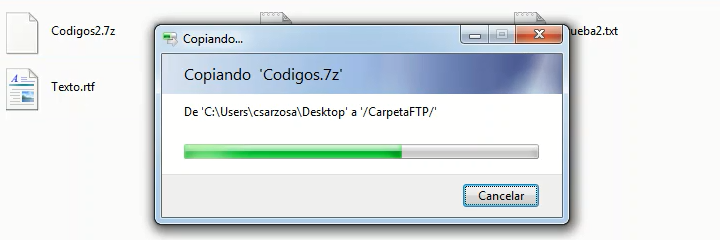
Se ingresan las credenciales.



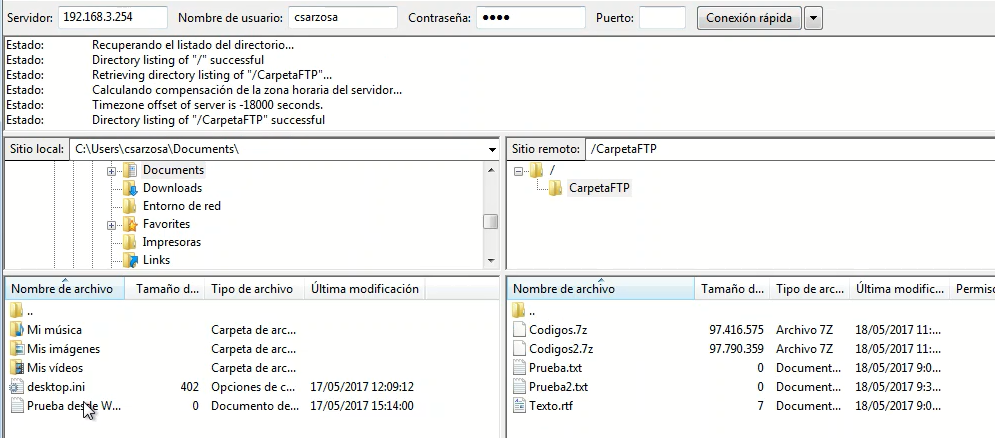
Se accede a la carpeta.



Se copian los elementos.

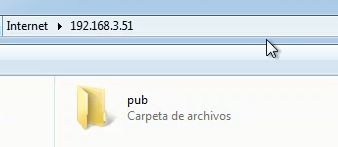


Se revisa el contenido



Se revisa la carpeta pública





## **Análisis de resultados**

* Se puede seleccionar cuales usuarios tienen permisos de lectura o escritura.
* FTP es una aplicación de software muy útil que puede tener un enorme beneficio para un sitio Web o de computación colaborativa en la que los archivos deben ser compartidos entre los socios comerciales.
* Para mejorar el rendimiento del servidor FTP, podemos establecer límites en la velocidad de descarga y subida.

## **Conclusiones y recomendaciones**

* FTP es un servidor que ayuda a que la configuración de archivos sea controlada de una manera adecuada entre usuarios.
* Ayuda a que las conexiones sean más pero no brinda una gran seguridad ya que no cuenta con ningún tipo de cifrado.
* Cuando se utiliza una red TCP/IP el protocolo FTP ayuda a definir la manera en que los datos deben ser transferidos a través de una red.

## **Bibliografía**

[1] Gil, 2010, P.Gil, J. Pomares, F.A. Candelas, “Redes y Transmisión de Datos”. Publicaciones Universidad de Alicante, 2010. Transparencias asociadas al libro en Repositorio de la Universidad de Alicante (RUA)

[2] Torres, 2001, F. Torres, F.A. Candelas, S.T. Puente, “Sistemas para la Transmisión de Datos”. 2º Edición. Publicaciones Universidad de Alicante, Alicante, 2001.

[3] Barcia, 2005, N. Barcia, C. Fernandez, S. Frutos, G. Gómez y otros, “Redes de computadores y arquitecturas de comunicaciones. Supuestos prácticos”. Prentice-Hall, Madrid, 2005.

[4] Beasley, 2008, J. S. Beasley, “Networking”. 2º Edición. Pearson Education, Michigan, 2008.

[5] Berná, 2002, J.A. Berná, M. Pérez, L.M. Cr3espo, “Redes de Computadores para Ingenieros en Informática”. Publicaciones Universidad de Alicante, Alicante, 2002.

[6] Cisco, 2008ª, “Academia de Networking de Cisco Systems: Guía del primer año CCNA 1 y 2”. 3º Edición. Cisco Press, Madrid, 2008.

[7] Cisco, 2008b, “Academia de Networking de Cisco Systems: Guía del segundo año CCNA 3 y 4”. 3º Edición. Cisco Press, Madrid, 2008.