UF1272: Administración y auditoría de los servicios web

Elaborado por: Belén Gisbert Vercher

Edición: 5.0

EDITORIAL ELEARNING S.L.

ISBN:978-84-16424-67-2 • Depósito legal: MA 726-2015

Impreso en España - Printed in Spain

Presentación

Identificación de la Unidad Formativa

Bienvenido a la Unidad Formativa **UF1272: Administración y auditoría de los servicios Web.** Esta Unidad Formativa pertenece al **Módulo Formativo MF0495_3: Administración de servicios Web** que forma parte del Certificado de Profesionalidad **IFCT0509: Administración de servicios de Internet**, de la familia de **Informática y Comunicaciones**.

Presentación de los contenidos

La finalidad de esta Unidad Formativa es enseñar al alumno a administrar y auditar los servicios Web para asegurar y optimizar su rendimiento e instalar, configurar y administrar el servidor de aplicaciones y la conexión con sistemas gestores de bases de datos.

Para ello, en primer lugar se estudiará la administración de contenidos del servidor Web, el servidor de aplicaciones de servicios Web y el acceso a sistemas gestores de bases de datos. También se analizará la descripción de arquitecturas distribuidas en múltiples servidores, la gestión de actualizaciones de servidores y aplicaciones, y por último, la auditoría y resolución de incidentes sobre servicios Web.

Objetivos de la Unidad Formativa

Al finalizar esta Unidad Formativa aprenderás a:

– Administrar los contenidos gestionados por el servidor Web, los accesos realizados y el rendimiento según especificaciones de diseño normativa de la organización y legislación vigente.

– Instalar, configurar y administrar el servidor de aplicaciones en el sistema informático como proveedor de datos para los servicios Web.

– Seleccionar, instalar y configurar los métodos de acceso a sistemas gestores de bases de datos para utilizar sus recursos en sitios Web dinámicos.

– Aplicar procedimientos de auditoría y resolución de incidencias en la explotación de un servicio Web.

Índice

UD1. Administración de contenidos del servidor web 9

1.1. Procedimientos de actualización de contenidos 11

1.1.1. FTP 13

1.1.2. FTPS 29

1.1.3. SFTP 43

1.1.4. Introducción a sistemas de gestión de contenidos (CMS) 56

1.2. Organización de contenidos 58

1.3. Control de versiones 60

1.4. Técnicas de gestión de permisos 62

1.4.1. Perfiles 70

1.4.2. Grupos 72

1.4.3. Roles 74

1.5. Procedimientos de optimización del rendimiento del servidor Web 76

1.5.1. Técnicas de optimización 78

1.5.2. Parámetros de calidad de servicio y usabilidad 80

1.5.3. Pruebas de optimización 84

1.5.4. Simulación de generación de carga Web con herramientas específicas 86

1.6. Servidores de estadísticas..... 87
1.6.1. Estructura y campos de un fichero de log 89
1.6.2. Concepto de sesión 146
1.6.3. Mecanismos de seguimiento de sesiones..... 148
1.6.4. Instalación de un analizador de logs sencillo..... 149
1.7. Normativa legal relacionada con la publicación de contenidos Web 161
1.7.1. Salvaguarda de logs 162
1.7.2. LOPD..... 164

UD2. Servidor de aplicaciones de servicios web 175

2.1. Descripción de funciones y parámetros de configuración..... 177
2.1.1. Parámetros recomendados según el escenario..... 237
2.2. Procedimientos de implantación 240
2.2.1. Comprobación de arranque, funcionamiento y parada 247
2.2.2. Verificación de la instalación 249
2.3. Análisis y elaboración de la documentación de operación.... 252

UD3. Acceso a sistemas de bases de datos..... 263

3.1. Motores de base de datos de uso más frecuente en aplicaciones web (ORACLE, SQL Server, MySQL) 265
3.1.1. Protocolos de acceso..... 373
3.1.2. Modelos de seguridad (por IP, por usuario contraseña, seguridad integrada, combinación de estas...).. 375
3.2. Bibliotecas de acceso..... 377
3.2.1. ODBC, JDBC, DSN-Less ODBC, Ole DB..... 378
3.2.2. Implantar módulos de acceso (instalar controladores ODBC, crear un DSN...)..... 380

