

SISTEMAS WINDOWS

Centro de Formación del PAS
Universidad de Sevilla

Juan Antonio Ruiz Rivas

juanan@us.es

Febrero 2005

SISTEMAS WINDOWS.....	1
1. ACERCA DE ESTE CURSO.....	7
OBJETIVOS DEL CURSO.	9
<i>Aspectos de Windows no cubiertos.</i>	9
<i>Destinatarios del curso.</i>	9
1.1. ACERCA DE LAS PRÁCTICAS.	10
<i>Cuaderno de prácticas.</i>	10
<i>Ordenador de prácticas.</i>	10
1.2. ACERCA DE ESTE MANUAL.	11
<i>Registro de versiones.</i>	11
2. FAMILIA DE SISTEMAS WINDOWS.	13
2.1. WINDOWS PARA MS-DOS.	15
<i>Características de Windows 3.x.</i>	15
2.2. WINDOWS 95, 98 Y ME.	16
<i>Características de Windows 9x.</i>	16
2.3. WINDOWS NT.	17
<i>Características de Windows NT.</i>	17
2.4. WINDOWS 2000.	18
<i>Características de Windows 2000.</i>	18
2.5. WINDOWS XP.	19
<i>Características de Windows XP.</i>	19
2.6. PERSPECTIVAS ACTUALES.	20
2.7. WINDOWS 2000 Y WINDOWS XP COMO EJEMPLOS PRÁCTICOS DEL CURSO.	21
2.8. REFERENCIAS.	22
3. INSTALACIÓN DEL SISTEMA.	23
3.1. REQUISITOS PREVIOS A LA INSTALACIÓN.....	25
<i>Requisitos mínimos.</i>	25
<i>Hardware compatible.</i>	25
3.2. PRÁCTICA: INVENTARIANDO LAS CARACTERÍSTICAS DE UN EQUIPO INFORMÁTICO	27
<i>Hoja de inventario de equipo informático.</i>	29
3.3. PRÁCTICA: CREAR UN DISQUETE DE ARRANQUE CON UTILIDADES PARA PARTICIONAR EL DISCO DURO 30	
<i>Disquete de arranque MSDOS con Ranish Partition Manager.</i>	30
3.3. PARTICIONES Y FORMATOS	31
<i>Introducción.</i>	31
<i>Sistema de archivos.</i>	31
<i>Particiones y volúmenes.</i>	32
<i>Formato.</i>	34
3.4. PRÁCTICA: UTILIZANDO EL "ADMINISTRADOR DE DISCOS" DE WINDOWS 2000.	35
3.5. CONTROLADORES DE DISPOSITIVOS.....	36
3.6. PRÁCTICA: INSTALANDO UN CONTROLADOR DE DISPOSITIVO.	37
3.7. REFERENCIAS.	38
4. COMUNICACIONES Y REDES.	39
4.1. COMPONENTES DE RED.....	41
<i>Dispositivos físicos.</i>	41
<i>Protocolos.</i>	41
<i>Clientes y Servicios.</i>	41
4.2. CONFIGURACIÓN DE TCP/IP.	43

<i>Redes ocultas</i>	44
4.3. PRÁCTICA: CONFIGURANDO TCPIP EN WINDOWS.....	46
<i>Configuración IP actual del sistema</i>	46
<i>Instalación de TCP/IP</i>	47
4.4. RECURSOS COMPARTIDOS.....	48
<i>Compartir recursos con precaución</i>	48
4.5. PRÁCTICA: COMPARTIENDO RECURSOS EN WINDOWS.....	49
<i>Windows XP</i>	49
<i>Windows 2000</i>	49
4.6. REFERENCIAS.....	51
5. LA LÍNEA DE COMANDOS.....	53
<i>cd</i>	53
<i>dir</i>	53
<i>attrib</i>	53
6. ACTUALIZACIÓN DEL SISTEMA.....	55
6.1. PRECAUCIONES.....	57
6.2. ACTUALIZACIONES DISPONIBLES.....	58
<i>Windows Update</i>	58
<i>Hot-Fix</i>	58
<i>Service Pack</i>	58
6.3. CÓMO Y PORQUÉ MANTENER UN SISTEMA ACTUALIZADO.....	60
<i>Cuando no debemos actualizar</i>	60
6.4. PRÁCTICA: ACTUALIZANDO CON WINDOWS UPDATE.....	61
6.5. REFERENCIAS.....	62
7. SEGURIDAD.....	63
7.1. SEGURIDAD EN WINDOWS.....	65
7.2. PROTEGERSE CONTRA LOS VIRUS.....	66
<i>Instala un antivirus</i>	66
<i>Cómo funciona un antivirus</i>	66
<i>Como configurar un antivirus</i>	67
<i>Como y cuando actualizar nuestro antivirus</i>	67
<i>No confiarnos en nuestro antivirus</i>	67
7.3. COPIAS DE SEGURIDAD.....	68
<i>Soporte físico</i>	68
<i>Periodicidad</i>	69
<i>Estrategia de almacenamiento</i>	69
<i>Datos que debemos respaldar</i>	69
<i>Copia de seguridad centralizada</i>	70
7.4. CONTRASEÑAS SEGURAS.....	71
7.5. REFERENCIAS.....	72
8. EL REGISTRO DE WINDOWS.....	73
8.1. INTRODUCCIÓN AL REGISTRO.....	75
8.2. ESTRUCTURA DEL REGISTRO.....	76
8.3. EL EDITOR DEL REGISTRO.....	78
8.4. PRÁCTICA: HACIENDO COPIA DE SEGURIDAD DEL REGISTRO.....	80
8.5. PRÁCTICA: CAMBIANDO ALGUNAS CLAVES DEL REGISTRO.....	81
<i>Programas que se cargan al iniciar Windows</i>	81
<i>Localización de los archivos de instalación</i>	81
<i>Automatizar el inicio de sesión en red</i>	81
8.6. REFERENCIAS.....	82

9.	RESOLUCIÓN DE PROBLEMAS EN WINDOWS	83
9.1.	COMPROBACIONES BÁSICAS ANTE LA EXISTENCIA DE UN PROBLEMA.	85
	<i>Herramienta de información del sistema.....</i>	<i>85</i>
	<i>Programa de configuración del sistema de Windows.....</i>	<i>85</i>
	<i>Comprobador de archivos de sistema.</i>	<i>86</i>
	<i>Comprobador del registro.</i>	<i>86</i>
9.2.	RECUPERACIÓN DE ARCHIVOS DEL SISTEMA.	87
9.3.	REFERENCIAS.	88
10.	APÉNDICES.	89
10.1.	HISTORIA DE WINDOWS	91
	<i>Windows 1.0.....</i>	<i>91</i>
	<i>Microsoft Windows 2.0.....</i>	<i>91</i>
	<i>Windows 3.0.....</i>	<i>91</i>
	<i>OS/2 1.....</i>	<i>91</i>
	<i>OS/2 2.0.....</i>	<i>92</i>
	<i>Windows 3.1 y Windows 3.11.....</i>	<i>92</i>
	<i>Windows NT.....</i>	<i>92</i>
	<i>Windows 95 - Desarrollo.....</i>	<i>93</i>
	<i>Windows NT 3.1.....</i>	<i>93</i>
	<i>Windows 95 - Lanzamiento.....</i>	<i>93</i>
	<i>OS/2 3.0 y 4.0.....</i>	<i>94</i>
	<i>Windows NT 4.0.....</i>	<i>94</i>
	<i>Windows 98.....</i>	<i>94</i>
	<i>Windows 98 Second Edition.....</i>	<i>94</i>
	<i>Windows Millennium Edition.....</i>	<i>94</i>
	<i>Windows 2000.....</i>	<i>94</i>
	<i>Windows XP.....</i>	<i>94</i>
	<i>Progresión de MS-DOS:.....</i>	<i>95</i>
	<i>Progresión de OS/2:.....</i>	<i>95</i>
10.2.	DISCO DURO.....	96
	<i>Cabezas, cilindros y sectores.....</i>	<i>96</i>
	<i>Particiones y formato.....</i>	<i>96</i>
	<i>Referencias.</i>	<i>96</i>
10.3.	PROTOCOLOS TCP/IP.....	98
	<i>Protocolos de comunicaciones.</i>	<i>98</i>
	<i>¿Qué es TCP/IP?.....</i>	<i>98</i>
	<i>Arquitectura de protocolos TCP/IP.....</i>	<i>99</i>
	<i>Descomposición en niveles de TCP/IP.....</i>	<i>99</i>
	<i>Nivel de aplicación.</i>	<i>99</i>
	<i>Nivel de transporte.....</i>	<i>100</i>
	<i>Nivel de red.....</i>	<i>100</i>
	<i>Nivel de enlace.....</i>	<i>101</i>
11.	REFERENCIAS.....	103
11.1.	REFERENCIAS EN ESPAÑOL.....	105
	<i>Generales.....</i>	<i>105</i>
	<i>Instalación del sistema.....</i>	<i>105</i>
	<i>Comunicaciones y redes.</i>	<i>105</i>
	<i>Seguridad.....</i>	<i>105</i>
11.2.	REFERENCIAS EN INGLÉS.....	106
	<i>Generales.....</i>	<i>106</i>
	<i>Instalación del sistema.....</i>	<i>106</i>
12.	GLOSARIO DE TÉRMINOS INFORMÁTICOS.....	107

13. HOJAS DE PRÁCTICAS	111
<i>Creando un disquete de arranque</i>	<i>113</i>
<i>Hoja de inventario de equipo informático</i>	<i>115</i>
<i>Trabajando con particiones y formatos.....</i>	<i>117</i>
<i>Utilizando el "administrador de discos" de Windows.</i>	<i>118</i>
<i>Instalando un controlador de dispositivo.</i>	<i>119</i>
<i>Configurando TCP/IP.....</i>	<i>120</i>
<i>Compartiendo recursos en red.</i>	<i>121</i>
<i>Actualizando Windows.....</i>	<i>122</i>
<i>Realizando una copia de seguridad.....</i>	<i>123</i>
<i>Haciendo copia de seguridad del registro.....</i>	<i>124</i>
<i>Cambiando algunas claves del registro.....</i>	<i>125</i>

1. Acerca de este curso

- Objetivos del curso.
- Acerca de las prácticas.
- Acerca de este manual.

Objetivos del curso.

La finalidad del curso es capacitar a los participantes para instalar y mantener sistemas informáticos basados en Windows 2000 y Windows XP en sus versiones “professional”.

Al finalizar el curso los participantes sabrán:

- Realizar la instalación más adecuada a las características del equipo y a las necesidades de los usuarios del sistema.
- Instalar aplicaciones y configurar nuevos dispositivos.
- Resolver problemas de funcionamiento.
- Configurar una red basada en Windows.
- Mantener actualizado el sistema.
- Mantener unos niveles de seguridad adecuados.
- Trabajar con el registro de Windows.

Aspectos de Windows no cubiertos.

Debe quedar claro desde un principio que aunque este curso va dirigido a responsables e instaladores de sistemas Windows no vamos a tocar aspectos de gestión desde el punto de vista de un administrador de red. No abordaremos, por tanto, la cuestión de los dominios o directorios activos, la instalación y configuración de servicios de red, seguridad frente a intrusos, etc. Puedes encontrar información sobre algunos de estos temas en las referencias existentes al final de este manual.

Otros aspectos que no tocaremos serán temas de programación o arquitectura interna de estos sistemas.

Destinatarios del curso.

Este curso va dirigido a usuarios con conocimientos medios sobre los sistemas operativos Windows 95/98, Windows 2000 Professional y Windows XP Professional que necesiten un mayor dominio sobre el sistema en entornos de trabajo críticos o en la administración de una instalación con varios equipos en red que funcionen bajo Windows.

Se presuponen por tanto unos conocimientos mínimos en el manejo básico del sistema operativo: iniciar sesión en el sistema, funcionamiento y utilidades del escritorio de Windows, manejo del Explorador de Archivos y configuración básica del equipo con las herramientas del Panel de Control.

1.1. Acerca de las prácticas.

Debido a la naturaleza de este curso para realizar muchas de las prácticas es recomendable contar con un ordenador de prácticas distinto al ordenador con el que estamos siguiendo el curso o a cualquier ordenador con el que estemos trabajando en la actualidad. Esto es debido a que en algunos casos la realización de la práctica supondrá la pérdida de toda o parte de la información y el software instalado en el PC. En cualquier caso aparecerá una nota de aviso en la descripción de las prácticas correspondientes.

En la versión presencial de este curso dispondremos de equipos en los que se haya habilitado el arranque remoto a partir de imágenes de sistemas operativos Windows 2000 y Windows XP, con lo cual podremos restaurar cualquiera de estos sistemas en el equipo sin excesiva pérdida de tiempo.

La realización de las prácticas debe hacerse normalmente después de acabar la correspondiente sesión teórica donde se explican los fundamentos del tema tratado. Para ello basta con respetar el orden establecido en este curso.

Cuaderno de prácticas.

En cada práctica se pedirá al alumno que tome algunas anotaciones. Le recomiendo que anote los resultados de las prácticas en un cuaderno de prácticas.

Este manual incluye al final unas hojas en blanco rotuladas con los nombres de cada práctica en donde podremos tomar dichas notas.

En algunos casos estas anotaciones serán muy valiosas para volver el sistema a su estado original.

Ordenador de prácticas.

Requisitos mínimos de los equipos:

- Microprocesador: Intel Pentium II o AMD K5
- Disco duro: 2,5 GB.
- Memoria RAM: 64-128 MB.

Para las prácticas de red:

- Dos o más equipos que cumplan los requisitos mínimos expuestos arriba.
- Dos o más tarjetas de red ethernet.
- Un concentrador ethernet o tomas de red en servicio.

1.2. Acerca de este manual.

En principio concebí este documento como manual de un curso presencial para el Centro de Formación del PAS de la Universidad de Sevilla, aunque espero que pronto se convierta en el manual de un curso a través de Internet y finalmente en un documento de referencia para cualquiera que lo necesite.

No me reservo los derechos de autor y me encantaría que fueran copiados y utilizados por todo aquel que lo considere de interés siempre bajo los términos de la licencia GNU que aparece al final del documento.

A fecha de hoy el manual se encuentra inacabado en algunos de sus capítulos y es posible que contenga cierta cantidad de errores o imprecisiones. Agradecería cualquier reporte de error o mejora que podáis hacerme llegar, aunque sólo se trate de una coma mal puesta, a mi dirección de correo electrónico: <mailto:juanan@us.es>.

Registro de versiones

- Febrero 2002 – Windows experto
- Abril 2002 – Windows 98 avanzado
- Septiembre 2002 – Windows avanzado
- Mayo 2003 – Windows avanzado
- Octubre 2003 – Sistemas Windows
- Octubre 2004 – Sistemas Windows
- Febrero 2005 – Sistemas Windows

2. Familia de sistemas Windows.

- Windows para MS-DOS.
- Windows 95, 98 y Me.
- Windows NT.
- Windows 2000.
- Windows XP.
- Perspectivas actuales.
- Windows 98 y Windows 2000 como ejemplos prácticos del curso.
- Referencias.

2.1. Windows para MS-DOS.

Las primeras versiones de Windows fueron concebidas como una interfaz gráfica para un sistema operativo que carecía de ella: MS-DOS.

Las versiones publicadas de este Windows son: 1.0, 2.0, 3.0, 3.1 y 3.11.

Características de Windows 3.x.

- Entorno gráfico para el sistema operativo MS-DOS.
- Arquitectura de 16 bits.
- Sistema de archivos: FAT
- La última versión, "Windows 3.11 para grupos de trabajo", tenía soporte para redes punto a punto y resultó ser muy estable.

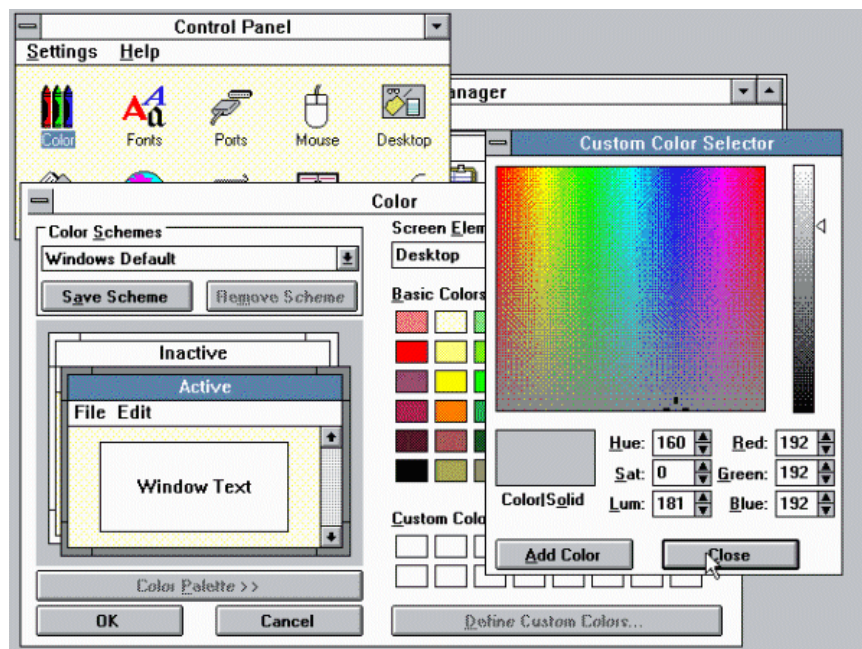


Imagen: Captura de pantalla de Windows 2.

2.2. Windows 95, 98 y ME.

La segunda generación de aquel Windows que corría sobre MS-DOS fue concebida y publicitada como un nuevo sistema operativo aunque realmente seguía siendo una interfaz gráfica muy avanzada corriendo sobre un MS-DOS mejorado.

Las versiones publicadas de este sistema son: 95, 95 OSR2, 98, 98 Second Edition y Windows Millenium Edition (ME).

Dejando a un lado todas las críticas que pueden hacerse a estas versiones de Windows, hay que reconocer que este sistema operativo ha revolucionado la forma de trabajar con PCs y ha supuesto una buena base para un sinnúmero de aplicaciones informáticas de gran calidad y envergadura, desde aplicaciones ofimáticas hasta sistemas de edición de vídeo digital que nadie hubiera concebido corriendo sobre un PC en los tiempos del DOS.

