MF0952_2: Publicación de páginas web

Elaborado por: Juan Jesús Florido Torres

Edición: 5.0

EDITORIAL ELEARNING S.L.

ISBN: 978-84-16424-42-9 • Depósito legal: MA 607-2015

Impreso en España - Printed in Spain

Presentación

Identificación del Módulo Formativo:

Bienvenido/a al **Módulo Formativo 0952_2: "Publicación de páginas web".** Este módulo formativo es parte del Certificado de Profesionalidad **IFCD0110: "Confección y publicación de páginas web"** de la familia profesional **Informática y Comunicaciones**.

Presentación de los contenidos:

La finalidad de este módulo formativo es adquirir conocimientos para desarrollar la publicación y el mantenimiento de páginas web. Para ello, estudiaremos las características de seguridad en la publicación de nuestro sitio web, las herramientas de transferencia de archivos, el posicionamiento en buscadores, las aplicaciones de publicación automatizada, los procedimientos de publicación y las pruebas de verificación y depuración de páginas web.

Objetivos del Módulo Formativo:

Al finalizar este módulo formativo habrás aprendido a:

– Identificar los recursos disponibles en el sitio web y crear la estructura de almacenamiento para la publicación de las páginas y sus componentes.

– Transferir los archivos al sitio de publicación, usando las herramientas establecidas según especificaciones recibidas.

– Verificar las páginas transferidas, teniendo en cuenta criterios de calidad y "usabilidad" para garantizar su funcionalidad.

– Exponer las páginas desarrolladas en buscadores y directorios de acuerdo a los criterios de disponibilidad prefijados.

Índice

UD1

Características de seguridad en la publicación de páginas web

1.1. Seguridad en distintos sistemas de archivos
    1.1.1. Sistema operativo Linux
    1.1.2. Sistema operativo Windows
    1.1.3. Otros sistemas operativos

1.2. Permisos de acceso
    1.2.1. Tipos de acceso
    1.2.2. Elección del tipo de acceso
    1.2.3. Implementación de accesos

1.3. Órdenes de creación, modificación y borrado
    1.3.1. Descripción de órdenes en distintos sistemas
    1.3.2. Implementación y comprobación de las distintas órdenes

1.1. Seguridad en distintos sistemas de archivos

Todos los sistemas operativos poseen un componente llamado "sistema de archivos" (también denominado como ficheros o filesystem en inglés). La función del sistema de archivos es almacenar y organizar correctamente los archivos y su contenido, de modo que se pueda acceder a ellos de manera fácil y eficaz.

Los principales procesos llevados a cabo por el sistema de archivos se resumen en los siguientes puntos:

– Asignar espacio a los archivos.

– Gestionar el espacio libre.

– Administrar el acceso a los datos resguardados.

Concretamente, el sistema de archivos servirá para almacenar archivos, organizarlos de forma jerárquica, acceder a ellos, direccionarlos y recuperar los datos que contienen.

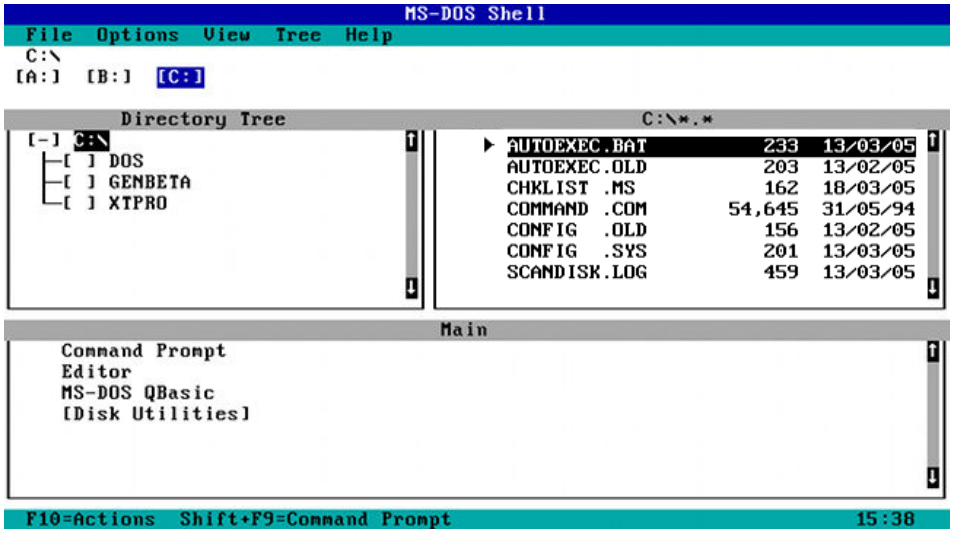
Por lo general, cada sistema operativo tiene su propio sistema de archivos. Por tanto, es evidente que el sistema de archivos que elijamos va a depender del sistema operativo con el que estemos trabajando. Cabe destacar que, mientras más reciente sea nuestro sistema operativo, mayor número de archivos admitirá.