3.3. Mecanismos de comunicación en una arquitectura web en tres capas 386

3.3.1. SOAP, RPC, WebServices 387

3.4. Verificación de la conexión a la base de datos 389

UD4. Descripción de arquitecturas distribuidas en múltiples servidores 399

4.1. Modelo de tres capas 401

4.2. Tolerancia a fallos 435

4.3. Reparto de carga 527

4.4. Almacenes de estado de sesión (ASP.NET State Service…) 529

4.5. Almacenes de caché (Memcached…) 530

4.6. Servidores proxy 534

UD5. Gestión de actualizaciones de servidores y aplicaciones 543

5.1. Entorno de desarrollo y preproducción 545

5.2. Procedimientos de despliegue de actualizaciones 552

UD6. Auditoría y resolución de incidentes sobre servicios web .. 563

6.1. Medición de la calidad del servicio prestada 565

6.1.1. Parámetros de calidad 569

6.1.2. Disponibilidad del servicio 570

6.1.3. Acuerdos de prestación de servicio (SLAs) 572

6.2. Gestión de vulnerabilidades en aplicaciones web 574

6.2.1. Herramientas de detección de vulnerabilidades en aplicaciones web (p.e. Nikto) 580

6.3. Diagnóstico de incidentes en producción..... 585
6.3.1. Monitorización 590
6.3.2. Herramientas de medición del rendimiento (contadores del sistema Windows, Apache mod_status...)..... 593
6.4. Técnicas de resolución de incidentes..... 600
6.4.1. Medidas de contención. Workarounds..... 602
6.4.2. Análisis causa–raíz 605
6.4.3. Gestión proactiva de problemas 612

Glosario 621

Soluciones 627

UD1

Administración de contenidos del servidor web

1.1. Procedimientos de actualización de contenidos
- 1.1.1. FTP
- 1.1.2. FTPS
- 1.1.3. SFTP
- 1.1.4. Introducción a sistemas de gestión de contenidos (CMS)

1.2. Organización de contenidos

1.3. Control de versiones

1.4. Técnicas de gestión de permisos
- 1.4.1. Perfiles
- 1.4.2. Grupos
- 1.4.3. Roles

1.5. Procedimientos de optimización del rendimiento del servidor Web
- 1.5.1. Técnicas de optimización
- 1.5.2. Parámetros de calidad de servicio y usabilidad
- 1.5.3. Pruebas de optimización
- 1.5.4. Simulación de generación de carga Web con herramientas específicas

1.6. Servidores de estadísticas
- 1.6.1. Estructura y campos de un fichero de log
- 1.6.2. Concepto de sesión
- 1.6.3. Mecanismos de seguimiento de sesiones
- 1.6.4. Instalación de un analizador de logs sencillo

1.7. Normativa legal relacionada con la publicación de contenidos Web
- 1.7.1. Salvaguarda de logs
- 1.7.2. LOPD

1.1. Procedimientos de actualización de contenidos

Un **servidor web** es un programa informático que procesa una aplicación que tiene que ver con dicho servidor, por lo que puede realizar dos tipos de conexiones: unidireccionales y bidireccionales. A su vez, estas conexiones pueden ser: síncronas o asincrónicas hacia el cliente que lo esté usando, por lo que puede hacer una respuesta en cualquier idioma.

Cuando el cliente lo requiera, todo **servidor web** puede ofrecer y responder a sus peticiones mediante una **página web** expuesta en un navegador.

Por otra parte, es como un sitio o lugar donde se alojan aplicaciones o sitios por medio de un navegador que se comunica con el servidor. Todo ello por medio del **protocolo HTTP.**

El servidor web puede ser un lugar donde se alojen lasa aplicaciones o sitios mediante un navegador que se comunica con el servidor, generalmente mediante el protocolo HTTP perteneciente a la capa de aplicación del modelo OSI.