La última versión de la saga: Windows Millenium, era mucho menos estable que Windows 98 SE, incorporaba pocas novedades interesantes frente a ella, y fue tan rápidamente reemplazada con Windows XP Home que pocos usuarios y organizaciones migraron a ella.

La versión más estable de esta familia resultó ser Windows 98 SE.

Características de Windows 9x.

- Sistema operativo híbrido entre MS-DOS y el propio Windows.
- Multitarea y arquitectura de 32 bits.
- Utiliza el modo protegido del 80386.
- Sistema de archivos: FAT mejorada con VFAT y en Windows 95 OSR2 se pasa de FAT 16 a FAT 32.
- Amplio soporte para acceder a redes de ordenadores.

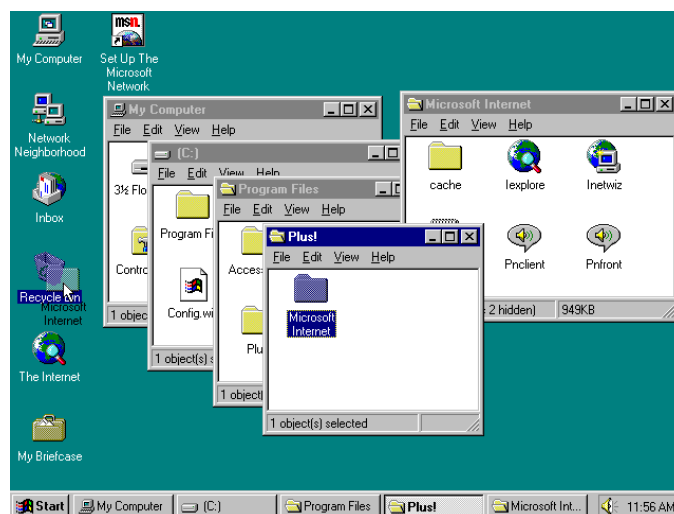


Imagen: captura de pantalla de Windows 95

2.3. Windows NT.

Windows NT fue un sistema operativo desarrollado por Microsoft para su uso en estaciones de trabajo y servidores de red. Desde su concepción fue un sistema robusto, seguro y basado en la arquitectura cliente/servidor. Con el tiempo los sistemas basados en Windows NT han acaparado una gran cuota de mercado en cuanto a número de servidores instalados.

Quizás la mejor baza de Windows NT frente a otros sistemas operativos de servidor ha sido la facilidad de instalación, configuración y mantenimiento del sistema, esto hace que la curva de aprendizaje de este sistema sea fácilmente accesible a cualquier usuario con unos conocimientos medios de informática.

El desarrollo de Windows NT se produjo más o menos entre la aparición de Windows 3.11 y Windows 95. Las primeras versiones tenían por tanto la apariencia de Windows 3.11

Características de Windows NT

- Arquitectura de 32 bits.
- Sistema de ficheros: NTFS, también soportaba FAT16 y HPFS.
- Multitarea, multiproceso y multiusuario.
- Basado en microkernel.

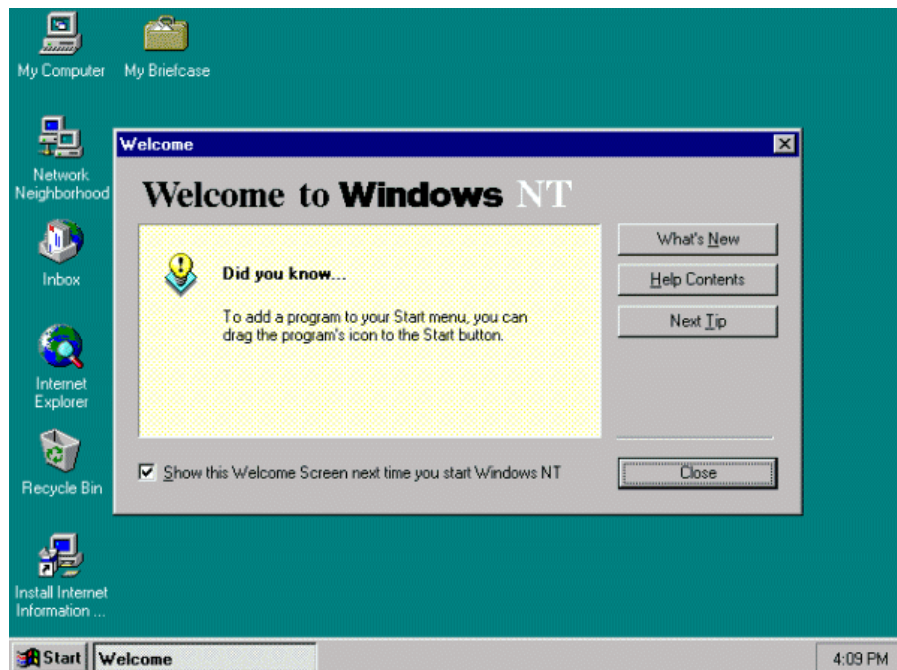


Imagen: captura de pantalla de Windows NT 4.

2.4. Windows 2000.

Windows 2000 constituyó una evolución sustancial desde Windows NT sobre todo en servicios de red pero también en su interfaz gráfica.

Sólo ha existido una versión de Windows 2000, parches aparte, que sin embargo se presenta en distintos sabores: *Professional*, *Server*, *Advanced Server* y *Enterprise Server*, cada una con más servicios y prestaciones.

A la espera de las nuevas versiones de Microsoft, Windows 2000 es la solución actual de Microsoft en la gama de servidores.

Características de Windows 2000.

- Arquitectura de 32 bits.
- Núcleo del sistema basado en NT.
- Sistema de archivos: NTFS, FAT16 y FAT32
- Nuevos servicios de red, destacando entre ellos el Active Directory.
- Se ha añadido encriptación nativa al sistema de ficheros NTFS.

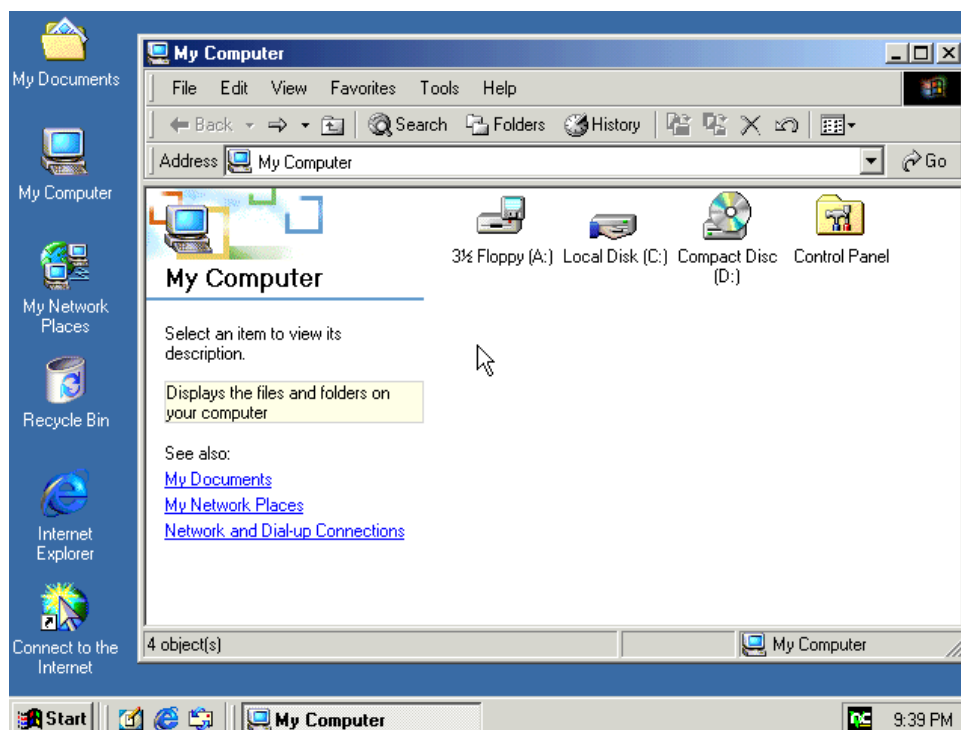


Imagen: captura de pantalla de Windows 2000.

2.5. Windows XP.

Con Windows XP llega la fusión entre las dos líneas de sistemas operativos desarrollados por Microsoft, sobre un núcleo de NT se montan una serie de servicios que puedan abarcar desde el usuario casero a los grandes servidores de red, pasando por los usuarios profesionales y pequeños servidores de oficina.

Windows XP es el último sistema de la saga Windows, se encuentra disponible en cuatro versiones: *Home*, *Professional*, *Tablet PC* y *64 Bits*. De momento Microsoft ha bautizado la línea de servidores correspondiente a Windows XP como Windows 2003 Server.

Características de Windows XP.

- Núcleo del sistema basado en NT, no quedan "restos" de MS-DOS.
- Sistema de archivos: NTFS, FAT16 y FAT32
- Nueva interfaz gráfica.
- Firewall de serie (a partir de SP2)
- Seguridad en red mejorada.

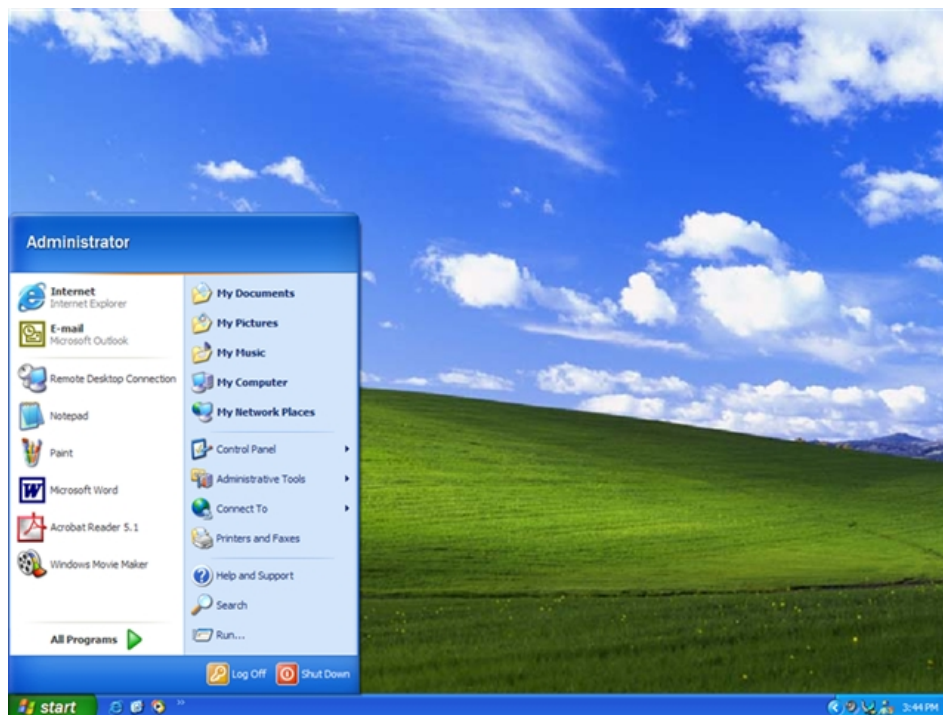


Imagen: captura de pantalla de Windows XP.

2.6. Perspectivas actuales.

Las sucesivas versiones de este sistema operativo (y las de cualquier otro), van requiriendo cada vez más prestaciones del hardware sobre el que van instalados, por lo que los usuarios que no han ido renovando sus equipos se han quedado anclados en el sistema que mejor se desempeñaba sobre estos, es por ello que actualmente se siguen utilizando casi todas las versiones de Windows: NT, 98, 2000 y XP.

La tendencia actual es la ir migrando todos los sistemas a Windows XP, pero aún así es de esperar que muchos usuarios sigan utilizando versiones anteriores porque su hardware o su software no sean compatibles con los nuevos sistemas. En cuanto a las versiones para servidor está disponible ya Windows 2003.

2.7. Windows 2000 y Windows XP como ejemplos prácticos del curso.

Este curso se ha basado en los sistemas operativos Windows 2000 y Windows XP. De este modo entendemos que quedan cubiertas las dos versiones más utilizadas actualmente en las aulas de informática de la Universidad de Sevilla.

En cualquier caso ambos sistemas operativos comparten muchos aspectos comunes, casi todo lo que se diga para uno servirá para el otro, aunque encontraremos algunas cosillas cambiadas de sitio.

2.8. Referencias

- Microsoft; *Microsoft Windows*; <http://www.microsoft.com/spain/windows/>
- Enciclopedia libre; Historia de Windows;
[http://enciclopedia.us.es/index.php/Historia de Windows](http://enciclopedia.us.es/index.php/Historia_de_Windows)
- Historia de Windows con capturas de pantalla(en inglés);
<http://www.neowin.net/articles.php?action=more&id=53>

3. Instalación del sistema.

- Requisitos previos a la instalación.
- Particiones y formatos.
- Práctica: trabajando con particiones y formatos.
- Práctica: utilizando el "administrador de discos" de Windows.
- Controladores de dispositivos.
- Práctica: instalando un controlador de dispositivo.
- Referencias.

3.1. Requisitos previos a la instalación.

La instalación de un sistema con Windows no requiere demasiadas consideraciones, hoy por hoy un PC y Windows están casi "hechos el uno para el otro" y saben a que atenerse. La mayoría de los dispositivos serán configurados correctamente durante la instalación del sistema operativo, no obstante alguno de ellos requerirá alguna ayuda por nuestra parte.

Un buen consejo antes de comenzar la instalación de cualquiera de estos sistemas es leerse, aunque sea de forma rápida, los archivos de texto **instalar.txt** que aparecen en el directorio raíz del CD de instalación, podemos encontrar ahí soluciones a muchos problemas y trucos que pocos conocen.

Requisitos mínimos.

Windows 2000 Professional.

- Procesador compatible Pentium 166 MHz o superior.
- 64 MB de memoria RAM mínimo; 128 MB recomendados, 4 GB máximo.
- Disco duro de 850 MB + 2 MB por cada 1 MB de memoria RAM. Se requerirá más espacio dependiendo de los componentes instalados, el uso de FAT requiere de 100 a 200 MB adicionales, la instalación a través de la red puede requerir otros 100 a 200 MB adicionales para archivos temporales.

Windows XP

- Procesador compatible Pentium 233 MHz o superior.
- 64 MB de memoria RAM mínimo; 128 o 256 recomendados.
- Disco duro de 1,5 GB

Tienes información para todos los sistemas operativos de Microsoft en la siguiente página web: <http://support.microsoft.com/default.aspx?scid=kb;es;304297>

Hardware compatible.

Si todavía no hemos adquirido los equipos podría ser una buena idea elegir los componentes entre la lista de compatibilidad de hardware testado por Microsoft.

En Windows 2000 puede encontrarse una copia de la lista de compatibilidad hardware en el propio CD de instalación y en la dirección: <http://www.microsoft.com/whdc/hcl/search.msp>

Para Windows XP podemos visitar la siguiente dirección (de momento en perfecto inglés): <http://www.microsoft.com/windows/catalog/>

Antes de comenzar a realizar la instalación de los equipos sería conveniente hacer un pequeño inventario de las características y los componentes de cada PC así como de los periféricos que tenemos que instalar. Si estos componentes ya están funcionando bajo otro sistema operativo y no son "Plug and Play" sería una buena opción anotar los parámetros de configuración como IRQ y direcciones de memoria.

A continuación debemos hacer acopio de todos los controladores de dispositivo y de los periféricos que deseemos instalar, vendrán en disquete o en CD-ROM, quizás necesitemos buscar algunos en Internet.

Por último, si vamos a conectar los equipos en red debemos conocer la infraestructura de red de que disponemos en nuestra organización y si vamos a utilizar el protocolo TCP/IP las direcciones IP que van a utilizar nuestros equipos o si existe en nuestra red un servidor DHCP que automáticamente asigne estas direcciones. Si esto último te suena un poco a chino quizás puedas dejar estos valores tal como parezcan por defecto en la instalación y revisarlos cuando llegemos al tema de comunicaciones y redes.

Lo más cómodo es tener todos estos datos recogidos en una base de datos que iremos actualizando a medida que agreguemos nuevos equipos o nuevos componentes. Un poco más abajo os mostramos una hoja de inventario tipo con los datos que podrían incorporarse a dicha base de datos. (Existe otra copia de esta hoja al final del manual para que podáis utilizarla durante el curso).

Para aprender a sacar toda esta información de un sistema ya instalado con Windows 2000 o XP vamos a hacer una sencilla práctica pero antes no olvides hacer una copia de seguridad si el equipo contiene datos que no podemos perder.

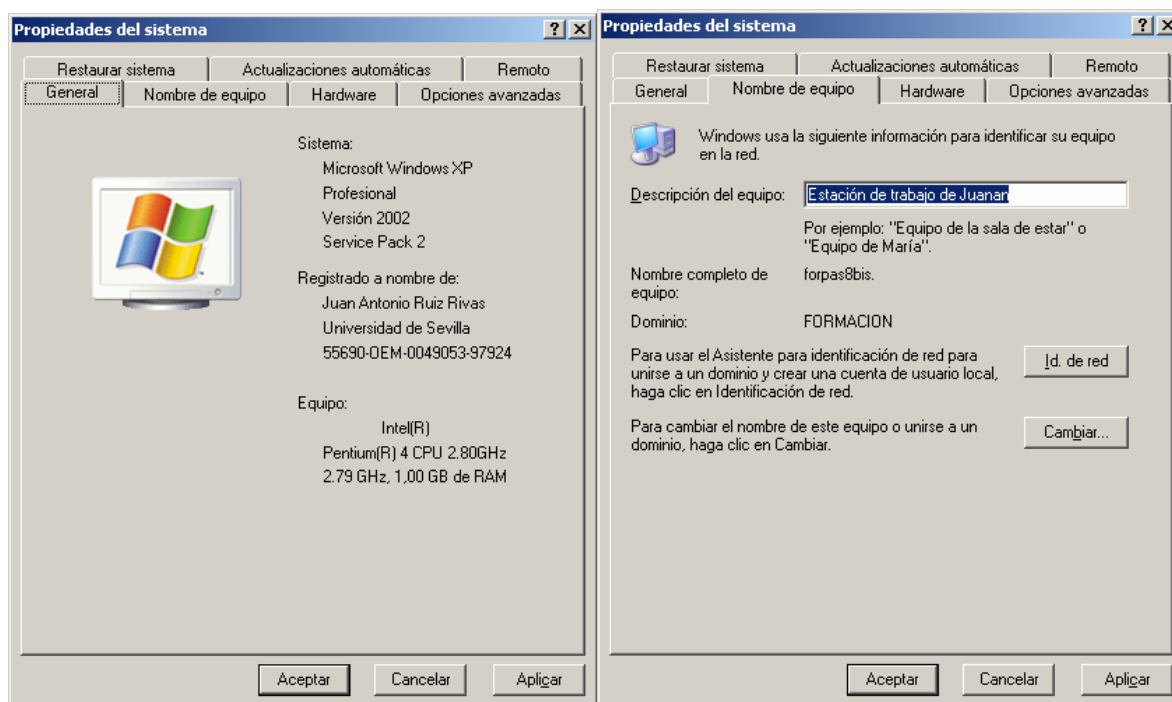
3.2. Práctica: inventariando las características de un equipo informático

Para realizar este inventario vamos a partir de un equipo con Windows 2000 o XP instalado, si el equipo no tuviera ningún sistema operativo instalado podemos recabar estos datos del proveedor de los equipos y de nuestro administrador de red.