Para representar el sistema de archivos se suele hacer de dos maneras:

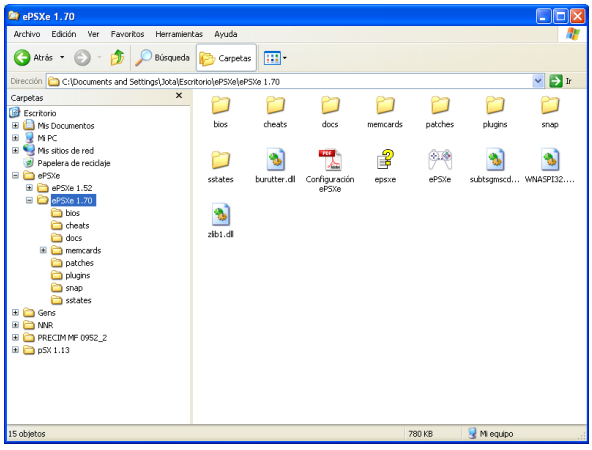
– Forma textual. Un ejemplo lo encontramos en el Shell de DOS.

– Forma gráfica. Un ejemplo lo hallamos en el explorador de Windows.

El modo gráfico contiene las ya populares denominaciones de "carpetas" que contienen "documentos" y "archivos", e incluso pueden tener más carpetas. Qué duda cabe, como ya hemos descubierto en este apartado, que los sistemas de archivos son parte integral de los sistemas operativos modernos.



Ejemplo de sistema de archivos en forma textual con Shell en MS-DOS.



Ejemplo de sistema de archivos en forma gráfica con explorador de Windows XP.

Los sistemas de archivos suelen poseer directorios que relacionan los nombres de los archivos con los propios archivos. Esto lo hace incluyendo el nombre del archivo al índice de una tabla de asignación de archivos como en el caso de los inodos del sistema operativo Unix.

Sobre la estructura de los ya mencionados directorios, existen dos tipos:

– Estructura plana (no es lo usual).

– Estructura jerárquica (también denominada ramificada o "en árbol"; es la más usada normalmente).

Las estructuras jerárquicas en los sistemas de archivos suelen emplear lo que se denomina "ruta". La ruta es una cadena de texto asociada a la ubicación exacta de un archivo. Lo cierto es que, dependiendo del sistema operativo que estemos utilizando, la nomenclatura de la ruta va a variar ligeramente.

En general, todas las rutas contienen una secuencia de nombres de directorios y subdirectorios. Como ya hemos explicado, en la estructura jerárquica esto quiere decir que se ordenan los directorios y sus subdirectorios de izquierda a derecha, dividiéndose entre ellos con algún símbolo como la barra (/) o la barra invertida (\). Asimismo, la ruta suele contener el nombre del archivo en el tramo final, seguido de su extensión.

Veamos dos ejemplos con dos sistemas operativos diferentes.

Juan, que utiliza Windows XP, desea abrir una imagen que se encuentra en sus documentos. La ruta que emplea el sistema de archivos será:

```
C:\Documents and Settings\Juan\Mis Documentos\Imagen.jpg
```

En este caso:

– "C:" sería la unidad de almacenamiento donde se halla la imagen.