¿Cómo se ejecuta el servidor web en un ordenador?

Se mantiene **esperando peticiones de un cliente** mediante una página web que se exhibe en el navegador o mostrando un mensaje de error si se detecta. Por ejemplo, si tecleamos en el navegador cualquier www, éste realiza una petición **HTTP** al servidor de dicha dirección. El servidor le envía al cliente el HTTP y éste lo interpreta en su pantalla, mostrando fuentes, colores y la colocación d objetos y textos. El servidor sólo se limita a transferir el código de la página sin llevar a cabo ninguna interpretación de la misma.

Además los servidores web pueden entregar **aplicaciones web**, las cuales son porciones de código que se ejecutan cuando se realizan ciertas peticiones o respuestas HTTP.

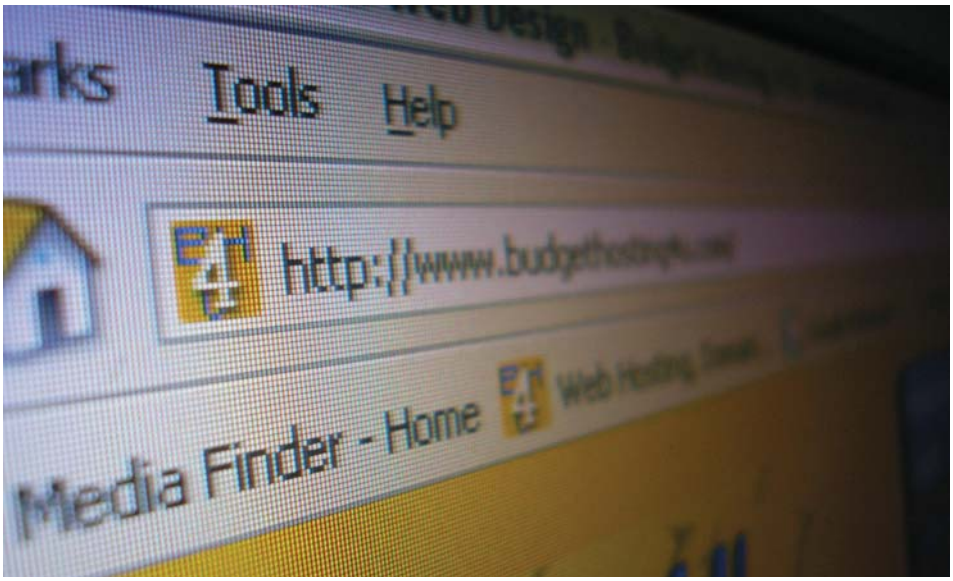
Existen dos tipos de aplicaciones web:

- **Aplicaciones en el lado del cliente**: el cliente web es el encargado de ejecutarlas en el ordenador o dispositivo del usuario. Por ejemplo: las aplicaciones tipo Java o JavaScript.
- **Aplicaciones en el lado del servidor**: el servidor web ejecuta la aplicación; y después se genera un código **HTML**; el servidor toma este código recién creado y lo envía al cliente por medio del protocolo HTTP.

El hecho de que HTTP y HTML estén íntimamente ligados no debe dar lugar a confundir ambos términos. HTML es un lenguaje de marcas y HTTP es un “protocolo”.

Para poder poner al día alguna aplicación o proceso de los programas que hayan podido quedarse atrasados, simplemente bastará con estar provisto de la información y las indicaciones, de forma que el proveedor pueda hacerse cargo de procesar, seleccionar, redactar y publicar el material en su sitio web periódicamente conforme a lo que indiquen los usuarios, como norma general.

En los subpuntos que vamos a indicar a continuación, podremos ver los diferentes **procesos de actualización** de los diferentes servidores web, de manera que llevándolos a cabo, podremos hacer las actualizaciones que corresponden.



