**FTP:**

FTP es un protocolo de intercambio de archivos (anterior a Internet). A día de hoy todavía se utiliza en algunos contextos. Para intercambiar archivos entre usuarios suelen utilizarse más otras alternativas como el P2P o el alojamiento en la nube.

Hoy en día, es muy habitual emplear gestores de FTP como por ejemplo FileZilla o WinSCP, para subir los contenidos al hosting o administrar sus ficheros de forma segura.

Las siglas de FIP significan File Transfer Protocol, que se traduce como Protocolo de Transferencia de Archivos Como su nombre indica, se trata de un protocolo que permite transferir archivos directamente de un dispositivo a otro

El protocolo FTP tal cual es un protocolo inseguro, ya que su información no viaja cifrada Sin embargo, en 2001 esto se solucionó con el protocolo FIP/TLS, que le añade una capa SSH para hacerlo más seguro y privado.

Las conexiones FTP son cliente/servidor Esto quiere decir que un ordenador tiene que estar configurado como servidor FTP y el usuario se conecta a él como un cliente. En los ordenadores, los datos del protocolo FTP se envían a través de los puertos 20 y 21, que son los que están asignados en todos los equipos para llevar a cabo sus transferencias de archivos

**Seguridad FTP:**

FTP no es seguro. Se orientó a ofrecer la máxima velocidad en la conexión, pero debido a su antigüedad no fue diseñado con mecanismos de seguridad. Uno de los inconvenientes que tiene es que todo el intercambio de información se realiza en texto plano Todo el proceso, desde el login del usuario en el servidor, la transferencia de los archivos, etc., se realiza sin cifrar Por lo tanto, un posible atacante podria capturar este tráfico, acceder al servidor o hacerse con los archivos transferidos

Existen dos variantes de FTP que han sido desarrolladas para aplicar una capa segura sobre este protocolo, FTPS y SFTP.

**FtPS:** Se trata de una conexion FTP empleando el protocolo SSL. (Secure Socket Layers) © TLS (Transport Layer Security), estas conexiones utilizan un certificado de seguridad que cifra todo el proceso desde las identificacides, hasta el intercambio de ficheros Fillezilla te permite conectar usando tanto FTP como **FtPS**.

**SFTP:** SSH File Transfer Protocol emplea el protocolo SSH (Secure Shell) para cifrar el proceso de conexión y el intercambio de información entre el cliente y el servidor.

**Seguridad FTP Activo**

Es el funcionamiento por defecto. Para establecer la conexión para transferir los comandos, el cliente FTP abre un **puerto local superior a 1023 y se conecta al servidor a través del puerto 21/TCP** de este.

Una vez conectado, el cliente ya puede enviarle comandos al servidor y deberá establecer la conexión para transferir la información. Esto lo hará enviando el **comando PORT para especificar su dirección** IP y el número de puerto que abrirá para esa nueva conexión con el servidor que le escuchará a través del puerto 20/TCP

**Seguridad FTP Pasivo**

Para establecer la conexión para transferir los comandos, el cliente FTP abre un **puerto local superior a 1023 y se conecta al servidor a través del puerto 21/TCP** de este.

Una vez conectado, el cliente ya puede enviarle comandos al servidor, y deberá establecer la conexión para transferir la información. Esto lo hará mediante el envío del **comando PASV para activar el modo pasivo**; y el servidor le responderá un número de puerto superior a 1023 que tenga disponible, para que sea a este puerto al que se conecte el cliente a través de un nuevo puerto local superior a 1023.

**Usuarios FTP**

**Usuario anónimo**: usuario con una cuenta que suele llevar el nombre de anonymous y no dispone de contraseña. Normalmente este tipo de usuarios solo suelen tener permiso de lectura sobre los archivos para permitir su descarga.

**usuario registrado**: Debe existir en el servidor FTP. Este usuario puede ser de dos tipos, y los privilegios de los mismos se configuran en el propio Servidor. Usuario del sistema (existe en el ordenador) o usuario FTP (solo existe para el servicio FTP).

**Servidor de Aplicaciones**

Dispositivo de software que proporciona servicios de aplicación a las computadoras cliente. Un servidor de aplicaciones generalmente gestiona la mayor parte (o la totalidad) de las funciones de lógica de negociación y de acceso a los datos de las aplicaciones.

**Servidor de Aplicaciones**

* permiten implementar diferentes capas de la aplicación, como la interfaz de usuario, la lógica de negocio, la gestión de sesiones de usuario o el acceso a bases de datos remotas.
* Incluyen middleware (o software de conectividad) que les permite intercomunicarse con variados servicios, para efectos de confiabilidad, seguridad, no-repudio, etc.
* Ofrecen a los desarrolladores una Interfaz para Programación de Aplicaciones (API), de tal manera que no tengan que preocuparse por el sistema operativo o por la gran cantidad de interfaces requeridas en una aplicación web moderna.
* Dan soporte a una gran variedad de estándares, tales como HTML, XML, IIOP, JDBC, SSL, etc., que les permiten su funcionamiento en ambientes web (como Internet)
* Ofrecen conexión a una gran variedad de fuentes de datos, sistemas y dispositivos

**JavaDoc: ¿Qué es?**

JAVADOC, es una herramienta del SDK que permite documentar, de una manera rápida y sencilla, las clases y métodos que se proveen, siendo de gran utilidad para la comprensión del desarrollo.

**JavaDoc: y Etiquetas**

Un comentario de documento está escrito en HTML y debe preceder a

Declaración de:

clase,

campo,

constructor,

método.

Se compone de dos partes: una descripción seguida de etiquetas de bloque.

las etiquetas de bloque son:

@param

@return

@see.