Hay muchas herramientas y comandos que nos van a permitir hacer esta radiografía de nuestro equipo, aquí usaremos las más conocidas.

Propiedades del sistema

Se puede llegar a esta utilidad de varias formas, la más cómoda es hacer clic con el botón secundario del ratón sobre el icono “**Mi PC**” y luego elegir “**Propiedades**”. También existe un icono etiquetado “**Sistema**” al que se puede acceder desde el “**Panel de Control**”.

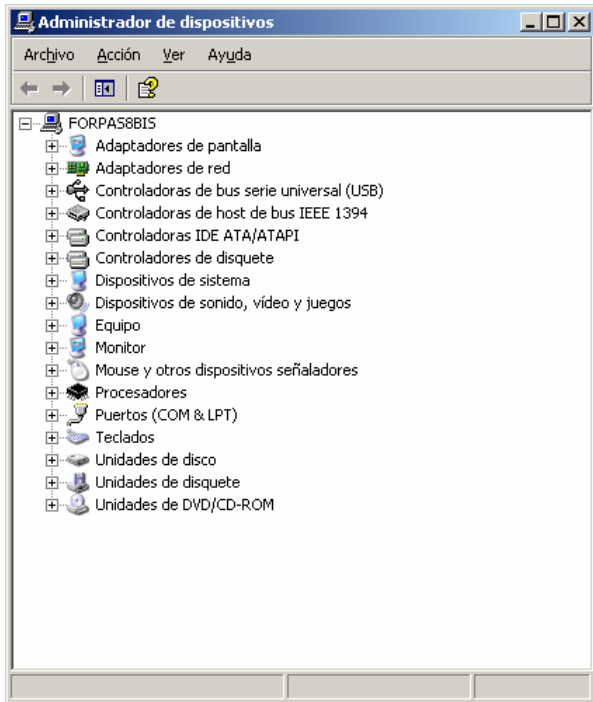


En la pestaña “**General**” podemos ver el sistema operativo y la versión instalada en nuestro equipo, así como el tipo y la velocidad del microprocesador y la cantidad total de memoria RAM.

Desde la pestaña “**Nombre del equipo**” podemos ver y cambiar ese dato, además de la pertenencia a un dominio o a un grupo de trabajo.

Por último desde “**Hardware**” podremos acceder a una de las herramientas que más nos van a ayudar en nuestro inventario: el “**administrador de dispositivos**”.

Administrador de dispositivos



ipconfig

ipconfig es una herramienta de línea de comandos que nos va a dar casi toda la información que necesitamos sobre nuestra configuración de red.

Para utilizarla hacemos clic en **Inicio** -> **Ejecutar** -> Tecleamos **cmd** y escribimos “**ipconfig /all**”

Hoja de inventario de equipo informático.

Nombre del equipo	
Datos IP (Nº. IP, máscara, encaminador)	
Dominio o grupo de trabajo	
Marca y modelo	
BIOS (fabricante, revisión y fecha)	
Procesador	
Módulos de RAM (número y capacidad)	
Discos duros (marca, modelo y capacidad)	
CD-ROM (marca, modelo, velocidad)	
Tarjeta de red (marca, modelo, chipset, IRQ)	
Dirección MAC	
Tarjeta de vídeo (marca, modelo, chipset, IRQ)	
Tarjeta de sonido (marca, modelo, chipset, IRQ)	
Módem (marca, modelo, chipset, IRQ)	
Controladora SCSI (marca, modelo, chipset, IRQ)	
Otros componentes o periféricos	
Observaciones	

3.3. Práctica: Crear un disquete de arranque con utilidades para particionar el disco duro

Cada sistema operativo trae su propio gestor de arranque integrado, pero para realizar ciertas tareas en nuestro PC es interesante a veces contar con un sistema de arranque alternativo para poder arrancar.

Disquete de arranque MSDOS con Ranish Partition Manager.

Lo primero que vamos a hacer es crear un disquete de arranque desde Windows XP que cargará MSDOS en nuestro PC

1. Introduce en la disquetera un disquete en blanco o uno cuyos archivos no necesites, ¡vamos a borrar toda la información en él!
2. Desde “Mi PC” sitúa el cursor sobre el icono de la disquetera y con el botón secundario del ratón selecciona “Formatear...”
3. En el cuadro de diálogo que aparece marcamos la casilla “Crear un disco de inicio de MSDOS”
4. Pulsamos “Iniciar” para crear nuestro disco de arranque.
5. Desde la página web <http://www.ranish.com/part/> descargamos el programa “Ranish Partition Manager”.
6. Descomprimos el fichero que hemos descargado al disquete. Particiones y formatos.

Nota: la utilidad de crear un disquete de arranque MSDOS no está disponible en Windows 2000.

3.3. Particiones y formatos

Introducción.

Antes de instalar Windows en el disco duro de nuestro equipo tendremos que preparar éste adecuadamente, la preparación incluye los siguientes pasos:

1. Crear una o más particiones en el disco duro.
2. Crear volúmenes en la partición extendida (si la hemos creado).
3. Activar la partición primaria.
4. Decidir que sistema de archivos vamos a utilizar en cada partición.
5. Formatear las particiones que hayamos creado.
6. Arrancar el sistema desde un disquete o un CD-ROM de arranque.
7. ¡Ya podemos instalar el sistema!

Aunque realmente estos pasos nos los va a ahorrar el asistente de instalación es importante tener una serie de conceptos claros que luego nos ayudarán a la hora de solucionar problemas.

La elección del sistema de archivos va a condicionar los tipos y tamaños de partición que tendremos que crear, así que empezaremos por aquí.

Sistema de archivos.

Windows 2000 y XP nos ofrecen la posibilidad de trabajar con dos sistemas de archivos: FAT y NTFS.

FAT

FAT (*file allocation table*) es el sistema de archivos utilizado originalmente por MS DOS y posteriormente mejorado para ser utilizado en cualquier versión de Windows.

Sus defensores argumentan que es más rápido que NTFS y que la partición puede ser accedida desde cualquier versión de Windows.

La versión de FAT que utilizan Windows 2000 y XP recibe el nombre de FAT32.

NTFS.

Sistema de archivos diseñado específicamente para Windows NT (NT File System) con el objetivo de crear un sistema de archivos eficiente, robusto y con seguridad incorporada desde su base. También soporta compresión nativa de ficheros y encriptación (esto último sólo a partir de Windows 2000).

Es el sistema ideal para las particiones de gran tamaño requeridas en estaciones de trabajo de alto rendimiento y servidores. Puede manejar discos de hasta 2 terabytes.

Desde Windows 2000 es posible convertir unidades FAT a NTFS, pero no al contrario.

Los inconvenientes que plantea son:

- Necesita para si mismo una buena cantidad de espacio en disco duro por lo que no es recomendable su uso en discos menores de 400 MB.
- No es compatible con MS-DOS, Windows 95 ni Windows 98.

Todos estos sistemas de archivos, y algunos más pueden convivir en un mismo duro siempre que se encuentren en particiones distintas, la decisión más delicada siempre será la de la primera partición primaria (C:) pues de ella depende el tipo de sistema operativo que podremos instalar en el equipo.

En la siguiente tabla se presenta resumida la información de compatibilidad entre sistemas operativos y sistemas de archivos (el signo más indica compatibilidad).

	FAT	VFAT	FAT 32	NTFS
DOS	+			
Windows 95	+	+		
Windows 95 OSR2	+	+	+	
Windows 98	+	+	+	
Windows NT	+	+		+
Windows 2000	+	+	+	+

Particiones y volúmenes.

Nota: Al crear o modificar las particiones en el disco duro perderemos la información que existiera previamente en este. Antes de leer estas secciones es recomendable leer el apéndice sobre discos duros.

Antes de particionar un disco duro no existe ninguna estructura lógica en este, una vez que comencemos a definir particiones tendremos la siguiente estructura:

- **Sector de arranque** (Master Boot Record).
- Espacio particionado (definido en la **tabla de particiones**).
 - **Particiones primarias:** sólo contienen una **unidad lógica**.
 - **Partición extendida:** pueden contener varias unidades lógicas.
- Espacio sin particionar.

A continuación vamos a explicar cada uno de estos conceptos.

Sector de arranque.

Es el primer sector del disco duro. Aquí se almacena la tabla de particiones y un programita encargado de ceder el control al sector de arranque de la partición activa cuando el equipo se inicia. En inglés se le denomina *Master Boot Record*.

Tabla de particiones.

Espacio del sector de arranque donde se almacena la información sobre las particiones definidas en el disco duro. Esto es, donde empiezan, donde acaban, de que tipo son y cual es la partición activa.

Partición.

Una partición es un espacio de almacenamiento definido dentro de un disco duro con un tamaño definido y constituido por secciones contiguas dentro de un disco duro.

Partición primaria.

Es un tipo de partición que se caracteriza por:

- Puede ser activada y, por tanto, cargar un sistema operativo.
- Sólo se puede definir una unidad lógica en ella.

En un disco duro puede haber hasta cuatro particiones primarias pero Windows 98 sólo soporta una. Windows 2000 soporta varias particiones primarias y puede ser instalado en cualquiera de ellas, sin embargo el programa que gestiona el arranque siempre tendrá que estar en la primera partición primaria del primer disco duro.

Partición extendida.

Se caracteriza por:

- No puede ser activada, por tanto no puede cargar un sistema operativo, aunque si puede contener los archivos de este. (Algunos gestores de arranque, por ejemplo el LILO de Linux, pueden cargar un sistema operativo que reside en una unidad extendida, sin embargo el propio gestor de arranque ha de estar en una partición primaria activa.)
- Se pueden definir una o más unidades lógicas dentro de ella.
- En un disco duro sólo puede haber una partición extendida.

Unidad física.

Cada disco duro es una unidad física distinta. El concepto de unidad física es utilizado por ejemplo por la BIOS del ordenador cuando reconoce las unidades de almacenamiento disponibles en el equipo.

Hay otros dispositivos que se reconocen como unidades físicas: disqueteras, lectores y grabadores de CDROM o DVD, discos ZIP y discos magneto-ópticos.

Unidad lógica.

Las unidades lógicas se definen siempre dentro de una unidad física de un disco duro, concretamente dentro de una partición. En una partición primaria sólo puede definirse una unidad lógica, sobre una partición extendida pueden definirse varias.

El resto de dispositivos de almacenamiento mencionados más arriba (disqueteras, lectores y grabadores de CDROM o DVD, discos ZIP y discos magneto-ópticos) se comportan como unidades lógicas y unidades físicas a la vez. Sobre estos soportes no se pueden definir particiones, algunos de ellos han de ser formateados con el sistema de archivos adecuado antes de usarse, otros no.

El concepto de unidad lógica es el que utiliza el sistema operativo. Sobre ellas trabajaremos cuando demos formato al disco con un sistema de archivos.

En Windows 2000 y XP una unidad lógica puede extenderse sobre varias particiones de varias unidades físicas.

Formato.

Cuando hablamos de formatear un disco duro podemos estar refiriéndonos a dos conceptos distintos:

- **Formato físico:** se aplica a todo el disco duro y se realiza desde la BIOS o desde programas especiales. Este formato no debe ser alterado por el usuario pues se corre el riesgo de dañar el disco duro. También se le suele llamar **formato de bajo nivel**.
- **Formato lógico:** se aplica a las particiones del disco duro, se suele realizar antes de instalar un sistema operativo o si queremos cambiar el sistema de ficheros de una unidad. S de este tipo de formato del que estamos hablando en este curso.

Al dar formato a una partición lo que hacemos es preparar a esta para utilizar un determinado sistema de ficheros. En este proceso se reserva un espacio (o varios) para la propia gestión del sistema de ficheros y se determina el tamaño del *cluster* o grupo. En este proceso se suele perder toda la información contenida anteriormente en el disco duro.

3.4. Práctica: utilizando el "administrador de discos" de Windows 2000.



3.5. Controladores de dispositivos.

Windows suele venir preparado para soportar cualquier hardware (por "soportar" entendemos que el sistema operativo y el hardware son compatibles) fabricado para PC.

Normalmente encontraremos los controladores (drivers) en el CD-ROM de instalación de Windows para hardware fabricado antes de la fecha de lanzamiento de nuestro sistema operativo. Para hardware fabricado con posterioridad recurriremos a los discos que nos proporcione el fabricante o buscaremos en la página web de éste.

Durante la instalación del sistema se detectarán casi todos los dispositivos conectados a nuestro PC, en caso de que no esté disponible algún controlador Windows nos pedirá que aportemos un controlador adecuado.

En Windows tenemos las siguientes opciones para indicarle donde buscar el controlador:

- Unidad de disquete.
- Unidad de CD-ROM.
- Actualización de Windows (buscará en el sitio web de Microsoft)
- Especificar una ubicación (en el disco duro o en una unidad de red).

Una vez Windows haya localizado una fuente adecuada para instalar los controladores es probable que nos pida identificar de forma concreta el modelo del dispositivo que estamos instalando, ya que suele ser frecuente que los archivos que contienen los controladores den soporte a varios modelos del mismo fabricante, por lo que tendremos que elegir el más adecuado a nuestro caso.

3.6. Práctica: instalando un controlador de dispositivo.

Esta práctica pretende familiarizarte con la instalación y desinstalación de controladores de dispositivos en el sistema y enseñarte a reconocer la versión de cada controlador.

NOTA: Si trabajamos con Windows 2000 y no tenemos ningún descompresor instalado podemos bajarlo desde <http://www.winzip.com> o <http://winrar.com.es>



3.7. Referencias.

- Microsoft; Requisitos mínimos para los distintos sistemas operativos de Microsoft; <http://support.microsoft.com/default.aspx?scid=kb;es;304297>
- Microsoft; *Lista de compatibilidad hardware para Windows 2000*; <http://www.microsoft.com/whdc/hcl/search.msp>
- Microsoft; *Catálogo de hardware para Windows XP*; <http://www.microsoft.com/windows/catalog/>
- Saulo Barajas; *Discos duros y particiones*; consultado el 26/01/2002; <http://www.saulo.net/pub/ddypart/> Inmejorable tratado sobre discos duros y particiones.
- José Manuel Tella Llop; *Disco duro y particiones*; http://www.multingles.net/docs/disco_duro_y_particiones.htm Una buena explicación de lo que es un disco duro, como funciona y como trabajar mejor con él.
- HelpDriver; <http://www.helpdrivers.com/espanol/index.htm>
- Download.com; *Drivers (en inglés)*; <http://download.com.com/2001-2014-0.html?tag=dir>

4. Comunicaciones y redes.

- Componentes de red.
- Configuración de TCP/IP.
- Práctica: configurando TCP/IP en Windows.
- Recursos compartidos.
- Práctica: compartiendo recursos en Windows.
- Referencias.

4.1. Componentes de red.

Los componentes de red de Windows son el conjunto de dispositivos físicos, protocolos y servicios que nos permiten conectarnos a otros equipos en red o acceder a otras redes como Internet.

En este tema daremos una visión de conjunto de cada uno de estos componentes, en sucesivos temas veremos en profundidad algunos de estos componentes.

Dispositivos físicos.

Son los adaptadores, puertos o periféricos que nos permiten conectarnos físicamente a la red. Los más usuales son: adaptadores de red ethernet y módems.

Un **adaptador de red** es una tarjeta de comunicaciones que conectamos a nuestro equipo para poder acceder a una red local (y posiblemente a Internet a través de esta misma red local). Hay diversos tipos de adaptadores en función del tipo de cableado que se utilice en la red, pero actualmente el más común es del tipo ethernet utilizando un interfaz o conector rj-45. Las tarjetas de red ethernet pueden variar en función de la velocidad de la red ethernet, normalmente 10MB o 10/100MB (esta última permite conectarse a redes que vayan a 10 o a 100MB). Otro tipo de adaptador muy extendido hasta hace poco era el que usaba conector BNC.

Los **módems** pueden ser tarjetas internas o bien dispositivos externos que permiten conectarnos a una red (normalmente Internet pero puede ser cualquier otra) utilizando la línea telefónica común. Hay distintos tipos de módem en función de la velocidad de transmisión que alcancen: 14.400, 28.800, 36.600 y 56.600 bps.

Hay otros tipos de dispositivos físicos para conectarse a una red como **tarjetas RDSI, adaptadores inalámbricos, módems ADSL**, etc.

En este curso nos centraremos en el uso de adaptadores de red ethernet.

Protocolos.

Un protocolo es un lenguaje especial que utiliza un sistema informático para comunicarse con otro. Los protocolos suelen estar organizados en distintas capas, siendo cada una de estas capas un protocolo en si, es por esto que muchas veces debemos referirnos a ellos como familia de protocolos. Por ejemplo TCP/IP es una familia de protocolos compuesta entre otros por los protocolos: TCP, UDP e IP.

En este curso hablaremos de la familia de protocolos **TCP/IP**.

Clientes y Servicios.