Servidor web: buscador con http

1.1.1. FTP

FTP son las siglas en ingles de "**File Transfer Protocol**", que en español significa "Protocolo de Transferencia de Archivos" en informática. FTP es un **protocolo de red creado para la correcta transferencia de archivos** entre sistemas conectados a una misma **red TCP**, que significa "Transmission Control Protocol", en español: Protocolo de control de transmisión, el cual está basado en la arquitectura de cliente y servidor.

Desde el equipo del cliente, se puede conectar a un servidor para que pueda enviar archivos o para descargarlos desde él. El **sistema operativo** que se utilice en cada equipo **es indiferente**.

Protocolo de Transferencia de Archivos FTP

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

Problema que normalmente surge en FTP y como solucionarlo

FTP suele presentar un tipo de **problema**: éste está pensado para ofrecer una conexión de máxima velocidad, pero no es así en **la seguridad**, ya que se intercambia todo tipo de información (login, password, etc) del usuario dentro del servidor hasta que se complete la transferencia del archivo y en texto sin cifrarse, por lo que ese tráfico y transferencia se puede capturar, apropiarse de los datos personales o de seguridad, acceder al servidor y, finalmente, robar los archivos privados.

Para **solucionar este problema,** son de gran utilidad aplicaciones como **SCP** (**Secure Copy o SCP** es un medio de transferencia segura de archivos informáticos entre un host local y otro remoto o entre dos hosts remotos, usando el protocolo **Secure Shell (SSH))** y **SFTP (SHH File Transfer Protocol,** completamente diferente a **FTP)**, incluidas en el paquete **SSH (Secure SHell,** en español: intérprete **de órdenes segura, es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red)**, que permiten transferir archivos pero cifrando todo el tráfico.

El servidor FTP

El **servidor FTP** es un programa que se ejecuta en un servidor, el cual está conectado a **internet** y también a otro tipo de redes, tales como: LAN. El servidor FTP permite el **intercambio de datos** entre distintos ordenadores y/o servidores.

Normalmente, este programa-servidor FTP no se encuentra en ordenadores personales, sino que deben conectarse a uno remoto para así poder intercambiar información.

Los servidores FTP suelen proporcionar **alojamiento web** o suelen hacer el papel del **servidor backup** en empresas para guardar y subir archivos de cierta importancia. Por lo tanto, existen los protocolos **SFTP**, cuyos **datos se transmiten cifrados**.

La historia de FTP

El **primer Internet** fue utilizado por científicos de la informática, ingenieros, físicos, y bibliotecarios. No había nada “fácil de usar” al respecto. No había ordenadores personales en aquellos días, y cualquiera que lo utilizó, tuvo que aprender a usar un complicado conjunto de comandos que son específicos de cada sistema. Quedó claro que para transferir archivos de un sistema a otro, era necesario un conjunto de comandos estándar (un protocolo).

El **protocolo FTP**, permitiendo la transferencia de archivos entre sistemas remotos, fue publicado por primera vez como una "solicitud de comentarios" (una colección de notas técnicas y organizativas sobre Internet), el 16 de abril de 1971. Desde su creación, FTP ha sido el protocolo estándar utilizado para transferir archivos entre ordenadores remotos. Los desarrolladores del protocolo de transferencia de archivos (FTP), tuvieron que equilibrar la necesidad de un amplio conjunto de funcionalidad, con el deseo de un protocolo que era simple y fácil de implementar. **RFC 959**, Protocolo de transferencia de archivos (FTP), se publicó en octubre de 1985.

Revisar los FTP, incluyendo la adición de nuevos comandos, ahora es la base de la especificación para FTP. Desde entonces, una serie de otras normas se han publicado y definen otras extensiones, como mejores medidas de seguridad. Este **conjunto de normas** todavía se utilizan hoy en día.