– "\Documents and Settings\Juan\Mis Documentos\" son los directorios y subdirectorios en orden jerárquico (de izquierda a derecha). Es decir, "Mis Documentos" se encuentra en la carpeta "Juan", que a su vez se halla en "Documents and Settings". A todo esto se le denomina ruta.

– "Imagen" sería el nombre que se le da al archivo, y su extensión (".jpg") que identifica qué tipo de archivo es.

Por su parte, Mireia quiere escuchar su canción preferida en el sistema operativo Unix. La ruta entonces sería:

```
/home/mireia/música/canción.wav
```

En este caso:

– "/" es el directorio principal del sistema de archivos.

– "/home/mireia/música/" es el nombre de la ruta.

– "canción.wav" es el nombre del archivo y su extensión.

Los sistemas de archivos se pueden clasificar también en tres tipos:

1. Sistema de archivos de disco. Usan diversos dispositivos de almacenamiento, llamados "discos". Los discos son dispositivos físicos donde se guarda información permanente, pudiendo ser fijos (como en el caso de la mayoría de discos duros) o removibles. Vamos a ver algunos ejemplos de unidades de almacenamiento de datos que usan discos removibles:

   · Disquetera

   · CD-ROM

   · DVD-ROM

   · Lector de tarjetas de memoria

   Este sistema de archivos de disco es en el que nos vamos a centrar mayormente. En él encontramos algunos sistemas como FAT, EXT2 o ISO 9660.

2. Sistema de archivos de red. Este sistema accede a sus archivos mediante una red. Podemos dividirlo en dos tipos:

   · Sistema de archivos distribuidos, los cuales no proporcionan una E/S de datos en paralelo. Algunos sistemas de archivos de este tipo pueden ser AFS o Coda.

- Sistema de archivos paralelos, los cuales sí proporcionan E/S de datos en paralelo. Ejemplos de este tipo de sistemas pueden ser PVFS y PAFS.

3. Sistema de archivos de propósito especial. Son aquellos sistemas que no pueden considerarse ni de archivos de disco ni de archivos de red. Algunos ejemplos pueden ser ARCHFS, UDEV y ROMFS.

De izquierda a derecha y de arriba hacia abajo: disco duro; disquete de 3,5"; disco CD-ROM; y tarjeta de memoria SD.

Prácticamente, todos los dispositivos de almacenamiento que emplean los sistemas de archivos lo hacen permitiendo el acceso a sus datos mediante bloques (a menudo llamados "sectores") de un mismo tamaño. La longitud de estos sectores suele ser de 512 bytes cada uno.

Por tanto, el sistema de archivos va a organizar los sectores en archivos y directorios, registrando cuáles pertenecen a un archivo y cuáles a otro. Asimismo y por lógica, también se encargará de saber qué sectores no han sido utilizados en dichos archivos. También se encarga de conocer las direcciones físicas de cada sector.

Como ya sabemos, un sistema de archivos también puede acceder a datos generados de manera dinámica y sin la necesidad de que un dispositivo de almacenamiento intervenga en ello. Es decir, en la práctica, un sistema de archivos también puede gestionar los datos de, por ejemplo, una conexión de red.

Actualmente, la tecnología nos ofrece la posibilidad de tener discos de gran capacidad. Si realizamos una "partición de disco" podemos obtener útiles ventajas. Particionar un disco duro es prácticamente como dividirlo en varios. Esto nos da la posibilidad de agrupar la información dependiendo de la importancia que tenga para nosotros, o del orden y la organización que queramos darle.

Esto conlleva, claro está, tener la posibilidad de instalar varios sistemas operativos en nuestro propio disco duro. Si tengo un disco duro de 160GB, puedo decidir instalar Windows en una partición de 90GB, Linux en una segunda partición de 70GB y una tercera partición de 480MB para la memoria virtual de Linux.