Los clientes de red nos permiten iniciar una sesión en un servidor dando un nombre y una contraseña y utilizar recursos disponibles en esos servidores o en otros equipos de forma remota. Los servicios de red nos permiten poner a disposición de otros usuarios nuestros recursos.

En este curso veremos:

Cliente para redes Microsoft: nos permite conectarnos a un servidor de dominio o a otros equipos con Windows.

Compartir impresoras y archivos para redes Microsoft: es un servicio en nuestro equipo que permite a otros usuarios conectarse a los recursos que queramos poner a su disposición.

4.2. Configuración de TCPIP.

La capacidad de TCP/IP para mover información en una red, por grande que sea y sin perder datos, su sistema de nombres y direcciones, y su facilidad para saltar de una red a otra lo convierten en el candidato ideal para cualquier red de ordenadores dispuesta a no quedarse dentro de las paredes de un edificio. TCP/IP es el protocolo con el que nos conectamos a Internet.

Necesitamos conocer algunos datos antes de comenzar a configurar una red basada en este protocolo:

- Direcciones IP.
- Máscara de red.
- Dirección del servidor de nombres.
- Dirección del encaminador (*gateway*).
- Nombre de host y nombre de dominio (no son imprescindibles).

Nota: si en nuestra red existe un servidor DHCP no necesitaremos asignar a mano ninguno de estos parámetros, durante la instalación de TCPIP dejaremos activada la opción: **Dirección IP asignada por el servidor**. Sin embargo es recomendable que estemos familiarizados con estos conceptos para saber administrar correctamente nuestra red.

Si no tenemos acceso a una red corporativa o queremos trabajar en una red aislada podemos usar las direcciones asignadas a redes ocultas.

Ahora veremos brevemente que significa cada uno de estos parámetros.

Dirección IP.

Número binario formado por cuatro octetos.

En su translación a decimal una dirección IP se compone de cuatro cifras separadas por puntos, cada una de estas cifras puede variar entre 0 y 255. Aquí tienes algunos ejemplos de direcciones IP:

150.214.141.130

130.10.1.200

10.150.130.5

Normalmente las direcciones que usarás en tu red te vendrán dadas por una instancia superior si son direcciones reales de Internet o las podrás elegir tú si se trata de direcciones ocultas para una intranet. En este último caso no podrás acceder directamente a Internet.

Necesitas una IP distinta para cada ordenador que vayas a configurar, normalmente las direcciones que te asignen serán consecutivas, a esto lo llamamos un rango de direcciones.

Máscara de red.

La máscara de red tiene el mismo formato que una dirección IP. Sirve para que el protocolo TCP/IP sepa distinguir entre la información que se envía a un equipo de nuestra propia red o a un equipo de otra red. En el segundo caso dicha información se enviará al encaminador o router. Todos los equipos de tu red tendrán normalmente la misma máscara de red.

Servidor de nombres.

También recibe el nombre de DNS (del inglés *Domain Name Server*). Es el equipo al que preguntará el nuestro cuando necesite traducir un nombre de Internet (por ejemplo: *coyote.acme.com*) a su dirección IP. Necesitamos indicar la dirección del DNS a nuestro equipo para que este sepa a quien dirigirse. Podemos tener más de un servidor de nombres asignados.

Si vamos a trabajar con una red oculta seguramente no dispondremos de acceso a un servidor de nombres.

Encaminador.

Recibe también los nombres de *gateway* o *router* en inglés. Es el equipo que encaminará hacia el exterior la información que no va a dirigida a ningún equipo de nuestra propia red. Podemos tener más de un encaminador en una red aunque no es muy corriente.

Nombre de host y nombre de dominio.

Aunque no son imprescindibles también podemos consignar un nombre de Internet para nuestro equipo de manera que podamos dirigirnos a él de esta forma en lugar de utilizar la dirección IP. Un nombre de Internet sería algo así como *coyote.acme.com*.

Este nombre se compone de dos partes: el llamado **nombre de host** (nombre de la máquina, *coyote* en nuestro ejemplo) y el **nombre del dominio** al que pertenecemos (*acme.com* en nuestro ejemplo). No confundamos este nombre de dominio con el concepto de "dominio" en Windows NT y 2000.

Normalmente nuestro nombre de host estará registrado en el servidor de nombres (DNS) de nuestra organización y lo podemos elegir nosotros mismos. El nombre de dominio nos viene dado por la organización a la que pertenecemos.

Redes ocultas.

Dentro del reparto de direcciones IP hay varios rangos de direcciones reservadas a redes aisladas (no conectadas a otras redes) o que al menos no van a acceder a Internet directamente.

En nuestro caso podemos utilizar el siguiente rango de direcciones reservadas: 192.168.0.0 - 192.168.255.255. Que suponen un total de 65025 direcciones IP.

Como posiblemente en nuestra red oculta haya menos de 253 equipos podemos usar las direcciones IP que van de: 192.168.1.1 a 192.168.1.254. Estos equipos pueden usar la

siguiente máscara: 255.255.255.0 y en principio no necesitamos servidor de nombres ni encaminador (no vamos a salir de la red local).

4.3. Práctica: configurando TCPIP en Windows.

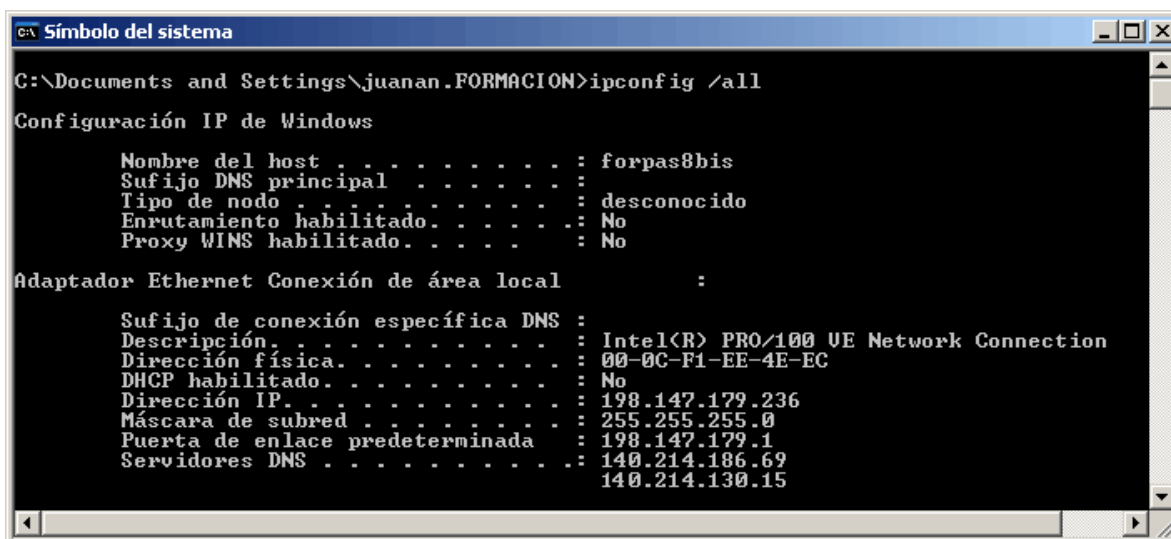
Nota importante.

En esta práctica instalaremos y configuraremos una red local con Windows utilizando el protocolo TCP/IP. El desarrollo de esta práctica no provocará pérdida de datos pero vamos a eliminar la configuración de red (si la hubiera), no obstante anotaremos previamente la configuración IP actual del sistema. En cualquier caso siempre es preferible trabajar con un ordenador de prácticas.

Configuración IP actual del sistema.

Para ver la configuración actual del sistema para el protocolo TCPIP:

1. Ejecutamos la orden **ipconfig /all** desde una ventana de comandos.
2. Si aparece un aviso anunciando que no hay datos de configuración IP disponibles significa que no tenemos instalada la tarjeta de red o que no hemos instalado el protocolo TCPIP. Por tanto no tenemos ningún dato que anotar y pasamos directamente a configurar los datos de configuración IP (punto 1 del siguiente apartado).
3. Se muestra un listado con los datos de configuración IP para el adaptador del equipo.



```
C:\Documents and Settings\juanan.FORMACION>ipconfig /all

Configuración IP de Windows

Nombre del host . . . . . : forpas8bis
Sufijo DNS principal . . . . . :
Tipo de nodo . . . . . : desconocido
Enrutamiento habilitado. . . . . : No
Proxy WINS habilitado. . . . . : No

Adaptador Ethernet Conexión de área local :

Sufijo de conexión específica DNS :
Descripción. . . . . : Intel(R) PRO/100 VE Network Connection
Dirección física. . . . . : 00-0C-F1-EE-4E-EC
DHCP habilitado. . . . . : No
Dirección IP. . . . . : 198.147.179.236
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada : 198.147.179.1
Servidores DNS . . . . . : 140.214.186.69
                             140.214.130.15
```

4. Anotamos en nuestra libreta el **Nombre del host** **Dirección IP**, la **Máscara de subred**, la **Puerta de enlace predeterminada** y los **Servidores DNS**. Si estos datos están en blanco pasamos directamente al punto 7.
5. Anotamos también la **Dirección física**, aunque este dato no podemos cambiarlo es conveniente que lo tengamos anotado pues identifica de forma inequívoca al ordenador en la red independientemente de la IP que le tengamos asignada.


6. Una vez anotados todos estos datos vamos al icono **Red** del **Panel de Control** y desde allí borramos el protocolo TCP/IP para poder instalarlo de nuevo. A continuación reiniciamos el sistema.

Instalación de TCP/IP

1. Abrimos el icono **Red** del **Panel del Control**, pulsamos el botón **Agregar** elegimos el tipo de elemento **Protocolo** en la siguiente ventana escogemos **Microsoft** y **TCP/IP**.
2. Una vez instalado lo configuramos de nuevo utilizando todos los datos que hemos anotado previamente y reiniciamos el equipo para que los cambios hagan efecto.

4.4. Recursos compartidos.

Compartir recursos con precaución.

Una de las mayores ventajas de instalar una red local es la capacidad de compartir recursos entre los ordenadores que forman la red. No obstante tenemos que pensar que cada recurso compartido es una puerta abierta en nuestro sistema que tendremos que asegurar y vigilar. A este respecto debemos seguir dos estrategias en paralelo: compartir sólo lo imprescindible  asegurar con contraseñas adecuadas lo que se comparta.

Compartir lo imprescindible

Aunque es más cómodo compartir un disco duro completo que tres directorios específicos merece la pena el esfuerzo. Al compartir el disco duro completo quedaría también expuesto nuestro directorio del sistema. Esto puede ser una oportunidad para un intruso o incluso una fuente de errores para los propios usuarios que accedan a la carpeta compartida. Por todo esto lo más adecuado sería estudiar detenidamente que necesitamos compartir exactamente.

Proteger los recursos

Para evitar daños voluntarios o involuntarios es importante también establecer cuidadosamente las contraseñas para proteger los recursos compartidos. Además de utilizar buenas contraseñas es muy importante tener claro cual de los dos tipos de acceso existentes debemos dar a cada usuario. En principio siempre nos plantearemos el dar a todos acceso de sólo lectura, esto puede proteger a nuestro equipo de la llegada de virus o troyanos desde otro sistema y puede evitar que otros usuarios borren involuntariamente nuestros datos. En algunos casos habrá que dar acceso completo a algún recurso, hagámoslo con cuentagotas y usemos contraseñas distintas para este tipo de acceso.

Si nuestros equipos forman parte de un dominio podemos especificar las configuraciones de acceso a los recursos de una forma mucho más personalizada y granular

4.5. Práctica: compartiendo recursos en Windows

Windows XP

Abra el **Explorador de Windows** (Inicio->Todos los programas->Accesorios->Explorador de Windows) y busque la carpeta o unidad que desea compartir.

Si ha iniciado sesión en un dominio, haga lo siguiente:

1. Haga clic con el botón secundario del *ratón* (ratón) en la carpeta o unidad que desee compartir y, a continuación, haga clic en **Compartir y seguridad**.
2. Haga clic en **Compartir esta carpeta**.
3. Establezca las opciones que desee y, después, haga clic en **Aceptar**.

Si no ha iniciado sesión en un dominio o está ejecutando Windows XP Home Edition, haga lo siguiente:

1. Haga clic con el botón secundario del ratón en la carpeta o unidad compartida y, después, haga clic en **Propiedades**.
2. En la ficha **Compartir**, haga clic en **Compartir esta carpeta en la red**.
3. Establezca las opciones que desee y, después, haga clic en **Aceptar**.

Windows 2000

1. Abra el **Explorador de Windows** y ubique la carpeta o unidad que desea compartir.
2. Haga clic con el botón secundario del ratón en la carpeta o unidad y después en **Compartir**.
3. En la ficha **Compartir**, haga clic en **Compartir esta carpeta**.
4. Establezca las opciones que desee y, después, haga clic en **Aceptar**.

Notas

- Para compartir carpetas y unidades, debe iniciar la sesión como miembro del grupo Administradores, Operadores de servidores o Usuarios avanzados.
- Para abrir el Explorador de Windows, haga clic en **Inicio**, seleccione **Programas**, **Accesorios** y, a continuación, haga clic en **Explorador de Windows**.
- Si la ficha **Compartir** no está visible, intente usar el complemento **Servicios** para iniciar el servicio Servidor.

- Si la carpeta ya está compartida, haga clic en **Nuevo recurso compartido** y escriba el nombre nuevo del recurso.
- Puede ocultar la carpeta compartida de forma que no se pueda examinar si escribe \$ como el último carácter del nombre del recurso. Los usuarios no podrán ver esta carpeta compartida cuando examinen con Mi PC o el Explorador de Windows, aunque podrán asignarla si conocen el nombre, incluyendo el dólar.
- En Windows 2000 Professional, el límite máximo de usuarios es 10 con independencia del número que escriba en **Permitir**.
- Puede usar el complemento **Carpetas compartidas** para crear y administrar las carpetas compartidas, ver una lista de los usuarios que están conectados a la carpeta compartida a través de una red y desconectar a uno o a todos ellos, y ver una lista de archivos abiertos por usuarios remotos y cerrar uno o todos los archivos abiertos.

4.6. Referencias.

- Federico Reina y Juan Antonio Ruiz; *Introducción a las redes de área local*;
http://enete.us.es/docu_enete/varios/redes/indice.asp

5. La línea de comandos

Adorada por algunos y temida por muchos la línea de comandos de cualquier sistema operativo es lo más parecido a hurgar en las entrañas del sistema operativo para sacar de su interior el máximo rendimiento posible.

Un sistema operativo tiene tal cantidad de comandos, opciones y configuraciones que es imposible trasladarlas todas al universo de las ventanas y los iconos, así que para hacer ciertas cosas hay que “pringarse” y zambullirse en la línea de comandos.

Aunque en este curso no vamos a llegar a estos niveles si es conveniente tener al menos unas nociones básicas de lo que es la línea de comandos, como invocarla y como trastear luego un poco con ella.

Para acceder a la línea de comandos desde Windows lo más sencillo es pulsar “Inicio -> Ejecutar -> command”. Ya tenemos nuestra ventanita negra. Ahora vayamos con algunos comandos sencillos.

cd

Del inglés “change directory”: cambiar directorio. Este comando nos sirve para movernos por el árbol de directorios de cualquier unidad de nuestro sistema. Algunos ejemplos:

- `cd \` - va al directorio “raíz” de la unidad.
- `cd directorio` - va al directorio designado, siempre que sea “hijo” del actual
- `cd ..` - va al directorio “padre” del actual, si ya está en el raíz no hace nada.

dir

Muestra los ficheros en el directorio actual por defecto, o en el que le indiquemos como parámetro. Ejemplos:

- `dir` - muestra todos los archivos y directorios del directorio actual (excepto los ocultos y de sistema)
- `dir documentos*.txt` - muestra todos los archivos del subdirectorio “documentos” con extensión txt.
- `dir /s` - muestra todos los archivos y directorios contenidos en la unidad
- `dir |more` - hace un listado parando pantalla por pantalla

attrib

Muestra, establece o quita los atributos de sólo lectura, modificado, sistema y oculto asignados a los archivos o a los directorios. Utilizado sin parámetros, muestra los atributos de todos los archivos del directorio actual. (**a**=modificado, **r**=sólo lectura, **h**=oculto, **s**=sistema).

ver

Muestra la versión del sistema operativo que estamos usando.

cmd

Ejecuta una nueva ventana del intérprete de comandos

help

Muestra todos los comandos disponibles en la línea de comandos. Es un buen recurso para aprender más sobre la línea de comandos. Si queremos saber más sobre algún comando en concreto utilizaremos el modificador “/?” a continuación del nombre del comando sobre el que queremos saber, por ejemplo: `dir /?`

6. Actualización del sistema.

- Precauciones.
- Como y porqué mantener un sistema actualizado.
- Referencias.

6.1. Precauciones.

Realizar una actualización de nuestro sistema o de algunos de sus componentes puede conllevar algunos riesgos, es por ello necesario tomar algunas precauciones de iniciar la actualización:

- Realizar una copia de seguridad de todo el sistema antes de instalar.
- Realizar una copia de seguridad del registro.
- Leer los ficheros "leame" o "readme" que suelen acompañar a los ficheros de instalación.

Algunas de estas precauciones, si no todas, también pueden aplicarse a la hora de instalar aplicaciones en nuestro equipo.

6.2. Actualizaciones disponibles

Veamos a continuación los recursos de que disponemos para mantener nuestros sistemas Windows actualizados.

Windows Update.

Windows Update es una utilidad de Windows que se encarga de revisar nuestro equipo para determinar si se necesita realizar alguna actualización del sistema operativo, aplicar algún parche de seguridad, etc.

Al pulsar sobre el icono de Windows Update nos lleva a una página web de Microsoft que mediante un control "Active X" chequea nuestro sistema para verificar las actualizaciones que debemos realizar, las actualizaciones realmente necesarias reciben el nombre de "actualizaciones críticas".

Windows Update dispone de un catálogo central denominado "Actualizaciones de productos" que incluye las nuevas mejoras de productos como archivos de sistema, controladores de dispositivo, "Service Pack" y características nuevas de Windows. Estas mejoras se recomiendan en función de las necesidades específicas de su equipo.