Software de cliente FTP

Un **cliente FTP** es una **pieza de software** que se debe instalar en tu ordenador con el fin de conectarse a un **servidor FTP**. Este software gestiona toda la complejidad del **protocolo FTP** Es fácil de usar, apuntar y hacer clic, así como arrastrar y soltar las aplicaciones con gráficos front-end a las interfaces de línea de comandos muy ligeros. Muchos navegadores de Internet (Internet Explorer, Mozilla, Opera, etc.) incluso tienen clientes simples que se han construido en el derecho. Hay un gran número de **clientes de software de FTP** disponibles en la actualidad. Todos con sus propias ventajas y desventajas. Algunos de los más populares son:

- **WS_FTP:** Proporciona una interfaz totalmente gráfica para conectar y transferir archivos. Soporta todos los tipos básicos de conexiones.

- **CuteFTP:** Proporciona una interfaz totalmente gráfica para conectar y transferir archivos. Soporta todos los tipos de conexión que incluye seguro en la versión Pro.

- **FTP Voyager:** Proporciona una interfaz totalmente gráfica para conectar y transferir archivos. Soporta todos los tipos de conexión que incluye seguro.

- **Java_Applets:** Proporciona una interfaz totalmente gráfica para conectar y transferir archivos. Soporta todos los tipos de conexiones seguras. Este tipo de cliente está creciendo en uso. No requiere que el usuario instale ningún software en su máquina en absoluto. Sólo se necesita un **Java habilitado para Navegador de Internet** .La mayoría de los navegadores modernos, como Microsoft Internet Explorer, pueden ser configurados por el administrador del sitio en sí FTP, por lo que no hay ninguna configuración en el lado del usuario. **MTFTP.com** ofrece una demostración de este tipo de cliente.

Tipos de Conexiones FTP

Aunque las conexiones pueden variar, todas las **conexiones FTP** consisten en un **sistema de dos puertos**. Existe el **Puerto Comando** (a veces llamado el Puerto de control, basado en Telnet) para enviar y recibir todos los comandos, y hay un **puerto de datos** (utilizando el protocolo TCP) para transferir datos (es decir: archivos, directorios). Las conexiones FTP pueden variar en función de cualquiera de estos tres factores:

– **Modos de conexión:** A veces, estos son llamados **modos de transferencia**, pero para mayor claridad se llama modos de conexión.

  El modo de conexión se establece en el comienzo mismo de cualquier transacción FTP. Este modo depende de qué tipo de estructura de archivos utiliza el servidor. La mayoría de los sistemas modernos utilizan una **estructura de archivos binarios**. Algunos sistemas UNIX o Mainframe mayores, pueden utilizar una estructura de archivos ASCII. En la mayoría de los casos, este modo se decide por el servidor y el software de cliente detecta automáticamente cuál de estos dos modos se pueden usar.

– **Modos de transferencia:** Hay dos tipos de modos de transferencia que especifican cómo y dónde se transmiten los datos hacia y desde el cliente. **Active** es el método por defecto utilizado en la mayoría de los casos, sin embargo, en algunos casos en los que un servidor de seguridad se está utilizando una conexión pasiva, puede resolver los problemas con los puertos que está bloqueando los comandos. Estos dos tipos de modos de transferencia tienen diferencias en cómo se transfieren los datos:

  · **Activo (Especificado con el comando Port)**

    Con **ftp activo**, **el cliente especifica al servidor cómo se realizará la transferencia**. El cliente elige un puerto y le dice al servidor cual es para enviar los datos a la misma. El servidor inicia una conexión con el cliente en ese puerto y envía los datos.

    Muchas veces hay **un problema** con el modo activo. Cada ordenador conectado a Internet tiene una dirección IP única asignada. Esta dirección IP única es cómo se identifican los ordenadores para enviar y recibir datos a través de Internet. Por razones de seguridad y otras, muchas redes de la empresa tienen una única dirección IP para toda su red. **Esta dirección IP se asigna uno a un router**. A cada equipo se le asigna una **dirección IP local**. Todo el tráfico de Internet se envía al router. El router reenvía el tráfico saliente de Internet utilizando su dirección IP. El router también recibe todo el tráfico y la encamina al ordenador correcto en la red de Internet entrante. Cada equipo individual en la red sólo sabe la dirección IP local.