Si volvemos a lo ya comentado, cada sistema operativo comportará un tipo diferente de sistema de archivos, por lo que hay que tener en cuenta todo esto en torno al tema de la seguridad. Y es que al realizar una partición, deberemos especificar qué sistema de archivos va a utilizar dicha partición. Esto es necesario, como ya sabemos, para que la partición sepa cómo va a organizar los datos y cómo va a operar sobre ellos.

Más adelante comprobaremos los sistemas de archivos más comunes en Linux, en Windows y en otros sistemas operativos. Pero antes, vamos a abarcar el concepto de seguridad en los sistemas de archivos.

Progresivamente se van desarrollando cada vez más aplicaciones y servicios para entornos web. A estos puede accederse mediante el navegador, ya sea desde redes internas de las empresas o a través de Internet. Es obvio que se necesita blindar de manera minuciosa a los servidores web, ya que son las computadoras centrales en un sistema de red que van a proveer dichos servicios al resto de computadoras.

Existen numerosos efectos de no disponer de una instalación segura en el servidor web. Dichas consecuencias pueden ser:

– Robo de información confidencial.

– Modificación en el aspecto o contenido de la web (lo que se denomina también como defacements).

– Caídas del servidor.

– Problemas de seguridad por la configuración.

– Inyección de código malicioso.

Para blindar la integridad de la información que contiene el sistema informático, debemos detallar las directrices y mecanismos encaminados a tal fin. Las características de dichos mecanismos y su eficacia enmarcan al sistema en una u otra categoría: sistema seguro o sistema inseguro.

Lo primero de todo es dotar de ciertos rasgos el entorno donde se halla la instalación de los equipos. En este sentido, lo que hay que conseguir de manera primordial es:

– Impedir el acceso a los equipos a personas no autorizadas.

– Un buen mantenimiento y estado de los equipos y el material.

– Eliminar o paliar riesgos de causa de fuerza mayor (inundaciones, incendios, terremotos, cortocircuitos…).

Si no llevamos a rajatabla la consecución de estos aspectos, la instalación y los equipos pueden verse seriamente comprometidos, destruyéndose y perdiéndose en muchos casos la valiosa información contenida en ellos.

Actualmente se tienen noticias y se conocen numerosos casos en los que se viola la privacidad de sistemas informáticos, por personas no autorizadas que consiguen saltarse los accesos. Dichas personas, además de obtener información que es confidencial, tienen la oportunidad de manipularla o eliminarla. El problema aumenta si nos paramos a pensar en la naturaleza de dichos datos, puesto que pueden ser datos bancarios, datos oficiales que manejan Gobiernos y Estados, etc.

Cabe mencionar que no todas las violaciones de privacidad se deben a accesos no permitidos; en ocasiones nosotros mismos instalamos en nuestros equipos, sin percatarnos, los denominados malware o también llamados “virus informáticos”. Las consecuencias de este software pueden ser imaginadas: destrucción de información y daños irreparables.

Los "virus informáticos", también llamados malware, son software malintencionado. Son pequeños programas que actúan por su cuenta, reproduciéndose y ejecutándose de manera autónoma, sin el permiso y sin el conocimiento del usuario, y cuyo fin es alterar el normal funcionamiento del ordenador.

Qué duda cabe que a nivel legislativo y ético se han desarrollado, en diversos países, normas que regulan la seguridad informática de los sistemas, con el fin de proteger el derecho a la intimidad de la información de las personas.

Apache es el servidor web más común y utilizado en todo el mundo. Al ser gratuito, de código abierto (pudiendo correr sobre cualquier plataforma), contar con amplias posibilidades de configuración y poseer excelentes módulos de seguridad, se ha convertido prácticamente en uno de los servidores más fiables de Internet. Además cuenta con una enorme facilidad de instalación y administración.