Si no podemos localizar el icono de Windows Update en nuestro sistema podemos acudir directamente a la dirección web <http://windowsupdate.microsoft.com/>

Hot-Fix.

Microsoft mantiene una base de datos con todas las actualizaciones disponibles para Windows, estas actualizaciones reciben el nombre de "Hot-Fix". Los "Hot-Fix" suelen ir encaminados a solucionar un solo problema y su instalación suele conllevar alguna manipulación en el registro.

Cuando el número de Hot-Fix es significativo y Microsoft así lo decide se libera un "Service Pack".

Service Pack.

Un Service Pack es un conjunto de hot-fix o parches distribuidos en un solo paquete. Además son acumulativos, por tanto, instalando el último disponible no es necesario instalar los anteriores.

Es muy recomendable que después de instalar nuestro sistema con Windows busquemos el último Service Pack disponible y lo instalemos también. Además tenemos que tener en cuenta que si reinstalamos algún componente del sistema desde el CD original o agregamos algún nuevo hardware al sistema es conveniente reinstalar de nuevo el último Service Pack.

La ventaja de los Service Pack frente a los Hot-Fix es que no requieren manipulación posterior en el registro, se instalan de una vez y están mejor testados por Microsoft, sin embargo no tienen la inmediatez de un Hot-Fix cuya instalación es a veces realmente crítica, sobre todo en cuestiones de seguridad.

Tanto unos como otros suelen depender de la versión del lenguaje en que hayamos instalado nuestro sistema, por lo que es importante que nos descargemos la versión adecuada.

Existen Hot-Fix y Service Packs disponibles para otras aplicaciones de Microsoft como "Internet Information Server", "SQL Server" o "Microsoft Office".

Para quien tenga una conexión a Internet que no le permita bajarse los inmensos ficheros de un Service Pack es conveniente saber que estos suelen ser distribuidos a menudo en los CDs que acompañan a las revistas especializadas en informática.

6.3. Cómo y porqué mantener un sistema actualizado.

Las razones para mantener un sistema actualizado pueden resumirse en los siguientes puntos:

- Solucionar problemas de seguridad.
- Solucionar problemas de funcionamiento.
- Obtener nuevas prestaciones.

Cuando no debemos actualizar.

Normalmente no debemos precipitarnos a instalar cualquier actualización del sistema sin pensarlo dos veces, muchas veces un equipo que está funcionando correctamente puede empezar a dar problemas después de una actualización, otras veces la actualización sencillamente no es necesaria.

Por ejemplo alguna actualización o hot-fix de seguridad quizás no sea necesaria en nuestro sistema porque éste no está expuesto a ese ataque, o el error que corrige el parche afecta a una utilidad o servicio del sistema operativo que nunca utilizamos.

Por todo esto suele ser aconsejable leer antes los beneficios que nos puede aportar la actualización o los problemas que trata de cubrir.

No obstante casi siempre es aconsejable instalar los Service Pack, suelen estar suficientemente garantizados y su instalación no suele dar problemas, aunque por supuesto han ocurrido excepciones a esta norma.

En cualquier caso si finalmente nos decidimos a actualizar un sistema cuyo funcionamiento es crítico debemos cubrirnos siempre las espaldas con una copia de seguridad completa.

6.4. Práctica: actualizando con Windows Update.



6.5. Referencias.

- Microsoft; *Windows Update*; <http://windowsupdate.microsoft.com/>



7. Seguridad.

- Seguridad en Windows.
- Protegerse contra los virus.
- Copias de seguridad.
- Práctica: haciendo una copia de seguridad.
- Contraseñas seguras.
- Referencias.

7.1. Seguridad en Windows.

Windows 2000 y Windows XP son sistemas preparados para dar seguridad. Sin embargo esta seguridad no viene "de fábrica". Aunque ahora las cosas parecen estar cambiando la política de Microsoft ha sido siempre sacrificar seguridad a favor de facilidad.

Por tanto un sistema con Windows tendrá el grado de seguridad que nosotros configuremos, desde ninguna seguridad hasta los requisitos más exigentes de autoridades internacionales en el tema.

Para ello incorpora una colección de tecnologías y herramientas que se escapan de los objetivos de este curso. Algunos consejos para mantener un sistema moderadamente seguro con Windows 2000 o XP serían:

- Utilizar el sistema de ficheros NTFS.
- No utilizar la clave de administrador para acceder normalmente al sistema.
- Configurar los permisos de ficheros adecuados a cada grupo de usuarios en un sistema multiusuario.
- Configurar auditorías básicas de seguridad y hacer un seguimiento periódico desde el visor de sucesos.

Aparte de utilizar estos recursos, y muchos otros disponibles debemos respetar también las siguientes reglas básicas:

- Protegerse contra virus y troyanos.
- Hacer copias de seguridad.
- Compartir recursos con precaución.
- Utilizar recursos desconocidos con precaución.
- Cuidar las contraseñas.

7.2. Protegerse contra los virus.

Los virus informáticos han llegado a convertirse en el principal quebradero de cabeza de muchos usuarios y de todos los administradores de red. Es por ello conveniente estar al tanto de los virus que pueden atacarnos, de los efectos que provocan y de cuales son las formas de contagio más usuales.

Ahí van cinco reglas de oro para disminuir las posibilidades de una infección:

1. Instala un antivirus.
2. Aprende como funciona.
3. Configúralo adecuadamente.
4. Mantenlo actualizado.
5. No te fíes de él.

Instala un antivirus.

Esto lo hace cualquiera, pero no basta con eso.

Cómo funciona un antivirus.

Los antivirus más usuales son programas residentes en memoria que trabajan continuamente en segundo plano monitorizando los archivos que transitan por nuestro ordenador.

Un antivirus trabaja comparando el contenido de los archivos de nuestro ordenador con una serie de patrones que aparecen en los virus de los que él tiene constancia. De aquí surgen dos cuestiones interesantes:

- ¿Qué archivos debe monitorizar nuestro antivirus y cuándo debe hacerlo?
- ¿Qué sucede si un archivo se encuentra infectado con un virus que el antivirus desconoce?

Cuando instalamos un antivirus en nuestro sistema lo primero que hará será buscar virus en la memoria principal del ordenador (memoria RAM), luego analizará el sector de arranque de nuestro disco duro (refugio habitual de algunos virus) y por fin chequeará los archivos existentes en nuestro disco duro. Si no encuentra ningún virus el antivirus se instala y desde ese momento comienza a trabajar a la sombra, analizando sólo aquellos ficheros que se vayan invocando: los que se copian en nuestro disco duro, los que se cargan para ser ejecutados y algunos de los que se leen para mostrar su contenido.

Es importante en este momento ver como está configurado nuestro antivirus, ante que acciones reacciona, que tipo de ficheros está vigilando, si está configurado para prevenirnos de los virus que pueden entrar por el correo electrónico, etc.

Como configurar un antivirus.

Los antivirus normalmente vienen configurados por defecto para monitorizar o escanear al menos todos los archivos ejecutables y scripts (exe, com, bat, pif, dll, vbx, etc.) que son los únicos que permiten que un virus pueda actuar en nuestro sistema. Además de estos, otros archivos en apariencia inocentes como los documentos de Word y Excel pueden infectar nuestro sistema ya que pueden contener macros que también se ejecutan como si de cualquier otro programa se tratara. Algunos virus también pueden pasar la inspección dentro de ficheros comprimidos que al descomprimirse pueden infectar nuestro sistema si son ejecutados. Todo esto se puede configurar en nuestro antivirus, incluso podemos pedirle que escanee absolutamente todos los ficheros, esto último sin embargo puede hacer que baje el rendimiento en algunos equipos escasos de recursos.

Otro paso importante en la configuración de un antivirus es indicarle al programa que posibles medios o vías de infección debe vigilar para impedir la entrada de estos dañinos programas, así podemos configurar el antivirus para que escanee la entrada de virus a través del correo electrónico, de los disquetes, de la red e incluso de páginas web que visitemos. Si usamos estos recursos debemos protegernos frente a ellos mediante estas opciones.

Por último es importante configurar nuestro antivirus para que se actualice periódicamente.

Como y cuando actualizar nuestro antivirus.

Casi todos los antivirus actuales suelen venir preparados con alguna utilidad que se conecta a un recurso de Internet de forma periódica para bajar nuevos patrones de virus y mantenerse actualizado. Pero casi ninguno de ellos realiza esta labor si no lo configuramos previamente, es importante saber cuando se está actualizando nuestro antivirus y si se está haciendo adecuadamente.

En el panel "**Acerca de**" de casi todos los antivirus suele venir la fecha del último archivo de actualización que nos hemos descargado.

En la actualidad casi todos los fabricantes liberan nuevas actualizaciones cada semana aunque puntualmente lo pueden hacer con mayor frecuencia, por ello no está de más tener nuestro antivirus para que compruebe si existen actualizaciones diariamente.

No confiarnos en nuestro antivirus.

Nada es perfecto, nuestro antivirus tampoco. Confiarnos ciegamente en él puede ser en ocasiones tan pernicioso como no tener ninguno instalado.

No debemos dejar de mantener copias de seguridad de nuestros datos, no debemos abrir a la ligera cualquier archivo que nos envíen por correo electrónico o por cualquier otro medio, sobre todo si no los hemos solicitado, por último debemos mantenernos informados de los nuevos peligros a los que no exponemos visitando con cierta frecuencia alguna sitio en Internet relacionado con temas de seguridad o suscribiéndonos a alguna lista de distribución de noticias.

7.3. Copias de seguridad.

A veces escucho a alguien decir que ha perdido meses de trabajo por culpa de un virus informático o de una avería en el disco duro. Bueno, esa ha podido ser la causa inmediata, pero el único responsable de la pérdida es el usuario o administrador que ha dejado de hacer, o que nunca ha hecho, sus copias de seguridad. Confiar nuestros datos a algo tan volátil como los platos magnéticos de un disco duro es jugar a la ruleta rusa con ellos, más nos valdría empezar a escribir nuestros trabajos en la pared.

Una de las mayores catástrofes que pueden ocurrir en nuestro ordenador o en alguno de los que administramos es la pérdida de datos equivalentes a horas de trabajo nuestras o de otras personas. Un sistema operativo con sus aplicaciones se puede instalar en horas, un disco duro averiado se puede reemplazar por otro, pero los datos de un equipo pueden suponer semanas o años de trabajo y a menudo son irremplazables. Y ahora que tire la primera piedra quien tenga copias de seguridad de todos los datos de los que debería tener respaldo.

Por ello una de las primeras cosas que debemos plantearnos al adquirir un ordenador o una instalación de ordenadores es como vamos a hacer las copias de seguridad, las preguntas que tenemos que responder son:

- ¿En qué soporte físico?
- ¿Con qué periodicidad?
- ¿Con que estrategia de almacenamiento?
- ¿De qué datos?
- ¿Centralizada o local?

Soporte físico

El soporte físico viene muy condicionado por dos parámetros: presupuesto disponible y volumen de datos.

Los dispositivos más usuales para hacer copias de seguridad de menor a mayor precio son:

- Regrabadora de CDROM.
- Disco magneto-óptico y similares.
- Grabadora de DVD.
- Unidad de cintas (*streamer*).

La regrabadora de CDROM es la mejor solución en un equipo particular o en instalaciones pequeñas. Además de servirnos para hacer copias de seguridad de CDs que hayamos adquirido la podemos utilizar como dispositivo para hacer copias de seguridad de nuestros propios datos. Tenemos que tener en cuenta que la capacidad máxima de un CD es de 740 MB o quizás el doble comprimiendo los datos. Realizar copias de seguridad utilizando dos o más CDs es muy engorroso, pero a veces no queda otra opción. Utilizaremos CDs

regrabables para las copias más frecuentes y CDs grabables para las más espaciadas y que vayamos a almacenar definitivamente.

Los discos magneto-ópticos y similares pueden ser también una buena opción, aunque por lo general tienen menos capacidad que un CD. No obstante los discos se pueden reutilizar casi eternamente y son muy rápidos.

La grabadora de DVD puede ser una opción económica y de gran capacidad cuando se hagan más populares, aunque quizás ya puedan constituir una buena opción.

Las unidades de cintas son los dispositivos más habituales de copia de seguridad en cualquier instalación informática que se precie. Hay una gran oferta en cuanto a precio y prestaciones pero para empezar a hablar de fiabilidad el coste al menos triplica el de la grabadora de CDs, en cualquier caso la capacidad de almacenamiento también aumenta en proporción.

Periodicidad

La periodicidad con que hemos de realizar las copias de seguridad vendrá en función de la tasa de cambios (archivos nuevos y archivos modificados diariamente). En instalaciones de varios usuarios debemos hacer las copias diariamente, en equipos caseros quizás podamos hacerla semanalmente.

Estrategia de almacenamiento

A veces podemos seguir haciendo copias de seguridad durante meses sin advertir que hemos perdido información importante, si siempre reciclamos el soporte habremos perdido dicha información para siempre. Es por esto que cada cierto tiempo debemos almacenar de manera definitiva nuestras copias de seguridad.

Una buena idea es reutilizar un mismo soporte unas cuantas veces y hacer luego sobre el mismo una última copia de seguridad que archivaremos definitivamente.

Para llevar todo esto a buen puerto es conveniente hacerse un pequeño esquema de cómo vamos a hacer nuestras copias de seguridad. Sobre este esquema iremos marcando las copias de seguridad que vayamos haciendo para llevar un mejor control.

Datos que debemos respaldar

Si podemos permitirnoslo deberíamos tener copia de seguridad del sistema completo, de esta forma podemos poner rápidamente en funcionamiento el equipo de nuevo en caso de que se produzca cualquier problema. Esta opción es muy recomendable si hacemos las copias desde un servidor de red como veremos en el próximo apartado.

Si este volumen de datos es demasiado alto para nuestros dispositivos de copia de seguridad lo mejor será acostumbrarnos a utilizar una partición o unidad lógica del disco duro sólo para los datos de trabajo y hacer únicamente copia de dicha unidad. Si tenemos problemas de espacio no deberíamos almacenar en esta unidad archivos de terceros que podemos recuperar por otros medios (por ejemplo Internet).

Copia de seguridad centralizada

Cuando hablamos de varios equipos conectados en red podemos hacer las copias de seguridad desde un solo equipo. Esto centralizará el trabajo del encargado de hacer las copias de seguridad y abaratará costes.

Tenemos dos opciones: compartir en red las unidades con los datos desde cada estación y hacer las copias de seguridad desde el servidor o bien guardar los datos desde cada estación siempre en un único equipo la red y hacer copias sólo de este equipo.

La elección posiblemente dependa de la forma en que trabajemos actualmente en nuestra red, aunque tener los datos en un ordenador central parece la opción más eficiente y segura.

7.4. Contraseñas seguras.

Muchos usuarios piensan que la importancia de los datos que tienen almacenados en un equipo no justifica el uso de una contraseña complicada para protegerlas. Esto puede ser un buen argumento pero hemos de pensar que cuando usemos una contraseña insegura no estamos comprometiendo sólo la seguridad de nuestros datos o nuestra cuenta sino la del sistema completo del cual somos usuarios. Igualmente puede quedar comprometida la seguridad de la red donde se encuentra dicho sistema. Normalmente los atacantes de un sistema intentan siempre hacerse pasar por un usuario cualquiera del sistema para luego ir ganando privilegios administrativos.

Existen una serie de reglas universales para que las contraseñas que con tanta frecuencia utilizamos sean un poco más seguras. He aquí algunas de ellas.

- Nunca utilizar el nombre de usuario como contraseña o una pequeña variación de este.
- No utilizar datos personales que puedan ser averiguados fácilmente: apellidos, DNI, fecha de nacimiento, etc.
- Utilizar contraseñas de 7 o más caracteres. Mezclando letras y números y si el sistema lo permite utilizando signos de puntuación. Esto hace que la contraseña sea más robusta frente a ataques de fuerza bruta (programas que van probando combinaciones de letras y números hasta que hallan la contraseña).
- No utilizar palabras que existan en el diccionario. Normalmente el ataque contra una contraseña comienza pasando un diccionario de palabras contra esta.
- Cambiar periódicamente nuestras contraseñas.
- No utilizar las mismas contraseñas en sistemas que requieren niveles de seguridad distintos.

7.5. Referencias

- Hispasec; <http://www.hispasec.com>
- *Sección de seguridad de Microsoft Technet en Inglés;* <http://www.microsoft.com/technet/security/> Información muy actualizada
- *Lista de correo NTBugtraq;* <http://www.ntbugtraq.com/> Sitio web de esta lista de correo que discute temas de seguridad en Windows NT, Windows 2000, Windows XP y aplicaciones relacionadas.
- *Página web del CERT;* <http://www.cert.org/> Equipo de respuestas a emergencias en computadoras
- David Chernicoff; *Copias de seguridad: Estrategias;* http://www.w2000mag.com/atrasados/1999/33_julago99/articulos/opinion.htm Se trata de un artículo ilustrativo y simpático sobre como encarar una estrategia de copias de seguridad.
- *Registro de Windows;* <http://zdnet.terra.com.hn/sp/helptips/stories/guides/1,,8015832,00.html> Describe en detalle como y porqué hacer copias de seguridad del registro de Windows.
- Mc Afee; <http://www.mcafee.com>
- <http://www.antivirus.com>
- <http://www.avp.ch>
- Panda Software; <http://www.pandasoftware.es>

8. El registro de Windows.

- Introducción al registro
- Estructura del registro.
- El editor del registro.
- Práctica: haciendo copia de seguridad del registro.
- Práctica: cambiando algunas claves del registro.
- Referencias.

8.1. Introducción al registro.

El registro es una base de datos que contiene prácticamente toda la información de configuración de nuestro sistema. Almacena la información de configuración del propio sistema operativo, del hardware, de la de las aplicaciones instaladas y las preferencias establecidas por cada usuario del sistema. Windows continuamente hace referencia a esta información durante su funcionamiento.

Aprender a trabajar con el registro nos va a permitir configurar un sistema con un grado de meticulosidad difícil de alcanzar de otra forma, así como aprender a realizar copias de seguridad de la información en él contenido nos protegerá de algunos desastres y nos puede ahorrar muchas horas de trabajo.