Como se indicó anteriormente, con el modo activo, **el cliente elige el puerto**. El cliente envía su puerto junto con su dirección IP al servidor para establecer la conexión de datos. Debido a que el cliente envía su dirección IP local, el servidor intenta establecer la conexión de datos utilizando la dirección IP local. Esta dirección IP local no es accesible desde Internet porque el intento de conexión falla. La solución al problema es utilizar el modo pasivo.

- Pasivo (Especificado con el comando Pasv)

  Con transferencias pasivas, el cliente pide la conexión al servidor de datos y el servidor especifica cómo se hará la transferencia. El servidor elige un puerto y luego le dice al cliente que se conecte a ese puerto para recibir los datos.

– Tipos de cifrado

- SSL

  El cifrado es una forma de proteger los datos mientras se están transfiriendo. Hay varias maneras de cifrado de datos en una transferencia FTP.

  El método más común es el uso de **SSL** (Secure Socket Layer). SSL es un protocolo desarrollado por Netscape en 1994 para transmitir documentos de forma segura a través de Internet. SSL utiliza un sistema criptográfico que utiliza dos claves distintas para cifrar los datos. Hay una **clave pública** conocida por todos y una **clave privada**, conocida sólo por el destinatario del mensaje. Por supuesto, esto es manejado por el propio protocolo.

  Tipos de SSL

  › Implícito

    SSL implícito se utiliza para requerir los clientes FTP para ser "SSL habilitado." Con SSL implícito, la conexión se configura inmediatamente para la comunicación segura y sin texto claro se pasa entre el cliente y el servidor en cualquier momento. Estos servidores generalmente se ejecutan en el puerto 990. **El acceso s**ólo se **permitirá a los clientes que admiten SSL**. También no es necesario ningún comando AUTH cuando se utiliza SSL implícito, ya que todas las conexiones de control y de datos están seguras.

› Explícito

SSL explícito se utiliza para **proporcionar acceso a una mezcla de clientes FTP**. Con SSL explícito, la conexión comienza como cualquiera conexión FTP regular (sin cifrar). El cliente FTP tiene la opción de continuar **sin cifrar**, como una sesión de FTP regular, o emitir el comando AUTH y cambiar a modo secure-FTP. Además, cuando un usuario solicita datos confidenciales, el servidor puede luego pedir al cliente actualizar a una conexión segura. L**a ventaja de SSL explícito es que no se requiere SSL del cliente**, por lo que los clientes de más edad podrán acceder al servidor.

· SFTP (Secure FTP)

SFTP no es FTP (un programa que se puede ejecutar a través de una conexión Secure Shell (SSH)) .En una conexión SSH, todas las operaciones se realizan de forma cifrada utilizando la autenticación de clave pública y compresión. **SFTP es un programa de transferencia de archivos interactivo**, similar a FTP. Se conecta y se registra en un host especificado, entonces entra a modo de comando interactivo como FTP. La diferencia es que **SFTP sólo se puede utilizar en una conexión SSH**. Una conexión Secure Shell (SSH), da al usuario más poder que una conexión FTP. SFTP es sólo uno de muchos programas en un servidor que se pueden ejecutar a través de una conexión SSH. Normalmente, SSH es utilizado por el personal de TI para administrar un servidor. La copia y descarga de archivos es sólo una de las muchas cosas que tienen que hacer y SFTP proporciona una forma de hacer precisamente eso.

· TLS (Transport Layer Security)

SSL ha existido por durante más de una década. **TLS se supone que es el sucesor de SSL** y está basado en SSL 3.0. Fue desarrollado principalmente por lo que la **IETF (Internet Engineering Task Force)** y podría tener un estándar abierto, apoyada por la comunidad y que podría ser ampliado con otros estándares de Internet. Por desgracia, no hay mucho desarrollo con TLS. No hay muchas diferencias entre SSL y TLS. Sin embargo, **no inter operan**, pero TLS pueden transformarse en SSL3 si es necesario. Al igual que SSL, tanto de forma explícita como implícita, se puede utilizar con TLS. **SSL sigue siendo la norma.**