Antes de seguir adelante, hay que recordar un aspecto muy importante. ¿Qué nivel de seguridad requiere la instalación informática? Dependerá de los siguientes puntos:

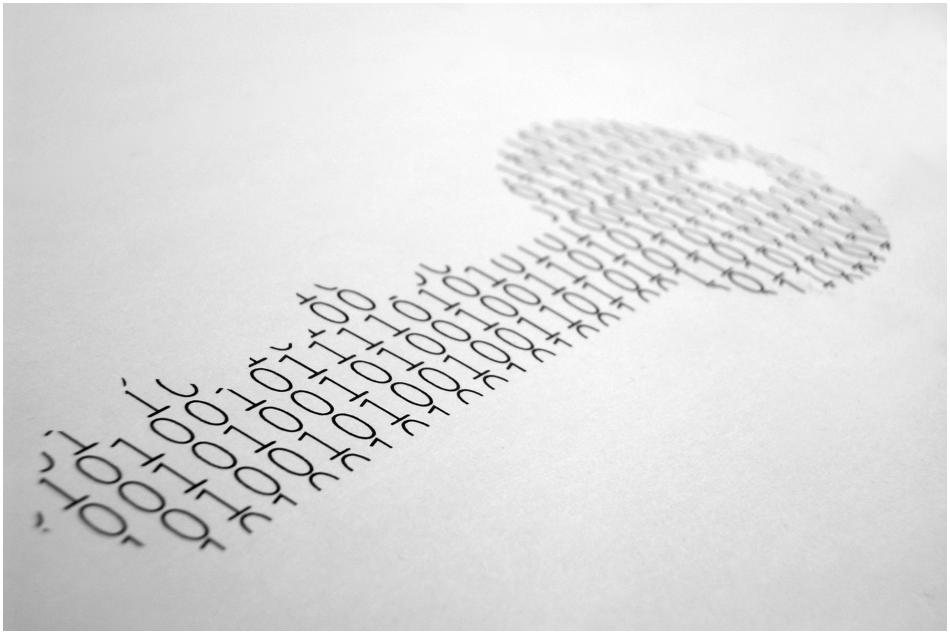
– Si tiene un gran número de archivos y/o mucha información en sus contenidos.

– Si hay un número elevado de datos de usuarios y organizaciones que están contenidos en sus archivos.

– Si existe un alto grado de confidencialidad de la información.

– Si existe una gran difusión, entendida como el número de personas que conocen la instalación y qué tipo de archivos contiene.

– Si es una zona de riesgo de causas de fuerza mayor.



La seguridad de nuestro sistema informático es primordial para mantener la integridad de sus datos y contenidos.

Por todo lo que hemos ido estudiando, qué duda cabe que no es lo mismo una instalación bancaria que un equipo destinado al uso doméstico.

Vamos a analizar el tema de la seguridad desde dos puntos de vista diferentes: la seguridad externa y la seguridad interna.

Los mecanismos de seguridad de un sistema informático colaboran entre sí para que, si una persona consigue quebrar alguna de las protecciones, se encuentre con otras que le impidan seguir adelante.

La seguridad se divide en externa o interna.

SEGURIDAD EXTERNA	Está relacionada con la instalación del sistema informático y el acceso que tienen las personas a él y a la información que contiene. Protege la instalación de intrusos y desastres como inundaciones e incendios.
SEGURIDAD INTERNA	Relacionada con los circuitos del sistema y los aspectos de seguridad del sistema operativo. Trata los controles incorporados al hardware. Asegura la confiabilidad, operabilidad e integridad de los programas y los datos.

La seguridad externa será aquella que proteja al sistema informático sin que este intervenga directamente. A su vez, la seguridad externa se divide en otros dos grupos:

SEGURIDAD FÍSICA	Es el tipo de seguridad encaminada a que agentes físicos no destruyan parte o totalidad de la información que el sistema contiene.
SEGURIDAD DE ADMINISTRACIÓN	Encaminada a impedir el acceso lógico de personas físicas al sistema informático con el fin de eliminar o manipular información.

Seguridad Externa

Siguiendo con la seguridad externa, y centrándonos en la seguridad física, ya sabemos que va a proteger al sistema de agentes físicos. Algunos agentes físicos que pueden amenazar la estabilidad y seguridad de la instalación son:

– Acceso y destrucción física por parte de personas.