No obstante tenemos que tener muy en cuenta que trabajar con el registro es muy delicado, podemos realizar cambios que pueden dejar inutilizado el sistema o perder importantes parámetros de configuración. Es importante asegurarnos que tenemos una copia de seguridad actualizada del registro antes de empezar con él y aún así andarnos con pies de plomo al crear, modificar o eliminar claves del registro. No hagamos cambios en el registro si no sabemos lo que estamos haciendo, posiblemente no haya marcha atrás.

8.2. Estructura del registro.

El registro está organizado como una estructura jerárquica en forma de árbol, las "hojas" del árbol, llamadas **valores** son pares ordenados con un nombre y un valor, las "ramas" del registro reciben el nombre de **claves**.

Esta estructura jerárquica nos permite encontrar cualquier valor del registro de forma parecida a como indicamos la ruta de un fichero en un árbol de directorios, por ejemplo HKEY_CLASSES_ROOT/batfile/DefaultIcon almacena la información del icono que se mostrará cuando listemos ficheros con extensión ".bat".

En la tabla siguiente se muestran las claves principales o "raíces" del registro.

Carpeta o clave	Descripción
HKEY_CURRENT_USER (HKCU)	Contiene la raíz de la información de configuración del usuario que ha iniciado la sesión. Aquí se almacenan las carpetas de usuario, los colores de pantalla y la configuración del Panel de control. Esta información se conoce como perfil de usuario.
HKEY_USERS (HKU)	Contiene la raíz de todos los perfiles de usuario del equipo. HKEY_CURRENT_USER es una subclave de HKEY_USERS.
HKEY_LOCAL_MACHINE (HKLM)	Contiene información de configuración específica del equipo (para cualquier usuario).
HKEY_CLASSES_ROOT (HKCR)	Es una subclave de HKEY_LOCAL_MACHINE\Software. Aquí se almacena la información que asegura que se abre el programa correcto al abrir un archivo con el Explorador de Windows.
HKEY_CURRENT_CONFIG (HKCC)	Contiene información acerca del perfil de hardware que utiliza el equipo local al iniciar el sistema.


En la tabla siguiente se indican los tipos de datos definidos y utilizados por el sistema.

Tipos de datos	Descripción
REG_BINARY	Datos binarios sin procesar. La mayor parte de la información de los componentes de hardware se almacena en forma de datos binarios y se presenta en el Editor del Registro en formato hexadecimal.
REG_DWORD	Datos representados por un número de 4 bytes de longitud. Muchos parámetros de controladores de dispositivo y de servicios son de este tipo, y se presentan en el Editor del Registro en formato binario, hexadecimal o decimal.
REG_EXPAND_SZ	Cadena de datos de longitud variable. Este tipo de datos incluye variables que se resuelven cuando un programa o un servicio utilizan los datos.
REG_MULTI_SZ	Una cadena múltiple. Los valores que contienen listas o valores múltiples legibles suelen ser de este tipo. Las entradas están separadas mediante espacios, comas u otras marcas.
REG_SZ	Cadena de texto de longitud fija.
REG_FULL_RESOURCE_DESCRIPTOR	Serie de tablas anidadas, diseñadas para almacenar una lista de recursos para un componente de hardware o un controlador.

8.3. El Editor del registro.

No existe ningún icono en el menú de Inicio de Windows para cargar el editor del registro, así que lo lanzamos con **Inicio -> Ejecutar -> regedit**.

Una vez iniciado veremos dos paneles: el de la izquierda nos muestra algo parecido a un árbol de directorio, que son las claves del registro representadas en formas de carpetas, a la derecha podremos ver los valores contenidos en la clave que tengamos seleccionada en el panel de claves.

Pulsando en  iconos en forma de carpeta del panel izquierdo iremos abriendo claves y expandiendo otras claves subordinadas, los valores contenidos en cada clave aparecerán en el panel de la derecha. Pulsando en los nombres de los valores del panel de la derecha podremos editar el contenido de estos.

Veamos ahora como trabajar con las claves y los valores.

Para agregar una clave.

1. Abra la lista del Registro en el lugar donde desea agregar la clave nueva.
2. Haga clic con el botón secundario del ratón en la carpeta donde desea agregar la clave nueva.
3. Vaya a Nuevo y después haga clic en Clave. La clave nueva aparecerá con un nombre temporal.
4. Escriba el nombre de la nueva clave y presione ENTRAR

Para agregar un valor.

1. Abra la lista del Registro en la carpeta donde desea agregar el valor nuevo.
2. Haga clic con el botón secundario del ratón donde desee agregar el valor nuevo
3. Vaya a Nuevo y después haga clic en el tipo de valor que desee agregar. El valor nuevo aparecerá con un nombre temporal.
4. Escriba el nombre de la nueva carpeta y presione ENTRAR.

Para cambiar un valor.

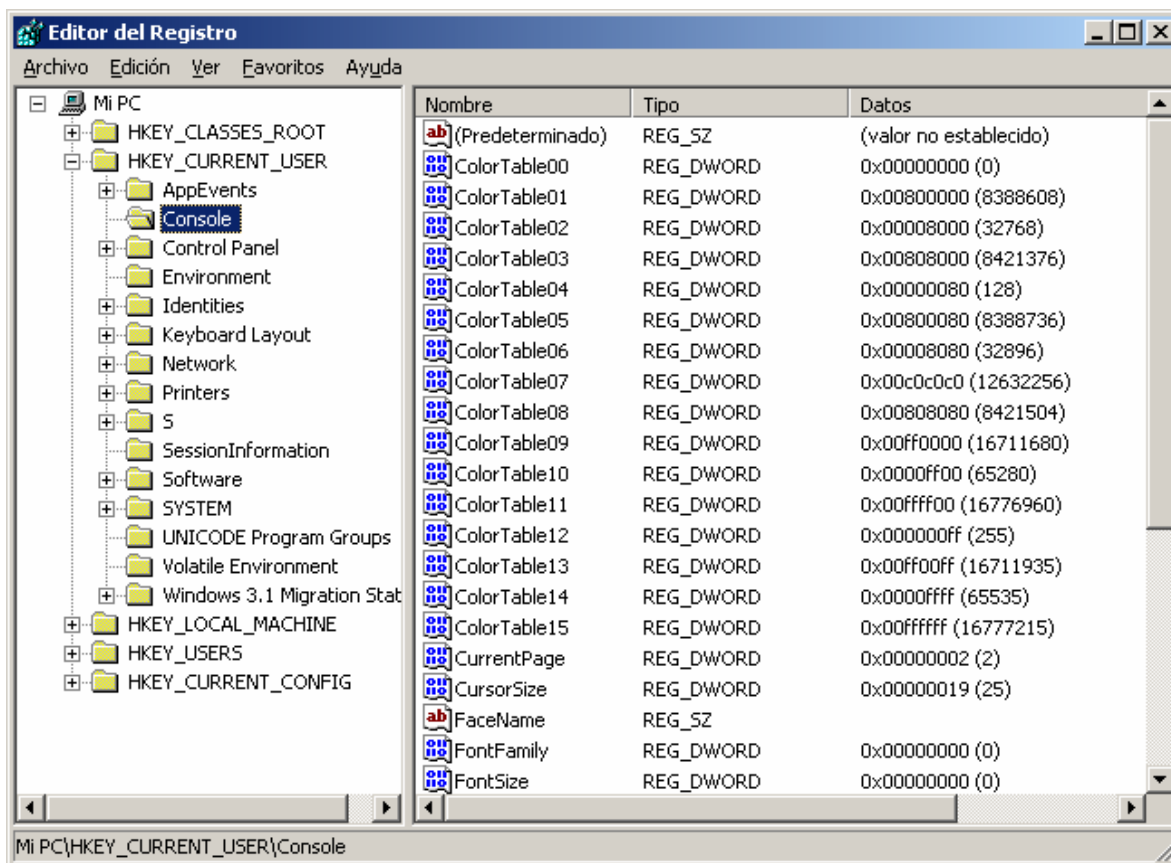
1. Haga doble clic en el valor que desea cambiar.
2. En Información del valor, escriba los nuevos datos del valor.

Para eliminar una clave o un valor.

1. Busque la clave o el valor que desea eliminar. No necesita abrirlo.
2. Haga clic con el botón secundario del ratón en una clave o en un valor y después haga clic en Eliminar.

Para cambiar el nombre de una clave o de un valor.

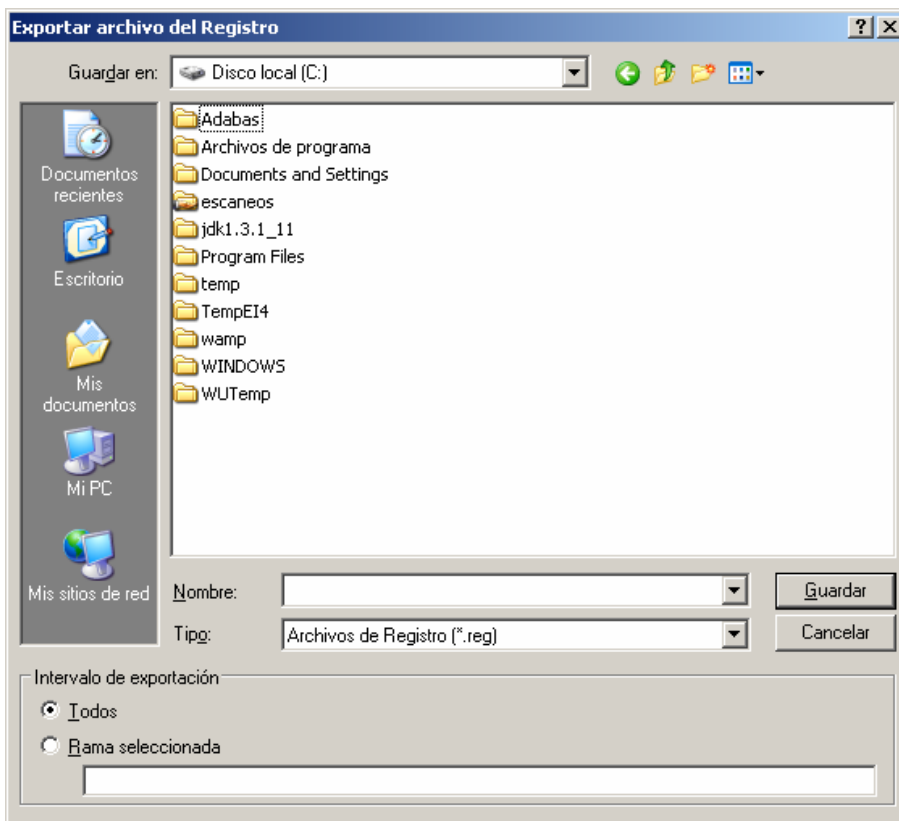
1. Busque la clave o el valor al que desea cambiar el nombre. No necesita abrirlo.
2. Haga clic con el botón secundario del ratón en la clave o el valor cuyo nombre desee cambiar y después haga clic en Cambiar nombre.
3. Escriba el nuevo nombre y, a continuación, presione ENTRAR.



8.4. Práctica: haciendo copia de seguridad del registro.

Antes de curiosear por el registro y hacer modificaciones “peligrosas” conviene tener una copia completa de su contenido.

1. Ejecutamos **regedit** desde **Inicio ->Ejecutar**.
2. Desde el menú **Archivo** seleccionamos **Exportar**.
3. En el cuadro de texto **Nombre del archivo** escribimos "Registro completo", en el cuadro de texto **Guardar en** comprobamos que aparece "Escritorio".
4. En la sección **Intervalo de exportación** seleccionamos la opción **Todos** para guardar el registro completo.
5. Hacemos clic en **Guardar** y nos salimos del Editor del registro.



Para restaurar esta copia del registro sólo tenemos que hacer doble clic en el fichero que acabamos de crear.

También pueden hacerse copias completas del registro con la utilidad **scanreg** desde la línea de comandos.

8.5. Práctica: cambiando algunas claves del registro.

Programas que se cargan al iniciar Windows.

Estos programas se cargarán antes de iniciar sesión en el sistema:

```
HKEY_LOCAL_MACHINE \Software\Microsoft\Windows\CurrentVersion\
```

Mirar y modificar los valores de `Run` y `RunOnce` que deseemos.

Localización de los archivos de instalación.

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Setup
```

Cambiar el valor de `SourcePath` a la ruta que queremos utilizar cada vez que el sistema solicite el disco de instalación, lo más cómodo puede ser ubicar estos en una unidad de red.

Automatizar el inicio de sesión en red.

Cambiaremos los siguientes valores en la clave

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Winlogon
```

- `DefaultUserName`: nombre del usuario con el que iniciaremos sesión.
- `DefaultPassword`: contraseña de dicho usuario.
- `AutoAdminLogon`: poniendo este valor a 1 se habilita el inicio de sesión automático, si lo ponemos a 0 queda deshabilitado.

8.6. Referencias.

- Jerry Honeycut; *Windows 98 Registry Handbook*; Editorial QUE; 1998.
- *Registro de Windows*; Describe en detalle como y porqué hacer copias de seguridad del registro de Windows;
<http://zdnet.terra.com.hn/sp/helptips/stories/guides/1,,8015832,00.html>
- Busca las palabras: "Windows", "Registry", "Tip" en cualquier buscador de Internet, www.google.com por ejemplo.

9. Resolución de problemas en Windows.

- Comprobaciones básicas ante la existencia de un problema.
- Problemas de conexión a red.
- Recuperación de archivos del sistema.
- Referencias.

9.1. Comprobaciones básicas ante la existencia de un problema.

- Comprobar si tenemos nuestro antivirus actualizado y hacer un chequeo a fondo del equipo con este.
- Utilizar la herramienta "Información del sistema" para ver cualquier dispositivo o software que esté ocasionando problemas.
- Utilizar el "Programa de configuración del sistema" para reiniciar nuestro equipo en modo interactivo y buscar una posible causa del problema durante el arranque.
- Utilizar el "Comprobador de archivos de sistema".
- Utilizar el "Comprobador de registro".
- Comprobar el espacio disponibles en la partición del sistema (C:), chequear el estado del disco duro con *chkdsk* y realizar una desfragmentación del mismo si fuera necesario.

Herramienta de información del sistema.

Nos permite conocer el estado actual del sistema con gran cantidad de detalles y detectar cualquier dispositivo o software que esté ocasionando problemas.

Esta herramienta es de gran utilidad además para conocer a fondo el funcionamiento de Windows y sus componentes. De paso proporciona acceso a casi todas las herramientas de chequeo y reparación del sistema.

Se lanza desde **Inicio/Programas/Accesorios/Herramientas del Sistema/Información del Sistema** o también desde **Inicio/Ejecutar/msinfo32**).

Programa de configuración del sistema de Windows.

El "Programa de configuración del sistema" (Msconfig.exe) automatiza los pasos de la solución de problemas con la configuración de Windows. Este programa permite modificar la configuración del sistema mediante un proceso de eliminación utilizando casillas de verificación, lo cual reduce el riesgo de errores de escritura.

Para iniciar "msconfig" vaya a **Inicio/Ejecutar/msconfig**

Copia de seguridad de los archivos del sistema

Este programa también puede crear copias de seguridad de los archivos del sistema antes de comenzar la sesión de solución de problemas. Es interesante crear copias de seguridad de los archivos del sistema para asegurarse de que se pueden deshacer las modificaciones efectuadas durante la sesión de solución de problemas. Para ello, haga clic en la ficha **General**, en **Crear copia de seguridad** y después en **Avanzado**.

Crear un entorno limpio para solucionar problemas

Para crear un entorno limpio para solucionar problemas haga clic en **Inicio de diagnósticos: cargar interactivamente controladores de dispositivos y software**, haga clic en **Aceptar** y, a continuación, haga clic en **Sí** para reiniciar el equipo.

El menú de inicio de Windows aparecerá en modo de “línea de comandos” cuando se reinicie el equipo. Seleccione **Confirmación paso a paso** de las opciones de menú y procese todos los archivos salvo el Config.sys y el Autoexec.bat. Si esta opción hace que el equipo deje de responder, reinicielo, seleccione **Confirmación paso a paso** de nuevo y procese todos los archivos salvo el Autoexec.bat. Algunos equipos no se inician adecuadamente sin procesar el archivo Config.sys. Después de iniciar Windows determine si aún están presentes los síntomas.

Comprobador de archivos de sistema.

Puede usar el **Comprobador de archivos de sistema** para verificar la integridad de los archivos del sistema operativo, para restaurarlos si están dañados, y para extraer archivos comprimidos (como los controladores) desde los discos de instalación.

Es muy conveniente que haga copia de seguridad de los archivos existentes antes de restaurar los archivos originales, para ello puede utilizar esta misma herramienta.

Para utilizar este programa vaya a **Inicio/Programas/Accesorios/Herramientas del sistema/Información del sistema**. Desde ese programa utilice **Herramientas/Comprobador de archivos de sistema**. También puede usar **Inicio/Ejecutar/sfc**.

Comprobador del registro.

El sistema mantiene siempre una copia de seguridad de la configuración del registro (incluyendo la información de la cuenta de usuario, los enlaces de protocolo, la configuración del programa de software, y las preferencias del usuario). Puede usar la copia de seguridad si el registro actual encuentra algún problema.


Cada vez que reinicia el equipo, el **Comprobador del registro** explora automáticamente el registro. Si nota un problema, reemplaza automáticamente el registro con la copia de seguridad. Si el registro contiene alguna entrada que haga referencia a un archivo que ya no existe (como por ejemplo un archivo .vxd), no será corregido por el Comprobador del registro.

También es conveniente utilizar este programa para actualizar la copia de seguridad del registro antes de instalar nuevo software o hardware.

Para utilizar este programa vaya a **Inicio/Programas/Accesorios/Herramientas del sistema/Información del sistema**. Desde ese programa utilice **Herramientas/Comprobador del registro**. También puede usar **Inicio/Ejecutar/Scanreg**.

9.2. Recuperación de archivos del sistema.

A veces al eliminar un virus de nuestro ordenador o debido a un mal cierre del sistema podemos perder algún archivo necesario para el funcionamiento normal de este, si tenemos un equipo con la misma versión del sistema operativo cerca podemos simplemente buscar el archivo en el otro equipo y transferirlo al nuestro mediante un disquete.