Comandos

Los **comandos** son el cómo se realiza la comunicación entre cliente y servidor. Todos los servidores FTP admiten un conjunto estándar de comandos como se especifica por **RFC 959**. En la mayoría de los casos con el uso del moderno software de cliente FTP, no hay necesidad de que el usuario conozca alguno de estos comandos. Estos clientes manejan esto de forma transparente para el usuario, dando al usuario la comodidad de apuntar y hacer clic. Los **comandos FTP** se pueden dividir en cuatro categorías:

– Comandos de Control de Acceso

  Los Comandos de control de acceso **especifican identificadores de control de acceso**. En su mayoría, se ocupan de que se esté accediendo al servidor y qué privilegios que tiene el usuario. Todos los siguientes son considerados los comandos de control de acceso:

  · USER (Usuario – Nombre de Usuario)

    El **comando usuario** es **requerido por el servidor de acceso a su sistema de archivos**. Este comando será normalmente el **primer comando enviado después de la conexión**. Los servidores pueden permitir un nuevo comando de usuario para pasar en cualquier momento con el fin de cambiar la cuenta con el que se ha identificado. Esto tiene el efecto de purgar cualquier usuario, la contraseña y la información de cuenta ya suministrada al comienzo de la secuencia de inicio de sesión. Todos los parámetros de transferencia no se han modificado y cualquier transferencia de archivos en curso se completa bajo los viejos parámetros de control de acceso de nombre de usuario.

  · PASS (Contraseña)

    Este comando viene inmediatamente después de la orden del usuario, y, para la mayoría de los sitios, **completa el inicio de sesión y establece los privilegios de control de acceso**.

  · ACCT (Account – Cuenta)

    Este comando no está necesariamente relacionado con el comando USER, ya que algunos sitios pueden requerir una cuenta de inicio de sesión y otros sólo para los privilegios específicos, tales como el almacenamiento de archivos. Si esto no es necesario al iniciar la sesión el comando, puede emitirse en cualquier momento.

    En muchos sistemas modernos, este comando no se aplica debido a los riesgos de seguridad e información de cuenta que está directamente vinculada a **usuario**.

- CWD (Change Working Directory – Cambio de Trabajo del Directorio)

  Este comando permite al usuario trabajar con un directorio diferente para el almacenamiento de archivos o recuperación sin alterar su entrada o la información contable. Los parámetros de transferencia se mantienen sin cambios. Un nombre de ruta debe especificarse después de este comando.

- CDUP (Change to Parent Directory – Cambio de Directorio de Padres)

  Este comando es un caso especial de la caquexia crónica, y se incluye para **simplificar el cambio de árboles de directorios entre sistemas operativos** que tienen diferentes sintaxis para nombrar el directorio padre. Se considera un comando de control de acceso porque el directorio padre se especifica típicamente por la información de usuario o cuenta.

- SMNT (Structure Mount – Estructura Montaje)

  Este comando permite al usuario **montar un sistema de archivos diferente**, sin alterar su entrada o la información contable. Los parámetros de transferencia son de manera similar sin cambios. Puede especificar un nombre de ruta o directorio. En muchos sistemas modernos, este comando no se aplica debido a los riesgos de seguridad.

- REIN (Reinitialize)

  Este comando **terminará la sesión de usuario y purgará toda la información de cuenta**. Se permitirá cualquier transferencia en curso para ser completado. La sesión se restablecerá a la configuración predeterminada y la conexión se deja abierta. Esto es idéntico al estado inmediatamente después de que se abra la conexión. Un comando **usuario** podrá expedirse para iniciar sesión.

- QUIT (Logout and Quit – Salir)

  Este comando **termina un USUARIO y, si una transferencia de archivos no está en curso, el servidor cierra la conexión de control y termina la sesión**. Si una transferencia de archivos está en curso, la conexión permanecerá abierta hasta que el traslado devuelva un resultado hasta que el servidor cierra la conexión. Si deseas que la conexión permanezca abierta, pero te gustaría cerrar la sesión y volver (incluso como otro usuario), el comando REIN sería mucho más adecuado.