Un método más sencillo puede ser buscar los archivos en los ficheros .CAB del CD-ROM de instalación de Windows. En principio puede representar un problema averiguar en que fichero .CAB concreto se encuentra el archivo que necesitamos pero emos para ello este pequeño truco.

1. Pulsamos **Inicio, Buscar, Archivos y carpetas**.
2. Pedimos archivos con la extensión .CAB.
3. Que contengan el texto... y ahí ponemos los archivos que estamos buscando (por ejemplo cool.dll)
4. Ponemos como ruta nuestro CD-ROM o nuestro disco duro y obtendremos el fichero .CAB que hemos de abrir para obtener nuestra presa.
5. Hacemos doble clic sobre el fichero .CAB para que se muestre su contenido y arrastramos el fichero que buscábamos a la localización donde debería estar.

9.3. Referencias.

- <http://www.sarc.com>
- <http://www.annoyances.org>
- <http://www.antivirus.com>

10. Apéndices.

- Historia de Windows.
- Disco duro.
- Protocolos TCP/IP.
- Windows XP sobrevivir al primer día.

10.1. Historia de Windows

Windows 1.0

En 1985 Microsoft publicó la primera versión de Windows (Windows 1.0), una interfaz gráfica de usuario (GUI) para su propio sistema operativo (MS-DOS) que había sido incluido en el IBM PC y ordenadores compatibles desde 1981. La interfaz gráfica fue creada después del MacOS de Apple. La primera versión de Microsoft Windows nunca fue demasiado potente, ni tampoco se hizo popular. Estaba duramente limitada debido a los recursos legales de Apple. Por ejemplo, las ventanas sólo podían disponerse en mosaico sobre la pantalla; esto es, nunca podían solaparse u ocultarse unas a otras. Tampoco había "papelera de reciclaje" debido a que Apple creía que ellos tenían la patente de este paradigma o concepto. Ambas limitaciones fueron eliminadas cuando el recurso de Apple fue rechazado en los tribunales. Por otro lado, los programas incluidos en la primera versión eran aplicaciones "de juguete" con poco atractivo para los usuarios profesionales.

Microsoft Windows 2.0

Microsoft Windows 2 salió en 1987, y fue un poco más popular que la versión inicial. Gran parte de esta popularidad la obtuvo de la inclusión en forma de versión "run-time" de nuevas aplicaciones gráficas de Microsoft, Microsoft Excel y Microsoft Word para Windows. Éstas podían cargarse desde MS-DOS, ejecutando Windows a la vez que el programa, y cerrando Windows al salir de ellas. Windows 2 todavía usaba el modelo de memoria 8088 y por ello estaba limitado a 1 megabyte de memoria, sin embargo mucha gente consiguió hacerlo funcionar bajo sistemas multitareas como DesqView.

Windows 3.0

La primera versión realmente popular de Windows fue la versión 3.0, publicada en 1990. Ésta se benefició de las mejoradas capacidades gráficas para PC de esta época, y también del procesador microprocesador 80386 que permitía mejoras en las capacidades multitarea de las aplicaciones Windows. Esto permitiría incluso ejecutar en modo multitarea viejas aplicaciones basadas en MS-DOS. Windows 3 convirtió al IBM PC en un serio competidor para el Apple Mac.

OS/2 1

Durante la segunda mitad de los 80, Microsoft e IBM habían estado desarrollando conjuntamente OS/2 como sucesor del DOS, para sacar el máximo provecho a las capacidades del procesador Intel 80286. OS/2 utilizaba el direccionamiento hardware de memoria disponible en el Intel 80286 para poder utilizar hasta 16 M de memoria. La mayoría de los programas de DOS estaban por el contrario limitados a 640 K de memoria. OS/2 1.x también soportaba memoria virtual y multitarea. Más adelante IBM añadió, en una de las primeras versiones de OS/2 un sistema gráfico llamado Presentation Manager (PM). Aunque en muchos aspectos era superior a Windows, su API (Programa de Interfaz

de Aplicaciones) era incompatible con la que usaban los programas Windows. (Entre otras cosas, Presentation Manager localizaba el eje de coordenadas X, Y en la parte inferior izquierda de la pantalla como las coordenadas cartesianas, mientras que Windows situaba el punto 0,0 en la esquina superior izquierda de la pantalla como otros sistemas informáticos basados en ventanas). A principio de los 90, crecieron las tensiones en la relación entre IBM y Microsoft. Cooperaban entre si en el desarrollo de sus sistemas operativos para PC y cada uno tenía acceso al código del otro. Microsoft quería desarrollar Windows aún más, mientras IBM deseaba que el futuro trabajo estuviera basado en OS/2. En un intento de resolver estas diferencias, IBM y Microsoft acordaron que IBM desarrollaría OS/2 2.0 para reemplazar a OS/2 1.3 y Windows 3.0, mientras Microsoft desarrollaría un nuevo sistema operativo, OS/2 3.0, para suceder más adelante a OS/2 2.0. Este acuerdo pronto fue dejado de lado y la relación entre IBM y Microsoft terminó. IBM continuó desarrollando IBM OS/2 2.0 mientras que Microsoft cambió el nombre de su (todavía no publicado) OS/2 3.0 a Windows NT. (Microsoft promocionó Windows NT con tanto éxito que la mayoría de la gente no se dio cuenta de que se trataba de un OS/2 remozado.) Ambos retuvieron los derechos para usar la tecnología de OS/2 y Windows desarrollada hasta la fecha de terminación del acuerdo.

OS/2 2.0

IBM publicó OS/2 versión 2.0 en 199x. Esta versión suponía un gran avance frente a OS/2 1.3. Incorporaba un nuevo sistema de ventanas orientado a objetos llamado Workplace Shell como sustituto del Presentation Manager, un nuevo sistema de ficheros, HPFS , para reemplazar al sistema de ficheros FAT de DOS usado también en Windows y aprovechaba todas las ventajas de las capacidades de 32 bit del procesador Intel 80386. También podía ejecutar programas DOS y Windows, ya que IBM había retenido los derechos para usar el código de DOS y Windows como resultado de la ruptura.

Windows 3.1 y Windows 3.11

En respuesta a la inminente aparición de OS/2 2.0, Microsoft desarrolló Windows 3.1, que incluía diversas pequeñas mejoras a Windows 3.0 (como las fuentes escalables TrueType), pero que consistía principalmente en soporte multimedia. Más tarde Microsoft publicó también Windows 3.11 (denominado Windows para trabajo en grupo), que incluía controladores y protocolos mejorados para las comunicaciones en red y soporte para redes punto a punto.

Windows NT

Mientras tanto Microsoft continuó desarrollando Windows NT. Para ello reclutaron a Dave Cutler, uno de los jefes analistas de VMS en Digital Equipment Corporation (hoy parte de Compaq) para convertir NT en un sistema más competitivo. Cutler había estado desarrollando un sucesor del VMS en DEC (Digital Equipment Corporation) llamado Mica, y cuando DEC abandonó el proyecto se llevó sus conocimientos y algunos ingenieros a Microsoft. DEC también creyó que se llevaba el código de Mica a Microsoft y entabló una demanda. Microsoft finalmente pagó 150 millones de dólares y acordó dar soporte al microprocesador Alpha de DEC en NT. Siendo un sistema operativo completamente nuevo

Windows NT sufrió problemas de compatibilidad con el hardware y el software existentes. También necesitaba gran cantidad de recursos y éstos estaban solamente disponibles en equipos grandes y caros. Debido a esto muchos usuarios no pudieron pasarse a Windows NT. La interfaz gráfica de NT todavía estaba basada en la de Windows 3.1 que era inferior a la Workplace Shell de OS/2.

Windows 95 - Desarrollo

En respuesta a ello Microsoft comenzó a desarrollar un sucesor para Windows 3.1 cuyo nombre clave era Chicago. Chicago iba encaminado a incorporar una nueva interfaz gráfica que compitiera con la de OS/2. También se pretendía introducir arquitectura de 32 bits y dar soporte a multitarea preventiva, como OS/2 o el mismo Windows NT. Sin embargo sólo una parte de Chicago comenzó a utilizar arquitectura de 32 bits, la mayor parte siguió usando una arquitectura de 16 bits, Microsoft argumentaba que una conversión completa retrasaría demasiado la publicación de Chicago y sería demasiado costosa. Microsoft desarrolló una nueva API para remplazar la API de Windows de 16 bits. Esta API fue denominada Win32, desde entonces Microsoft denominó a la antigua API de 16 bits como Win16. Esta API fue desarrollada en tres versiones: una para Windows NT, una para Chicago y otra llamada Win32s, que era un subconjunto de Win32 que podía ser utilizado en sistemas con Windows 3.1. De este modo Microsoft intentó asegurar algún grado de compatibilidad entre Chicago y Windows NT, aunque los dos sistemas tenían arquitecturas radicalmente diferentes.

Windows NT 3.1

Windows NT 3.1 (la estrategia de marketing de Microsoft era que Windows NT pareciera una continuación de Windows 3.1) apareció en su versión beta para desarrolladores en la Conferencia de Desarrolladores Profesionales de Julio de 1992 en San Francisco. Microsoft anunció en la conferencia su intención de desarrollar un sucesor para Windows NT y Chicago (que aún no había sido lanzada). Este sucesor habría de unificar ambos sistemas en uno sólo y su nombre clave era Cairo. (Visto en retrospectiva Cairo fue un proyecto más difícil de lo que Microsoft había previsto y como resultado NT y Chicago no sería unificados hasta la aparición de Windows XP.

Windows 95 - Lanzamiento

Microsoft adoptó "Windows 95" como nombre de producto para Chicago cuando fue publicado en Agosto de 1995. Aunque compartía mucho código con Windows 3 e incluso con MS-DOS, Windows 95 tenía dos grandes ventajas para el consumidor medio. Primero, aunque su interfaz todavía corría sobre MS-DOS, tenía una instalación integrada que le hacía aparecer como un solo sistema operativo: uno ya no necesitaba comprar MS-DOS e instalar Windows encima. Segundo, introducía un subsistema en modo protegido que estaba especialmente escrito a procesadores 80386 o superiores, lo cual impediría que las nuevas aplicaciones Win32 dañaran el área de memoria de otras aplicaciones Win32. En este respecto Windows 95 se acercaba más a Windows NT.

OS/2 3.0 y 4.0

IBM continuó vendiendo OS/2, produciendo versiones posteriores como OS/2 3.0 y 4.0 (también llamado Warp). Pero con la llegada de Windows 95 OS/2 comenzó a perder cuota de mercado. Aunque OS/2 seguía corriendo aplicaciones de Windows 3.0 carecía de soporte para las nuevas aplicaciones que requerían Windows 95. Al contrario que con Windows 3.0, IBM no tenía acceso al código fuente de Windows 95; y tampoco tenía el tiempo ni los recursos necesarios para emular el trabajo de los programadores de Microsoft con Windows 95.

Windows NT 4.0

Después de la aparición de Windows 95, Windows NT continuaba usando la interfaz de Windows 3.1. Entonces Microsoft publicó Windows NT 4.0 que tenía la nueva interfaz de Windows 95 pero sobre Windows NT.

Windows 98

El 25 de Junio de 1998 llegó Windows 98, que era una revisión menor de Windows 95. Incluía nuevos controladores de hardware y el sistema de ficheros FAT 32 que soportaba particiones mayores a los 2 GB permitidos por Windows 95.

Windows 98 Second Edition

En 1999 Microsoft sacó al mercado Windows 98 Second Edition, cuya característica más notable era la capacidad de compartir entre varios equipos una conexión a Internet a través de una sola línea telefónica.

Windows Millennium Edition

En 2000 Microsoft introdujo Windows ME que era una copia de Windows 98 con más aplicaciones añadidas. Windows ME fue un proyecto rápido de un año para rellenar el hueco entre Windows 98 y el nuevo Windows XP.

Windows 2000

En este mismo año vio la luz Windows 2000, una nueva versión de Windows NT muy útil para los administradores de redes y con una gran cantidad de servicios de red.

Windows XP

La unión de Windows NT/2000 y Windows 3.1/95/98/SE se alcanzó con Windows XP liberado en 2001 en su versión Home y Professional. Windows XP usa el kernel o núcleo de Windows NT.

Progresión de MS-DOS:

- MS-DOS
- Windows 1.0
- Windows 2.0
- Windows 3.0
- Windows 3.1
- Windows 3.11
- Windows 95
- Windows 95 OSR2
- Windows 98
- Windows 98 SE
- Windows ME

Progresión de OS/2:

- OS/2 1.3
- OS/2 2.0
- NT 3.1
- NT 3.5
- OS/2 3.0
- OS/2 4.0
- NT 3.51
- NT 4.0
- Windows 2000
- Windows XP

10.2. Disco duro.

Dispositivo de almacenamiento masivo de datos utilizado en ordenadores. Se caracterizan por su gran capacidad de almacenamiento y la alta velocidad de lectura y escritura.

Un disco duro es una caja herméticamente cerrada en cuyo interior se disponen una serie de platos metálicos apilados girando a gran velocidad. Cada plato está recubierto por sus dos caras con una capa magnética que es la que almacena los datos contenidos en el disco. Sobre estos platos se desplazan unos brazos con unos cabezales o cabezas en sus extremos que son los encargados de leer o escribir impulsos magnéticos en el disco duro.

Hay distintos estándares a la hora de fabricar un disco duro, los más utilizados son IDE y SCSI.

Cabezas, cilindros y sectores.

Cada una de las superficies magnéticas de un plato se denomina *cara*. El número total de caras de un disco coincide con el número de *cabezas* pues cada cabeza se encarga de leer los datos de una única cara del disco.

Cada una de las caras se divide en anillos concéntricos llamados *pistas*. Se utiliza el término *cilindro* para referirse a la misma pista de todos los discos de la pila.

Por último los *sectores* son las unidades mínimas de información que puede leer o escribir un disco duro. El número de sectores de un disco suele darse como sectores por pista. Generalmente su tamaño es de 512 bytes.

La geometría de un disco duro se define en función del número de cilindros, cabezas y sectores. Con estos parámetros obtendremos la capacidad de almacenaje de información (o "tamaño") del disco duro.

Tomemos como ejemplo un disco duro con 6253 cilindros (6253 pistas por cara), 16 cabezas (8 platos x 2 caras) y 63 sectores (63 sectores por pista):

$$6252 * 16 * 163 = 6.303.024 \text{ sectores}$$

$$6.303.024 * 512 \text{ bytes/sector} = 3.227.148.228 \text{ bytes (aprox. } \cdot 3 \text{ GB)}$$

Particiones y formato.

Tal como sale de fábrica el disco duro no puede ser utilizado por un sistema operativo. Primero tendrá que ser formateado a "bajo nivel", luego tenemos que definir en él una o más particiones y por fin aplicaremos un formato lógico o "de alto nivel" que pueda ser entendido por nuestro sistema operativo.

Referencias.

- Saulo Barajas; *Discos duros y particiones*; consultado el 26/01/2002; <http://www.saulo.net/pub/ddypart/> Inmejorable tratado sobre discos duros y particiones.

- José Manuel Tella Llop; *Disco duro y particiones*;
http://www.multingles.net/docs/disco_duro_y_particiones.htm Una buena explicación de lo que es un disco duro, como funciona y como trabajar mejor con él.
- Julio César Chávez; *Disco duro*;
<http://www.monografias.com/trabajos/discoduro/discoduro.shtml>

10.3. Protocolos TCP/IP.

Protocolos de comunicaciones.

Los protocolos que se utilizan en las comunicaciones son una serie de normas que deben aportar las siguientes funcionalidades:

- Permitir localizar un ordenador de forma inequívoca.
- Permitir realizar una conexión con otro ordenador.
- Permitir intercambiar información entre ordenadores de forma segura, independiente del tipo de maquinas que estén conectadas (PC, Mac, AS-400...).
- Abstracter a los usuarios de los enlaces utilizados (red telefónica, radio enlaces, satélite...) para el intercambio de información.
- Permitir liberar la conexión de forma ordenada.

Debido a la gran complejidad que conlleva la interconexión de ordenadores, se ha tenido que dividir todos los procesos necesarios para realizar las conexiones en diferentes niveles. Cada nivel se ha creado para dar una solución a un tipo de problema particular dentro de la conexión. Cada nivel tendrá asociado un protocolo, el cual entenderán todas las partes que formen parte de la conexión.

Diferentes empresas han dado diferentes soluciones a la conexión entre ordenadores, implementando diferentes familias de protocolos, y dándole diferentes nombres (DECnet, TCP/IP, IPX/SPX, NETBEUI, etc.).

¿Qué es TCP/IP?.

Cuando se habla de TCP/IP, se relaciona automáticamente como el protocolo sobre el que funciona la red Internet. Esto, en cierta forma es cierto, ya que se le llama TCP/IP, a la familia de protocolos que nos permite estar conectados a la red Internet. Este nombre viene dado por los dos protocolos estrella de esta familia:

- El protocolo TCP, funciona en el nivel de transporte del modelo de referencia OSI, proporcionando un transporte fiable de datos.
- El protocolo IP, funciona en el nivel de red del modelo OSI, que nos permite encaminar nuestros datos hacia otras maquinas.

Pero un protocolo de comunicaciones debe solucionar una serie de problemas relacionados con la comunicación entre ordenadores, además de los que proporciona los protocolos TCP e IP.

Arquitectura de protocolos TCP/IP.

Para poder solucionar los problemas que van ligados a la comunicación de ordenadores dentro de la red Internet, se tienen que tener en cuenta una serie de particularidades sobre las que ha sido diseñada TCP/IP:

- Los programas de aplicación no tienen conocimiento del hardware que se utilizara para realizar la comunicación (módem, tarjeta de red...)
- La comunicación no esta orientada a la conexión de dos maquinas, eso quiere decir que cada paquete de información es independiente, y puede viajar por caminos diferentes entre dos maquinas.
- La interfaz de usuario debe ser independiente del sistema, así los programas no necesitan saber sobre que tipo de red trabajan.
- El uso de la red no impone ninguna topología en especial (distribución de los distintos ordenadores).

De esta forma, podremos decir, que dos redes están interconectadas, si hay una maquina común que pase información de una red a otra. Además, también podremos decir que una red Internet virtual realizara conexiones entre redes, que ha cambio de pertenecer a la gran red, colaboraran en el trafico de información procedente de una red cualquiera, que necesite de ella para acceder a una red remota. Todo esto independiente de las maquinas que implementen estas funciones, y de los sistemas operativos que estas utilicen.

Descomposición en niveles de TCP/IP.

Toda arquitectura de protocolos se descompone en una serie de niveles, usando como referencia el modelo OSI. Esto se hace para poder dividir el problema global en subproblemas de más fácil solución.

Al diferencia de OSI, formado por una torre de siete niveles, TCP/IP se descompone en cinco niveles, cuatro niveles software (aplicación, transporte, red y enlace) y un nivel hardware. A continuación pasaremos a describir los niveles software, los cuales tienen cierto paralelismo con el modelo OSI.

Nivel de aplicación.

Constituye el nivel mas alto de la torre TCP/IP. A diferencia del modelo OSI, se trata de un nivel simple en el que se encuentran las aplicaciones que acceden a servicios disponibles a través de Internet. Estos servicios están sustentados por una serie de protocolos que los proporcionan. Por ejemplo, tenemos el protocolo FTP (File Transfer Protocol), que proporciona los servicios necesarios para la transferencia de ficheros entre dos ordenadores.

Otro servicio, sin el cual no se concibe Internet, es el de correo electrónico, sustentado por el protocolo SMTP (Simple Mail Transfer Protocol).

Nivel de transporte.

Este nivel proporciona una comunicación extremo a extremo entre programas de aplicación. La maquina remota recibe exactamente lo mismo que le envió la maquina origen. En este nivel el emisor divide la información que recibe del nivel de aplicación en paquetes, le añade los datos necesarios para el control de flujo y control de errores, y se los pasa al nivel de red junto con la dirección de destino.

En el receptor este nivel se encarga de ordenar y unir las tramas para generar de nuevo la información original.

Para implementar el nivel de transporte se utilizan dos protocolos:

- **UDP:** proporciona un nivel de transporte no fiable de datagramas, ya que apenas añade información al paquete que envía al nivel inferior, solo la necesaria para la comunicación extremo a extremo. Lo utilizan aplicaciones como NFS y RPC, pero sobre todo se emplea en tareas de control.
- **TCP (Transport Control Protocolo):** es el protocolo que proporciona un transporte fiable de flujo de bits entre aplicaciones. Esta pensado para poder enviar grandes cantidades de información de forma fiable, liberando al programador de aplicaciones de la dificultad de gestionar la fiabilidad de la conexión (retransmisiones, perdidas de paquete, orden en que llegan los paquetes, duplicados de paquetes,...) que gestiona el propio protocolo. Pero la complejidad de la gestión de la fiabilidad tiene un coste en eficiencia, ya que para llevar a cabo las gestiones anteriores se tiene que añadir bastante información a los paquetes a enviar. Debido a que los paquetes a enviar tienen un tamaño máximo, como mas información añadida el protocolo para su gestión, menos información que proviene de la aplicación podrá contener ese paquete. Por eso, cuando es mas importante la velocidad que la fiabilidad, se utiliza UDP, en cambio TCP asegura la recepción en destino de la información a transmitir.

Nivel de red

También recibe el nombre de **nivel Internet**. Coloca la información que le pasa el nivel de transporte en datagramas IP, le añade cabeceras necesaria para su nivel y lo envía al nivel inferior. Es en este nivel donde se emplea el algoritmo de encaminamiento, al recibir un datagrama del nivel inferior decide, en función de su dirección, si debe procesarlo y pasarlo al nivel superior, o bien encaminarlo hacia otra maquina. Para implementar este nivel se utilizan los siguientes protocolos:

- **IP (Internet Protocol):** es un protocolo no orientado a la conexión, con mensajes de un tamaño máximo. Cada datagrama se gestiona de forma independiente, por lo que dos datagramas pueden utilizar diferentes caminos para llegar al mismo destino, provocando que lleguen en diferente orden o bien duplicados. Es un protocolo no fiable, eso quiere decir que no corrige los anteriores problemas, ni tampoco informa de ellos. Este protocolo recibe información del nivel superior y le añade la información necesaria para su gestión (direcciones IP , checksum)

- **ICMP (Internet Control Message Protocol):** proporciona un mecanismo de comunicación de información de control y de errores entre máquinas intermedias por las que viajan los paquetes de datos. Estos datagramas los suelen emplear las máquinas (gateways, host,...) para informarse de condiciones especiales en la red, como la existencia de una congestión, la existencia de errores y las posibles peticiones de cambios de ruta. Los mensajes de ICMP están encapsulados en datagramas IP.
- **IGMP (Internet Group Management Protocol):** este protocolo está íntimamente ligado a IP. Se emplea en máquinas que emplean IP multicast. El IP multicast es una variante de IP que permite emplear datagramas con múltiples destinatarios.

También en este nivel tenemos una serie de protocolos que se encargan de la resolución de direcciones:

- **ARP (Address Resolution Protocol):** cuando una máquina desea ponerse en contacto con otra que conoce su dirección IP, entonces necesita un mecanismo dinámico que permite conocer su dirección física. Entonces envía una petición ARP por broadcast, o sea, a todas las máquinas. El protocolo establece que solo contestará a la petición, si esta lleva su dirección IP. Por lo tanto solo contestará la máquina que corresponde a la dirección IP buscada, con un mensaje que incluya la dirección física. El software de comunicaciones debe mantener una caché con los pares IP-dirección física. De este modo la siguiente vez que hay que hacer una transmisión a esa dirección IP, ya conoceremos la dirección física.
- **RARP (Reverse Address Resolution Protocol):** a veces el problema es al revés, o sea, una máquina solo conoce su dirección física, y desea conocer su dirección lógica. Esto ocurre, por ejemplo, cuando se accede a Internet con una dirección diferente, en el caso de PC que acceden por módem a Internet, y se le asigna una dirección diferente de las que tiene el proveedor sin utilizar. Para solucionar esto se envía por broadcast una petición RARP con su dirección física, para que un servidor pueda darle su correspondencia IP.
- **BOOTP (Bootstrap Protocol):** el protocolo RARP resuelve el problema de la resolución inversa de direcciones, pero para que pueda ser más eficiente, enviando más información que meramente la dirección IP, se ha creado el protocolo BOOTP. Este además de la dirección IP del solicitante, proporciona información adicional, facilitando la movilidad y el mantenimiento de las máquinas.

Nivel de enlace

Este nivel se limita a recibir datagramas del nivel superior (nivel de red) y transmitirlo al hardware de la red. Pueden usarse diversos protocolos: DLC (IEEE 802.2), Frame Relay, X.25, etc.

La interconexión de diferentes redes genera una red virtual en la que las máquinas se identifican mediante una dirección de red lógica. Sin embargo a la hora de transmitir información por un medio físico se envía y se recibe información de direcciones físicas. Un diseño eficiente implica que una dirección lógica sea independiente de una dirección física,

por lo tanto es necesario un mecanismo que relacione las direcciones lógicas con las direcciones físicas. De esta forma podremos cambiar nuestra dirección lógica IP conservando el mismo hardware, del mismo modo podremos cambiar una tarjeta de red, la cual contiene una dirección física, sin tener que cambiar nuestra dirección lógica IP.

Extraído de: Introducción a las redes de área local;
http://enete.us.es/docu_enete/vari0s/redes/indice.asp

Autores: Federico Reina Toranzo, Juan Antonio Ruiz Rivas.

11. Referencias.

- Referencias en Español.
- Referencias en Inglés.

11.1. Referencias en Español.

Generales.

- Microsoft; *Sitio de soporte*; <http://www.micorosoft.com/spain/support/>
- Microsoft; *Technet en español*;
<http://www.microsoft.com/spain/technet/homepage.asp>
- Microsoft; *Windows 98*; <http://www.microsoft.com/spain/windows98/>
- Federico Reina y Juan Antonio Ruiz; *Enete*; <http://enete.us.es>

Instalación del sistema

- Saulo Barajas; *Discos duros y particiones*; consultado el 26/01/2002;
<http://www.saulo.net/pub/ddypart/> Inmejorable tratado sobre discos duros y particiones.
- José Manuel Tella Llop; *Disco duro y particiones*;
http://www.multingles.net/docs/disco_duro_y_particiones.htm Una buena explicación de lo que es un disco duro, como funciona y como trabajar mejor con él.

Comunicaciones y redes.

- Federico Reina y Juan Antonio Ruiz; *Introducción a las redes de área local*;
http://enete.us.es/docu_enete/varios/redes/indice.asp

Seguridad.

- David Chernicoff; *Copias de seguridad: Estrategias*;
http://www.w2000mag.com/atrasados/1999/33_julago99/articulos/opinion.htm
Artículo ilustrativo y simpático sobre como encarar una estrategia de copias de seguridad.
- *Registro de Windows*;
<http://znet.terra.com.hn/sp/helptips/stories/guides/1,,8015832,00.html> Describe en detalle como y porqué hacer copias de seguridad del registro de Windows.

11.2. Referencias en Inglés.

Generales

- Microsoft; *Support*; <http://support.microsoft.com/> Ayuda y soporte de Microsoft
- *Annoyances.org*; <http://www.annoyances.org/> Como su nombre indica este sitio trata de ayudarnos a sobrellevar las molestias que nos produce Windows

Instalación del sistema.

- Microsoft; *Lista de compatibilidad para Windows 98*; <http://www.microsoft.com/hwtest/hcl>
- HelpDriver; <http://www.helpdrivers.com/espanol/index.htm>
- Download.com; *Drivers (en inglés)*; <http://download.com/2001-2014-0.html?tag=dir>

12. Glosario de términos informáticos

Acceso directo: un icono que está vinculado a un archivo o carpeta. Cuando hace doble clic en un acceso directo, el elemento principal se abre.

Aplicación: programa (normalmente complejo) de ordenador diseñado para cumplir un fin determinado (procesar texto, reproducir sonido, detectar virus,...). Cada aplicación suele tener su carpeta en el disco duro y un icono para ejecutarla.

BIOS: abreviatura de *Basic Input-Output System* (Sistema básico de entrada-salida). Es un chip situado en la placa base del ordenador que controla las interacciones entre el microprocesador y el resto de los componentes básicos del equipo tales como el disco duro o el teclado. Errores o incompatibilidades de la BIOS son causas comunes de los problemas que se encuentran al actualizar a nuevas versiones de Windows.

Bit: la unidad más pequeña de información. Un bit puede tomar dos valores: 0 y 1. Los equipos informáticos trabajan siempre con agrupaciones de 8 bits denominadas bytes.

Byte: Unidad de información formada por ocho bits. Equivalencias: 1024 bytes son iguales a un **kilobyte (KB)**, 1024 kilobytes son iguales a un **megabyte (MB)**, 1024 megabytes son iguales a un **gigabyte (GB)**.

Cluster: unidad mínima en que se divide el disco duro con el sistema de archivos FAT. Cada cluster puede ocupar un número entero de sectores que tiene que ser potencia de 2 (1, 2, 4, 8, 16,...). Todos los cluster de una partición de un disco duro tienen el mismo número de sectores.

Conector RJ45: conector utilizado en el cableado de redes ethernet. Tiene un aspecto parecido a un conector telefónico pero con 8 patillas en lugar de las 4 que tiene este.

Controlador (driver): pequeño programa que hace que un dispositivo hardware pueda interactuar correctamente con el sistema operativo. Es conveniente tener siempre instalados los controladores más específicos y actualizados para aprovechar todas las características del dispositivo y de la manera más eficiente.

CPU (central process unit): unidad de procesamiento central. Este es el dispositivo del ordenador que coordina y dirige al resto. Normalmente la CPU de un ordenador está constituida por un circuito integrado llamado microprocesador.

Disco duro: Dispositivo de almacenamiento masivo de datos utilizado en ordenadores. Se caracterizan por su gran capacidad de almacenamiento y la alta velocidad de lectura y escritura. Más información en **apéndice sobre discos duros**.

Desfragmentación: el proceso de reescribir un archivo a secciones adyacentes de un disco duro. Con el tiempo, partes de un mismo archivo pueden estar fragmentadas (dispersas en diferentes áreas del disco duro). La fragmentación reduce la velocidad del disco. Los

sistemas operativos que sufren este problema suelen incorporar herramientas específicas para realizar esta tarea.

Driver: ver **controlador**.

DVD: disco compacto de alta capacidad. Este disco puede almacenar suficientes datos para una película de duración completa. Debe tener un dispositivo DVD o un reproductor para poder utilizar discos DVD.

Ethernet: norma o estándar (IEEE 802.3) que determina la forma en que los puestos de la red envían y reciben datos sobre el medio físico. Originalmente fue diseñada para enviar datos a 10 Mbps, aunque posteriormente ha sido perfeccionado para trabajar a 100 Mbps o 1 Gbps. Utiliza el protocolo de comunicaciones CSMA/CD (*Carrier Sense Multiple Access / Collision Detect* - Acceso múltiple con detección de portadora y detección de colisiones).

Intranet: una red privada en una organización basada en los mismos servicios y protocolos que Internet (TCP/IP, WWW, FTP, correo electrónico, etc.). Una intranet puede estar conectada a Internet.

Internet: una red mundial de equipos formada por infinidad de redes. Si tiene acceso a Internet, podrá obtener información de escuelas y universidades, gobiernos, empresas e individuos. La base de Internet es el protocolo TCP/IP.

LAN: Red de área local. Un grupo de equipos conectados en red en la misma ubicación.

LINUX: sistema operativo de código libre parecido a UNIX en algunos aspectos.

Memoria RAM (*randomize access memory*): memoria de acceso aleatorio. Es un dispositivo de almacenamiento temporal de datos de acceso muy rápido que la CPU del ordenador utiliza para leer y escribir datos. La memoria suele medirse en bytes.

Microprocesador: circuito electrónico altamente integrado para control computacional, son utilizados como CPU en ordenadores, aunque también pueden encontrarse en otros dispositivos electrónicos complejos como automóviles, impresoras, etc. Los microprocesadores modernos están integrados por millones de transistores y otros componentes empaquetados en una cápsula del tamaño de un sello de correo. Las partes lógicas que componen un microprocesador son, entre otras: unidad aritmético-lógica, registros, unidad de control, memoria y bus de datos. Parámetros significativos de un micro son su ancho de bus, medido en bits y la frecuencia de reloj a la que trabajan, medida en hertzios.

Módem: dispositivo que permite conectarnos a una red (normalmente Internet pero puede ser cualquier otra) utilizando la línea telefónica común. Hay distintos tipos de modem en función de la velocidad de transmisión que alcancen: 14.400, 28.800, 36.600 y 56.600 bps son las más comunes actualmente.

MSDOS: Primer sistema operativo desarrollado por Microsoft para ser utilizado en ordenadores personales (PC). Estaba basado en una interfaz de línea de comandos, o sea el usuario tecleaba una orden y pulsaba la tecla "Enter" para que el sistema la procesara.

PC (*personal computer*): ordenador personal. Con este nombre nos referimos a un tipo especial de ordenador que en principio se concibió para ser utilizado por pequeñas empresas o usuarios particulares, en contraposición a los grandes ordenadores o

mainframes que son utilizados por muchos usuarios simultáneamente y suelen ser propiedad de grandes empresas u organizaciones estatales.

RAM: ver memoria RAM.

Registro de Windows: es la base de datos donde se guarda toda la información sobre la configuración del sistema operativo, hardware instalado, aplicaciones, usuarios y preferencias.

Tarjeta de red: dispositivo que utilizan ordenadores o impresoras para poder acceder a una red local. Hay diversos tipos de adaptadores en función del tipo de cableado que se utilice en la red, pero actualmente el más común es del tipo ethernet utilizando un interfaz o conector rj-45. Las tarjetas de red ethernet pueden variar en función de la velocidad de transmisión, normalmente 10 MB o 10/100 MB. Otro tipo de adaptador muy extendido hasta hace poco era el que usaba conector BNC.

TCP/IP: familia de protocolo de comunicaciones en red utilizado originalmente en sistema UNIX y extendido universalmente por haberse convertido en el protocolo de comunicaciones de Internet. Más información en apéndice sobre **protocolos TCP/IP**.

UNIX: sistema operativo para estaciones de trabajo y servidores

Versiónes de Windows: hasta la fecha de escritura de este documento las versiones de Windows que han aparecido por orden cronológico son: 1.0, 2.0, 3.0, 3.1, 3.11, 95, 95 OSR2, 98, 98 Second Edition (SE) y Millenium Edition (ME). Y las de Windows NT: 3.1, 3.5, 3.51, 4.0, 2000 y XP. Más información en apéndice sobre la **historia de Windows**.

Web: La parte gráfica multimedia de Internet compuesta por millones de páginas web.

13. Hojas de prácticas

- Creando un disquete de arranque.
- Hoja de inventario.
- Trabajando con particiones y formatos.
- Utilizando el "administrador de discos" de Windows.
- Instalando un controlador de dispositivo.
- Configurando TCP/IP en Windows.
- Compartiendo recursos en red.
- Actualizando Windows.
- Realizando una copia de seguridad.
- Haciendo copia de seguridad del registro.
- Cambiando algunas claves del registro.

Creando un disquete de arranque

Hoja de inventario de equipo informático.

Nombre del equipo	
Datos IP (Nº, IP, máscara, encaminador)	
Dominio o grupo de trabajo	
Marca y modelo	
BIOS (fabricante, revisión y fecha)	
Procesador	
Módulos de RAM (número y capacidad)	
Discos duros (marca, modelo y capacidad)	
CD-ROM (marca, modelo, velocidad)	
Tarjeta de red (marca, modelo, chipset, IRQ) / Dirección MAC	
Tarjeta de vídeo (marca, modelo, chipset, IRQ)	
Tarjeta de sonido (marca, modelo, chipset, IRQ)	
Módem (marca, modelo, chipset, IRQ)	
Controladora SCSI (marca, modelo, chipset, IRQ)	
Otros componentes o periféricos	
Observaciones	

Trabajando con particiones y formatos.

Utilizando el "administrador de discos" de Windows.

Instalando un controlador de dispositivo.

Configurando TCP/IP.

Compartiendo recursos en red.

Actualizando Windows.

Realizando una copia de seguridad.

Haciendo copia de seguridad del registro.

Cambiando algunas claves del registro.